UNITED STATES PATENT & TRADEMARK OFFICE
BEFORE THE PATENT TRIAL & APPEAL BOARD

- - - - - - - - - - - - - - - - - - x

COMPASS BANK, COMMERCE BANCSHARES, INC. AND FIRST NATIONAL BANK OF OMAHA :

Petitioners :

vs. : No. IPR 2014-00786

INTELLECTUAL VENTURES, II, LLC :

Patent Owner :

- - - - - - - - - - - - - - - - - - x

December 10, 2014

Washington, D.C.

VIDEOTAPED DEPOSITION OF:

DR. GEORGE KESIDIS

was called for examination, pursuant to notice, taken at Kutak Rock, 1101 Connecticut Avenue, N.W., Suite 1000, Washington, D.C., commencing at 9:10 a.m., before Misty Klapper, a Notary Public in and for the District of Columbia, when were present on behalf of the respective parties:

Case
Compass, et al. v.
Intellectual Ventures
IPR2014-00786

Exhibit
2019
Intellectual Ventures

c4ea61a5-485d-4192-937b-dc6133d2c9f4

APPEARANCES:

JASON JACKSON, ESQ.
Kutak Rock, LLP
1650 Farnam Street
Omaha, NE 68102
AND
MARC VANDER TUIG, ESQ.
Senniger Powers
100 North Broadway
17th Floor
St. Louis, MO 63102
AND
GEOFFREY GAVIN, ESQ.
Jones Day
1420 Peachtree Street, N.E.
Suite 800
Atlanta, GA 30309
COUNSEL FOR THE PETITIONERS

BRIDGET O'LEARY SMITH, ESQ.
Knobbe Martens
2040 Main Street
14th Floor
Irvine, CA 92614
COUNSEL FOR THE PATENT OWNER

ALSO PRESENT:

Ellen Hebert, Video Operator

Don Coulman, Intellectual Ventures

c4ea61a5-485d-4192-937b-dc6133d2c9f4

C O N T E N T S

E X H I B I T S

Note: Exhibits retained by counsel.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

P R O C E E D I N G S

(Thereupon, the video operator made a statement for the record and counsel introduced themselves)

Whereupon:

DR. GEORGE KESIDIS,

was called for examination, and, after being duly sworn, was examined and testified as follows:

EXAMINATION BY COUNSEL FOR THE PATENT OWNER

BY MS. SMITH:

Q. Good morning.

A. Good morning.

Q. Okay. Could you please state your name and current address for the record?

A. George Kesidis. I live at 692 Tanager Drive, State College, Pennsylvania.

Q. Okay. Okay. Have you been deposed before?

A. I have.

Q. All right. So you're familiar with the

c4ea61a5-485d-4192-937b-dc6133d2c9f4

procedures.

So you understand that you're testifying under oath today?

A. Yes.

Q. Okay. And you understand your testimony has the same effect as if you were testifying in court?

A. Sorry?

Q. You understand that your testimony has the same effect as if you were testifying in court?

A. Okay. I wasn't sure an IPR is considered court --

Q. Well --

A. -- but, sure.

Q. -- okay. And you understand that a Court Reporter is recording a transcript of your testimony?

A. I do.

Q. Okay. And a video -- videographer is recording a video of your testimony?

A. I do.

Q. And do you understand that a transcript or video may be given to the panel of administrative

c4ea61a5-485d-4192-937b-dc6133d2c9f4

patent judges at the Patent and Trademark -- Patent Trial and Appeal Board?

A. I -- I do.

Q. Okay. Any reason you can't provide truthful and accurate testimony?

A. No.

Q. Okay. Good health?

A. Yes.

Q. Okay. Any medications that would impact your ability to testify today?

A. No.

Q. Okay. I'm embarrassed to ask this, but have you ever been charged or convicted of a felony?

A. No.

Q. Okay. That was easy.

Are you receiving any compensation for your time today?

A. I am, yes.

Q. Okay. How much?

A. For testimony it's $600 an hour.

Q. Okay. And from whom are you receiving the compensation?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. From -- I guess directly from, I -- I think, Cahn & Associates, who recruited me as an expert. I -- I think it's C-A-H-N.

Q. Okay.

A. And I think they, in turn, bill the -- the Plaintiffs, I suppose.

Q. Okay. Okay. So did you sign an engagement agreement pertaining to your involvement in this IPR?

A. With -- with Cahn.

Q. With Cahn, okay.

A. Yeah, with Cahn, not directly with counsel or the -- the Plaintiff.

Q. And so somebody from Cahn countersigned the engagement agreement?

A. That's right.

Q. Okay.

A. I don't have it with me, but I'm sure I can make it available.

Q. That's okay.

Were there any companies identified in the engagement agreement?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. Yes.

Q. Okay. Which --

A. I'm -- I'm sorry. I guess. I'm not sure. I -- I haven't looked at it in six months.

Q. Okay.

A. I'm assuming that the -- the three banks were -- were named.

Q. Okay.

A. And maybe the case itself was named. IV may have been named, but I don't -- I don't recall. I haven't looked at the form in months.

Q. Okay. And I assume you're being compensated for your time in this IPR proceeding?

A. I thought you already asked that, but yeah. Yeah.

Q. For your time today. Just in this proceeding --

A. Oh, yes.

Q. -- in general.

A. In general, yes.

Q. Okay. Okay. And how much -- how much have you received to date?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. I -- I think about $20,000, but I'm not sure.

Q. Okay.

A. Maybe -- about $20,000.

Q. And does the -- the compensation agreement -- the compensation arrangement the same, you received the payment from Cahn?

A. Yeah, I -- I bill Cahn.

Q. Okay.

A. And then what he does, I guess, is add the service fee and so on.

Q. And is your compensation rate different for non-testimony work?

A. Yeah.

Q. Oh, okay. What's that?

A. The -- I've forgotten the number. I believe it's -- I believe it's 450 --

Q. Okay.

A. -- for non-testimony.

Q. So before becoming involved in this proceeding, were you ever a consultant or employee of a bank?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. Ever?

Q. Ever.

A. Let's see, when I was a kid I -- I worked for IBM on a work term and -- in the downtown Toronto office. And I believe the work involved a client that was a bank. So to the extent that that is --

Q. Okay.

A. -- yes or no, but this would be 1980s.

Q. Okay. And so other than that --

A. I don't think I've worked for a bank other than that, no.

Q. Okay. So other than that arrangement that you had mentioned back in the '80s, any other work for IBM?

A. The arrangement was -- yeah, I was on a -- I was on a work term. I actually was a co-op student as an undergraduate. So that was why I -- I worked for IBM for one or two semesters.

Q. Okay.

A. In the '80s.

Q. Okay. So nothing after that?

A. No, I didn't work for IBM after that.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Okay. And were you ever a consultant -- do any consulting or were you ever an employee of Intellectual Ventures?

A. No.

Q. Okay. Do you have any ownership interest in a bank, such as stock or options?

A. I don't think so, no.

Q. Okay. What about IBM?

A. No.

Q. Okay. Have you ever received any compensation from or on behalf of IBM?

A. No.

Q. Do you know -- so you -- you mentioned that you're affiliated with Penn State, correct?

A. I don't think I mentioned that, but I am affiliated with Penn State, yes.

Q. Okay. Do you know if your department receives funding from IBM?

A. I don't know.

Q. Okay.

VIDEO OPERATOR: Sorry, Doctor, can I ask you to slide your microphone up?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

THE WITNESS: Is that what happened? Is that what you're saying? Sorry, you were giving me hand signals and I wasn't listening. I wasn't paying attention. Sorry.

VIDEO OPERATOR: Thank you.

BY MS. SMITH:

Q. Have you discussed IBM with anyone within maybe the last two years?

A. How do you mean discussed?

Q. Just -- just in general.

A. IBM comes up.

Q. Okay.

A. Students go work there and colleagues work there. I meet people from IBM all the time.

Q. Does the name Eugene Goryunov mean anything to you?

MR. JACKSON: Objection, scope.

THE WITNESS: I don't know that I've heard the name before.

BY MS. SMITH:

Q. Okay. Does the name Ken Adamo mean anything to you?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. No.

MR. JACKSON: Objection, scope.

BY MS. SMITH:

Q. Does the name Steven Bellovin mean anything to you?

A. Steven's name I've heard before. I haven't met the man, but I -- I've heard of him and read his papers.

Q. Okay.

A. Goryunov, I may have heard the name before, but I -- I don't know who he is or --

Q. Okay. Have you ever had written communication with Dr. Bellovin?

A. I don't think so.

Q. And I think you mentioned you've never spoken with him, correct?

A. I don't think I've spoken with him, no. I mean, we may have been on a -- there may have been an E-mail that was mailed to a bunch of people and we were on the mailing list together, but that -- that doesn't constitute direct communication I don't think.

Q. Okay. Have you ever heard of

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Intellectual Ventures prior to becoming involved in this proceeding?

A. I have heard of IV, yes.

Q. Okay. In what context?

A. I do patent cases, so I understand IV is a patent owner.

Q. Did you have an opinion of Intellectual Ventures before becoming involved in this case?

A. Clarify what you mean by an opinion.

Q. Just a personal opinion. Do you have any feelings about Intellectual Ventures?

A. They -- they own a lot of patents and they litigate, so that's -- that's all I know, but I --

Q. Okay. I'm going to give you a copy of Exhibit 1001.

A. Thanks.

Q. Thank you.

(Thereupon, Exhibit Number 1001, previously marked, was identified.)

MS. SMITH: Here's a copy for you.

THE WITNESS: Do you want to put a

c4ea61a5-485d-4192-937b-dc6133d2c9f4

sticker on this?

BY MS. SMITH:

Q. No, actually, they're all premarked in this one, so we get off easy today.

A. Okay.

Q. So this is a copy of the Declaration you submitted in this IPR proceeding?

A. That's correct, yes, I believe.

Q. Okay. And could you turn to the last page?

A. Okay.

Q. All right. Is that your signature?

A. I'm sorry, yes, that's my signature.

Q. Okay. So from time to time I may refer to this document, Exhibit 1001, as your Declaration. I'll try to give you the exhibit number, but sometimes I forget. So just so the record is clear, if I'm using the word Declaration, I'm referring to Exhibit 1001. And I am imprecise, so I may slip up from time to time and call it your report or expert report. And if I do, just to be clear, report refers to the Declaration of Exhibit 1001.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

And who drafted this Declaration?

A. I did.

Q. Okay. Was anybody else involved?

A. Versions of the draft went back and forth between counsel and myself, so counsel was involved.

Q. Did you work with anyone who is not an attorney?

A. I don't think so.

Q. Did you work with anyone associated with IBM?

A. No. Oh, for this -- for this, no.

Q. Can you explain the process of drafting this Declaration?

MR. JACKSON: Objection, privileged.

You can answer the question, just be sure not to reveal any attorney/client --

THE WITNESS: Okay.

MR. JACKSON: -- or work product communication.

THE WITNESS: I believe I was retained about -- in April time frame this year and I was given some instruction as to how to -- you know, generally

c4ea61a5-485d-4192-937b-dc6133d2c9f4

what should go in the report, how it's different from an expert report for a patent trial.

And there was prior art that was made available that was suggested to me and I considered it. Like I said, my memory is not that great, but April, May, but my understanding was that, you know, I drafted some things and it went back and forth with counsel and we converged on a final draft, I believe, sometime late May.

BY MS. SMITH:

Q. And did -- did you prepare the first draft?

A. I prepared a preliminary draft, right.

Q. And did you type -- type the preliminary draft?

A. Oh, yeah.

Q. Okay.

A. I mean, I -- it was a draft in electronic form.

Q. Okay. So can you describe how you were first contacted to work on this project?

A. Well, as I said before, I wasn't

c4ea61a5-485d-4192-937b-dc6133d2c9f4

contacted directly from -- by the banks or their counsel. I was contacted by this fellow Cahn. So I'm assuming that he was retained by counsel to look for experts.

Q. Okay.

A. How he found my name, I have no idea. It may have been through a referral, in fact. Maybe that --that was likely what happened.

