IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX, INC. AND HULU, LLC,	§	
	§	CASE NO. IPR2020-00052
PETITIONERS,	§	
	§	U.S. PATENT NO.
V.	§	8,139,651
	§	
DIVX, LLC,	§	
	§	
PATENT OWNER.	§	

REMOTE DEPOSITION OF
SETH NIELSON
JANUARY 13, 2021

REMOTE DEPOSITION OF SETH NIELSON, produced as a witness at the instance of the Petitioners and duly sworn, was taken in the above styled and numbered cause on Wednesday, January 13, 2021, from 10:08 a.m. to 3:17 p.m., before TAMARA CHAPMAN, CSR, RPR-CRR in and for the State of Texas, reported remotely by computerized stenotype machine in Austin, Texas, pursuant to the Federal Rules of Civil Procedure and any provisions stated on the record herein.

Job No. 187372

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0001
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A P P E A R A N C E S

FOR THE PETITIONERS:
Jeffrey Liang, Esq.
Harper Batts, Esq.
SHEPPARD MULLIN RICHTER & HAMPTON
379 Lytton Avenue
Palo Alto, CA 94301

FOR THE PATENT OWNER:
Bridget Smith, Esq.
LOWENSTEIN & WEATHERWAX
1880 Century Park East
Los Angeles, CA 90067

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0002
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

I N D E X

	PAGE
APPEARANCES.....	2
SETH NIELSON	
EXAMINATION	
By Mr. Liang.....	4
REPORTER'S CERTIFICATION.....	133

E X H I B I T S

	PAGE	LINE
Exhibit 1014, Block Diagrams (No Bates- 4 pages)	78	17
Exhibit 1015, Practical Cryptography in Python, Learning Correct Cryptography by Example, Seth James Nielson and Christopher K. Monson (No Bates - 380 pages)	89	22
Exhibit 1016, Kerberos Ticket (No Bates - 1 page)	111	17
Exhibit 1017, 9,184,920 Chart (Netflix) - Claim 2 (No Bates - 3 pages)	128	5

PREVIOUSLY MARKED EXHIBITS

	PAGE	LINE
Exhibit 1004	57	4
Exhibit 1006	87	24
Exhibit 2009	36	18
Exhibit 2024	59	7

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0003
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

S. NIELSON - 01/13/2021

MR. LIANG: Jeffrey Liang and Harper Batts for the petitioner.

MS. SMITH: And this is Bridget Smith for the patent owner.

SETH NIELSON,

having been first duly sworn pursuant to the Emergency Order regarding the COVID-19 State of Disaster, Paragraphs 2.b and 2.c, testified as follows:

EXAMINATION

BY MR. LIANG:

Q. Good morning, Dr. Nielson.

A. Good morning.

Q. So how many depositions have you given previously?

A. I'd say it's in the neighborhood of 20.

Q. Okay. I'm sure you're very familiar with many of the rules, but I'll go over a few of them anyway just to make sure we're on the same page.

A. Sure.

Q. You understand that you're under oath to tell the truth today. Right?

A. I understand that, yes.

Q. Okay. And when we -- so we'll need verbal responses because this is being transcribed today.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0004
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

And there is no videographer, so we'll just need to make sure the court reporter can get your response.

A. Sure.

Q. Yeah, you know, you can take breaks when you need, but I just ask there is no question pending. All right?

A. Sure.

Q. And you are not allowed to discuss your testimony today with your counsel during breaks. Understood?

A. Sure.

Q. If you don't understand a question, let me know and I'll rephrase, but otherwise I'll assume that you understood the question. Is that fair?

A. Yes.

Q. Okay. And you have to answer my questions unless your attorney instructs you otherwise. Understood?

A. Yes.

Q. Are you on any medication today?

A. I take medication for blood pressure and cholesterol.

Q. Okay. But any reason that you can't -- and neither of those would prevent you from

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0005
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

testifying accurately or truthfully today?

A. Correct.

Q. And is there any reason you can't provide accurate and truthful testimony today?

A. No.

Q. So you're here to give testimony for the interparty review proceedings regarding U.S. Patent No. 9,184,920. Is that correct?

A. I believe that is the correct number. I recognize the last three digits more frequently, but I believe that is the correct number.

Q. Right. And so today we'll refer to that patent as the '920 patent. All right?

A. Yes.

Q. Okay. You have submitted two declarations in this proceeding. Right?

A. Yes.

Q. Okay. Were there -- are you aware of any errors in your declarations?

A. I haven't found any.

Q. Okay. Is there anything in either of your declarations that you want to change?

A. No. My testimony has not changed. My opinions have not changed.

Q. Okay. And did you draft your declarations?

A. I authored all of the opinions in the declarations. I had assistance in drafting.

Q. What did you review when you were preparing your declarations?

A. I believe I have a list of the materials I reviewed listed as part of that.

Q. Okay. Did you -- did you review the institution decision?

A. I have reviewed the institution decision. That obviously was not out before the first declaration.

Q. Did you review it before signing your second declaration?

A. I know I reviewed parts of it. I can't remember if I went through the whole thing.

Q. Okay. While preparing your second declaration?

A. Yes.

Q. Okay. And how much time did you spend preparing your first declaration?

A. I don't know. It was a lot of work. I don't remember how much time went into it. I don't

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0007
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

know. A couple of weeks, maybe.

Q. Yeah, I mean, just approximately do you remember about the number of hours?

A. I remember better that there were a couple of weeks of some intense work, but I don't remember hours.

Q. You submitted a -- let me ask you this. How are you being -- how are you being -- are you being compensated for your work in this matter?

A. I am.

Q. And how are you being compensated?

A. The normal way, hourly.

Q. What is your hourly rate?

A. I believe my hourly rate is $500 an hour.

Q. For this matter?

A. Yes.

Q. And what do you typically charge for your other consulting work at Crimson Vista?

A. That is my normal consulting rate. The reason I was -- had to think about it for a minute, because I had a couple recently where I worked at a discount for various reasons. So I just had to think through it.

Q. Okay. So do you remember approximately

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0008
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

how many hours you billed for that first declaration?

A. I don't.

Q. What about the second declaration, the more recent one? Do you remember approximately how many hours you spent preparing that second declaration?

A. How long do I think that was? I have -- I don't do my own invoicing, so I don't see the invoices when they go out. So I'm not sure. I don't remember for absolute certain. I know I put in -- let me think. I know I put in at least 15 hours. I don't remember if it was more than that.

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

A. I started reviewing the reports that I wrote and the documents that supported it, I guess, starting Saturday or so.

Q. And how much time in total did you spend preparing for this deposition?

A. I guess that would be about ten hours, I guess.

Q. Did you review any documents while preparing for this deposition?

A. Yes. I reviewed my reports, the patent,

you know, the materials that, you know, I've relied on for my opinion.

Q. Were all those materials listed in your materials considered?

A. Yes.

Q. Okay. Did you review any other documents in preparation for your deposition today?

A. No.

Q. In total -- and I'm talking both for your declaration and this deposition -- how much time did you -- have you spent reviewing the '920 patent?

A. That's a good question. I definitely reviewed parts of it, especially some of the claim language. I don't think that's where I spent the bulk of my time, though.

Q. Have you ever reviewed the -- read the entire specification of the '920 patent?

A. Yes.

Q. And do you believe you have an adequate understanding of the '920 patent?

A. I do.

Q. Is there anything you find to be unclear about the '920 patent?

A. I don't think I've come across any

problems in preparing my opinions.

Q. Okay. But when you were reviewing the '920 patent, was there anything that you read that you thought was somewhat unclear about the patent?

A. I don't remember anything.

Q. When were you first approached by DivX regarding being an expert for them in this matter?

A. I believe it was in the month of May.

Q. May 2020?

A. Yes. That's my best recollection.

Q. Have you ever done any work for DivX before May 2020?

A. No.

Q. Now, we're doing this deposition remotely. So I just want to ask if you have access to any documents in front of you?

A. I have printed copies of my report, the '920 patent, and the four pieces of art that were asserted as prior art.

Q. Okay. And to be clear then, those four pieces would be -- would be the reference Chen Exhibit 1004; Grab-333, Exhibit 1005; Candelore Exhibit 1006; and Kocher, Exhibit 1007.

Is that right?

A. Correct.

Q. Okay. Those are all of the documents that you have access to?

A. Yes.

Q. Okay. So we may share some exhibits today and I think we just tested that over Zoom. And since I can't hand you documents in person, I might ask you to open some of those documents if we do use some.

A. Sure.

Q. But unless I ask you to, please don't access anything on your computer during your deposition today.

A. Sure.

Q. All right. So you're the founder of Crimson Vista. Is that right?

A. Correct.

Q. And I guess I'm just looking at your CV. Actually, looking at your first declaration, Paragraph 18, you mention you're the -- you're the founder of -- wait a second. Okay. Yeah.

And what does Crimson Vista do?

A. Crimson Vista is a boutique computer consulting company, primarily focused on issues of computer security.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0012
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Are there any other tech areas that you -- tech that Crimson Vista handles?

A. Well, it's -- it's kind of like there are a lot of interrelated areas. So, for example, I consulted once on a matter relating to potentially fraudulent cybersecurity insurance claims. It had to do with whether or not the software development that was being submitted as an expense was legitimate -- reasonable, realistic for the features and -- and requirements that were being given. So I mentioned that as an example of software development is -- is often interrelated to some of the computer security work that I do. And so I do a lot of work with people with their software, both reviewing it, analyzing it, identifying potential problems with it.

I also -- as is kind of common for computer security, I have quite a background with computer networking so sometimes I'm asked to consult on questions related to network architectures. But those are kind of -- but computer security is kind of the anchor point, I guess you could say.

Q. Okay. So beyond computer security, are there any other technological areas that you consider yourself to be an expert in?

MS. SMITH: Object to form.

Excuse me. Object to form.

A. I think I have listed the areas of my expertise. I think, in fact, I just included those, so software, computer security, networking. Within computer security, I would emphasize my subfield of cryptography.

Q. You mentioned your subfield of cryptography. I noticed your CV mentions applied cryptography. Is there a difference there or is that just some phrasing?

A. No, there is definitely a difference. So I am definitely not the mathematician that works out the mathematics of cryptography. Applied cryptography, you start with what are called, you know, these building blocks or black boxes or whatever you want to call them. Primitives is sometimes the term we use. So AES encryption is a primitive. I am not qualified to talk about why the AES algorithm is secure. That's more of the mathematicians. I mean, I can talk about the general around it, but the math part of it, that's -- that would be different.

But -- but in terms of all of the

constraints that are required for AES to work correctly, all the different modes of operation, where you would use one over another, the security properties that you get out of it, how you build systems securely using those things, that's -- that's applied cryptography.

Q. Okay. And I'm just looking at your -- I'm just looking at your CV and, you know, you mentioned that there were -- just looking at your CV and you mentioned that there were -- you know, you had listed the areas you consider yourself an expert in. And it looks like you have listed applied cryptography as the first one.

A. Yes.

Q. IOT devices and IOT security as the second one. IOT, that -- what does that stand for?

A. That stands for internet of things.

And by the way, I don't know that you should read too much into the ordering in terms of where I listed as first or foremost. I organized my CV in a number of ways that I thought made sense. But I don't want it to imply that, you know, this is No. 1 and this is No. 2 in my order of what I -- what I know most.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0015
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Understood. Understood. Okay.

And can you explain -- can you explain a little bit what internet of things is.

A. Sure. So internet of things is kind of this idea that -- really it's kind of -- I mean, it's existed longer. I think the term first emerged even before the year 2000. But the idea was that all of -- you know, for a long time, what was connected to the internet were people's desktop computers. And so the internet largely meant that it's a computer sitting on a desk or maybe a laptop even once we got Wi-Fi.

Then we started having all kinds of devises connect to the internet, watches, refrigerators, thermostats, doorbells. Some people consider medical to be part of IOT once we started connecting up all of the infusion pumps and monitors and sometimes even pacemakers or whatever else. All of these things started getting connected to the internet and you start to realize that you can take any particular thing and come up with a way to connect it to the internet. It introduces some new problems.

Q. I see. Okay. So it's very -- it's -- I

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0016
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

see.

So the internet of things is related to networking?

A. Well, it's not just related to networking. It's what things you decide to connect to the network.

Q. Uh-huh.

A. For example, you put some very low-powered device connected to the network. Well, it's low power. It's low -- it's -- it maybe doesn't have a general purpose processor. It might have a hardware-specific module, how secure is it, is it as secure as the general purpose that we have already had a good shakedown for and have a lot of experience making it secure. If it's low power, can it support the cryptography, or if it's not being used by a human very often, will we notice if it gets hacked. It introduces just a number of problems that just weren't the same when what was connected to the internet was desktops.

Q. Got it. Okay.

And so just going through this list here -- and I understand that there is no particular ordering. So the lists you have on your CV of your

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0017
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

areas of subject matter expertise would be applied cryptography, IOT devices and IOT security, network security, malware and viruses, privacy, miscellaneous security technologies, and software engineering and software analysis. Is that right?

A. Those are what's listed on my CV. Uh-huh.

Q. Okay. And are there any other areas you consider yourself to be an expert in?

A. I think that's a fairly good list.

Q. Okay. Now, what percentage of your time is spent -- so what percentage of your time is spent, you know, working for Crimson Vista?

A. So I pretty much work full-time as a consultant at Crimson Vista, and then because I like to hurt myself, I also teach for fun.

Q. Where do you teach at?

A. I'm currently teaching as an adjunct professor at the University of Texas at Austin. I currently teach one course for undergraduate students on computer security and a second course on cybersecurity in general for law students.

