UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

HONORABLE DAVID O. CARTER, JUDGE PRESIDING

- - - - - - -

```
ECHOSTAR SATELLITE CORP.,   )
et al.,                     )
               Plaintiffs,  )
                            )
 vs.                        ) No. SACV-03-950-DOC
                            ) DAY 2
 NDS GROUP PLC, et al.,     )
                            )
               Defendants.  )
____________________________)
```

(Testimony of David Mordinson)

REPORTER'S TRANSCRIPT OF PROCEEDINGS

Santa Ana, California

April 10, 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

♀

I-N-D-E-X

PAGE

DAVID MORDINSON 4

♀

SANTA ANA, CALIFORNIA; THURSDAY, APRIL 10, 2008; A.M. SESSION

(Jury present.)

DAVID MORDINSON, PLAINTIFF'S WITNESS, SWORN

THE COURT: Would you please be seated here in the witness box which is just to my left.

Once again there is an interpreter with the gentleman.

Could I get the interpreter's name, please?

THE INTERPRETER: Hebrew interpreter Ayalla Dollinger. My oath is on file.

THE COURT: Thank you very much.

Mr. Mordinson, do you speak any English?

THE WITNESS: Yes, I do.

THE COURT: Do you need the services of the interpreter throughout your entire testimony, or do you feel capable of testifying in English and then if you need further translation or help relying upon the interpreter?

THE WITNESS: I will use the services of the interpreter during the course of my testimony.

THE COURT: Thank you.

This will be direct examination then by Mr. Hagan on behalf of Echostar of Mr. Mordinson.

Mr. Mordinson, would you state your full name, sir.

16:00:56 THE WITNESS: David Mordinson.

THE COURT: Would you spell your last name, sir.

THE WITNESS: M-o-r-d-i-n-s-o-n.

THE COURT: It appears that you speak very good English. Why don't we have the interpreter here, and if you need her services, then we will rely upon them.

THE WITNESS: I would like to be sure that my answers are exact and I understand the questions exactly to provide a truthful answer.

THE COURT: All right, thank you.

Counsel, your direct examination.

DIRECT EXAMINATION

BY MR. HAGAN:

Q Good afternoon, Mr. Mordinson.

A Good afternoon.

Q My name is Chad Hagan. I am one of the lawyers representing plaintiffs EchoStar and NagraStar in this litigation.

We have met before haven't we, sir?

A Yes.

Q In fact, we met on two separate occasions when we conducted your deposition for almost 14 hours; is that correct?

A Yes.

Q And through the course of that deposition, you

♀

16:02:02 testified the majority of the time in English?

A Yes.

Q And if today just as in your deposition -- if I ask a question and you don't understand the question, you can either ask me to clarify, or you can certainly use the interpreter that you brought with you today?

A Can you ask that question again?

Q Sure. Let me go slower.

If I ask you a question and you don't understand it or you need the interpreter, then just let us know, and we will pause for you?

A I will.

Q Mr. Mordinson, you are employed by the defendants in case, case?

A Yes.

Q What is your official title with the defendants?

A At the moment?

Q Yes, sir.

A I am a technical consultant for NDS marketing Europe and Israel.

Q When did you first start working for the defendants?

A I started working for NDS in September 1997.

Q And you started at NDS Israel's office; is that correct?

A Yes.

♀

16:03:11 Q And you started there as an engineer?

A Yes.

Q When you started to work for the defendants, they didn't tell you at that time that part of your job would be hacking into their competitors' technology; is that correct?

A I was hired as a software engineer and security analyst which I was supposed to be a security analyst and incur also hacking into security systems.

Q Now, as you understood it, when you started working for NDS in 1997, they were in the business and still are of providing conditional access technology, correct?

A Yes, that's correct.

Q And one of NDS's largest clients, especially in the United States, is DirecTV?

A Yes.

Q NDS competes in the conditional access market with the plaintiff NagraStar?

A With Nagra Vision.

Q And NagraStar is Nagra Vision's United States presence as you understand it, correct?

A Yes.

Q So in the United States, NDS competes directly with NagraStar?

A Yes.

Q NagraStar's largest client as you understood it at the

16:04:49 time of your deposition in the United States is the plaintiff Echostar?

A Yes.

Q Echostar competes with DirecTV to provide satellite television?

A Yes.

Q Now, when you started with NDS in 1997, it's fair to say that the defendants' encryption technology was compromised, correct? I can rephrase.

When you started working for NDS in 1997, you understood as an engineer for the company at that time that the defendants' technology was compromised or hacked, correct?