Q. And this was around April I think you mentioned?

A. Again, around that. It could have been late March, but I'm not sure.

Q. And what did Mr. Cahn tell you?

MR. JACKSON: Objection, privileged.

You can -- you can reveal the generalities of your relationship with Cahn, but don't go into specific communications.

THE WITNESS: I believe -- I believe that he sent me an E-mail with the patents, the '084 and '694 patents. This normally happens when an overture occurs to an expert because, you know, the -- the question is do I -- can I read these patents and

c4ea61a5-485d-4192-937b-dc6133d2c9f4

understand them.

I don't think the initial overture had any more information than that, other than maybe the parties in suit, but I don't remember exactly. But I believe the patents were -- were sent to me -- before I signed anything, I mean.

Q. Okay. What did you do to prepare for this deposition?

A. Again, it's been some time and it's been a busy year, so I really just began with my -- I'm going to use the worth report too -- so I began with my reading my report and the references cited in it. I shouldn't say began. That's pretty much all I did.

Q. Okay. Did you meet with counsel?

A. Sorry, you're right, I did meet with counsel yesterday.

Q. Okay. Who was present?

A. Jason and the two Marks, C. and K.

Q. Okay. And about how long did you meet?

A. And Geoff was on the phone.

Q. Okay.

A. Met yesterday for about six hours, maybe

c4ea61a5-485d-4192-937b-dc6133d2c9f4

more, maybe a little more.

Q. Did you review any documents besides the -- the Declaration and the -- and the cited references?

A. No.

Q. Did you bring any documents with you today?

A. No, I did not.

Q. Did you discuss your deposition with anyone?

A. The fact that I was going to give a deposition?

Q. Okay.

A. How do you mean?

Q. Anything. In any way.

A. I think people know I was in D.C. to give a deposition. Several of my friends know I was in D.C. to give a deposition.

Q. Did you discuss the substance of your testimony with anybody --

A. No.

Q. -- besides counsel?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

MS. SMITH: Okay. All right. So if you can just pass this to him.

THE WITNESS: That's a better idea.

MS. SMITH: Yeah.

MR. JACKSON: Thank you.

MS. SMITH: You're welcome.

THE WITNESS: My CV.

BY MS. SMITH:

Q. So this is your CV.

A. Okay.

Q. And I'm assuming you've seen this document before today?

A. Sure.

Q. Okay. So your CV identifies some consulting work relating to various litigations.

A. Um-hmm (affirmative).

Q. Right? Okay. Can you describe who you represented and the outcome of those engagements?

A. All right. Let me just turn to the section.

Q. I think they start around page 13.

A. Right, under the banner grants and

c4ea61a5-485d-4192-937b-dc6133d2c9f4

contracts.

Q. Yep.

A. I'm sorry, I'm just going to have to go through. So I represented -- I'm not sure represented is the right word -- I was the expert for the defense for a case involving a company called Spodify. That case settled in September. It involved work in the same time frame of the work for this case, so spring/summer time frame.

There are actually two cases with another law firm, both settled. So I -- I don't have it listed here. I didn't really do much work on the other case at all.

The litigation with -- so involving AT&T, AT&T -- I -- I worked for -- that wasn't a patent case. That was litigation involving AT&T's business practices and there were suits involving states, I believe California and Illinois.

I was deposed in that case. I only testified at trial in one case, just in case I forget to say that and you wanted to know.

In 2011 I worked for a company called F5

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Networks. The law firm is listed there.

Q. Okay.

A. I was an expert for F5 I should say.

Q. I'm sorry, I interrupted. Were they the plaintiff or defendant?

A. That's a good question. There was a countersuit, so I'm thinking initially it was defendant and then when they countersued I was also expert as a --

Q. Okay.

A. Just a minute. Let me try to remember. Initially F5 was the defendant and then they countersued on a set of patents that they held. The -- the other side was A10, a company called A10, which also does sort of load -- networking and load balancing.

For the Spodify case I didn't mention the plaintiff was, I believe, Nonend.

The next page, so in 2007, 2008 I was expert for Extreme Networks, a company that makes internet switches.

Q. Would they be a plaintiff or defendant?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. They were defendant and I forget the name of the plaintiff. It was an old DEC patent, but I forget the name of the plaintiff.

In the -- 2005, 2008 I was an expert for SRI. The defendants in those cases -- sorry, that was the plaintiff in that case and the defendants were ISS, which was -- by the time the trial came along, it was, I believe, purchased by -- by IBM, so maybe IBM was the defendant. And the other defendant was Symantec.

Am I giving you enough information or is it -- so I'm just walking through --

Q. Yeah. Yeah, perfect.

A. -- so in '04, '05 I worked for -- I was expert for Riverstone and I believe the -- the -- the plaintiff was some -- was a Japanese company. It may have been Toshiba, but I'm not 100 percent sure. And it was for something called MPLS technology, kind of a network protocol.

Q. Okay. So Riverstone was the defendant?

A. Riverstone was the defendant, right.

Do you want me to just discuss litigation

c4ea61a5-485d-4192-937b-dc6133d2c9f4

consulting activity or any consulting activity or --

Q. Just -- well, starting with litigation for right now.

A. I think that's -- I -- I may have written a report in a patent case when I was working in Canada. I think I did that once, but I -- I've forgotten. Yeah, I've forgotten.

Q. Okay.

A. Yeah. No, sorry, there is one in '98 where I wrote a -- I wrote -- I wrote a report. I don't even believe I was deposed in that case. I'm not sure what happened with it.

Q. Okay. And do you -- do you know if -- so this is the Newbridge one --

A. Yeah, '98.

Q. -- is that correct?

All right. And so were they the plaintiff or defendant?

A. They were defendant.

Q. Defendant, okay.

A. But I -- I just don't remember the -- I don't remember much about the case and I for sure

c4ea61a5-485d-4192-937b-dc6133d2c9f4

wasn't deposed at that point.

Q. So at the beginning you had mentioned -- I think it was just after you had discussed Spodify -- that there was another case where you were retained as an expert and you mentioned that it wasn't listed here.

Are -- are you allowed to disclose whom you represented?

A. That was also Spodify.

Q. Oh, it was also Spodify.

A. There were two Spodify cases.

Q. Oh, okay.

A. One involved -- I mean, probably spent 98 percent of the time on the first case and I was kind of being held in -- in position for the second one, but then they both settled out, so I did very minimal work on the second case --

Q. Okay.

A. -- which is why it's not listed there.

Q. Okay. So are there any expert witness engagements that are not on your CV besides that one Spodify one that you mentioned?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. No.

Q. Okay. And have you ever done -- besides this proceeding, have you ever done consulting work related to administrative proceedings, such as IPRs or covered business method --

A. No.

Q. -- proceedings?

A. Not before this --

Q. Before this.

A. -- IPR, no.

Q. Okay. So you've testified under oath before. I think we established that. So you mentioned once you've -- you've testified in court?

A. That's right.

Q. Okay. And which -- which engagement was that?

A. That was the SRI case.

Q. That was SRI. And in which of these proceedings were you deposed?

A. All of them, except the first one I mentioned, the one in '98.

Q. Okay.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. And the one I -- the one I neglected to clarify. There were two Spodify cases. So the other one there was no report written, so there was nothing to be deposed about.

Q. Okay. Any hearings that you might have been -- testified under oath in a hearing?

A. No, I don't think so.

Q. Okay. So I'm going to give you a copy of a new exhibit. This one has been marked as Exhibit 2007.

MS. SMITH: This is the service copy for you.

MR. JACKSON: Thank you.

(Thereupon, Exhibit Number 2007, previous marked, was identified.)

BY MS. SMITH:

Q. Okay. Have you seen this paper before today?

A. Yeah. I guess, yes.

Q. Okay.

A. I have no memory of it though.

Q. Okay. So you understand that Symantec

c4ea61a5-485d-4192-937b-dc6133d2c9f4

and ISS moved the District Court to limit your testimony under Federal Rule of Evidence 702 in the --

MR. JACKSON: Objection --

MS. SMITH: -- SRI case?

MR. JACKSON: -- foundation.

THE WITNESS: I have no memory of this, so I -- I guess I -- can I sit and read it?

BY MS. SMITH:

Q. Sure, of course.

A. Okay. I'm -- I'm beginning to remember this. I'm not familiar with Rule 702, but I remember the issue.

Q. Okay. So what do you remember about this issue?

A. This case had to do with -- with patents that were issued around 1998. At the time in 1998 I was not working in the area of security.

Q. Do you know the outcome of this motion?

A. I believe it was denied, yeah, but I -- you know, I'm not sure.

Q. Do you know of any other instances where a party has moved to limit or exclude your testimony

c4ea61a5-485d-4192-937b-dc6133d2c9f4

before a district court?

MR. JACKSON: Objection, foundation, relevance.

THE WITNESS: I -- I don't. I had forgotten about this motion, so.

BY MS. SMITH:

Q. Okay. So I would like to refer again to your Declaration.

A. Okay.

Q. Okay? This is Exhibit 1001.

Do you consider yourself an expert on firewalls?

A. Yes.

MR. JACKSON: Objection, form.

THE WITNESS: I'm sorry.

To the extent that I'm serving in this capacity, yes.

BY MS. SMITH:

Q. Is there an extent that you don't consider yourself an expert on firewalls?

A. I don't really practice. I don't run firewalls and practice them, although I've taken a

c4ea61a5-485d-4192-937b-dc6133d2c9f4

course on how to configure a pix firewall with Cisco ten years ago, so I have some experience with the software, but typically I interact with students and people in industry that do this kind of work. Of course I read a lot of papers on the subject matter.

Q. So I want to turn to paragraph 31.

A. Sorry, where? In which?

Q. Paragraph 31. It's on page 15.

A. Of -- of which document?

Q. Exhibit 1001. We're still on 1001.

A. Oh, okay. I'm sorry, 1001 is my report?

Q. Yes, that's right.

A. Okay. Paragraph 31?

Q. Um-hmm (affirmative).

Okay. So in paragraph 31 you gave your opinion on the qualifications of a person having ordinary skill in the art, correct?

A. Yes.

Q. Okay. How did you arrive at this definition?

A. Well, I -- I considered the -- the patents-in-suit, maybe that's not the way to describe

c4ea61a5-485d-4192-937b-dc6133d2c9f4

them, the patents, '694 and '084 patents, particularly the '694 patent here, and the prior art that was cited and I asked myself one of ordinary skill what's -- what is their required background to be able to read and understand these references.

Q. Okay. When did you first start working on firewalls?

A. Let's see, I -- around 2000, 2001 time frame I began working in security by sort of immersing myself in the literature. And I got my first NSF grant in the security area around 2003, my first Ph.D. student working in security around that same time. So prior to 2000 -- prior to coming to the U.S. I -- I wasn't really working in security. I was familiar with some of the concepts and -- but not -- not really working in the area.

Q. So I want to take us back to October 1998.

A. Okay.

Q. And in October 1998 would you have considered yourself an expert in firewalls?

A. No, I -- I don't think in October '98 I

c4ea61a5-485d-4192-937b-dc6133d2c9f4

was, I mean, apart from, you know, a super -- superficial understanding of their -- of their -- their functions; but certainly in October '98 I could -- I could read and understand these references.

Q. In October 1998 would you have considered yourself a person of ordinary skill in the art under your definition of -- in paragraph 31?

A. Yes.

Q. Okay. Why is that?

A. Sorry. Essentially I had been working in networking since 1990 before the web. And by '98 I -- you know -- I had my bachelor's degree in electrical engineering and graduate degrees in electrical engineering and computer science in 1990/1992.

Q. Okay. Did you have one or two years of work experience in firewalls in October '98?

A. I did not.

Q. So --

A. I'm sorry, is that my phone or is that somewhere else?

Q. I think it's outside.

A. It's outside, sorry.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. In -- so now going to one year later, October 1999 --

A. Okay.

Q. -- okay, would you have considered yourself an expert in firewalls in October 1999?

MR. JACKSON: Object to form.

THE WITNESS: Like I said earlier, I -- I didn't really start reading security literature in about 2000.

BY MS. SMITH:

Q. Okay.

A. In retrospect, if I were to begin reading references on firewalling I -- I think I would have as easily digested them in '98, '99 as I did beginning in 2000.

