UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

HONORABLE DAVID O. CARTER, JUDGE PRESIDING

- - - - - - -

ECHOSTAR SATELLITE CORP., et al., Plaintiffs,

vs.

NDS GROUP PLC, et al., Defendants.

No. SACV-03-950-DOC
DAY 3, Vol. I

REPORTER'S TRANSCRIPT OF PROCEEDINGS

Santa Ana, California

April 11, 2008

SHARON A. SEFFENS
Federal Official Court Reporter
United States District Court
411 West 4th Street, Room 1-053
Santa Ana, California 92701
(714) 543-0870

SHARON SEFFENS, U.S. COURT REPORTER

I-N-D-E-X

PLAINTIFFS' EXHIBITS:	MARKED	RECEIVED
(None)		
DEFENSE WITNESSES:		
(None)		
DEFENSE EXHIBITS:	MARKED	RECEIVED
Exhibit 809		54

SANTA ANA, CALIFORNIA; FRIDAY, APRIL 11, 2008; 8:00 A.M.

(Jury present.)

THE COURT: The jury is present. Counsel are present. The parties are present.

Mr. Mordinson is present.

Good morning.

THE WITNESS: Good morning.

THE COURT: This is Mr. Hagan's continued direct examination of Mr. Mordinson on behalf of Echostar.

DAVID MORDINSON, PLAINTIFFS' WITNESS, PREVIOUSLY SWORN

DIRECT EXAMINATION (Continued)

BY MR. HAGAN:

Q Good morning, Mr. Mordinson.

A Good morning.

Q You understand that you are still under the oath to tell the truth that you took yesterday; is that correct?
A Yes.
Q It's the same oath that you took at your deposition. Do you recall that?
A Yes.
Q Right before we broke yesterday for the afternoon, we were talking about your completion of the Headend Project where you actually tested successfully the hack methodology that NDS developed for EchoStar's system. Do you recall that?

♀

07:58:47 A Yes.
Q After you tested that hack, I believe your testimony was that you went back over to NDS Israel and you prepared a written a report; is that correct?
A Yes.
Q I would like to take a look at the report this morning and go through some of the sections of it.
MR. HAGAN: Christine, can you provide Mr. Mordinson with a copy of Exhibit 98?
For the record, Your Honor, Exhibit 98 has already been received in evidence.
THE COURT: Thank you.
BY MR. HAGAN:
Q If could you take a moment to look over that document and let the jury know if you recognize it.
A Yes, I do.
Q Can you tell them what that is?
A This is my report, a report that I wrote upon completion of the Headend Project.
Q And this report is dated if you look at the very top right-hand corner November 1998; is that correct?
A Yes.

23 Q And this was the actual final version of the Headend
24 Report that you prepared, correct?
25 A Yes.

07:59:46 1 Q There were a couple of earlier versions and some
2 drafts; is that right?
3 A I believe so, yes.
4 Q And then you captured all of the information that you
5 learned about Echostar's system and the hack that you
6 developed for Echostar's system, and you put it in this
7 final report?
8 A Yes.
9 Q I believe Mr. Shkedy testified yesterday that you
10 distributed this report to certain members of HRC, the Haifa
11 Research Center; is that correct?
12 A Yes.
13 Q You also stored a copy of this report on the servor at
14 NDS HAIFA?
15 A I don't remember, sir. This report was stored on my
16 computer in encrypted form is what I am certain of, but I
17 don't remember anything about saving it on a servor.
18 Q Do you recall if you e-mailed that report out to
19 anyone?
20 A No.
21 Q But you do recall that you hand-delivered a copy of it
22 to Hayim Shen-Or (phonetic), your supervisor at one point in
23 time?
24 A Yes.
25 Q And you went over the results of the hack that you

08:00:45 1 developed with Mr. Shen-Or?

A Say again, please.
Q You went over the results of the Headend Project, your hack for Echostar's system, with Mr. Shen-Or?
A Yes.
Q And you explained to him how you were able to do what you did it with Echostar's system?
A Yes.
Q As you sit here today, you don't know whether or not Mr. Shen-Or provided that information to anyone else within the company, correct?
A Yes.
THE COURT: You are using double negatives. If I read this back, that's an ambiguous answer.
MR. HAGAN: Certainly. Let me clarify it.
THE COURT: He didn't answer it ambiguously. It's in combination with the question. Reask the question.
BY MR. HAGAN:
Q I apologize, Mr. Mordinson.
As you sit here today, you are not aware of whether or not Mr. Shen-Or provided that information from your hack methodology to anyone inside the company, correct?
A That's correct.
Q And you are also not aware whether or not Zvi Shkedy provided this report or the information contained within

♀

this report to any other employees at NDS, correct?
A Correct.
Q And if Mr. Shkedy testified yesterday under oath that he in fact did give a copy of your report to Oliver Kommerling, you have no reason to disbelieve that, correct?
A Well, when I read the deposition of Mr. Shkedy, I paid attention that Mr. Shkedy continually confused two projects which were very similar from his point of view, this project which is the Headend Project and another project which dealt with the same chip called ST16. I think that could be a

basis for confusion that Mr. Shkedy testified about.
Q You don't think Mr. Shkedy would come in and mislead any of these jurors do you?
A No.
Q You think that Mr. Shkedy is an honest person?
A Yes, of course.
Q So if he told the ladies and gentlemen of the jury that he gave a copy of your report to Oliver Kommerling, you have no reason to believe him do you, sir?
A If he said so, no.
Q And we will take about that other system in a minute. I think you are referring to the encryption technology used by Canal+; is that correct?
A Yes.
Q And the Canal+ system is another competitor of NDS?

08:03:19 A Used to be, yes.
Q And that was another one of the defendants' competitors that you reverse engineered?
A Yes.
Q Did you create a similar report for the Canal+ system that described the weaknesses in that chip?
A Yes.
Q And you think that may have been the one that Zvi Shkedy provided to Oliver Kommerling?
A I am going to ask you to repeat that.
THE COURT: Do you need an interpreter?
THE WITNESS: I need him just to slow down.
MR. HAGAN: I apologize.
BY MR. HAGAN:
Q You believe that -- the sense of confusion here is you think that perhaps Zvi Shkedy gave the report on the Canal+ system to Oliver Kommerling, correct?
A I believe so.

Q And we will come back to that in a minute.

MR. HAGAN: Permission to approach the well, Your Honor.

THE COURT: You may.

MR. HAGAN: Can we put up the first page of the report, and let's zoom in on Section 2, please.

BY MR. HAGAN:

Q Mr. Mordinson, do you have a copy of Exhibit 98 in front of you?

A Yes.

Q If you look at Section 2 on the first page, it's entitled "Hardware"?

A Yes.

Q It says the chip that you used was the Thompson ST16CF54; is that correct?

A Yes.

Q And that was the chip that Echostar used in its security system?

A Yes.

Q That's not a chip that NDS used in its system, correct?

A Correct.

Q In fact, the Thompson chip that Echostar used had completely different architecture than the chip that NDS used?

A Can you define the architecture?

Q You are familiar with the architecture of these microcontrollers?.

A Yes.

Q There are two different types as I understand it, correct?

A Yes.

Q There is the Harvard architecture on the one hand?

11

08:05:19 A Yes.
Q And then there is the Von Neumann architecture on the other hand?
A Von Neumann is a kind of common architecture that would describe the principles of building computers or building microprocessors. It can be implemented in several ways.
Q The chip that you hacked for Echostar, the Thompson chip, used a Von Neumann architecture; is that right?
A Yes.
Q Are you familiar with any of the aliases that Chris Tarnovsky used on behalf of the defendants?
A No.
Q If Chris Tarnovsky testified that he used an alias Arthur Von Neumann or Von, you don't have any reason to disprove that, correct?
A I just have an idea about it.
Q You would agree with me that hacking Echostar's Von Neumann architecture could not help you in any way with the NDS chip using the Harvard architecture, correct?
A Actually, yes, it did use a chip with Von Neumann architecture. I can name at least one.
Q Not with the DirecTV system here in the United States, though; isn't that right?
A I think the P3 card was using the Von Neumann architecture.