A Correct.

Q And you knew that that technology was hacked both in the United States and in European countries, correct?

A Yes.

Q And NDS engaged in two things to try to get their technology a little bit better as you understood it, correct?

A Can you be more specific?

Q During the 1997 time frame when you started to work for NDS, the technology that NDS provided was hacked, correct?

A Yes.

Q And NDS took certain steps to try to improve that

♀

16:06:14 technology, correct?

A Correct.

Q One of those steps was to hire some of the hackers that were responsible for hacking into that technology, correct?

A I don't know what you are talking about. Can you name some?

Q Certainly.

You are familiar with the name Christopher Tarnovsky and Oliver Kommerling aren't you, sir?

A Yes.

Q And you understood that Chris Tarnovsky and Oliver Kommeling were hired to come and work for NDS, correct?

A Chris Tarnovsky, yes, I knew him as an NDS employee. Oliver Kommeling, I didn't know if he was an NDS employee or not.

Q You understood that Mr. Kommerling had a special relationship with NDS; is that correct?

A Please define "special relationship."

Q You understood that Mr. Kommerling was doing consulting work for NDS?

A That's my understanding.

Q And you understood that at that time -- withdraw. You understood that prior to NDS hiring Mr. Kommeling he was engaged in illegal hacking activity, correct?

A I know that.

16:07:34 Q And NDS hired Mr. Kommerling in '97 -- or at least retained some type of consultancy agreement with him in '97, and Mr. Kommerling taught you and some of the other engineers in Haifa how to reverse engineer and hack?

A That's correct.

Q In fact, Mr. Kommerling has notority in this area because he has published an article with an individual named Marcus Koon. Are you familiar with that article?

A Yes, I know of this article published by Oliver Kommerling together with Marcus Koon.

Q You recall that the name of that publication was "Design Principles of Tamper-Resistent Smart Cards"?

A Possibly, yes.

Q And you understood that Mr. Kommerling published this article prior to forming a consultancy relationship with NDS, correct?

A According to my knowledge, this article was published in 1999.

Q So two years after he started working?

A Yes.

Q And is it fair to say that Mr. Kommerling taught you and Zvi Shkedy certain techniques to attack the computer chip or microcontroller that is contained within Smart Cards?

A It was mostly to Zvi Shkedy, not to me.

16:09:13 Q And those are some of the invasive attacks that Haifa Research Center used?
A Yes.
Q In addition to the defendants hiring some of these hackers in 1997, they also engaged in reverse engineering and hacking its competitors' technology?
A Correct.
Q And you were principally involved in those efforts weren't you?
A I was.
Q You and the gentleman that the jury heard from this morning, Zvi Shkedy?
A Yes.
Q If I understand it correctly, Mr. Shkedy was the defendants' engineer that reverse engineered the hardware on the chip, correct?
A Yes.
Q In other words, he popped that chip out and used some of the techniques taught by Mr. Kommerling to pull the code -- the secret encryption code out of that chip; is that correct?
A I would not agree with the definition of "secret encryption code."
Q Let's briefing go through the steps from your deposition.

♀

16:10:21 A Okay.
Q Mr. Shkedy first pulled the chip, the CPU or microcontroller, off of Echostar's access card?
A Yes.
Q After he did that, he used nitric acid to dissolve the epoxy that was surrounding that chip?

A Yes.

Q Once he did that, he used hydrofluoric acid to delayer the chip?

A Yes.

Q Then he used an optical microscope to analyze the fine layers that he had decapsulized from the chip?

A Yes.

Q After he did that, Mr. Shkedy engaged in what you called a biological process where he used his mind to analyze the chip, correct?

A Yes.

Q Then Mr. Shkedy used a FIB, or what we have referred to as a focus ion beam, in order to disconnect the instruction latch and expose the data bus on that chip?

A In this particular chip, yes.

Q And these are some of the same invasive attack techniques that Mr. Kommerling had taught you and Zvi Shkedy?

A Yes.

16:11:42 Q Now, once Mr. Shkedy was able to pull the code out of Echostar's microcontroller, that's where you came in; is that right?

A Yes.

Q You were a software engineer?

A Yes.

Q And it was your job on behalf of the defendants to take that code and disassemble it, correct?

A Yes.

Q Can you explain to the jury what disassembling of code means?

A Disassembling of code consists of turning the binary code, or what was written in machine language which is not understandable by humans, into kind of a language that can be understandable by humans and can be analyzed. This process is called disassembling.