Q. Okay. Did you use a firewall before October 1998?

A. Sorry, can you clarify use?

Q. In any way. There's no -- there is a very broad question.

Did you ever use a firewall before October '98?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. If I --

MR. JACKSON: Object to form.

THE WITNESS: I'm sorry.

If I'm -- if I'm typing away on a workstation and that workstation is protected by a firewall, does that mean -- does that satisfy that condition?

BY MS. SMITH:

Q. It -- it could be.

A. Well, in that case yes.

Q. Okay. And did you ever configure a firewall before October '98?

A. I did not.

Q. Okay. October '99?

A. I did not.

Q. Okay. Have you ever been involved in implementing a -- a firewall?

MR. JACKSON: Object to form.

THE WITNESS: About ten years ago I participated in a -- sort of a short course offered by Cisco on how to configure their PIX firewall. So in that sort of laboratory setting I -- I did mess around

c4ea61a5-485d-4192-937b-dc6133d2c9f4

with the -- the PIX firewall, but beyond that, no.

BY MS. SMITH:

Q. Were you working in the field of security before 2000?

MR. JACKSON: Object to form.

THE WITNESS: I believe I already answered that. I -- I didn't really start working in security, specifically in security, until about 2000.

BY MS. SMITH:

Q. Okay. And I'm not positive that I asked this question. When did you first begin working in the field of firewalls?

A. Well, firewalls are a place where certain ideas in security could be implemented. So as soon as I started working on my grant, my first grant in security, and with my first grad student, some of the ideas could have been implemented in firewalls. So you could say as of around 2002, 2003, specifically producing ideas that could be deployed in a firewall.

Q. When did you first publish in the field of security?

A. Pardon me, let me just peruse my

c4ea61a5-485d-4192-937b-dc6133d2c9f4

conference publications real quick.

Q. Sure.

A. It's likely paper number 88 under my conference list I might identify as my first security-related publication.

Q. Okay.

A. The first topic I worked on was traceback, so -- and -- and the first -- the first student in security that I mentioned is -- is -- the last name is Hamadeh, so 86 -- the paper is 86 and 88.

Q. Okay. And when did you first publish in the field of firewalls?

A. Like I said, it's sort of a peculiar question because, you know, some of these ideas in traceback could be implemented in a firewall, so -- but did we advocate for an implementation in a firewall in those papers? Likely not.

So I'm -- I'm not sure that I specifically advocated for an implementation of -- of any of the things that I published in security specifically at a firewall. You know, the -- I mean, there were papers on network security, so an intrusion

c4ea61a5-485d-4192-937b-dc6133d2c9f4

detection system might involve a firewall, like publication 61, but -- yeah, but that specifically advocate in this paper for implementation in a firewall, likely not.

Q. Okay. And I would -- I just wanted to return to Exhibit 2007.

A. Okay.

Q. Page 8 of 20 -- it's marked at the bottom.

A. Oh, I see.

Q. Okay. And I'm looking at the first sentence of the second paragraph there, and it says Dr. Kesidis, however, has admitted he was neither an expert nor a person of ordinary skill in the art in the field of cyber security or intrusion detection prior to November 1998.

Do you see that?

A. Yes.

Q. Did you, in fact, testify that you were neither an expert nor a person of ordinary skill in the art in the field of cyber security or intrusion detection prior to '98?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

MR. JACKSON: Objection, relevance, hearsay, foundation.

THE WITNESS: I -- I really have no memory of the circumstances. By the definition of ordinary skill in this -- in -- for this case that I agreed to, which is different, and I believe it's different because of the -- again, counsel advised me one of ordinary skill -- you know -- one of the tests is that they have to be able to read and understand references that were in play for this case at that time. And I believe the definition of ordinary skill was informed by that.

And that's why -- I'm not sure where the definition of ordinary skill is in this document, if it's recited, the one I agreed to, but if -- if that was the case and -- and that definition of ordinary skill for this -- in this context involved experience with -- with security, then I had already said that I had no experience with security prior to 2000.

BY MS. SMITH:

Q. Okay.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. Again, I -- it's in the context of the case.

Q. Okay. All right. All right. I'm going to next give you a copy of Exhibit 1004.

(Thereupon, Exhibit Number 1004, previously marked, was identified.)

THE WITNESS: Can we just pause a minute to let this go by?

BY MS. SMITH:

Q. Sure. That's a good idea.

A. Is this the President going by? Is that -- it just seems like about 100 cars out there.

MR. JACKSON: There are fire engines as well, so it's likely not the President.

BY MS. SMITH:

Q. All right. All right. That's better.

A. That's better.

Q. Thank goodness.

All right. So you've seen this document before today?

A. Of course, yes.

Q. I should hope so. Okay.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

When was the last time you reviewed it?

A. Yesterday.

Q. Okay, great. So I may periodically refer to this document as the '694 patent --

A. Very good. Very good.

Q. -- okay?

All right. I'll try to give you the exhibit number, but I usually forget to do that so you'll understand what I mean --

A. Okay.

Q. -- when I say the '694 patent.

When did you first become aware of this patent?

A. Like I said earlier, it was likely in the E-mail sent by the expert witness recruiter, March/April time frame of this year. I can't be sure of that, because just what customarily what these recruiters do is that they just -- they send you the -- the patents in question.

Q. Okay. Did you ever hear of any of the inventors on this patent?

A. No. No, I don't know them.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. So you had mentioned before when we were talking about your consulting arrangements, you had mentioned some work for AT&T.

What was -- what was the work that you did for AT&T?

A. So for AT&T the -- AT&T -- just a minute here. I'm not sure -- I'll try not to say anything I shouldn't. But the cases in question had to do with their IPTV business.

Q. Okay.

A. So AT&T provides IPTV services, essentially broadcast television, over internet. Actually, everyone does these days. In addition, they -- in so doing, they also provide for delivery of what's called PEG, Public Education and Government channels. These are your -- your local channels. I'm not sure what it is in D.C. but anyway, think high school football games.

And the way they -- that AT&T was delivering the PEG channels was a little bit different than the way PEG channels were delivered in legacy broadcast television format. And so the states were

c4ea61a5-485d-4192-937b-dc6133d2c9f4

concerned about this and that's what the litigation was about. It was basically IPTV technology.

Q. Okay. And you were providing consulting services on behalf of AT&T?

A. Right. Mayer Brown was AT&T's counsel in this so-called PEG litigation.

Q. Okay. Have you ever performed any infringement analysis of the '694 patent?

MR. JACKSON: Objection, scope.

THE WITNESS: No.

BY MS. SMITH:

Q. And did you ever see any documents relating to potential infringement of the '694 patent?

A. No.

MR. JACKSON: Objection, scope.

THE WITNESS: I'm sorry. Sorry about that.

No, I have not.

BY MS. SMITH:

Q. Okay. Are you aware of any commercial products at all incorporating or embodying the subject matter of claim one of the '694 patent?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

MR. JACKSON: Objection, form, scope.

THE WITNESS: I believe that nowadays current -- currently firewalls perform what's called stateful inspection of packets. What -- one of the references I cite I call dynamic firewalls, but -- that include consideration of payload information. So.

I think most firewalls, commercial firewalls, have some ability to examine payloads and -- and consider stateful signatures. I can't really recite modern firewalls because I haven't looked at prospectuses and, you know, the firewall that I cite, the only product I cite as a product is -- is the Norman firewall in my report.

Q. Okay. I am going to give you a copy of Exhibit 1009.

(Thereupon, Exhibit Number 1009, previously marked, was identified.)

BY MS. SMITH:

Q. Okay. You've seen this document before today, correct?

A. Yes.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Okay. When was the last time you reviewed it?

A. Yesterday.

Q. When did you first become aware of this publication?

A. I believe April/May time frame of this year.

Q. Okay.

A. I may have read it long before that, but I have no memory.

Q. Did you ever hear of any of the authors?

A. I know -- I know of Avi Rubin. I may have met him once, but I know of him. I've also heard of the other two authors before, but I -- I don't know them as --

Q. Okay.

A. Yeah.

Q. So you -- you've heard of them, but you don't personally know them?

A. No, I don't personally know them.

Q. Okay.

A. I mean, I -- I met -- I met Avi Rubin.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

So I shouldn't say I just heard of him, but, you know --

Q. Oh, okay. When did you meet him?

A. I -- I couldn't tell you really the first time, but I attend principal investigator meetings for the NSF SaTC program. So these are like biannual meetings that have been going on for some time, so the community kind of meets each other. And then I haven't been on a panel -- I don't believe I've been on a -- a panel with him before, but -- in fact, I'm pretty sure I haven't, but I may have been on a panel with him too.

Q. Have you ever spoken to him before?

A. I don't think I've had a meaningful conversation. I mean, it may have been just shake hands and say hello, but that's pretty much it. Yeah, I don't think I've had a meaningful conversation with him before, but I may have met him at a panel at one of these PI meetings. It's hard not to meet people at these PI meetings.

Q. When was the last time you saw him?

A. I couldn't tell you. Likely met him two

c4ea61a5-485d-4192-937b-dc6133d2c9f4

years ago at the -- the last PI meeting. There's another one in January, but the last one I think was in 2012.

Q. Okay. So more than a year ago?

A. Oh, yeah. Yeah.

Q. Okay.

A. And, again, if I had met him then, it wouldn't -- it wasn't a substantive exchange. I have no direct memory of anything.

Q. Okay. All right. And now I'm going to give you a copy of Exhibit 1011.

(Thereupon, Exhibit Number 1011, previously marked, was identified.)

THE WITNESS: Do you mind referring to Rubin as Rubin? I've already forgotten all the numbers.

BY MS. SMITH:

Q. Sure. Absolutely. This one is -- well, we'll refer to this one as Cunningham.

A. Very good. Thank you.

Q. And you've seen this document today?

A. Just now. Before you mean.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Yeah, before today.

A. Right.

Q. Okay. And when was the last time you reviewed it?

A. Yesterday.

Q. Yesterday, okay. When did you first become aware of this patent?

A. Again, it's around the same time, April/May time frame.

Q. Did you ever hear of any of the inventors?

A. No.

Q. Great. All right. And here is a copy of Exhibit 1010. I guess we'll refer to this one as Norman.

(Thereupon, Exhibit Number 1010, previously marked, was identified.)

BY MS. SMITH:

Q. And have you seen this document before today?

A. Yes.

Q. Okay. When was the last time you

c4ea61a5-485d-4192-937b-dc6133d2c9f4

reviewed it?

A. Yesterday.

Q. Okay. And when did you first become aware of it?

A. Around April/May --

Q. Okay.

A. -- time frame.

Q. Had you ever heard of the Norman company before?

A. Not -- no.

Q. Okay.

A. It's -- let me just -- I'll just back that up. In the previous SRI case I considered a lot of prior art before 1998 and the Norman firewall may have been among the prior art that was in play. I don't think it was, but I may have been -- I may have seen something from this company --

Q. Okay.

A. -- in a previous case, but I -- I don't have any memory of it.

Q. So do you know any individuals involved in writing this paper?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. I do not.

Q. Okay.

A. I -- wait, let me back up. The authors are not mentioned, so I don't know that I don't know.

Q. Okay.

A. I may know them. I may not. I don't -- I can't say. I can't answer that question.

Q. All right. Okay. I'm going to refer again to your report or Declaration, Exhibit 1001.

A. Okay.

Q. Okay. So on pages three and four, it's paragraph seven, you refer to a couple of other references that I'm going to just call Abraham, I think that's Exhibit 1008; RFC 791, Exhibit 1006 and RFC 1122, Exhibit 1007.

A. Yes.

Q. Okay. So I guess we'll take them one by one.

Were -- were you aware of any of those references before April/May of this year?

A. Certainly the RFCs.

Q. Okay.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. I've been aware of those RFCs for a very long time, in fact. Anyone working in networking would have encountered them. Abraham, no.