♀

12

08:06:39 Q You weren't using the P3 card at this time?
A No, but this --
Q Let's talk about the '98 time period when you developed your hack.
MR. HAGAN: Christine, if you can help him.
BY MR. HAGAN:

Q Turn to page 11 of your Headend Report.
Do you have that page in front of you, Mr. Mordinson?
A Yes.
Q Now, Section 3 of your report on page 11, Exhibit 98, is entitled "Attack Tactics"; is that right?
A Yes.
Q And 3.1 just underneath that you entitled "Attack on the Chip's Hardware"; is that correct?
A Yes.
Q In this section of your report, you are describing in detail how NDS attacked the hardware for Echostar's chip in its security system, correct?
A It's described in the document, yes.
Q Nothing in Section 3 or 3.1 talking about this attack deals with the NDS chip, correct?
A Correct.
Q And these are your words here in this section, "Attack Tactics" and "Attack on the Chip's Hardware"? You wrote that?

♀

08:08:07 A Yes.
Q Let's take a look at the next page, page 12 of your report. There is a diagram on the top portion of that page.
Can you explain to the ladies and gentlemen of the jury what that diagram is?
A It's a figure. That's another diagram. I believe it's an image taken by the microscope from the chip, so it's a photographic image. On this image, we can see the hardware or actually the circuit in which can be found the loud input signal to the instruction register.
Q And this is for Echostar's security system, correct?
A That's for the chip that was used by Echostar's security system.
Q If you look at Sections 3.2 and 3.3 --

MR. HAGAN: Can we blow those up?

BY MR. HAGAN:

Q 3.2 talks about the RAM ghost effect or address aliasing for Echostar's chip; is that correct?

A Yes.

Q And you were the one that discovered this property of Echostar's microcontroller; is that right?

A Yes.

Q And you did that on behalf of NDS for the Headend Project?

A Yes.

♀

08:09:53 Q Right below that there is Section 3.3, and that is entitled "Stack Override."

At your deposition, I believe you said that is the same thing as the IO buffer overflow; is that correct?

A Yes.

Q And you discovered that property for Echostar's chip; is that right?

A Yes.

Q And you did that as part of your work for NDS, correct?

A Yes.

Q And you agreed with me yesterday and I believe you testified to the jury that the posting in December of 2000 that you looked at for your deposition utilized both of these properties, the RAM ghost effect and the IO buffer overflow; is that correct?

A Yes.

Q Let's take a look at pages 15 through 17 of your report.

Do you have that portion of your report in front of you, Mr. Mordinson?

A Yes, I do.

Q On page 15 of your report, the bottom section is labeled 3.5. Do you see that?

24 A Yes.
25 Q You entitled that section "3M Hack Possibilities." Do

08:11:36 1 you see that?
2 A Yes.
3 Q Can you explain to the ladies and gentlemen what a 3M
4 hack is?
5 A A 3M hack is a commonly used term which applies to the
6 technique which one can use the basic or the minimal
7 subscription to the service and get all of them. Actually,
8 3M stands for the slogan of Three-Musketeers, which means
9 one for all, all for one. This is the basic idea behind it.
10 Q Let's take a look at the next page, page 1640.
11 On this page, Mr. Mordinson, you are describing in
12 detail different possibilities to hack Echostar's security
13 system, correct?
14 A Yes.
15 Q And the first one, 3.5.1, deals with pay per view?
16 A Yes.
17 Q And you understand what pay per view is or PPV?
18 A Yes.
19 Q And that's when you order a movie at home, and you pay
20 for it through your monthly bill?
21 A Basically, yes.
22 Q In this section of your report, you are describing how
23 to circumvent EchoStar's technology to accomplish this, in
24 other words, how to get around the security system and steal
25 those pay per view channels, correct?

08:13:16 1 A Yes.
2 Q The next section, 3.5.2, deals with cloned universal

subscriptions or cloned cards; is that correct?
A Yes.
Q Can you explain to the jury what you mean when you say a cloned Echostar Smart Card?
A "Cloning" is also a common term. It means when you take an image off of one card and you write it or apply this image to other cards, you make them look exactly the same through the set-top-box, so in this way, you can copy or clone a subscription from one card to another.
Q If you would turn briefly to page 39 of your report.
MR. HAGAN: Can we blow up the title portion of Appendix H, page 39.
BY MR. HAGAN:
Q Now, in this section of your report, Mr. Mordinson, you are describing in detail how to perform a 3M hack for Echostar's security system; is that correct?
A Yes.
Q You are providing the code or the instructions on how someone would apply that to create the 3M card that you just talked about, correct?
A Yes.
Q Now, if you would look back at page 16, Section 4.0 -- do you have that page in front of you, sir?

08:15:20 A Yes.
Q Section 4 is entitled "3M Hacking Practice"?
A Yes.
Q Section 4.1 deals with Echostar's DISH network system here in the United States; is that correct?
A Each network that operates in the United States.
Q So in this section of the report, you are providing instructions in detail on how to create a 3M hack for Echostar's security system here in the United States?
A It did not provide instructions.

Q You are providing specific details about a 3M hack for Echostar's security system in the United States, correct?
A It provides descriptive details about what was there.
Q And the instructions, the actual code, is in Appendix H that we just looked at?
A Yes.
Q That's the actual recipe or code, correct?
A A recipe? It's an implementation. It's not a recipe.
Q You would agree with me that you and Zvi Shkedy maintained a compilation of all of this information, these different hacks, in what you called a cookbook, correct?
A We called it a cookbook, but it has been managed by the Development Team in Jeruslem.
Q The Development Team for the defendants?
A Yes.

♀

08:16:51 Q Can you tell the ladies and gentlemen what was in that cookbook?
A Well, cookbook is the code name of the document. It's an informal name of the document which was managed by the Development Team in Jeruslem. It was for the purpose of -- to develop security systems, particularly Smart Cards, and it was -- consisted of possible security flaws or possible attacks and propose countermeasures against those attacks.
Q One of the attacks that you included in your cookbook was the attack that you developed for Echostar's security system; is that correct?
A I cannot agree with your -- my cookbook because I testified that it was managed by the Jeruslem team.
Q I apologize. I'm not trying to imply that it was your cookbook. It was the defendants' cookbook?
A Yes.
Q Now, let's take a look at page 18 -- actually, we are going to take a look at a page from your initial draft report. I believe it's Trial Exhibit 2.

MR. HAGAN: Your Honor, this trial exhibit was admitted into evidence yesterday through Mr. Shkedy.

THE COURT: It's 2-A.

MR. HAGAN: 2-A. I apologize.

BY MR. HAGAN:

Q Give us a second, Mr. Mordinson, and we will come back

08:18:43 to that.

The defendants' cookbook for hack possibilities which included a hack on Echostar's security system was maintained in the Jeruslem office -- where was that cookbook kept?

A I never saw a cookbook because it was kept secret. One of the reasons why it was kept secret by the Jeruslem Development Team is that they wouldn't want us to know security violators or the Security Quality Assurance Group about countermeasures and about the protective measures that they introduced into the Smart Cards because it would --

THE COURT: Move that microphone just to that side. More it that way and then move it closer. We want to hear you.

THE WITNESS: Because the fact that exposure of the cookbook to a security violation group would influence our expertise. Therefore, we were not given access to this cookbook.

BY MR. HAGAN:

Q So the cookbook that the defendants kept with the hack receipes among other things in it, you didn't have access to that; is that correct?

A Yes.

Q That kept that information separate and apart from you?

A Yes.

Q And you don't know who had access to that cookbook?

A Me personally, no.
Q Now, looking at page 14 of Exhibit 2-A -- that's the initial draft of your Headend Report -- if you look down on the third column to the right on page 18 --
THE COURT: Page 18 of 2-A or the Headend Report?
MR. HAGAN: Of Exhibit 98.
THE COURT: The Headend Report.
BY MR. HAGAN:
Q Do you have that in front of you, Mr. Mordinson?
A Yes.
Q What was the purpose of creating this spreadsheet or this portion of your report?
A It was created to describe findings, results, of this project.
Q The results of the project to hack Echostar's system, correct?
A The results of the project of reverse engineering Echostar's system.
Q You testified yesterday that you went further than just reverse engineering. You actually created a hack for EchoStar's system and tested that hack; isn't that right?
A Yes, that's what I testified.
Q In the third column of -- if you look down to the second to the last box --
MR. HAGAN: Can we blow that up?