Q During the course of your work -- let me back up for a second. The project that you and Zvi Shkedy worked on for the defendants where you reverse engineered Echostar's Conditional Access System was referred to as to the Headend Project; is that correct?

A Yes.

Q Now, your portion of the Headend Project, about how many months did that take?

A I started to work on the code that Zvi Shkedy extracted

16:13:07 from the chip in April -- I believe it was in the beginning of April 1998. It took me almost four months -- or four-and-a-half months to get a complete understanding of this code, and after that I prepared a report about the findings on this project.

Q During your work on the Headend Project, in addition to disassembling the code, you also analyzed that code?

A Yes.

Q In order to perform that analysis, you created certain software applications?

A Yes.

Q One of those software applications was a program called SC Talk, correct?

A Yes.

Q And the SC stands for Smart Card?

A Yes.

Q What was the purpose of creating that application?

A The SC Talk application was helping to communicate with the Smart Card.

Q You also developed a software for purposes of the Echostar project called Get ATR, correct?

A Yes.

Q What does the ATR stand for?

A ATR stands for after to recent. According to the standard, which every Smart Card should comply with, the

16:14:46 first message that Smart Card sends in response to a recent signal to the device that reads the -- hosts the Smart Card is a short message. This message is a standard message.

THE COURT: Move the microphone just a little closer to you. Thank you.

BY MR. HAGAN:

Q Now, SC Talk and Get ATR were not the only software applications that you personally developed for use in the Echostar project, correct?

A Yes.

Q You also developed a software application that you referred to as Sniff Host?

A Yes.

Q And can you explain to the jury what the purpose of that application was?

A Sniff Host was an application that was communicating with a sniffer device, therefore the name, and this application was responsible to get information from a sniffer device and record it on a file on a disk of a personal computer.

Q Now, did you develop any other software applications for purposes of the Echostar project other than Sniff Host, Get ATR, and SC Talk?

A As far as I recall, I developed also file forma converters, which had to convert data from one forma to

16:16:21 another.

Q And that software application was used to convert some of the code that Zvi Shkedy had extracted from the card, correct?

A Among other things, yes.

Q Now, did anyone assist you in developing these software applications that you used and the defendants used in reverse engineering EchoStar's technology?

A No.

Q You developed those software applications as part of your work for the defendants?

A Yes.

Q You developed those software applications specifically for use in reverse engineering work that you did for the defendants, correct?

A Yes.

Q Have you patented any of these software applications?

A I'm sorry?

Q Have you applied for patents on any of the software applications that you developed?

A According to my knowledge, software is not subject for patenting.

Q Have you applied for any sort of intellectual property rights for the these software applications that you developed?

♀

16:17:26 A I'm sorry. Can you repeat that?

Q Have you made an application for any intellectual property rights for the software applications that you developed for use in the Echostar project?

A No.

Q Once you were able to disassemble the code, you analyzed Echostar's code in order to try to out the memory locations?

A Yes.

Q You mapped out for instance where the RAM or Random

Access Memory starts?

A Yes.

Q You mapped out where the ROM and EEPROM memory locations are?

A Yes.

Q Can you explain to the jury the difference between ROM and EEPROM that you analyzed from Echostar's code?

A Certainly. ROM stands for read on the memory. This memory is programmed in the production stage and cannot be modified during the lifetime of the Smart Card or the chip. EEPROM stands for electronically erasable programmable read on the memory, which can be modified anytime and data retained in this memory even if the power supply is disconnected.

Q Now, once you have mapped out the memory locations, you

16:19:07 began to study and analyze those memory locations as part of your work on the reverse engineering project, correct?

THE INTERPRETER: I'm sorry, counsel. Can you repeat the question again?

BY MR. HAGAN:

Q Once you mapped out the memory locations from Echostar's code, you then analyzed those memory locations and the ROM, RAM, and EEPROM code contained within them?

A Actually, the code is contained on the ROM and EEPROM. RAM does not contain any code because it's Random Access Memory, and its content is lost when the power supply is disconnected.

Q Thank you. You are the expert in this case. Let me rephrase my question.

Once you mapped out the ROM and EEPROM, you analyzed both those memory locations and the code as part of your work for the defendants, correct?

A Yes.

Q And one of the reasons that you analyzed that code was to determine whether or not there were vulnerabilities or weaknesses in Echostar's security system, correct?

A   Yes.

Q   And, in fact, that was the main goal to use your words of the Headend Project, correct?

A   No.

16:20:46 Q   What was the main goal then?