Q. Oh, okay. What percentage of your time is spent as a consultant for legal matters?

A. That's an interesting question because

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0018
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

some things have overlap, but I would probably describe it as 50/50.

Q. Now, I see in Paragraph 20 of your declaration, you mention "Through Crimson Vista, I also support the Crypto Done Right project."

So what is that? Is that like a book?

A. No. So Crypto Done Right started out as a project at Johns Hopkins. I used to live in Maryland and I was an adjunct professor at Johns Hopkins University. I was also the director of advanced research projects in their information security institute.

We were approached by some people at Cisco and the lead was concerned about how the best practices -- that's -- that's even too light of a way of saying it.

Cryptography is hard to use. Individuals like myself know the ins and outs. We know what you should use, when you should use it, how you should use it, but we then turn it over to people like -- you know, even just a person running a website these days, if they're running a web server, they're supposed to configure their server with this cryptography and it has all of these options. They

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0019
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

look at those options and it's hard for them to know what do these mean in practice, you know. The applied cryptographers know, but there are more people using cryptography than just applied cryptographers.

So we embarked on a project of coming up with a knowledge base for people who aren't applied cryptographers who are just -- maybe they are just programmers. Maybe they are IT people. Maybe they are managers and they've heard "regulatory requirements this," but they don't know what the actual security implication is. And so the website is designed to provide those individuals with the information that they need to correctly use their cryptography for whatever circumstance they find it in.

I guess I should -- your question was about what I said in my declaration, Crimson Vista. Since leaving Johns Hopkins, I have remained involved in the project and I'm currently kind of sponsoring it. It's -- we're transitioning it into its own standalone nonprofit organization so that's -- that's kind of an ongoing process right now. The website is still hosted at Johns Hopkins while we're in the

transition phase.

Q. I see.

And just looking at -- poking around the website, it looks like there are some "to do" placeholders. Would you consider that to be a work in progress, the Crypto Done Right project?

A. It definitely is, and, in fact, we're trying to almost turn it into a community-supported effort where it would be kind of like Wikipedia but more like we would have editors and there would be specific -- we -- we're worried that if we just turned it into Wikipedia, all the people who know cryptography will just write to cryptographers. We want to have our editors make sure that we're taking the content and we are correctly directing it towards the people who have to use the cryptography in something.

Q. Got it.

And further down in your Paragraph 20, you mention that you coauthored a book called "Practical Cryptography in Python."

A. Correct.

Q. That sounds like an entry-level book on cryptography. Is that accurate?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0021
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. It's very much targeting beginners who have never done cryptography before.

Q. Okay. And how -- how would you describe that -- your book, "Practical Cryptography in Python"?

A. I mean, kind of like we just said. It targets people who have not done cryptography before, but it assumes, for example, they know programming. So it walks through a number of examples in the book of programming, using the Python programming language, various cryptographic operations. And then kind of in that same spirit of Crypto Done Right, there is a focus on how you do the cryptography correctly. But just because something works in one situation doesn't mean it works in another. And we show -- you know, in the book, we actually have a few places where we have them program it wrong and then break it so they can see how it breaks if you don't do it right.

Q. I see.

Now, in this case, the level of ordinary skill in the art that you've applied is a person with a bachelor's degree in electrical engineering, computer science, or similar field with at least two

years of experience in video encryption and cryptography or a person with a master's degree in electrical engineering, computer science, or a similar field with a specialization in video encryption and cryptography. Is that right?

A. I don't have it in front of me. That sounds correct.

Q. Would you have met this definition of a POSITA on March 14th, 2006?

A. Yes.

Q. Now, you are providing rebuttal opinions in this case for -- for Dr. Patrick McDaniel. Is that right?

A. Yes. I have read his reports and provided rebuttal to them.

Q. Before reading his report and before this matter, had you ever heard of Dr. McDaniel?

A. His name sounded familiar. I don't think I've ever met him in person.

Q. Would you consider Dr. McDaniel to be a respected professor in computer security?

A. I don't think I'm -- I haven't heard anything negative about him, but I -- I have not done that analysis, I guess you would say. I don't have

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0023
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

anything to say one way or the other.

Q. Okay. One of the prior art references in this case is Exhibit 1007, which is a patent application from Paul Kocher. Have you ever heard of Paul Kocher before?

A. The name doesn't ring a bell.

Q. Another reference in this case is Exhibit 1006, which is a patent application to Brant Candelore. Have you ever heard of Mr. Candelore?

A. No.

Q. Are you aware that the Candelore reference, Exhibit 1006, is a patent application assigned to Sony?

A. I don't remember if I noted that or not. I don't think that factored into my opinions.

Q. Is Sony a major player in digital video distribution?

A. I don't think my expertise is on the business side of who has market share and whatever else. I don't think I can comment on that.

Q. You'd agree that in the 2005-2006 time frame, Sony played a big role in digital video. Right?

MS. SMITH: Object to form.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0024
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. I don't know -- I don't -- the question is a little bit vague. I mean, big role in what. I don't know all that Sony was doing in the 2000 time frame compared to anybody else. If you have a technical question about something they did, I can probably answer that better.

Q. Are you aware of whether Sony played a role in digital video, for example, with DVDs?

A. I don't remember what their role in it. I've studied the cryptography of the disc more than all the different people behind it.

Q. You're not aware if Sony played a role in, for example, Blu-ray discs?

A. Well, again, I know a lot of the media companies, Sony and others, were very interested in protecting their content. As I said, I've studied more of how it was protected rather than who wanted to protect it.

Q. Do you know whether Sony manufactured a lot of video equipment in the 2005-2006 time frame?

A. I think I bought video equipment from Sony. So, you know, I'm aware that there is something out there, I just -- I'm not -- that's not my area of expertise.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0025
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Do you know if Sony was involved in any video standards?

A. It wouldn't surprise me if they were. A lot of the major companies like to play parts in the standards body.

Q. Do you know if Sony designed any conditional access systems?

A. I don't know. I'm not sure. I was trying to think of some of the -- of what I knew, but I -- I don't remember.

Q. What were the companies that manufactured conditional access systems from the 2005-2006 time frame?

A. Oh, goodness. There was one that was from that time period, but it was -- what was it called? Smart something. It ended up not taking off. I'm trying to remember what it was called. There was -- there was one that was proposed. It had "smart" in the title somewhere. And they got some buzz for a while right in that time frame, the 2005 or so time frame, and then it didn't work out. They didn't survive. I'm trying to think of what their name was.

Shoot. I can't remember. There was -- that was one I looked at, but I don't remember the

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0026
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

name of it at the time.

Q. Okay. Can you think of any other companies that made conditional access systems before 2006?

MS. SMITH: Object to form.

A. I don't know company names that did, no.

Q. I want to go back to a question. Do you have -- are you aware of the SSL and TLS standards?

A. Sure.

Q. What are they?

A. So these are more commonly used for internet traffic. So basically SSL came first. In fact, TLS is really just a reversioning of SSL. So I'll just call it TLS, but I'm -- I'm talking about both insofar as SSL was its predecessor.

TLS is used to secure traffic on top of our standard network transport protocols like TCP, and it is designed to provide confidentiality and integrity for connections. What that means is that the data is both confidential, unauthorized parties can't read it, and it's got authentication. And that's tied in with the integrity principle, which means that you know the data comes from the party that you think it comes from.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0027
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Is TLS widely used?

A. Very widely used. It is probably the most widely used encrypt- -- well, I don't know if that's true. Certainly on the internet it's the most widely used security protocol. We're using it right now. You know, I mean, it's the air you breathe on the internet.

Q. You mean for the Zoom call we're using TLS?

A. For web browsers, pretty much everything we're doing when we touch the web. There are -- it's funny because it used to not be quite that way. It used to be that only some websites are encrypted and now just about every website you go to is encrypted. They are very few that aren't. Most of your apps on your phone when they're talking back to the home server, they're going to be using TLS. It's -- it's used a lot.

Q. Are you aware that Paul Kocher was the architect for TLS and SSL?

A. I did not remember that. I mean, I've read the original paper, so I guess obviously I've seen his name before, but it didn't stick in my head.

Q. With that in mind, that Paul Kocher was

the architect of SSL and TLS, would you consider him to be a widely respected cryptographer?

A. Obviously he would get a lot of attention for having authored TLS.

Q. Would you consider the author of TLS to be widely respected?

MS. SMITH: Object to form.

A. The only -- I'm sure -- I'm sure there's nothing bad I would have to say about him. I guess the only reason I'm hesitant to -- I mean, I just don't hear his name thrown about for, you know, for, you know, applied cryptography in the -- you know, in casual conversation. So, I mean, I'm sure -- I don't have anything negative to say about him. If you're asking me if I hear a lot about him, no. No, I don't.

Q. I'd like to ask you a few questions about MPEG streams.

A. Sure.

Q. What's the relationship between a elementary stream and a packetized elementary stream?

A. So the elementary stream is the -- the content -- there's a specific content type, so video will be one elementary stream, audio will be an

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0029
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

elementary stream. You can also have elementary streams of things like subtitles and some of that kind of information.

Then when you create a packetized elementary stream, you create -- so you have to put on -- so they have packetized elementary stream abbreviated to PES, which I will just call PES if that's okay. If ever I'm not clear, feel free to ask me for clarification. But I'll say PES to refer to packetized elementary stream.

And when you take the elementary stream, you turn it into a packetized elementary stream by putting on a PES header which has some information about the stream and you chop it up into pieces, each piece getting this PES header.

In the documentation, though, just as a caution, there will be times where it just throws out in passing an elementary stream that it's sometimes clearly talking about, at least in the context where it is. You've got the packetized elementary stream and it's just referring to it as the elementary stream.

Q. Okay. And what's the relationship between a packetized elementary stream and a transport

stream?

A. Right. So the transport stream is designed for transport. Not to be cute, but that's actually why the name is what it is. It's designed for transport and it's very specifically designed for lossy transport, meaning packets can be lost or delayed or otherwise not arrive at the destination when you need them.

The transport stream is fixed to 188 bytes. That -- that link, by the way, came from the development of networks in the '90s. They thought that the IP networks, what we use today, weren't going to be good enough. And so ATM was this alternate technology -- Asynchronous Transfer Mode, ATM, everybody thought it was going to become way, way better than our normal IP networks, and it didn't succeed.

But because transport stream technology for MPEG was under development in this time period, they made these transport packets of a small enough size that they would fit in an ATM packet.

But you take this 188 packet and typically you've got a header, I think it's four bytes, and then you take some chunk of a packetized elementary

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0031
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

stream, like 184 bytes of it, and you stick it into the rest of this TS packet.

And so you're going to have multiple packet -- multiple packetized elementary streams and so you'll interleave this into the TS transport stream where you take 184 bytes from this one and I put it into the first TS packet and then 184 bytes from the audio one and put it into the next TS packet, and you kind of interleave it throughout the -- the transport of these packetized elementary streams. Obviously when the transport stream is received, you then have to be able to recreate the packetized elementary streams on the other end.

Q. And the use of transport streams and packetized elementary streams was known in the art before 2005?

A. Yes.

Q. What is -- I'm seeing this term, I just wanted to ask you. What is an access unit?

A. So access unit -- I mean, it's one of those things where you start having -- I think there's some overlapping terminology here. So the access unit in the elementary streams is kind of like what is your fundamental chunk. Right. And it

depends on the type of elementary stream. So for video, an access unit could be a frame. I don't remember what it is for audio, but audio doesn't use frames obviously. Not video.

But it would be some chunk that is -- some kind of fundamental chunk, some way of recognizing a component, you know. It could be, I don't know, tenth of a second of audio or something like that.

Q. Okay. And then a PES packet, which you just described to us, represents an access unit in the elementary stream. Is that right?

A. Yes.

Q. And then PES packets are broken down -- are divided up into transport stream packets. Is that right?

A. They're chopped up and placed into transport stream packets, yes.

Q. A transport stream packet will be smaller than a PES packet. Right?

A. Most likely, uh-huh.

Q. And for video, a PES packet is a video frame. Right?

A. I believe that is correct. Uh-huh. An access unit.

Q. And for video, a transport stream packet is then a portion of that video frame. Right?

A. Yeah. Obviously if we're talking about a transport stream packet that is carrying part of that video PES packet, then that will be carrying a portion of the -- the video in the PES packet.

Q. Is it your opinion that conditional access systems scramble transport stream packets?

A. Well, I mean, I think it's clear from the documentation that transport streams support scrambling. I think I've described that at some length in my report.

Q. Right. So then I think you're saying that -- so is it your opinion that conditional access systems then scramble transport stream packets?

A. They can. They don't have to. I mean, I guess that's the biggest reason I'm kind of -- maybe I'm clarifying your question. Are you asking me if they have to or are capable of?

Q. I see. Okay. Are conditional access systems capable of scrambling transport stream packets?

A. Yes. Although, just to be absolutely 100 percent clear, I don't know that this matters,

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0034
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

but I'll just, for clarity, when you say "scramble the packet," you're actually scrambling the packet data but not the packet header.

So like I said, the TS packet is 188 bytes. I believe it's the first four bytes that are the header. That part is not scrambled, and then the 184 remaining bytes are. Well, and even that depends.

There are situations where you can't scramble all of it. But my point is, is that yes, you can scramble portions of the data being transported in the transport stream packet.

Q. Can CA systems scramble a packetized elementary stream?

A. So the standards permit a limited form of scrambling of the PES packet.

Q. What is that limited form of scrambling?

A. Well, I go over this in my report. I don't know if you want to send me my report, but I'll jump into the sections that start going into the details of the limitations.