Q. Okay. When did you first become aware of the RFCs? Ballpark is okay.

A. I don't -- early '90s.

Q. Early '90s, okay.

A. I believe they're both -- sorry, where -- where are the RFCs mentioned?

Q. I think they're the last two.

A. Oh, I see, on page four?

Q. Yeah.

A. Yeah, I -- I guess early '90s, maybe even late '80s.

Q. Okay.

A. It -- let me just clarify that last answer. If -- if -- not -- certainly I looked at the RFCs, if not -- a lot of -- particularly the first one, it's cited extensively in textbooks.

Q. All right.

A. So whether I looked at it directly or -- or read captions of it from textbooks, but I -- I

c4ea61a5-485d-4192-937b-dc6133d2c9f4

believe one of the first things I did was look at the original source of some of these things when I started working in networking around 1990.

Q. Okay. So we're going to start a new line of questions, so I think it might be a good time for our first break.

THE WITNESS: Okay.

MR. JACKSON: Sounds good.

VIDEO OPERATOR: This marks the end of tape one in today's videotaped deposition of Dr. George Kesidis.

Going off the record, the time is 10:12 a.m.

(Thereupon, a brief recess was taken.)

VIDEO OPERATOR: This marks the beginning of tape two in today's videotaped deposition of Dr. George Kesidis.

Going back on the record, the time is 10:29 a.m.

BY MS. SMITH:

Q. Okay. Welcome back.

A. Thanks.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Did you discuss the deposition at all during the break?

A. No.

Q. Okay. So I am going to be referring now to your report and to Rubin. So that's exhibits 1001 and 1009.

A. I got it.

Q. Okay. And I'd also -- if you want to refer to it, you might want to have the patent out. So that's Exhibit 1004.

A. Okay. Got it.

Q. Okay. Great.

So the preamble of claim one of the patent recites a packet.

Where in your Declaration did you identify the element of Rubin corresponding with the packet of claim one?

A. So if you look at the chart for Rubin in combination with Abraham on page 27, there's a caption from -- a quote from Rubin that uses the word packet. I'm sorry, let me flip over to the chart, applying Rubin with an anticipation argument and it furthermore

c4ea61a5-485d-4192-937b-dc6133d2c9f4

refers to terms such as TCP and UDP and IP packet, the preamble. This is on page 32. And other quotes in 33 that refer to IP, TCP, et cetera.

Q. Anything else?

A. I'm referring directly to the charts. I -- I -- I -- what -- I'm quoting from Rubin, but Rubin is suffuse with -- the context of Rubin is -- is -- is internet operations and firewall, internet operations and so they're referring to IP packets, TCP/IP packets.

Q. My question was, was there anything else in your Declaration, any other paragraphs, that would identify the element of Rubin corresponding with the packet in claim one?

A. Oh, elsewhere in the Declaration?

Q. Yeah.

A. I'm sorry, I do have textual descriptions outside of the claim charts where I refer to Rubin. So, for example, in paragraph 41 I'm quoting Rubin and the expression packet filters. Packet is -- is mentioned there, paragraph 41. That's in the context of -- of a combination argument. Obviousness by

c4ea61a5-485d-4192-937b-dc6133d2c9f4

combination argument with Abraham.

Also in paragraph 42, again, the word packet is used in a quote from Rubin. It -- it's kind of hard not to quote a paragraph or two from Rubin and not get the word packet in there somewhere.

Q. Anything else?

A. Again, even when it's not explicitly -- the word packet is not explicitly mentioned, it's implicitly there. For example, the quote in paragraph 44, a Java applet might be in transit. The firewall could unpack the archive as it arrives. What is it unpacking? It's unpacking packets. The packets are being unpacked, or -- or decapsulated is another word.

Q. Anything else in your Declaration that identifies the element of Rubin corresponding with packet in claim one?

A. Like I said, I -- I think pretty much any reference to Rubin explicitly or implicitly involves packets. So -- in the -- the other claim elements, the quotations from Rubin, for example, on page 23 the Java class file is either explicitly or implicitly being borne in the payloads of IP packets, on page 23,

c4ea61a5-485d-4192-937b-dc6133d2c9f4

paragraph 51.

Like I said, I think pretty much every quote that I've taken from -- from Rubin either, again, explicitly or implicitly involves TCP/IP packets and IP packet.

Q. So I just want to make sure I -- I understand your testimony.

We had talked about the claim charts on page 27, 32, 33, paragraphs 41, 42, 44 and 51.

Are there any other paragraphs?

A. Well, I did say pretty much every -- every other quote from -- I mean, you can look at all the claim charts, that -- the entire claim chart for -- involving Rubin. So, for example, 27 where Rubin is used the word packet is either explicitly or implicitly in play. Sorry. Let me look at the -- the claim charts for -- for Rubin as a --

Q. Okay.

A. -- as an anticipation argument. So if you look at page 32 I've already said. Page 33, packet filtering firewall in the first quote from page two. Again, packet filter is mentioned in the second

c4ea61a5-485d-4192-937b-dc6133d2c9f4

quote from -- from pages two and three.

Packet filters again mentioned in the quote from page nine. IP packets are mentioned again in the quote from page 10.

Continuing on page 34, the quote, the -- the -- some of the quotes from the preamble are repeated in the -- in the individual -- in the claim elements. Again, IP packet in the quote from page two, on page three, four and all the other quotes. Again, if the word packet is not explicitly mentioned in one of these quotes, it's certainly implicitly there. Going on to page 35 to -- to -- to 38.

Q. Okay. So anything else other than what you identified there?

A. In my report the -- the direct quotes and the discussion, the verbal discussion of the paragraphs before the charts, that -- that's pretty much it, yeah.

Q. Okay. All right. We're done with packet.

And claim one also recites in element A at least one header parameter.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Where in your Declaration did you identify the element of Rubin corresponding with the at least one header parameter of claim one?

A. I would say everywhere Rubin refers to the word packet, Rubin is talking about internet firewalls. So it's referring to a TCP/IP packet, certainly an IP packet. And IP packets have several header parameters. I think a -- a header without a parameter is not a header.

Q. So my question was where in your Declaration did you identify the element of Rubin corresponding with the at least one header parameter, so paragraph and page number.

A. So if I look at element A for Rubin as an anticipation argument on page 34, it's referring to IP packets. IP packets possess header parameters. TCP headers, UDP headers, they possess parameters. Specifically in the second paragraph on page two, cited on my page 34 and page two of Rubin, it's referring to the source IP, IP destination and other fields. The fields are synonymous with parameters. Oh, that's great. Thank you.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Okay. Anywhere else in your Declaration you identify the element of Rubin corresponding with the at least one header parameter in claim one?

A. I'm not sure if I cite that paragraph, let's see, Rubin in combination with Abraham. I'm not sure I use Rubin for element A in combination of Abraham, so I don't, but I expect that -- sorry, let me just press on here. I -- I'm not sure if I discuss it in text, in a textual paragraph outside of the claim charts. That -- I think maybe in the motivation to combine Abraham and Rubin I also mentioned that both of them are talking about network packets, internet packets.

Q. Anything else?

A. I guess that's it.

Q. Okay. So claim one also in the context of limitation A recites receiving.

Where in your Declaration did you identify the element of Rubin corresponding with the receiving of claim one?

A. Well, firewalls inherently receive packets. They really couldn't even begin to function

c4ea61a5-485d-4192-937b-dc6133d2c9f4

unless they -- they receive packets. Rubin -- so in my chart on page 27 in the preamble, in combination with Abraham, Rubin discloses packet filtering. In order to filter any -- a packet, you need to receive it.

Again, the same set of charts -- sorry, not in the same set of charts. Let me press on and go to the Rubin anticipation argument. So you see a packet filtering -- I'm quoting from page two of Rubin on page 34 of my report.

Q. Okay.

A. Packet filtering firewall examines each packet. In order to examine a packet, you have to receive it. I think that's -- that's pretty much the connection. That's the evidence I'm using there.

Q. Okay. Where in your Declaration -- oh, sorry. Limitation B -- sorry, I'll start over.

Limitation B of claim one recites an access rule. Where in your Declaration did you identify the element of Rubin corresponding to the access rule of claim one?

A. So I'm going to focus on the charts,

c4ea61a5-485d-4192-937b-dc6133d2c9f4

because I -- I may have also mentioned in the text, using the charts for support, quotes. So I'm -- I'm looking now at pages 34 and 35 under element B of my report -- I'm sorry, can you say -- can you ask the question again?

Q. Sure. Where in your Declaration did you identify the element of Rubin corresponding to the access rule of claim one?

A. So if we look at -- okay, so if -- if we look at the -- the paragraph from Section 5.1 of Rubin, this describes an operation wherein a Java applet is detected and it is removed. The response is to remove the applet from the HTML file and then pass on the remainder of the HTML file.

So in that the -- the -- from that you -- the reader understands that the -- the -- the contents of multiple packet payloads were examined and a determination was made that an applet was resident in the HTML file.

And because of that test was satisfied, the reaction -- the response was to filter out the offending content, in this case the Java applet

c4ea61a5-485d-4192-937b-dc6133d2c9f4

itself -- to remove it, I should say. I shouldn't say filter. I should say remove it. So that's an example of an access rule. Access in that case is denied for that portion of the HTML payload, of the HTML file I should say.

In Section 5.3 it's simpler. The simple access rule is that if the -- if the signature of a Java applet CA FE BA BE -- pardon my sexism, it's not my doing -- but, anyway, if that signature is detected, then all the -- the -- the applet itself is blocked or the whole file containing it is blocked. So the access rule in this case is -- involves blocking the -- the Java applet and all the associated packets.

Q. Okay. Just so that I understand, was it your testimony with respect to 5.1 that -- that the act of removing the applet was the access rule?

A. No, the -- the rule is not the act. So the rule prescribes an action. So if a test is satisfied, then an action is prescribed. So I would say the -- it's -- the act of blocking is a part of the rule, but it also involves a test, so -- of the

c4ea61a5-485d-4192-937b-dc6133d2c9f4

object being considered.

And collectively that test, combined with a prescribed action, is what I would call an access rule and what I believe the -- that's what the patent means by it.

Q. So is there an element in Rubin corresponding to the access rule of claim one?

A. I -- I believe there are multiple elements in Rubin and they're quoted in -- in my charts under claim 1-B in page 34 and 35. It's abbreviated for Section 5.1. My quote is abbreviated. But what that Section 5.1 is prescribing is a -- a test for CA FE BA BE. If the test is satisfied, then the pruning out of the Java -- the offending Java applet from the HTML file, so it's almost like a partial block; whereas in 5 -- 5.3 it's suggesting simply block all -- all the packets involved in the session that -- in which the Java applet was transmitted.

So the -- the -- the -- the access rule or control action is -- is the act of blocking or pruning out the -- the Java applet. And implicitly

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the test to determine whether the access rule should be applied is simply checking whether CA FE -- I shouldn't say simply -- just checking whether CA FE BA BE is resident in -- in the file being transferred with other context, with other context that Rubin explains.

So I -- I'm simplifying the test because Rubin is aware that the signature CA FE BA BE may be, for lack of a better expression, accidentally present in non-Java -- non-Java transmissions and so other context may be brought to bear to make sure that this, in fact, is a Java applet.

Just continuing on page 35, the quote at the bottom involves blocking applets. The quote at -- the second to last quote involves blocking applets. So those are actions. And we see the context I was referring to a moment ago that you're -- you might be looking at an HTML file. And if you see CA FE BA BE inside a plain text HTML file, that may tip you off that there's a Java applet embedded.

So that's part of the test -- part of the test that forms part of the rule and then the act

c4ea61a5-485d-4192-937b-dc6133d2c9f4

is -- is, in this case, blocking or -- or partially filtering.

Q. Is the element of Rubin corresponding to the access rule of claim one explicitly or implicitly disclosed?

A. I think it's explicitly disclosed. The signature is explicitly given. It's not a hypothetical. It's an actual signature. And the action is explicitly given.

So it -- to me it has both -- both pieces of an access rule, the test and the -- the action as a consequence of whether the test passes or fails.

Q. Let's see, claim 1-B also recites contents of the payload of the packet.

Where in your Declaration did you identify the element of Rubin corresponding with the contents of the payload of the packet of claim one?

