IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE KIMBERLY J. MUELLER, JUDGE

---o0o---

UNITED STATES OF AMERICA,

Plaintiff,

vs.

No. 2:13-CR-00082

MATTHEW KEYS,

Volume 4
Pages 305 through 470

Defendant.
____________________________________/

---o0o---

REPORTER'S TRANSCRIPT OF PROCEEDINGS

JURY TRIAL

VOLUME 4

THURSDAY, OCTOBER 1, 2015, 8:30 A.M.

---o0o---

For the Government:

BENJAMIN B. WAGNER, U.S. ATTORNEY
501 I Street, Suite 10-100
Sacramento, California 95814
BY: MATTHEW DEAN SEGAL
and PAUL ANDREW HEMESATH
Assistant United States Attorneys

(Appearances continued next page...)

Reported by:

KATHY L. SWINHART, CSR #10150
Official Court Reporter, 916-446-1347
501 I Street, Room 4-200
Sacramento, California 95814

Proceedings reported by mechanical stenography,
transcript produced by computer-aided transcription.

APPEARANCES (Continued)

For the Government:

UNITED STATES DEPARTMENT OF JUSTICE
Computer Crime and Intellectual
Property Section
1301 New York Avenue NW, Suite 600
Washington, D.C. 20530
BY: JAMES ANTHONY SILVER
Deputy Chief

For the Defendant:

LAW OFFICES OF JAY LEIDERMAN
5740 Ralston Street, Suite 300
Ventura, California 93003
BY: JASON SCOTT LEIDERMAN

TOR EKELAND, P.C.
195 Plymouth Street, Fifth Floor
Brooklyn, New York 11201
BY: TOR EKELAND
and MARK H. JAFFE

# INDEX

# GOVERNMENT'S EXHIBITS RECEIVED IN EVIDENCE

| NO.: | DESCRIPTION: | PAGE: |
|---|---|---|
| 112 | E-mail series | 447 |
| 303 | Assembler security logs | 348 |
| 506 | Screenshot from Keys computer | 381 |
| 605 | IRC chat on 12/09/10 | 375 |

SACRAMENTO, CALIFORNIA

THURSDAY, OCTOBER 1, 2015, 8:39 A.M.

---o0o---

(Jury not present.)

THE CLERK: Calling criminal case 13-82, the United States versus Matthew Keys. This is on for jury trial, and today is day four.

THE COURT: Good morning.

MR. LEIDERMAN: Good morning, Your Honor.

MR. SEGAL: Good morning, Your Honor.

MR. EKELAND: Good morning, Your Honor.

THE COURT: Do we have everyone we need?

MR. HEMESATH: Mr. Silver will be here in just a moment. We can proceed without his presence.

THE COURT: All right. All counsel are here. Agent Cauthen is here. Mr. Keys is here.

Can we call the jury in?

MR. HEMESATH: Yes.

THE COURT: All right. Let's do that.

(Jury present.)

THE COURT: You may be seated.

Good morning, Ladies and Gentlemen of the jury. Welcome back to court. Happy October. We've turned over one month.

So we are ready to go. I'm going to ask the government to call its next witness. Mr. Hemesath?

MR. HEMESATH: Yes, Your Honor. At this time, the government calls Armando Caro.

THE CLERK: Mr. Caro, please come forward. I need to take your photograph this morning. If you can stand there against the wall facing me, please. Thank you.

Thank you. Please step into the witness stand, remain standing, and raise your right hand.

ARMANDO CARO, GOVERNMENT'S WITNESS, SWORN

THE WITNESS: I do.

THE CLERK: Thank you. You may be seated.

Will you please say and spell your first and last name for the record.

THE WITNESS: Armando Caro, A-R-M-A-N-D-O, C-A-R-O.

THE COURT: You may proceed.

DIRECT EXAMINATION

BY MR. HEMESATH:

Q. Good morning.

A. Good morning.

Q. Mr. Caro, can you tell me what it is that you do for a living?

A. I work in IT, system administration, management, architecture.

Q. For whom do you work right now?

A. Currently I work for Capital Group.

Q. I'm sorry?

A. Currently I work for Capital Group.

Q. Capital Group. What does Capital Group do?

A. They're a fund management company, the financial industry.

Q. And what is your exact title with Capital Group?

A. Senior systems administrator.

Q. Okay. Can you tell me a little bit about what those responsibilities as systems administrator entail for Capital Group?

A. Currently I'm in the engineering space, which is I'm responsible for designing, engineering and producing a product, our outcome that the company requires to run its business. It's system design and documentation that would be handed over to the operators that take care of those systems.

Q. How long have you been in that position at Capital Group?

A. Just over a year now.

Q. What were you doing before that?

A. I was doing consulting work for a company called Frontier Communications.

Q. And how long had you been with Frontier Communications or were you consulting for Frontier --

A. I was an independent sales consultant to them, but I was doing it for approximately a year.

Q. And before that?

A. Before that, I worked for Tribune Media.

Q. And what was your position when you left Tribune Media?

A. Managing director, architecture and security operations.

Q. What year was that then that you left?

A. 2011.

Q. 2011.

A. I'm sorry. No, that's not right. I started in 2009. I did three and a half years. 2012.

Q. 2012. Okay. Well, that's my next question actually.

When did you start with Tribune Media?

A. October 2009.

Q. Do you recall what your title was when you started with Tribune?

A. Managing director, architecture.

Q. So you started as a managing director?

A. Yes.

Q. And before that, what were you doing?

A. I was director of messaging and directory operations at Clear Channel Communications.

Q. And before that?

A. I was in the Air Force, a communications specialist.

Q. What did you do in the Air Force?

A. Ah, system administration. Essentially the same job with a military spin.

Q. Very good.

And any training other than those jobs?

A.  I went through training for the Air Force.  I worked in San Jose when I was going to school at San Jose State.  I was enrolled in computer engineering at the time.  And I worked several IT positions for companies in the valley.

Q.  Okay.  Thank you for that, for that history.

When you say that you worked for Tribune and you said Media Company, was it Tribune Company before that?

A.  I think the official title is Tribune Company.

Q.  Okay.  Could you tell me who you worked -- who your clients were that you reported to.

A.  My clients that I reported to?

Q.  Well -- I'm sorry.  Your managers, let's say, that you reported to.

A.  So my direct manager was Jeff Dorsey, the VP of operations, and he was my direct reporting manager.

Q.  Could you tell me, while you were working at Tribune Company, who you served in terms of the people that would make requests of you on a day-to-day basis?

A.  In my role as the head of architecture for all the systems that Tribune technology managed and operated and serviced, my customers would be the IT division itself and the business.  So in respect to what the business requested in new feature capability, functionality, I would have to incorporate that into what we could do with the technology we owned or had to procure.

And in respect to the IT division itself, the operations team needed optimization, improvement, or life cycle replacement of aging equipment.  I would be involved in the analysis and putting forth the decision to make that -- to go with what was requested.  So the portfolio is what I managed.

Q.  And where were you physically located while you were doing this work?

A.  I lived in San Antonio during the whole time I was working at Tribune, but I flew week in, week out to Chicago.  Monday I would be flying out, and Friday I would fly home.