Q. Okay. Well, sure. Let's go to -- which report are you referring to?

A. I have a little bit in -- well -- so let's

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0035
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

start with the first one.

Q. Okay. Yeah. Let's go -- let's go to your first report, then, and you can direct me to what the -- the portion that you want to refer to.

A. Sure.

Q. I believe you said you have a copy of it in front of you?

A. I have a paper one. Would you prefer that I use that or would you prefer to send me an electronic copy?

Q. No, I think if you have a -- are all of the documents in front of you unmarked?

A. Unmarked.

Q. Okay. So it's totally plain?

A. Totally plain.

Q. Yeah. So if you could just use the printed version in front of you for Exhibit 2009, I believe, you are referring to now.

(Discussion off the written record.)

A. Paragraph 70 of my initial report. Would you like me to read the parts that I'm referring to?

Q. Sure.

A. Okay. I'm going to start in the second sentence that begins with "This scrambling."

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0036
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

"This scrambling can be applied to the PES packets before they are broken into TS packets, or scrambling can be applied to the TS packets, after the PES packets are broken up. Scrambling the PES packets enables the stream to include scrambled and unscrambled data within the multiplexed data. But even when scrambled on the PES 'packet,' it is actually treated just like TS scrambling. The PES data is broken up into TS packets and then scrambled." The reference that follows describes that process. The broadcast engineering reference book at the section identified.

Q. And then after a stream has been split into transport packets and placed into a transport stream, it's no longer possible to process video frames at that point. Is that right?

A. That's correct. The transport stream level is completely agnostic to the type of data it's carrying. It doesn't have any semantic processing. So what I mean by that is, the transport stream is designed to carry data. It doesn't have information about, okay, this is video, this is audio, this is subtitles. It's just transport stream data.

Actually, let me -- I want to clarify one

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0037
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

point on that. The transport stream packet does carry identifiers so it knows which packetized elementary stream the data belongs to. I don't mean to imply that it doesn't have any marking data. I mean that it doesn't have any processing data for, okay, I've got video or I've got audio or I've got subtitles.

Q. So can you process transport stream packets to encrypt a portion of a video frame?

A. Well, I think I explained that in my report, that there isn't really a concept of a video frame in the transport stream.

Q. I see. So it sounds like you're saying it can't be done?

A. Well, I think what I'm trying to say is that there may be situations in which data is encrypted that -- and that data was originally part of a PES packet which was originally a frame, but that there is no process at the transport level in which video frames are identified, portions identified, those portions encrypted, and then those portions can be identified as part of a frame pulled out and unencrypted.

I'm saying that there is no frame -- there

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0038
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

is no frame concept.

Q. So can a CA system go in and encrypt a specific block of, say, 64 bits inside a video frame?

MS. SMITH: Object to form.

A. Are you talking about at the PES level or are you talking about the TS level?

Q. Let's start -- I'm sorry. Were you about to say something?

A. No, go ahead. I'll stick with that clarifying question first. We'll go from there.

Q. Okay. Well, let's start with the PES level. Can a CA system go in at the PES level and encrypt a block of 64 bits inside a video frame?

A. Well, there's a couple of different ways to answer that. So the first one is, when you are sticking a PES packet into a TS packet, as we discussed, the PES packet will almost certainly be larger, which means you're splitting a PES packet over multiple TS packets. All right?

Now, in the very first packet, the first packet has the PES header as well as the PES data. The -- the standards require that. If you are encrypting at the PES level, you don't encrypt the PES header.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0039
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

So you could, if your PES header, which can be -- I mentioned the TS header I think is like 4 bytes. The PES header is more variable and can be longer. It's possible that if you put in enough header bytes into the first TS packet, and there were only 64 content bytes at the end of it, those 64 bytes would be encrypted as part of the encrypted -- that would be the encrypted part of that TS packet. So that's one way that I can think of that that would happen.

The other thing to consider is, if you are using a block cipher that is 64-bit block, like DES, or even triple DES, then the way it works is -- that always works on 64 bits at a time -- wait -- 64 -- 32 -- oh, you were asking me about bytes. I apologize. You were saying bytes. I switched to bits, so that wouldn't apply there.

Q. Well, let me -- let me ask you that question, then, in terms of bits. So, you know, can a CA system go in at the PES level and encrypt a block of 64 bits inside a video frame?

A. Right. And just one -- this is really pedantic, but just for clarity I'm just going to emphasize. When we say what a CA system can do,

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0040
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

obviously a CA system could do whatever it wants. I'm talking about the standards and, you know, the MPEG-2 TS standards, right? So I'm -- here's how the standards work, and then how somebody implements it, hopefully they're following the standards, otherwise it probably won't do them too much good.

When we're -- when we're talking about encrypting with a block cipher, AES, DES, all of those, they all work on a specific size at a time. But that doesn't mean that's the only data they're encrypting.

So what you do -- in fact, when we get to the Grab reference, the Grab-333, if that's one we get to today, it talks about a mode called CBC. It's a cipher block chaining mode. And the idea is that because the block cipher can only encrypt in chunks, you encrypt with one chunk and then you feed that data into the next chunk and then into the next chunk and then into the next chunk so that you end up kind of encapsulating everything that you encrypt.

So even though it's doing it in these chunks, you still end up encrypting a larger selection of data collectively using the CBC mode.

Q. Your previous answer you referenced the --

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0041
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

you mentioned that you're here to explain how standards -- how the standards work, but that people don't necessarily have to follow the standards. Are you referring to proprietary systems?

A. No, no. What I'm stating is -- like I said, I was being just a little bit pedantic. There are standards that are accepted by region. So there is a standard that's for North America, there is a standard that's for Europe. It's accepted by country for the broadcast standards.

And so when you want to broadcast within one of these countries, you have to follow the standard. And then obviously you could program your system to do something wrong, but then it wouldn't operate correctly.

So when you're asking could a CA do such and such, well, yes, they could program it counter to the standards, but then it wouldn't be operational within the -- within the country.

Q. If you were going to create a proprietary system where you controlled the transmission and receiving side, then you could -- you could deviate from a standard and still make an operational system. Right?

A. I mean, any time you -- well, I don't know. I don't know if there are legal or regulatory reasons why that's not allowed.

Q. Right. And I think as you said before, you're not really an expert on the business side of things. Right?

A. Correct.

Q. But just technologically speaking, if you create a proprietary system where you control the transmitting and receiving side then you can deviate from a standard and still make an operational system. Right?

A. I mean, if you're --

MS. SMITH: Object to form.

A. If you're deviating from the standard you don't have to follow the standard at all, so, I mean, I guess you can do whatever you want.

Q. Right. And when you design the system as you want, you deviate from a standard, a proprietary system, you can make a system that works. Right?

MS. SMITH: Object to form.

A. There are all kinds of ways you could design a CA system. So, I mean, if your question is, is MPEG the -- MPEG-2 TS the only possible way you

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0043
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

could transport packets from one place to another, of course the answer is no.

Q. So going back, then, to the question about the encryption of specific bits. I believe what you were explaining then is that a CA system can go in and encrypt specific blocks of bits inside a video frame if it's operating on an elementary or packetized elementary stream. Is that right?

A. No, that's not what I testified. We've only been talking about TS so far. We haven't even gotten to PES level.

Q. I'm sorry. I guess maybe there is a little mix-up. Let me just ask the question again because my previous question was actually directed at the PES level. So I just wanted to make sure we're on the same page then.

So can a CA system go in at the PES level and encrypt a block of 64 bits inside a video frame?

A. I apologize. Now that you mention it, yes. The reason I was thinking about the TS level is separate. But, yes, okay.

So my answer is this. For the standards that I'm aware of, the PES encryption has to be done in a very specific way. Like I say in my report

here, it has to be done in a way that is more or less like the TS encryption. And there are a lot of reasons for that.

Q. When you say "more or less like the TS encryption," what do you mean by that?

A. Well, what I mean by that is this. The system takes the PES packet and breaks it up into chunks, and then it encrypts it or scrambles it largely like TS level. The only potential difference being, like I was saying a little bit ago, well, the PES header is not allowed to be scrambled, but you're still taking these 184-byte chunks minus a header, if that's for the first packet, and you run them through the decoder.

And, in fact, important to this conversation, I think it's actually in my second report. In fact, I know it is. There is another -- the standards make another point that is really critical to this that I'm going to pull up here. I'm turning to my second declaration here for clarity, for the stenographer. Let me find this here.

This is it. This is it. This is Paragraph 47 of my second report.

I'm going to read the whole paragraph, but

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0045
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the emphasis is the quote from the ETSI standard, E-T-S-I standard. But let me read the whole paragraph for context.

"But it is also not obvious to combine PES level partial-frame encryption of video with PES level scrambling of audio. The digital video broadcasting standard cautions that use of different scrambling circuits creates problems with" --

Q. Let me stop you here. I've got the report in front of me and I'm reading the paragraph. So can you just explain how -- you don't have to read the whole thing. I mean, it's in the record. So can you just explain how this relates to your answer?

MS. SMITH: Object to form.

A. Sure. The really critical thing here is this quote from the ETSI standard.

"In order to avoid complex implementations at the consumer receiving equipment, only a single descrambling circuit shall be required."

This is talking about the descrambling that you use, whether you're using TS, PES, any of those, all have to be descrambleable by the same descrambling circuit.

So when I say that PES has to work more or

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0046
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

less like TS, part of what I'm emphasizing here is you have to design a single circuit that can descramble TS packets and PES packets, and that's one of the reasons why they have the PES scrambled the way they describe it, where you have to break it up into the 184-byte chunks and you have to do this and you have to do that, so that you don't end up having a system that has to have multiple descrambling circuits if you switch back and forth between TS and PES level scrambling.

Q. So CA systems can switch back and forth between transport stream and PES level scrambling?

A. Well, they're not allowed to use both at the same time. They're not allowed to both scramble the PES level and scramble the TS level. You have to pick.

But you can have -- you can have a system that can do one or the other, and can obviously change between them once it's, I guess, a new program or some way of recognizing that a switch should happen.

But you can't do the switch in such a way that you would end up with, well, I've got this packetized elementary stream that I've been

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0047
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

scrambling and now I'm trying to scramble the TS packets because they can't both be scrambled at the same time.

Q. So can a CA system encrypt just the central area of a video frame?

MS. SMITH: Object to form.

A. Well, as I've just described, that's not how PES level or TS level encryption work.

Q. So a CA system can't just encrypt the central area of the video frame?

MS. SMITH: Object to form.

A. I'm not saying it isn't possible in other levels, but they can't do it at the PES level or the TS level.

Q. And what level would it be possible for a CA system to just encrypt the central area of a video frame?

A. Well, if you wanted to do something at a higher level, I suppose you could put in custom operations above -- once -- you know, at a layer above. I don't know exactly how you would do that. I mean, that's probably not very realistic either because of the complexities involved, but you're not going to do it at the PES level or TS level.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0048
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. So a video frame includes a number of smaller components. And I just wanted to ask you about some of these, some terms that I've heard. Have you ever heard of a macroblock?

A. Yes, I have. But I don't remember off the top of my head what it is.

Q. Have you ever heard of a slice?

A. Yes. I'm trying to remember what that is.

A slice -- I don't remember off the top of my head what that does either.

Q. Do you know what a coding unit is?

A. A coding unit. Well, I think I know what it is, but I don't want to guess, so I'll not try here.

Q. Do you know what the different types of frames there are in an MPEG video?

A. Yeah. I mean, I know the basic. There is the I frame and the B frame. And I'm trying to remember the third one. P frame I think it is. I know the basic operations of how those work.

Q. Well, how do those different frame types work?

A. Yeah. So the basic idea is that you -- okay. So background.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0049
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

If you were going to just have a frame that was like a picture, you would have to have enough data for every single pixel in the picture. And the bigger the resolution, the more pixels that is. And the more color options there are, the more data has to be encoded for each pixel. And that turns out to be a lot of data.

I think something like a 640 by 480, which is very small by today's standards, frame at 32-bit color is like 1.2 megabytes for a single frame. And if you have to have 24 frames a second, that starts to add up really, really quickly.

So the motion picture group and others started working on ways that they could do compression, so that they could compress the data to make it more efficient for storage, and especially for transmission.

So there is two different types of compression. There is lossy compressions, and that means that you can get back most of the data, but not necessary all of it, and then there is lossless compression, which means you'll get back exactly what you started with.

So video -- video encodings like MPEG use

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0050
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

a combination of both lossy and lossless.

Now, with these different frames, for example, one of the ways that they're able to reduce significantly the amount of data that has to be stored in every frame is they take advantage of statistical redundancies.

So the idea is that in a video, even if you have to have 24 frames in a second, in most sequences a lot of those bits, a lot of those pixels aren't going to change.

So you can start out with kind of a foundational frame, and I believe that's the I frame. And you start with this first frame that is going to have, I'm going to say, all of the data, even though you still do compression on it. But the idea is that you can restore the entire frame.

But then you can have subframes where the next frame in the sequence has a couple of different ways of -- of reducing how much it has to have. It can have just simple differences. Like right now while you see me talking on the video screen, most of the background around me is staying exactly the same. Even most of my body position is staying exactly the same.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0051
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

And so in between frames, you'd only have to have the differences between, say, my hand moving up or my hand moving down in each one of those frames.