A. Im -- implicitly the signature recited for a Java applet, CA FE BA BE, does not reside in the header. It must reside in the payloads. So it's -- it's -- it's implicitly there.

This is why the -- the payloads are

c4ea61a5-485d-4192-937b-dc6133d2c9f4

collected and the files reconstituted. This is the whole point of -- of Rubin's discussion, is to reconstitute a file from the packet payloads.

So when you say, for example, on page 35, the second to last quote from page nine, unpack the archive as it arrives, you're unpacking it from the payloads of the received packets. When you're referring to a zip file, that file is borne in the payloads of the packets, for example.

You're searching -- in -- in the second quote, you're searching IP packets for that four byte signature. That four byte signature is disclosed to be in the payloads because it's a Java applet. It's not in the header.

Q. Element B of claim one also recites selecting an access rule.

Where in your Declaration did you identify the element of Rubin corresponding with the selecting of claim one?

A. So in -- in talking about packet filtering, so filtered doesn't necessarily involve a single access rule. It could have hundreds or

c4ea61a5-485d-4192-937b-dc6133d2c9f4

thousands, many thousands, of -- of rules. Again, each rule is a test.

If the test is satisfied, then, you know, as -- I should say as a consequence of the test, an action is prescribed. So selecting -- I think one of ordinary skill would understand that selecting here is applying a test to -- to a -- a packet. So you're applying tests to packet -- to packets, deciding on what actions to take based on those tests.

Q. Does -- oh, I'm sorry.

A. The -- the selecting part -- you know, the -- the test could involve context. So certain access rules could be applied to -- need -- need to be applied to only certain types of packets, but you can combine a context with the test itself to create a kind of a meta-test. So I view the selecting as basically the testing step.

Q. Does Rubin disclose hundreds or thousands of tests?

A. I think Rubin discusses prior art in firewalls. So I -- I think in -- in -- in section two Rubin discusses prior arts -- prior art in firewalls

c4ea61a5-485d-4192-937b-dc6133d2c9f4

and he doesn't recite examples of -- of specific tests conducted by -- by packets. Sorry. It doesn't explicitly cite or explain specific tests and how many there are, but it -- it -- it certainly discusses firewalls as of the -- the time of publication and refers to, for example, 16, an early firewall.

I -- I think Rubin's contribution is -- is a new rule, a new rule involving the CA FE BA BE signature of a -- of a Java applet. And there's also the -- the publication by Cheswick and Bellovin '94 that they're citing, which I expect, and citations five and six are, you know, existing publications on firewalls, which probably recite different -- different access rules.

Q. Okay. You might have answered my question, but I'm going to ask it again.

Does Rubin -- does Rubin disclose hundreds or thousands of tests?

A. I -- I don't know. I -- in the background -- explicitly, no, I don't see on section two that it's saying that, you know, the -- the size of or the -- the number of tests that are

c4ea61a5-485d-4192-937b-dc6133d2c9f4

involved in commercial firewalls at the time.

Q. Does Rubin disclose more than one test?

A. Yes, it discloses different tests. So it -- it talks about tests that may involve determining -- first determining if -- if packets are -- if a -- if a -- if a section is bearing a zip file, and then based on that, acting to unpack the zip file and, having done that, scanning the zip file for CA FE BA BE.

However, if the -- the HTML file arrives in plain text, then obviously you don't have to unpack it, so -- unzip -- unzip it, so you would directly assemble the HTML file and -- and check for CA FE BA BE in that case.

So there are different contextual -- sorry, let me just get a specific reference that comes to mind. I'm just looking for the place where they talk about the potential for false positives requiring context. So, again, they do disclose it somewhere -- I just can't see it right now -- where -- so, for example, doing -- on -- on page 35 of my report, the last quote, doing this without killing legitimate

c4ea61a5-485d-4192-937b-dc6133d2c9f4

traffic is not easy. So they are referring to the fact that it's possible by checking for CA FE BA BE that you may mistaken another type of communication that happens to have that signature.

So considering -- considering the contextual issues prior to the checking of CA FE BA BE, they -- they do have a plurality of rules that they disclose.

Q. Okay. Claim one recites -- claim 1-C recites implementing.

Where in your Declaration did you identify the element of Rubin corresponding with the implementing of claim one?

A. So I believe that implementing is the control action after the test. I think -- my interpretation is selecting is the -- as I said -- the test itself -- the tests themselves -- and the control action is the -- is the implementation, what is the response as a result of the tests.

So implementing -- implementing could actually be a super set of activity. I mean, implementing could be both the test and the response.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

The -- so the -- it -- the implementing is the -- is the -- is the blocking, for example, that's recited in -- on page 35 in the quote from page eight or the -- the partial -- the pruning out of Java applets from a transmitted HTML file in the -- in the quote from -- from page seven.

So the -- the fact that you're both testing and acting upon the rule is -- which as recited in those two examples is evidence of implementing.

Q. Let's see, claim 1-C also recites a combination of the contents of the packet received in step A and the contents of at least one other packet.

A. Right.

Q. Where in your Declaration did you identify the element of Rubin corresponding with the recited combination?

A. So the combination revisits element B, selected element B, which my interpretation is that this test needs to -- need -- must consider by element B the payload of the packet received in A and must consider that. That's limitation -- my reading of

c4ea61a5-485d-4192-937b-dc6133d2c9f4

limitation B.

And, in addition, it -- it -- it -- it must depend on the contents of one other packet. Generally speaking, Rubin's big point in going to the proxy is that CA FE BA BE may be split across packet boundaries. So Rubin explicitly recites something that I think was obvious to one of ordinary skill, that if you're looking for a signature in application-level information, the process of fragmenting a file or an application-level message into packet payloads does not respect word boundaries or the -- whatever boundaries are delineated in your signature. So that signature could be spread across multiple payloads. That's Rubin's basic message.

It gets worse if it's also zipped. If it's zipped, it means you have to unzip the -- the message in order to apply your test. So which means you have to gather the -- the packet payloads together, unzip them, then apply the test.

So -- sorry, I'm -- I'm going to go to the chart again under C. So it's referring to a proxy host whose function is to reconstitute the message,

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the application layer message, and that reconstitution inherently involves -- in sort of a multi-packet message is decapsulating the packets and merging them together to reconstitute the message that was being sent.

Again, the idea of signatures that are applied to applets or to HTML files, those are things in payloads, generally in a plurality of payloads. Sorry, let me just quickly get the right quote.

So, again, in -- on page 37 Rubin makes this explicit. For example, blocking CA FE BA BE the simplest scheme requires searching IP packets for that four byte signature; however, those four bytes need not arrive in the same packet and, if split up, the individual packets may arrive out of order. So the point is that if you're testing for that signature, Rubin is saying that signature may require examining multiple packet payloads.

But I reiterate that any application layer signature, such as part of an application -- application layer message, one of ordinary skill in networking understands how messages are segmented or

c4ea61a5-485d-4192-937b-dc6133d2c9f4

fragmented into -- into IP packet payloads. And the concern is that examining those packets on the fly, as a firewall would -- as a firewall may, may not -- you may not get the information you need to apply the test.

Selecting is applying the test to decide what then to do about the -- the message being sent. And the -- the -- the natural thing to do is to consider multiple packet payloads as a consequence.

Q. Okay. So element 1-C of the patent states that the access rule is selected.

Where in your Declaration did you identify the element of Rubin corresponding with the is selected of claim one?

A. Again, to reiterate, my explanation of selected in element B had -- had to do with applying a test to the object in question, which is a packet or plurality of packets in this case.

So the test is being applied -- the test is to search for CA FE BA BE signature. The -- that's the -- the selection rule. So the packets, whose payloads contributed to the reconstituted file

c4ea61a5-485d-4192-937b-dc6133d2c9f4

containing CA FE BA BE, those packets were selected by that test.

Q. Okay. So in paragraph 43 of your Declaration at the top of page 19 you state that, Rubin blocks all inbound files that contain a specific four byte hex signature, CA FE BA BE, that is present in all Java class files, correct?

A. Yes, that's right. That's according to one embodiment of Rubin, I should say, maybe that's not the right word, but 5.3 is what I'm referring to, Section 5.3 of Rubin.

Q. All right. In the next sentence you say, because this signature may span more than one packet payload, Rubin recommends the use of an application proxy to apply the access rule based on the contents of the payloads of multiple packets.

Do you see that?

A. I do.

Q. Okay. In your opinion, is -- the blocking of CA FE BA BE is an access rule that is applied, correct?

A. So, yeah, I -- sorry. The -- the access

c4ea61a5-485d-4192-937b-dc6133d2c9f4

rule is to test for CA FE BA BE. And given that the test is satisfied, perhaps with other elements of the test, other contextual information to reduce false positives, then the act is to block. The -- the action, I should say. The action is to block, right, so.

Q. Okay. And the title of the Rubin article is Blocking Applets at the Firewall, correct?

A. That's correct. That's what I'm reading.

Q. Okay. Is it correct that Rubin's solution for blocking applets at the firewall is to apply a rule to block the CA FE BA BE signature?

A. With other types of contextual information to reduce false positives, yes.

Q. Okay.

A. That's -- that's what they're suggesting.

Q. The rule in -- in Rubin is a pass/drop rule, correct?

A. Not necessarily, no, because -- it's a pass/drop rule with regard to the Java applet. But in Section 5.1 if you're considering the rule as applied to a file, the whole message being communicated from

c4ea61a5-485d-4192-937b-dc6133d2c9f4

server to client, then it's really a pruning. It's like a partial pass. You let the rest of the file through and you just remove the Java applet. So it's blocking of the Java applet or passing.

Q. Okay. So I'm going to now turn to Cunningham, which is Exhibit 1011.

A. Okay.

Q. All right. And I think that your discussion of Cunningham starts at page 51, but, you know, of course I want you to refer to anything in your Declaration --

A. Okay.

Q. -- when we're discussing Cunningham.

So you should know the drill by now. So where in your Declaration did you identify the element of Cunningham corresponding with the packet of claim one?

A. So in -- in claim one, I'm looking at the chart on page 52 of my report, in the first paragraph quoted from the -- Cunningham's abstract, he's referring to data packets. And generally he -- he's referring to a network firewall, an internet firewall,

c4ea61a5-485d-4192-937b-dc6133d2c9f4

which carries data packets.

Q. Okay. And element 1-A refers to at least one header parameter.

Where in your Declaration did you identify the element corresponding with the at least one header parameter?

A. Sorry, 1-A?

Q. Yeah.

A. So you see the figure in my chart of Cunningham with 1-A, we see that there's a little schematic of -- of a -- of a packet and there's an abbreviated header, in this case I believe an Ethernet header because it's six bytes. Destination address, source address and type, those are header parameters. You might -- you might also call the checksum at the end, it's a trailer, but same spirit.

Q. And where in your Declaration did you identify the element of Cunningham corresponding to the payload of claim 1-A, claim element 1-A, sorry?

A. Well, in the same figure there's data, again, page 52 of my report, the figure 3 from Cunningham. The payload in this case would be the

c4ea61a5-485d-4192-937b-dc6133d2c9f4

data with respect to the -- the packet or frame that's being described, in this case an Ethernet frame.

Q. Okay.

A. Also, when you refer to a packet as being a data packet, that expression, because packets can be transmitted with -- with no payloads, they could just be messages borne indicating information in the headers, a data packet, you know, essentially conveys that there's -- there's a payload with data in it.

Q. So claim 1-A, claim element 1-A, sorry, recites receiving.

And where in your Declaration did you identify the element of Cunningham corresponding with the receiving of claim one?

A. Well, if we look at the preamble from the abstract of Cunningham, a method of, and system, for monitoring. So monitoring is -- is receiving. And certainly in order to control something, you have to have intercepted the -- the thing you're trying to control to some extent. Sorry, let me strike that, the last part I said in the case -- in the context of Cunningham.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

But the monitoring part is what I would call -- call evidence of receiving in the -- in the abstract. But, generally speaking, firewalls receive packets. It's -- it's just what firewalls do. It's inherent in what a firewall does. It can't operate otherwise.

In the quote from Cunningham from column three, collecting and assembling data packets, you're collecting data packets, that's receiving and collecting.