Q.  Were the systems that you were working on just located in Chicago?

A.  No.

Q.  Where were they located?

A.  So we had two main data centers.  We had Chicago, and then we had L.A. Times.

Q.  So when you say L.A. Times, what relationship does L.A. Times have to Tribune Company?

A.  Tribune Company owned L.A. Times.

Q.  Did Tribune Company own any other newspapers?

A.  They owned eight.

Q.  Did they own anything else?

A.  TV stations.

Q.  How many TV stations do they own; do you know?

A.  I want to say 23.

Q. Did they own any in Sacramento?

A. Yes.

Q. Which one did they own in Sacramento?

A. I do not remember the call letters.

Q. Did the Tribune Company have a content management system?

A. Yes.

Q. Do you remember what that was called?

A. P2P.

Q. And what does P2P stand for?

A. Power to the producer, I believe.

Q. All right. Did that system require credentials to access the system?

A. Yes.

Q. And how were those credentials assigned?

A. They were given by the administrator of that system.

Q. Were they given to just anyone?

A. No. You had to be in a role to get access to the system.

Q. All right. Do you -- you've already stated that you were working with Tribune Company based on your date range in December of 2010; is that correct?

A. Yes.

Q. Do you remember an incident involving the L.A. Times in about that time?

A. Yes.

Q. What do you remember about that?

A. I remember an incident where a service incident came up that was reporting a -- at the time what was believed to be a malfunction in the system, and the content was not being generated as intended or had failed to generate as intended.

Q. Do you remember where you were when you received that news?

A. I was in the office.

Q. The office in Chicago?

A. Chicago.

Q. Uh-huh.

So what did you do as a result of that notice that you received?

A. Well, at the time, since it was an operational issue because it was believed to be a malfunction, I was just made aware as management staff. It wasn't until the issue was deemed a more serious issue, such as a compromise of security or system integrity that I got involved.

Q. And why did you get -- why did you get involved?

A. I was in charge of the security operations team at Tribune. So, in essence, we had a -- it's called a CSIRT, a computer incident response team, security response team, and I managed that group. And so any incident that came up, I would be the one responsible for the execution of that group to respond to it.

Q. So do you recall what the first thing is that you did after you got notice?

A.  Essentially we activated the CSIRT, which is get everyone involved.  Part of that group is different individuals from different disciplines across the company to be -- to contribute to the effort since their skill set is required.  So that was the first thing we did, activate the CSIRT.

I would ensure all the managers of those people who were involved were aware that their resources were being taken and that they need to make themselves available for this.  And then we started our fact-finding analysis efforts.

Q.  So why couldn't you just fix it yourself?

A.  Well, I didn't have any operational access to the system since that wasn't my responsibility.  My group isn't responsible for the day-to-day operations of those systems.

Q.  So do you recall who you charged with that responsibility to fix it?

A.  It would have been the operations group.  Off the top of my head, Tad Lin would have been involved, Matt Dobbertien as operations manager for the servers.  It would have been a whole list of people.  I don't recall off the top of my head.

Q.  And you were managing these people?

A.  I wasn't their direct manager.  I was managing their efforts in this incident, yes.  I was responsible for their activities as it pertains to what we did here.

Q.  Okay.  So as a result of your efforts, did you come to any initial conclusions about what had happened?

A. Well, from the information that we gathered, a user ID had logged into the system and had accessed an article and had changed the content and then posted the content.

Q. And why did you come to that conclusion?

A. Because the evidence was in the log.

Q. So what evidence -- describe to me the evidence that you saw in the log.

A. A log entry of a user ID logging into the system, so requesting access, passing a password and authenticating to it. The user ID requesting the article. The user ID making an edit to the article and committing it. And then the user ID posting that article to the live website.

Q. So what kind of log was this information found in?

A. It would be in the P2P system log.

Q. Is that also known as the Assembler log?

A. Yes.

Q. Did you find the log -- the pertinent log entries yourself?

A. No.

Q. Do you know who did?

A. No, I don't remember.

Q. Was it somebody on your team?

A. Somebody on the response team, yes.

Q. Did you review those Assembler log entries?

A. I would have looked at them, yes.

Q. All right. So then what happened?

A. Well, once we identified the user ID, we went to see who that ID was assigned to. And the ID had been assigned to I believe a female employee that had left the company or was no longer with the company, so her ID should have been inactive, but it wasn't.

And we obviously deactivated the ID. And then through the principle of assumed breach, meaning you assume that you've been compromised and take all actions to stop it without having to seek any further evidence, we asked everyone to change their passwords. And we proceeded to look for any points in the system to harden in case the breach had been through a -- a vector that we didn't currently know about or identify.

Q. So when you say everyone had to change their passwords, could you describe that a little bit more.

A. Yes.

So the P2P system had its own user database of IDs that could log into the system. So everyone who had an ID in that system was asked to change their passwords.

Q. And how was that communicated to those persons in the system that had to change their passwords?

A. Probably through e-mail. I'm not certain who did it, how they did it, but it was communicated to them.

Q. And do you know if passwords were in fact changed as a result?

A. I don't remember knowing or seeing any direct evidence, but

I was reported to that it had been done.

Q. So other than shutting down the N. Garcia username that you described, what else did you do? Or what else did you direct people to do?

A. During the course of the event, there was a remediation effort, which was to identify and fix whatever caused the event. And then we proceeded to look at what changes in design architecture or functionality that needed to be done to prevent or close any loopholes or vulnerabilities that exist in the system.

At that time, we did not know how the user -- how the ID got compromised. We just knew that it was.

Q. So with regard to that effort of not knowing how, why was it important to know how the user got in?

A. So that it couldn't happen again.

Q. Could you describe what efforts that you directed to find out who had breached the system?

A. So the article had been modified with a user tagline of Chippy leet. And it was curious to understand what that phrase was because it wasn't relevant to the article, it stood out.

And through googling that name, a handful of hits had come up on the Google search which led us to look through those articles or those postings, and one of them had been a blog posting of --

MR. EKELAND: Objection, Your Honor.

MR. HEMESATH: So let me stop you right there.

THE COURT: All right.

MR. HEMESATH: And I'm going to back up just a little bit. If we could look at previously admitted Exhibit 503.

Q. Do you recognize this?

A. Yes.

Q. And what is this?

A. This is the article that was modified.

Q. Okay. Now you mentioned the words Chippy leet. I look at this, and I see Chippy 1337. Could you explain why you said Chippy leet?

A. Yes. So the 1337 is a clever way of spelling a word using numbers. And in Internet jargon, 1337 is pronounced leet.

MR. EKELAND: Objection, Your Honor.

THE COURT: Overruled.

BY MR. HEMESATH:

Q. And do you know what, generally speaking in your experience, leet would refer to?

THE COURT: Just answer yes or no first.

THE WITNESS: Yes.

BY MR. HEMESATH:

Q. What does it refer to?

A. It's a sub proclamation that you're good at something.

Q. Like elite?

A. Yes.

Q. Where had you seen that before?

A. Users would create game tags with the phrase leet in it to signify that they're a really good game player.

Q. I see.

So you were describing before with regard to your reaction to the term Chippy leet what you did. So if you could continue with that, telling us what you did with that term Chippy leet.

A. After seeing the article, it stands out the phrase Chippy leet. And the content of the article was modified versus the previous article. So we, myself and another security operator, started to research the user tag Chippy leet.

Q. And how did you research that?

A. Using Google.

Q. What did your Google results result in?

A. We found a bunch of postings from -- relating to this user tag, and one of them was a blog posting --

MR. EKELAND: Objection, Your Honor.

THE COURT: What's the objection?

MR. EKELAND: Hearsay.

MR. HEMESATH: It's not for the truth.

THE COURT: What is it offered for?

MR. HEMESATH: It's offered for how he eventually came to his conclusions.

THE COURT: In the form of an evidentiary --

MR. HEMESATH: The blog statements themselves, there's no point to offering those for whether what they said was actually true, but they led to a place.

