

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1473325-000

Total Deleted Page(s) = 166

Page 6 ~ Duplicate;
Page 7 ~ Duplicate;
Page 10 ~ Duplicate;
Page 11 ~ Duplicate;
Page 21 ~ b6; b7C; b7E;
Page 22 ~ b6; b7C; b7E;
Page 23 ~ b6; b7C; b7E;
Page 24 ~ b6; b7C; b7E;
Page 25 ~ b6; b7C; b7E;
Page 26 ~ b6; b7C; b7E;
Page 30 ~ Duplicate;
Page 34 ~ Duplicate;
Page 36 ~ b6; b7C;
Page 38 ~ b3; b6; b7C; b7E;
Page 39 ~ b6; b7C; b7E;
Page 40 ~ b6; b7C; b7E;
Page 41 ~ b6; b7C; b7E;
Page 42 ~ b6; b7C; b7E;
Page 43 ~ b7E;
Page 44 ~ b6; b7C; b7E;
Page 45 ~ b7E;
Page 46 ~ b6; b7C; b7E;
Page 47 ~ b6; b7C; b7E;
Page 48 ~ b6; b7C; b7E;
Page 49 ~ b6; b7C; b7D; b7E;
Page 50 ~ b6; b7C; b7E;
Page 51 ~ b6; b7C; b7E;
Page 52 ~ b6; b7C; b7E;
Page 53 ~ b6; b7C; b7E;
Page 54 ~ b6; b7C; b7E;
Page 55 ~ b6; b7C; b7E;
Page 56 ~ b6; b7C; b7E;
Page 57 ~ b6; b7C; b7E;
Page 58 ~ b6; b7C; b7E;
Page 59 ~ b6; b7C; b7E;
Page 60 ~ b6; b7C; b7E;
Page 61 ~ b6; b7C; b7E;
Page 62 ~ b7E;
Page 63 ~ b6; b7C; b7E;
Page 64 ~ b6; b7C; b7E;
Page 65 ~ b6; b7C; b7E;
Page 66 ~ b6; b7C; b7E;
Page 67 ~ b6; b7C; b7E;
Page 68 ~ b6; b7C; b7E;
Page 69 ~ b6; b7C; b7E;
Page 70 ~ b6; b7C; b7E;
Page 71 ~ b6; b7C; b7E;
Page 72 ~ b6; b7C; b7E;
Page 73 ~ b6; b7C; b7E;
Page 74 ~ b6; b7C; b7E;
Page 75 ~ b3; b6; b7C; b7E;
Page 77 ~ b6; b7C; b7E;
Page 78 ~ b6; b7C; b7E;
Page 79 ~ b6; b7C; b7E;
Page 80 ~ b6; b7C; b7E;
Page 82 ~ b6; b7C; b7E;
Page 83 ~ b6; b7C; b7E;
Page 84 ~ b6; b7C; b7E;
Page 85 ~ Duplicate;
Page 86 ~ Duplicate;
Page 95 ~ Duplicate;
Page 96 ~ Duplicate;
Page 97 ~ Duplicate;
Page 98 ~ Duplicate;
Page 103 ~ Duplicate;
Page 105 ~ Duplicate;
Page 106 ~ Duplicate;

Page 107 ~ Duplicate;
Page 108 ~ Duplicate;
Page 120 ~ b6; b7C; b7E;
Page 121 ~ b6; b7C; b7E;
Page 122 ~ b6; b7C; b7E;
Page 123 ~ b6; b7C; b7E;
Page 124 ~ b6; b7C; b7E;
Page 125 ~ b6; b7C; b7E;
Page 126 ~ Duplicate;
Page 127 ~ b6; b7C; b7E;
Page 128 ~ b6; b7C; b7E;
Page 129 ~ b6; b7C; b7E;
Page 130 ~ b6; b7C; b7E;
Page 131 ~ b6; b7C; b7E;
Page 132 ~ Duplicate;
Page 133 ~ Duplicate;
Page 134 ~ Duplicate;
Page 135 ~ Duplicate;
Page 139 ~ Duplicate;
Page 140 ~ Duplicate;
Page 147 ~ b6; b7C; b7E;
Page 148 ~ b3; b6; b7C; b7E;
Page 149 ~ b6; b7C; b7E;
Page 150 ~ b6; b7C; b7E;
Page 153 ~ b6; b7C; b7E;
Page 154 ~ b6; b7C; b7E;
Page 155 ~ b6; b7C; b7E;
Page 156 ~ b6; b7C; b7E;
Page 157 ~ b6; b7C; b7E;
Page 158 ~ b6; b7C; b7E;
Page 159 ~ b6; b7C; b7E;
Page 160 ~ b6; b7C; b7E;
Page 161 ~ b6; b7C; b7E;
Page 162 ~ b6; b7C; b7E;
Page 163 ~ b6; b7C; b7E;
Page 164 ~ b6; b7C; b7E;
Page 165 ~ b6; b7C; b7E;
Page 166 ~ b6; b7C; b7E;
Page 167 ~ b7E;
Page 168 ~ b6; b7C; b7E;
Page 169 ~ b6; b7C; b7E;
Page 170 ~ b6; b7C; b7E;
Page 174 ~ b6; b7C; b7E;
Page 178 ~ b6; b7C; b7E;
Page 179 ~ b6; b7C; b7E;
Page 180 ~ b6; b7C; b7E;
Page 181 ~ b6; b7C; b7E;
Page 186 ~ b6; b7C; b7E;
Page 187 ~ b6; b7C; b7E;
Page 188 ~ b6; b7C; b7E;
Page 189 ~ b6; b7C; b7E;
Page 192 ~ b6; b7C;
Page 193 ~ b6; b7C;
Page 195 ~ Duplicate;
Page 199 ~ Duplicate;
Page 204 ~ Duplicate;
Page 205 ~ Duplicate;
Page 206 ~ Duplicate;
Page 209 ~ Duplicate;
Page 210 ~ Duplicate;
Page 216 ~ Duplicate;
Page 217 ~ Duplicate;
Page 218 ~ Duplicate;
Page 219 ~ Duplicate;
Page 221 ~ b3; b6; b7C; b7E;
Page 222 ~ b6; b7C; b7E;
Page 224 ~ b3; b6; b7C;
Page 225 ~ b3; b6; b7C;
Page 226 ~ Duplicate;
Page 227 ~ Duplicate;
Page 228 ~ Duplicate;
Page 231 ~ Duplicate;
Page 232 ~ Duplicate;

Page 240 ~ Duplicate;
Page 241 ~ Duplicate;
Page 242 ~ Duplicate;
Page 243 ~ Duplicate;
Page 244 ~ Duplicate;
Page 245 ~ Duplicate;
Page 247 ~ Duplicate;
Page 254 ~ OTHER - Sealed Pursuant to Court Order;
Page 255 ~ OTHER - Sealed Pursuant to Court Order;
Page 256 ~ OTHER - Sealed Pursuant to Court Order;
Page 257 ~ OTHER - Sealed Pursuant to Court Order;
Page 262 ~ b6; b7C; b7E;
Page 263 ~ b6; b7C; b7E;
Page 264 ~ b6; b7C; b7E;
Page 265 ~ b6; b7C; b7E;
Page 266 ~ b6; b7C; b7E;
Page 267 ~ b6; b7C; b7E;
Page 268 ~ b6; b7C; b7E;
Page 271 ~ b6; b7C; b7E;
Page 272 ~ b6; b7C; b7E;
Page 273 ~ b6; b7C; b7E;
Page 274 ~ b6; b7C; b7E;
Page 275 ~ b3; b6; b7C; b7E;
Page 278 ~ b3; b6; b7C; b7E;
Page 283 ~ Duplicate;
Page 286 ~ Duplicate;

XXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXX

SURVEILLANCE LOG -

DIVISION

Date

11/10/98

Page 1 of 2

b3
b6
b7C
b7E

File #

Case Agent

Log Prepared By

 Clear Partly Cloudy Rain Overcast Partly Sunny Sunny

Day of week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

Personnel Involved

b6
b7C
b7E

LOCATIONS COVERED (IN CHRONOLOGICAL ORDER)

L1

L2

L3

L4

L5

L6

SUBJECTS OBSERVED (MALE)

M1

M2

M3

M4

SUBJECTS OBSERVED (FEMALE)

F1

F2

F3

VEHICLES OBSERVED (LICENSE #/YEAR/MAKE/MODEL/COLOR)

V1

V2

V3

V4

V5

DET A 2 1998

b3
b6
b7C
b7D~~WORK COPY~~
~~DO NOT FILE~~
~~DO NOT FILE~~

TELEPHONES USED (NUMBER AND LOCATION)

SURVEILLANCE LOG - [REDACTED] DIVISION
CONTINUATION SHEET

Date 11/10/98 Hours of Coverage [REDACTED] Page 2 of 2

File # [REDACTED] Case Agent [REDACTED] Log Prepared By [REDACTED]

Time	Initial's	Observations	P/A
		Spot check at [REDACTED] At (L-1) revealed no pertinent vehicles.	
		Spot check at [REDACTED] (Lx) showed no pertinent vehicles.	
		Spot check at (L-2) [REDACTED] negative.	
		Spot check at (L-2) [REDACTED] negative.	
		Spot checks at (L-1) & (L-2) negative.	
		Spot check (L-2) negative. FISKE discontinued	

b3
b6
b7C
b7E

b6
b7C
b7E

b6
b7C
b7E

~~DO NOT COPY~~
~~DO NOT FILE~~

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

10/14/98

[REDACTED] System Administrator, Echo
 Communications, 119 Franklin Avenue, New York, NY 10013,
 telephone [REDACTED] was contacted by the interviewing
 agent. After being advised of the purpose of the interview,
 [REDACTED] provided the following information:

b6
b7C

Echo Communications' (Echo) Uniform Resource List (URL)
 is www.echonyc.com. The computer that acts as the server for
 this URL is a [REDACTED] computer, running [REDACTED]

b7E

[REDACTED]
 Echo offers paid membership for anyone interested in its services.
 These services are advertised as a "virtual community". Echo has
 about 1000 active members. All members have access to the server
 via Telnet, and most members access the server in this way.
 Furthermore, all members have access to the file "/etc/passwd".
 Echo maintains about 8 computers on its local network, and about
 4 of those are hosted by Echo for other individuals.

b6
b7C
b7E

[REDACTED] was asked by the interviewing agent if she was
 aware of a file called [REDACTED] on her system. [REDACTED]
 verified that this file did, in fact, exist. She stated that she
 was not aware what the purpose of this file was, as it was not
 used as part of Echo's normal business. She provided the
 interviewing agent a copy of the contents of this file.

b3
b6
b7C
b7E

UPLOADED

WITH/TEXT
 WITH/OUT TEXT
 BY [REDACTED]
 DATE 12-9-98

10/14/98

Investigation on 10/14/98 at New York, NY

File # [REDACTED] Date dictated 10/14/98

by SA [REDACTED]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency;
 it and its contents are not to be distributed outside your agency.

b6
b7C

302

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 10/1/98

[redacted] (Protect Identity), telephone [redacted]
[redacted] contacted the interviewing agent. After being advised of
the identity of the interviewing agent, [redacted] provided the
following information:

The New York Times hack that occurred on September 13,
1998 [redacted]

[redacted]
[redacted] concluded that
he would contact the interviewing agent with any further
information regarding [redacted]

b6
b7C
b7Db6
b7C
b7D

Investigation on 10/1/98 at New York, NY (telephonically)
File # [redacted] Date dictated 10/1/98
by SA [redacted]

b3
b6
b7C
b7E

b3
b6
b7C
b7D
b7E

[Redacted Box]
DEC 03 1998

HHS-DO [Redacted Box]

[Redacted Box]
302

DATE 13-01-98
EXPIRE DATE 13-01-98
EXTENSION 01-01-98
LOCATION CENTRAL

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

11/10/98

[redacted] (Protect Identity), [redacted]

[redacted] telephone [redacted]

[redacted] was contacted by the interviewing agent. After being advised of the identity of the interviewing agent, [redacted] provided the following information:

[redacted] stated that he has been [redacted]

[redacted]

[redacted] continued that [redacted]

[redacted]

[redacted] continued that [redacted]

Investigation on 11/10/98

at [redacted]

File [redacted]

Date dictated

11/10/98

by SA [redacted]

b6
b7C
b7Db6
b7C
b7Db6
b7C
b7Db6
b7C
b7Db3
b6
b7C
b7D
b7E

[redacted]

b3
b7E

Continuation of FD-302 of [redacted], On 11/10/98, Page 2

[redacted] He also stated that [redacted]

b6
b7C
b7D

[redacted]

b6
b7C
b7D

[redacted] concluded that he would be available for further questions.

UPLOADED

FILEDXT

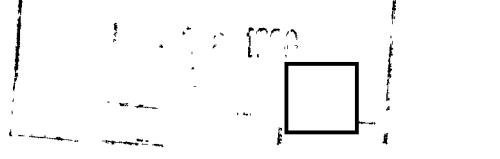
WORD DOC

PDF

DATE 12-9-98



.lead.ec



b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/02/1998

To: [redacted]

Attn: Squad 4

From: New York

C-37

Contact: SA [redacted]

212.384.3187

Approved By: [redacted]

(X) [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]

b3
b6
b7C
b7E

AKA HACKERS FOR GIRLIES (HFG);
NEW YORK TIMES-VICTIM;
CITA;
OO:NY

Synopsis: Set lead to interview [redacted]

regarding [redacted]

b6
b7C

Enclosures: Forbes background article dated on New York Times
hack dated 11/16/98; printouts from [redacted] with a
picture that is believed to be [redacted]
photo and information.

Details: On the morning of September 13, 1998, the New York
Times website (www.nytimes.com) was hacked by a group known as
HACKERS FOR GIRLIES (HFG). The hackers altered the NY TIMES
website with a webpage containing various text messages and
graphic images. As a result, the NY Times took their computers
off-line for approximately nine hours. The hackers erased the
audit logs maintained on the computer.

HFG has claimed responsibility for hacking the New York
Times, NASA, MOTOROLA, PENTHOUSE, ELITEHACKERS.ORG and RT66.COM.
Numerous Confidential Informants (CI's) have advised that [redacted]
[redacted]

b6
b7C

b6
b7C
b7D

To: [REDACTED] From: New York
Re: [REDACTED] 12/02/1998

b3
b6
b7C
b7E

According to [REDACTED]
met [REDACTED] over the Internet. [REDACTED] moved out to [REDACTED] and
[REDACTED] and believed to be in contact with [REDACTED]
[REDACTED] associates with many of the [REDACTED] area hackers including
the [REDACTED]

b6
b7C

LEAD (s) :

Set Lead 1:

[REDACTED]

b6
b7C

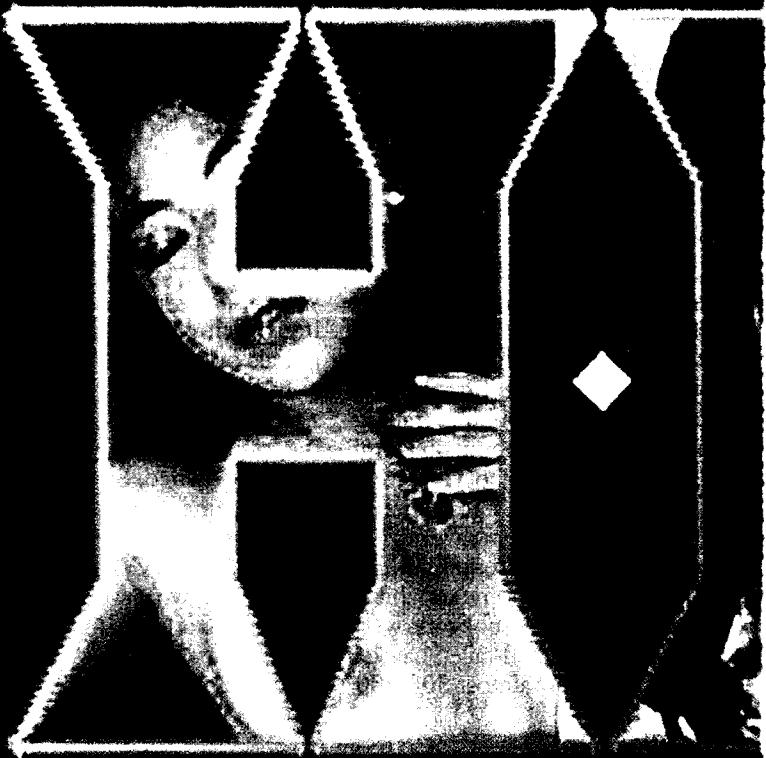
AT [REDACTED]

Interview [REDACTED] about any
knowledge she may have regarding [REDACTED] past hacking
activities, the New York Times hack and HFG. New York plans to
execute search warrants in the [REDACTED] division in the near
future. If possible, NEW YORK request the interview be done the
day the search warrants are executed. NEW YORK will contact
[REDACTED] regarding the date.

♦♦

"We were long gone whe

A Forbes reporter meets with the ringleader of the gang that hacked the New York Times. Here's an inside look into the picaresque underworld of Slut Puppy and Master Pimp.



By Adam L. Penenberg

HACKING F

Slut Puppy and his partner in crime, Master Pimp, hacked the *New York Times* on Sept. 13 because they were bored and couldn't agree on a video to watch.

They are members of the cyberspace gang, "Hacking for Girlies" (HFG), and for six months this year operated out of Slut Puppy's three-room condo, a place so tidy, so clean, it seemed positively un hackerlike. Of course, that didn't mean there were no telltale signs that hackers typed here. The blinds were drawn, the only light source beamed from computer screens. It could just as easily have been 3 a.m. as 3 p.m.

On the condition we protect his anonymity, Slut Puppy agreed to give this FORBES reporter an inside account of the group's hacksplorts.

If you operate on the Internet, you could get hacked. The highwaymen of the Internet are loosely affiliated brotherhood (and sisterhood) of techno-savvy people who make a hobby of puncturing what they regard as the pomposities of society. As far as breaking the law is concerned, they think of themselves as kind of cross between the Scarlet Pimpernel and Robin Hood—harassing people they don't like by thumbing their noses at the law.

Members of the brotherhood took over the *New York Times'* Web site for three hours on that day, replacing the welcome screen with one tinged with nudity and obscenity. In a diatribe Slut Puppy roasted *Times* technology reporter John Markoff for his coverage of imprisoned hacker-martyr Kevin Mitnick.

he pulled the plug"



OR GIRL13Z

To the people at the *New York Times*, the prank was sacrilege. When they discovered the hacked page and were unable to restore their own news content, the Timesters were forced to shut down the site for nine hours. While *Times* technicians located and plugged security holes, the company reported the hack to the FBI. Joseph Valiquette, spokesman for the FBI's New York office, confirmed that the agency's computer crime squad is investigating.

Today the perpetrators are two of the most wanted fugitives in cyberspace.

Although the *Times* prank may have been Hacking for Girlies' most spectacular hack, the newspaper was not its first target. In April of this

year it penetrated Rt66 Internet, an Albuquerque Internet service provider. Over the next four months the gang claimed assaults on, among others, NASA's Jet Propulsion Laboratory, Motorola and *Penthouse* magazine before returning to Rt66 in August.

To penetrate the *Times*, Slut Puppy and Master Pimp employed what is called a remote root buffer overflow. By transmitting too many data into a targeted zone, then tracking and manipulating the characters that could not fit into that space, they were able to trick the system into running their commands as if they were being issued by *New York Times* system administrators.

After wheedling their way inside the server, they pulled down the *Times'* front page and replaced it with one shown in part here, a fake layout that Slut Puppy had composed with two other members of HFG: Sidekick Slappy and Daddy Sweetcakes, both of whom work off-site and communicate with the gang exclusively over the Internet.

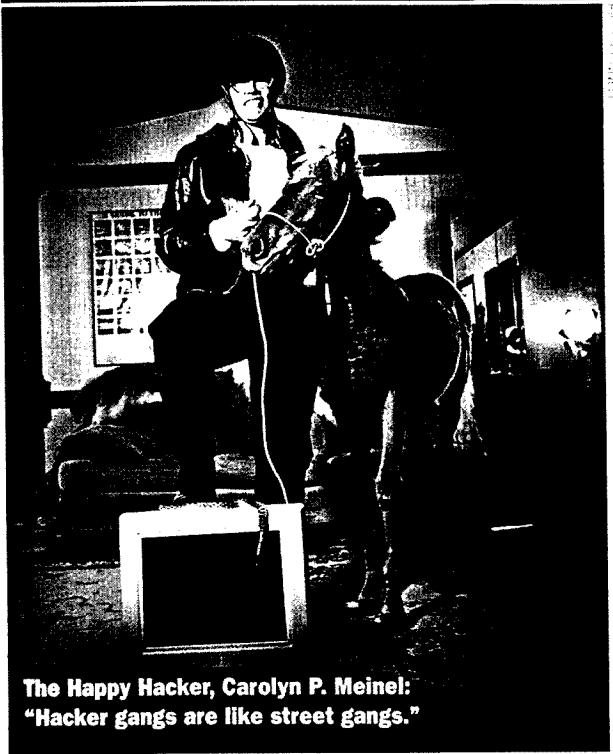
Slut Puppy and Master Pimp were able to control so many functions on the site that when *Times* technicians tried to pull their hacked page and replace it with standard news content, the

hackers, who had logged off by then, used a program that automatically slipped their page back. For almost three hours this went back and forth, until the *Times* took its site off-line. Chortles Slut Puppy, "They seemed to have no idea how we got in—or how to stop us."