But you can also do even more advanced things, like motion compensation. And that's where the compression algorithm actually looks for the same set of pixels, like say my hand moving across the screen. So you don't even have to do full deltas. You can say, hey, this set of pixels that was in this spot is going to move delta X far, blah, blah, blah, in this direction in the next frame.

And so these smaller frames allow you to kind of recreate the sequence from the initial establishing frame.

Q. Okay. And then what is an I frame then?

A. I think if I have my ordering right, I believe the I frame is the initial one.

Q. What's a B frame?

A. That's one of the intermediate ones.

Q. And what was -- I believe you said it was a P frame?

A. I think it's P. I can't remember -- I think B is the more common one. It's kind of -- I

can't remember what P is used for. They all fit into this compression architecture I just described.

Q. Okay. And what's the difference between a B and a P frame?

A. I don't remember off the top of my head. They're both intermediate frames. I just can't remember what the difference is.

Q. What's a group of pictures, which I believe is --

MS. SMITH: Object to form.

Q. -- abbreviated with the letters GOP?

A. I don't remember.

Q. How does quantization fit into the type of prediction that you were just discussing above?

A. So quantization -- I hope I'm pronouncing that correctly. Quantization is the idea of recognizing a quantum of data. So some chunk of data that -- well -- okay. So I guess I'm more familiar with it in terms of compression than in the motion compensation.

But the -- the idea is that if you have -- you can -- you can get a little bit of lossy compression if -- if you just record the information on maybe a -- 4 pixels in a -- in a square rather

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0053
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

than each pixel individually.

And so especially with some of our higher-resolution images, that kind of loss of granularity won't be visible to the human eye, especially if we put it in parts of the background image that aren't where the action or the focus is happening.

Q. I see. So quantization relates to a reduction in resolution?

A. Well, it can. I mean, if -- if you -- if you have a technical document you want me to see that is using it for the motion compensation, I can probably explain that one, too.

The one that I'm familiar with off the top of my head is where you can reduce your resolution just a little bit in a way that's not noticeable to the human eye or not very noticeable, but you can get a pretty good reduction in -- in space.

Q. Is that -- is that how MPEG video works?

A. I'm pretty -- yeah, I think that -- yes, I know that's used in MPEG.

Q. I see. So an MPEG video, then quantization uses a reduction of resolution to compress the data?

A. That is one of the forms of compression used in MPEG is to reduce resolution in what is supposed to be an unnoticeable or almost unnoticeable way.

Q. I see. So MPEG video uses quantization to reduce the number of pixels in a frame in a way that's unnoticeable or almost unnoticeable?

A. I believe that is what -- so MPEG uses that. I'm pretty sure that's quantization if it's -- if that term is being used somewhere else, that's -- that's a possibility. If you -- again, if you have a document you want me to look at, I'm happy to.

But that compression mechanism is used in MPEG.

Q. Have you ever heard of the phrase "CABAC," which is capital C, capital A, capital B, capital A, capital C?

A. It's not ringing a bell.

Q. Have you ever heard of the phrase "entropy encoding"?

A. Yes. Yes, I have, entropy encoding. I'm trying to remember what this one is. I've -- I've heard the phrase. I -- I don't remember exactly how it worked. I don't remember which compression

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0055
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

mechanism it is.

Q. Okay. How does MPEG video use binarization?

MS. SMITH: Object to form.

A. I don't remember. I'd have to -- I'd have to see a document.

Q. Would you agree that parts of elementary streams can be scrambled for conditional access systems?

MS. SMITH: Object to form.

A. Well, I think I've described a couple of times here how at the TS level and the PES level, that is only performed across the entire elementary stream.

THE STENOGRAPHER: If we could take a break.

MR. LIANG: Sure. We'll be back at 9:50.

(Break.)

Q. Dr. Nielson, did you discuss your testimony today with your counsel at any point during that break?

A. No.

Q. You've provided some opinions in this

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0056
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

matter regarding a prior art reference called Chen, which is -- has been marked in this proceeding as Exhibit 1004. Right?

A. Yes.

Q. Is it your opinion that Chen discloses a conventional conditional access system?

A. I just prefer to double-check my report. I think those are the words I used, but I'd prefer to have the text in front of me.

(Pause.)

Well, I mean, discloses. Chen describes a conditional access system as a background system. So, I mean, obviously, Chen's invention is not a conditional -- is not a -- Chen's invention builds upon a conventional conditional access system.

Q. And just for simplicity today, you know, if I -- if I refer to a conditional access system as a CA system, the letters CA, all caps, you'll understand that I'm referring to conditional access systems?

A. Yes.

Q. Okay. Would a -- and would a -- withdrawn.

Would a person of ordinary skill in the

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0057
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

art have needed to modify Chen's implementation in order to combine it with Grab-333?

A. Well, I think I explained how you really can't combine those. They're not really compatible for combination, at least not the way described for sure.

Q. I see. So a person of ordinary skill in the art wouldn't have combined Chen with Grab-333 because they describe incompatible implementations. Is that right?

A. Well, the way that I describe it in my report I think is better than the way you were wording it right there. Let me find the way I was wording it.

Yeah, yeah, yeah. So this is Paragraph 55 of my report. Right in the middle, it says, "In particular, Chen and Grab-333 relate to different technology components that operate on different data structures at different levels of abstraction."

It's not really an implementation problem, per se. It's deeper than that.

Q. I see. So because they operate on different data structures and different levels of abstraction, then it wouldn't have been obvious to

incorporate Grab-333 into Chen. Am I understanding that correctly?

A. Yeah. I would actually say that it would make the proposed combination incompatible.

Q. Now, if we could go to your second declaration, Paragraph 17. So this is Exhibit 2024, Paragraph 17. And let me know when you get there.

A. I have it.

Q. Okay. Now, towards the middle -- towards the middle of this paragraph, it reads, "But I could find no mention that the CPU performs scrambling or descrambling in Chen's improvement over Figure 1 or in the standard implementation in Figure 1 itself."

Do you see that?

A. I do.

Q. Okay. So it sounds like Chen's hardware doesn't use a CPU for scrambling or descrambling. Is that right?

A. Yes.

Q. And partial encryption is only beneficial for set-top boxes if the CPU performs the scrambling or descrambling. Right?

A. Well, that's not how I would word it. I think there is two separate arguments here and we

need to talk about them separately.

So the first argument is, what is the benefit. Right? So one of them has -- one of the issues that is being addressed here is the benefit of Grab on a reference like Chen. That -- that's one separate issue.

Because I believe -- correct me if I'm wrong. I think your question was -- if I'm remembering it correctly, I think you said you would need a -- you were asking me if you would need a CPU to perform partial frame encryption.

Q. Yeah. So my question is whether partial encryption is only beneficial for set-top box if the CPU performs the scrambling or descrambling?

A. So I think I explain here in my report that set-top boxes use a descrambling circuit and this is consistent with all the evidence I could find about conventional access -- or conditional access systems. And that a algorithm that is designed to reduce the processing of a central processing unit isn't going to provide the same benefits to a system that uses a dedicated circuit.

Q. And so, therefore, there wouldn't be a motivation to apply Grab-333 to Chen because Chen 's

partial encryption wouldn't be beneficial for Chen's hardware?

A. That was one of the arguments that I made, yes.

Q. I think I misspoke. I think I said Chen's partial encryption. I meant Grab-333's partial encryption.

A. Yes, I guess I interpreted that as in the combined system where Chen would have a partial frame encryption, it does not get the benefit because of the differences in hardware.

Q. So these hardware decryption circuits are -- well, withdrawn.

Let me -- let me go to Paragraph 15 of Exhibit 2024. Let me know when you're there.

A. Paragraph 15?

Q. Yeah.

A. Yes, I have it.

Q. Okay. And so this paragraph, you discuss something called a SoC. What is that?

A. System on chip.

Q. Okay. And then after that, you mentioned ASIC. What is that?

A. Oh, I'm trying to remember what the

acronym stands for. It's basically where you encode into hardware like a specialized function. So, for example, if you've been following the -- anything with Bitcoin, the miners come up with faster and faster ASICs. They're these basically specialized manufactured boards that do the specific purpose.

Q. And how -- what's the relationship between an SoC and an ASIC?

A. Well, so a lot of times when you're going to do an ASIC, you know, you're going to -- you're going to build in -- so -- so -- okay. Look. So in a desktop computer, you have, like, modular components and so it's like, oh, I can plug in the RAM over here and the memory over -- or -- that is the memory. The RAM over here, the generic CPU over here, specialized hardware on a expansion board. A system on chip builds these all into a single piece of hardware, a single chip. For example, smartphones will put all of these components onto a single processor that's a system on chip.

Q. And an ASIC is -- I believe you were explaining it's -- it's like a chip that's designed for a specific --

A. Purpose.

(Simultaneous speaking.)

Q. -- packetization (phonetic)?

A. Yeah.

Q. When you were explaining the dedicated encryption units earlier, were you referring to an implementation on a ASIC?

A. Well --

MS. SMITH: Objection to form.

THE WITNESS: Sorry.

MS. SMITH: Objection to form.

A. Well, yeah, so it would be built into the system on chip. I mean, it's possible that you could have it be somewhere else on the board, but it's also reasonable for it to be built into the system on chip. Either way, that's not really relevant to either Chen's disclosure or the problem with the partial frame encryption benefits.

Either way, I guess what I want to state is either way, what you had in these set-top boxes were these decryption, descrambling circuits. They were usually manufactured by a third party. They were mass manufactured and then you would build them into your system, including a system-on-chip-type implementation.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0063
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Do these hardware descrambling circuits have limits on how much data they can encrypt -- I mean -- I'm sorry -- decrypt per second?

A. Well, I mean, everything has a limit. But the chips were designed to function in realtime. So in terms of their speed, they were able to descramble the scrambled content fast enough for displaying on the screen.

Q. If a dedicated hardware descrambling circuit has less data that it needed to decrypt, then the hardware would require less circuitry for its implementation?

A. No, in fact, that's probably the opposite.

Q. Why is that?

A. Well, part of what makes the descrambling circuit so simple is the relatively straightforward operation. Here is a fixed-sized chunk of data, descramble it. In, out, we're done. Now if you have to start putting in additional inputs about which pieces are encrypted and which pieces are decrypted, then the circuitry gets considerably more complicated.

Q. So the increased amount of logic it takes to figure out whether to encrypt or decrypt

something, in your view, is more complex and takes more processing power than the operation of decrypting itself?

A. Well, certainly selecting the portions to be -- so you now have a lookup. You've got -- so Simplified Circuit No. 1 where we're just decrypting all the data that's passed -- or descrambling all the data that's passed to us, the data goes in, all the data is processed, data goes out.

And a lot of these scrambling algorithms were originally not full encryption algorithms. They were intended to be fast bit shifting, et cetera, et cetera. Yeah. You just shove all the data in, you apply the algorithm and you spit it out.

Now if you have to have logic that says okay, for this piece you need to jump to this part and start here and decrypt this much but not the other parts, then, yes, that makes it a far more complicated circuit for a dedicated piece of hardware.

Q. So Grab-333 explains that when you're using partial encryption, then it can -- withdrawn. Let me rephrase.

Is it your opinion that Grab-333 teaches

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0065
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

partial encryption on a general purpose CPU?

A. Yes.

Q. Does Grab-333 teach that running partial encryption in software on a CPU will save computational -- will save you computation in comparison to having to decrypt the entire video stream?

A. Yes. For a general processing CPU, that is true.

Q. You would agree that Grab-333 has to implement logic in software to figure out which blocks to encrypt and which ones -- withdrawn.

You'd agree that Grab-333 has to implement logic in software to figure out which blocks to decrypt and which ones don't need to be decrypted?

A. Yeah. So the general purpose processor already has general purpose processing. In computer science terms, right, we've got something that's Turing complete, meaning we already have a processor that can compute anything. So we already have a complicated circuit.

Within that complicated circuit we can throw some software operations at it, and in the general purpose scenario then we end up with a

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0066
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

savings. But if you're manufacturing, especially mass manufacturing across a wide range of providers, a chip that is going to do a specific operation, then it is definitely simpler to decrypt an entire -- or descramble an entire input rather than having to provide additional inputs and additional circuitry that handle the partial descrambling.

As a side note, this is why the standards, right, said if you are going to do PES level decryption you still have to have just one descrambling circuit. We need something that's simple, that's easy to mass produce, that doesn't get too fancy, that can be mass distributed in all of these set-top boxes. It's a process that has to be simple for the circuitry, and also not generic.

That's why we have to have it designed to work for both the TS scrambled packets and the PES scrambled chunks that are in the TS packet so that with one hardware circuit with no extra complexities we can just throw data in and at very quick speeds and get the descrambled data out.

Q. I think we talked before, you've done a lot of work with software analysis and I take it you are -- I take it you work with C, C++ and Python.

Right?

A. Yes.

Q. Have you ever designed any hardware with -- well, let me -- withdrawn.

Have you ever used Verilog before?

A. Very minimal.

Q. Have you ever designed a hardware circuit before?

A. No.

Q. If I was designing a hardware decryption circuit from scratch, then the -- would you agree that the -- that I would be able to implement the -- withdrawn.

Let me ask it this way. If I'm designing a hardware encryption circuit from scratch, would you agree that the amount of data that I'm trying to decrypt per second, that by decreasing that amount of data, I would decrease the amount of circuitry I would need to implement the decryption process?

A. Not necessarily. So suppose that like we have in a scenario where we need to be -- for example, if you could guarantee that it would always be 16 bytes as opposed to 184 bytes, maybe.