THE COURT: All right. So with that clarification, that the contents of any blog testified about is not being -- are not being offered for the truth of the contents, I'll allow the testimony.

BY MR. HEMESATH:

Q. So you were --

THE COURT: Do you have the question -- all right.

BY MR. HEMESATH:

Q. So you were saying that you saw a blog posting and that --

A. The information that the Google research revealed was a blog posting of someone with the tag Chippy leet bragging about a vulnerability that individual created and posted some code, a code snippet, meaning a section of code, that illustrates his cleverness. And in that code snippet, there was reference to an IRC article that the code would send data to.

Q. And so what did you do as a result of that information?

A. We went to the IRC article, the IRC channel.

Q. And can you tell us more about that IRC channel.

A. So in that channel --

MR. EKELAND: Objection, Your Honor.

THE COURT: What's the objection? The question is a bit vague. Why don't you focus the question.

MR. HEMESATH: Okay.

Q. Can you briefly explain what you mean by IRC channel?

A. IRC stands for Internet relay chat, and it's a protocol that you would access to communicate with others on the Internet. And we logged into that IRC channel.

Q. When you say log into that IRC channel, what does that procedure -- what procedures did you follow?

A. To log into an IRS channel, all you have to do is know the name of the channel, the server that it's on and connect. If the channel is not secure, you can get right in.

Q. When you say not secure, do you mean --

A. It doesn't require a password.

Q. And when you get in, what does that look like?

A. It looks like a terminal with a bunch of text, people posting their comments or conversation.

Q. So just text, no graphics?

A. You can get them using special commands, but they're not displayed.

Q. Meaning the graphics?

A. Yes.

Q. So it's mainly text?

A. It is text.

Q. So when you got to IRC channel that was referenced in the Google research, what did you see there?

A. So at this point I wasn't actively involved in the IRC activities. I saw the terminal. My security operator was the one actually doing the IRC log-in activities.

Q. What was the name of your security operator?

A. Dylan Kulesza.

Q. Okay. So throughout this activity, I'm speaking just of what you've described so far with regard to finding the identity of the person responsible, do you know how many hours you spent?

A. About a week's worth of time.

Q. A week's worth of time. Could you tell us how many hours?

A. 40 hours is a week, a workweek.

Q. And how are you so sure you spent 40 hours in a workweek on that particular task?

A. What task specifically?

Q. On the task of what you've described, which was stopping the intrusion and then identifying the intruder.

A. Can I clarify?

Q. Yes.

A. So you mean from when I first was notified that the incident was happening until the point where we concluded we think we know what is going on?

Q. Yes, but only including those two categories of things.

A. About 20 hours, half of that.

Q. About half of that?

A. Uh-huh.

Q. Okay. What else other than those two things did you do with regard to a reaction to this incident?

A. Well, being in charge of architecture and security, I would have had to review the design, the operation activities, the system integrity, and what work would need to be done to improve the security posture, rectify any deficiencies in the system, and ensure that we had proper procedures to handle this since it was a user ID that had been compromised, it was an ID that was no longer active from a user perspective.

Q. So does that mean you were improving the system to make sure that it would not happen again?

A. Yes.

Q. And that's -- and you're not including that time in the 20 hours that you just talked about, right?

A. No.

Q. Okay. In that first week, other than the 20 hours that we're talking about, so we can make sure we're talking about the same thing, what were the other 20 hours that you were spending time on? So if it's a 40-hour workweek, you spent 20 hours on the thing that you were just saying that you spent 20 hours on, what was the other 20 hours spent doing?

A. So of the 40 hours, 20 hours would have been to try to track down the source of the compromise.

Q. Uh-huh.

A. The other 20 hours would have been to address the compromise and remediate it.

Q. Okay. Tell me what that means.

A. Well, we had to make system changes. We had to get the users to change their IDs. We had to gather all the logs. I had to review, from a managerial standpoint, what is our next step? Are we adequately addressing this? Are we sure we've closed the door? Were the engineers doing their assigned tasks, management oversight?

So there was a lot of administrative work to be done as well as communicating to the business and my senior executive management what was going on.

Q. So that was in direct response to the incident?

A. I think in my mind that's all direct response to the incident.

Q. Could you have not done those things in response to this incident?

MR. EKELAND: Objection, Your Honor, calls for speculation.

THE COURT: Sustained.

MR. HEMESATH: So let's talk about what else you did past this week with regard to this incident. And by this week, I mean the first week.

Q. Can you tell me what else that you did with regard to your position at Tribune at that time?

A. Okay. So beyond the week of responding and addressing the situation, since we couldn't make significant system changes right up front without knowing more data as well as assessing our security posture, I spent the next several months with my security team and architecture team to review what changes we need to make in overall architecture, overall system design, and any new technologies or products that would help us react faster, identify vulnerabilities quicker, identify system deficiencies faster, implement a program that would help us address this through the system life cycle. So designing a system implementing proper security deterrence or elements into our system design. And then are we operating with the security facet in mind.

Q. What you just described was not counted within the 40 hours that you described?

A. No.

Q. Initially this is completely -- this is making the system better; is that correct?

A. Making the environment better.

Q. So to loop back around to what happened after your IRC research, do you recall what you did with that information?

A. When we first determined it was a possible compromise, we contacted the authorities, which we were then directed to the FBI and were given a contact. Once we identified that the -- we had thought we had located the identity or the identity of the hacker, we passed that information on to the FBI.

Q. Do you remember when in the week that you've been describing that occurred?

A. I do not remember exactly when.

Q. Before this, had you had any direct contact with anyone at Fox 40 in Sacramento?

A. No.

Q. Mr. Caro, how much -- and I realize this is a personal question, but how much money did you make as a salary in 2010 with your job with Tribune Company?

A. I made $180,000 a year.

Q. Sir, is that 180 or 108?

A. 180, one eight zero.

Q. 180.

Do you recall calculating your hourly rate?

A. Yes.

Q. And how did you calculate your hourly rate?

A. I took my annual salary, took the number of weeks in a year and the number of hours in a week, divided that by my -- divided my salary by that number.

Q. When you say hours in a week, you don't mean the total number of hours?

A. I mean a general work -- 40 weeks -- or 40 hours of a workweek.

Q. So 180 divided by 2,080; is that correct?

A. I believe so.

Q. Okay. Oh, I'm sorry to jump back.

With regard to the change of the passwords that was required, in your experience in a Tribune Company environment, how long would it have taken a typical user to change a password?

A. About two to five minutes.

Q. Why do you say two to five minutes?

A. The act of typing in the password takes relatively seconds, but thinking up a new one that you haven't used before, that meets the complexity of the requirements, that has the proper length usually takes a user a little bit longer to come up with one that they will remember.

Q. I see.

MR. HEMESATH: One moment, Your Honor.

(Government counsel conferring.)

MR. HEMESATH: Thank you, Your Honor. No further questions.

THE COURT: All right. Cross-examination, Mr. Ekeland?

MR. EKELAND: Yes, Your Honor.

Excuse me just one moment to get set up here. Or actually do you guys -- can you put 503 back up?

CROSS-EXAMINATION

BY MR. EKELAND:

Q. Good morning, Mr. Caro. My name is Tor Ekeland. I represent the defendant Matthew Keys along with Jay Leiderman and Mark Jaffe. And that's the defendant over there at the end of the table. I'm just going to ask you a few quick questions. This won't be long.

I just wanted to go back to -- you testified that you spent 20 hours in responding to this incident, correct, at one point?