On his hacked page Slut Puppy included several pointed references to John Markoff, the *Times* reporter who co-wrote the 1996 book *Takedown*, which detailed the search and capture of Kevin Mitnick, a hacker who faces a 25-count indictment on a variety of computer and wire-fraud charges. Mitnick, whose trial starts in January, has become a martyr to hackers.

Although Slut Puppy knows Mitnick broke the law, he and many other hackers blame Markoff

Slut Puppy's message to the *New York Times* may be obscene, but he insists, "We do have ethics."



The Happy Hacker, Carolyn P. Meinel:
"Hacker gangs are like street gangs."

for hyping Mitnick's crimes in *Takedown*, for which he reportedly shared a \$750,000 advance. The book is also being turned into a movie, which will undoubtedly increase pro-Mitnick protest activities in cyberspace.

Markoff says he loses no sleep over Mitnick, who has already pleaded guilty and served time for possession of unauthorized access codes to cellular phones and for violating parole. "You have to wonder how deep these hackers' thinking goes," Markoff says. "If they have a political cause, they are accomplishing the exact opposite of their goal. No one is doing more to promote the upcoming movie than the hackers themselves."

Markoff wasn't the only one to make it onto HFG's hit list. Carolyn P. Meinel of Cedar Crest, N.M. is its public enemy number one.

Meinel is the author of *The Happy Hacker*, a kind of Hacking for Dummies volume chock-full of folksy golly-gee-isms interspersed with geek talk. The goal of the book is to teach "newbies" how to hack legally. The book's tone irks many of the more sophisticated hackers, who claim to be on a mission to show how porous most computer security is—the law be damned.

And here was Meinel asserting in

public forums that hacker groups were like street gangs, forcing teenage initiates to commit crimes to gain membership. "Meinel has this idea that as the Happy Hacker she is this noble leader among leaders," Slut Puppy says. "But she pretends to know more than she does, so we thought, 'Let's make her life hell.'"

After a cozy Easter Day dinner in April, John Mocho, co-owner of Rt66 Internet, was showing his son and grandson how to upload family photos to his wife's Web site. The hackers had nothing against Rt66. Their target was one of the ISP's customers.

A wholesome family scene turned downright unwholesome when Mocho tried to access his ISP's front page. Instead of the usual welcome screen, he was met with a picture of one of his customers, 52-year-old mother of six Carolyn Meinel, posing on the cover of a fictional publication, "Crack Whore Magazine," as well as her credit card number. A gang Mocho had never heard of, calling itself Hacking for Girlies, claimed responsibility.

While his son rushed his grandson into the next room, Mocho went after the hackers. "I had never been hacked before," he said. "This was my ISP, my customers. I wanted them off as soon as possible."

Mocho launched a preemptive strike. He typed in the Unix command "kill-9," which he assumed would cripple the hackers' ability to issue commands. Seconds later Mocho was booted off his own network.

Figuring there was only one sure way to get rid of them, he jumped into his car and, driving 55 mph in a 30 mph zone, made it to his office in three minutes flat. Mocho cursed the

day he had let his partner, Mark Schmitz, and the ISP's system administrator, Damian Bates, convince him to accept Meinel as a customer. A lightning rod for hackers, she had already been kicked off five other ISPs.

Schmitz and Bates had preached the First Amendment. No one, they argued, should be forced off an ISP because a bunch of hackers didn't like her. Schmitz and Bates also figured their computer security was solid.

They figured wrong, Mocho thought grimly. After gaining entry to his office, Mocho grabbed a network cable and yanked hard. Rt66 was cut off from the Internet. The phone would start taunting Mocho any minute now, with irate customers threatening to switch ISPs.

Mocho estimated that the hackers had been inside the network 20 minutes—30 tops. Enough time to have compromised it. In their haste to leave, however, he surmised that they had left behind a standard "root kit"—software designed to take and maintain control over another's system. This, in his mind, indicated they were amateurs, which cheered him. "From a technical point, this meant they had no magic ship to get in," Mocho said. "They probably compromised a user's account, stole someone's password."

Says Hacking for Girlies ringleader Slut Puppy: "Security was so lax we didn't know they had a firewall installed until we read about it in the New York Times the next day."

What he did not realize was that HFG had not used a root kit; evidently it had been left behind by some other hackers. In fact, HFG had sailed in undetected on that magic ship Mocho was so sure wasn't there, burrowed deep inside millions of lines of ISP code.

It took Mocho and company 20 hours to get Rt66 up and running again. During this process someone either missed a machine or inadvertently installed a snapshot of the hacked

system by accident. For whatever reason, the back door HFG had slipped in through remained open. Using that same flight path, Hacking for Girlies would return to Rt66 in August.

But long before reattacking Rt66, the hackers maintained continual access to the system: sifting through customers' E-mail, noting any security improvements. Since they despised Meinel, they read all of her mail.

Although Mocho believed the Easter hack was the first time HFG had violated his ISP, Slut Puppy says he took many a joyride through Rt66's servers well before then. It was during one of these jaunts that Slut Puppy noticed that Rt66 was employing a product called Tripwire.

If any files are altered by a hacker, this software is designed to alert the system administrator. But Slut Puppy knew a technique for getting around it. Because Tripwire works by comparing numbers it assigns to each file, all he had to do was adjust the numbers that were already on the system. It's like altering the answers on an exam to match yours, no matter how outlandish they are.

While Slut Puppy hummed "Get your clicks on root 66" and designed the Web page, Master Pimp bounced through some ISPs to camouflage their itinerary. Using the existing back door,

customers and the credit card companies."

Meinel also says the hackers can come after her all they want. "Sure helps me sell more books," she contends.

After the Easter hack, when the ISP was considering tossing her off the network, Meinel swore to Rt66 that the credit card the hackers stole had not come from the ISP's credit card file. Later, Meinel admitted that she had been mistaken. This is key because Rt66 took her word the credit card file had not been breached.

Slut Puppy, on the other hand, was amazed that Rt66 didn't do anything to remove the credit card file from the network after the Easter hack.

So, on Aug. 7 Slut Puppy and Master Pimp, entering Rt66's servers the same way they did in April, made off with the whole customer credit card file—1,749 card numbers in all.

"It was so easy getting back into their system with the same back door, we wondered if they had set a trap," Slut Puppy said.

This hack not only resulted in the ISP shutting down for some 60 hours but also forced Rt66 to rebuild its security from scratch.

What is unfortunate is that Rt66, by doing the right thing in alerting the FBI and credit card companies to the security breach, has suffered for its good deeds. Even with its rebuilt security—Rt66 is now one of the most secure ISPs in New Mexico—the ISP has lost 15% of its 5,000 or so members since the August hack.

"I respect the hackers' skills," Rt66 system administrator Bates grumbles, "although I didn't appreciate the obnoxious way they demonstrated them."

Internet Security Systems (ISS) of Atlanta, Ga., one of the big names in computer security, has donated a remote monitoring station for the Rt66 network. ISS hopes to trap Hack-

ing for Girlies the next time it tries to invade the system.

But Slut Puppy already knew about ISS' presence in Rt66 from one of his many well-placed sources. "Needless to say, we don't plan on returning anytime soon," he says.

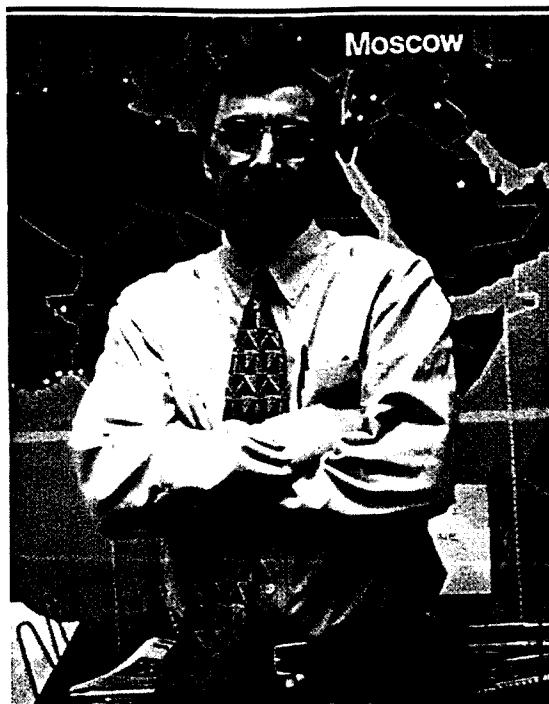
Of course, Slut Puppy knew that hacking the *New York Times* was a lot riskier than attacking Rt66—the newspaper has immense clout in Washington, D.C. The day after the *Times* hack, Slut Puppy and Master Pimp packed up the computers used in their hack spree and passed them on to others for safekeeping. Any data gleaned from their other crimes were either deleted or protected by powerful 1,024-bit encryption.

"Even we don't know where all of the equipment is," Slut Puppy says. "And my password to the encryption is probably unbreakable, too, since it is more than 40 characters long, case-sensitive, and combines letters, numbers and symbols. We've planned not just for the day the FBI comes—we've even planned for a hostile raid where the Feds actually plant evidence."

The group plans to lie low until law enforcement moves on to bigger and better cases. By the way, whence the name Hacking for Girlies? "Chicks dig hacking," explains Slut Puppy.

MOSCOW

THE SEATTLE TIMES



Times reporter John Markoff: "Sure, I was pissed."

"We've planned not just for the day the FBI comes—we've even planned for a hostile raid where the Feds actually plant evidence."

Master Pimp typed in a keyword and within ten seconds had control of one of Rt66's servers. From there he traversed over to the system's powerhouse, "Mack," where Slut Puppy replaced Rt66's home page with HFG's.

"Rather than continuing the gunfight, we cleaned up our tracks by erasing logs and left," Slut Puppy said. "We were long gone when he pulled the plug."

As it happens, Meinel says that on a personal level the hackers "have hardly done any harm to me. They hurt bystanders. They harm the ISPs, their

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/02/1998

To: [redacted]

Attn: SA [redacted]

From: New York

C-37

Contact: SA [redacted]

212.384.3187

(X) [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]

b6
b7C

AKA HACKERS FOR GIRLIES (HFG);
NEW YORK TIMES-VICTIM;
CITA;
OO:NY

Synopsis: Set lead to interview [redacted]
regarding HACKERS FOR GIRLIES and the New York Times hack.

b6
b7C

Reference: Numerous calls between SA [redacted] and SA [redacted]

Details: On the morning of September 13, 1998, the New York Times website (www.nytimes.com) was hacked by a group known as HACKERS FOR GIRLIES (HFG). The hackers altered the NY TIMES website with a webpage containing various text messages and graphic images. As a result, the NY Times took their computers off-line for approximately nine hours. The hackers [redacted]
[redacted]

b6
b7C
b7D
b7E
b3

HFG has claimed responsibility for hacking the New York Times, NASA, MOTOROLA, PENTHOUSE, ELITEHACKERS.ORG and RT66.COM. Numerous Confidential Informants (CI's) have indicated that [redacted]
[redacted]

ROUTINE
FBI-NY
12-9-98

file # [redacted]
DEC 03 1998

FBI-BJ

b3
b6
b7C
b7E

To: [REDACTED] From: New York
Re: [REDACTED] 12/02/1998

b3
b6
b7C
b7E

LEAD (s) :

Set Lead 1:

[REDACTED]

b6
b7C

AT [REDACTED] WASHINGTON

Interview and polygraph [REDACTED]
about any knowledge he may have regarding the New York Times hack
and HFG. New York plans to execute search warrants in the
[REDACTED] division in the near future. If possible, NEW YORK
request the interview be done the day the search warrants are
executed. NEW YORK will contact [REDACTED] division regarding the
date.

♦♦

7/26

Upload# _____

Initials/Date

Case Agt: 12/4/98
Desk
Searched
Serialized 12/4/98
Indexed
Filed 12/4/98

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/16/98

Source, who is not in a position to testify, provided the following information:

HACKING FOR GIRLS (HFG,) a computer hacking group believed to be responsible for the recent NEW YORK TIMES web page hack,

b7D

Investigation on 09/16/98 at N/A
File # dictated
by SA

b3
b6
b7C
b7D
b7E

SURVEILLANCE LOG - [REDACTED] DIVISION

b3
b6
b7C
b7E

Date 11-24-98 Hours of Coverage [REDACTED] Page 1 of 2

File # [REDACTED] Case Agent [REDACTED] Log Prepared By [REDACTED]

Clear Partly Cloudy Rain
 Overcast Partly Sunny Sunny

Day of week
 Monday [REDACTED] Tuesday X Wednesday [REDACTED] Thursday [REDACTED] Friday [REDACTED] Saturday [REDACTED] Sunday [REDACTED]

Personnel Involved [REDACTED]

b6
b7C
b7E

LOCATIONS COVERED (IN CHRONOLOGICAL ORDER)

L1 [REDACTED] 
 L2 [REDACTED]
 L3 [REDACTED]

L4 [REDACTED]

L5 [REDACTED]

L6 [REDACTED]

SUBJECTS OBSERVED (MALE)

M1 [REDACTED]
 M2 [REDACTED]
 M3 [REDACTED]
 M4 [REDACTED]

SUBJECTS OBSERVED (FEMALE)

F1 [REDACTED]
 F2 [REDACTED]
 F3 [REDACTED]

VEHICLES OBSERVED (LICENSE #/YEAR/MAKE/MODEL/COLOR)

V1 [REDACTED]
 V2 [REDACTED]
 V3 [REDACTED]
 V4 [REDACTED]
 V5 [REDACTED]

b3
b6
b7C
b7E

TELEPHONES USED (NUMBER AND LOCATION)

DEC 19 1998
 Modifi [REDACTED] /98

**SURVEILLANCE LOG - [REDACTED] DIVISION
CONTINUATION SHEET**

b3
b6
b7C
b7E

Date

11-24-98

Page 2 of 2

Hours of Coverage

File #

ANSWER

Digitized by srujanika@gmail.com

**Case
Agent**

Log Prepared
By

Time

Initials

Observations:

P/A

BEGIN SURVEILLANCE OF

(L-1) AND

(1-2)

OBSENUĒ

IN PARKING LOT.

V-1 IN PARKING LOT L-1 & L-2.

V-1 IN PARKING LOT L-1 & L-2.

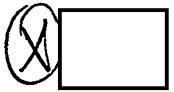
V-1 IN PARKING LOT L-1 & L-2 NO CHANGE ON

ACTIVITY

~~RECORDED~~ ~~SEARCHED~~ ~~INDEXED~~ ~~SERIALIZED~~ ~~FILED~~

F* A * C * S * I * M * I * L * E C * O * V * E * R S * H * E * E * T

The New York Times
electronic media company
1120 Avenue of the Americas
New York, NY 10038



Number of pages (including cover sheet) 2

b6
b7C

FAX TO:	<input type="text"/>
COMPANY NAME:	<u>FBI</u>
FAX NUMBER:	<u>212-384-4660</u>
PHONE NUMBER:	<input type="text"/>

FROM:	<input type="text"/>
PHONE NUMBER:	<input type="text"/>
FAX NUMBER:	<input type="text"/>
SENT BY:	<input type="text"/>

b6
b7C

COMMENTS:

b3
b6
b7C
b7E

[redacted] - here's the info on the ~~the~~ addresses
you gave me. [redacted] [redacted]

If there is any problem with this transmission, please contact send
number. Thank You.

12/1/1998



FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE**Date:** 10-27-98**To:** ADIC, New York**From:** New York**Contact:** SA [redacted] [redacted]b6
b7C

C-37

Approved By: [redacted]**Drafted By:** [redacted]**File Number(s):** 66-8260 SUB D (Pending)**Title:** [redacted]

b7E

Synopsis: SAC and SSA approval for [redacted]**Details:** Writer requests [redacted] to be issued for **no longer than a period of 6 months**, for the following:b6
b7C
b7E

[redacted]

b6
b7C
b7DAUTHORIZATION FOR [redacted]The [redacted] requested is authorized for official Bureau business and must be returned when authorization expires.SAC Signature [redacted]Date: 10-16-98

SSA Signature [redacted]

Date: 10-28-98

SA Signature [redacted]

Date: 10-27-98

[redacted] IS FOR TEMPORARY USE ONLY, NOT TO EXCEED 6 MONTHS

10-27-98

b3
b6
b7C
b7E

[redacted]

b6
b7CDate: 12-10-98Send to FAX Number 212 384-4660**Please deliver the following page(s):**

TO: Special Agent [redacted]
From: [redacted] Records

b6
b7CTotal number of pages including this cover page 4

IF YOU DO NOT RECEIVE ALL OF THE PAGES, PLEASE CALL US BACK AS SOON AS POSSIBLE. Telephone # [redacted]b6
b7C

The information contained in this message is intended only for the addressee or addressee's authorized agent. The message and enclosures may contain information that is privileged, confidential, or otherwise exempt from disclosure. If the reader of this message is not the intended recipient or recipient's authorized agent, then you are notified that any dissemination, distribution or copying of this message is prohibited. If you have received this message in error, please notify the sender by telephone and return the original and any copies of the message by mail to the sender at the address noted above.

b3
b6
b7C*A State Accredited Agency S*

b7E

Date 12-10-98

Birth Credit Criminal Death INS Marriage* Motor Vehicle Other _____

To OPC Buded

Return to SA File number C-37 ext. 3187

Name and aliases of subject, applicant, or employee, and spouse

<u> </u>	<u> </u>
----------	----------

Addresses

Residence

Business

Former

*Date and place of marriage _____
(if applicable) _____

Race <u>W</u>	Sex <input checked="" type="checkbox"/> Male <input type="checkbox"/> Female	Age	Height	Weight	Hair	Eyes
---------------	--	-----	--------	--------	------	------

Birth date Birthplace _____

Arrest Number	Fingerprint classification	Criminal specialty
---------------	----------------------------	--------------------

Social Security Number <u> </u>	Drivers License Number <u> </u>
---------------------------------	---------------------------------

D/L Photo OI

Specific information desired

Results of check

Please
call for pick-up.