A   The main goal of this project was to get the complete understanding of the Echostar -- Nagra Conditional Access System. That's it.

Q   When you say Nagra, you are referring to Echostar's system supplied by NagraStar?

A   Yes.

Q   The plaintiffs in this case?

A   Yes.

Q   Now, once you extracted the code, converted the code, analyzed the code, you were able to determine that there were certain inherent flaws or vulnerabilities in that code; isn't that correct?

A   Yes.

Q   And one of those was the IO buffer overflow?

A   It's not exactly that.

Q   Are you familiar with the term "IO buffer overflow"?

A   Yes.

Q   In fact, that term is in the document that you created, the Headend Report, that we looked at earlier today?

A   Yes.

Q   And IO stands for "input/output"; is that correct?

A   Yes.

Q   Explain to the jury what you mean by buffer overflow.

A   Certainly. The buffer overflow technique or IO buffer

16:22:04 overflow technique consists of filling the IO buffer, which is supposed to store the data that is passed through the Smart Card, so filling this buffer -- this extra information will override the data which is located after -- in memory located after this IO buffer is placed in it. In this way, somebody can modify the data which was not supposed to be modified in RAM.

Q Now, the microprocessor that the defendants used at this time didn't have an IO buffer overflow vulnerability did it?

A No.

Q So studying that particular vulnerability in Echostar's system certainly didn't help NDS improve its technologies in any way, correct?

A Okay, yes.

Q In addition, you also determined through your analysis of Echostar's system that you could execute code in the RAM portion of the memory; is that correct?

A Yes, that's correct.

Q And what do you mean by executing code in RAM? Can you explain that to the jury?

A Codes, which means machine instructions that the media processor of the Smart Card is executing, they allocate it in memory and are fetched one by one by the microprocessor. These instructions can be located in memory which can be

16:23:46 RAM, ROM, or EEPROM in this particular architecture, so putting codes or putting instructions into RAM isn't different from putting them into ROM or into EEPROM. All it takes is just to make the microprocessor execute them.

Q And you determined from the defendants' analysis and your analysis of Echostar's security system that you could

execute code in the RAM portion of the card, correct?
A   Yes.
Q   That includes malicious or pirate code?
A   Not necessarily.
Q   In fact, you used some of that type of code in order to dump the EEPROM, for example?
A   I used code to dump EEPROM.
Q   And you executed that code in the RAM portion of the memory?
A   Yes.
Q   Now, you also determined from reverse engineering Echostar's security system that there was an inherit characteristic called RAM ghosting effect or address aliasing; is that correct?
A   RAM ghost effect, yes.
Q   Can you explain to the ladies and gentlemen what RAM ghost effect is?
A   Actually, it's more general than RAM ghost effect. It's memory ghost effect. A good analogy for this can be if

16:25:39 you look at the number of a house at a particular address and you just ignore, for example, the hundred of this number and look only at 10 and the rest, the last two digits of the house -- if you are delivering correspondence, for example, to house No. 101 or 201 or No. 1, the oldest correspondence will arrive exactly at the same house because there is no difference between those addresses if you ignore the hundred.

It's similar in a microprocessor. When you address memory, you have to specify the number of the house that you are addressing it to. If you ignore the major part of the address -- the more significant part of the address, you will get -- it will get to the same location even if you address it to a different location.
Q   Now, it took me quite a bit of time to understand this

concept in the deposition, so let me see if I have it right now, and let's try to explain it to the jury in a way that they can get their arms around it.

Your hacking and reverse engineering of Echostar's security system identified three characteristics: the IO buffer overflow, the RAM ghost effect, and the ability to execute code in RAM, correct?

A The third is a particular technique that utilizes the latter two. I would say the memory ghost effect or memory analyzing and the possibility to execute code from RAM. IO

16:27:58 buffer overflow is the technique that used these two vulnerabilities.

Q So the IO buffer overflow was the exploit or the technique that you were able to use in order to leverage the other two vulnerabilities: the RAM ghost effect and the executing code in RAM, correct? Do you want me to repeat it?

THE INTERPRETER: Yes.

BY MR. HAGAN:

Q Utilizing the IO buffer, in other words, overflowing that buffer was the method that you discovered to leverage both the RAM ghost effect and the ability to execute code in RAM?

THE COURT: You may have to break that down if it's being translated. Let's make sure the translator got that.

THE WITNESS: What do you mean by leverage?

MR. HAGAN: Let me try to rephrase it.