BY MR. HAGAN:
Q -- you include in your report the word "Nipper"; is that right?
A It was written in Smart Card.
Q And it uses different letters, right, capital, lower case, capital, lower case? That's the way it's written in

Echostar's code?
A Exactly what was written.
Q And you extracted -- or the defendants -- you and Zvi Shkedy extracted this key or this phrase out of Echostar's Smart Card?
A Yes.
Q And that's exactly what it looked like with a capital "N," the lower case "i", the capital "P," the lower case "p," the capital "E," and the lower case "r"?
A I believe so, yes.
THE COURT: You said "I believe so." That's hedging to me. Answer the question.
THE WITNESS: Yes.
BY MR. HAGAN:
Q And then you put that information into your report, correct?
A Yes.
Q And that report went into the cookbook that the defendants had?

♀

08:23:30 A I don't know.
Q You provided that report to Shen-Or and Zvi Shkedy; is that right?
A Yes.
Q Did you give it to anybody else?
A No.
Q We are going to come back to that in a minute.
You understood from looking at the postings on the Internet of the hack methodology for Echostar's system that the person taking credit for that posting used an alias of Nipper?
A I don't recall that.
Q Let's take a look at that exhibit.
MR. HAGAN: Do you have that, Christine?
MR. HAGAN: What exhibit number is that?

THE COURT: 998.
BY MR. HAGAN:
Q Mr. Mordinson, do you have that exhibit in front of you?
A Yes.
Q This is the hack methodology from the posting that you looked at in preparation for your deposition; is that right?
A It looks like that, yes.
Q If you look at the bottom, it's signed "NiPpErClAuZ OO," correct?

A Yes.
Q Let's also take a look at the December 24 Internet posting.
MR. HAGAN: Do we have that with us, Christine?
Give us a second to find that. We will come back to it.
BY MR. HAGAN:
Q So you would agree with me from looking at Exhibit 998 that the person who signed this particular posting used an alias of Nipper?
A Yes.
Q And that was the same secret key word that you found in developing the hack for Echostar's system, correct?
A It's written differently, with lower case and upper case differently.
Q It alternates in the reverse order; is that right?
A No.
Q Sorry?
THE COURT: Why don't you put up 998.
MR. HAGAN: Let's blow up that portion of 998 and zoom in on the word "Nipper."
BY MR. HAGAN:
Q Now, looking at that portion of Exhibit 998,

Mr. Mordinson, you will agree that that's the same key, "Nipper," that you found in your report, but it alternates

the letters differently, correct?
A Yes.
Q Now, Mr. Shkedy testified yesterday that if a person wishing to post information on the Internet about Echostar's code or hack of Echostar's system -- if they were doing their job properly, you wouldn't be able to tie that post back to them.
Do you have any reason to disagree with Mr. Shkedy's testimony?
A No.
Q You have no reason to disagree with him on that point?
A No.
Q Now, a moment ago I asked you if you gave this report that described the hack for EchoStar's system that you created on behalf of the defendants to anyone other than Hayim Shen-Or or Zvi Shkedy, and you said no, correct?
A You lost me. Sorry. Can you repeat the question?
Q I will ask it very slowly.
Mr. Mordinson, I asked you a few minutes ago if you had given a copy of this report, the hack for Echostar's system that you developed, to anyone other than Zvi Shkedy and Hayim Shen-Or, and you testified that you had not; is that correct?
A Yes.
Q But in reality, you did share this report and the

information -- or at least some of the information about the hack that you developed for Echostar with a gentleman by the

name of Chris Tarnovsky; is that correct?
A That's not correct.
Q You did not share this information with an individual named Chris Tarnovsky?
A I cannot answer your question yes or no. I have to explain.
Q It's not a difficult question, Mr. Mordinson.
Did you or did you not at any point in time provide any of the information in Exhibit 98, the hack methodology that you developed on behalf of the defendants, to Chris Tarnovsky?
A I did not provide information from this report to Chris Tarnovsky.
Q Did you show any portions of this report to Chris Tarnovsky?
A Yes.
Q Thank you, Mr. Mordinson.
You knew at the time that you showed Chris Tarnovsky the hack -- part of the hack methodology that you developed for the defendants that he was employed by the defendants, correct?
A Yes.
Q And you knew at the time that you shared this

information with Chris Tarnovsky that he was a former satellite hacker and pirate, correct?
A No, I didn't know that Chris Tarnovsky had any history of piracy or hacking.
Q You testified yesterday that NDS as part of its efforts to fix the compromise of its system went out and hired certain hackers, and you told the jury that two of those hackers were Chris Tarnovsky and Oliver Kommerling. Were you telling the truth yesterday?
A Yes.
Q So you knew at the time that you shared this

information with Chris Tarnovsky -- you showed him parts of your report, the hack that you developed for Echostar's system --

MR. SNYDER: Objection, improper impeachment. These are not inconsistent at all.

THE COURT: Overruled.

BY MR. HAGAN:

Q You knew at that time that Chris Tarnovsky was an NDS employee and a former satellite hacker and pirate?

THE COURT: Before you answer that, counsel, it was ambiguous yesterday. I understand that he may have another answer about when this was shared, but it's ambiguous.

Counsel, you may proceed.

♀

08:31:50 THE WITNESS: I remember that I testified yesterday that I knew that Oliver Kommerling was a former hacker, but I recall counsel's question in light of two persons. I said I didn't know that Chris Tarnovsky was a pirate or a hacker, but I said that I knew that Oliver Kommerling was, and that's true.

BY MR. HAGAN:

Q I will represent to you, Mr. Mordinson, that Christopher Tarnovsky is going to take the stand, and he is going to admit --

THE COURT: This is a different question than the impeaching question you just attempted to ask.

BY MR. HAGAN:

Q Let's talk about when you shared this information with Chris Tarnovsky.

You flew back over to the United States and met with Mr. Tarnovsky at his house, correct?

A Can you be specific when?

Q We will talk about the date in a minute. I just want

to know how you got there.

You flew from NDS Israel to California to meet with Chris Tarnovsky?

A Yes.

Q I believe your testimony at your deposition was this was in 2001, correct?

08:33:03 A August 2001, correct.

Q When you got to Mr. Tarnovsky's house, you talked about a number of technical things, one of which was the hack on Echostar's system, correct?

A No.

Q You didn't talk about the hack of Echostar's system at all with Mr. Tarnovsky?

A No.

Q At some point during that meeting you did show him part of your report, correct?

A Yes.

Q The report that you labeled "Secret"?

A Yes.

Q The report that you testified to yesterday and Zvi Shkedy testified that in the wrong hands could teach hackers around the world how to compromise and steal Echostar's programming, correct?

A Yes.

Q And after you showed that report to Chris Tarnovsky, you and Mr. Tarnovsky -- let's back up for a minute. I am getting ahead of myself.

You didn't bring that report with you in printed form did you?

A I did not.

Q You had it on your laptop?

08:34:09 A In electronic form encrypted, yes.
Q When you got to Chris Tarnovsky's house, you went into his office, correct?
A His office is located at his house.
Q And you understood that Mr. Tarnovsky worked out of his house for NDS?
A Yes.
Q His NDS office was his house, correct?
A Yes.
Q So you went to Chris Tarnovsky's NDS office, and you had a copy of your report on your laptop?
A Yes.
Q And then you hooked your laptop up to Chris Tarnovsky's printing system?
A To the network, yes.
Q To his network. And then you printed out portions of of your report?
A Yes.
Q You don't recall which specific portions those were?
A No, I don't.
Q You also don't know whether or not Chris Tarnovsky's network saved a copy of the entire report before you printed out the portions that you printed, correct?
A Well, I have to explain. I can be sure that the entire report stayed in a secured encrypted form on my computer

08:35:21 because my computer was equipped with antivirus and firewall means, which is the standard policy of the NDS Data Security Group. On the other hand, I didn't send the entire report over Chris Tarnovsky's network. I sent just two or maybe three pages that I cannot recall which of those pages of the report.
Q And then you printed out those pages of the report?