Thanks. - 3187

SEARCHED
SERIALIZED
INDEXED
FILED

DEC 11 1998

<u> </u>	<u> </u>
----------	----------

b3
b6
b7C
b7E

b3
b6
b7C
b7E

b6
b7C



b3
b6
b7C
b7E

The following investigation was conducted by squad 17 and documented by Special Agent (SA) [redacted]

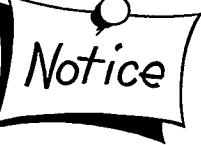
Surveillance Date: 11/24/98
Day: Tuesday
Weather: Sunny

A Physical Surveillance was conducted in the vicinity of [redacted]
[redacted] at which time the following observations were noted:

b6
b7C
b7E

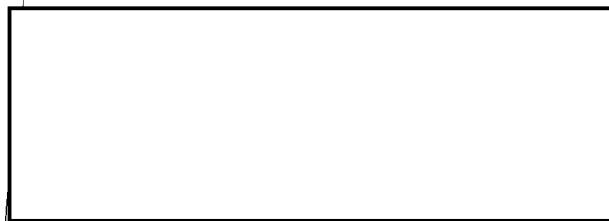
<u>Time</u>	<u>Initials</u>	<u>Observations</u>
[redacted]		Begin surveillance of [redacted] [redacted] (L-1) and [redacted] (L-2), Observe [redacted] [redacted] (V-1) in [redacted] parking lot
		V-1 in parking lot L-1 & L-2
		V-1 in parking lot L-1 & L-2
		V-1 in parking lot L-1 & L-2 no change in activity
		[redacted]

b6
b7C
b7E



Notice

This document
has been uploaded into



b3
b7E

SURVEILLANCE LOG - [REDACTED] DIVISION

b3

b6

b7C

b7E

Date

12-14-98

Page 1 of 3

Hours of Coverage [REDACTED]

File # [REDACTED]

Case Agent [REDACTED]

Log Prepared By [REDACTED]

 Clear Partly Cloudy Rain Overcast Partly Sunny Sunny

Day of week

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

Sunday

b6

b7C

Person [REDACTED]

LOCATIONS COVERED (IN CHRONOLOGICAL ORDER)

L1 [REDACTED]

L2 [REDACTED]

L3 [REDACTED]

L4 [REDACTED]

L5 [REDACTED]

L6 [REDACTED]

b6

b7C

b7E

SUBJECTS OBSERVED (MALE)

M1 [REDACTED]

M2 [REDACTED]

M3 [REDACTED]

M4 [REDACTED]

SUBJECTS OBSERVED (FEMALE)

F1 [REDACTED]

F2 [REDACTED]

F3 [REDACTED]

VEHICLES OBSERVED (LICENSE #/YEAR/MAKE/MODEL/COLOR)

V1 [REDACTED]

V2 [REDACTED]

V3 [REDACTED]

V4 [REDACTED]

V5 [REDACTED]

b3

b6

b7C

b7E

TELEPHONES USED (NUMBER AND LOCATION) [REDACTED]

JAN 05 1999 [REDACTED]

SURVEILLANCE LOG - [REDACTED] DIVISION
CONTINUATION SHEET

Date	[REDACTED]		Hours of Coverage	[REDACTED]	Page 2 of 3
12-14-98	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	b3 b6 b7C b7E
File #	[REDACTED]	Case Agent	[REDACTED]	Log Prepared By	[REDACTED]
Time	Initials	Observations			P/A
<p><i>SURVEILLANCE STARTED AT [REDACTED]</i></p> <p><i>(E-1) AND (V-1) WAS PARKED IN</i></p> <p><i>FRONT OF [REDACTED] V-1 [REDACTED]</i></p> <p><i>(L-2) [REDACTED]</i></p> <p><i>AND (V-2) [REDACTED] LOCATED IN PARKING LOT.</i></p> <p><i>(M-1) w/m, [REDACTED]</i></p> <p><i>GETS INTO V-2 AND DEPARTS L-2.</i></p> <p><i>V-2 ARRIVES AT L-3, [REDACTED]</i></p> <p><i>M-1 ENTERS AND GOES INTO THE [REDACTED]</i></p> <p><i>V-2 DEPARTS L-3</i></p> <p><i>V-2 ARRIVES AT (L-4) [REDACTED]</i></p> <p><i>(V-3) [REDACTED] IS PARKED</i></p> <p><i>IN FRONT OF L-4 AND (V-4)</i></p> <p><i>AND (V-5) [REDACTED] PARKED IN</i></p> <p><i>DRIVEWAY,</i></p> <p><i>M-1 AND (M-2) w/m [REDACTED]</i></p> <p><i>[REDACTED] EXIT L-4 AND ENTER V-2</i></p> <p><i>AND DEPART.</i></p> <p><i>V-1 IN DRIVEWAY AT L-1</i></p> <p><i>END OF SURVEILLANCE.</i></p>					

b3
b6
b7C
b7E

b6
b7C
b7E

b6
b7C
b7E

b6
b7C
b7E

b6
b7C

SURVEILLANCE LOG - [REDACTED] DIVISION
CONTINUATION SHEET

b3
b6
; b7C
b7E

Date		Page 3 of 3
12-14-88	Hours of Coverage	

File #	Case Agent	Log Prepared By
--------	------------	-----------------



The following investigation was conducted by squad 17 and documented by [redacted]

b3
b6
b7C
b7E

Surveillance Date: 12/14/98
Day: Monday
Weather: Partly Cloudy

A Physical Surveillance was conducted in the vicinity of [redacted]

[redacted] at which time the following observations were noted:

b6
b7C
b7E

<u>Time</u>	<u>Initials</u>	<u>Observations</u>
[redacted]		Surveillance started at [redacted] (L-1) and (V-1) was parked in front of [redacted] V-1 [redacted]
[redacted]		(L-2) [redacted] and (V-2) [redacted] located in parking lot
[redacted]		(M-1) w/m [redacted] gets into V-2 and departs L-2
[redacted]		V-2 arrives at L-3, [redacted] M-1 enters and goes into the [redacted] [redacted]
[redacted]		V-2 departs L-3
[redacted]		V-2 arrives at (L-4) [redacted] (V-3) [redacted] is parked in front of L-4 and (V-4) [redacted] and (V-5)

b6
b7C
b7E

b6
b7C
b7E

[REDACTED] parked
in driveway

b6
b7C
b7E

[REDACTED] M-1 and (M-2) w/m [REDACTED]
[REDACTED] exit
L-4 and enter V-2 and depart

[REDACTED] V-1 in driveway at L-1

[REDACTED] End of surveillance.



(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/22/1998

To: New York

Attn: SA
SA

b3
b6
b7C
b7E

From: [redacted]

Squad 4

Contact: SA [redacted]



[redacted]

By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] Pending)

Title: HACKING FOR GIRLIES,
ET AL;
New York Times - Victim
CITA;
OO:NY

Synopsis: Results of interview with [redacted] and the appropriate documentation.

b6
b7C

Enclosures: One original and one copy of FD-302 interview with [redacted] along with original interview notes in 1A envelope for New York Division.

Details: [redacted] was interviewed at his place of residence on 12/16/1998. He was questioned regarding his [redacted]

[redacted] Hackers For Girlies which hacked the web page of the New York Times. The results of the interview are documented on the accompanying FD-302.

♦ ♦

[redacted]

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
JAN 05 1999	
FBI - NEW YORK	

[redacted]

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/18/98

[redacted] born [redacted] social security
account number [redacted] who resides at [redacted]
[redacted] telephone number [redacted] was
interviewed at his place of residence regarding his possible
involvement in some internet hacking activity. After being
advised of the identity of the interviewing agents and the nature
of the interview, he provided the following information:

[redacted]

b6
b7Cb6
b7C

Investigation on 12/16/1998 at [redacted]
File # [redacted] Date dictated 12/18/1998
by SA [redacted] b7E

b3
b6
b7C
b7E

[redacted]

b3
b7E

Continuation of FD-302 of [redacted]

, On 12/16/1998

, Page

2

[redacted]

b6
b7C

[redacted] These men are [redacted] and [redacted]. [redacted] met [redacted] at a Def Con convention in Las Vegas, Nevada. [redacted] said that [redacted] was formerly employed at [redacted] in [redacted] and later in [redacted] where he performed [redacted]. Per [redacted] has the most extensive data base bar none of all bugs used in connection with an intrusion detection system product. [redacted] stated that, "for a company with products (goods to sell), his [redacted] database is golden." [redacted] had the foresight to see where the security needs would go. On average, other similar databases are only 2-4 years old compared to [redacted] which was compiled over the last six years. [redacted] performs penetration, network auditing and research and development work, as well as other functions at [redacted] stated that he knew [redacted] used internet nicks or handles of [redacted] and [redacted] as well as others that he couldn't recall at the time. He also stated that [redacted] could currently have a web page. In the past, [redacted] has had a web page which has been changed a few times.

b6
b7C

[redacted] met [redacted] through internet relay chat (IRC) rooms. He had been looking for someone with strong skills and said that [redacted] was highly recommended by his internet associates. At [redacted] is focused primarily in research and development of security software. He has also been developing operating software. [redacted] said [redacted] uses the handle or nickname of [redacted] but that he frequently rotates his internet handles so [redacted] isn't sure what he is currently using.

b6
b7C

Another employee named [redacted] works at [redacted] in software development. However, he is not compensated monetarily but, rather, with stock in the company.

b3
b7E

Continuation of FD-302 of [redacted]

, On 12/16/1998 , Page

3

[redacted] stated that he worked for [redacted] where he was in charge of developing. One of [redacted] responsibilities was to help create the company's web page for which he laid out the blue print and concept. [redacted] also designed the concept for the [redacted] web page. He has worked significantly with computers and has several at his personal residence. However, only two PCS and a Macintosh are currently working. He is very familiar with the internet but claims that he mostly conducts business related matters over the internet as opposed to casual browsing. He stated that he does not have a web page. His handles change and/or are rotated frequently but he uses [redacted]

b6
b7C

When asked what he knew about HFG (Hacking For Girlies), [redacted] responded that everybody has heard of them over the internet. He was aware that they hacked into the New York Times and that another group (LOU) hacked into several sites in Japan in retaliation to HFG. He could not explain the connection between LOU and HFG and stated that, other than what he has read in magazine articles, he doesn't know anything about HFG.

Asked if he knew whether [redacted] or [redacted] were associated with HFG, [redacted] stated that he would be very surprised if they were because he believes that they would have too much to lose. He also said that he has heard them "rip" on people that hack. He said that if they hacked the New York Times that they would be "screwing" him and he doesn't believe that they would do that to him. He also stated that [redacted] has been [redacted]

b6
b7C
b7E

[redacted] and views it as an unlikely conflict of interest that [redacted] would be hacking [redacted]
[redacted]

[redacted] stated that he was familiar with the web site [redacted]. He explained that he was not responsible for the web page, but rather, [redacted] of [redacted], an IRC [redacted] chat room acquaintance, set up the web page. Asked about whether [redacted] could be involved with HFG, [redacted] said that it would be unlikely because he doesn't believe that [redacted] has the skill to be a hacker. When asked about the link from [redacted] to [redacted] explained that [redacted] was probably trying to throw business to [redacted].

b6
b7C

[Redacted]

b3
b7E

Continuation of FD-302 of [Redacted], on 12/16/1998, Page 4 b6
b7C

handles [Redacted] claimed that he was not familiar with the handles [Redacted] His sentiment is that the names are so long that they would be irritating if used in IRC.

The following is a description of [Redacted]

b6
b7C

Name:

DOB:

SSN:

Sex:

Height:

Weight:

Build:

Hair:

Address:

Telephone Number:

[Redacted]

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/16/98

[redacted]
[redacted] was advised of the identity of the interviewing agents and the purpose of the interview.

b6
b7C

[redacted] was served with a "2703(f)" letter from the United States Attorney, Southern District of New York, dated December 14, 1998, and signed by AUSA [redacted].

[redacted] advised he knew [redacted] and that [redacted] used to have some of his equipment co-located at [redacted]. Approximately three months ago [redacted] had a friend remove the equipment from [redacted]. [redacted] stated that [redacted] keeps computerized records and information for 90 days after the termination of service of a client, therefore [redacted] may or may not have deleted records/account information for [redacted]. [redacted] stated that he was very aware of the meaning of the letter and that he would fully comply with it when he receives an appropriate Order.

b6
b7C

[redacted] has taken a class on complying with the Electronic Communications Act and received instruction from a Department of Justice Attorney. [redacted] advised two of the partners in [redacted] are attorneys and they would not do anything to cause their being disbarred. [redacted] would not acknowledge whether [redacted] currently had any information on [redacted] without being first served with the Order.

Investigation on 12/16/98 at [redacted]
File # [redacted] Date dictated 12/16/98
by SA [redacted]

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/16/98

[redacted] Internet Engineer, [redacted]

[redacted] DOB: [redacted] SSAN: [redacted], was advised of the identity of the interviewing agents and the purpose of the interview. [redacted] provided the following:

[redacted] met [redacted] during the winter of 1994 over the Internet chat room called #hackers. [redacted] was having trouble with some IRC software compilation for a client. At the time, [redacted] was living in [redacted] attending [redacted]

[redacted] decided to check with some hackers to see if anyone knew how to fix her problem. After meeting [redacted] on the Internet, [redacted] began corresponding with him via E-mail, IRC sessions, the telephone and even sent him her picture. [redacted] visited [redacted] during spring break. [redacted] then dropped out of school and started living with [redacted]. [redacted] also met his roommate [redacted]

[redacted] obtained employment at a [redacted] near [redacted] worked in the computer and cellular telephone department. [redacted] also worked at [redacted] [redacted] lived in an apartment near [redacted]. Eventually [redacted] got a job working as a Help Desk representative for [redacted] which was recently purchased by [redacted]. [redacted] moved to [redacted] where they lived together for approximately one and one half years. [redacted] believes they split up in the summer of 1996. [redacted] split up with [redacted] because she was annoyed with his friends and their activities.

[redacted] and friends would have activities called "group nights" wherein they would hack into other systems and go through trash at businesses. Group nights were part of the hacker group [redacted], of which they were all members. Group nights were also called [redacted] Nights". Trash hauls produced computer printouts of information and electronic hardware. For instance, at one time their apartment had twenty-one 19" monitors of which approximately one half worked. [redacted] stated that she felt group night activities was something in which she could get into trouble over and possibly lose her job at [redacted]. [redacted] felt [redacted] was a negative impact on her life and so wanted to keep away from him. Just before [redacted] broke up with [redacted]

Inves [redacted] t [redacted]
 File # [redacted] Date dictated 12/16/98
 by SA [redacted]

b6
b7Cb6
b7Cb6
b7Cb6
b7Cb3
b6
b7C
b7E

[redacted]

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 2

b6
b7C

"stuff" started appearing in the apartment. This stuff was things which [redacted] knew they couldn't afford (computer equipment, telephones etc.). [redacted] attitude on hacking seemed to be changing. After moving away from [redacted] was constantly asked by [redacted] roommates to store computer equipment at her house. She refused.

[redacted] stated that [redacted] and his friends hacked into many companies including NASA, NETCOM, US West, and Stonehenge. The purpose of the hacking was to [redacted]

b6
b7C
b7E

[redacted] had Electronic Serial Numbers (ESN's) for cellular telephone numbers. They also had the "burners" to reprogram the cell phones. Typically [redacted] would dial into the [redacted] which was a "trusted" system by many other systems, and then attack other systems. [redacted] would also collect credit card information, but would never use them to obtain anything of value. [redacted] also collected interesting E-Mail. [redacted] usually just wanted to look around and have a challenge.

[redacted] described [redacted] as a huge collector of information. [redacted] wanted to have everything. [redacted] helped [redacted] edit and write for an on-line magazine called [redacted] and covered a large range of topics. [redacted] hasn't talked to [redacted] very much since he moved to [redacted] moved there in approximately [redacted] and prior to that hadn't been employed for about one year. [redacted] had moved to [redacted] to work for [redacted] but his position was closed shortly after taking the job. While at [redacted] talked about computer security at military bases. [redacted] then went to work for [redacted]. At [redacted] does computer security consulting, security advisories, and maintains a database on how to hack systems, bugs, patches etc.

[redacted] stated that she suspects that [redacted] did the NY Times hack but has no proof, and [redacted] has never admitted it to her. The Times hack was signed by [redacted] has used [redacted] as a hacker handle in the past. [redacted] has a problem with how the press writes articles on hackers. The press has put out articles on people that [redacted] and [redacted] knew

b6
b7Cb6
b7C

[redacted]

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 3

b6
b7C

personally but were blatantly not true. [redacted] is very anti-government, but needs money so he will speak at government functions. [redacted] doesn't know if [redacted] is a member of the group "Hackers For Girlies". [redacted] is very vague, even with people he is close to. [redacted] when asked if he has done something, will often grin or wink, but he won't say if he did it. [redacted] used to call [redacted] his "girlie". The press did approach [redacted] to ask if [redacted] was responsible for the Times hack. [redacted] who works at a Help Desk for [redacted] has two or three friends who are members of the group [redacted] is a group that offers help to secure computer systems. [redacted] releases software that shows vulnerabilities of computer systems and can be described as similar to SATAN.

[redacted] described herself and [redacted] as being on the edge of the hacker scene. [redacted] described hacking groups as being a very close knit society. While [redacted] doesn't really hack, she has "been around" and knows the people. [redacted] uses the hacker handle of [redacted] has a domain called [redacted] which is a free service for people who need it. [redacted] gives [redacted] a [redacted] as an employee benefit.

b6
b7C

[redacted] have seven computers connected to their system. [redacted] does a lot of Web development. The computers are configured with various operating systems such as Windows, Unix, etc., and are networked together. Two of the computers belong to [redacted]. When [redacted] went to work for [redacted] she kicked most of the users off because she didn't want them hacking into the [redacted] system.

[redacted] described the following members of [redacted] as follows:

b6
b7C

[redacted] and leader of [redacted] at the time she was involved with them. [redacted] now believes that hacking is stupid. [redacted] feels [redacted] thinks this way because [redacted] hacked into [redacted] with [redacted] LNU (Last Name Unknown) and got caught. [redacted] has married and is trying to be responsible.

[redacted]

b3
b7EContinuation of FD-302 of [redacted], On 12/16/98, Page 4 b6
b7C

[redacted] Was interviewed by law enforcement (possibly the FBI) regarding [redacted]. Has since moved to [redacted]

[redacted] was not the leader, but a lackey.

[redacted] LNU. Not a big player, but fixed everyone's cars when they broke down.

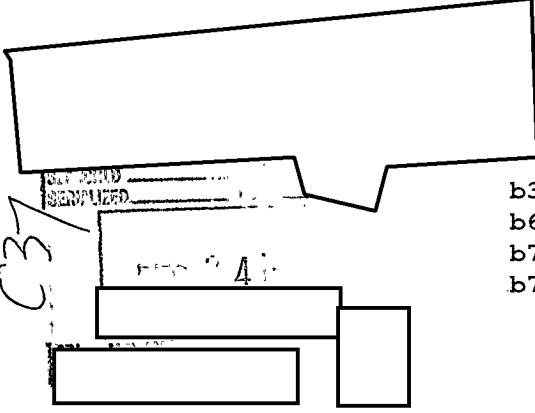
[redacted] (phonetic, but [redacted]). An annoying kid who "pissed" everyone off and was kicked out of the group.

[redacted] Doesn't know anything about him.

[redacted] Doesn't know anything about him.

[redacted] advised that [redacted] is no longer active and everyone who was involved with [redacted] has abandoned it. [redacted] stated that it was easy to hack when all you had was a job that paid \$6.00 per hour (like [redacted]). A lot of the people in [redacted] have grown up, have responsibilities and jobs that they don't want to lose. [redacted] now wants to keep hackers out of her system. [redacted] just got accepted at [redacted] and will be focusing on a computer science and multi-media degree. [redacted] ultimately wants to create computer games.

b6
b7Cb6
b7C



b3
b6
b7C
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/17/1998

✓ To: NEW YORK

Attn: SA [redacted]

From: [redacted]

SQUAD 4

Contact: SA [redacted]

Approved By: [redacted]

Certified By: [redacted]

e ID #: [redacted] (Pending) [redacted]

Title: [redacted];

et al;

CITA;

OO: New York

Synopsis: To report coverage of lead to serve [redacted]

[redacted] with 2703(f) letter, and to interview [redacted]

Reference: [redacted]

Enclosures: Enclosed for New York is the following: 1. The original and two copies of an FD-302 interview of [redacted]
2. A 1-A envelope containing interview notes of [redacted] 3. The original and two copies of an FD-302 interview of [redacted]
4. A 1-A envelope containing interview notes of [redacted]

Details: On December 16, 1998, [redacted] was served with a 2703(f) letter signed by AUSA [redacted] was cooperative. On December 16, 1998, [redacted] Internet Engineer, [redacted] was interviewed regarding her knowledge of [redacted]. Details are in the enclosed FD-302. [redacted] considers this matter closed.

♦♦

b3
b6
b7C
b7Eb3
b6
b7C
b7Eb6
b7Cb6
b7C



Forgot where you filed
the fax cover sheet template?

WIRED

Top Stories
Business
Culture
Technology
Politics
General News

enter email : OK

Today
The Past 7 Days

Quotes (enter ticker):

GO

Today's Summary
Incomes
Particulars

Web St.

DATEK
ONLINE
TRADE NOW

N
N
W CLICK
HERE!

WIRED MAGAZINE



Issue 6.12
Subscribe to WIRED
Special offer

HOTWIRED

Email Dept.
Webmaster/
Web 101
FAQs
Feedback
Customer Support

Wired News

SEARCH

Printing?
Use [this](#) version.

CULTURE
[Today's Headlines](#)

[Building Digital
Pyramids](#)

[Video Fracas Erupts
on Web](#)

[Real Life Trumans](#)

[The Not-So-Happy
Hacker](#)

[The Wright Stuff](#)

[Humane Designs for
Cube Farms](#)

[RIAA Unveils Anti-MP3
Plan](#)

[The PowerPoint
Amateur Hour](#)

[Zelda Gets Naughty](#)

[Wall of Voodoo](#)

[Hit and Run No. CLIII](#)

Christmas card
list getting
out of hand?



b6
b7C

The Not-So-Happy Hacker

by Arik Hesseldahl

NEW YORK — A woman identified as an enemy of the crackers who attacked *The New York Times* online site recently says the FBI now considers her a suspect as well.

"The FBI has no rational reason to consider me a suspect," said Carolyn Meinel, a New Mexico computer security consultant.

Meinel, author of *The Happy Hacker* and founder of an [online community](#) by the same name, held a sparsely attended press conference in New York Wednesday to publicize what she says amounts to harassment by the FBI.

Meinel claims that FBI investigators, eager to make an arrest in the high-profile case, are following a trail gone cold. The result, she said, has been a bitter stalemate. She said she would like to cooperate with the Bureau's investigation, but fears that doing so might lead to her wrongful indictment.

When told by FBI agents that she was a suspect, Meinel said she was asked to take a lie detector test. She agreed at first, but following the advice of lawyers and friends, Meinel later refused.