A. Yes.

Q. And do you ordinarily log your time hourly when you worked for Trib Co?

A. No, I wasn't required to log my time.

Q. Okay. And did you record your time in your response to this incident as you worked on it? Aka, did you record it -- say you finished working on the day whatever you worked, an hour or two in responding to this incident, did you write down your time immediately afterwards and log it?

A. Yes. We --

Q. You did.

So you say the 20 hours is a precise figure or is that an estimate?

A. That is what I estimate.

Q. That is what you estimate.

So the time that you're stating here in court, they're all estimates, correct?

A. Yes.

Q. That's a yes? Okay. Thank you.

I just want to draw your attention to Government's Exhibit 503. This is the incident that you were responding to, the change of the headline in this article; is that correct?

A. Yes.

Q. And the way that this article was changed, somebody logged into the Trib Co system using a username and password, correct?

A. Yes.

Q. And the system responded as it was programmed to do because it thought it was a valid username and password and gave access to whoever accessed the system, correct?

A. Yes.

Q. So there was no impairment to the functionality of Tribune's P2P system or the CMS, it functioned exactly like it was supposed to?

MR. HEMESATH: Objection, that is a legal conclusion he's asking for.

THE COURT: Well, overruled, but the jury is to understand that this is not a legal expert, and the terms that Mr. Ekeland is using are not being used in a legal manner.

So as a layperson, given what you understand the words to mean, you may respond.

THE WITNESS: Can you repeat the question?

MR. EKELAND: Yes.

Q. So basically -- I believe the username was N. Garcia. Do you recall that?

A. Yes.

Q. Right.

So when whoever was using the username N. Garcia logged in with that username and that password, the system did exactly what it was programmed to do, it gave that person access, correct?

A. Yes.

Q. Right.

And so when that person got in, that person was able to edit the article in the P2P system just like any other Trib Co employee would be able to if they had logged in with their username and password; is that correct?

A. Not any, no.

Q. I'm sorry. Not any?

A. No.

Q. No? Why not?

A. You had to be in the position of a content producer. That ID had to belong to you to use it and the intent that you would modify an article to generate your own content.

Q. Right.

But N. Garcia wasn't in that position. It was a username and password that allowed somebody to get in just like anybody else who had that type of username and password could get in and edit the article, correct?

A. That type meaning N. Garcia?

Q. Yes.

A. No. N. Garcia belonged to N. Garcia.

Q. What did you say?

A. N. Garcia belonged to N. Garcia.

Q. Right.

But N. Garcia, the username and password, had the rights associated with it to edit the article, right?

A. Yes.

Q. And nothing -- there was no code that was transmitted to the P2P system that changed its functionality in any way, correct?

A. No.

Q. Okay. And you're not aware of any impairment to the functionality of the L.A. Times website as a result of this log-in, correct?

A. Yes.

Q. Yes?

A. Yes.

Q. And so you're saying that username and password logging in, that the system recognized as valid credentials, impaired the functionality of the L.A. Times website?

A. The functionality of the L.A. Times website was to have news for the consumers to read and be trustworthy. The functionality of the website was to produce valid content. This is not valid content.

Q. Right.

But the username and password just edited the article precisely like it was programmed to as if somebody from -- an editor from Trib Co who had this access could have gone in and edited it any way they wanted, correct?

A. Yes.

Q. Okay. So -- and you're not aware of any -- the L.A. Times website did not go down because of this access, correct?

A. I do not believe so.

Q. And you're not aware of any impairment to the Fox 40 website because of this access, correct?

A. No.

Q. And you're not aware of any change to the underlying code running your websites because of this access, correct?

A. Correct.

Q. Is that -- was that a yes?

A. Correct. Yes.

Q. Okay.

MR. EKELAND: No further questions, Your Honor.

THE COURT: All right. Redirect?

MR. HEMESATH: Yes, Your Honor.

## REDIRECT EXAMINATION

BY MR. HEMESATH:

Q. The Assembler log saves its commands in terms of code, correct?

A. No.

Q. Could you explain that.

A. The Assembler log would log the activity of the system based on whatever the code said it needed to generate a log entry for.

Q. In order to generate a log entry or in order to generate a command that resulted in a log entry, would someone have had to have transmitted a code or command?

A. A command, yes.

Q. And -- I'm sorry.

When I say code, in your profession that means something specific. Could you tell me what that means.

MR. EKELAND: Objection.

THE COURT: Overruled.

THE WITNESS: Code is the language that you use to instruct computers what to do. It is either compiled or interpreted, and it is how you make computers function the way they do.

BY MR. HEMESATH:

Q. Can you explain the relationship between the words "code" and "command"?

MR. EKELAND: Objection.

THE COURT: Overruled.

THE WITNESS: So I can command the computer to give me a listing of all the files on that computer, but that command is foreign to the computer unless it has the code to understand that I'm asking for all enumeration of all the files that it stores and how to access that through the hardware, how to generate an output, how to format it and present it to the screen.

So the command would be directory. The code would execute all the steps necessary to generate that information.

BY MR. HEMESATH:

Q. So when someone purporting to be N. Garcia, as you've testified, sent a command, what effect did that have on the system's integrity?

MR. EKELAND: Objection.

THE COURT: What's the objection?

MR. EKELAND: Calls for speculation and also expert testimony, Your Honor.

THE COURT: Well, this person is not testifying as an expert. But based on what he has said about his job, I'm going to allow him to respond as a layperson.

You may respond.

THE WITNESS: Repeat the question, please.

BY MR. HEMESATH:

Q. Based on your previous testimony that N. Garcia transmitted or someone purporting to be N. Garcia transmitted a command, what effect did that have on system integrity?

A. If it was a proper command, it would post the information. If it was an improper command, it would put the system in a compromised state.

Q. The fact that you found N. Garcia to be an unauthorized user, what effect did that have on system integrity?

A. The system was designed to allow users who were authorized to generate content with editorial integrity, to put that content on the business website, which was the product of the company. If that information and product was not in line with the spirit of the company's being an editorial news agency, it would compromise the value of the company and its integrity as a news source.

Q. What about the integrity of the security of the system?

A. The integrity of the system would mean that we cannot ensure that anyone who had access was of -- was appropriate.

Q. Is that why you asked everyone to change their passwords?

A. Yes.

Q. Is that why you did your investigation as to whom?

A. Yes.

Q. Mr. Ekeland asked you about the 20 hours that you spent in direct response. In fact, what was your testimony with regard to your direct response to this incident?

A. In my mind, it's all direct response.

Q. But certainly not including the upgrades you did after the week to improve the system?

MR. EKELAND: Objection.

THE COURT: Hold on one second. What's the objection?

MR. EKELAND: Leading.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. Can you tell us in clearer terms what you did in direct response to the incident in terms of hours and what you did again.

A. So 40 hours of direct response from the issue being reported to me, managing it through to its inevitable conclusion, handing it off to the FBI to take the case and all of the activities between then.

Q. And then after that?

A. After that, I was fulfilling my role as the director of architecture and security to ensure that we were not -- we were in a better posture not to be compromised again.

Q. Mr. Ekeland asked you if that 40 hours, or 20 hours as he put it, was speculation or, rather, he said whether it was an estimate.

What was the absolute minimum that you believe that you spent in direct response that week?

MR. EKELAND: Objection.

THE COURT: What was the objection?

MR. EKELAND: Calls for speculation.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. How do you recall so well whether it was 40 hours that you spent on that week?

A. It was a very clear incident in my mind on what happened. The exact number I do not recall, but the estimate of a week was what I remember working on that event.