But the problem is, you can't guarantee

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0068
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

that it's always going to be 16 bytes. Even in Grab, it's variable and you assume that it can go all the way up to the full frame. So now you have to have a processor that has to be -- or a circuitry, dedicated circuitry that has to be able to handle the wide input and the narrow input down to variable sizes. No, I don't think that that is necessarily simpler circuitry.

Q. If there is an upper limit, then it would -- then you would -- it would have decreased the amount of circuitry required?

A. It might. As I mentioned earlier, we often work in -- in chunk sizes, right, so if we're talking about AES, we're always working on 16 bytes at a time. So doing 16 bytes versus doing 64 bytes might be a very, very, very simple modification to a circuitry because I'm just repeating it four times.

Q. So in your example of AES, do you know whether the hardware decryption circuits in CA's systems used multiple AES units within them?

A. I don't, because there is some -- so if you look at the listed standards, a lot of times it will say something to the effect of the actual descrambling algorithm is confidential.

So unfortunately, I don't get to have access into how that works.

Q. Do you think that a CA system would need to use multiple AES units inside its hardware decryption in order to decrypt a fully encrypted MPEG video stream in realtime?

MS. SMITH: Object to form.

A. That's an interesting question. I think I was mentioning that CBC is the system where you have to use AES on a 16-byte block and then you carry the output from one into the next.

So when you're using CBC, it's very, very, very difficult, more or less impossible to parallelize. So I think the only advantage you would get out of having multiple AES units is for simultaneously decrypting multiple streams.

Q. Did CA systems use AES in CBC mode?

A. The only times I've seen modes mentioned, it said CBC. Where there's always a question in my head is what they were doing with the scrambling circuits where you're not allowed to see it. And I think that changed at some point to shift so that -- I think now it is all AES CBC. I think. I don't know when that change happened, but it's either an

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0070
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

unknown descrambling that I don't know or an AES CBC that I do. Grab-333 also describes using AES and CBC mode.

CBC used to be the common one. It's kind of fallen out of favor now and we're kind of moving away from it a lot. But CBC used to kind of be the go-to mode of operation for AES.

Q. What are the other modes of AES?

A. So there's a couple. There was one called output feedback mode -- or no. OFB. Output -- yeah. Output feedback mode. No. Output -- OFB. I'm trying to remember what the B stood for. It was never super common.

The more common one that kind of started to be used more than CBC was counter mode. Counter mode is completely different. You would almost not recognize them as being the cryptographic operation, even though they both use AES.

And then nowadays we don't even use either of those. We use AES GCM is a common one. GCM stands for Galois. Okay, court reporter. G-L-O-I-S [sic]. Maybe there's an E. I think it's just S. Galois. G-A-L-O-I-S. Galois Counter Mode.

And Galois Counter Mode is very

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0071
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

interesting because it combines both the confidentiality doing the encryption with a message authentication code at the end. So it's called a combined mode of operation. Way, way, way better.

In TLS, for example, the new 1.3, they don't even have anything other than combined modes of operation. So that's Galois Counter Mode and CCM, which is -- I can't remember what it stands for. It kind of does something like cyber block chaining mode but it also involves a -- a authentication code at the end.

So the reason why counter mode gets a lot of attention is because counter mode can be parallelized in the -- in the original counter mode, it could be parallelized as long as you didn't need a message authentication code. And in the new version, the Galois Counter Mode, you still get some parallelization on both the encryption and the generation of the message authentication code at the end.

Q. Why is it that the counter mode can be parallelized?

A. It's really fascinating. Are you ready for having your mind blown? I don't know. It blew

my mind the first time I learned about it years ago.

Basically in counter mode you don't encrypt the data with AES directly. Okay. Instead, what you do is you take a counter, and for simplicity when we're teaching it we often just start at 0, but you actually pick a randomized starting point.

So let's say that we took the number 0, 16 bytes of 0, and encrypted it. We'd get some kind of -- it would look random on the output. And then if we encrypted 1, then we'd have another 16 bytes. And then we encrypt 2 and we have another 16 bytes, and we generate this stream. And then we XOR the plaintext with the output from the counterencryption to get the ciphertext.

So it turns out that when you XOR plaintext with random data, the output is random. And if you XOR plaintext with what's called pseudorandom where we encrypted a number but the encrypted output looks random, unless you have the key that was used you can't get anything out of the XOR data.

I don't know if that made sense or not, but hopefully --

Q. Let me see if I can try to understand and

walk through that. Okay. So in counter mode you have an index?

A. A starting number we -- yeah. Sure.

Q. Okay. And that index will increment for each block?

A. Yes. And you AES encrypt each of those numbers, which means you can parallelize because you know how many numbers you're going to need, or roughly. Right? Like if I'm encrypting five megabytes then I just -- I can -- I can have those numbers. Right? Like for each -- let's -- you used the term "AES unit," which I don't know that that's a technical term, but it's close enough. You've got some AES block cipher. Right?

So you take the starting number plus whatever block number we're on. Like let's say that you had 16 AES units. Okay. So the first time you want to parallelize, you put into the first one 0, into the second one 0 plus 1, into the next one 0 plus 3. You ram it all through and out comes out, in parallel, 16 times 16 bytes of key string.

And then you can XOR this with the plaintext and now you have -- and XOR is very fast, by the way. I mean, almost -- just incredibly fast.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0074
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

So now you XOR this data. We call it a key stream. It's a stream of what we call key material. And you XOR it with the plaintext and now you have that much plaintext encrypted.

Q. I see. You're calling this stream key material to distinguish it from the key?

A. Yes. So you still just have a regular AES key, and it's used on all of the AES units, using your terminology. But what we're doing is we're kind of like expanding the key. Right? We're generating a stream of key material that you can XOR with the plaintext.

Decryption, by the way, is also fascinating because you don't actually use AES in decrypt mode. It turns out with XOR that if you XOR something twice you get back the original. So you generate the exact, for decryption, you generate the exact same key stream.

Q. Uh-huh.

A. And then you XOR it with the ciphertext and out pops the plaintext.

Q. I see. So the key stream is material that you use with the XOR operation, but the encryption key is different. And that's one of the inputs to

the AES?

A. The AES unit. Yeah. The AES unit has to be configured with a key. So again, even if you're parallelizing, you're going to use the same key on each of those. But what you're -- so, again, you don't always start with zero. You'll start with a nonce or -- you should only use it once. So nonce stands for "number used once," I think is how they combine it together.

It's pretty easy to pick a random number when you're talking about 16 bytes. That's a lot of numbers. That's a lot of numbers. So you can pick a random one and you have that be your starting point. And then you just counter mode up from them.

Q. And when you're doing counter mode decryption, each of the blocks that you're decrypting, they can be decrypted independent from each other?

A. Correct.

Q. And you used some terminology. I want to back up to some basic terminology just to make sure we're on the same page on this.

A. Sure.

Q. And you may find some of these questions

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0076
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

to be super basic, but I just want to make sure that I understand this correctly.

So what is plaintext?

A. Plaintext is the term we use for the decrypted or original data.

Q. And then what is ciphertext?

A. Ciphertext is what we call the data after some encryption process or scrambling process has been applied.

Q. Okay. So encryption converts plaintext into ciphertext?

A. Yeah, or you decrypt ciphertext into plaintext. I mean, I know that there's technically the term decryption, but encryption generically covers the process of converting one to the other.

Q. Okay.

A. I mean, don't get me wrong. If I have ciphertext I say I decrypt it. Right? I don't say I encrypt it. I'm simply saying we talk about an encryption algorithm like AES, we don't -- I don't know why. I didn't write this stuff. We don't call it -- technically, we don't call it a decryption algorithm, although it is one. Right? It's just, I don't know, we're lazy. We just call it an

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0077
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encryption algorithm, and we know that AES can both encrypt and decrypt.

Q. I see. I'm going to share with you a document through the chat window, and let me know when you get it.

MS. SMITH: Is this a new exhibit that hasn't been marked?

MR. LIANG: Yes.

MS. SMITH: I'm going to object under 401, 402, 403, 801 and 802.

A. All right. I have it downloaded now. Let me open it up.

Q. Yeah. Let me know when you open it and you're looking at Page 1.

A. I got it. Okay. Yes.

(Exhibit 1014 was marked.)

Q. So I handed you, or sent you, what's been marked as Exhibit 1014. This is a set of diagrams that have been generated -- that I generated because I thought it might -- we might start discussing encryption today, it might be helpful to have some pictures to reference.

So on Page 1 we have four blocks of plaintext that are encrypted into four blocks of

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0078
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

ciphertext. Do you see that?

A. I do. I see the diagram.

Q. You see the diagram. Okay. And then on Page 2 we have the -- on Page 2 we have those four blocks of ciphertext being converted back into plaintext. Are you following me so far?

A. Yes.

Q. Okay. So then if we were running counter mode that you were just explaining, then I guess let's say the index that you were talking about for these blocks, for Block 1 could be -- the index could be 1, for Block 2 the index would be 2, Block 3 the index would be 3, and Block 4 the index would be 4. Is that fair?

A. Yes.

Q. Okay. So then if we go to Page 3, this is an example where Block 2 has now been lost. If we're using AES in counter mode, then is it correct that Blocks 1, 3, and 4 could still be decrypted?

A. It is if you assume you know which block number they are.

Q. Uh-huh.

A. If this were -- if, for example, in this chart you tried putting Block 3 in for Block 2

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0079
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

because you didn't know it had been lost, then everything would be wrong thereon after.

Q. Right. But if you know you last Block 2 you can decrypt the rest of the blocks?

A. If you know the block numbers you can decrypt each one individually, or counter mode.

Q. Or counter mode.

Now, I'd like to close this exhibit and go back to your declaration.

A. Which one?

Q. Exhibit 2024.

A. Sure. I have it.

Q. Paragraph 37. And partway -- halfway through, in parentheses, there is a sentence that says "Depending on the methodology, it is possible that the entire affected portion cannot be decrypted."

Do you see that line?

A. I do.

Q. So based on our conversation just now, it sounds like the methodology you're referring to would be something like CBC. Is that right?

A. Yes.

Q. And then in the previous sentence -- in

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0080
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

the previous sentence it says "Irrespective of which encryption methodology is implemented, when an unknown loss of data within an encrypted portion in Figure 5 occurs, the remainder of the affected portion cannot be decrypted on the receiving end."

And it seems to me that -- in that context, are you referring to encryption methodology as -- in terms of the algorithm like AES versus DES?

A. Well, I'm including counter mode here in terms of the methodology for how you encrypt. You'll notice in the sentence I say "an unknown loss of data," which we just -- I think we just talked about that, that if you have an unknown loss of data you can't finish decrypting it.

Q. And an unknown loss of data would happen if you lost a packet but you didn't know that you lost a packet?

A. Yeah, or how many or which number it was. I think I mention in my report that one of the reasons why TS stream is preferred is because the TS packets are numbered in such a way that you can detect when something is missing.

That's -- there is more of a complicated process of trying to figure out what's missing, for

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0081
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

example, if you had done some encryption at the PES level.

Q. You said before that CA systems do encrypt at the PES level. Right?

A. They can, and some standards allow for it.

Q. So then how do those systems figure out what's missing when they're encrypting at the PES level?

A. Yeah. So when they're encrypting at the PES level, this is, once again, why you try and do everything like you would do -- well, okay. So first of all, let's also be clear that there is no evidence I've seen anywhere that counter mode is used. All the evidence I've seen mentioned, whether it's in Grab, whether it's in documents, anything I've seen is all used CBC mode.

When you encrypt -- so there is also -- so there is a little bit -- again, I don't know when a shift happened. There was a time where it said the scrambling algorithm was proprietary. And then I've seen other documents that talk about using AES within the TS packets.

So when you're doing PES level encryption, but you do it the TS style, which is, once again,

that is so important that I mentioned earlier today that it says you encrypt the PES packets like you would encrypt the TS packets.

Then what happens is, you're going to treat each individual TS packet like its own individual encryption. So what I mean by that, when you use CBC mode with the TS packets, you start the -- you restart the CBC process with each TS packet. So if you lose a TS packet, it doesn't affect any of the subsequent ones.

When you encrypt at the PES level but you plug it in to the TS packet done the same way you would do TS, meaning you restart your CBC mode for that chunk of the PES chunk that's in that TS packet so that if that TS packet is lost it doesn't affect the rest of your PES level decryption.

Q. It sounds like what you're saying is if you encrypt at the PES level and you treat the chunks in the PES packet like they were individual TS packets, then it wouldn't actually be a more complicated process of trying to figure out what's missing when there is packet loss?

MS. SMITH: Object to form.

A. All the data --

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0083
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

(Simultaneous speaking.)

THE WITNESS: I'm sorry.

MS. SMITH: Object to form.

A. My other comment was about figuring out where the TS packet fits into the PES packet. What I am saying is all of the encrypted data in the encrypted chunk are all in the same packet so it's all lost together. Any other encrypted data that you get is going to be independent of that.

Q. I see. So in a CA system, if you're scrambling at the transport stream level, and you're scrambling the entire data portion of video, then if you lose one packet, then you lose that packet, but the rest of the video data in the other transport stream packets can still be decrypted?

A. Correct. And that also applies to the PES level as long as you follow the limitations that are put on by the standard. Meaning, you're largely going to treat it like TS -- in fact, the biggest reason why you would do PES level over TLS level isn't to give you any kind of different security apparatus or features or benefits. It's so that you can say in this stream I'm only going to encrypt the video, but not the audio. Right?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0084
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

It's so that you can have a little bit more granularity over what's encrypted. But you encrypt it pretty much using the same process. It allows you to have a single decoding chip, a single descrambling chip. And it allows you to have the benefits of the -- you know, you can tolerate a small amount of packet loss with negligible impact on the quality.