"I was told that the only reason they ask for a lie detector test is when they want to trip you up and get you to say something they can use to ask for an indictment," she said.

Later, Meinel was told she was not a suspect in the case, but that the request to take the lie detector test still stood.

FBI Special Agent Doug Beldon said he had no comment on the case, and would not confirm or deny that the attack is under active investigation. Published reports say that the FBI's computer-crimes unit is handling the case.

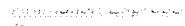
Meinel was one of several people named in a message posted on *The New York Times* Web site by Hacking for Girlyies in an attack that



01/24/98

12/17/98 5:50 PM

b3
b6
b7C
b7E

A small graphic showing four search engines: Excite, Lycos, Infoseek, and WebCrawler.

Search engines

Such.com

HOTBOT

Search

Shopping

occurred on 13 September. The message
appears in the HTML code of the page.

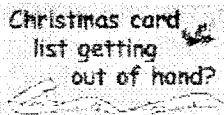
1 of 2 [Next Page](#)[Wired News Staff](#)[Wired News is coming](#)[Contact us](#)

Wired News delivered
by [Globe Express](#),
[Inbox Direct](#),
or [PointCast](#)



BASKETBALL

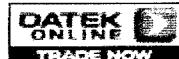
CLICK & GO



WIRED

[Top Stories](#)
[Business](#)
[Culture](#)
[Technology](#)
[Politics](#)
[General News](#)
[enter email](#)
[Today](#)
[The Past 7 Days](#)
[Quotes \(enter ticker\):](#)

GO

[Today's Summary](#)
[Indexes](#)
[Portfolios](#)


WIRED MAGAZINE



Issue 6.12

[Subscribe to WIRED](#)
[Special offer!](#)

HOTWIRED

[Front Door](#)
[Netmonkey](#)
[Web 101](#)
[CGI Gallery](#)
[Glossary](#)

Wired News

SEARCH

[Printing?](#)
 Use [this](#) version.

The Not-So-Happy Hacker Page 2

continued

Others taunted by the HFG statement included *New York Times* reporter John Markoff and Tsutomu Shimomura, a computer security expert who assisted the FBI in the arrest of Kevin Mitnick. Markoff and Shimomura co-wrote a controversial book about the Mitnick case, *Takedown*. A movie based on the book is under development by Miramax Films.

"She is writing a chapter about us in her second book.... Her goal all along has been to lead us on, watch us get busted, then write about us, à la Markoff/Mitnick, Shimomura/Mitnick, Quittner/MOD, Stoll/Hess. See a pattern forming here? We sure do," HFG wrote.

The group claimed that Meinel asked them "to hit a bigger and more trafficked site," according to the statement. "She told us that she is almost done with the book."

A second edition of *The Happy Hacker* has just appeared, which Meinel made available to reporters. She scoffed at suggestions that her connection to the attack had helped sell more books.

"I had the chance to exploit this incident in September and didn't. I've been a lousy publicist for this book," she said.

When first contacted by [Wired News](#) on 13 September, the day of the *Times* attack, Meinel denied any relationship with HFG. "I don't know who they are in real life," she said at the time, denying their claim that she was writing about them. "I hope they come to their senses before they wind up in jail."

Meinel said the first she had heard of HFG was on 7 August, when the group allegedly hacked Route 66, a New Mexico ISP where Meinel holds an account. Whoever cracked the ISP apparently also downloaded a file containing 1,749 credit card numbers.

Details of the attack on the ISP were reported in *Network magazine* last month. The story includes

CULTURE
[Today's Headlines](#)
[Fireteams Get Fired Up](#)
[Building Digital Pyramids](#)
[Video Fracas Erupts on Web](#)
[Real Life Trumans](#)
[The Not-So-Happy Hacker](#)
[The Wright Stuff](#)
[Humane Designs for Cube Farms](#)
[RIAA Unveils Anti-MP3 Plan](#)
[The PowerPoint Amateur Hour](#)
[Hit and Run No. CLIV](#)
[Wall of Voodoo](#)

[CULTURE NEWS](#)[Suck.com](#)[HOTBOT](#)[Search](#)
[Shopping](#)[Wired News staff](#)[Wired News is hiring](#)[Contact us](#)[Wired News delivered by Outlook Express,
In-Box Direct,
or PointCast](#)

Wired magazine last month. The story includes an interview with individuals claiming to be the perpetrators.

Having written about the cracker underground in her book and for *Scientific American*, Meinel is no stranger to their wrath. She detailed a history of telephone and email harassment against her dating back two years. She said she has been kicked off of four ISPs as a result of various hacking attacks against her. Each attack was reported to the FBI, she said, who took reports, but did little.

Meinel said she was approached by an FBI agent in 1997 and asked to write a proposal for teaching the bureau about computer criminal tactics. That offer was abruptly rescinded when a teenage associate of Meinel's was raided by the FBI on suspicion of hacking crimes. Meinel said she suspects the boy, called "Foobie" in her book, was framed by her critics in the cracker underground.

One former cracker-turned-computer-security consultant — Brian Martin, who goes under various handles, including Mea Culpa and Jericho — has published the details of his complicated ongoing feud with Meinel.

Related Wired Links:

[Mitnick's Trial Delayed](#)

4 Dec 98

[All the News That's Fit to Hack](#)

14 Sep 98

[Hacker Can't Get Access](#)

2 Sep 98

[A Low-Key Mitnick Protest](#)

16 Jul 98

[Hackers to Shake Down Takedown](#)

16 Jul 98

[Hack and Ye Shall Learn](#)

19 Nov 96

[<< Back 2 of 2](#)

[Send us feedback](#) | [Work at Wired Digital](#) | [Advertise with us](#)
[About Wired Digital](#) | [Our Privacy Policy](#)

[Copyright © 1994-98 Wired Digital Inc. All rights reserved.](#)

SEARCH PLAN

[REDACTED]
HACKING FOR GIRLIES,
ET AL;
NEW YORK TIMES - VICTIM;
OO:NY

b3
b6
b7C
b7E



[REDACTED]

[REDACTED]

SEARCH PLAN

SERIALIZED [REDACTED] INDEXED [REDACTED] FILED [REDACTED]

DEC 22 1998

[REDACTED]

[REDACTED]

b3
b6
b7C
b7E

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/28/1998

To: FBI Headquarters

Attn: SSA [redacted]
CART

✓ From: New York

C-37

Contact: SA [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]

b6
b7C

AKA HACKERS FOR GIRLIES (HFG);
NEW YORK TIMES-VICTIM;
CITA;
OO:NY

Synopsis: Recognition of the efforts of CART examiners [redacted] in connection with the search of [redacted] on December 16, 1998.

b6
b7C
b7E

Details: SA [redacted] would like to personally thank [redacted] in the search of [redacted] on December 16, 1998. Their assistance in carrying out an extremely complicated [redacted] was invaluable.

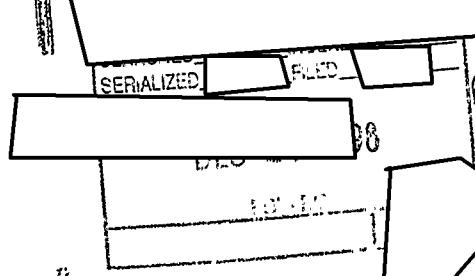
[redacted] are to be commended for taking initiative to [redacted] Furthermore, this assisted the SAs [redacted] at another search location.

b6
b7C
b7E

They arrived the night of 12/15/98. [redacted] started at approximately 9:30 am on 12/16/98 and ended at about 1:30 am on 12/17/98. On 12/17/98 at approximately 8:00 am, they returned home.

UPLOADED

WITH/TEXT ✓
WITH/OUT/TEXT _____
BY [redacted]
DATE 1-4-99



b3
b6
b7C
b7E

To: FBI Headquarters From: New York
Re: [redacted] 12/28/1998

b3
b7E

The team came prepared and went way above the call of duty. [redacted] performed in a professional manner that was not only recognized by the SAs but by employees of the ISP. As a result, a favorable impression was left [redacted]

b6
b7C

Appreciation is extended to [redacted] who are to be commended for their efforts and professionalism.

♦♦

- 1 -

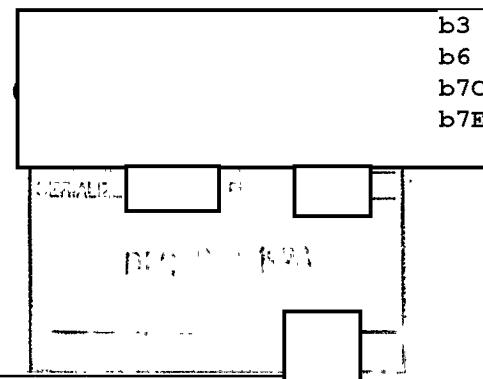
FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/16/98

A search warrant was executed on 12/16/98 for the premises known as [REDACTED] [REDACTED]. FBI personnel departed [REDACTED] FBI headquarters at approximately 8:00 am. Entry of the premises occurred at 8:55 am. The members of the entry team were Special Agent (SA) [REDACTED] [REDACTED], Special Agent (SA) [REDACTED] Special Agent (SA) [REDACTED], Special Agent (SA) [REDACTED] and Special Agent (SA) [REDACTED]. Following a knock and announce by SA [REDACTED], occupant and subject [REDACTED] opened the door. Subject [REDACTED], also an occupant of the apartment, was discovered in the bedroom upon entry by the team.

Once the scene was secured, entry photographs were taken by SA [REDACTED] and the photograph log was maintained by SA [REDACTED]. Immediately following the photographs a search of the premises was conducted. Attached is a copy of the evidence inventory sheets that itemize the evidence removed from the apartment. The scene was released to [REDACTED] and all personnel exited at about 3:26 pm.

b6
b7Cb6
b7C
b7E

b3
b6
b7C
b7EInvestigation on 12/16/98 at [REDACTED]File # [REDACTED] Date dictated 12/16/98

by SA [REDACTED]

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/05/99

SOURCE, who is not in a position to testify, provided the following information:

For more information about the study, please contact Dr. [REDACTED] at [REDACTED].

b6
b7c
b7d

10. The following table summarizes the results of the study. The first column lists the variables, the second column lists the sample size, and the third column lists the estimated effect sizes.

b6
b7c
b7d

SOURCE believes that

SOURCE BELIEVES CHAT

b6
b7C
b7D

Investigation on 11/04/98-12/28/98 at New York, NY

File # Date dictated 01/05/99

by SA

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b3
b6
b7C
b7D
b7E

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/06/1999

To: FBIHQ LAB
New York

Attn: CART, Room 4315
Attn: Evidence Control Unit

From: New York
C-37
Contact: SA [redacted]

ext.3187

Approved By: [redacted]

Drafted By: [redacted] [redacted]

Case ID #: [redacted] (Pending)
66E-HOC1155003 (Pending)

1045

Title: Hacking for Girlies;
Et al;
New York Times - Victim
CITA
OO:NY

Reference: Telephone call from SA [redacted] to SA [redacted]
[redacted] regarding captioned matter.

b3
b6
b7C
b7E

b6
b7C

Synopsis: Request assistance of FBIHQ, CART Unit that computer search assistance is needed in connection with captioned case.

Details: On September 13, 1998, the New York Times website (www.nytimes.com) was hacked by a group known as HACKERS FOR GIRLIES (HFG). The hackers altered the NY TIMES website with a webpage containing various text messages and graphic images. As a result, the NY Times took their computers off-line for approximately nine hours.

On December 16, 1998, a search was executed in [redacted] on subjects residence. As a result, evidence listed below was seized. Its believed the computers seized where used in the hack. The computers run a [redacted] operating system [redacted] encrypted files.

b3
b6
b7C
b7E

Writer requests evidence received by 01/06/98 from [redacted] be forwarded to FBI Headquarter CART Unit, Room 4315, for analysis. The following piece of evidence should be forwarded/analyzed:

Barcode

Description

[redacted]	UPLOADED
------------	----------

WITH/TEXT _____
WITH/OUT TEXT _____
BY _____
DATE 1-14-99

file = evid2-hq.ee

E-1146
[Signature]

b3
b6
b7C
b7E

To: FBIHQ LAB
From: New York
Re: [redacted]

01/06/1999

Attn: CART, Room 4315

b3
b7E

[redacted]
The remaining evidence will remain in New York.

To: FBIHQ LAB
From: New York
Re: [redacted] 01/06/1999

Attn: CART, Room 4315

b3
b7E

LEAD (s):

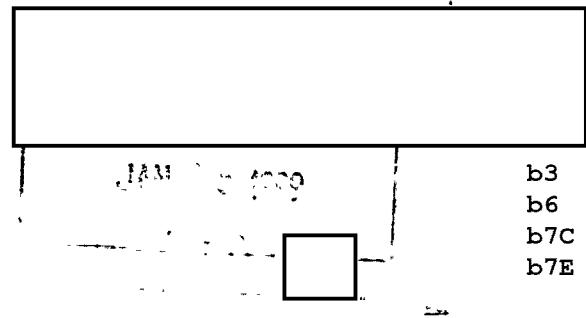
Set Lead 1:

FBI HEADQUARTERS

AT WASHINGTON DC

Request that a CART FE be assigned to provide assistance to New York for the analysis of evidence.

♦♦



JAN 15 1989



b3
b6
b7C
b7E

Date 11-24-98

NY

Birth Credit Criminal Death INS Marriage* Motor Vehicle Other _____

To OPC Buded

Return to SA File number C-37 ext 3187

Name and addresses of subject, applicant, or employee, and spouse
[Redacted]



Addresses

Residence _____

Business _____

Former _____

*Date and place of marriage
(if applicable) _____

Race	Sex <input type="checkbox"/> Male <input checked="" type="checkbox"/> Female	Age	Height	Weight	Hair	Eyes
------	--	-----	--------	--------	------	------

Birth date [Redacted] Birthplace _____

Arrest Number _____ Fingerprint classification _____ Criminal specialty _____

Social Security Number [Redacted] Drivers License Number [Redacted] - NY
[Redacted] D/L Photo Other

Specific information desired

Results of check



11/24/75

CCH
11/24/98

Please call for
pick-up.

Thanks.

b3
b6
b7C
b7E

b6
b7C

JAN 15 1969

b3

b6

b7c

b7E



INVESTIGATIVE INFORMATION REQUEST FORM

FBI, Butte Information Technology Center
400 North Main Street, Room #115
Butte, Montana 59701

- Commercial Telephone (406) 782-2304
- FTS: (406) 782-2304 FAX: (406) 782-9504, 782-9507 & 782-7418
- Secure FAX & STU III: (406) 782-2304, Ext. 26

TO: FBI, BUTTE INFORMATION TECHNOLOGY CENTER

Date: 11-13-98

Forfeiture/Seizure Related: Type of Request: FAX Telcal Mail

BITC Record #: 184577

ITC Use Only:
Date/Time In: 11/13 13:50 am pm
Date/Time Out: 11/13 11:38 am pm

Database(s) Used:

- | | | |
|--------------|---------------|-----------|
| 1. _____ | 5. <u>CDB</u> | 9. _____ |
| 2. _____ | 6. <u>ZN</u> | 10. _____ |
| 3. _____ | 7. _____ | 11. _____ |
| 4. <u>MN</u> | _____ | 12. _____ |

Handled By: _____

b3

b6

b7C

b7E

Requestor: SA

Phone #: _____ FAX #: 212-384-4660 UCFN: _____

Office/RA: NY

Precedence: ROUTINE IMMEDIATE

(UCFN (Line #) is required)

(Emergency/Crisis Situation)

SEARCH CRITERIA (Attach additional sheets if necessary)

Name - Last: _____ First: _____ Middle: _____

Alias: _____ Sex: f DOB1: _____ DOB2: / /

SSAN1: _____ SSAN2: _____ Spouse: _____

Fugitive: Yes No Driver's License #: _____ State: _____

RESIDENCE

Street Address: _____ City/State: _____ Zip: _____ Phone: _____

BUSINESS

Business Name: _____ Street Address: _____

City/State: _____ Zip: _____ Phone: _____ Business ID#: _____

CHECK DESIRED SEARCH PARAMETERS (Please check only those that are needed)

 1. Specific Information Desired Social Security #, Current Address, DOB

- 2. Determine All Individuals Associated with Social Security Number(s)
- 3. Report Validity of Social Security Number
- 4. Determine Who is Associated with Telephone Number(s)
- 5. Determine Address of Business/Person (U.S. _____, _____, _____ State(s))
- 6. Determine Property Owned by Individual (U.S. _____, _____, _____ State(s))
- 7. Determine Who Owns Property Listed Above
- 8. Determine Who Resides at Address Listed Above
- 9. Determine Financial Background Info, i.e., Bankruptcy, Judgments, Liens, UCC filings, or Lawsuits
- 10. Determine Corporate Business Info, i.e., Officer, Director, Registered Agent _____

(Person/Business)

 11. Customs Border Crossings / Subject query / I-94 info (circle one) 12. Federal Prison Inmate Information 13. Telemarketing Complaints

Reply From: FBI, Butte Information Technology Center (BITC)

Return Reply To:

SAC, _____

Attention: _____

Based on search criteria, marked records are attached:

- Possible Identifiable Records
- Other Peripheral Information

- Brief Synopsis of Information Found
- No Information Found

SS AN =
DOB =

b6

b7C

REPLY FORM - INVESTIGATIVE INFORMATION SERVICES

To help us better serve your investigative needs, please complete and return to:

FBI, Butte Information Technology Center
400 Main Street, Room #115
Butte, Montana 59701

BUTTE ITC RECORD #: 184577 UCFN: [REDACTED]
ANALYST: [REDACTED] SUBJECT: [REDACTED]

Was the information provided helpful to your investigation? YES NO
If NO, please let us know how we could be more helpful to your investigation: _____

b3
b6
b7C
b7E

ACCOMPLISHMENT(S) resulting from information:

PERSON(S): (Enter total number applicable to each of the following)

_____ FBI Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

_____ Local Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

_____ Subject(s) Arrested Located Identified

(Forward photo of Subject arrested with this Reply form)

_____ Witness(es) Located Identified

_____ New Witness(es) Located Identified

BUSINESS(ES): (Enter total number applicable to each of the following)

_____ New Business(es) Identified

_____ New Business Associates/Associations Identified

_____ Financial Audit Trail(s) Enhanced

ASSET(S): (Enter total number applicable to each of the following)

(TYPES: C = CASH R = REAL PROPERTY P = PERSONAL PROPERTY)

_____ Asset(s) Located Identified [VALUE: _____ TYPE: _____]

_____ Asset(s) Subject to Seizure/Forfeiture [VALUE: _____ TYPE: _____]

_____ Potential Economic Loss Prevented [VALUE: _____ TYPE: _____]

OTHER: (Enter total number applicable to each of the following)

_____ New Case(s) Initiated _____ New Lead(s) Generated

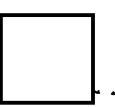
COMMENTS: _____

1 - Case File [REDACTED]

1 - BITC

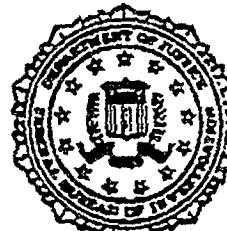
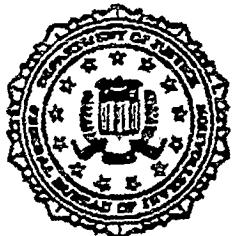
b3
b7E

PLEASE RETURN TO: BUTTE ITC



b3
b6
b7C
b7D

Federal Bureau of Investigation

Date: 12/04/98

PLEASE DELIVER THE FOLLOWING PAGES TO:

Name: SA ✓Agency: FBI ✓Phone #: () ✓FAX NUMBER: (212) 384-4660 ✓*This Facsimile Message is being sent by:*Name: ✓I WILL SEND THE ORIGINAL FAX TO YOU ✓ ✓ ✓b6
b7C

✉ FAX # → (303) 629-7171 ✉

Number of Pages, INCLUDING this Cover Sheet 2 ✓Approval ✓Date Sent: ✓Time Sent: ✓Initials: ✓b6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/24/1999

To: New York

Attn: SA [redacted]

From: Butte ITC

Investigative Information Services Center (IISC)

Contact: [redacted] 406-496-3805

b3
b6
b7C
b7E

Approved By: [redacted]



Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]
BUTTE REQUEST 189832

Synopsis: Results of database searches conducted by IISC.

Enclosures: Attached are copies of printouts setting forth results of inquiries conducted by IISC and a Reply Form.

Details: U.S. name search located one record for showing Social Security Account Number [redacted] address of [redacted]

b6
b7C

Credit bureau search on number [redacted], show this number was issued in [redacted] in the state of [redacted], and is being utilized by [redacted] the most current address listed is [redacted]

No criminal history record located.

[redacted]

SEARCHED _____	INDEXED _____
SERIALIZED _____	FILED _____
FEB 02 1999	
FBI - NEW YORK	
[redacted]	[redacted]

[redacted]

b3
b6
b7C
b7E

b3
b7E

To: New York From: Butte ITC
Re: [redacted], 01/24/1999

b3
b7E

LEAD (s) :

Set Lead 1:

NEW YORK

AT NEW YORK

Complete and return Reply Form to Butte ITC.