Q. Do you recall doing anything else that week?

A. Whether it was 39, 38, 41 hours, I remember it being a week of my time.

Q. Do you recall doing anything else that week?

A. Sure, I had other responsibilities. I was in charge of 50 plus people. I had day-to-day operations to make sure happened as well as long nights addressing this.

Q. Do you recall working more than 40 hours that week total?

A. Yes.

Q. You do recall that?

A. Yes.

Q. Okay.

MR. HEMESATH: Thank you very much.

THE COURT: Any recross?

MR. EKELAND: No, Your Honor.

THE COURT: All right. Is this witness excused?

MR. LEIDERMAN: He is by the defense.

THE COURT: You're excusing this witness, Mr. Hemesath?

MR. HEMESATH: Yes, Your Honor. Thank you.

THE COURT: All right. You're excused, sir. You may step down.

The government's next witness?

If you want to stand and stretch, you may. We'll take a full break around 10:00.

Who are you calling next?

MR. HEMESATH: Mr. Kulesza.

THE COURT: All right.

THE CLERK: Mr. Kulesza, please come forward. I need to take your photograph. If you can stand with your back against the wall facing me, please.

Great. Step into the witness stand behind you, remain standing, and raise your right hand.

DYLAN KULESZA, GOVERNMENT'S WITNESS, SWORN

THE WITNESS: I do.

THE CLERK: Thank you. You may be seated.

Will you please say and spell your first and last name for the record.

THE WITNESS: My name is Dylan Kulesza. D-Y-L-A-N. Last name Kulesza, K-U-L-E-S as in Sam, Z as in zebra, A.

DIRECT EXAMINATION

BY MR. HEMESATH:

Q. Good morning.

A. Good morning.

Q. Could you tell me what you do for a living?

A. I work for Optiv Security, and I perform security strategy assessments and CISO activities. CISO activities are executive level roles that oversee the cyber security programs for, you know, large companies.

Q. I'm sorry. You said Optiv. Could you spell that?

A. Optiv, O-P-T-I-V.

Q. Where is that based?

A. Based out of Colorado. They have multiple offices across the United States.

Q. And is that where you work for them?

A. No, I work remotely, but that is considered my prime location.

Q. And where do you work?

A. I'm based out of San Antonio, Texas. So I work remote and travel to organizations almost weekly.

Q. Okay. And how long have you been with Optiv?

A. I've been with Optiv now for three weeks.

Q. Oh, congratulations.

A. Thank you.

Q. What did you do before you worked with Optiv?

A. So I briefly worked at Tesoro Corporation in San Antonio, Texas, and that was a duration of six weeks. And --

Q. What did you do for Tesoro?

A. For Tesoro, I oversaw the enterprise architecture group.

Q. Okay. And that was for six weeks?

A. Correct.

Q. And why did you leave Tesoro to go to Optiv?

A. I felt that Optiv would be a better career path for me going forward, and I would get a lot more experience than where I was currently at, so I elected to leave Tesoro.

Q. What about before Tesoro, what were you doing?

A. Before Tesoro, I was VP of engineering, security and architecture for Tribune Publishing Company.

Q. And that was your title, VP of engineering and security and architecture?

A. Correct.

Q. How long did you have that title?

A. I had that title for over a year.

Q. What about before that at Tribune?

A. Before that, my title would have been either director of infrastructure and security or enterprise security architecture. It was a brief transition with the director of all.

Q. And do you recall when you started at Tribune or any of its related --

A. Yeah. March of 2010.

Q. March of 2010.

And what was your title at that time?

A. Originally my title was I think data architect.

Q. Data architect.

And then before that, before Tribune Company?

A. Before Tribune Company, I worked at Clear Channel Communications, now known as iHeartMedia.

Q. Before that?

A. Before that, I worked for USAA.

Q. And could you tell us what USAA is?

A. USAA is a financial institution, primarily servicing military officers.

Q. And do you have an educational background?

A. Correct. I have a Bachelor's in management information systems.

Q. Where did you get that from?

A. University of Texas, San Antonio.

Q. And what year did you graduate?

A. 2006.

Q. Okay. So based on what you've said, you were working at Tribune Company in December of 2010; is that correct?

A. Correct.

Q. Do you recall responding to an incident at about that time?

A. I do.

Q. Can you tell us about that.

A. We received a call from the business stating that our website latimes.com was compromised, and it had an article or a statement that Chippy leet was here.

Q. Do you recall who was supervising you at that time?

A. Armando Caro.

Q. So what -- do you remember where you were when you heard about this news?

A. I was in the San Antonio office when I heard the news.

Q. And what did you do in reaction to the news?

A. In reaction to the news, a team was assembled to start triaging the issue. And one part of the team focused on the initial response to identify how the compromise occurred and how to quickly remediate it. And I focused on understanding who may have compromised us and what other threat we were vulnerable to.

Q. So why a team?

A. There are many roles in an organization, and everyone has their own specialties, and so there is a requirement to collaborate with others in gathering information during a security incident.

Q. You said that you were in charge of finding out who; is that correct?

A. Correct.

Q. Why was it important to find out who as opposed to just stopping access so that the intruder --

A. Correct.

So, you know, you kind of want to understand, let's say if your house is broken into, you know, was this a random act? Did somebody just come in randomly and break into your house? Or do you want to further understand and see could this person come back again? Do they pose a threat to yourself or, in this case, a threat to the organization?

Q. Uh-huh.

So what did you do with regard to finding out who broke into the house?

A. So part of my research involved looking on Google or other search sites with keywords such as Chippy leet, trying to gain information on who may have compromised the organization. And so that's really the kind of process I took to finding out who may have broke in.

Q. And what did you conclude as a result of those actions?

A. So through those actions, we discovered that there was a reference to an IRC server. An IRC is a form of communication online that individuals can join and talk to each other. And through that IRC server, we were able to identify how to connect to it and validate that there were individuals on that server talking in regards to the incident.

(Government counsel conferring.)

BY MR. HEMESATH:

Q. What did you do with that information when you found out about it?

A. I believe we were already in communication with the FBI at the time. So when we gathered that information, we packaged it up to hand off to the local agent.

Q. So could you tell us how much time that you spent on that task?

A. So for that task of doing the research on who attacked the organization, I would have spent probably, you know, 8 to 16 hours for that activity. There were other activities, but specific to understanding who attacked the organization, it was anywhere between 8 and 16 hours.

Q. How do you remember that so well?

A. A little bit of it is experience. After going through security incidents, you understand that you'll spend approximately maybe four to six hours in the initial triage of what's happening. Perhaps you'll spend another 8 to 12 or whatever duration on understanding the threat that is attacking the organization. And then you'll also know that you'll spend, you know, anywhere between 20 or 40 hours on further evidence gathering and the forensics.

Q. So after that initial 12 to 16 hours that you described, did you do anything at all with regard to this incident going forward?

A. Could you further elaborate?

Q. Yes.

So getting past these sets of actions that you've already described, the finding out who and so forth, what else did you do with regard to this incident?

A. So after finding out who, a series of actions occurred after that. One would be continuing to look at our application, in this case it was a website, a content management system that allows you to publish content, seeing if there were any other vulnerabilities.

When this attack occurred, there were concerns within the executive leadership that it could occur again, and so time was spent in trying to understand how someone could breach it.

And then this was kind of the point in the organization where we started looking at how to upgrade our defenses, how to upgrade our infrastructure to better secure ourselves going forward.

Q. So in the time that you spent doing that, what you just described, was any of that included in your estimate of --

A. No, it was not.

Q. -- 8 to 12 hours?

Okay. In that 8 to 12 hours, in addition to identifying on Google and so forth, did you review Assembler logs?