A Yes.
Q And you showed them to Chris Tarnovsky?
A Yes.
Q But you didn't let him touch the report did you, sir?
A When it was in my hand, no.
Q You held it the entire time?
A Maybe I put it on the table nearby me, but it was in my possession all the time.
Q Chris Tarnovsky testified at deposition that you flipped the pages of the report that you printed out for him.
Do you have any reason to disagree with his testimony?
A No.
Q After you showed Chris Tarnovsky your report, you and Mr. Tarnovsky went into the garage, and you shredded it?
MR. SNYDER: Objection. That misstates his testimony. The testimony was there were two or three pages --

08:36:37 THE COURT: I'm sorry?
MR. SNYDER: It misstates the testimony. Counsel has repeatedly referred to showing the report. The witness's testimony is clearly that he printed only two or three pages, and it misstates his testimony to continually refer to Mr. Mordinson showing the report to Mr. Tarnovsky.
MR. HAGAN: I will rephrase, Your Honor.
BY MR. HAGAN:
Q I'm sorry, Mr. Mordinson. I am not trying to mislead you.
As to the pages of your report that you printed out at Chris Tarnovsky's house, after you showed him that information, you and Mr. Tarnovsky took those pages of your report and you shredded them?
A Yes.

Q Are you familiar with the term "proof of concept"?
A Yes.
Q Can you tell the ladies and gentlemen of the jury what that term means?
A Well, in my understanding, proof of concept is a process -- when you develop a concept or that something is theoretically possible, what you want to prove is that the concept that you developed is really valid in practice.
Q I'm sorry. I didn't catch the last part. The process that you developed is what?

08:38:00 A Is valid in practice.
Q "Is valid in practice." It means it works?
A Yes.
Q You created a proof of concept for the Echostar hack?
A You can treat it this way, yes.
Q But you didn't stop there did you, Mr. Mordinson? You went further, and you actually developed that hack that you described in your proof of concept?
A I lost you. Sorry. I cannot understand the question.
Q I apologize. We will use the demonstrative we used yesterday to talk about this.
You just testified that proof of concept is when you show something you developed is valid, show that it works; is that correct?
A Yes.
Q And you created a proof of concept for a hack on Echostar's security system, correct?
A You can treat it this way, yes.
Q But you didn't stop there? You actually developed that hack through codes and instructions, correct?
A Sorry. I understand English. I just don't understand your question. Is that different from your first question? I can't understand it.
Q Proof of concept according to your testimony is just

showing conceptually what you created would work, right?

SHARON SEFFENS, U.S. COURT REPORTER

♀

33

A Yes.
Q But you went further? You and Zvi Shkedy actually reprogrammed an Echostar Smart Card, and then you used that reprogrammed card up in Canada in a basement to steal Echostar's signal, correct?
A No.
Q I believe you testified yesterday that you came to the United States for a second trip in 1998, right?
A Yes.
Q And you brought an Echostar Smart Card with you, correct?
A Yes.
Q You brought the computer with you that had portions of your Headend Report -- or portions of the underlying data?
A Can you be specific what portions you mean?
Q It had information on your computer in files that you had developed as part of the Headend Report -- or the Headend Project, correct?
A I would like to exclude any mention of Headend Report because it was prepared after the trip to Canada in September 1998.
Q The whole project itself was called the Headend Project?
A Yes.
Q And then you used to create the Headend Report?

SHARON SEFFENS, U.S. COURT REPORTER

♀

34

A Yes.
Q So you brought your computer with you to the United States that had information about Echostar's security

system that you developed as part of the Headend Project?
A That's correct.
Q And you took that information, and you finalized the actual hack once you got to North America?
A Yes.
Q And then you used the device that you testified about yesterday, the stinger, that NDS built and you reprogrammed an Echostar Smart Card?
MR. SNYDER: Objection. Misstates the testimony. There has been no mention of a stinger.
BY MR. HAGAN:
Q You brought the device that NDS created called the sniffer?
A Yes.
Q And you used that device, that sniffer, to reprogram an Echostar Smart Card, correct?
A Yes.
Q And then you used that reprogrammed Smart Card in an Echostar system in a basement in Canada?
A Yes.
Q And you were able to successfully test the proof of concept hack methodology that you developed as part of the

08:42:05 Headend Project, correct?
A Yes.
Q And you understood at least at the time of your deposition that a hack methodology for Echostar's system was posted on the Internet in December of 2000, correct?
A The posting that I saw that was related to the posting in December 2000 didn't explain the methodology of a hack.
Q It described how to use the methodology and extract the EEPROM for Echostar's Smart Card?
A It did not include any explanations. It included just the code.

Q You looked at the December 24 posting?
A I don't recall the date. I think this is the posting I saw. I don't see any particular date on it.
Q The posting that you looked at -- let's be on the same page here. I know this is technical, and it's hard for me to understand it. The posting that you saw had EEPROM from an Echostar Smart Card, correct?
A A portion, yes.
Q Was that EEPROM modified in any way?
A Yes.
Q In your report, you talk about how to extract the EEPROM from an Echostar Smart Card?
A It's included in the report, yes.
Q Now, earlier you said that you also on behalf of NDS

reverse engineered the Canal+ System; is that right?
A Yes.
Q Did you use the same processes and techniques that Oliver Kommerling had taught you and the equipment in the Haifa lab to do the Canal+ Project that you did for Echostar's project?
A Yes.
Q And you understand as you sit here today that the Canal+ code -- the secret code for that system was also posted on the Internet, correct?
A Yes.
Q It's your understanding that that posting had the same time and date stamp that the code you extracted in Haifa?
A Yes.
Q And that is another project that related to reverse engineering NDS's competitor's system?
A Yes.
MR. HAGAN: Pass the witness, Your Honor.
THE COURT: Cross-examination. This will be by Mr. Snyder on behalf of NDS.

CROSS-EXAMINATION

BY MR. SNYDER:

Q Good morning, Mr. Mordinson.

A Good morning.

Q My name is Darin Snyder for the defendants.

08:46:00 Mr. Mordinson, Mr. Hagan didn't give you a chance to tell the jury a little bit about yourself.

Could you tell us where you live, please?

A I live in Israel in the city of Haifa.

Q How long have you lived there?

A Almost 16 years.

Q Where were you born, Mr. Mordinson?

A I was born in Moscow, Russia.

Q Did you move from Moscow to Israel?

A Yes.

Q And why did you move to Israel?

A I has just graduated from the university, and I was a young engineer. I was looking for a way to develop myself, and the economic and political situation in Russia in those days were bad, so I moved to Israel which offered me much more opportunities to develop myself and just a more free life and whatever.

Q Mr. Mordinson, how many languages do you speak?

A Well, I speak Russian. I speak Hebrew fluently. I speak English. There is a place for improvement. And I used to speak German. I still speak a bit of German.

Q So you are essentially testifying in your third language?

A Yes.

Q We should all be so proficient.

08:48:49 Mr. Mordinson, are you married?
A Yes.
Q Do you have a family?
A Yes.
Q Could you tell the jury a little bit about your family?
A Well, I have a wife, and I have two beautiful daughters. The youngest is almost two years old, and the older is six-and-a-half and going to school in September.
Q Mr. Mordinson, who do you work for?
A I'm working for NDS.
Q How long have you worked for NDS?
A I have been working for NDS for more than ten years.
Q Before you started working for NDS, did you receive any degrees?
A Yes.
Q What degrees did you obtain?
A I graduated from the Moscow Institute of Aviation Technology. It's a technological institute.
Q Is that an engineering degree?
A Yes.
Q Have you been a practicing engineer since you graduated from the Moscow Technical Institute?
A Yes.
Q What do you do for NDS now?
A Well, I'm working for the NDS Marketing Group as a

08:50:04 technical consultant in presales and business development.
Q And how long have you been in that position?
A Almost one year.
Q So you moved to that position in about 2006?
A In the beginning of 2007. Before that I was working in the Haifa Research Center as a member of the Haifa Research Center.