♦♦

FD-302 (Rev. 8-8-95)



INVESTIGATIVE INFORMATION REQUEST FORM

FBI, Butte Information Technology Center
400 North Main Street, Room #115
Butte, Montana 59701

- Commercial Telephone (406) 782-9534
- FTS: (406) 782-2304, 782-9504, 782-9507 & 782-7418
- Secure FAX & STU (406) 782-4664, Ext. 26

ITC Use Only:	BITC Record #:	189832
Date/Time In:	1-21-1999	<input type="checkbox"/> am <input type="checkbox"/> pm
Date/Time Out:	1-21-1999	<input type="checkbox"/> am <input type="checkbox"/> pm
Database(s) Used:		
1. <i>CDS</i>	5. _____	9. _____
2. <i>TRW</i>	6. _____	10. _____
3. <i>EF</i>	7. _____	11. _____
4. <i>NIC</i>	8. _____	12. _____
Handled By: _____		

TO: FBI, BUTTE INFORMATION TECHNOLOGY CENTER

Date: 1-21-99

Forfeiture/Seizure Request: _____

Type of Request: FAX Telcal MailReply: FAX Telcal MailRequestor: SA [redacted]Phone #: 212-384-3187 FAX #: 212-384-4660 UCFN: [redacted]

(UCFN (File #) is Required)

Office/RA: New YorkPrecedence: ROUTINE PRIORITY IMMEDIATE

Approximate turnaround times (48 hrs) (24 hrs) (2 hrs)

SEARCH CRITERIA (Continuation sheets if necessary)

Name - Last: [redacted]First: [redacted] Middle: _____

Alias: _____

Sex: F DOB: [redacted] DOB2: / /

SSAN#:

SSAN# _____ Spouse: _____

Fugitive: Yes

Driver's License #: _____ State: _____

RESIDENCE (PAST)

Street Address: [redacted]City/State: [redacted] Zip: [redacted] Phone: _____

BUSINESS

Business Name: _____

Street Address: _____

City/State: _____

Zip: _____ Phone: _____ Business ID#: _____

CHECK DESIRED

ITEMS (Please check only those that are needed)

 1. Specific InformationCurrent Address, Social Security #, Criminal history

- 2. Determine Who is Associated with Social Security Number(s)
- 3. Report Validity of Social Security Number
- 4. Determine Who is Associated with Telephone Number(s)
- 5. Determine Address of Business/Person in U.S. _____, _____, _____ State(s))
- 6. Determine Property Owned by Individual (U.S. _____, _____, _____ State(s))
- 7. Determine Who Owns Property Listed Above
- 8. Determine Who Resides at Address Listed Above
- 9. Determine Financial Background Info, i.e., Bankruptcy, Judgements, Liens, UCC filings, or Lawsuits
- 10. Determine Corporate Business Info, i.e., Officer, Director, Registered Agent _____ (Person/Business)
- 11. Customs Border Crossings / Subject query / I-94 info (circle one)
- 12. Federal Prison inmate information
- 13. Telemarketing Complaints

Reply From: FBI, Butte Information Technology Center (BITC)

Return Reply To
SAC: _____

Attn: _____

Used on search criteria, marked records are attached:

1. Basic Identifiable Records

 Brief Synopsis of Information Found

2. Other Peripheral Information

 No Information Found

REPLY FORM - INVESTIGATIVE INFORMATION SERVICES

To help us better serve your investigative needs, please complete and return to:

FBI, Butte Information Technology Center
400 Main Street, Room #115
Butte, Montana 59701

189832
BUTTE ITC RECORD #: UCFN
ANALYST: SUBJECT:

b3
b6
b7C
b7E

Was the information provided helpful to your investigation? YES NO
If NO, please let us know how we could be more helpful to your investigation: _____

ACCOMPLISHMENT(S) resulting from information:

PERSON(S): (Enter total number applicable to each of the following)

_____ FBI Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

_____ Local Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

_____ Subject(s) Arrested Located Identified

(Forward photo of Subject arrested with this Reply form)

_____ Witness(es) Located Identified

_____ New Witness(es) Located Identified

BUSINESS(ES): (Enter total number applicable to each of the following)

_____ New Business(es) Identified

_____ New Business Associates/Associations Identified

_____ Financial Audit Trail(s) Enhanced

ASSET(S): (Enter total number applicable to each of the following)

(TYPES: C = CASH R = REAL PROPERTY P = PERSONAL PROPERTY)

_____ Asset(s) Located Identified [VALUE: _____] TYPE: _____

_____ Asset(s) Subject to Seizure/Forfeiture [VALUE: _____] TYPE: _____

_____ Potential Economic Loss Prevented [VALUE: _____] TYPE: _____

OTHER: (Enter total number applicable to each of the following)

_____ New Case(s) Initiated _____ New Lead(s) Generated

COMMENTS: _____

1 - Case File

1 - BITC

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/24/1999

To: New York

Attn: SA [redacted]

From: Butte ITC

Investigative Information Services Center (IISC)

Contact: [redacted] 406-496-3805

Approved By: [redacted]

(X)

[redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: [redacted]
BUTTE REQUEST 189833

b3
b6
b7C
b7E

Synopsis: Results of database searches conducted by IISC.

Enclosures: Attached are copies of printouts setting forth results of inquiries conducted by IISC and a Reply Form.

Details: Drivers license search located [redacted] record
license [redacted], listing an address of [redacted]

b6
b7C

Social Security search using name and address from
drivers license located Social Security Account number [redacted]
[redacted] as being associated to [redacted] Most current address
listed is [redacted]

No criminal history record located.

[redacted]

SEARCHED	INDEXED
SERIALIZED	FILED
FEB 02 1999	
[redacted]	[redacted]

[redacted]

b3
b6
b7C
b7E

To: New York From: Butte ITC
Re: [redacted] 01/24/1999

b3
b7E

LEAD (s) :

Set Lead 1:

NEW YORK

AT NEW YORK

Complete and return Reply Form to Butte ITC.

♦♦



INVESTIGATIVE INFORMATION REQUEST FORM

FBI, Butte Information Technology Center

400 North Main Street, Room #115
Butte, Montana 59701

- Commercial Telephone (406) 782-9504
- FTS: (406) 782-2304 FAX: (406) 782-9504, 782-9507 & 782-7418
- Secure FAX & STU III. (406) 782-2304, Ext. 26

ITC Use Only:	BITC Record #:	
Date/Time In:	1-21-99 1532	<input type="checkbox"/> am <input checked="" type="checkbox"/> pm
Date/Time Out:	1-21-99 1500	<input type="checkbox"/> am <input checked="" type="checkbox"/> pm
Database(s) Used:		
1. <u>CNS</u>	5. _____	9. _____
2. <u>TRV</u>	6. _____	10. _____
3. <u>EF</u>	7. _____	11. _____
4. <u>NCIC</u>	8. _____	12. _____
Handled By: _____		

b3
b6
b7C
b7E

TO: FBI, BUTTE INFORMATION TECHNOLOGY CENTER

Date: 1-21-99Forfeiture/Seizure Related: Type of Request: FAX Telcal Mail Reply: FAX Telcal MailRequestor: SA [Redacted]Phone #: 212-384-3187 FAX #: 212-384-4666 UCFN: [Redacted]Office/RA: New YorkPrecedence: ROUTINE PRIORITY IMMEDIATE

Approximate turnaround times: (48 hrs) (24 hrs) (2 hrs)

SEARCH CRITERIA (Attach additional sheets if necessary)

Name - Last: [Redacted] First: [Redacted] Middle: [Redacted]Alias: [Redacted] Sex: F DOB1: [Redacted] DOB2: / /SSAN1: [Redacted] SSAN2: [Redacted] Spouse: [Redacted]Fugitive: Yes No Driver's License #: [Redacted] State: [Redacted]

RESIDENCE

Street Address: [Redacted] City/State: [Redacted] Zip: [Redacted] Phone: [Redacted]

BUSINESS

Business Name: [Redacted] Street Address: [Redacted]City/State: [Redacted] Zip: [Redacted] Phone: [Redacted] Business ID#: [Redacted]

CHECK DESIRED SEARCH PARAMETERS (Please check only those that are needed)

1. Specific Information (e.g., Current Address, Social Security #, Criminal history)

- 2. Determine All Incidents Associated with Social Security Number(s)
- 3. Report Validity of Social Security Number
- 4. Determine Who is Associated with Telephone Number(s)
- 5. Determine Address of Business/Person (____ U.S. _____, _____, _____ State(s))
- 6. Determine Property Owned by Individual (____ U.S. _____, _____, _____ State(s))
- 7. Determine Who Owns Property Listed Above
- 8. Determine Who Resides at Address Listed Above
- 9. Determine Financial Background Info, i.e., Bankruptcy, Judgements, Liens, UCC Filings, or Lawsuits
- 10. Determine Corporate Business Info, i.e., Officer, Director, Registered Agent _____

(Person/Business)

- 11. Customs Border Crossings / Subject Query / I-94 Info (circle one)
- 12. Federal Prison Record Information
- 13. Telemarketing Complaints

Reply From: FBI, Butte Information Technology Center (BITC)

Return Reply To:
SA: _____

A telephone number: _____

Based on search criteria, marked records are attached:

 Identifiable Records Brief Synopsis of Information Found Other Peripheral Information No Information Found

REPLY FORM - INVESTIGATIVE INFORMATION SERVICES

To help us better serve your investigative needs, please complete and return to:

FBI, Butte Information Technology Center
400 Main Street, Room #115
Butte, Montana 59701

189833
BUTTE ITC RECORD #: UCFN
ANALYST: SUBJECT:

b3
b6
b7C
b7E

Was the information provided helpful to your investigation? YES NO
If NO, please let us know how we could be more helpful to your investigation: _____

ACCOMPLISHMENT(S) resulting from information:

PERSON(S): (Enter total number applicable to each of the following)

FBI Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

Local Fugitive(s) Arrested: FBI Local Date _____

(Forward photo of Fugitive arrested with this Reply form)

Subject(s) Arrested Located Identified

(Forward photo of Subject arrested with this Reply form)

Witness(es) Located Identified

New Witness(es) Located Identified

BUSINESS(ES): (Enter total number applicable to each of the following)

New Business(es) Identified

New Business Associates/Associations Identified

Financial Audit Trail(s) Enhanced

ASSET(S): (Enter total number applicable to each of the following)

(TYPES: C = CASH R = REAL PROPERTY P = PERSONAL PROPERTY)

Asset(s) Located Identified [VALUE: _____] TYPE: _____

Asset(s) Subject to Seizure/Forfeiture [VALUE: _____] TYPE: _____

Potential Economic Loss Prevented [VALUE: _____] TYPE: _____

OTHER: (Enter total number applicable to each of the following)

New Case(s) Initiated New Lead(s) Generated

COMMENTS: _____

1 - Case File

1 - BITC

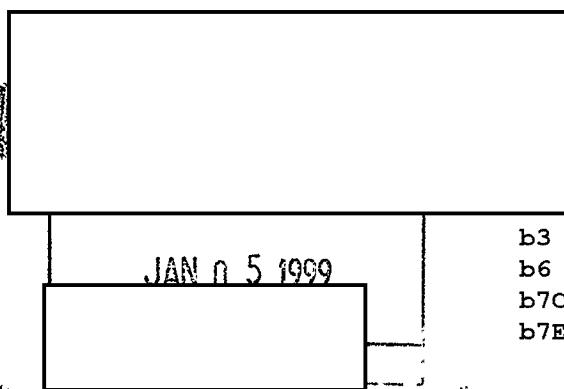
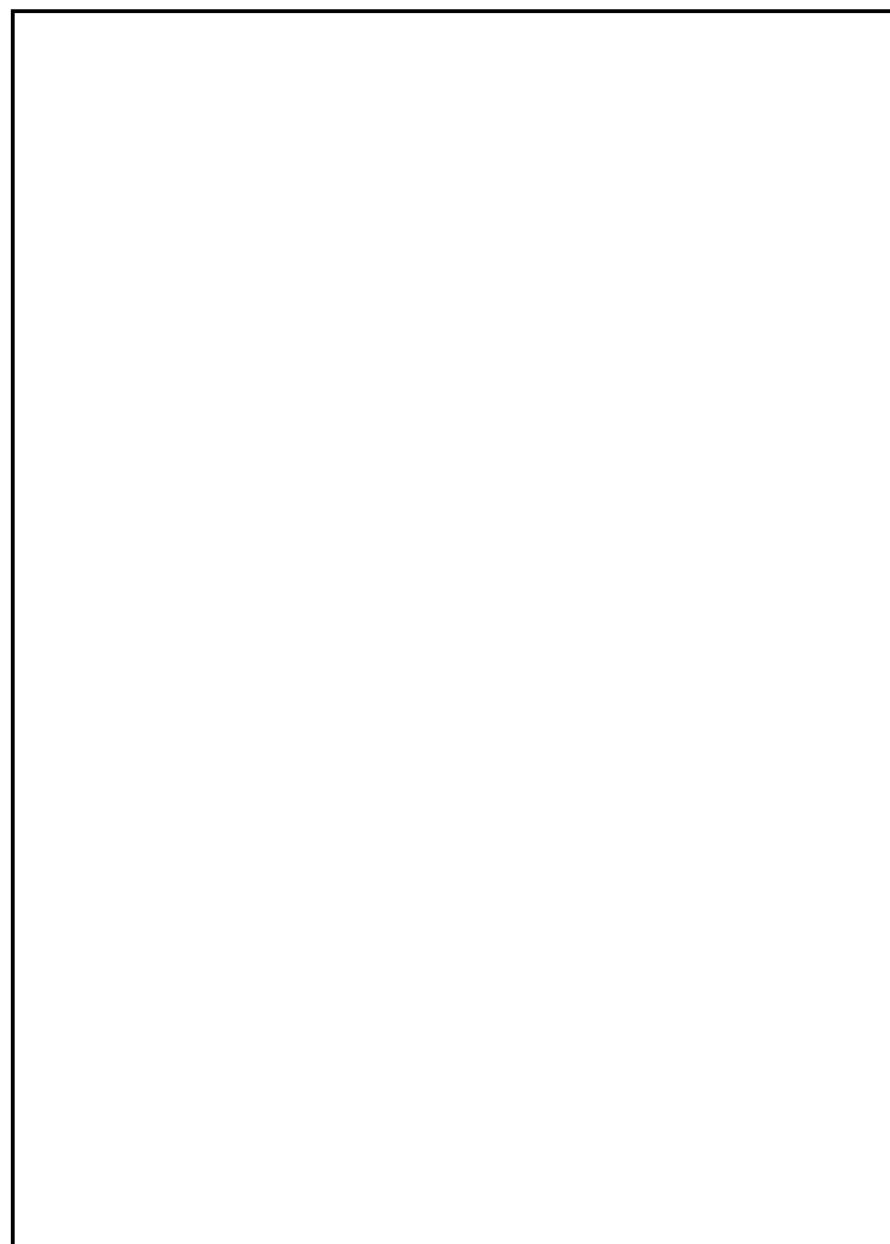
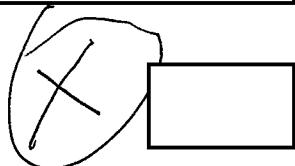
FBI - New York

From: [redacted]
Sent: Monday December 28 1998 12:40 PM
To: [redacted]

b6
b7C
b7E

Cc: [redacted]

Subject: Hacking for Girlies and FBI news



sac solo for info

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/04/99

Security Number [REDACTED]

DOB [REDACTED]

Social [REDACTED]

(1) [REDACTED]

b6
b7C

[REDACTED] was interviewed at his place of employment.

After being advised of the identity of the interviewing agent and the nature of the interview, he provided the following information:

[REDACTED] learned from [REDACTED] employee, that a hacker known as [REDACTED] claimed credit for New York Times (NYT) hack. A couple of weeks later, [REDACTED] was telling people that [REDACTED] were responsible the NYT hack.

b6
b7C

[REDACTED] uses the alias [REDACTED] on IRC. [REDACTED] heard a rumor on IRC that [REDACTED] was a member of HACKING FOR GIRLIES (HFG). [REDACTED] heard that [REDACTED] told others [REDACTED]

During the summer of 1998, [REDACTED] performed an authorized network scan against [REDACTED] as a business deal.

b3
b6
b7C
b7E

[REDACTED] gave [REDACTED] user accounts on [REDACTED] that they beta tested different security software packages on [REDACTED]

[REDACTED] since 1996.

SERIALIZED [REDACTED]

JAN 07 1999

UPLOADED

WITH/TEXT [REDACTED]
 WITH/OUT/EX [REDACTED]
 BY [REDACTED]
 DATE 01/04/99

E. Marshall
Sergeant

File # [REDACTED] 302

b3
b6
b7C
b7EInvestigation on 01/04/99 at [REDACTED]File # [REDACTED] Date dictated 01/04/1999

by SA [REDACTED]

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 12/08/1998

To: FBIHQ

Attn: CART Unit

From: New York

C-37

Contact: SA [redacted]

212-384-4506

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HACKING FOR GIRLIES;
VICTIM - NEW YORK TIMES;
CITA;
OO:NY

Synopsis: Request CART Headquarters assistance for search on Wednesday December 16, 1998, and follow-up examination.

Enclosures: (1) Color photocopy of computers to be examined.

Details: On Wednesday, December 16, 1998, a search warrant will be executed at [redacted]
[redacted]

b6
b7C

[redacted] is believed to be associated with the hacking group "Hacking For Girlies" (HFG). HFG is responsible for hacking the New York Times web page on September 13, 1998.

The assistance of CART Headquarters is requested to properly [redacted]

[redacted] Furthermore, it is requested that [redacted]

At

the present time, it is anticipated that the search will begin the morning of December 16, 1998. Case agents [redacted] (212) 384-3187 and [redacted] (212) 384-4506, will provide an operations order with exact search time, location and staging area.

b6
b7C
b7E

♦♦
UPLOADED

WITH/TEXT _____
WITH/OUT/TEXT _____
BY _____ DATE 1-28-99

SEARCHED	[redacted]	INDEXED	[redacted]
SERIALIZED	[redacted]	FILED	[redacted]
DEC 8 1998			
FBI - NEW YORK			

b3
b6
b7C
b7E

Cart.ec

b3
b6
b7C
b7E

Car-1.ec

UPLOADED

WITH/TEXT

WITH/OUT

BY

DATE 1-28-00

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/08/1998

To: New York

Attn: A/ASAC

FMU - NYO

From: New York

C-37

Contact: [redacted]

ext. 4506

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HACKING FOR GIRLIES;
VICTIM - NEW YORK TIMES;
CITA;
OO:NY

b3
b6
b7C
b7E

Synopsis: Request approval to pay for rental car expenses to be incurred by SA [redacted] during travel to [redacted]

[redacted]
b6
b7c

Details: SA [redacted] was approved for travel to the [redacted] division for the purposes of obtaining and executing a search warrant of (2) premises, one of which is occupied by [redacted] who are members of Hacking For Girlies (HFG), a computer hacker group, and the other of which is computers belonging to one of the subjects [redacted]. HFG has claimed responsibility for obtaining unauthorized access and replacing the New York Times web page on September 13, 1998.