Q. So element 1-B of the '694 patent recites an access rule.

Where in your Declaration did you identify the element of Cunningham corresponding to the access rule of claim one?

A. So Cunningham uses the same expression, for example, from column four as I recite on page 53 for element 1-B, access control rules may be applied at the time a connection is established or may depend upon application protocol data following a successful connection. So here they're -- sorry, what was your question, you -- where is the access rule?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Yeah. What --

A. Okay.

Q. Where in the Declaration did you identify the element of Cunningham corresponding to the access rule of claim one?

A. So furthermore, the next quote from Cunningham I -- it refers to a rules base, which is a data base of -- of tests together with prescribed actions that depend on the consequence of the test, the outcome of the test.

Q. And where in your Declaration did you identify the element of Cunningham corresponding with the contents of the payload of the packet of claim one?

A. So in -- in layer -- protocol layering, including the OSI hierarchy, application layers are high and network layers are low. So Ethernet is layer two. Data-link layer is layer two. IP is layer three. TCP is layer four. Application layers are above that.

So when -- when -- again, 53, second paragraph, the reference is to higher level decisions

c4ea61a5-485d-4192-937b-dc6133d2c9f4

can be formed after a connection has been established and the contents -- so higher level means application layer decisions.

Similarly, when it refers to low level information, it's referring to information that's evident only in -- among individual packets, Ethernet frames and -- and IP packets and the like.

MR. JACKSON: George, if you could slow down in some of your --

THE WITNESS: Are you able to -- is my speech slurred?

MS. SMITH: It's fast.

THE WITNESS: Am I okay?

BY MS. SMITH:

Q. Slow down.

A. Okay. I'll slow down.

Okay. So in -- in this case because it's -- it's Ethernet -- I'm continuing at the top of page 54 from the quote from Cunningham for -- for 1-B -- because it's Ethernet, Ethernet is sitting there in layer two and its payloads are going to be IP packets, for example, and -- and sort of TCP/IP

c4ea61a5-485d-4192-937b-dc6133d2c9f4

packets.

So if you want to perform a test on higher-layer information, you need to kind of go into the payload of -- of -- on -- at the IP or TCP level if you want to perform a test, apply an access rule based on -- an access rule corresponding to that layer, you have to look at the payload of the Ethernet frame.

And then the underlined portion that's highlighted in page 54 in my report, layer seven information or application layer information is acquired by assembling the data packets, for example, on E-mail environment, the application layer information that may include -- that may be relevant to application of the rules base may include information within the subject line of an E-mail message. This information is acquired only upon accessing the data fields in the data packet of the E-mail message.

In fact, they're -- you're -- you're going within the payload to the payload of the TCP/IP packet embedded in the Ethernet frame and looking for

c4ea61a5-485d-4192-937b-dc6133d2c9f4

subject -- E-mail subject information that's -- that's included there.

Q. So element 1-B recites selecting.

Where in your Declaration did you identify the element of Cunningham corresponding with the selecting of claim one?

MR. JACKSON: Counsel, you're referring to step B or C selecting? I'm sorry.

MS. SMITH: Yeah, I -- I think it was 1-B. Did I --

MR. JACKSON: I think --

MS. SMITH: Oh, sorry, 1-B, yeah.

THE WITNESS: 1-B.

Again, I -- I feel that the selecting -- my -- my interpretation of the selecting action is applying the test and determining -- sorry, is applying the test portion of -- of an access control rule and -- and then the -- the full implementation of the rule includes the -- the action that's prescribed as -- as a consequence of the outcome of the test.

So on page 53 Cunningham invokes

c4ea61a5-485d-4192-937b-dc6133d2c9f4

access control rules, which, in my opinion, have to have these two pieces to them. So by the rules are applied means that packets are selected according to the tests prescribed in the rules. And the -- the control action that depend on the outcomes of those tests are -- are implemented. And, similarly, application rules bases is mentioned in the second quote.

BY MS. SMITH:

Q. Actually, I have some more questions on Cunningham, but I need to take a quick break. This is going to be real short, like five minutes.

VIDEO OPERATOR: This marks the end of tape two in today's videotaped deposition of Dr. George Kesidis.

Going off the record, the time is 11:29 a.m.

(Thereupon, a brief recess was taken.)

VIDEO OPERATOR: This marks the beginning of tape three in today's videotaped deposition of Dr. George Kesidis.

Going back on the record, the time is

c4ea61a5-485d-4192-937b-dc6133d2c9f4

11:39 a.m.

BY MS. SMITH:

Q. Okay. Thanks for the break everybody.

So when -- when we broke we were talking about, I think, the selecting and implementing steps of claim one.

A. Okay.

Q. And -- and I think I -- I've forgotten your answer. You might have said it and I've forgotten, but where in your Declaration did you identify the element of Cunningham corresponding with the implementing of claim one?

A. So -- so I -- in page 54 under my chart for element C they're -- in the first quote they're talking about applying the access control rules. And then in the second citation from column seven of Cunningham, this enables access management control to -- to base decisions upon information. So the -- the decisions that are being based are the -- are the control actions that are a consequence of the -- the tests being -- being selected -- the packets being selected. And, again, the reference to decisions in

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the third paragraph refer to an implementation.

Q. Okay. And so element 1-C recites a combination of the contents of the packet received in step A and the contents of at least one other packet.

Where in your Declaration did you identify the element of Cunningham corresponding with the recited combination?

A. So in -- in the first -- sorry. So sorry, let me just clarify the answer to your previous question, some additional information from the first paragraph, a connection attempt may be denied, a previously established connection may be broken. Here they're referring to connections, for example, TCP connections. Layer four, TCP is connection oriented, so there are ways of terminating those connections and effectively dropping all the packets associated with them.

So now to answer your question regarding the -- the combination, in the second paragraph the workstation then has the capability of piecing together the fragments of multiple packet signal. So they're talking about combining information from

c4ea61a5-485d-4192-937b-dc6133d2c9f4

multiple packets. Various layer in the -- particularly the application layer. So when they're referring to the application-layer information, that is information necessarily in the payloads; the uppermost application layer.

So higher level decisions -- sorry, the quote from page -- so column eight of Cunningham, I mean, they refer to an E-mail environment and they're referring to a -- a test or a rule based on the subject line of an E-mail message. And that subject line could be very long in general. It could -- it could straddle multiple packet payloads. Certainly the -- the contents of the E-mail message could straddle multiple packet payloads.

In the quote from column 10 they refer to assembled data packets. Until sufficient information is required (sic) regarding the node-to-node transmission, that's sufficient information to apply a prescribed test. And, again, it's -- it has acquired sufficient higher-layer information, reading that I -- I -- I understand that there -- there's a plurality, if you don't have enough right now, you have -- you

c4ea61a5-485d-4192-937b-dc6133d2c9f4

don't have as many payloads as you need, you're getting more payloads coming in to create the sufficient amount of information.

Referring back to your previous question regarding implementing, the top of page 56, the controller may generate a signal that disables the connection, an example of that could be to transmit a TCP reset or TCP FIN command. If you detect that something is offensive about the -- or not desirable -- about the communication, you can terminate the -- the connection that way and -- and effectively drop all the packets associated with the session.

Now, again, I -- the very last paragraph of -- from -- on page 56 from Cunningham that I quote from column 10, they're talking about acquiring sufficient information to apply a test. Implicitly to me that's -- sorry, that -- that quote does not necessarily convey payloads. It could be -- it could be headers. So I just -- I withdraw that comment.

I'm sorry, let me just see the -- the figure. Sorry, yeah. So the -- in -- in the figure

c4ea61a5-485d-4192-937b-dc6133d2c9f4

that it's referring to there's a block called assemble communication specific packets. So the act of assembling to me is -- is piecing together the -- the payloads to reconstitute the higher-level message in order to apply the test sufficiently.

Q. Okay. And element 1-C recites is selected.

So where in your Declaration did you identify the element of Cunningham corresponding with is selected of claim one?

A. So the -- the act -- again, the act of applying the rules, if I kind of work backwards from page 56, once you have sufficient information, enough packets to -- packet payloads -- to apply a specific test, you apply the test and that's -- that's the act of selecting the packets. Then you can decide on the -- the prescribed control action as a consequence.

Q. Okay. I'm going to refer now to the Cunningham reference itself.

A. Okay.

Q. Okay. So first I'm going to refer to figure five. It's on page seven of Exhibit --

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. Okay.

Q. -- 1011. Okay. And now that I've referred to it, I will immediately not refer to it and go to column four. Now I'm on page 11.

A. Okay.

Q. Column four, line 66 to 67.

A. Oh, that's the -- I'm sorry, I'm in the wrong place.

Q. Yeah, so --

A. That was -- that was on the last page that said column four, but column four of the patent, yes.

Q. Yeah, under the brief description of the drawings it says that, this is a view of a graphical user interface, GUI, in accordance with one embodiment of rules configurations.

Correct?

A. Um-hmm (affirmative).

Q. Okay. And now with respect to column eight, lines 25 to 29, it states that the -- the GUI of figure five is used by a system operator to configure the rules base that determines the action of

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the access control modules, 30, 32 and 34 of figure two, correct?

A. That's what I'm reading, yes.

Q. Okay. Perfect. And so would you agree that the rules in Cunningham are configured by a system operator?

MR. JACKSON: Objection, form, calls for speculation, foundation.

THE WITNESS: Well, first of all, I believe this is just an embodiment.

Second of all, it's not -- even this embodiment is not saying that all the rules need to be configured this way. Some of them may be, you know, pre-configured. So I should say not all the rules need to be configured manually. Some of them could be pre-configured.

Did I answer your question?

BY MS. SMITH:

Q. What -- what did you mean by a pre-configured rule?

A. There may be other rules that don't require manual configuration by a system administrator

c4ea61a5-485d-4192-937b-dc6133d2c9f4

that are in operation. There -- there may be signatures of attacks that are context-free. If the signature is there, it's definitely bad, drop it. And that may be something that is sort of a -- you know -- a signature that's just an automatically updated -- an automatic update to your firewall.

Access control rules tend to have some -- be somewhat of the form described in figure five. You have to have as part of the test is -- is an identity and a resource, so -- and some kind of permissions for that resource. And the permissions would be -- could be the control action if the -- if the test is -- is satisfied.

Q. Does Cunningham disclose pre-configured rules?

A. I don't -- I don't know. I -- I -- I think -- so Cunningham refers to -- in its section on background -- refers to firewalls in the art. And firewalls in the art have many rules associated with them. Not all of them would be manually configured because access control policies, specific ones such as those recited in figure five, tend to involve specific

c4ea61a5-485d-4192-937b-dc6133d2c9f4

resources, like the identities of specific individuals or devices. They require some amount of manual configuration. That -- that's all that Cunningham is acknowledging there.

Q. Is there an explicit disclosure in this background arts -- arts section regarding pre-configured rules?

A. Only implicitly through its -- its brief mention of firewalls at the top of column two.

Q. Okay.

A. You know, perhaps -- again, I haven't looked at this reference -- perhaps also some disclosure is given indirectly through his discussion of the patent in column two, line 45. The -- in fact, the example there -- yeah, I mean, I -- I -- I guess not explicitly in the background section. I haven't read the patent with this question in mind, so -- so I'm not sure. Yeah, I'm not sure.

Q. How much time would you need to consider whether Cunningham discloses pre-configured rules?

A. Again, I believe it does because these rules were existent in the -- in the art. Rules such

c4ea61a5-485d-4192-937b-dc6133d2c9f4

as the one recited by -- by Rubin, such as a rule saying block all Java applets inbound to the domain, that doesn't require -- I mean, it -- sorry, let me -- let me amend what I said earlier.

So typically when you -- when an institution receives -- when you receive a firewall, it was my understanding that many of them are delivered so that they block everything. So the user has to activate or someone, system security administrator, has to activate the rules that permit packets through, as well as the rules that block certain types of activity.

So all of that is under the control of the administrator. What I'm -- what I'm trying to say is that the -- the -- the rules illustrated in figure five with reference to column four are -- are not the only types of rules. There could be rules such -- well, I guess -- I guess all types of rules that we're discussing in this deposition could fit into this mode.