BY MR. HAGAN:

Q You developed a technique in order to hack Echostar's ROM 3 access card, correct?

A Yes.

Q And that technique included overflowing the input/output buffer, correct?

A   Yes.

16:29:22 Q   Once you overflowed the buffer, you were able to use the RAM ghosting effect or address aliasing to remap code that overflew the buffer to other parts of the RAM memory locations, correct?

A   Let me explain it in my way.

Q   Certainly.

A   As I explained the principles of IO buffer overflow, by overflowing the buffer, I was able to implant code or put the code into the RAM and make the microprocessor execute it, and the basic of this method or technique was the memory ghost effect and the possibility to execute code from RAM. That's it.

Q   You also -- in addition to the IO buffer overflow, the RAM ghost effect, and the ability to execute code in RAM, you determined that there were two other characteristics for Echostar's card? Those were the index variable and exception handling; is that correct?

A   I don't recall.

Q   Are you familiar with the term "index variable" as it relates to Echostar's security system?

A   I don't recall that. Sorry.

Q   We will take a look at your Headend Report a little bit later, and we will see if it refreshes your recollection.

Once you finished your analysis of Echostar's security system, the code that had been extracted, you used that

16:31:14 information to develop or construct a method to hack Echostar's card, correct?

A Yes.

Q Prior to doing that, though, you had to get some type of data communication logs from an Echostar receiver and a Echostar Smart Card, correct?

A Yes.

Q In order to get that information, you and Zvi Shkedy came over to the United States, correct?

A Yes.

Q When was that?

A The first time was in June 1998.

Q And you and Mr. Shkedy flew over to the United States from Israel, correct?

A Yes.

Q You flew over to the United States as part of your work for the defendants?

A Yes.

Q And you flew over to the United States pursuant to their instructions in fact, correct?

A Yes.

Q When you got to the United States, though, you didn't go to an NDS office did you?

A No, we didn't.

Q You didn't go to an NDS employee's home did you?

♀

16:32:25 A No.

Q In fact, you didn't go to any official establishment at all did you?

A We didn't.

Q You were instructed to go to two homes of private citizens that you didn't know, correct?

A We were instructed to go to one private home, and the second was our decision.

Q The second was your personal decision?

A Not my personal decision, but we experienced some difficulties in the first house, and, therefore, we had to use an alternative location.

Q Let me back up for a second and make sure we understand this.

The defendants instructed you to fly over to the United States in order to log the data stream between one of my client's Smart Cards and their set-top-boxes, correct?

A Yes.

Q But they didn't tell you to go to any official establishment? They told you to go to this private residence?

A Yes.

Q Did you ask anyone why you weren't going to an NDS office or any type of official facility to conduct this research?

16:33:39 A No, I didn't ask.

Q Is there any particular reason why not?

A No.

Q At your deposition, you told me that the reason was that it was obvious? The Headend Project was supposed to be kept secret, correct?

A Yes.

Q And not just the part of the project when you flew over to the United States with Mr. Shkedy but all aspects of the project, correct?

A Yes.

Q All the work that you did and Zvi Shkedy did on behalf of the defendants to hack Echostar's security system, you you were instructed to keep that secret?

A Yes.

Q When you got to the United States, you had to capture this data stream? You used a device that the defendants developed; is that right?

A Yes, we developed it.

Q That device is called the sniffer?

A Yes.

Q As I understand it, that device plugs into both the Echostar receiver and then has a slot for the Echostar Smart Card, correct?

A You don't describe it exactly, but in principle, that's

16:34:48 it.

MR. HAGAN: Your Honor, can we set up a demonstrative in the well of the courtroom? I have spoken to Mr. Snyder about this at the break, and it's my understanding that the defendants do not have any objection.

THE COURT: As long as you both agree, I am more than pleased do that.

MR. SNYDER: If it's the one we were shown, Your Honor, we have no objection.

BY MR. HAGAN:

Q While we are going to get that, let's talk a little bit about this process that you and Zvi Shkedy engaged in when you came to the United States.

You hooked this device up, the sniffer, that the defendants developed to an Echostar subscriber's system, correct?

A Yes.

Q And that device was able to capture the data stream that went back and forth between the Echostar Smart Card and the Echostar receiver, correct?

A Yes.

Q And you needed to log that data as part of your efforts to hack Echostar's security system or at least to speed up the process?

A To speed up the process, yes.

16:36:29 Q Now, Mr. Mordinson, we heard Zvi Shkedy testify earlier today that the reason you had to come to the United States was because you weren't able to receive Echostar's encrypted signal from NDS's office in Israel; is that correct?