In order to conduct the necessary travel involved, including surveillance of location to be searched, travel to the US Attorney's offices, FBI office, and other relevant locations, it is necessary that SA [redacted] have ready access to a vehicle. FBI [redacted] does not have a spare vehicle for this purpose. It is therefore requested that SA [redacted] receive approval to rent a car during captioned travel.

b6
b7c

♦♦

WFL

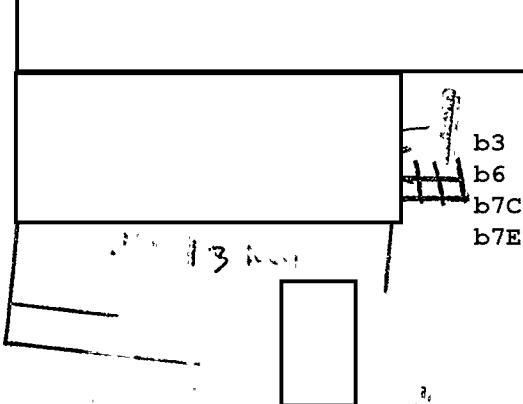
e-doc →



302

UPLOADED

WITH/TYPE:
WITH:
BY:
DATE: 1-28-99



b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/17/98

[REDACTED] home address [REDACTED]
[REDACTED] home telephone number [REDACTED] work telephone
number [REDACTED] pager number [REDACTED], social security
number [REDACTED] after being advised of the identities of the
interviewing agents, provided the following information:

b6
b7c

[REDACTED] is employed by [REDACTED] and works
in the [REDACTED] He has been
with the [REDACTED] since approximately January, 1997. [REDACTED] is
involved with software development and writes Internet security
tools. The [REDACTED] is physically located in [REDACTED]
[REDACTED] but [REDACTED] prefers to remain in [REDACTED] has
never used social security number [REDACTED] and has never used
one other than [REDACTED] lives [REDACTED]

b6
b7c

All of [REDACTED] ties with the hacker community were
severed in approximately [REDACTED] after [REDACTED]
[REDACTED] A couple of years ago, [REDACTED] had contact with
someone who went by the name [REDACTED] real name [REDACTED]
[REDACTED] (phonetic).

b6
b7c

AKA [REDACTED] used the handle [REDACTED] when he was involved in
the cracker community. [REDACTED] now goes by the name [REDACTED] when
online. The only reason that one would use a handle would be to
remain anonymous, and he has no reason to do that now. [REDACTED] does
not have a computer at home, and has not since [REDACTED] does
have a workstation at [REDACTED] and can access the Internet with this
workstation.

b6
b7c

[REDACTED] was aware of the New York Times hack only by
reading a "ZDNet" (an on-line news publication), article on the
topic. [REDACTED] has never heard of the group "hacking for girlies",
and stated that times must have changed since he used to hack,
because girls were never into hacking. [REDACTED] cited the IBM
commercial in which a girl is portrayed as a hacker, and stated
that the scenario was not realistic because a female would never
be present in that situation. To his knowledge, [REDACTED] has never

Investigation on 12/16/98 at [REDACTED]

File # [REDACTED] Date dictated _____

by [REDACTED]

b3
b6
b7C
b7E

Continuation of FD-302 of [redacted]

, On 12/06/98

, Page

2

b3
b7E

been to the New York Times web site, unless he clicked on a link to an article, which would have automatically taken him to the site. [redacted] stated that he would have immediately left the site because it prompts for a username and password, and he has never signed up for their service.

[redacted] has never heard of [redacted] but the name [redacted] sounded familiar. [redacted] then remembered that [redacted] [redacted] and that he was familiar with him because he may have electronically mailed (e-mailed) [redacted] with a request to [redacted] work for the company. This request came about 4 or 5 months ago. [redacted] declined the request, but did suggest a product that [redacted] could use in their [redacted] project. [redacted] stated that these e-mails were the extent of his contact with [redacted] does not know [redacted]

[redacted] has "made a 180 degree turn" from his hacking days, and now he doesn't even like hackers. When [redacted] was involved in hacking, he did it only for the "intellectual pursuit", never for political reasons. [redacted] has never used the screen name [redacted] and does not know anyone who does. [redacted] does not know anyone who goes by the name [redacted]

[redacted] uses a "sniffer" (a program intended to capture all data traffic on a computer network) at work, but only on systems that he is authorized to use, and only for legitimate business purposes. He used to use a sniffer as a hacker, which enabled him to [redacted] among other things, on compromised networks. [redacted] has never written a sniffer, and stated that there would be no need to, as sniffers are publicly available. [redacted] used a sniffer written by [redacted] [redacted] hacker who went by the name [redacted] [redacted] remembered naming the sniffer that he would install on a compromised system [redacted]

[redacted] in an attempt to conceal it from system administrators. [redacted] never stored his logs in a file or directory called [redacted] nor has he heard of anyone using that name.

b6
b7Cb6
b7Cb6
b7C
b7E

b3
b7E

Continuation of FD-302 of [redacted], On 12/06/98, Page 3

[redacted] has not heard of "The Well", but stated "EchoNYC" sounded familiar. [redacted] has heard of [redacted] and knows [redacted] [redacted] a technical support employee at [redacted] has never hacked [redacted] remembered hacking a web site in 1993 or 1994, in order to [redacted] In 1992 or 1993, [redacted] with the help of another hacker known as [redacted] remembered gaining access to [redacted] but never remembered [redacted] was [redacted] mentor and associate. [redacted] shared all of their tools and exploits. [redacted] described [redacted] as a dangerous individual who was loud, violent, and obsessed with serial killers. [redacted] was truly a genius, and was writing packet sniffers only a week after learning the computer language C. [redacted] identified [redacted] as [redacted] who lived in [redacted] near [redacted] last communication with [redacted] was in September, 1994.

b6
b7C
b7E

[redacted] also knew a hacker known as [redacted] in approximately 1994. [redacted] real name is [redacted] whose parents live in [redacted] heard that [redacted]

b6
b7C

[redacted] does not know [redacted] nor has he ever heard of her. He knows who [redacted] is, and stated that he [redacted]

[redacted] concluded by saying that the Internet is different from what it was when he was a hacker, and described it as very broad, and taking many different directions. He stated that the group "hacking for kiddies, or whatever they call themselves" is probably just going through a phase, and that they will outgrow this activity, much like [redacted] himself has done.

b6
b7C

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/21/98

[redacted] telephones [redacted]
 and [redacted] was contacted during a search of his premises. After being interviewed about certain aspects of the facts of this investigation, [redacted] and the agents engaged in conversation about the circumstances providing indications of [redacted] involvement in the HACKERS FOR GIRLIES (HFG) Group. [redacted] provided information which included the following:

[redacted] was shown an issue of FORBES Magazine that was found during the search of his apartment. [redacted] stated that he was familiar with an article in that magazine about the HFG hack of the website of the NEW YORK TIMES (NYT). [redacted] attention was drawn towards the photographic image of a woman that appeared in the article. Specifically, the article shows a copy of what the HFG group replaced the NYT's website with during the hack. The HFG group replaced the NYT website with the letters "HFG", and the "H" contained the photograph being discussed with [redacted]. [redacted] stated that he did not recognize the photograph as being the same as one found on the website of [redacted]

[redacted] again acknowledged that he had met with the FORBES reporter who wrote this article, [redacted] on a visit that [redacted] had made to [redacted] stated that [redacted] had only come to visit him in [redacted] once. [redacted] admitted that he picked up [redacted] when he arrived that day at the airport, and brought him back to the airport that same day when he departed. [redacted] said he was with [redacted] the full time that he was in [redacted] with the exception of those moments when [redacted] was "in the bathroom". [redacted] said that the only apartment that he brought [redacted] to in [redacted] was the one in which this interview and search were taking place.

[redacted] acknowledged that the circumstances he was describing, and the information contained in the FORBES article made it "look bad" for him.

[redacted] continued to deny that he was a member of HFG, [redacted] 302

Investigation on 12/16/98 at [redacted]

File # [redacted]

by SSA [redacted]
SSA [redacted]

Date dictated

12/16/98

SEARCHED
SERIALIZEDINDEXED
FILED

JAY 04 1000

FBI — NEW YORK

b6
b7cb6
b7cb6
b7cb3
b6
b7C
b7E

Continuation of FD-302 of [redacted]

, On 12/16/98 , Page 2

[redacted]
that he had participated in the hack of the NYT website, and that the "condo" described in the FORBES article was the same dwelling as the one he was currently in.

[redacted] again admitted that he used the name [redacted] in his computer activities. [redacted] stated that if the evidentiary trial in the NYT hack led to his [redacted] account, he would assert that it must have been because this account was compromised by other hackers.

[redacted] said he had spent about 15 minutes explaining to [redacted] what a "buffer overflow" was in layman's terms. He also pointed out that he explained some of the features of the computer software known as "Tripwire". When asked why [redacted] didn't just provide this information via telephone to [redacted] [redacted] did not have an explanation.

During the discussion with the Agents, [redacted] acknowledged being familiar with the FBI's investigation of [redacted] and others. He was interested in knowing whether it was true that the FBI would not investigate crimes unless the damage involved exceeded \$10,000. [redacted] wanted to know whether the NYT had calculated the damage to their system because of the HFG hack, and whether that figure was public information. [redacted] was also interested in knowing how the Federal Sentencing Guidelines worked.

As the Agents were departing [redacted] residence, SSA [redacted] commented to [redacted] that, as [redacted] could see, no evidence being seized pursuant to the search warrant had been "planted" by the FBI. Upon hearing this, [redacted] shot back that while he didn't think that these Agents had planted evidence, he wasn't sure about the "eighteenth" Agent he might encounter. SSA [redacted] was not present to hear that exchange.

b3
b6
b7C
b7Eb6
b7Cb6
b7Cb6
b7Cb6
b7C

(12/31/1995)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 12/09/1998

To: [REDACTED]
FBIHQ
New York

Attn: SSA [REDACTED]
Attn: SSA [REDACTED] NIPC
Attn: A/ASAC [REDACTED] WCC

b6
b7C

From: New York
C-37
Contact: SA [REDACTED] X3187

Approved By: Gonzalez Victo [REDACTED] M

Drafted By: [REDACTED]

Case ID #: [REDACTED] (Pending)

b3
b7E

Title: HACKING FOR GIRLIES;
VICTIM - NEW YORK TIMES;
CITA;
OO:NY

Synopsis: The purposes of this EC are to: (1) document concurrence of SAC [REDACTED] and SAC New York (Div II) for travel by New York SAs to [REDACTED] Division for execution of search warrants and interviews of members of "HACKING FOR GIRLIES" group; (2) request assistance from [REDACTED] Division to swear out and execute search warrants in [REDACTED] on 12/6/98; (3) request travel approval by SAC New York for three SAs and two SSAs to conduct investigation in [REDACTED] on this complex and high-profile 2 SSAs.

b6
b7C

Details: Captioned matter concerns an attack that took place on September 13, 1998 against a computer owned and operated by the New York Times newspaper establishment. The computer that was victimized houses the computer files and code for the New York Times internet webpage and its related on-line services. The attack gave the subjects unauthorized access to the New York Times computer (in violation of Title 18 USC Section 1030), and that unauthorized access was used to take down the true NY Times webpage and replace it with graphic images and text installed by the hackers.

The images installed were mildly pornographic and bore the initials "HFG", of the subject group "HACKING FOR GIRLIES". The text that was installed contained a diatribe against NY Times reporter [REDACTED] and others who had covered hacker stories. While this was embarrassing to the NY Times, the aspect during the time that the attack was successful readers of the NY Times on-line website were deprived service.

UPLOADED

WITH/TEXT _____
WITH/OUTTEXT _____
BY _____
DATE 1-08-99

SEARCHED INDEXED
SERIALIZED FILED

DEC 22 1998

b3
b6
b7C
b7E

Girlies.ec

To: [REDACTED] From: New York
Re: [REDACTED] 12/09/1998

b3
b6
b7C
b7E

The investigation by SAs [REDACTED] and [REDACTED] [REDACTED] has been intensive and exhaustive since that date. Through technical analysis of computerized forensic evidence, personal interviews and source information, the investigative trail has led to the [REDACTED] vicinity. Through the valuable assistance of SAs in the [REDACTED] office, several possible subjects have been identified and located, along with the locations of computers holding data relevant to the case.

The investigative strategy is to have SAs [REDACTED] and [REDACTED] travel to [REDACTED] Division on 12/13/98 so as to have 12/14 and 12/15 to prepare the execution of the search warrants on 12/16/98. During the 14th and 15th, the 27 page affidavit prepared by these SAs will be presented to a local Federal Magistrate in support of an application for search warrants.

b6
b7C

One search warrant will be served on [REDACTED]

[REDACTED] It will authorize the Agents to seize computerized data relevant to the NY Times hack and will require CART assistance (to be provided by FBIHQ).

Another search warrant will be executed at [REDACTED] [REDACTED] This is the residence of possible subjects [REDACTED] white male, approximately [REDACTED] years of age, and [REDACTED] white male, approximately [REDACTED] years of age. It is anticipated that approximately [REDACTED] [REDACTED] will be seized pursuant to the warrant at that location with CART assistance (to be provided by FBIHQ). During the execution of the search warrant, efforts will be made to thoroughly interview [REDACTED] and [REDACTED] separately, using the combined skills of a senior SSA or SA and a technically proficient computer crime SA for each interview.

b6
b7C
b7E

Discussions with SSA [REDACTED] in [REDACTED] indicated that SAC [REDACTED] concurs with travel by NY personnel. The [REDACTED] division does not have experienced SA personnel with computer training who could be available to conduct or assist in these interviews. The NYO has identified the following personnel, in addition to SAs [REDACTED] and [REDACTED] who have relevant experience and an understanding of the facts of the case: SA [REDACTED], SSA [REDACTED], and SSA [REDACTED]. It is planned that SA [REDACTED] and SSA [REDACTED] and [REDACTED] would travel to [REDACTED] on 12/15 for participation in interviews on 12/16. Return travel would occur on 12/17.

b6
b7C

A third possible subject of this case is [REDACTED] [REDACTED], white male, approximately [REDACTED] years of age, believed to reside at [REDACTED] While there

To: [REDACTED] From: New York
Re: [REDACTED] 12/09/1998

b3
b6
b7C
b7D

is no probable cause to support a search of [REDACTED] residence, it is very important that [REDACTED] be interviewed about this matter simultaneously with the interviews of [REDACTED] and [REDACTED] because [REDACTED] is believed to be a member of HFG. SA [REDACTED] is an SA with three years in the FBI, has obtained convictions in computer crimes investigations and is CART certified. He, along with another agent will interview [REDACTED]

b6
b7C

[REDACTED] FBI New York wishes to express its appreciation to the [REDACTED] Division for their continued assistance in this case.

To: [REDACTED] From: New York
Re: [REDACTED] 12/09/1998

b3
b6
b7C
b7E

LEAD (s):

Set Lead 1:

[REDACTED]

AT [REDACTED]

Provide assistance by designating an agent(s) to participate in the swearing out of aforementioned search warrants, and their execution on 12/16/98. Please advise NY whether any Bucars and HTs can be provided for transportation and communication assistance.

♦♦



From the Desk Of:

A/ASAC [redacted]

WHITE COLLAR CRIME BRANCH
DIVISION 2 - BRANCH "2"
x2802



b6
b7C

DATE _____

ADIC

A/CSSA [redacted] (CS)

SAC GONZALEZ

SSA [redacted] (C-1)

SAC _____

SSA [redacted] (C-2)

ASAC _____

SSA [redacted] (C-3)

CDC

SSA [redacted] (C-4)

MEDIA OFFICE

SSA [redacted] (C-12)

SSA [redacted] (C-14)

A/SSA [redacted] (C-21)

SSA [redacted] (C-28)

SSA [redacted] (C-32)

SSA [redacted] (C-33)

SSA [redacted] (C-37)

[redacted]

Vic offered [redacted]

[redacted]

- Also, pls send this

Email to [redacted]

Good luck [redacted]!

[redacted]

b6
b7C

Date 1-26-98

Birth Credit Criminal Death INS Marriage* Motor Vehicle Other _____

To OPC Buded

Return to SA C-37 ext 3187 File number _____

Name and aliases of subject, applicant, or employee, and spouse
 

Addresses

Residence _____

Business _____

Former _____

*Date and place of marriage _____
(if applicable) _____

Race <u>White</u>	Sex <input type="checkbox"/> Male <input checked="" type="checkbox"/> Female	Age	Height	Weight	Hair	Eyes
-------------------	--	-----	--------	--------	------	------

Birth date _____ Birthplace _____

Arrest Number _____ Fingerprint classification _____ Criminal specialty _____

Social Security Number _____ Drivers License Number _____
 D/L Photo Other _____

Specific information desired

Results of check

Please call
for pickup.
Thanks.

SEARCHED INDEXED SERIALIZED FILED JAN 2 1999

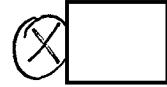
b3
b6
b7C
b7E

b6
b7C

b3
b6
b7C
b7E

1/26/98

1/28/99

FAX**Two pages to follow****Please deliver to:** [redacted] **FBI**b6
b7C**Fax number:** **212-384-4660****From:** [redacted] **The New York Times**
Tel: [redacted]**Date:** **January 28, 1998**b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

01/25/99

Social Security Number [REDACTED] Date of
 Birth [REDACTED] work phone number [REDACTED] was interviewed
 at his residence [REDACTED]
 After being advised of the identity of the interviewing agent and
 the nature of the interview, he provided the following
 information:

In the early part of 1998, [REDACTED]
 an Internet Service Provider in [REDACTED]
 worked alone as a [REDACTED] research
 department. After learning about [REDACTED] warned [REDACTED]
 security department about [REDACTED] hacker background. As a
 result, [REDACTED] sent an employee from their security department to
 [REDACTED] to watch [REDACTED] for a couple weeks. [REDACTED] was
 the [REDACTED] security department employee sent to watch [REDACTED]
 believed [REDACTED] were long time friends.

Around December 1997, [REDACTED] bragged to another [REDACTED]
 employee about his hacking and exploits. [REDACTED]
 supervisor at the time, put a sniffer on [REDACTED] computer for
 approximately four days. [REDACTED] computer IP address was
 [REDACTED] and the DNS address was [REDACTED]. The
 sniffer logs showed [REDACTED] compromising numerous computers. A
 list of the compromised computers was provided to the writer. In
 addition, the sniffer captured an email between [REDACTED] and [REDACTED]
 [REDACTED] (ph), [REDACTED]. The email directed [REDACTED] to
 hack [REDACTED] and change [REDACTED] routing tables. [REDACTED] had
 [REDACTED] analyze the logs. After reviewing the logs, [REDACTED] contacted
 the victims to notify them that their computer's had been
 compromised.

According to the sniffer logs, [REDACTED] commonly launched
 intrusions from [REDACTED] compromised computers by [REDACTED]

Once a computer was compromised, [REDACTED]

Investigation on 01/24/99 at [REDACTED]

File # [REDACTED] Date dictated 01/25/ [REDACTED]

by SA [REDACTED]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6
b7Cb6
b7Cb6
b7Cb6
b7C
b7Eb3
b6
b7C
b7E

[redacted]

b3
b7E

Continuation of FD-302 of [redacted], On 01/24/99, Page 2

read email and greped for "security", "hack", [redacted] and
"exploit". In addition, [redacted] commonly [redacted]
[redacted]

b6
b7C
b7E

[redacted] heard recently that [redacted] was [redacted]
[redacted] for [redacted]

b3
b6
b7C
b7E

SEARCHED INDEXED
SERIALIZED FILED

JAN 26 1999

FBI - DC

302

99

DATE BY WHICH
SERIALIZED
UPLOADED

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

12/21/98

[REDACTED] Date of Birth [REDACTED] POB [REDACTED]
 [REDACTED] Social Security Number [REDACTED]

b6
b7C

1,245

[REDACTED] telephone numbers [REDACTED]
 [REDACTED] was interviewed at his residence during the execution of a search warrant on the above referenced address. Supervisory Special Agent (SSA) [REDACTED] was present during the search and much of the interview. After being advised of the identity of the interviewing agents and the nature of the interview, he provided the following information:

During the early morning hours of September 13, 1998, [REDACTED] was in his bedroom using his computer to Internet Relay Chat (IRC), email, and work on his webpage at [REDACTED]. [REDACTED] couldn't recall the exact time, but acknowledged that he was online all night until around 8 or 9 am that morning. [REDACTED] used [REDACTED] (an ISP) dial-up account, but could not recall the account or user id. [REDACTED] advised he no longer used the account. [REDACTED] had multiple sessions open and received an email message from [REDACTED]. The message indicated the New York Times website had been hacked. [REDACTED] immediately went to the New York Times website (www.nytimes.com) to verify the hack. Five to ten minutes later, [REDACTED] posted the email to the [REDACTED]. A few minutes later, [REDACTED] reloaded the New York Times webpage and saw the corrected webpage. [REDACTED] did not view the website again that day. [REDACTED] was sleeping in his own room during the early morning hours of September 13, 1998.

b3
b6
b7C

Upon viewing the hacked page, [REDACTED] saw the HACKING FOR GIRLIES (HFG) hacked page. [REDACTED] laughed when he saw the HFG hacked page because the victim was the New York Times. [REDACTED] was amused because millions of people rely on the New York Times for their news. [REDACTED] was surprised that a website like the New York Times had not been hacked earlier.. [REDACTED] had discussed the subversion of information theory with others on IRC many times. [REDACTED] followed the New York Times hack closely because he needed to be aware of new exploits and vulnerabilities used by hackers. The New York Times was a big website and was considered one of the ten most secured sites about two years ago.

b6
b7C

Investigation on 12/16/98 at [REDACTED]
 File # [REDACTED] Date dictated 12/21/98
 by SA [REDACTED]

b3
b6
b7C
b7E

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 2

b6
b7C

[redacted] admitted he had hacked in the past, [redacted]
[redacted] computers.
[redacted] advised he had retired from hacking
[redacted]

b6
b7C
b7E

[redacted] knew HFG was a hacking group that had hacked Rt66.com, NASA, MOTOROLA, PHRACK, New York Times, and others. HFG was unique because they embedded text comments into the HTML code of the hacked pages. [redacted] denied he or [redacted] were members of HFG. [redacted] denied ever calling anyone [redacted] or [redacted]. [redacted] believed HFG member [redacted] was the same hacker that used the alias [redacted] (ph) a couple years ago. [redacted] knew [redacted] well and gave him a shell account on his [redacted] domain. [redacted] never met [redacted] in person, but communicated with [redacted] via email. [redacted] last contact with [redacted] was over two years ago. [redacted] told [redacted] he was [redacted]

b6
b7C

[redacted] was asked by SSA [redacted] if his apartment was the apartment described in the HFG article in FORBES dated 11/16/98. [redacted] stated that he did not want to answer the question because he could incriminate himself. Later, [redacted] denied that his residence was the residence described in the article. [redacted] advised the article mentioned a condominium, but his residence was an apartment.

b6
b7C

[redacted] met [redacted] FORBES reporter, online about a year and a half ago and helped [redacted] with technical aspects in past hacking articles. [redacted] asked [redacted] to help him with a story about [redacted] [redacted] came to [redacted] residence to get help with technical aspects regarding the HFG article that he was writing. During the three hour meeting, [redacted] explained buffer overflows and Tripwire to [redacted]. After the meeting at around 4:30 pm or 5:00 pm, [redacted] and [redacted] had dinner at [redacted]. After dinner, [redacted] and [redacted] returned to [redacted] residence. [redacted] took a nap while [redacted] watched TV. A few hours later, [redacted] drove [redacted] to the airport. [redacted] took a flight back to New York.

b6
b7C

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 3

[redacted] met [redacted] at DEFCON IV or V. [redacted] and [redacted] discussed starting a computer security/intrusion company. At the time, [redacted] was not interested because he had a good job working at [redacted] as a computer security consultant. Around March 1998, [redacted] was laid off from [redacted] and had no other job offers. [redacted] and [redacted] then decided to start the computer security/intrusion company they had discussed earlier. [redacted] moved from [redacted] to [redacted] to start [redacted].

b6
b7C

[redacted] provided \$50,000 as start-up capital. [redacted] did not contribute any start-up capital. [redacted] had no business for the first five months, but it was starting to pick up. In November 1998, [redacted] ran out of money and as a result [redacted] had not been paid one or two paychecks.