So one could disallow anyone from any device at any time downloading a Java applet. So a --

c4ea61a5-485d-4192-937b-dc6133d2c9f4

a security administrator is in control of what gets in and what gets out and is -- is responsible for applying the security policies of the business through implementation of the firewall.

So I -- I just take it back. I -- I think in practice any firewall will be, to some extent, configured manually.

Q. Okay. So you -- I -- I believe you just testified that in addition to the rules shown in figure five, there could be other kinds of rules.

Is that your testimony?

A. They -- I guess they could fit in -- into the framework that's -- that's illustrated in the GUI. A -- a context-free rule, a signature for a virus, under any circumstances you don't want that virus in your -- in your network, that could be implemented as -- well, the signature for the virus is not really stipulated here, right, in this table. That's -- that was why I was raising the issue, that the description of the test itself is not described, is not given here.

So there might be additional information

c4ea61a5-485d-4192-937b-dc6133d2c9f4

not given here for the -- the signature of a virus or CA FE BA BE, for example. Where would -- where would the signature CA FE BA BE be listed here. It would be, perhaps, in the comments. It doesn't really make a lot of sense, but you could have a -- you know -- if it's a virus signature, there could be a wild card for who, where, when under any circumstances and then there would be a description of the -- like a disclosure of the signature itself that's being -- that -- that's forming the test. That's why I responded the way I responded.

Q. Does -- does Cunningham disclose a CA FE BA BE signature?

A. Again, I -- I think it's inherent in -- in its -- your reference to firewalls. So he -- he refers, at the top of column two, to firewalls and access control policies. So firewalls implement access control policies involving identities of individuals and devices and their permissions vis-a-vis resources, including access to external websites and the like.

Q. Are you suggesting that all firewalls

c4ea61a5-485d-4192-937b-dc6133d2c9f4

look at the CA FE BA BE signature?

A. No.

Q. Okay.

A. That particular signature at this time, no; but firewalls at that time may have looked for signatures of virus and other types of -- of attack behavior that had been carefully characterized and deployed on firewalls.

Q. Are you suggesting that all firewalls looked at virus signatures?

MR. JACKSON: Objection, scope, calls for speculation.

THE WITNESS: I -- I don't know that all firewalls looked at virus signatures, but certainly -- certainly fire -- firewalls at the time were not simply -- I shouldn't say simply -- did not only implement access control policies. They also implemented objective signatures to -- to remove packets or groups of packets that were deemed threatening to the -- the domain.

And all I'm just saying is that those signatures are not represented in figure five.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

I -- I think that Cunningham is not looking to contribute an invention toward -- in this discussion of column four, it's -- it's not looking specifically toward other types of firewall signatures. It's really sort of describing what you see here.

BY MS. SMITH:

Q. Okay. I'm referring now to page 56 of your Declaration with reference to figure seven.

A. Okay.

Q. Would you agree that in figure seven the rules are sequentially applied one after another in steps 98 through 104 after sufficient information has been acquired to apply the rule base as determined in step 96?

A. 98 to 104?

Q. Um-hmm (affirmative).

A. Specifically 98, 100, 104 and considering the branch 102.

Q. Right.

A. That -- that's my understanding of the flow chart.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Q. Okay. Would you agree that Cunningham teaches that the rules in a rule set are consulted in a top down order and in Cunningham the system works its way down a list of rules in determining a match?

MR. JACKSON: Objection to form, foundation.

THE WITNESS: I -- I'm not sure what you mean by top down order. The rules are stored in a data base in some order; is that what you're --

BY MS. SMITH:

Q. Well, I'm actually referring to column ten, lines 65 through 67.

A. Okay.

Q. So it says that the rules in a particular set are consulted in a top down order.

A. Sorry, I -- I didn't -- I didn't actually recite that passage, so ten, line 67?

Q. Yeah.

A. I see it.

Q. So do you have an opinion whether Cunningham teaches that the rules in a rule set are consulted in a top down order; in Cunningham the

c4ea61a5-485d-4192-937b-dc6133d2c9f4

system works its way down a list of rules in determining a match?

MR. JACKSON: Objection, form, foundation, calls for speculation.

THE WITNESS: I'm -- I'm just lost at where I am right now. So column ten, line 65 --

BY MS. SMITH:

Q. Through 67.

A. Oh, I see.

Q. Yeah.

A. Step 100 -- I -- I think just reading, as you've -- as you pointed out, it's simply saying the rules are listed -- yeah, they're -- they're listed in some order in the rules data base or the rules base, and whatever that order is, if they are tested sequentially out of that data base, that's -- in this embodiment, that's what I'm reading as well.

Q. Okay. So I'm now going to refer to the combination of Norman and Rubin. I think it starts at page 38 of your Declaration, but --

A. Give me a second. I'm just going to --

Q. Sure.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. -- get out the right references. Okay.

Q. Okay. Okay. So the preamble of claim one recites a packet.

And where in your Declaration did you identify the element of Norman or Rubin corresponding with packet in claim one?

A. So I discussed Rubin's disclosures regarding the limitations of the claim. So is it okay for me to just focus on what Norman is reading?

Q. Sure.

A. So in claim -- sorry, in paragraph 60 I refer to -- in the context of claim 1-A -- that Norman is receiving a packet. You know, and generally speaking, Norman is -- is an internet firewall. The title of it -- reference is to firewalls and internet security. Internet packets are being transmitted inside the internet and firewalls are -- are -- are considering them.

If I refer to the chart, again, at page 44, claim one, the preamble, I make a citation to Norman at page three, most network security devices on the market employ some sort of packet routing and

c4ea61a5-485d-4192-937b-dc6133d2c9f4

filtering.

Moreover, on page 45, packet filtering is referred to from a quote, Norman page three. Internet security products, again, internet inherently involves the transmission of internet packets, IP packets. I again refer to a packet filter in the quote from page four.

Q. And where in your Declaration did you identify the element of Norman or Rubin corresponding with the at least one header parameter of claim one?

A. I've already discussed how Rubin discloses a header parameter. And any IP packet -- I think any -- any communication packet in general has a -- a header of some kind and the header inherently has a parameter.

But certainly internet packets have header parameters. And Norman discloses that it -- it operates in the internet on internet packets, as I've discussed per the preamble.

Moreover, they -- at the bottom of page 45, referring to Norman, a Norman reference from page eight, sorry, Norman quote from page eight, the packet

c4ea61a5-485d-4192-937b-dc6133d2c9f4

header information can be used for filtering. Packets can be filtered by protocol, origin, destination, IP address, port, physical device, et cetera. Those are -- those are parameters or fields in -- in an IP packet header.

Q. So element 1-A recites receiving a packet.

Where in your Declaration did you identify an element of Norman or Rubin corresponding with receiving in claim one?

A. So, again, with Rubin I've already answered the question earlier.

With -- with Norman, let me repeat that I -- I think it's inherent that firewalls receive packets; otherwise, they -- they couldn't do their job.

The quote from page three and four of Norman in the middle of page 45 of my report refers to packet filtering. Again, it's -- it's inherent that that would involve receiving packets in order to be able to filter them.

Again, at the bottom of page 45 it's

c4ea61a5-485d-4192-937b-dc6133d2c9f4

referring to packet header information, which can't be known unless the packets have been received.

Q. Element 1-B of claim one recites an access rule.

Where in your Declaration did you identify the element of Norman or Rubin corresponding to the access rule of claim one?

A. Well, access rules -- so Norman in -- includes virus control. So it -- it refers to some kind of scanning for what it reports. Again, at the time of application I'm not sure what this -- I've forgot exactly what the date of this reference is -- October 1995 -- that if there were over 7000 known viruses and by scanning all incoming files for those viruses it's using either the binary or some -- some other kind of signature.

So in my opinion what that means is that it -- it's testing received packets. It's testing received packets based on the -- the -- these -- these virus signatures. And because we're talking about virus, the virus itself will be borne in the payloads of the packets.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

So the virus would not be in the headers of the packets. So the -- the virus is borne in the payloads of the packets. And so it's -- it's fulfilling the -- the payload limitation as well.

Again, searches all incoming files -- proceeding to page 46 of my report, a quote from pages five and six of Norman -- searches all incoming files. So the act of searching for selected text, the word selected is actually used in there, so the -- the selected text is text that -- like CA FE BA BE -- would indicate something that is of concern to the security administrator.

And the process of searching packets is the -- is the selecting -- you know, when -- when you find packets that match or even if you find those that don't, you're selecting packets and applying tests.

Again, because the word file is used here, it's understood to one of ordinary skill the file is borne inside the payloads of packets. In general, multiple payloads.

Proceeding with the examples from Norman

c4ea61a5-485d-4192-937b-dc6133d2c9f4

on page nine, there are two quote -- two examples, one involves -- repeats the -- the antivirus example that I mentioned earlier. The other involves a -- a hotword module, which is very similar -- actually, very similar -- similar to the CA FE BA BE signature recited in -- in -- in Rubin.

The example given is there -- there are documents that are associated with a secret project called The Alpha Project and those documents may have -- will have the words The Alpha Project, quote/unquote, embedded in them. And, again, the documents are -- you know, one of ordinary skill would understand those documents when they're -- they're being transmitted over the internet and intercepted by a firewall will be borne in the payloads of multiple packets in general.

And so you're -- you're -- you're testing for The Alpha Project to see if that -- if that collection -- if that -- if that title is present in the payload of a packet.

Q. So is there a specific test that's disclosed in Norman that corresponds to the access

c4ea61a5-485d-4192-937b-dc6133d2c9f4

rule of claim one?

A. There is a specific test. They give an example of The Alpha Project. It's an illustrative example, but it's a specific one. Moreover, they also refer to certain file types that involve -- that are compressed versions of -- of -- that, you know, basically could be compressed versions of executables of a virus or text. And so they -- there are specific rules corresponding to unpacking, say, a zip file arriving in the payloads of a plurality of packets and then applying an anti-virus signature -- an anti-virus test to the received contents of the unzipped file. That's at the bottom of the first paragraph of my report, page 47.

They don't -- I don't think Norman in this prospectus recites a specific virus signature among the 7,000 that they -- they claim to have deployed. But the -- The Alpha Project example is an illustrative example, but it's a concrete one, in my opinion.

Q. So is the access rule the text -- the search for the text string Alpha Project?

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. That would be the test portion of the access rule and the -- as a consequence of that test, the prescribed control action would be to -- to block transmission --

Q. Okay.

A. -- of that -- of -- of that set of packets. But just to be clear, it may be permitted -- there may be context there. In other words, the blocking may occur at a gateway to the outside world, but it may be permitted within the -- within the domain.

So the file transmissions may be permitted within the domain, may be blocked, you know, wherever the firewall happens to be located. Certainly at -- at -- what Norman is saying is that the gateway to the outside world you want to put a firewall there that blocks exfiltration of any file that has The Alpha Project in it.

Q. Okay. So an example of an access rule might be if the text Alpha Project exists, then block transmission?

A. If -- if it's detected in the payloads of

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the packets, then block the transmission.

Q. Okay.

A. I think we're jumping the gun into C, but anyway.

Q. Okay. And so element 1-B recites contents of the payload of the packet.

Where in your Declaration did you identify the element of Norman or Rubin corresponding with the contents of the payload of the packet of claim one?

A. I discussed this with Rubin, that CA FE BA BE is necessarily part of a Java applet, which would necessarily be in a -- in a payload. It would be in the header.

Similarly, from the examples that -- if you -- you know -- at the -- sorry -- the top of page 47 from -- from Norman, any virus is borne in the payloads of packets and so anti-virus checkers would -- would look at the payloads of packets as a consequence.

A file that's part of The Alpha Project and has The Alpha Project's name in it or some other

c4ea61a5-485d-4192-937b-dc6133d2c9f4

file that's unrelated to The Alpha Project, those would be borne in the payloads of packets.

And Norman does talk about -- I'm sorry. Sorry, that's -- yeah, that's in -- in addition to what I said about Rubin. Sorry, let me take that -- so Norman -- sorry, a quote from page five/six regarding virus control, Norman scans all incoming files. So files, again, have to do with -- with payloads of packets, searches all incoming files for selected text, et cetera.