Q. And when you're encrypting at the PES level, then if you follow the limitation where you're encrypting the PES packet based on the size of the transport stream of packets, then --

A. Let me just interrupt you there, just to -- I think I can give an example that will clarify and answer your question.

Suppose we did cipher block chaining mode across the entire PES packet from beginning to end. Right? So we start at the beginning and we do 16 bytes, then 16 bytes all the way to the end.

If anything gets lost anywhere in the middle, you cannot decode, decrypt, descramble the rest after that point.

Q. Okay.

A. But if we follow the limitations that are

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0085
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

expressed, we're going to take a 184-byte chunk, we're going to stick it in the TS packet, and we're going to start CBC there and end it there. And then when we get the next 184-byte chunk, we will restart CBC for those 184 bytes, and then the next one will be independent, so that any lost data, it only -- there is no impact on decrypting the rest of the PES level encryption because it's still really being done at each TS packet's boundaries.

Q. I see. So if we follow those limitations that you described, then if at the transport stream layer you figure out that you've lost a packet, and even when you're decrypting at the PES level you know, hey, you know, I've lost this packet in the middle, but it doesn't matter because I can still decrypt the rest of the PES packet?

MS. SMITH: Object to form.

A. You don't even need to necessarily know that you've lost a packet. What you're saying is -- in fact, you're still going to be doing this more or less at the TS level, even though it's PES level encryption. So you get this TS packet. It's PES level encrypted, but you decrypt that 184 bytes independently and that gets put into the PES level.

And so if you lose one, it doesn't affect your ability to decrypt the next TS packet chunk.

Q. I see. So that's how CA systems implemented PES level encryption?

MS. SMITH: Objection; foundation. Objection; form.

A. That's how it's described in the standards. So I assume that's how they built their systems.

Oh, and -- I mean -- also just to be -- I mean, even there, just for clarity, like North American systems disallowed PES altogether. So I guess I should say some of the CA systems in some countries that did do PES encryption would have followed the standard, and I see no evidence to suggest that they didn't.

MR. LIANG: Okay. So I think we've been going for a little bit. Let's take a break and go off the record.

(Break.)

Q. Okay, Dr. Nielson. I'd like to -- I believe you said earlier you had a copy of Candelore Exhibit 1006 in front of you. If you could pull that up and let me know when you have it.

A. Yes, I have Candelore right here.

Q. Okay. Can we turn to Paragraph 38, please?

A. Yes, I have Paragraph 38.

Q. Okay. And it reads "EMM 250 may be used to deliver access rights (sometimes referred to as 'entitlements') 270 to digital device 115."

Do you see that?

A. I do.

Q. What is an access right in this context?

A. So EMM messages are basically -- they deliver capabilities to the set-top box or the receiver. Basically what its current subscription level is, I don't know, just different configurations for what you're allowed to view and so forth.

Q. Okay. And then an entitlement refers to an access right?

A. Yeah, they typically use the word "entitlement" in CA systems. I don't know why. That always struck me as a little funny, like we entitle you to watch some program of ours.

(Discussion off the written record.)

Q. Okay. And if we turn to Paragraph 39. Would you agree that Candelore teaches that the EMM

can contain multiple keys?

A. Well, it might be able to contain multiple keys. I've expressed in my report that all Candelore describes with service keys is one service key to one EMM message.

Q. If an EMM can contain multiple keys, but in your opinion only one of those keys is the service key, then what are the other keys that are in the EMM?

A. Well, they could be related to any number of things, including some of the elements that are listed in there, like certificates or whatever. I don't know what's in Candelore's mind. I can only speak to what's in the text.

Q. Okay. So I am sharing through the chat window a somewhat large file. So it is on its way. And let me know when you get it. This will be Exhibit 1015.

MR. LIANG: And for the court reporter, this will be a new exhibit.

(Exhibit 1015 was marked.)

A. Yes, I have it.

MS. SMITH: I'm going to object to the document under 401, 402, 403, 801, and 802.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0089
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Okay. Dr. Nielson, do you have Exhibit 1015 in front of you?

A. I do.

Q. Okay. Do you recognize Exhibit 1015?

A. I do. It appears to be an electronic copy of the book I wrote that we referenced earlier in the deposition.

Q. Okay. Now, if we could turn to Page 268 of the book, which has been stamped at the bottom with Page 0278. Let me know when you get there.

A. I have it.

Q. Okay. Now, this section begins a discussion of Kerberos.

A. Yes.

Q. What is Kerberos?

A. Kerberos was an early form of what we now kind of call single sign-on. Only when we think of single sign-on today, we think of single sign-on for like the internet. You sign in to Google or Facebook, and it allows you to serve in to other services that are -- worked-out agreements.

Kerberos was more of like your local network single sign-on, so that you could sign in to Kerberos, and once you were signed into Kerberos, you

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0090
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

could access the protected printer, the protected file system, protected resources of the network, the directory of employees, et cetera.

Q. On Page 0278, there's a sentence about the second paragraph of this section on Kerberos. At the end it says, "What's really cool about it is that, while extensions have been added to use PKI for certain components, the core algorithms all use symmetric cryptography."

What is symmetric cryptography?

A. Symmetric cryptography is any cryptographic operation where there is a single key used for an operation and its inverse. So if we're talking about encryption, a single key is used to both encrypt and decrypt. AES is an example of symmetric cryptography.

The opposite is, of course, asymmetric cryptography, where we talk about public keys and private keys, where you have to use two keys to do an inverse operation.

Q. So why is it cool that Kerberos uses symmetric encryption?

A. Well, the reason that we wanted to put this in there is that nowadays public key

infrastructure and the asymmetric algorithms are kind of seen as the way of doing certain kinds of operations, and we wanted to illustrate that this older -- well, I don't know that it's older. I guess they emerged at the same time. This less -- it used to be more popular. It's less well-known now. Technology solved some of the same problems of public key infrastructure using symmetric keys.

Q. What kind of problems are you referring to?

A. Well -- so let's go back to TLS that we talked about earlier. TLS is used when you make a network connection to a website. Right? So let's say that you're connecting to your bank. Most people, when they're using the internet, worry about whether or not their data is being kept secret, but they probably aren't always thinking about am I actually talking to the right website.

So it doesn't matter if all of your data is encrypted if you're talking to the --

MS. SMITH: Hello. Wait. Hello. Can you hear me? Hello.

THE WITNESS: We can hear you.

(Discussion off the written record.)

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0092
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. So when you connect to your bank, you'd really like to not have connected to the mob or some foreign, you know, hacker group pretending to be your bank. Right?

And so one of the things that happens when you do a TLS connection is there's a certificate exchange, where the website basically has to prove that it's the website that it claims to be. And we use what's called the public key infrastructure for this, where when you get the certificate from the bank, they both prove that they're the owner of that certificate, but your browser has to check a higher-level certificate from what's called a certificate authority. We call those CAs, by the way. So I'll work really hard to make sure we don't overload our terminology here.

But when you get your higher-level certificate from the certificate authority, it's able to verify that this is a valid certificate for the valid party and that you know you're connecting to the bank.

In Kerberos, they're basically similar kind of issues where you might have two parties that want to communicate with each other. They need to

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0093
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

know that they're communicating with the right party. They need a session key between themselves, but instead of using certificates and public keys, we use standard -- not standard but we use just symmetric encryption to achieve the same result. And -- and instead of having a certificate, you use a -- the trusted third party. So there is a trusted third party that you -- that both -- both sides have to trust and then they're able to set up a trusted communication stream between each other. That's analogous to when you're connecting to your bank, the trusted third party is the certificate authority that is enabling you to trust that the bank is who they say they are.

Q. Does that mean that symmetric encryption isn't really used anymore?

A. Oh, no, no, no, no, that's not what I'm saying at all. In fact, in TLS after you do the certificate exchange and all the asymmetric keys, then you switch over and start using symmetric keys. So it's still used a lot. It's just not always used for authentication, which in the Kerberos case it is and so that was kind of the cool feature.

Q. So in TLS, if you're using asymmetric

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0094
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

encryption at the beginning, why not just keep using it to encrypt all the content, too?

A. Oh, that's terrible. Don't ever do that. If you were my student, I'd smack your hand a little bit.

So the reason is asymmetric encryption is not meant for bulk encryption, is the term we use. It's not meant for bulk encryption. It's not fast. First of all, it's just not fast. So let's start with that one.

RSA -- well, okay. Actually, there is a number of problems. Which one first?

Let's go with slow first. So RSA can encrypt data really slow. Compared to AES, it's just -- I mean, it's hardly comparable. You don't encrypt large data with it. That's not what its purpose is. So it's slow.

The other problem is that it's not even really adapted -- like we talked about cipher block chaining mode, there really isn't even a mode of operation like that for RSA. I think the biggest you can encrypt is the key size. So if you're using 2048-bit RSA, you can encrypt 2K and that's it. Right.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0095
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

So it's really not meant for bulk encryption. And, in fact, what we're using it in TLS isn't for encryption. It's actually for authentication. We call it entity authentication. We're using it as a mechanism of authenticating that we're talking to the right party.

The other problem I was going to mention that popped into my head just now is most of the asymmetric algorithms don't even do encryption at all. In fact, I think as far as I'm aware, RSA is the only one. The others can sign. They can do signatures. There's key exchange. There's a couple of other things, but I think except for RSA, none of the others can even encrypt at all. So you just don't use it for encrypting the data.

Q. I see. And just to be clear, RSA is a public key asymmetric algorithm?

A. Yeah, it's -- it's kind of the maybe most well-known. It's -- it used to be the most widely used. Now it's kind of fallen out of favor but a very well-known algorithm.

Q. I see. I think -- and I did -- I did read or at least skim through your book and I think you explain something like this earlier in the book. Let

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0096
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

me see if I can find it. One second.

Okay. I see. So Page 217 of your book, which has been stamped 0227. If you could turn there, please, and let me know when you're there.

A. I have it.

Q. Okay. So in this section which is titled, "Asymmetric and Symmetric: Like Chocolate and Peanut Butter," is this basically describing the concepts that you were explaining just now?

A. Well, it's also talking about how you use them together. So one of the things that you -- like in TLS, the initial handshake is all about being able to create on the fly a new symmetric key that's going to be used for the communications of that session. And so the idea is that you use the PKI, the public key infrastructure, to establish that I know I'm talking to the correct party. I know who you are. Everything's good there. Let's exchange a key and then we'll switch over to symmetric encryption for all of the bulk transport. That's what this section kind of gets into.

Q. I see.

A. My coauthor helped titled these sections. So, "Like Chocolate and Peanut Butter," that was

Chris' idea.

Q. It's a great combo.

Okay. And then in this third paragraph on this Page 0227, it says, "We first introduced the term session key in Chapter 4."

So the session key is the key you're referring to that gets negotiated and then used for symmetric key encryption?

A. Right. Correct. It's created as part of this. So it's temporary. You'll use it for this session and then never use it again.

Q. And it looks to me like the next two paragraphs, it looks like there's two sort of different examples. One of them explains on the receiving end the session keys are decrypted using the recipient's private key. So this paragraph seems to be describing an example where, you know, the session key is encrypted and sent over and then decrypted. Is that -- is that right?

A. Yeah. So -- so, as I said, RSA was one of the few that could actually encrypt data and so the way this was generated on the fly is you would have one side generate kind of a precursor -- we simplify down here and just say we're sending the session key,

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0098
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

but it's actually like a -- it's actually a prekey. But what happens is you have the one side -- so when your browser connects to the bank, the bank sends it a certificate. The certificate has a public key. If it's RSA, your browser can take -- it can generate on the fly a proto key like it's -- you'll see in a minute it's like a predecessor and then it can encrypt it with the RSA public key.

Once it's encrypted with the RSA public key, only the owner of the private key can decrypt it. And so then you send this proto key -- it's actually called the premaster secret. You send it over to the other side. The other side has the private key. They are the only party that can decrypt what you sent them. You can't even decrypt it again. You only have the public key. Right? But you already have it. So you've got it. They decrypt it. Now, you both have this pre-secret which you then use to derive -- there is actually multiple keys that are used in the bidirectional communication, and from that pre-secret, you derive the others.

Q. I see. And that's in this next paragraph. It says you can also derive symmetric keys from a base secret using key derivation functions. And

that's what you were describing here -- what you were just describing?

A. No, no, no. It's a little bit of overloaded terminology. There's derivation both ways, but there's a special thing we call the key derivation function and that's Diffie-Hellman is the most popular one, DH. You'll sometimes see an elliptic curve version, ECDH.

And what happens there -- it's also a public key/private key operation, but that's not super important for this part of the conversation. What happens is both sides send over some data that -- talking about having your mind blown. This -- this whole thing is like magic. Both sides can send over this -- these components and they can then on both sides derive the same key, but nobody else even listening to both of those messages get sent can.

So, like, if we were doing it in realtime here in this video chat, if -- if you had a Diffie-Hellman setup and I had a Diffie-Hellman setup, you and I could both send some data in the chat window. We could copy it down into our program. We could derive a key that you and I would now share

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0100
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

that nobody else listening in, the court reporter or Bridget would be able to derive the key, so now you and I would be able to exchange messages confidentially.

But in both cases, whether you send it over ahead of time using RSA encryption or you derive it using a KDF like -- oh, sorry, a key derivation function like Diffie-Hellman, either way -- I shouldn't call it that. We usually use key derivation separately. I'm going to strike that. Let me try again.