A. Assembler is one of the applications, and I provided some review of those logs, but that was not my primary task.

Q. But you did do some?

A. Correct.

Q. Why did you review what you reviewed?

A. Really looking at experience on the team, there was a few of us that had experience in reviewing logs, and so I was the second set of eyes to ensure that the assumptions were correct.

Q. So can you tell me at the point that you had identified the user N. Garcia as the username, why not stop the analysis and the work at that point?

A. So, you know, the example of the house, it's like driving up to your house and seeing that the door is wide open, and the lock is not broken. So you have to understand why is the door open? Did someone gain access to a key? Did someone pick the lock? How did they get into the house?

And so just looking at it from N. Garcia and disabling that account, that would be the same as just closing the door and locking it. So there were further steps that were required to validate that, the way the person got in, would they be coming back? If they tried to come back again, would they now try to go through the back door? Would they try to go through a window in the house to gain access?

Q. When you say the word "back door," can you tell us what you mean with regard to your specific security protocol that would lead you to believe that that would be a problem?

A. Yeah.

In security terms, a back door is a way for an attacker or a hacker to regain access. And so generally if the original way they were able to break into the system, if that is terminated or if that access is no longer available, an attacker will try to establish a back door, which is a way that they can gain access again.

And so in the house analogy, you know, a back door would be as simple as maybe someone, you know, unlocking a window on the side of the house. That's a way for that person to regain access.

Q. Would looking for the back door be considered a security upgrade?

A. That would not be considered a security upgrade. That would just be part of the incident response to ensure that, if the person compromised you, and you believe you've removed access, that you're not going to have a recurrence within the next, you know, few hours or the course of the next few days.

Q. Do you know how many users used the CMS?

A. The CMS system is used primarily between two to 3,000 individuals. That would be the editorial within the Tribune organization.

Specific to L.A. Times, there is probably three to four hundred that accessed the Assembler application.

Q. Do you know if someone outside the L.A. Times had access, would have had access to CMS content relating to L.A. Times?

A. Generally no one would have access to L.A. Times content outside of the L.A. Times staff. There are cases where the system administrators, the people that work on the computers and the applications, would have access to that content.

Q. So someone with that kind of access, could you describe the relationship a person who is supposed to have that kind of access and the concept of a super user, if you know what a super user is?

A. Correct. So most users, let's say, would be a content owner, and they own their own content. The content they would own would be content for L.A. Times.

Then there are what you would call a super user. And so if you think about how L.A. Times is one of many companies of Tribune -- you have L.A. Times, Chicago Tribune -- you would have content owners of L.A. Times and content owners of Chicago Tribune. But a super user would have access to both L.A. Times, Chicago Tribune or any of the other newspapers and also have the ability to create users across any of those properties.

Q. At what point were you able to rule out that there was not a super user credential at stake in this incident?

A. I was not directly involved in the super user identification. But from my understanding --

THE COURT: So wait for the next question.

THE WITNESS: Okay.

BY MR. HEMESATH:

Q. So what can you tell us, if anything, about your knowledge that the potential existence of a super user was a possibility in this --

MR. LEIDERMAN: I'm going to object. It calls for implied hearsay.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. Based on what you know, were you able to rule out the existence of an unauthorized super user?

MR. LEIDERMAN: It's the same objection. It calls for his knowledge and calls --

THE COURT: Sustained based on what I've heard so far.

MR. HEMESATH: We will get back to that.

Could I have -- Your Honor, at this time, based on stipulation, the government moves Exhibit 303 into evidence.

MR. EKELAND: I just need to look at it real quick.

(Counsel conferring.)

THE COURT: Do I have a 303 on my list?

MR. HEMESATH: Your Honor, it --

THE COURT: I have one in my binder. It's not on the list.

MR. HEMESATH: Yes, I can explain that if you'd like.

THE COURT: Is there a stipulation to admit 303?

MR. EKELAND: Yes, Your Honor. We saw it and discussed it this morning.

THE COURT: All right. So it's ten pages?

MR. HEMESATH: Yes.

THE COURT: All right. 303 is admitted.

(GOVERNMENT'S EXHIBIT 303, Assembler security logs, ADMITTED INTO EVIDENCE.)

BY MR. HEMESATH:

Q. Do you recognize the form of what is on the screen here?

A. What's on the screen would be a security log in our

Assembler application.

Q. And how can you tell that that's what that is?

A. One, the format where you see the first few numbers, which is an IP address; the second group of data, which is a date and time stamp. And then if you look past the word "post," there is the access save groups. That is characteristic of the Assembler application.

Q. Okay. So this is an Assembler log entry?

A. Correct.

Q. Can you take us through -- and understand that we are not IT professionals, but could you tell us a little bit about how you would interpret this particular log entry based on your day-to-day experience with such entries?

A. Correct.

So going through that example, if you look at the first number, that is an IP address. The simple way to think of an IP address is a phone number, it's the person that is calling you. So when you have caller ID on your phone, you see the number that someone is calling from, this would be equivalent with the IP address.

The second group there with the date, that would be the time that this event happened, the time that it was logged. And so you can see this occurred on December 8th, 2010.

The second piece of information there is the word "post."

Q. Oh, I'm sorry. Could we go back to this one.

Can you tell us what -- sorry. Can you tell us what this number means?

A. That should be the offset of time.

Q. Meaning?

A. So meaning the log was generated in GMT time. And then the minus eight would be the -- you know, between daylight savings time or Pacific time, the offset.

Q. So a time zone adjustment?

A. Correct.

Q. Okay. And the next?

A. The next piece of information, whenever someone goes to a website -- for example, you go to facebook.com -- typically your interaction occurs one of two ways. You're either getting information by saying get facebook.com or you're posting information. Perhaps you want to send a message to somebody or provide an update on, you know, some family event or picture.

And so in this case, when you see the word "post," the person has submitted information to the server.

Q. Is there an alternative to the command post?

A. Post is the primary way to post, send information to a server.

Q. What command would someone use if they were trying to receive information?

A. They would use the command get.

Q. Is that roughly the difference between uploading and downloading?

A.  Loosely, yes.

Q.  Okay.  So what about the next entry?

A.  So the next entry is showing the actual address that someone is going to.  So in the example of facebook.com, perhaps you go to www.facebook.com slash and your name, John dot Smith.

So in this example someone is going to access and save groups.  And when you look at save groups.ldap, L-D-A-P, LDAP is an acronym for lightweight directory authentication protocol.  And what that means is your username and password information is stored in that LDAP provider, and save groups is a way to add users into certain privileged accounts or owner accounts to have access to information.

Q.  Okay.  I think I got that.

What about the next section?

A.  And the next section as far as the HTTP or the 200?

Q.  Well, what do you think, reading from left to right, top to bottom, is the next relevant thing on that?

A.  The next relevant would be the number 200 because that means the information was successful, whatever was submitted was a success.  Numbers could be multiples, but 200 is the command okay.

Q.  So that you know that to be, like, the code for okay?

A.  Correct.

Q. What about the next number?

A. The next number is the size of the transmission. So it's a relatively small number so, you know, what came back was probably just a brief message saying successful. If it had been a much larger number, then it would be something similar to an image or a video file that is, you know, in much larger size than sending a command.

Q. All right. What about this next section?

And tell me if I've got it wrong in terms of the break, but that section that starts with HTTPS.

A. Yep. So what's occurring here is someone is editing the group, so that was most likely the prior -- the prior web page the user was on before submitting the post. And so in this case, someone was trying to edit the group and add a username of anon1234.