Q Before you started in that position, what was your position at NDS?
A I was a software engineer and security analyst.
Q Mr. Mordinson, do you also serve in your country's military?
A Yes.
Q When did you start your military service?
A In 1993.
Q Can you describe for the jury your military service?
A Yes. I am a radio operator with the ranking of sergeant in a fighting unit in the Army. After finishing my active duty, I am performing reserve duty every year.
Q When were you on active duty in the service?
A On active duty since 1993 to 1994.
Q Have you been in the reserves continuously since 1994?
A Yes.
Q And have you also been called to active duty while you have been in the reserves?

08:51:50 A Yes.
Q When were you most recently on active duty?
A I was on active duty during the Lebanese war in the summer of 2006.
Q Was that as a communications operator, Mr. Mordinson?
A Yes.
Q Let's go back for a moment -- actually maybe more than a moment -- to your work at NDS.
When you started at NDS, where did you work?
A Before that, I was working for -- I was working as a software developer and software engineer in various companies which developed, for example, point of sales for cash registers, software for insurance companies, like that. I was working for an IT Department at one time, customer support. I worked through all the positions in the software industry.

Q And when did you start with NDS?
A I started with NDS in September 1997.
Q When you started with NDS, what was your first position?
A My first position was software engineer and security analyst.
Q Where at NDS do you work?
A I work in the Haifa office located in the city of Haifa.

♀

08:53:31 Q What was the purpose of the Haifa office, Mr. Mordinson?
A The purpose of the Haifa office was to perform security evaluation and in this way improve NDS products.
Q Is that office sometimes called the Haifa Research Center?
A It's called the Haifa Research Center, its formal name for the department.
Q Has it ever been called any other names?
A Yes.
Q Is it sometimes called the Black Hat Team?
A Yes, informally. Internally it was called the Black Hat Team.
Q Why was it called the Black Hat Team?
A I actually don't know. "Black hat" is a common term in the industry describing groups or teams that perform the same work for the same purpose in other companies like IBM, for example.
Q When you say "the same work for the same purpose," what are you referring to?
A Security relation, design reviews. As I said, improve the security and quality of the products.
Q Does the name Black Hat Team mean to imply that you were doing something wrong?

25 A Absolutely not.

SHARON SEFFENS, U.S. COURT REPORTER

♀

42

08:54:42 1 Q Now, you mentioned, Mr. Mordinson, that the purpose of
2 the Black Hat Team was to help improve the security of NDS's
3 products.
4 A Yes.
5 Q How did it do that?
6 A Well, results of our work was delivered to the Jeruslem
7 Development Team. It was one-way communication. It's
8 informal. They provide us products that they want us to
9 evaluate, and we provided feedback. Maybe the most
10 successful slogan to describe it is break what we make, and
11 that's what we did.
12 Q Does the Haifa Research Center actually design any NDS
13 products?
14 A No.
15 Q What part of NDS is responsible for designing the NDS
16 products or cards?
17 A NDS products and -- security products are developed in
18 the Jeruslem office by the Jeruslem Development Team.
19 Q And what is the relationship between the Jeruslem
20 Development Team and the Haifa Research Center?
21 A Well, as I said, it's one-way communication. It means
22 that we provide our feedback about NDS products to Jeruslem,
23 and we were never told back any comments or anything else.
24 Q Has that relationship between the Jeruslem Design Team
25 and the Haifa Research Center changed over time?

SHARON SEFFENS, U.S. COURT REPORTER

♀

43

08:56:09 1 A In recent years, we became more involved into the
2 design of the products before they actually implemented
3 or -- before they have a prototype, so our influence on

development of a project or development afoot is changing in recent years.
Q Is the work that you do at the Haifa Research Center designed to assist NDS in fighting piracy?
A Yes, certainly.
Q Can you explain to the jury how the work that you do at the Haifa Research Center is designed to help fight piracy?
A Well, by reviewing the security of the products, we can find -- or attempt to find potential security flaws and report those flaws to the Jeruslem Development Team, so we give them a chance to close these holes or security flaws, fix them, and to release a superior product to the customer.
Q Is the information that you develop at the Haifa Research Center considered confidential?
A Absolutely.
Q Does NDS take special measures to help protect that information from disclosure?
A Yes.
Q Can you describe generally the measures that NDS takes to keep that information confidential?
A Well, like other sensitive materials, according to NDS security possibility which applies to all NDS departments,

08:57:51 we keep secure documentation and secure materials -- if they are in an electronic format, we kept them in encrypted form. If they are not in an electronic format, they were locked in a safe. NDS Haifa also had restricted access protected by our employee's Smart Card, and we had a secure network which was physically disconnected from the NDS global network. There are other means I just can't recall at the moment.
Q Does the Haifa Research Center also use physical security measures?
A Yes. As I said, it's restricted access. We had an alarm system in our offices, and for physical security also, we had to pass clearance which -- we had to have security

clearance which had to be renewed every three years.
Q Now, Mr. Mordinson, as part of your work at the Haifa Research Center, do you reverse engineer cards?
A Yes.
Q Did you reverse engineer NDS cards?
A Yes.
Q Did you reverse engineer cards from competitors?
A Yes.
Q Did you generally use the same techniques and approaches in reverse engineering NDS cards that you used on other company's cards?
A Yes.
Q Mr. Hagan went through yesterday several steps in the

08:59:29 process of reverse engineering a card. Do you recall that?
A Yes.
Q He talked about taking the chip out of the card, using different types of acid, for example. Do you recall that testimony?
A Yes.
Q Do you use that same process on NDS cards?
A Yes.
Q Is there any difference between the process that you use in reverse engineering an NDS card and a competitor's card?
A No.
Q But you do reverse engineer competitor cards?
A Yes.
Q Why does NDS reverse engineer competitor cards?
A There are two purposes actually of competitor intelligence in reverse engineering competitors' Smart Cards: The first was to get a complete understanding of the competitors' security system on the client side, which I mean the Smart Card. This was the goal. The purpose was to

use this information to improve NDS products and to assist Marketing.
Q Now, Mr. Mordinson, are you aware -- how does the information that you develop in reverse engineering cards -- how is that used by the Jeruslem design team?

09:00:50 A According to my knowledge, this information or feedback was introduced into the document whose formal name is cookbook, and this cookbook was used by the Development Team.
Q Have you ever seen the cookbook?
A No.
Q To the best of your understanding, what does the cookbook contain?
A To the best of my understanding, it contains potential security flaws and potential attacks that can be mounted in the security system, and it proposed countermeasures and other means that can prevent this attack from operating.
Q For purposes of the Haifa Research Center's work, is it important that you not see the contents of the cookbook?
A Absolutely.
Q Why is that?
A As I said, because of proposed countermeasures. So we could be aware of countermeasures that we could find or cure in NDS products if we could know this information, so our expertise would be influenced.
Q So if you knew how Jeruslem was getting around these attacks, it might make it easier for you to reverse engineer NDS cards?
A Yes.
Q In looking at NDS cards, have you sometimes seen

Jeruslem -- the Jeruslem Design Team's efforts to correct some of the deficiencies that you have identified in cards?
A Yes.
Q Can you give the jury an example of a kind of deficiency or vulnerability that you have seen corrected by the Jeruslem Design Team?
A Well, it will be a bit of technical stuff. First of all, what I can recall is glitch detectors. Glitch is a technique which is also called fault insertion. It deals with interference of electrical and supplying a power supply to the Smart Card. The purpose of this technique is to disturb the operation of the CPU or the microprocessor.
I saw in reverse engineering of this Smart Card that some -- some cards used this countermeasure in order to prevent fault insertion, but implementation of this method in this card was not sufficient enough to block this technique. What I saw in the NDS Smart Card was the implementation of glitch detectors was much more successful, and it managed to block glitches or such an attack.
Q Do you believe that their ability to make this improvement was the result of your reverse engineering work?
A I would like to believe so.
Q Mr. Mordinson, is reverse engineering unusual?
A No.
Q Is it a common industry practice?