Using a key agreement protocol like Diffie-Hellman, you end up with the premaster secret. Whether you transmitted it or you -- you created it on the fly in key agreement, you then derive your session keys from that premaster secret.

Q. So asymmetric encryption is used so that both sides arrive at a shared secret and then that shared secret is used by both sides to derive the encryption keys. Is that right?

A. Encryption, message authentication code. There is multiple keys.

Q. How does deriving a key differ from decrypting a key?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0101
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. So those are actually two completely different things. So let me see if I can explain.

The decryption of the key is so that both sides have a shared secret. So one side generates the secret, encrypts it using the public key, knows that only the owner with the private key can decrypt it. Therefore, only the owner will now share with them the secret they generated. Okay? That's the starting point.

Key derivation is similar, not the same, but similar to what we talked about earlier in AES where we generate a key stream. The idea is that you plug your secret into a function that generates additional what appears to be random data. So we call it a key block. And so what happens is, you get this big chunk of data and you literally just cut off, okay, I need 16 bytes for a key, I'll take the first 16 bytes for this encryption key and the next 16 bytes for this encryption key and the next 16 bytes for the authentication code key and you just divide it up however many pieces you need for whatever cryptographic algorithm, symmetric algorithms you've agreed on as part of the handshake.

One thing to clarify. I'm using TLS as my

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0102
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

example here. Right? There are other ways that you could potentially -- you could just take the shared secret and turn it into a key. Right?

In TLS, you -- you do this -- this derivation foundation to have the key block to have multiple keys for the session.

Q. I see. So you -- you could just use asymmetric encryption to encrypt a key, send it over, and the other party decrypts it and both of you just use it, or alternatively, you could use this kind of key derivation process that you've just explained?

A. And the reason why -- it depends on what you're going to do. All of these things depend on what it is that you're trying to do. If you're going to have bidirectional communication, you're going to need multiple keys. You don't use the same key in both directions -- well, what I mean is you're going to have two keys on both sides and the encrypt key on one side will be the decrypt key on the other side, but you don't use the same key for both -- on both sides. Right?

If you're going to have bidirectional communication, you pretty much need to derive some -- some subkeys. I don't like using subkey. What's a

better term? Derive some purpose keys for these different purposes. Right?

Q. Uh-huh.

A. If all you need is for them to have -- well, I mean like -- maybe like we're talking about with our EMMs like a work key that is going to be a long-term key that is actually probably used for derivating other keys, then, yeah, you can just send that and that key becomes the work key and you're done.

MS. SMITH: Object to form on the previous question.

Q. I'm going to go back to Kerberos and figure out how Kerberos does some of this stuff. So if we go back to the page that was stamped 0278.

A. What page in the book was that again?

Q. 268.

A. Okay. I've got it.

Q. So in this chapter I think you described some of the basic components of Kerberos to provide an introduction into how Kerberos works. Right?

A. Yes.

Q. But the examples in this chapter, they don't describe the full Kerberos protocol, do they?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0104
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. No, they don't. They are a simplified form to teach some of the principles.

Q. So then, for example, some of the messages described in the book may have additional components that aren't actually discussed in the book?

A. Absolutely. Yeah. These are not -- no, this is a -- this is a Kerberos-like exercise. This is not Kerberos. That's more complicated.

Q. If we go to the next page. How does a user log in to Kerberos?

A. Yeah, so the -- again, the kind of simplified concept is that Kerberos has an authentication server. Sometimes just abbreviated AS. And it already has to know you. So it's a trusted third party, it has to have your login credentials already in the system.

Typically the way this works is something like Alice sends -- Alice. I'm sorry. I should use terminology.

In cryptography it's very common for us to talk about party A and party B, just generic parties, and then we give them names. A is Alice, B is Bob, C is Charlie and so forth. So if I say Alice, I'm simply talking about the first user in this

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0105
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

description. So Alice wants to sign in to the Kerberos system. Alice sends a message to Kerberos that can be as simple as "I'm Alice, I'd like to log in."

Kerberos can -- Kerberos already knows her password that was put in as part of her registration in the system. It is, by the way, one of the potential weak points of Kerberos, is that if the AS is compromised, everybody's information is compromised. But you have to put your trust somewhere. In Kerberos, it's in this system.

So what will happen is Kerberos will take the user's password, use the password to derive a key. There are key derivation functions where you put in just plaintext and out comes however many bytes you need to have a key for AES or whatever. And then Kerberos will create a message that it sends back to Alice that is encrypted with this password -- key derived from the password.

So if Alice actually has the password, right, if she's really Alice and not somebody pretending to be Alice, then using the password, Alice is able to derive the same key and able to decrypt the incoming data.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0106
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

When you say "log on," this is kind of like the first step. Log on is a little bit complicated with Kerberos, but I figure let's go this far and then we can keep going if you like.

Q. Sure. If you go to Page 271, which I think is stamped 0281, I think there are some examples that explain this protocol you're describing. Let me know when you get there.

A. I have the page.

Q. So if we can start with this first example that says a user can log in just by sending their name using our protocol notation, here is how Alice logs in to the authentication server.

Can you explain what the A, arrow, AS:A means?

A. This is protocol notation so -- and actually, it's explained. I think I was just looking over it. It's explained a few pages up.

Arrow here -- and for the court reporter, it's an arrow facing right. Arrow here represents intent. A intends to send a message to AS.

We say intends because we're assuming that in this world messages can be intercepted or otherwise blocked. But we're just going to say A

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0107
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

intends to send a message to the authentication server. After the colon is the actual message.

And in this case, it's just A, meaning A's identity. So this would be Alice's name or her login name or user name or something like that.

Q. I think you said earlier AS is the authentication server. Right?

A. Yes.

Q. Okay. So in response, what does the authentication server send back?

A. So the authentication server, as you can see on the -- it's a few lines down, there's another protocol message. You can see AS, right arrow, A. This means the authentication server intends to send a message to Alice. After the colon we have braces. Inside the braces it has K_ -- not_. What's the -- subscript. K subscript session. The word "session."

And that's inside braces. The whole case of subscript session is inside braces. And outside of the braces it says K subscript A. What this means is we've got a session key, that's the K session, and it is encrypted. The braces mean the data in the braces are encrypted. And the KA outside tell you what key the data is encrypted under.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0108
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. This response is also called the Kerberos ticket. Right?

A. I -- this isn't the full ticket. Let me see. Because I believe what happens next is we have to use the session key to get the ticket. I want to see where that's described here.

Yeah. So if we go down to -- it's Page 276. It's stamped as 0286. You'll notice as you're going through these pages that I kind of update the messages as we go along, because there's more data that goes into them, some time stamps and some other things like that.

So what we have here at the bottom of 276 is an updated version of this messages where we send down -- we get -- we get the K session encrypted under KA as well as what is called the ticket granting ticket. So the ticket granting ticket is what you use to connect to the ticket granting server -- service and get -- and get other tickets to the services you want to access.

MR. LIANG: Let's go off the record.

(Break.)

Q. So we're back on the record. So I want to

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0109
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

follow up with a few more questions about this exhibit, 1015, that we were looking at before the break for lunch.

A. Sure.

Q. So we were talking about Kerberos, looking at Page 0286 of this book, and it looks here like the authentication server sends a session key that's encrypted with KA. Is that right?

A. That's correct, yes.

Q. And KA is a key that's derived from the user's password?

A. Yes.

Q. So then the key that encrypts the session key would be considered key encrypting key. Correct?

A. Sure. Uh-huh.

Q. The authentication server generates a Kerberos ticket and in that ticket there is information such as a session key, assigned expiration time, random number from the request, and name of the verifier. And all of this information is encrypted with a key derived from the user's password. Correct?

A. That sounds right. I don't think I have the more expanded version here in front of me. But

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0110
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

that sounds correct.

Now, you're calling it a Kerberos ticket. There's -- I just want to clarify there's two separate steps here, and it is covered in the book. You first have the authentication server that you just are getting identified from, and then secondly -- separately there is a ticket granting service.

And so in my text what I'm calling the Kerberos ticket is what is sent back from the ticket granting server.

Generically these messages are tickets, but what I'm calling the Kerberos ticket is on Page 282 of my book, or 0292, that is what's coming back from the ticket granting server.

(Exhibit 1016 was marked.)

Q. I see. I'm going to share with you Exhibit 1016, which I've put in the chat window. If you can open it and let me know when you have it open.

MS. SMITH: Object under 401, 402, 403, 801 and 802.

A. Yes, I have this in front of me.

Q. Do you recognize Exhibit 1016?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0111
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. I mean, not immediately, but it appears to be a declaration of mine in a previous IPR matter.

Q. If you look at the very last page, Page 77, is that your signature that appears there?

A. Yes.

Q. I'd like to turn to Page 51 of this Exhibit 1016. Let me know when you get there.

A. Yes. I have Page 51.

Q. So is it correct that the authentication server generates a Kerberos ticket that returns information such as the session key, the assigned expiration time, the random number of the request, the name of the verifier, which are all encrypted with the user's password registered with the authentication server?

A. Well, I mean, I say here in this declaration that Neuman teaches that. I'd have to see if that's the way Neuman described it. That sounds fine. I mean, like I said, these are all generically tickets.

And in a lot of cases the authentication server and the TGS are co-located, so I'm not sure if I was simplifying here or not, but typically the ticket is what comes from the ticket granting server.

Q. This description you have on Paragraph 100 of Exhibit 1016 sounds accurate to you?

A. It's -- it's reasonable.

Q. I'd like to close Exhibit 1016 and turn to Exhibit 2009. I think you have the printed copy if you want to go pull it up.

A. Which reference is that?

Q. That's your first declaration.

A. Got you.

Q. Let me know when you have it.

A. I have it.

Q. If we can turn to Page 12, please?

A. Sure. I've got it.

Q. This section explains the legal principles you applied in forming your opinions in this case. Right?

A. Yes.

Q. And I think this -- your second declaration doesn't actually have a legal principles section, but would it be fair to assume that you applied the same legal principles in your first declaration that are listed here in Exhibit 2009 and also in your second declaration, which is Exhibit 2024?

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0113
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. Yes. If there are no additional principles listed there, then these would have been the ones I was relying on.

Q. Can you take a look at Exhibit 2024 and let me know if there are additional legal principles?

A. (Pause.)

I don't see any.

Q. Okay. If we can turn to Page 15, please. There's a Section C, Obviousness, Paragraphs 35 through 38. Let me know when you get there.

A. I have that.

Q. Are Paragraphs 35 through 38 the legal principles you applied when forming your opinions on obviousness in this matter?

A. Yes.

Q. Did you apply any other legal principles that are not listed here in Paragraphs 35 through 38 regarding obviousness?

A. I can't think off the top of my head of anything else that I applied. But if I did it would have been written down. I don't have anything that's not written down.

Q. And can you point me to any portions of your declaration, either first or second, where you

disclose an opinion regarding obviousness relying on a legal principle that is not described in Paragraph 35 through 38?

MS. SMITH: Object to form.

A. I don't know off the top of my head. If there is a paragraph or citation you'd like me to look at, I'm happy to review it. I wasn't trying to hide any legal principles. If something is written down somewhere, I don't remember it, I'm happy to review it and tell you what I see there.

Q. Have you ever heard of the U.S. Supreme Court's KSR decision?

A. I have heard of KSR before.

Q. Are you aware of the obviousness rationale as described in KSR?

A. Obviously I am not an attorney and would not dare try to provide a legal opinion on what they mean, but I have seen them before and I'm sure I've cited them before in other reports that I've written.

Q. Sure. And, for example, are you aware of a rationale where the combination of familiar elements according to known methods is likely obvious when it does no more than deal with predictable results?

MS. SMITH: Object to form.

A. That sounds familiar.

Q. And are you aware of a rationale where substituting one known element for another to obtain -- regarding substituting one known element for another to obtain predictable results?

A. That also sounds familiar. I don't know if that's the exact language, but that sounds like the type of analysis that I've done.

Q. Okay. So you've analyzed those factors in previous cases where you've provided opinions. Right?

A. Yes.

Q. Okay. And have you disclosed any opinions in this matter where you've analyzed either of those KSR rationales?

A. Well, I think in the places where I analyzed obviousness I reached conclusions that it was not obvious at more fundamental grounds and so never reached those. Just as an example, we talked earlier today about incompatibility. Actually, on incompatibility I'm not going to try substitution when it's incompatible.

Q. So I guess I'm asking you, maybe we can

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0116
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

break this up, for whether you've disclosed any opinions in this case, in your -- in this matter with either your first or second declaration where you analyze the KSR rationale regarding the combination of familiar elements according to known methods for the '920 patent?

MS. SMITH: Object to form.

A. I don't think that I --

THE WITNESS: I'm sorry.

A. I don't believe I have anywhere in my report where I use those words. But I think my analysis would apply to those kind of evaluations.

Q. Is it your understanding that in conducting an obviousness analysis a precise teaching directed to the specific subject matter of the challenged claim need not be sought out because it is appropriate to take into account the inferences and creative steps that a person of ordinary skill in the art would employ?

MS. SMITH: Object to form.

A. I don't know if that's the entire text. I assume that it is of some standard that you're quoting from KSR. I -- I'm not sure if that's -- that's it, but I certainly understand that there is a

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0117
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

certain amount of creative processes that a person of ordinary skill in the art can do in a combination.

Q. Right. And under the KSR obviousness standard common sense is important and should be considered. Is that your understanding?