A Yes.

Q So you came over here to do it, right?

A Over here?

Q Over to the United States.

A Yes.

Q And when you got here, you set this equipment up, and you logged the data stream for what, 10 minutes, 20 minutes?

A I believe it was longer.

Q And you logged the data stream at a particular time? In other words, you didn't just log the data stream coming down from any program or any channel? You needed to log that data stream when the card was being paired or married to the receiver; is that correct?

A Yes.

Q Can you explain to the ladies and gentlemen of the jury what that process is for Echostar's system, the process of pairing or marrying a Smart Card with a receiver?

A The Smart Card as counsel said is married to the set-up-box in the way that the Smart Card and the set-up-box is the same key in order -- used in order to encrypt the communication -- certain communication between the Smart

♀

16:37:58 Card and IOD after the authorization or after the pairing.

MR. HAGAN: Can we take a look at the picture that has been marked as Plaintiff's Demonstrative No. 5 I believe? It's a picture of the sniffer.

BY MR. HAGAN:

Q I am handing you a copy of what we have previously used in this trial as Plaintiff's Demonstrative No. 5. Can you tell the jury what this is?

A Yes. From what I can see, I can see a sniffer device which is upside down of course for some reason. I see a Smart Card slot, and I see a tong, which is an adapter, and a flex cable connection between the devices.

Q This is the device that the defendants built?

A Yes.

Q If I understand it, the way this device works is you take Echostar's Smart Card, and you put it into one side of it? There is a slot for it?

A I can't hear you.

Q You put an Echostar Smart Card into the slot in this device that you call the sniffer?

A Correct.

Q And the other part of that device goes into the Echostar receiver?

A Yes, that's correct.

Q And the purpose of this device is to capture the data

♀

16:39:40 stream that goes between the receiver and the card?

A Yes.

Q Once you got that information, what did you do? What was the next step in your process to develop a hack for Echostar's security system?

A I analyzed messages running between the Smart Card and the set-up box because the communication between those devices consists of messages, so I couldn't distinguish between messages. By analyzing the software of the Smart Card, I could identify particular functions or particular blocks in the software which were responsible for parsing or processing those messages. In that way, it helped to speed up the process of analyzing.

THE COURT: Let's be careful with the terms.

Is a set-up box the same as the receiver?

MR. HAGAN: Yes.

THE COURT: Well, then you are going to change it. You used receiver, and the gentleman used set-up box. I just want to make sure the jury understands that.

BY MR. HAGAN:

Q Let's use the term you are familiar with, "set-top-box."

So the sniffer goes between the set-top-box and the card?

A No.

♀

16:41:07 Q Are there any other components outside of the access card, the set-top-box, the sniffer, and the computer that would you use to log the data?

A According to my knowledge and according to what you represented, I can see that this device is connected in parallel to the communication line between the Smart Card and the set-up box.

Q Is this the same device that you and Zvi Shkedy used in the United States?

A I believe so.

Q I will represent to you that your lawyers in this case produced this device for us to inspect. You don't have any reason to believe that they gave us a different device do you?

A No.

Q Now, once you had that logged data stream, you went back over to the defendants' office in Israel?

A Yes.

Q And you used that information as well as all of the other information that you and Zvi Shkedy developed in order to create a hack for Echostar's system?

A In order to analyze the Echostar system.

Q Well, you went a little bit further than that. Let's be fair.

You not only analyzed it, but you created a method to

♀

16:42:21 hack it?
A That's correct.
Q In fact, that's what you put in the Headend Report, among other things?
A Among other things, yes.
Q Now, once you developed that hack, you didn't stop at that point. You went a little bit further. You had to come back to North America to test that hack?
A Yes.
Q When was that?
A It was in September 1998.
MR. HAGAN: Permission to approach the well.
THE COURT: You may.
BY MR. HAGAN:
Q Again, in September '98, it was you and Zvi Shkedy that came back over here to the United States?
A I didn't hear you.
Q In September '98, the second trip, it was you and Zvi Shkedy again?
A Yes.
Q You came on this second trip as part of your work for the defendants?
A Yes.
Q They knew that you were coming over here to test the hack that you had developed?

♀

16:43:24 A Who?
Q The defendants. NDS knew that you and Zvi Shkedy were coming to the United States to test this hack?

A Yes.

Q When you got to the United States -- you flew from Israel to Baltimore?

A Yes.

Q What did you do next?