♀

A Yes. There are some companies that offer hardware and software reverse engineering services for hire.
Q Do you believe that there is anything wrong with reverse engineering?
A No.
Q Now, during the course of your testimony, there has been a common use of the word "hack."
Is there a difference in your mind between reverse

engineering and hacking?
A Yes.
Q What is reverse engineering?
A Reverse engineering is a process which is opposite of forward engineering. The purpose of this process is to understand how the thing works actually.
Hacking can include some steps of reverse engineering in order to understand the system functionality and system features, but hacking is more about looking or finding hidden features that they are by design or not by design in the product.
Q Mr. Mordinson, are you familiar with the term "piracy" or "satellite piracy"?
A Yes.
Q What is "piracy" or "satellite piracy"?
A Satellite piracy is a criminal activity whose intent is to steal satellite services or content delivered by

09:06:18 satellite and make money out of this illegal business.
Q Is reverse engineering and piracy the same thing?
A No, absolutely not.
Q Is hacking and piracy the same thing?
A No.
Q Now, Mr. Mordinson, when you reverse engineered competitor cards, did you only reverse engineer cards that NDS was also using?
A No.
Q Why did the Haifa Research Center reverse engineer cards or chips that NDS was not using?
A First of all, when you start reverse engineering, you don't really know what you expect to find. As I know, NDS was approached by chip manufacturers that offer their chips to NDS, so even if NDS doesn't use one particular Smart Card or a particular platform, it can be used for information to

know about other platforms.
Q Now, I just want to make sure everybody understands.
Not all of the competitor cards that the Haifa Research Center reverse engineered were cards that competitors or other companies asked you to reverse engineer, right?
A Right.
Q Part of that work was done to assist in the NDS design efforts?
A Yes.

09:07:43 Q How does it help NDS's design efforts to reverse engineer a competitor card?
A Well, as I said, countermeasures are protective measures that can be found in a particular platform. Even if they are not implemented well enough for NDS security requirements, they can bring out some ideas about how to improve NDS products and give us an idea about better implementation of those protective measures.
Q Mr. Hagan asked you some questions about chip arcitectures. Do you recall that?
A Yes.
Q Were some of the cards that you reverse engineered in the Haifa Research Center using a different architecture than the architecture of the chips that NDS uses?
A Yes.
Q I believe Mr. Hagan also asked you about Harvard and Von Neumann architectures.
A Yes.
Q Does the Echostar Smart Card use a Von Neumann architecture?
A Yes.
Q Do any of the NDS chips use a Von Neumann architecture?
A Yes.
Q Can you identify any of those for the jury, please?
A For the P3 card, I used Von Neumann architecture. I

51

09:09:14 1 think -- I can relate this to the card used in Europe as
2 well. Von Neumann architecture is more theoretical or a
3 high-level architecture. Basically Von Neumann architecture
4 is used by more or less all Smart Cards in atr.
5 Q Mr. Mordinson, before you start reverse engineering a
6 Smart Card, do you know what kind of architecture it has?
7 A No.
8 Q So before you start the reverse engineering project, do
9 you know whether or not it has the same architecture as a
10 NDS product?
11 A No.
12 Q Now, Mr. Mordinson, Mr. Hagan asked you about a
13 specific characteristic of the Echostar card called the IO
14 buffer overflow defect. Do you recall that?
15 A Yes.
16 Q Can you remind the jury generally what an IO buffer
17 overflow is?
18 A An IO buffer overflow is a known technique. It's
19 usually used only in microprocessors. It's used in personal
20 computer platforms as well. It consists of sending more
21 information to the client's side -- I mean to the program
22 that acquires information -- sending more information that
23 the buffer which is designed to store this information can
24 actually store it. In this way, the extra information that
25 is sent to the client will override the information stored

SHARON SEFFENS, U.S. COURT REPORTER

52

09:11:28 1 in the memory location where the IO buffer is located.
2 Q I believe Mr. Hagan asked you whether any of the NDS
3 chips had this IO buffer overflow defect or vulnerability.
4 Do you recall that?

A Yes.
Q Before you reverse engineer a chip, do you know whether or not it has any particular defects?
A No.
Q Do you know whether or not it has the IO buffer overflow vulnerability or defect?
A No.
Q Did you know before you started reverse engineering the Echostar card whether or not it had the IO buffer overflow vulnerability or defect?
A No.
Q Is there any way to know before you start a reverse engineering project whether any card is going to have any particular defect?
A No.
Q Now, Mr. Mordinson, let me ask you a little bit about the specific reverse engineering of the Echostar card.
Did you refer to it as the Echostar card?
A I'm sorry. I didn't hear.
Q The chip that you were reverse engineering, did you know it as the Echostar card?

09:12:49 A Yes.
Q And what was the name of that project?
A The Headend Project.
Q What was the purpose of the Headend Project?
A The purpose of the Headend Project was to get a complete understanding of Echostar's Conditional Access System on the client side.
Q Was one of the purposes of the Headend Project to assist piracy?
A No.
Q Was one of the purposes of the Headend Project to assist piracy of the Echostar system?

A No, absolutely not.
Q Did NDS ever use any of the results of the Headend Project to assist piracy?
A No.
MR. HAGAN: Objection. Calls for speculation.
THE COURT: Sustained.
BY MR. SNYDER:
Q Mr. Mordinson, did you ever use any of the results or information gathered in the Headend Project to assist piracy?
A No.
Q Are you aware of anyone else at NDS who has ever used any of the results of the NDS Headend Project to assist

09:13:54 piracy?
A No.
Q Are you aware of anyone anywhere in the world that has ever used the results of the NDS Headend Project to assist piracy?
A No.
Q Now, Mr. Mordinson, you described yesterday a little bit the equipment that was used and the techniques that were used for the reverse engineering.
A Yes.
Q Is any of the equipment that you used for reverse engineering of the Echostar Smart Card unusual?
A Absolutely not.
Q Is any of it difficult to obtain or use?
A No.
Q Are any of the techniques that you used to reverse engineer the Echostar Smart card unusual?
A No.
Q Have many of those techniques in fact been published?
A Yes.
Q Can I get you to look at, please, Exhibit 809? Can you

tell us generally what Exhibit 809 is?
A This is an article published by Oliver Kommerling and Marcus Kuhn. The title of this article is "Design Principles for Tamper-Resistent Smart Card Processors."

09:15:35 Q Who is Marcus Kuhn?
A Marcus Kuhn is a doctoral professor at the University of Cambridge.
Q When was this article published? I believe it's at the bottom.
A It was the 10th to the 11th of May 1999.
Q Generally, what does this article describe?
A This article describes techniques that can be used to compromise the security of the Smart Cards and perform reverse engineering of Smart Cards.
MR. SNYDER: Your Honor, I move for the admission of Exhibit 809.
MR. HAGAN: Objection, hearsay.
THE COURT: Overruled. It's received.
(Exhibit 809 received.)
MR. SNYDER: May I publish it?
THE COURT: You may.
MR. SNYDER: Could we bring up the first page and could you highlight the very top where it has the title and the author?
BY MR. SNYDER:
Q Is that's the title of the article?
A Yes.
Q And the two authors that are identified?
A Yes.

09:16:48 Q Who is the first author?
A Oliver Kommerling.
Q Does it identify Mr. Kommerling's affiliation, who he is with?
A That's what I know, Oliver Kommerling --
Q Does it have the name Advanced Digital Security Research underneath?
A Yes. It's his company that he is running.
Q That is Mr. Kommerling's company?
A Yes.
Q Who does the article identify as the other author?
A Marcus G. Kuhn.
Q Does it identify who Professor Kuhn is with?
A Yes. I believe he is a professor. I don't know his real title.
Q He is with the University of Cambridge?
A Yes.
Q Could we look, please, at the very bottom of the first column? Does that identify where this was published or where it was shown?
A Yes.
Q Can you identify that for the jury, please?
A It's the city of the USENIX workshop.
Q What is USENIX?
A USENIX is computer authorization of -- UNENIX is a

09:18:15 operating system of computers. It dealt with computer science and other subjects of computers.
Q Is USENIX a well known organization?
A Absolutely, yes.
Q And it's a worldwide organization?
A Yes.
Q Does USENIX put on conferences?
A Yes, usually once a year.