A. I believe I have used that before, yes.

Q. Have you disclosed any opinions in this matter, in either your first or second declaration, where you've analyzed the inferences and creative steps that a person of ordinary skill in the art would employ?

MS. SMITH: Object to form.

A. I have not used those words, no. But I think you can see that my analysis kind of goes at that kind of issue.

Q. Okay. So can you point me to a specific opinion in your declaration where you analyze the inferences and creative steps that a person of ordinary skill in the art would employ?

A. Sure. So I think we've already seen a little bit of this today. I'm in my first report, which is Exhibit 2009. Let me find a representative paragraph here.

(Pause.)

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0118
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

All right. Let's use Paragraph 82 as an example. The first two sentences I think get at exactly this issue. Do you want me to read those two sentences?

Q. Sure.

A. "First, the two technologies are different; one cannot optimize the other because they are different technologies, with different purposes, and different security profiles. Again, a frame and a transport stream packet are not the same thing and the combination is nonsensical."

Q. And where -- where in Paragraph 82 do you describe the creative steps that a person of ordinary skill in the art would employ?

A. Well, I guess what I'm saying is you --

MS. SMITH: Object to --

THE WITNESS: Sorry.

MS. SMITH: Object to form.

You can go ahead and answer.

A. Well, what I'm saying here is there isn't a creative steps to do because the two things don't fit together. The two things don't -- there isn't a creative set of steps to do in the inbetween.

Q. In the 2005 to 2006 time frame -- well,

actually, let me -- withdrawn.

Let me just -- you know, we've been using the phrase "person of ordinary skill in the art," and it's kind of a mouthful. So, you know, some -- in your report you've referred to this phrase, POSITA. That's capital -- all capitals, P-O-S-I-T-A. Does that stand for person of ordinary skill in the art?

A. It does.

Q. Okay. So I guess in this deposition if we refer to the POSITA, that's what we're going to be talking about. All right?

A. Yeah.

Q. Okay. So in the 2005 to 2006 time frame, would a POSITA have been able to compress and decompress video?

A. Yes.

Q. Would a POSITA have been able to use MPEG video standards?

MS. SMITH: Object to form.

A. I'm sorry. Could you -- can we be a little bit more specific? When you say "use them," are you just meaning can they implement what's described in the standards?

Q. Sure.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0120
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

A. Yeah.

Q. In the 2005 to 2006 time frame, would a POSITA have been able to encrypt and decrypt data?

A. Yes. Assuming we've got the appropriate context. Like we've talked about a couple of times today, encrypt and decrypt is very broad. That's a really broad umbrella. So I would assume that when we say a POSITA can encrypt and decrypt, they're capable of following the instructions to apply the cryptography in the context in which it's described by a standard or a -- or some other kind of guide.

I doubt a POSITA would be able to whip up their own encryption protocol or know how to correctly move from one context to another without significant security issues.

Q. Right. So AES and DES were both known in the art by that time. Right?

A. They were.

Q. So a POSITA would have known how to use AES with known operating modes to encrypt and decrypt data?

A. Again, following a guide on the correct parameters, sure.

Q. Right. And for the guides you're

referring to, those were known in the art. Right?

A. Right. I'm just saying it's not like the POSITA knows how to go apply an encryption protocol that's designed for one context into another context for which there is no guide.

Q. Wouldn't that fall into some of the types of creative inferences that a POSITA would be able to do?

A. No, certainly not for encryption. Absolutely not. That's where -- that's where half of the vulnerabilities came from people thinking they knew how to do something when they didn't.

Q. But in terms of these guides that you're referring to, would it be fair to say that there were many such guides on how to use encryption such as AES in the art by 2005, 2006?

A. Well -- so if we have a standard like MPEG that says use AES, this mode, this set of parameters from here to here, one of skill in the art can do that.

Q. But one of skill in the art would not be able to deviate from that standard. Right?

A. Not successfully. I -- that's kind of, I guess, the whole point of the Crypto Done Right

project that we talked about earlier. Is that most people, programmers, IT people, people working with these kind of things, unless they've got cryptography training, applied cryptography training, no, I would not trust them to make those creative steps and have it be successful.

Q. But if there is a reference in the art that does teach you, hey, use cryptography in this way, then by 2005-2006 a POSITA would have been able to follow that?

A. Yes.

MS. SMITH: Object to form.

A. Yes. If there is a guide and the guide is applicable to the situation that they're working with, sure.

Q. And we talked quite a while earlier about symmetric key cryptography. So by the 2005-2006 time frame, would a POSITA have been able to apply known symmetric key cryptography algorithms?

A. So, I mean, I guess my answer is the same. Actually, while we have my book open, I have an entire section in there called "You are not a cryptographer."

I don't know if you saw that section. But

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0123
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

I'm pretty forceful. You don't go messing around with cryptography. Just follow the recipes and do what you're told because you're not a cryptographer. So can somebody follow a guide and implement the cryptography the way specified? Yes. Should they be out trying to figure out where it works and how it works and if it will work? No.

Q. Would a POSITA in the 2005 to 2006 time frame have been able to partially encrypt video frames?

MS. SMITH: Object to form.

A. Well, I guess the Grab reference describes doing that at a certain level of abstraction.

Q. Okay. So you agree that the '920 patent does not invent partial encryption for video?

A. I don't think I ever stated that. I don't think that is an opinion I've expressed in my report.

Q. Well, let me ask you, do you believe that the '920 patent invents partial encryption of video?

MS. SMITH: Object to form.

A. Well, I think the safest way to say that is it invents what's claimed, and the claim limitations have a number of steps, and I believe that is what is the invention.

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0124
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

Q. Partial encryption of video was known before the '920 patent. Right?

MS. SMITH: Object to form.

A. I believe so. Again, at certain levels of abstraction. I'm not saying that it is prior art to the '920.

Q. What do you mean that -- so -- what do you mean by -- that you're not saying that -- well, let me ask it this way. Withdrawn.

Partial encryption of video was taught by various prior art references before the '920 patent. Do you agree with that?

MS. SMITH: Object to form.

A. Right. There are differences that describe what I think you could call partial frame encryption. All I was saying is that I'm not aware of anything that has the steps described in the claims of the '920 patent.

Q. In the 2005 to 2006 time frame would a POSITA have been able to use key ladders to distribute keys?

MS. SMITH: Object to form.

A. So key ladders are almost always used in the context. That specific name -- not the concept,

but that specific name is almost always used in conditional access systems. So key ladders have been used in conditional access systems, I believe, since the beginning.

Q. When is the beginning?

A. I think there was an introduction of some of the concepts. Oh, what was that date of that ITU -- I don't know. It's not one of the things that I've relied on. I'm just aware of -- so I don't know for absolute certain. I don't know. I'd have to look up and find out.

Q. Well, roughly it's -- is it in the '90s or before?

A. It's at least by the '90s.

Q. And by the 2005 to 2006 time frame would a POSITA have been able to use key hierarchies to distribute keys?

MS. SMITH: Object to form.

A. Once again, within a proper recipe guide, sure.

Q. And there were such recipe guides that existed in the art by 2005 to 2006?

A. Right. Like TLS doesn't use a three level. You could say -- well, I mean, with the

certificates you might say it's multi- -- three level. So, you know, that's an example of one way of doing it. You know, I'm pointing out that there is a lot of different ways of doing it. You'd have to follow the recipe.

Q. Do you have a copy of the '920 patent in front of you?

A. I do.

Q. If you could turn to Claim 2, please, and let me know when you get there.

A. Claim 2?

Q. Yeah.

A. I have Claim 2.

Q. Okay. Now, you see Claim 2 recites "The encrypted copies of the content encryption key are entries in the table." Do you see that?

A. I do.

Q. What is the antecedent basis for the phrase "the encrypted copies of the content encryption key"?

A. So I guess that would be here in Claim 1. Obtaining one or more copies of the content encryption key that are encrypted using one or more user encryption keys, including an active user

encryption key stored on the playback device.

Q. So I am sharing with you a document, 1017, through the chat. Let me know when you've opened it.

(Exhibit 1017 was marked.)

MS. SMITH: I'm going to object under 401, 402, 403, 801, 802.

A. Okay. I have it.

Q. I've handed you what's been marked as Exhibit 1017, which is a copy of DivX's infringement contentions for Claim 2 of the '920 patent. If I can direct you to the first page stamped 0001.

At the bottom of the page it explains that, "Within the MSL framework, the encrypted copy of the content encryption key is an entry, e.g. the returned 'Payload,' in the JSON structure, which is a key-value table. Thus, the encrypted copy of the content encryption key is an entry in a table."

Do you see that?

A. I see that language here.

Q. Okay. And in this sentence DivX points to a single encrypted copy of the content encryption key. Is that right?

A. I mean, I haven't seen this before. The language says "the encrypted copy." So, I mean,

that's what it says here in the text, but I'm not prepared to opine on this document.

Q. Okay. And if we turn to the -- and I think we just -- and as you just explained, the antecedent basis for the encrypted copies of the content encryption key for -- in Claim 2 refers back to a limitation in Claim 1 describing one or more copies of the content encryption key. Right?

A. Right.

Q. Okay. If we can turn to the next page of Exhibit 1017, you see there is a discussion of payload chunks. Right? Do you see that?

A. I see that section.

Q. Okay. And have you ever seen -- actually, let's go to the next page, Page 003. And you see there's the full sentence. It says "The encrypted copy of the content encryption key is returned as an MSL payload as shown from the network traffic during playback of Keith Richards: Under the Influence." Do you see that?

A. I see that language.

Q. Okay. So here again DivX is pointing to a single encrypted copy of the content encryption key. Is that right?

A. I'm only able to read what it says. I don't have any additional input to offer.

Q. Is DivX correct that Claim 2 is satisfied when only one copy of the content encryption key is an entry in the table?

MS. SMITH: Objection; form.

Q. Let me re-ask the question.

Is DivX correct that Claim 2 is satisfied when one copy of the content encryption key is an entry in the table?

MS. SMITH: Objection to form.

(Reporter admonishment.)

MS. SMITH: I'm also going to object as outside the scope of the declaration.

A. (Pause.)

Q. Is DivX correct that Claim 2 of the '920 patent is satisfied when only one copy of the content encryption key is an entry in the table?

MS. SMITH: Same objections.

A. So I can't speak to Netflix -- I'm sorry, not Netflix, DivX -- in any of the other litigations they're involved in. For purposes of my evaluation here, I have interpreted Claim 2 to require that there are multiple copies in a table.

MS. SMITH: Just so the record is clear before you continue, Mr. Liang.

Court Reporter, when -- I know that you're probably going to clear this up later, but it said "same objection." It was "same objections." I had two objections to the last question. So, please continue.

Q. Why does Claim 2 require multiple copies of the content encryption key?

A. Well, the language of the claim reads "Wherein the encrypted copies of the content encryption key are entries in a table."

It's all in the plural.

Q. Okay. So in your view, a person of ordinary skill in the art would have interpreted Claim 2 to require multiple copies of the content encryption key to the entries in a table?

A. That is how I interpreted it.

Q. And in your opinion is that how a person of ordinary skill in the art would have interpreted Claim 2?

MS. SMITH: Object to form, and outside the scope of declaration.

A. For the analysis that I did in my report,

that is what I interpreted one of ordinary skill in the art to understand.

MR. LIANG: Okay. Thanks. I'll pass the witness.

MS. SMITH: I have no redirect.

(Deposition concluded at 3:17 p.m.)

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0132
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

NETFLIX, INC. AND HULU, LLC,	§	
	§	CASE NO. IPR2020-00052
PETITIONERS,	§	
	§	U.S. PATENT NO.
V.	§	8,139,651
	§	
DIVX, LLC,	§	
	§	
PATENT OWNER.	§	

REPORTER'S CERTIFICATION
DEPOSITION OF SETH NIELSON
TAKEN JANUARY 13, 2021

I, TAMARA CHAPMAN, Certified Shorthand Reporter in and for the State of Texas, hereby certify to the following:

That the witness, SETH NIELSON, was duly sworn by the officer and that the transcript of the oral deposition is a true record of the testimony given by the witness;

That the original deposition was delivered to JEFFREY LIANG;

That a copy of this certificate was served on all parties and/or the witness shown herein on January 26, 2021.

I further certify that pursuant to FRCP No. 30(f)(i) that the signature of the deponent:

was requested by the deponent or a party

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0133
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

before the completion of the deposition and that the signature is to be returned within 30 days from date of receipt of the transcript. If returned, the attached Changes and Signature Page contains any changes and the reasons therefor;

X was not requested by the deponent or a party before the completion of the deposition.

I further certify that I am neither counsel for, related to, nor employed by any of the parties in the action in which this proceeding was taken, and further that I am not financially or otherwise interested in the outcome of the action.

Certified to by me this 21st day of January, 2021.

Tamara Chapman, CSR, RPR-CRR
CSR NO. 7248; Expiration Date: 12-31-22
TSG Reporting, Inc.
Firm Registration No. 615
Nationwide - Worldwide
Phone: (877) 702-9580
info@tsgreporting.com
www.tsgreporting.com

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0134
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)

ERRATA SHEET

Case Name:

Deposition Date:

Deponent:

Pg.	No.	Now Reads	Should Read	Reason
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____

_____

Signature of Deponent

SUBSCRIBED AND SWORN BEFORE ME

THIS ____ DAY OF _____, 2020.

_____

(Notary Public) MY COMMISSION EXPIRES:_____

Netflix, Inc. and Hulu, LLC - Ex. 1024, Page 0135
IPR2020-00558 (Netflix, Inc. and Hulu, LLC v. DivX, LLC)