Q. Okay. Element 1-B of claim one recites selecting an access rule.

Where in your Declaration did you identify the element of Norman corresponding with the selecting of claim one?

A. Again, I -- I -- I look at Norman, for example, on page 46, the quote from pages five and six, programmable Trojan control and confidential -- the Norman firewall searches, so the act of -- the act of searching -- sorry, let me just repeat that slowly because I know you're exasperated -- so programmable Trojan control and confidentiality assurance, page 46

c4ea61a5-485d-4192-937b-dc6133d2c9f4

of my report and page five to six of Norman, the Norman firewall searches all incoming files.

So to me the -- the act of searching, searching for what. It's searching for text such as -- as an example -- a text such as The Alpha Project. And that act of searching and when -- when it's detected you've selected the packets that -- you've selected the packets that -- for which you're about to apply a -- a -- a control action prescribed by the firewall.

Q. All right. Element 1-C recites implementing the access rule.

Where in your Declaration did you identify the element of Norman corresponding with the implementing of claim one?

A. So I'm interpreting the word implementing to be both applying the test and implementing the -- and -- and the control action. So if we look, for example, on page 48 of my report, quoting Norman at page nine at the bottom of that paragraph, the second paragraph on my report, page 48, when a virus is located the file transaction can be configured to be

c4ea61a5-485d-4192-937b-dc6133d2c9f4

blocked and/or logged. So that's a control action.

So you've selected packets or searched for packets according to a virus signature. You've located packets in this hypothetical, which you believe contain the virus, and you act upon that determination by blocking and/or logging the fact that you detect a virus.

At the bottom of page 48 of my report, quoting again from Norman, page nine, their -- their illustrative example of a hotword, The Alpha Project, when a file is cleared, it is then passed on by the pass -- the proxy process. That's the control action. So that's the complete access control rule implemented.

Q. And element 1-C recites a combination of the contents of the packet received in step A and the contents of at least one other packet.

Where in your Declaration did you identify the element of Norman corresponding with the recited combination?

A. So this is where we decided to use Rubin for support, because Rubin explicitly -- explicitly

c4ea61a5-485d-4192-937b-dc6133d2c9f4

talks about how the signature that they're interested in, CA FE BA BE, can be split across packet payload boundaries.

And to me, as I said before, one of ordinary skill in networking understands that a file, an application layer message, when it's fragmented into packet payloads, any signature that is present in that file can be split across payload boundaries.

So, for example, in Norman the -- the text, The Alpha Project, may land at the boundary because fragmentation doesn't respect word boundaries. It respects -- it respects characters, but not word boundaries, and -- and not even that if it's -- if the -- if the file is compressed.

But if it's plain text, the -- like, for example, the -- the letters T-H-E space A-L may be at the end of one packet payload and the next packet payload can begin with P-H-A space project, period.

And so what I'm reciting is a -- again, we're bringing Rubin in to be explicit about it, but I think that that possibility would be -- would be known to one of ordinary skill. And, as a result, a

c4ea61a5-485d-4192-937b-dc6133d2c9f4

signature like that is being applied to a file rather than to a single payload.

So to me reading Norman, even without the support of Rubin, I can say The Alpha Project, if I'm -- if I'm going to apply a signature like that in practice, I'm going to apply at the file level and inherently a file is, in -- in general, reconstituted out of the payloads of a plurality of packets.

But to bring Rubin in to make it explicit, that's what I already discussed in our -- in -- in my testimony on Rubin.

Q. Okay. Now I'm going to refer to the Norman reference in particular, so that's Exhibit 1010.

A. Okay.

Q. And I'm on page 13, Section 4.5.

A. Oh, okay. There seems to be two different page numbers here, so --

Q. Oh, I'm --

A. There's like a -- an exhibit page number and --

Q. -- looking at the --

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. Are you looking at the exhibit number?

Q. Yeah, exhibit number.

A. Okay. What page again, sorry?

Q. Thirteen.

A. Okay.

Q. Okay. Would you agree that the -- that Norman discloses the Norman firewall uses nothing but proxy services to pass traffic from one network to the other, no packets are allowed to pass directly?

MR. JACKSON: Objection, form, incomplete hypothetical, calls for speculation.

THE WITNESS: First of all, I -- I don't know that this figure represents all of the functionality of the Norman firewall. I suspect it does not.

I think this prospectus is -- this reference is discussing Norman's value add to, let's say, ordinary packet filters. So I -- I believe Norman is -- what's illustrated here is what Norman is doing above and beyond. It's -- it's trying -- it's trying to illustrate its -- its proxy and functionality.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Secondly, if -- I'm not sure I know what you mean by directly through.

BY MS. SMITH:

Q. I'm not interpreting Norman. I'm reading directly from Norman.

A. Okay. Can you --

Q. Are you suggesting that Norman doesn't say what I just said?

A. Can you show me where?

Q. Yes, I read the first two sentences of paragraph -- of Section 4.5.

A. Oh, okay. I wasn't there.

Q. Oh, okay.

A. Sorry. I was looking somewhere else.

Q. Okay. And I asked if you would agree that Norman discloses the Norman firewall uses nothing but proxy services to pass traffic from one network to the other, no packets are allowed to pass directly?

A. I'm -- I'm sorry, I wasn't reading what you're -- what you're saying. I was just reacting to the figure itself --

Q. Okay.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

A. -- at a high level. If that's what they say their -- their product does, then that's what it does.

Q. Okay. And now I'm referring to the figure below that in Section 4.5 on exhibit page number 13. And do you see where just below the figure Norman discloses, the figure above illustrates how an FTP transaction works through the Norman firewall, period; a unique feature of the Norman firewall is that the firewall will log into the workstation on the secure network to transfer the requested file back to the user.

Did I read that correctly?

A. You did, yeah.

Q. Okay. Based on the disclosure that we just discussed in the Section 4.5, is it correct that -- to say -- that in Norman's proxy system a -- a file is sent by the firewall via FTP after it logs into the workstation?

MR. JACKSON: Counsel, was that -- was that your question?

MS. SMITH: Yes. Yeah.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

MR. JACKSON: Objection, form, foundation, hearsay.

THE WITNESS: The -- the figure illustrates how a file is -- has to pass through the firewall in order to get to the remote host, which I assume the remote host is the user in question. Does that answer your question? I'm not sure.

BY MS. SMITH:

Q. I'm not sure either.

Would you agree that Norman's proxy system intercepts all packets?

MR. JACKSON: Objection, form and foundation.

THE WITNESS: To the extent what you said is a rephrasing of what's recited on page -- exhibit page 10 -- 13 of Norman, no packets are allowed to pass direct -- pass directly, yes.

BY MS. SMITH:

Q. Okay. Would you agree that the -- Norman's firewall will transfer the requested file via FTP after the firewall logs into the workstation?

MR. JACKSON: Same objections, form and

c4ea61a5-485d-4192-937b-dc6133d2c9f4

foundation.

THE WITNESS: Again, you're -- you're reciting the caption below the figure on exhibit page 13 of Norman, the Norman firewall -- so a unique feature of the Norman firewall is that the firewall will log into the workstation on the secure network to transfer the requested file back to the user. To the extent that you're basically restating that, I agree.

BY MS. SMITH:

Q. Is this a type of non-transparent proxy?

MR. JACKSON: Objection, form, foundation.

THE WITNESS: So to the extent that the users understand that they're logging in to -- so I'm not sure if Norman uses the expression transparency. Are you referring to how it's describing itself?

BY MS. SMITH:

Q. I was just asking whether the disclosure in Section 4.5 is a type of non-transparent proxy.

MR. JACKSON: Same objections to form and foundation.

THE WITNESS: To the extent that users --

c4ea61a5-485d-4192-937b-dc6133d2c9f4

the -- sorry, the quote from page 13, exhibit page 13 that I'm reading, users can be required to authenticate himself/herself to the firewall machine by actually logging into the system, because users can identify the firewall, if they're logging into something they understand is a Norman firewall, rather than the -- the workstation on the left of the figure, then it's non-transparent.

If the users believe -- in other words, if -- if the message sent from the user on the right-hand side, the remote host, if it's addressed to the workstation and it's forced to pass through the firewall, then it would be transparent.

If, on the other hand, the users are -- understand that the firewall is there and they're authenticating to the firewall, rather than to their workstation, then it would not be transparent. And I'm not sure how visible the Norman firewall is to the outside world.

I think it is transparent because in the last paragraph -- the second paragraph, I

c4ea61a5-485d-4192-937b-dc6133d2c9f4

mean, of Section 4.5, it's -- you know, it appears that in Section 4.5 that the user is logging into the firewall. And to the extent that it understands that it's logging into the firewall instead of the workstation, then it's not transparent.

Q. Okay.

MS. SMITH: I have no further questions.

MR. JACKSON: Counsel, can we take a break?

MS. SMITH: Yeah. Absolutely.

VIDEO OPERATOR: Going off the record. The time is 12:44 p.m.

(Thereupon, a brief recess was taken.)

VIDEO OPERATOR: Going back on the record. The time is 13:20 p.m.

MR. JACKSON: Petitioners have no further questions at this time and reserve the right to ask questions of Dr. Kesidis in the future as appropriate. This ends the deposition.

VIDEO OPERATOR: This concludes today's videotaped deposition of Dr. George Kesidis.

c4ea61a5-485d-4192-937b-dc6133d2c9f4

Going off the record. The time is 13:20 p.m.

(Thereupon, signature having not been waived, at 1:20 p.m. the deposition concluded.)

c4ea61a5-485d-4192-937b-dc6133d2c9f4

CERTIFICATE OF DEPONENT

I, Dr. George Kesidis, do hereby certify that I have read the foregoing pages, 1 through 123, inclusive, which contain a correct transcript of the answers given by me to the questions propounded to me herein, except for changes, if any, duly noted on the enclosed errata sheet.

G. Kesidis
WITNESS

Sworn and subscribed to before me this 15th day of December, 2014.

My commission expires:
August 2nd 2017

Notary Public:
Stacey M. Brubaker

COMMONWEALTH OF PENNSYLVANIA
Notarial Seal
Stacey M. Brubaker, Notary Public
Centre Hall Boro, Centre County
My Commission Expires Aug. 2, 2017
MEMBER, PENNSYLVANIA ASSOCIATION OF NOTARIES

CASE: Compass Bank v. IV, II
DEPOSITION OF: Dr. George Kesidis
TAKEN: December 10, 2014

PAGE	LINE	ERROR	CORRECTION	REASON
31	1	pix	PIX	acronym, proper name
106	18	file	"file"	ref to the word "file"
107	9,10,18	The Alpha Project	"The Alpha Project"	ref to words
108	3,18,22	The Alpha Project	"The Alpha Project"	
113	10	The Alpha Project	"The Alpha Project"	
115	5	The Alpha Project	"The Alpha Project"	

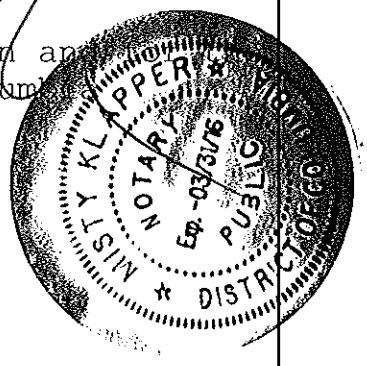
G Kesidis
Witness

CERTIFICATE OF NOTARY

I, MISTY KLAPPER, the officer before whom the foregoing deposition was taken, do hereby certify that the witness whose testimony appears in the foregoing deposition was duly sworn by me; that the testimony of said witness was taken by me in shorthand and thereafter reduced to typewriting by me; that said deposition is a true record of the testimony given by said witness; that I am neither counsel for, related to, nor employed by any of the parties to the action in which this deposition was taken; and, further, that I am not a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Misty Klapper
Notary Public in and for the
District of Columbia

MISTY KLAPPER
NOTARY PUBLIC DISTRICT OF COLUMBIA
My Commission Expires March 31, 2016



c4ea61a5-485d-4192-937b-dc6133d2c9f4