A In Baltimore, we had a rental car. We went to a house, private house, of Ms. Vared (phonetic). We took the set-up box from her, and we returned to Baltimore by the same car. We took a flight to Cleveland, and from Cleveland, we took another car, a rental car, and went to Windsor, Ontario, Canada.

Q Let me make sure I understand this. You flew to Baltimore, rented a car, and you went and picked up a Echostar receiver?

A Yes.

Q You didn't get that receiver from Echostar, right?

A No.

Q In fact, even though you could have purchased that receiver at Wal Mart Or target or Sears, you didn't do that either?

A No, we didn't.

Q You went to a private citizen's house to?

♀

16:44:53 A Yes.

Q One of the individuals that you came to the first time to capture the data stream between the receiver and the Smart Card?

A Yes.

Q You brought with you one of the Echostar Smart Cards that you had in the office in Israel?

A Yes.

Q You also brought a computer with you?

A Yes.

Q And on that computer, you had the hack software, the program, that you had developed for Echostar's system, correct?

A No. I composed it later. Let me explain. When counsel are talking about the software -- actually the image, the hacking, the knowledge existed. For example, the method or the technique to override IO buffer and implement code into the Smart existed on my computer. It was not particularly ready for establishing the hack. The image or what was tested was composed at a later stage in Ontario, Canada.

Q So you actually finalized the development of the hack in North America?

A In Canada.

Q In North America?

16:46:17 A Yes.

Q During the second trip that you made to the United States into Canada?

A Yes.

Q So you picked the receiver. You got your Smart Card, and you got the software that you had developed, and you finalized that on this trip? You rented another car, and you drove across the border into Ontario?

A Yes.

Q And when you got to Ontario, you didn't go to an NDS office, right?

A There is no NDS office in Ontario.

Q You didn't go to any official office did you?

A No.

Q You went to a basement in someone's house that you didn't know, correct?

A I didn't know, yes.

Q You went to the basement?

A Yes.

Q And when you got to the basement of this person's house you didn't know, you hooked up the Echostar receiver that you got in the United States to a satellite DISH like this one?

A It was not the DISH network. It was Express View.

Q Bell Express?

16:47:18 A Bell Express.

Q You understood at that time that Bell Express View also used the encryption technology developed and provided to Echostar by NagraStar?

A I realized it later during the trip.

Q So once you looked up the satellite DISH to the Echostar receiver, what did you do next?

A I'm sorry?

Q What did you do after you hooked up the Echostar receiver with the satellite DISH?

A I took the Smart Card that I brought from Israel and I finalized the image or the memory -- the EEPROM memory content for this card. I wrote this image to the card, and then I inserted it into the set-up box.

Q Does this look like one of the Echostar Smart Cards that you used?

A No.

Q What did the one you used look like?

A It was a blue color with a lot of types of various programming on it, with DISH network logo on it on the image side.

Q So the card was blue, and it had DISH network on it?

A Yes.

Q And different programming logos like HBO, Cinemax, Showtime --

16:48:48 A Like that. I don't remember exactly.

Q On the back of that card was the microprocessor?

A Yes.

Q That Zvi Shkedy ripped out of the card and reverse engineered and you analyzed?

A Like that one, yes.

Q Once you had the card you had to reprogram the card in order to test the hack you developed?

A Yes.

Q And you built a device to reprogram Echostar's access card, correct -- actually, you modified the sniffer that you had already developed?

A Yes.

Q With some of the software that you had developed?

A Yes.

Q So you took Echostar's card -- let me back up. It was Echostar's card at the time, right? It said "DISH Network" on it?

A It was DISH Network I believe.

Q You take Echostar card and you reprogram it with the sniffer device that the defendants developed?

A Yes.

Q And then you put the card into the receiver, correct?

A Yes.

Q Did it work?

16:49:48 A Yes.

Q Initially or did you have to take a couple of steps?

A The reception signal was not sufficient to establish the reception of the satellite signal -- I'm sorry. From the beginning, because we used not the original DISH network satellite DISH, the strength of the signal that we managed to acquire by this -- receive by this satellite DISH was not sufficient to establish a satellite system.

The problem was that the LNB that you see in the presentation of the block in the front of the DISH of the antenna -- this block was not suitable for receiving a signal from a DISH network satellite, so we had to somehow acquire or to buy this suitable LNB, or low noise block, which will give us enough strength of the signal.

Q The LNB that you were using initially was for a Bell Express View system?

A Yes.

Q So you tried to hack. It didn't work. Then you sent -- Zvi Shkedy went back into the United States to get an LNB that would work for Echostar's system?