Q Does this article indicate that it was published as part of one of those conferences?
A Yes.
Q Can you show the jury where it indicates that this paper was presented and then published?
A It's at the bottom I believe in the first column.
Q Does it show that it was in Chicago, Illinois, on May 10th and 11th of 1999?
A Yes.
Q Now, Mr. Mordinson, have you seen a copy of this article before?
A Yes.
Q Does this article describe many of the techniques that you used in reverse engineering Smart Cards?
A Yes.
Q Does it describe many of the techniques that you used in reverse engineering the EchoStar Smart Card?

09:19:28 A Yes.
Q If you could look at the second column on the first page where it says "Tampering Techniques," do you see that?
A Yes.
Q It identifies four different kinds of techniques under that. "Microprobing techniques," do you see that?
A Yes.
Q As part of your reverse engineering of the EchoStar Smart Card, did you use microprobing techniques?
A Yes.
Q The next bullet point says "software attacks." Did you see that?
A Yes.
Q As part of your reverse engineering of the EchoStar Smart Card, did you use software attacks?
A Yes.
Q Now let's take a look at some of the specific kinds of

techniques and attacks that this paper describes.

Could you look at the second page near the bottom of first column where it says "Invasive Attacks"? Then it has "Section 2.1.1: Depackaging of Smart Cards." Do you see that?

A Yes.

Q Is the depackaging of the Smart Card one of the techniques that you used in reverse engineering the EchoStar

♀

09:20:42 card?

A Yes.

Q Then if you could look, please, over to the next column, 2.1.2, where it says "Layout Reconstruction," do you see that?

A Yes.

Q Was that part of the techniques that you used in reverse engineering the EchoStar Smart Card?

A Yes.

Q If you could please turn to the fourth page of the exhibit, there is a Section 2.1.3 in the second column. It says "Manual Microprobing." Do you see that?

A Yes.

Q What is manual microprobing?

A Well, I described it my deposition, and yesterday Mr. Hagan explained it. This technique is supposed to put a very sharp, very tiny needle to touch the particular conductor on the Smart Card circuitry. This is manual. Therefore, it's called manual microprobing. Microprobing means the probe is the needle, so needle is the formal name for the probe.

Q Was manual microprobing one of the techniques that you used in reverse engineering the EchoStar Smart Card?

A Yes.

Q Could you please turn to the sixth page of the exhibit?

60

09:22:19 There is a heading that says "2.1.5: Article B Techniques." I want you to look at the paragraph above that, "In order to read out all memory cells without the help of card software" -- do you see that paragraph?
A Yes.
Q I am not going to have you read the whole thing, but could you describe generally for the jury what technique that paragraph is describing?
A This technique describes what's called linear code extraction. Linear code extraction consists of making the microprocessor scan continuously and sequentially the memory space from -- all memory space. In making the microprocessor do so, one can monitor the signal for data running on the databus of the microprocessor and figure out this data, and this data will be memory content. It then will be scanned linearly or continuously. Therefore, it's call linear code extraction.
Q Was this one of the techniques you used in reverse engineering the EchoStar Smart Card?
A Yes, to extract the code of the Smart Card.
Q Does this paper also describe other ways of attacking Smart Cards that we haven't talked about?
A Not that I see at the moment.
Q Can you please turn to the seventh page of the document? In the second column, there is a heading called

SHARON SEFFENS, U.S. COURT REPORTER

61

09:24:35 "Glitch Attacks." Do you see that?
A Yes.
Q What is a glitch attack?
A A glitch attack as I explained before is fault

insertion. It's introducing disturbances to the power supply or to clog the supply to the microprocessor and in this way interrupt or disturb the normal operation of the CPU or the microprocessor.
Q Is a glitch attack one of the ways that you can reverse engineer or hack a card?
A Oh, yes, certainly.
Q If you could look at the next page, please, page eight, in the second column, there is a heading that says "Current Analysis"?
A Yes.
Q Do you see that?
A Yes.
Q Could you describe for the jury very generally what current analysis is?
A Well, it can be described this way. An analogy of current analysis -- let's suppose you enter the room, and you turn on the lights. The current or the power -- the electricity power that your house consumes depends on how many light bulbs actually light, so in watching the current or the electricity parameters at the moment of lighting up

09:26:22 the lights, you can figure out how many lights are on. This is the principle of current analysis. So it can figure out what actually lights or what actual components are engaged in -- or operate at this particular time inside a microprocessor.
Q Is current analysis a way of reverse engineering or hacking into a Smart Card?
A Yes.
Q In reverse engineering the EchoStar Smart Card, did you use current analysis as one of the techniques?
A No.
Q In reverse engineering the EchoStar Smart Card, did you use glitching as one of the techniques?

A No.
Q But both of those techniques are published in this paper?
A Yes.
Q And this paper was published to the world in May 1999?
A Yes.
Q Now, Mr. Mordinson, you have been shown by Mr. Hagan a copy of your report, the Headend Report, that you did for this project. Do you recall that?
A Yes.
Q It's Exhibit 98.
Did you maintain that report as something that was

09:27:28 confidential?
A It's more than confidential. It's secret.
Q It's secret?
A Yes.
Q It's in fact marked "Secret"?
A Yes.
Q Mr. Mordinson, how did you maintain the secrecy of that report?
A I stored this report in encrypted form in my computer, and I didn't travel with any printout of this report. It was -- all this was according to NDS security policy.
Q When you say that it is kept in encrypted form on your computer, could you tell the jury generally what you mean?
A There is a special software called PGP, Pretty Good Privacy, which has proven to be a good tool or good software to protect secret materials in encrypted form stored in an electronic format on computer media.
Q You said it was called Pretty Good Privacy?
A Yes.
Q Is Pretty Good Privacy pretty good?
A It's more that pretty good. It's very good privacy.

Q Is it possible to hack into PGP encrypted material?
A No, no hacks or no companies have that is known since it was invented.
Q Mr. Mordinson, who has access to your laptop?

09:28:51 A Just me.
Q Other than on your laptop, did you keep copies of the Headend Report anywhere else?
A Not that I recall, no.
Q Did you give copies of the Headend Report to anyone?
A Yes.
Q Who did you give copies of the Headend Report to?
A I gave copies of the Headend Report to Mr. Zvi Shkedy and to Mr. Hayim Shen-Or.
Q Did you ever give anyone other than Hayim Shen-Or and Zvi Shkedy a copy of that report?
A No.
Q Now, you testified, Mr. Mordinson, that you and Mr. Shkedy made two trips to the United States as part of your reverse engineering project of the EchoStar card. Do you recall that?
A Yes.
Q Let's try and take those one at a time.
What was the purpose of the first trip?
A The first trip in June 1998 was to the United States in order to log or to record communication between the Smart Card and the set-top-box.
Q Why did you have to travel to the United States to do that?
A Well, it's because of geography. This work or this

09:30:12 test can be performed only in the place when it can receive a satellite signal. A satellite signal cannot be received in Israel or in Europe because the globe is sphere. If a satellite is on one side of the sphere, on the other side, you cannot receive it. It's a shadow of the globe.
Q Now, Mr. Mordinson, what did you say you were doing while you were in the United States? What did you call it?
A It was logging.
Q What is logging?
A Logging is recalling traffic or recalling communication running between the Smart Card and the set-top-box.
Q Why did you need to log the communications between the set-top-box and the Smart Card?
A Well, knowing the communications or protocol or messages that the Smart Card and the set-top-box exchange would greatly help reverse engineering and speed it up, so it was for efficiency.
Q While you were in the United States to log the communications between the set-top-box and the Smart Card, did you receive any EchoStar programming?
A No.
Q Did you receive any EchoStar programming that you weren't authorized to receive?
A No.
Q Did you decrypt any EchoStar programming?