[redacted] duties at [redacted] include maintaining the bug and exploit database, assisting [redacted] and [redacted] with client's technical questions, assisting in developing SECURE REMOTE STREAMING software (SRS), and maintaining the [redacted] webserver. [redacted] clients include [redacted] and others [redacted] could not recall.

b6
b7C

[redacted] stated he "hated [redacted]" because [redacted] had slandered and libeled him. A few years ago, [redacted] accused [redacted] of hacking [redacted] offered [redacted] part of the profits from [redacted] if he would help her. [redacted] wanted [redacted] to admit to hacking [redacted] so she could write about it. [redacted] refused [redacted] offer. [redacted] has tried to get [redacted] fired from every job he has held since meeting her. [redacted] admitted to calling [redacted] a [redacted]. If [redacted] had held her recent press conference in [redacted] he would have gone to harass her.

b6
b7C

[redacted] characterized [redacted] as an awful reporter whose stories about hacking were technically inaccurate. [redacted] stated that [redacted] first book "set him off". [redacted] was exploiting the hacker hype and his coverage of [redacted] was tacky. [redacted] did not like [redacted] exploiting [redacted] to make money. The media was hyping and sensationalizing the [redacted] case. [redacted] was a criminal, who broke the law and deserved to be caught. [redacted] felt the Government was treating [redacted]

b6
b7C

Continuation of FD-302 of [redacted], On 12/16/98, Page 4

b3
b6
b7C
b7E

unfairly because he had [redacted]

[redacted] met [redacted] when [redacted] co-located their computers at [redacted]. [redacted] described [redacted] as a nice guy who was technically competent, and who knew a lot about Berkeley Software Design (BSD). [redacted] and [redacted] have gone out socially to dinner. [redacted] met [redacted] [redacted] a system administrator for [redacted]. On another occasion, [redacted] and [redacted] came to [redacted] residence and hung out for a few hours with [redacted] and [redacted].

b6
b7C

Last year [redacted] met [redacted] [redacted] at the USENIX (ph) computer security conference. [redacted] was rumored to be a real good hacker that had retired from hacking. [redacted] talks to [redacted] on a regular basis. [redacted] last contact with [redacted] was approximately three weeks ago. During their last conversation, [redacted] was depressed that he might lose his job and a girl he really liked had rejected him. [redacted] often calls [redacted] looking for moral support and encouragement. [redacted] told [redacted] he's lonely in [redacted] and felt that [redacted] (ph) deserted him when [redacted] moved to [redacted] land. [redacted] have gone out to dinner and then to [redacted] several times. A few months ago, [redacted] spent an afternoon at [redacted] residence. On that occasion, [redacted] and [redacted] talked about Intrusion Detection Systems and other computer security issues. [redacted] communicates with [redacted] thru IRC. [redacted] uses a different alias every time he IRC. Last summer, [redacted] took [redacted] to dinner. At dinner, they discussed bugs and other technical problems [redacted] was having with its SECURE REMOTE STREAMING (SRS) software. The purpose of the dinner was to get [redacted] assistance on possible patches for the SRS software.

b6
b7C

[redacted] met [redacted] a.k.a. [redacted] [redacted] after moving to [redacted] works for [redacted] as a system administrator responsible for securing the [redacted] server and described [redacted] as a big crypto (encryption) guy. [redacted] lives in [redacted] but visits [redacted] frequently. [redacted] brings a laptop with him when he visits. [redacted] created graphics for [redacted] domain as well as [redacted] webpage at [redacted]. [redacted] didn't think [redacted] was a member of HFG, because [redacted] mirrored the HFG hacks on his webpage. [redacted] sent

b6
b7C

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 5

b6
b7C

[redacted] a tar file that contained all the HFG hacks. [redacted] could not recall why [redacted] sent the file to him.

b6
b7C

[redacted] met [redacted] a.k.a. [redacted] on IRC. [redacted] moved from [redacted] to [redacted] to live with [redacted]. They lived together for approximately one and a half years. [redacted] lives in [redacted] and works as a system administrator for [redacted]. [redacted] created many of the graphics that [redacted] had on his webpage. [redacted] and [redacted] had not talked to [redacted] since July 1998.

b6
b7C

Approximately three months before moving to [redacted] [redacted] met [redacted] on IRC. [redacted] and [redacted] discussed [redacted] working for [redacted] after graduating from high school. Before graduating, [redacted] went to [redacted] for a week. The purpose of the trip was to meet [redacted] and see if he and [redacted] were compatible roommates. Shortly after graduating, [redacted] moved from [redacted] to live with [redacted] in [redacted].

b6
b7C

[redacted] is proficient with the Linux and Solaris operating systems. [redacted] frequently uses his laptop computer which contains information about all of his accounts. [redacted] advised the laptop contained encrypted files. SA [redacted] asked [redacted] for the encryption password, but [redacted] refused. [redacted] advised that he wasn't sure what was in the encrypted files and that he wanted to protect himself. [redacted] has numerous shell accounts. [redacted] login/user id to his shell accounts is [redacted]. The only exception is [redacted] shell account at [redacted]. [redacted] user id is [redacted]. [redacted] uses the account to subscribe to [redacted] mailing list so he can monitor what [redacted] is saying about him.

b6
b7C

[redacted] denied having two social security numbers. [redacted] advised there was another [redacted] who lived in [redacted]. [redacted] stated that he recently dropped his middle name from his credit report. [redacted] denied changing the name on his credit report to [redacted]. [redacted] advised that the credit card representative may have misheard him when he was dropping his middle name. [redacted] never lived at [redacted] or had any contact with the residents living there.

[redacted] a.k.a. [redacted] is a WINDOWS NT system

[redacted]

b3
b7E

Continuation of FD-302 of [redacted], On 12/16/98, Page 6

administrator at [redacted].
[redacted] introduced [redacted] to his bosses at [redacted].
convinced his bosses to test the SRS software.

b6
b7C

[redacted] uses IRC to talk to most of his friends. He
hangs out in [redacted]
female IRC friends include [redacted] and
[redacted].

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription

1/29/99

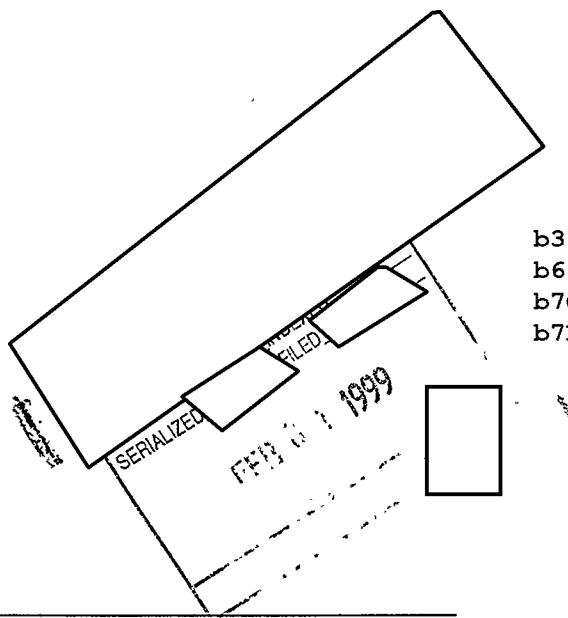
The following examination was conducted by a Computer Analysis Response Team (CART) Field Examiner:

SPECIMEN(S) :

 b6
 b7C
 b7E

UPLOADED

WITH TTD _____
WITH C _____
BY _____
DATE 2-3-99



Investigation on 1/29/99 at New York, NY

File # Date dictated by SAs and

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

 .302b3
b6
b7C
b7Eb3
b6
b7C
b7Eb6
b7C

(01/26/1998)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/29/1999

To: [REDACTED]
[REDACTED] (Info)
[REDACTED] (Info)
New York
[REDACTED] (Info)
[REDACTED]

Attn: MMOC, Squad 19
SA [REDACTED]

b6
b7C

From: National Security
CIU/CIOS/NIPC
Contact: SSA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

b3
b7E

Title: [REDACTED]

b6
b7C

INTRUSION - INFO SYSTEMS;

Synopsis: Dissemination of source information concerning captioned subject.

Details: Reference [REDACTED] EC to National Security [REDACTED], dated 12/28/1998.

b3
b6
b7C
b7D
b7E

For information of receiving offices, [REDACTED] advised the National Infrastructure Protection Center (NIPC) of source information obtained on 12/01/1998, concerning the captioned subject, identified as a computer "hacker" currently living in [REDACTED]

MAR 1 1999

To: [REDACTED] From: National Security
Re: [REDACTED] 01/29/1999

The source provided the following information pertaining to the captioned subject:

[REDACTED]

[REDACTED]

The source received this information from [REDACTED]

[REDACTED]

The following is [REDACTED] information pertaining to [REDACTED] respectively:

[REDACTED]

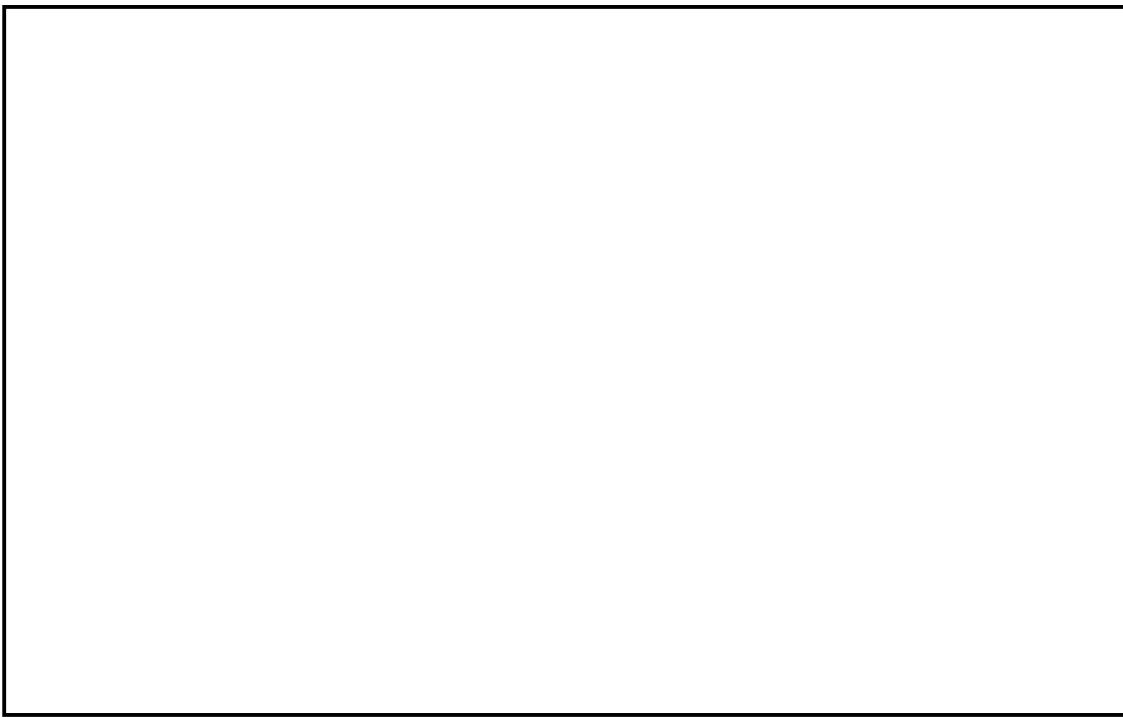
b3
b6
b7C
b7D
b7E

b6
b7C
b7D

b6
b7C
b7D

To: [REDACTED] From: National Security
Re: [REDACTED] 01/29/1999

b3
b6
b7C
b7D
b7E



The receiving offices were identified through a subject name search using FBI/ACS and this information is being provided for information purposes for whatever action deemed appropriate. Information provided to [REDACTED] Division, whereas the captioned subject reportedly resides within the [REDACTED] Division [REDACTED]
[REDACTED]

b6
b7C
b7D

The source expressed concern relating to the disclosure of their identity in relation to investigations of the captioned subject and any further questions pertaining to this information should be directed to the [REDACTED] Division, MMOC, Squad 19, SA
[REDACTED]

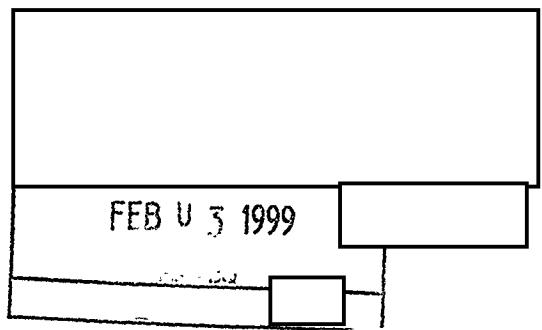
♦♦

b3
b6
b7C
b7E

"**UPLOADED**"

WITH/TEXT _____
WITH/OUTTEXT _____
BY _____
DATE 2-1999

File - "lead2703.cc"



FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 02/03/1999

To: [redacted]

Attn: SA [redacted]

✓From: New York

C-37

Contact: SA [redacted] 212.384.3187

Approved By: [redacted] [redacted]

Drafted By: [redacted]

Case ID #: [redacted] (Pending)

Title: HFG -HACKERS FOR GIRLS

Et al.

NEW YORK TIMES - VICTIM

CITA;

OO:NY

Synopsis: To set a lead to deliver a 2703(d) court order.

Reference: Telephone call between SA [redacted] and SA [redacted]

Enclosures: 2703(d) Court Order [redacted] issued in the Southern District of New York SDNY.

Details: On 02/03/98, a 2703(d) was issued for [redacted]
[redacted] from [redacted]

[redacted] has been contacted and is expecting the order.

b3

b6

b7C

b7E

b6

b7C

b7E

To: [REDACTED] From: New York
Re: [REDACTED] 02/03/1999

b3
b6
b7C
b7E

LEAD (s):

Set Lead 1:

[REDACTED]

AT [REDACTED]

b6
b7C
b7E

Hand deliver the enclosed 2703(d) Court Order
[REDACTED] issued in the Southern District of New York (SDNY) to
[REDACTED] at the following address:

[REDACTED]

♦♦

UPLOADED

WITH/TEXT _____

WITH/OUT TEXT _____

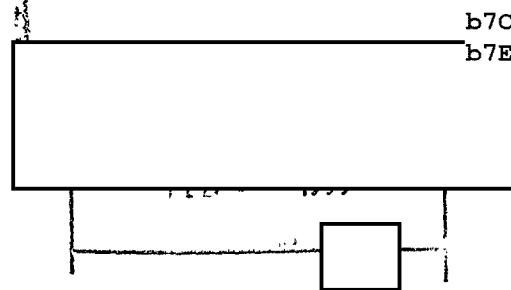
IE _____

DATE _____

SEARCHED

LEADS

file - "lead-grl.ec"



FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 01/26/1999

To: [redacted]

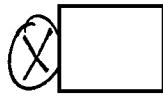
Attn: SA
Attn: SA
Attn: SA

From: New York

C-37

Contact: SA [redacted]

212-384-3187

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: [redacted] ding)

Title: HACKING FOR GIRLIES;
et al.;
New York Times - Victim
CITA
OO:NY

Synopsis: Interview female associates of [redacted]
a.k.a. [redacted]

b6
b7C

and [redacted] aka [redacted]

Enclosures:

a.k.a. [redacted] -Forbes article; DMV photo of [redacted]

b6
b7C

[redacted] a.k.a. [redacted] -Forbes article; two photos of [redacted]

a.k.a. [redacted] -Forbes article; five photos of [redacted]

Details: On the morning of September 13, 1998, the New York Times website (www.nytimes.com) was hacked by a group known as HACKING FOR GIRLIES (HFG). The hackers altered the NY TIMES website with a webpage containing various text messages and graphic images. On the hacked page, the text ridiculed [redacted]

b6
b7C

[redacted] a NY Times reporter and [redacted]. As a result, the NY Times took their main web servers off-line for approximately nine hours. Other parts of the website were down approximately a week. HFG has claimed responsibility for hacking the New York Times, NASA-Jet Propulsion Labs, MOTOROLA, PENTHOUSE, ELITEHACKERS.ORG and RT66.COM.

REFUGEE

To: [REDACTED] From: New York
Re: [REDACTED] 01/19/1999

b3
b6
b7C
b7E

On 12/16/98, search warrants were executed in the [REDACTED] division on [REDACTED] residence and [REDACTED]

b6
b7C

[REDACTED]
live together and work for [REDACTED]
was started by [REDACTED]

[REDACTED] and [REDACTED] were both interviewed about their involvement with HFG and the New York Times hack. [REDACTED] and [REDACTED] denied being members of HFG. However, [REDACTED] admitted he was interviewed in [REDACTED] by [REDACTED] FORBES reporter, for the HFG article. [REDACTED] also stated he "hated" [REDACTED] and that [REDACTED] was exploiting [REDACTED] for his own personal monetary gain. Additionally, [REDACTED] is the [REDACTED]
[REDACTED] As the [REDACTED] has a history of critiquing the media's coverage of hackers. [REDACTED] has a website [REDACTED] about his hatred for [REDACTED]

b6
b7C

As a result of the interviews and other evidence, [REDACTED] were identified as close personal friends of [REDACTED] and [REDACTED] communicates with them on Internet Relay Chat (IRC) [REDACTED] or email on a daily basis. During the interview, [REDACTED] was extremely nervous talking about his female friends. [REDACTED] may have confided with one of females regarding his involvement in HFG or the New York Times hack in order to impress them.

b6
b7C

To: [REDACTED] From: New York
Re: [REDACTED] 01/19/1999

b3
b6
b7C
b7E

LEAD (s):

Set Lead 1:

[REDACTED]

b6
b7C

AT [REDACTED]

Interview [REDACTED] a.k.a. [REDACTED] DOB [REDACTED]
Social Security Number [REDACTED]
[REDACTED] about any knowledge she may have regarding [REDACTED]
[REDACTED] and [REDACTED] past hacking activities, the New York
Times hack and HFG. [REDACTED] has no criminal history.

Set Lead 2:

[REDACTED]

b6
b7C

AT [REDACTED]

Interview [REDACTED] a.k.a. [REDACTED] DOB [REDACTED]
[REDACTED], Social Security Number [REDACTED]
[REDACTED] about any knowledge she may have
regarding [REDACTED] and [REDACTED] past hacking
activities, the New York Times hack and HFG. [REDACTED] has no
criminal history.

Set Lead 3:

[REDACTED]

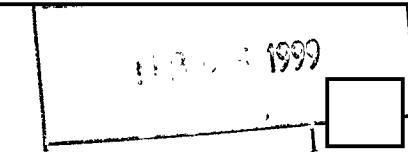
b6
b7C

AT [REDACTED]

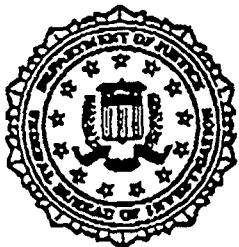
Interview [REDACTED] a.k.a. [REDACTED], DOB [REDACTED],
Social Security Number [REDACTED] Driver's License
[REDACTED] about any
knowledge she may have regarding [REDACTED] and [REDACTED]
[REDACTED] past hacking activities, the New York Times hack and
HFG. [REDACTED] has no criminal history.