A Yes.

Q He brings that back across the border to Canada, and you hook up that up to the DISH?

A Yes.

Q Then you test your hack again?

16:51:33 A Actually we didn't test the hack before. We didn't manage to establish the satellite system. The reception was very bad. Therefore, that was the reason to obtain the LNB or the part of antenna which was suitable for such a system, and once we obtained the low noise block suitable antenna, we tested the card.

Q Once you put the Echostar LNB onto the satellite DISH, you were able to successfully test the hack that you developed?

A Yes.

Q It opened up all of Echostar's channels?

A Yes.

Q And you knew that because you looked at the EPG, the Electronic Programming Guide?

A Yes.

Q So the hack that you developed on behalf of the defendants for Echostar's security system was a success?

A Yes.

Q Let's back up for just a second. You mentioned programming a minute ago.

You understand as part of your work for NDS that the programming content is scrambled because it's copyrighted?

A Yes.

Q And NDS or DirecTV just like Echostar is required to take certain steps in order to protect that copyrighted

16:53:06 programming, correct?

A I understand that, yes.

Q And one of those steps is to develop and utilize these Conditional Access Systems?

A Yes.

Q You understand that the copyrighted programming for Echostar and for DirecTV is sent out to its subscribers across the United States?

A Yes.

Q And those subscribers pay a monthly fee for that programming?

A I believe so.

Q As you understand it?

A Yes.

Q So if the hack that you developed for the defendants and successfully tested in Canada with Zvi Shkedy were to get out into the pirate community, that would allow them to steal Echostar's copyrighted programming, correct?

A Hypothetically speaking, yes.

Q Well, we don't have to talk about hypothetically, though, because you know that there was a hack methodology posted on the Internet on a pirate website in December of 2000?

A I got this knowledge in the summer of last year, yes.

Q You took a look at that methodology?

16:54:26 A Yes.

Q You took a look at the instructions to hack Echostar's system that was posted on the Internet?

A Can you be specific when?

Q You certainly looked at before you gave sworn deposition testimony in this case?

A Yes.

Q And you agreed with me at your deposition that there were certain fundamental similarities between the hack that was posted on the Internet and the hack that you developed on behalf of the defendants, correct?

A They use the same -- they utilize the same weaknesses and vulnerabilities, yes.

Q They use both hacks, the -- we will call the one on the Internet the Nipper hack because you understood that that was the alias they posted it?

A Can you repeat, please?

Q Your understanding of the hack that was posted on the Internet was posted under an alias Nipper, right?

A I don't remember that. It was represented to me in August last year, 2007, during preparation for my deposition. I didn't pay attention what was the name or alias of the person who posted it.

Q You are familiar with the name Nipper? You have heard that term before?

16:56:01 A Yes.

Q In fact, you discovered the term "Nipper" embedded inside Echostar's code that was pulled out of the microcontroller?

A I found this name in Echostar's EEPROM, yes.

Q In Echostar's code that you pulled out of the microcontroller?

A Yes.

Q Now, you agreed with me at your deposition that the hack that was posted on the Internet and the hack that you developed for the defendants both used the IO buffer overflow method of attack, correct?

A Yes.

Q You also agreed that both of those hack methodologies exploit the RAM ghost effect or address-aliasing characteristic of Echostar's system?

A Yes.

Q And that was an inherent characteristic that you discovered through your work on the Headend Project?

A I discover this, yes.

Q You also agree that both of those hacking methodologies use the ability to execute code in RAM in order to work, correct?

A Yes.

Q After you tested the hack that you developed for

16:57:40 Echostar's system, you went back over to NDS's office in Israel?

A Yes.

Q And you created a report, correct?

A Yes.

Q And you called that the Headend Report?

A Yes.

Q In that report, you described in specific detail the steps that you took to hack Echostar's security system?

A Yes.

Q You also you also described the IO buffer overflow, the RAM ghost effect?

A   Yes.

Q   And the ability to execute code in RAM, qualities of the card that you had discovered, correct?

A   Yes.

Q   And then you distributed this report to people within the Haifa Research Team?

A   Correct.

MR. HAGAN: Your Honor it's 5:00. I am at a stopping point in the cross-examination. If the jury wants to go home, we can conclude for the day.

THE COURT: All right.

*   *   *

♀

16:58:43

♀

16:58:43 -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 10, 2008

Sharon A. Seffens 4-10-08
SHARON A. SEFFENS, U.S. COURT REPORTER

♀

16:58:43