Q. Now let's be clear about what you mean by group.

A. So a group would be simply a group of entitlements or a group of privileges. And so you may have the ability to only read information in the application, and you would be a group of read only. You could be in a group where you own the content, where you can now edit the content as well as read it. And you could be in a group that has super user ability where you not only can edit and read content, but you have the ability to add additional users into the system.

Q. Okay. And I'll ask you more about that particular section in just a second.

Just so we can get through the rest of this line here, what -- how do you interpret the section after that?

A.  So the section after is generally information about the user who was connecting to the server or submitting the information.  So what this is telling me is the person was using Mozilla, or probably more known as Firefox, and they were connecting from a Macintosh computer.  And at the very end, you can confirm that it was Firefox by it actually stating that it was Firefox 3.6.8, which is the version.  So when you think of Windows 8, Windows 10, this was Firefox 3.6.

Q.  Okay.  So in relation to the term "anon1234," what can you tell us happened here?

A.  Anon1234 is not the name of an actual user.  And from experience looking at this behavior, it's telling me that someone is trying to put in a back door or an account that they can in the future regain access if the primary account that they have compromised becomes inaccessible.

Q.  And the relationship of that command that was sent and this IP address is?

A.  So it would mean that that IP address is the individual that is trying to create a back door into the system.

Q.  And this number means that it was successful?

A.  Correct.

Q.  Anything else that you can tell us about this particular entry?

A. No.

MR. HEMESATH: All right. Could I get the next page.

Is there any difference between what we just saw and this one? Okay. Let's go to the next page.

All right. And the next page. Okay.

Q. Are there a lot of log entries on this particular page?

A. It appears to be six entries.

Q. Okay. Let's start, if we can get the first one, with just the first one.

A. So the format is similar to the one prior where at the beginning you have the IP address that is being used. The second portion, you see the date and time. And then what's different in this is they're using the get command. So they're trying to get data, and they're trying to get the ability to edit a newsletter with an ID of 543.

543 is just an arbitrary number that references some news article on the website or in Assembler.

Q. I'm sorry. Which part of 543 -- this one right here?

A. Correct.

Q. Okay. All right. So now you described it before, but would the sender of this command have been uploading or downloading to use a more conventional term?

A. In this case, they would be getting the information or downloading it.

Q. And you say that because of the get command?

A. Correct.

Q. Can you tell us -- first of all, the date you say is November 3rd?

A. Correct.

Q. Okay. Can you tell what is being downloaded here?

A. Right here they're trying to gain access to a newsletter. And what we don't have context into is what newsletter 543 is.

MR. HEMESATH: Okay. Could we get the next log entry.

If we can move it down just so we can see the first one as well. There we go. Okay.

Q. So anything different about this particular one?

A. In this particular case, the user is trying to get information as well, but they're trying to get the e-mail page for a username of test1234.

Q. In your experience, is that a valid username?

A. That username would not be valid or, if it was valid, a mechanism for system administrators or super users to make tests or changes.

Q. And the time difference between the first one and the second one, what do you make of that?

A. The time difference is a little over a second between the two.

Q. Is that a second or a minute?

A. Excuse me, my apologies. That is a minute between the two.

MR. HEMESATH: Okay. All right. Could we look at the third one.

Q. And what can you tell us about this?

A. This line they're getting the images. So when a web browser is requesting information, it actually can make multiple requests at one time. And so this request here is getting an okay button, and typically an okay button would be used to submit information.

Q. But it's a get command?

A. But it is a get command.

Q. Got it.

And then this is at about the same time as the previous command?

A. Correct.

MR. HEMESATH: Okay. All right. Can we see the next one, please.

Q. All right. Anything more that you can tell us about this one in relation to the other three?

A. Here they're trying to get the taxonomy of the different product affiliates.

Q. What does taxonomy mean?

A. Taxonomy would be the -- really the hierarchy or classification of a -- in this case, classification of product affiliates.

Q. And when you say classification, what do you mean by that?

How they're related to one another?

A. Yeah. The simple way to think of a taxonomy is similar to animals, right, where you have mammals, amphibians. And in mammals, you can have, you know, the canine. Within canine, you can have different classifications.

Q. Like an org chart?

A. Similar, yes.

Q. And that is just after 2:40, the previous one; is that correct?

A. Correct.

MR. HEMESATH: Could we take a look at the next one.

THE COURT: We'll just go to the bottom of this page and then take our break.

BY MR. HEMESATH:

Q. And this is about a minute after that or 40 seconds after that; is that correct?

A. Correct.

Q. And what is happening here?

A. They're listing the XML template. An XML template -- XML is used generally to make templates, so think of it as a cookie cutter or a rubber stamp.

MR. HEMESATH: Okay. And we'll look at that last one.

Q. And what about this one?

A. The individual is getting the topics for a product affiliate, and that product affiliate would be KTXL.

Q. How can you tell that it's KTXL?

A. When you look at the -- so you have the get, and then you have the forward slash taxonomy forward slash search. The question mark there is basically stating it's going to be a parameter, meaning it's going to ask for a product affiliate, and the product affiliate it's requesting is KTXL.

Q. I see. Okay. And real quick, and then we'll move on.

All of these on November 3rd came from different IP addresses, the same IP address?

A. They all came from the same IP address.

Q. I see. Okay.

THE COURT: All right. That's a good time for our break. We'll take a 15-minute break. During the break, please remember all of my admonitions. We'll see you back here in 15 minutes. Thank you.

(Jury not present.)

THE COURT: You may step down. Just be back in your seat in 15 minutes. All right?

All right.

MR. HEMESATH: 10 minutes you said?

THE COURT: Well, 15 minutes for the jurors, so be ready a few minutes before.

MR. HEMESATH: Okay.

MR. SEGAL: We'll take ten.

THE COURT: All right.

(Recess taken.)

(Jury not present.)

THE CLERK: Come to order. Court is back in session.

THE COURT: All right. Let's bring the jury back.

Can you stand behind the counsel table until we have the jury in?

(Jury present.)

THE COURT: You may be seated.

Welcome back, Ladies and Gentlemen. We'll continue with the direct examination of Mr. Kulesza.

Just so we can be aware of our expectations, how long do you expect to continue with direct, Mr. Hemesath?

MR. HEMESATH: I would estimate another half an hour.

THE COURT: All right.

MR. HEMESATH: But I'm pretty bad at that, so we'll -- we'll see.

THE COURT: All right. We'll measure you in the next half hour.

MR. HEMESATH: Thank you.

Good morning again. Could we get Exhibit 303-004.

Q. So we were just looking at this exhibit a moment ago, and you were just pointing out to us that these IP addresses are the same; is that correct?

A. Correct.

Q. And it may be self evident, but in general what can you tell us about the relationship that you see between these time stamps ranging from 2:38 to 2:41?

A. You know, with the time stamps, all of these activities did occur during that time period relating to these log files or log entries.

Q. Okay. With regard to these log entries that happened at these times, you had told us at a previous time that the second of these two numbers here -- there's an example right there -- was the size. That's not going where I want it to go.

Do you see any log entries in this particular set that indicates a larger size than any of the others?

A. The largest log entry appears to be the second one.

Q. That one right there?

A. Correct.

Q. And this is a get command, correct?

A. Correct.

Q. So what does that mean? What do you interpret that to mean?

A. The user was getting information from the e-mail page regarding username test1234 and received a sizable bit of information relative to the other entries.

Q. What unit of size is reflected in this number here, 178,316?

A. That would be in bytes.

Q. So can you give us an idea of how big that is with regard to, say, a text file?

A. So a text file you would generally see one character, the letter A, consuming one byte. So in this case, you would have 178,316 characters being returned.