♀

09:31:55 A No.
Q Did you decrypt any EchoStar programming that you weren't authorized to receive?
A No.
Q What did you do with the information that you received when you logged the information from the set-top-box and the Smart Card?
A This information was stored in files, and I started to analyze these files to figure out the communication upon my

return to Israel.
Q How did you store those files?
A In electronic format in encrypted form.
Q Were they also kept on your laptop?
A Yes.
Q Were they kept anywhere else?
A No.
Q What device did you use to log the communications between the set-top-box and the Smart Card?
A Well, we used a device called a sniffer. This is a device -- a general purpose device that we developed for this kind of activity. Actually, this is as I said a general purpose microcomputer which can be configured by software and a couple of jumpers, interconnectors, to serve both the logging and as a Smart Card reader.
Q You said you called the device a sniffer?

♀

09:33:19 A Yes.
Q Is that a name that you invented?
A No.
Q Is the term "sniffer" a standard term in computer science?
A Yes.
Q What is a sniffer?
A A sniffer is a general tool used by system -- a sniffer is a general purpose tool. Usually it's software sometimes with a type of hardware. It's used by system administrators and system engineers in order to log or to record traffic on the network or in the communication line. It's used to -- as I can recall, for example, it's used by a sound microsystem -- an operating system called Solaris as a standard part of this operating system. An analogy for Solaris is Microsoft Windows. I suppose Microsoft Windows has such a component.

Q Has NDS ever used your sniffer device for any other purposes?
A Yes.
MR. HAGAN: Objection. Calls for speculation.
THE COURT: More foundation.
BY MR. SNYDER:
Q Are you aware that NDS has used your sniffer device for other purposes?

♀

09:34:38 A Yes.
Q How are you aware of that?
A Because I know about the product that NDS developed called CL Sniffer. During this project, 300 devices were manufactured, and the purpose of this project was to provide testing tools to system engineerings working in NDS testing and the Quality Assurance Lab.
Q So where are those devices used?
A In 2001, I believe was the first.
Q Where are they used?
A In Jeruslem and in testing labs. It's for quality assurance and quality control.
Q They are used for quality assurance and quality control of EchoStar's security system?
A No.
Q What are they used for the quality assurance and quality control of?
A Of NDS products. Let me explain.
Q Please.
A In the Jeruslem office, we have lamps which purpose is to -- the lamps in Jeruslem conduct operations -- they are designed to perform quality assurance and quality control for items that are then developed and provided to NDS customers.
Q Are any of those devices used for piracy,

69

09:36:53 Mr. Mordinson?
A No.
Q Now, Mr. Mordinson, you were also asked earlier about a trip that you and Mr. Shkedy made to Canada. Do you recall that testimony?
A Yes.
Q Why did you and Mr. Shkedy come from Israel and go to Canada?
A Zvi Shkedy took me to Canada.
Q What was the purpose of that trip?
A The purpose of this trip was to test the findings of this project and to get to understanding that our findings were right.
Q While you were on that trip, did you have materials with you related to the Headend Project, the reverse engineering of the EchoStar card?
A Yes.
Q Where were those materials kept?
A They were kept on my laptop in an electronic format in encrypted form.
Q Were they kept anywhere else?
A No.
Q Did you have that laptop with you during the entire trip?
A Yes.

SHARON SEFFENS, U.S. COURT REPORTER

70

09:38:10 Q During that entire trip in September 1998, did you communicate with Mr. Chris Tarnovsky?
A No.
Q Did you communicate with anyone in Canada other than the person that you were visiting?

A No.
Q Did you communicate with anyone in the United States other than the person from whom you got the set-top-box?
A No.
Q Now, Mr. Mordinson, Mr. Hagan seemed to make a big deal of the fact that you were testing your code in a basement at somebody's house.
Can you explain to the jury why you chose that location?
A Well, first of all, the basement -- the term "basement" was a room on the first floor which was half an office and had a window open to the backyard of the house. We mounted our satellite DISH in the backyard and ran wire or cable from the satellite DISH to the set-top-box, and it was convenient to use this window open to the backyard in order to run this cable.
Q Were you doing the work in that part of the house because you wanted to hide from people?
A No.
Q Were you doing the work in that part of the house

09:39:37 because you thought that there was something wrong with what you were doing?
A No.
Q While you were on this trip to the United States and then Canada -- let me break that down into two parts. While you were in the United States on this trip in September 1998, did you receive any satellite transmissions from the EchoStar system?
A No.
Q While you were in the United States on this trip, did you decrypt any transmissions from the EchoStar system?
A No.
Q While you were in Canada, did you receive transmissions

from the EchoStar system?
A Yes.
Q Did you decrypt some of those transmissions?
A Yes.
Q Did you understand, Mr. Mordinson, that receiving and decrypting those transmissions in Canada was legal?
A According to my understanding, yes.
Q You recorded the results of much of your work in the Headend Report that you have previously been shown. Do you recall that?
A Yes.
Q Exhibit 98? You don't remember? I'm sure everybody is

09:40:46 getting used to it by now, but let me just ask you a few general questions about that.
One of the things that you discovered was the RAM ghost effect; is that correct?
A Yes.
Q Now, you said in your testimony with Mr. Hagan that you discovered that. What did you mean by discovered?
A Discovery is the result of reverse engineering, so by analysis of code and by analysis of linear code, it goes to understanding that there is such a phenomenon which is called memory ghost effect. Particularly in RAM, random access memory, it was a RAM ghost effect.
Q Did you mean that you were the first person to figure that out?
A I didn't know about anybody else.
Q But you don't know whether anybody else is aware of that or not do you?
MR. HAGAN: Objection. Calls for speculation.
THE WITNESS: No.
THE COURT: Sustained.
BY MR. SNYDER:
Q Mr. Mordinson, you also said that you discovered the

stack override vulnerability?
A Yes.
Q What did you mean by discovered?

A It's the same, the result of reverse engineering and analysis of the code, so I was able to figure out that this vulnerability exists.
Q Do you know whether or not anyone else figured that out?
A No.
Q Now, Mr. Hagan also pointed you to the use of the term "3M hack." Do you recall that?
A Yes.
Q What does "3M" stand for?
A 3M stands for hack. It's a generally known term. The best way to describe it is the the slogan of the Three-Musketeers. The slogan is one for all, all for one. This technique consists of acquiring the minimal or base subscription, basic entitlements, and to watch all the programs, seeing all the services that are using the subscription.
Q Did you create the term "3M hack"?
A No.
Q Where does that term come from?
A Well, as I said, it's commonly known. It's usually used in slang.
Q That's the common term for that type of hack?
A Yes, more or less according to my understanding at that time.

Q Now, Mr. Hagan also pointed out that you had extracted

from the code the word "Nipper." Do you recall that?
A Yes.
Q Where in the card is that word found?
A It is found in the EEPROM area of -- in the storage area of EEPROM.
Q Is that word found in every card?
A I found it in every card.
Q So it wasn't you that discovered that? Anyone who looked at the EEPROM in an EchoStar Smart Card would find the same word; is that correct?
A Yes.
Q So it's not something unique to anything that you did?
A No.
Q Now, Mr. Hagan also asked you some questions about code that was eventually posted on the Internet. Do you recall that?
A Yes.
Q But Mr. Hagan actually didn't show you any of that code.
Can I ask you to look, please, at Exhibit 998 -- 511-A?
THE COURT: Just a moment. There is going to be confusion.
The code on page two at the top is going to be the same code that is on 998; is that correct?

♀

09:45:04 MR. SNYDER: That's not entirely correct.
THE COURT: Okay. Thank you very much.
MR. SNYDER: That's one of the things we are going to ask Mr. Mordinson about.
THE COURT: Thank you.
MR. SNYDER: You said Exhibit 998?
THE COURT: 998.
MR. SNYDER: That's correct. I thought you meant Exhibit 98.

THE COURT: No, 998.

MR. SNYDER: 998.

JUROR NO. 5: Could we take a break?

THE COURT: Yes.

You are not to discuss this matter amongst yourselves or to form or express any opinion concerning this case.

Have a nice recess.

(Recess.)

-oOo-

-oOo-

CERTIFICATE

I hereby certify that pursuant to Section 753, Title 28, United States Code, the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Date: April 11, 2008

Sharon A. Seffens 4/11/08

SHARON A. SEFFENS, U.S. COURT REPORTER

SHARON SEFFENS, U.S. COURT REPORTER