♦♦

b3
b6
b7C
b7E



Federal Bureau of Investigation

Date: January 21 1999

PLEASE DELIVER THE FOLLOWING PAGES TO:

Name: SA C-37 X-3187Agency: FBI NY Phone #: () FAX NUMBER: (212) 384-2745 *This Facsimile Message is being sent by:*Name:

✉ FAX # → ✉Number of Pages, INCLUDING this Cover Sheet 4

(6)

Approval: Date Sent: 1/21/99 Time Sent: 9:16 Initials:

b6
b7c

HACKER NEWS NETWORK

02-11-99

Write for HNN!



Complete Internet Privacy:
ANONYMIZER

FREE KEVIN

Powered by
OpenBSD

From: Adam Penenberg

Article: Hacker News Network

Feb. 8, 1999

re:

dated 02-08-99

Open letter to the hacking community:

Last week, Steve Silberman of Wired News called to tell me he and I and some other journalists had been duped by a psuedo-hacker named Christian Valor, AKA se7en. In April 1998, I'd posted a piece on the Forbes Digital Tool web site about Valor's kiddie porn vigilantism and the fact that law enforcement knew what he was doing, but turned a blind eye. Cool story. Too bad it turned out not to be true.

I was certainly in good company. Steve also had written about Valor's exploits, as had Newsday, the Independent in London, etc. Both Steve and I received letters from se7en's ex-girlfriend simultaneously last week, but Steve got on to the story first. I was out of town. Sad to say, he and I were the only ones to respond to her letter. I told Steve I wouldn't post anything until his story hit. (See "[Kid-Porn Vigilante Hacked Media](#)").

I can't comment on how Steve or the Independent or Newsday conducted their research, but I would like to share with all of you how I did mine, and what went wrong. I'm sure there are lessons to be learned.

As you may or may not know, I am no stranger to taking on journalists I think have concocted stories out of thin air. I broke the Stephen Glass story, the associate editor of The New Republic who made up a story on hackers and was later discovered to have made up some three dozen stories for a number of well-known publications (See "[Lies, damn lies and fiction](#)"). I also took on Beth Piskora of The New York Post, who I believe made up a sexy tech story on Organized Crime setting up phony companies for Y2K remediation, who then, she claims, inserted software to divert money from bank accounts (read: clients) to mob-controlled accounts. (See "[Phantom mobsters](#)"). This canard was picked up by Vanity Fair in a recent feature on Y2K. Vanity Fair has yet to admit it published a lie.

I hate it when you nail a journalist and instead of coming clean, he or she hides. This is what both Glass and Piskora have done. That's why I'm writing this note.

buffer
overflowhnn
archivese7en
kid-porn
vigilante
hacked media
journalists
duped
Christian Valor
AKA se7en
Wired News
Steve Silberman
Newsday
Independent
London
ex-girlfriend
simultaneously
last week
got on to the story first
was out of town
sad to say
only ones to respond
her letter
told Steve
wouldn't post anything
until his story hit
Kid-Porn Vigilante Hacked Media

Recent News

- [HNN Store Opens](#)
- [Se7en Exposed](#)
- [Off the Hook may go silent](#)
- [Buffer Overflows serious threat](#)
- [\[.tp\] domain cracked](#)
- [LoU China Iraq War](#)
- [Today](#)
- [Yesterday](#)
- [02/09/99](#)
- [02/08/99](#)
- [02/07/99](#)
- [02/06/99](#)

PISKOVA HAVE DONE. THAT'S WHY I'M WRITING THIS NOTE.

For my story (Kiddie porn vigilante) I knew I couldn't get on IRC and traffic in kiddie porn on a Forbes computer. You remember what happened to that journalist for NPR who did, and is now had to plead guilty to a felony all because he was ostensibly researching a story? So I relied on law enforcement, EHAP, and NAMBLA. I called literally 10 law enforcement officials who said they studied under Valor in one of his security courses. On the record, they would all vouch for se7en's hacking skills. Off the record, they all said they knew what he was doing but they didn't care. Everyone hates kiddie porn traffickers.

I also talked to EHAP, and they told me they were distressed by se7en's actions, because it gave hackers a bad name. Se7en should turn them over to the cops or the ISPs, they said, not break the law in going after them. They didn't say he was a fraud.

I also contacted NAMBLA through its web site. I asked if anyone knew a hacker named se7en, who was purportedly going after kiddie porn traffickers on IRC. I received a cryptic response, something along the lines of, "Yes, some of our members have been complaining about this guy. We just want to be left alone." End of conversation. He refused to turn over any other details.

So I felt confident that with all this cross-checking that Valor was who he said he was. Obviously, I made a mistake. I think the most important lesson I learned is that law enforcement doesn't have a clue what really goes on in hacking circles; they are not good sources for this. I also now won't write a hacking story unless I can meet the hacker face-to-face and actually see evidence that I can then verify with other hackers or computer security experts I trust. This is how I approached my story for Forbes magazine on the NY Times hack that ran last fall (available online at: <http://www.forbes.com/forbes/98/1116/6211132a.htm>).

If you want to send me taunting email, telling me what a fool I was, feel free. I'm at apenenberg@forbes.com. But you can't possibly be harder on me than I've been on myself this past week. You live, you learn.

Sincerely,
Adam Penenberg
Senior Editor, Forbes Magazine

02/06/99
02/05/99
02/04/99

H N N

These pages are Copyright © 1998 Hacker News Network All Rights Reserved.

AFTER THE HACK — Article

Questions Follow the Times Attack

by Arik Hesseldahl

Within days in mid-September, the Internet demonstrated both its massive strength and its scariest weakness. On September 11, tens of thousands of people downloaded the Starr Report from the many Web sites that made the text available, giving the new medium a sense of critical mass. And on September 13, hackers attacked the Web site of *The New York Times*, forcing editors to pull the plug on the digital edition of the newspaper of record for nearly nine hours. Months after the hack, lingering questions remain: Who carried it out? Why? Who's vulnerable?

The apparent goal was to bring attention to the case of jailed hacker Kevin Mitnick, the hacker underground's favorite martyr. For more than three years Mitnick has been awaiting trial on

Early on the morning of September 13, Bernard Gwertzman, the site's editor, and Richard Meislin, editor-in-chief of New York Times Electronic Media Co., discovered that the entry page to the *Times* site (www.nytimes.com) had been replaced with a page built by HFG, for "Hacking for Girly." This is a group that claims to have invaded the Web sites of organizations as diverse as NASA, Motorola, and *Penthouse* magazine.

People logging into the *Times* site found all this news unfit to print: a mildly obscene HFG logo, a rambling statement attacking Markoff for putting "Kevin" in jail, and attacks on Shimomura, Matt Richtel (another *Times* tech reporter), and Carolyn Meinel, a New Mexico computer security consultant who writes about hacking for *Scientific American*



Visitors to *The New York Times*'s Web site on September 13 got this on their computer screens.

a twenty-five-count federal indictment charging him with various hacking-related crimes, from wire fraud to unauthorized access to a federal computer. His trial is scheduled to begin April 20.

The "Free Kevin" crowd blames the *Times*, particularly its San Francisco-based technology reporter John Markoff, for causing Mitnick's arrest in 1995. Markoff's stories in the *Times* led to a book, *Takedown*, which he co-wrote with Tsutomu Shimomura, a California computer security expert who helped the FBI capture Mitnick. Supporters of Mitnick think the book exaggerates his alleged crimes. And now the book is about to become a movie, to be released in 1999 by Miramax.

and published a book on the subject, *The Happy Hacker*.

Times editors tried to publish over the vandalism, but the offending page kept reappearing. After a few hours they took the site offline completely and began to comb through the *Times*'s computers, looking for ways to correct the problem. Some parts of the site, including the *Times*'s archive files, remained offline for several days as security consultants looked for evidence of other, more subtle damage. Since the hackers had complete control, might they have, for example, changed the text of old stories, purloined a file of credit card numbers, or left a "back door" that would allow them to return?

As the FBI's computer crimes unit

continued to investigate, a *Forbes* reporter claimed to have succeeded where many others have failed: he found and interviewed two HFG members, who call themselves Slut Puppy and Master Pimp. The reporter was Adam Penenberg, best known for being the first to investigate one of Stephen Glass's fabricated *New Republic* stories. In the interview the two said they attacked the *Times* because they were "bored."

Other clues in the case point tentatively in the direction of Brian Martin, a Scottsdale, Arizona, computer security consultant and a frequent source of Penenberg's. Martin runs a computer security newsletter, and was one of the first to spread the word of the *Times* hack. Also known by the hacker name Jericho, Martin has a complicated grudge against Meinel, the New Mexico writer, over credit he thought he was due in her book.

In an interview, Martin conceded that he is certain that his name is on the FBI's list of suspects. He was also once widely suspected to be "Angry Johnny," a hacker who about two years ago, harassed reporters — Markoff included — with e-mail "bombs" (a technique of overwhelming a target's e-mail account with thousands of messages). HFG, in the text of the statement it posted on the *Times* site, announced the enlistment of a new member named Resentful Jonathan.

"Some people thought I was Angry Johnny. As a result, they thought I was Resentful Jonathan after the *New York Times* hack," Martin says. "They were incorrect on both."

Both the scheduled start of Mitnick's trial and the release of the movie based on *Takedown* could encourage further hacking incidents, whether by HFG or others. "It's inevitable," says John Vranesovich, the nineteen-year-old founder of AntiOnline, a clearinghouse for news of the hacking scene (www.antionline.com).

What can Web site managers do? "Securing your site is not an event, it's a process," Vranesovich says. "New system vulnerabilities are coming out every day. It's a constant challenge."

—Arik Hesseldahl

Hesseldahl writes frequently about Internet issues.

b6
b7C

FU

1
S
I

Fo
pa.
pr.
jo.
Yo
be.
sci
fr.
Co
ab
it
th
st:
Sc

]
th
de
m
L
w
b
n
u
n
r
o:
si
n
is
w

p
v
a
n
T
c
ir
h
c
ir
v
r
is

14
JANUARY/FEBRUARY 1999 COLUMBIA JOURNALISM REVIEW
b3
b7E

Automated Serial Permanent Charge-Out
FD-5a (1-5-94)

Date: 02/19/99 Time: 10:22

Case ID: [REDACTED]

Description: [REDACTED]

b3
b6
b7C
b7E

Type : OTHER

Date : 02/08/99

To :

From :

Topic: SEARCH DATABASE FORM FOR [REDACTED]

Reason for Permanent Charge-Out:

MISFILED

Employee: [REDACTED]

b3
b6
b7C
b7E

Upload# _____

Initials/Date

Case Agt:

Desk

Searched

Serialized:

Indexed

Filed

12/16/99

2/19/99

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/01/99

Source, who is not in a position to testify, provided the following information:

On or about [redacted]

[redacted]

b6
b7C
b7D

Investigation on 02/01/99 at [redacted] N/A
File # [redacted] Date dictated _____
by SA [redacted]

b3
b6
b7C
b7D
b7E



- Did you see this ?
- Indexing ?



SEARCHED	INDEXED
SERIALIZED	FILED
MAR 02 1999	
FBI - MEMPHIS	

b3
b6
b7C
b7E

- 1 -

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 01/11/99

Source, who is not in a position to testify, provided
the following information:

[Large redacted area]

(X) [Redacted box]

b6
b7C
b7D
b7E

Investigation on 01/11/99 at [Redacted] b3
File # [Redacted] Date dictated N/A b6
by SA [Redacted] b7C
b7D
b7E

SEARCHED INDEXED
SERIALIZED FILED

MAR 1 1999

FBI - NEW YORK

b3
b6
b7C
b7E



The Granny Hacker From Heck

Tuesday, February 23, 1999 at 11:43:38

by Carolyn Meinel - Writing For AntiOnline



[*About The Author](#)
[Print Friendly Version](#)
[Comment On This Story](#)

b6
b7C

I sit in my home office, slaving over a hot computer. It's an NT server; next to it is an Indigo running Irix 6.2. Across the room is my Slackware box. They are linked by, ta, da! Ethernet. Two modems hum with TCP/IP over PPP.

I'm the grannie hacker from heck. Elite d00dz tremble before my wrath. You don't believe me? Check out this (<http://www.attrition.org/slander/content.html>). See? Some of the scene's most dreaded hackers and brilliant computer security experts are trembling before my awesome skillz as, so they say; I run around erasing the systems files of helpless hacker boxes. I'm talking about people such as admitted black hat (<http://www.wired.com/news/news/culture/story/16872.html>) Brian Martin, AKA jericho, trembling in his boots. You know, the computer security professional from Repent Security, Inc. (<http://www.repssec.com>) Come on, check this out (<http://www.attrition.org/slander/content.html>) and see how terrified he is of me!

The AntiOnline Newsletter
 To get the latest news delivered to your inbox every day, just enter your e-mail address below.

AntiOnline's

 Software CDs Books Magazines Hardware And More.... [click here](#)

Heck, even some FBI agents think I've waged a war of naughty images plastered over the likes of the New York Times and PenthouseWeb sites -- that I'm the Hacking for Girliez gang. Don't believe me? Martin even has a sound bite on his Web site with me apparently confessing to their crimes! (<http://www.attrition.org/shame/www/admit.html>)

So how did I become the grannie hacker from heck? It all started in 1995 when I went to Def Con III. Being such a good housekeeper, I couldn't help but be the person who discovered a live phone line in the convention ballroom. Of course I sprawled out on the floor, plugged my laptop into the line and telneted into a shell account. Lo and behold, "Evil Pete" Shipley, leader of the Dis Org gang (<http://www.dis.org/doc.html>), strode over. He was quite a wonderment, with fangs and spurs and lovely black hair flowing to his waist. He crouched down beside me and asked, "You got a telnet session going?"

"Yup."

"May I borrow it for a minute? I need to do something at work."

That was when the naughty side of me took over, you know, the Mrs. Hyde thing. "Suurreee:)," I replied. I handed my laptop to him, then leaned over and clicked a function key.

"What did you just do?" Evil Pete demanded.

"I turned on logging." I tried to wipe the cat got the canary look off my face.

"You tried to steal my password!" Evil Pete stood up and started shouting, to no one in particular, "This woman tried to hack me! Bad hacker etiquette!"

"Sheesh," I pouted. "It's my computer, I can run keystroke logging if I want to!"

Maybe I was plum lucky. Full as that ballroom was with guys toting Miranda cards, not a single Fed rushed over to bust me. That was what really got me inspired. I could hack a big wig computer security fellow right in front of the Feds, and get away with it! The sense of power drove me mad, muhahaha....

Anyhow, that is how I got started persecuting the biggest and the baddest hackers and computer security experts on the planet.

Recently the organizer of Rootfest (<http://www.rootfest.org>) kicked me off the program of his hacker con because Evil Pete had warned him that I had put out a special, secret Guide to (mostly) Harmless Hacking showing newbies how to hack Pete's dis.org domain. Pete even showed him a copy of this GTMHH, a special edition of Vol.1, #3. It's one that you won't find anywhere on the Web, I think only Pete, Mr. Rootfest and I have copies of it. Anyhow, this smart move of Pete's has saved the planet from the live "how to hack" class I was going to teach at Rootfest.

Intoxicated as I am by hacking, nowadays my spinning wheel sits gathering dust, and a shirt I was sewing lies half-finished. I used to be such a sweet housewifey, I swear! You don't believe me? I have witnesses! I used to demonstrate wool carding at the New Mexico State Fair! I used to make gourmet goat cheese and station bouquets of cut flowers from my greenhouse in Martha-Stewart-approved locations about my home.

What caused my fall from the Better Homes and Gardens set? The sweet taste of being a meanie against the world's hairiest

hackers!

Sooo, will the rampage of grannie hacker from heck ever end? My victims are trying to figure out how to defend themselves against me. Evil Pete told the organizer of Rootfest that in self defense, my hacker victims have brought many lawsuits against me. Much more effective than a firewall, right? Especially against us Uberhacker grannies!

Now, I haven't seen any of these lawsuits, but as we all know, hackers never lie. The suspense is getting to me. When will this army of lawyers my victims have marshalled actually materialize? Will they sue me into submission? How much more damage will I and my Happy Hacker (<http://www.happyhacker.org>) army of newbies do before lawyers save the world from my depredations? Stop me before I hack again!

In the meantime, while waiting for the lawyers to save you, what can you do to keep me from making naughty body parts sprout on your Web site? Here are my top five suggestions:

- 1) Buy my Happy Hacker book. I don't rm the operating system of anyone who buys my book, because after reading it you will know enough to protect yourself from me. Also, when you see me trying to secure shell into your ftp port, you'll know I'm just yanking your chain.
- 2) Send me computer jokes. I'm a sucker for them and will be too busy laughing and forwarding them to my friends to hack you. The following is an example of something that meets my laughability standards:

An engineer, a systems analyst, and a programmer are driving down a mountain road when the brakes fail. They scream down the mountain gaining speed every second and screeching around corners. Finally they manage to stop, more by luck than by judgment, inches from a thousand foot drop to the jagged rocks on the valley floor. More than slightly shaken, they emerge from the car. "I think I can fix it," says the engineer. The systems analyst says, "No, I think we should take it into town and have a specialist examine it." The programmer, holding his chin between thumb and forefinger says, "Okay, but first I think we should get back in and see if it does it again."

- 3) Give me a 120 cubic meter Cameron hot air balloon with complete accessories, you know, stuff like a rate of ascent/descent meter, GPS, one ton king cab chase truck with Tommylift gate... I'll be so busy accidentally landing on the classified areas of Sandia Labs, Area 51 etc. that I'll retire my

computers next to the spinning wheel and unfinished shirt. I can see it now, "Gosh, Colonel, you know how these balloons are, I got caught in a thermal and next thing I knew I was here:)"

4) After we had a fight, my ex-husband used thermite to melt down our 30 mm Finnish antitank gun. Gimme another one. With ammunition. Or else.

5) Our church music director could use 50 copies of the score for Jesus Christ Superstar. If I can get some snivelling coward to give them to us in exchange for me promising not to hack him, maybe I can get to sing Mary Magdalene. If Lisa gets the part, I'll hack the church computer so Zippy the Pinheadisms creep into the bulletins.

I guess that's enough extortionate demands. I gotta get back to sneaking Trojans into military computers so I can launch World War III while making it look like Y2K bugs so I won't get into trouble. As for those computer security professionals I've been fubarbing, do you suppose I'll ever feel remorse? No way! If they want to call themselves computer security experts, they'd better be ready to take heat from the granny hacker from heck!

Carolyn Meinel (cmeinel@techbroker.com) is a computer fubar expert and clown princess of the non-profit Happy Hacker, Inc. She lives in Cedar Crest, NM with her long-suffering hubby, four cats, three horses, three dogs, two toads and two mosquito fish.

PS: The thing about the thermite is a slight exaggeration. Everything else is true -- remember, you read this on the Internet, so it must be true. Be sure to email a copy of this to Craig Shergold and everyone else your know and Bill Gates will give you \$1000. Be sure to put "Good Times" in the subject. If you don't email this out within ten days, you will be cursed with seven years of bad luck and wake up in a bathtub full of ice with your kidneys missing. Honest!



b3
b6
b7C
b7E

FEB 26 1990

FD-3500 (Rev. 1-22-68)





Date: 2/23/99

FILE #

SA

Det.

SSA

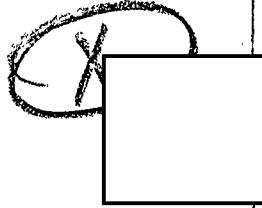
Supv.

ECT

Rotor

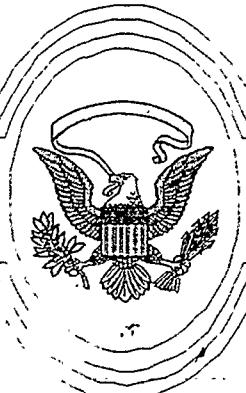
CF

(C-37)



- Attached is your **File Copy FD-192** for the above file number. Ensure it is initialed and entered into your case file for future reference.
- Attached are your **File and Package Copy FD-192's** for the above file number. Ensure the File Copy is initialed and entered into your case file for future reference. *Retain the Package Copy, original chain of custody form, and the enclosed bar-coded plastic envelope with your evidence for future submission into ECU storage.*
- Attached is your copy of an **Electronic Communication** with shipping information for evidence sent out of the New York Office. Please file it for future reference.
- Include the attached as a **1A Exhibit** in the file.

Please call if you have any questions. Thank you for your assistance.



Evidence Technician

x3640 / 3641 (Hudson Street Off-Site)
 x 3462 (26 Federal Plaza Office)

b3
b6
b7C
b7E

b6
b7C