Q. Thank you.

MR. HEMESATH: Could I get the next page, 005. And I apologize in advance that we're putting you through what must be a little bit like work.

Q. So what can you tell us about this particular entry?

A. Again, the similar log format with the IP address starting at the beginning, the time that this event occurred, a user requesting with the get command the e-mail page for username test5678. And then that being successful with the 200 number after the HTTP and returning one thousand eight hundred -- 187,976 bytes of data and coming from the navigation UI page. And the user was using Mozilla Firefox on a Macintosh computer. And, again, the Firefox version was 3.6.8.

Q. Was that the same version of Macintosh, the same version of Mozilla that we've been seeing through the previous exhibits?

A. Correct.

Q. And this IP address, was that the same IP address as the previous page that we were talking about?

A. I'd have to see the previous page.

MR. HEMESATH: Could we take a look at the previous page real quick?

THE WITNESS: Correct, the numbers were the same.

MR. HEMESATH: Okay. Could we see 005. Perfect, thank you.

Q. Were you the one that did geolocation work on that IP address?

A. I was not.

Q. Okay. All right. Let's go to the next one.

All right. So same question, what happened here?

A. A user with the IP address of 75.53.178.11 requested on November 22nd, 2010, the left arrow image, and that was successful, and it returned 120 bytes of data. And that came from the e-mail page UI with the username test5678. And, again, with the same web browser, the Firefox 3.6.8, from a Macintosh computer.

Q. Okay. And the next one? What about this one?

A. Very similar, but what is unique to this is that they're requesting a user find function of the website. And that would potentially allow them to look at or find other users that live in the system, other users that have access to the application.

Q. Okay. Next, please.

Same question, what about this one?

A. Again, similar to the prior log entries. In this case, they are getting an okay image file, and that image file came from, you know, the e-mail page test5678 from a Macintosh computer running Firefox.

Q. Okay. Safe to say that get images with a gif file and text, that's something that is going to happen frequently with regard -- in the same time as another command?

A. Correct. For example, when you go to google.com, and you go to search, above that search box there is usually an image that says Google or whatever clever image they're using. And so that just gets typically downloaded or requested by going to that page.

Q. Okay. So the next one. And this is a gif file?

A. Correct.

Q. All right. So let's go to the next one.

Is this another find user -- well, this is different, correct?

A. Correct.

Q. How is this different?

A. This is find user versus a generic find from the prior entry.

Q. So what happens with find user?

A. I could not speak to the Assembler application in detail to specifically tell you the behavior of find user versus find.

Q. Okay. And this is a post command, though; is that correct?

A. Correct.

Q. Okay. All right. Let's go to the next page.

All right. This is from November 3rd; is that correct?

A. Correct.

MR. HEMESATH: And we may be able to skip this page. I'm going to try to save us some time.

Okay. All right. So we're going to skip that page, because it appears to be a duplication.

Q. What about the first entry here?

A. So different from the prior entries is the IP address has changed. It's now 91.214.168.172. This is occurring on December 4th, 2010, and the user or individual requesting is getting the home page. So, again, going to Facebook or Google, you would see a get forward slash whenever you're requesting the default page for those websites.

Q. And I don't know if you can see below there. Is that basically the same thing as the next entry as well?

A. Correct. When you're looking at the client information, it is similar to the prior ones being from a Macintosh computer running Firefox 3.6.8. And another consistency between the prior entry is it's a Macintosh running on version 10.6, which has also been on the prior entries.

Q. And so the next entries down are substantially similar to the first one; is that correct?

A. Correct.

Q. Okay. So can we go to the fourth one right here.

What can you tell me about this entry?

A. So with that IP address ending in 172, on December 6th, a user has requested the welcome page, which would appear after logging in successfully to the application. And that is occurring, again, from the same version of Macintosh running 10.6 and from the same Firefox version of 3.6.8.

Q. All right. So let's look at the next one after that.
Same question.

A. Again, the same computer. In prior examples when we've seen a get, that ends in dot gif or G-I-F. This is similar to those type of requests where it's just providing you -- specifically a CSS file helps provide the color, the look and feel for the website. So it's just requested in addition to the other information on the page.

Q. And just for a little bit of context, how many of these log entries would you expect to exist or to have been generated within the CMS system on a given day?

A. We would see -- for CMS application, there could be upwards of a hundred or 200,000 plus log events per day for all the various users and IP addresses and requests that occur.

Q. A part of the job in finding the solution to this mystery was sifting through all those and finding these?

A. Correct.

MR. HEMESATH: All right. Let's go to 303-008.

Q. What can you tell us about this?

A. It's the same IP address ending in 172 on December 6th. This request is sending the post command. So post is the upload or sending of information, which differs from some of the prior examples with the get or the downloading.

This person -- this request is posting to the save user. And as you can see, it was successful with the 200 code. And it was posting from the edit user function of the web application for user name S. Scholbrock.

And how I would interpret this is someone has been able to successfully modify that username, and you would typically modify it to change some characteristic, either changing the password or changing the permissions of that user.

Q. You're saying that that command to change one of those aspects that you just mentioned came from a computer running Mozilla Macintosh -- or I'm sorry, not Mozilla -- from a Macintosh computer running this particular OS system running this version of Firefox, correct?

A. Correct.

Q. Can we take a look at -- and the time on that was 4:00 in the morning it looks like. Well, with the proper adjustment. Is that correct?

A. Correct.

Q. The next one.

What about this entry?

A. So, again, that account was modified for the same user from the same Macintosh computer running Firefox on December 8th.

Q. Now that was two days after the first one?

A. Correct.

Q. Would you be able to tell, looking at this, whether someone was executing this command or transmitting this command from within a Tribune system?

A. So the IP address, again similar to a phone number, that IP address does not exist in the --

MR. LEIDERMAN: I'm going to object as nonresponsive. It's a yes or no question.

THE COURT: Sustained. So disregard the answer so far.

MR. HEMESATH: So --

THE COURT: Repeat the question and provide a yes or no.

BY MR. HEMESATH:

Q. So you've told us whether you can. Tell us how you can tell us whether or not this was from within --

THE COURT: No, you need to go back to the threshold question.

MR. LEIDERMAN: I don't believe he said --

THE COURT: That's --

MR. HEMESATH: I see.

Q. Can you tell, looking at this -- yes or no -- whether or not this came from a Tribune computer?

A. Yes.

Q. How can you tell?

A. I can tell because the IP address or the phone number is not one that was issued or used by Tribune for internal purposes.

Q. I see. Can we take a look at the next entry, please.

So this appears on December 14th; is that correct?

A. Correct.

Q. So what can you tell me about this?

A. Very similar to the prior -- the prior logs. With the same IP address, on December 14th, a user was modified. But this time the user is different, and it's S. Scholbrock 2. But the command was issued from a computer that appears to be the same Macintosh running Firefox.

Q. Okay. And the next one?

Could we -- yeah.

A. Similar to the prior log entry occurring five seconds later. The same save user was attempted or the same save user occurred for username S. Scholbrock with the same computer with Macintosh running Firefox.

Q. Okay. Let's clear this. And fair to say same IP address?

A. Correct.

Q. And the series of dates are what they are, December -- I'm sorry -- December 6th, December 8th, December 14th?

A. Correct.

Q. And all the same version of Firefox and a Mac computer; is that correct?

A. Correct.

Q. All right. Next exhibit, please.

Okay. So now January 2nd. What can you tell us about this?

A. So the IP address has now changed, which is 75.53.171.204. This event occurred on January 2nd. And with the get statement only having a forward slash, a user went to the home page of the application, in this case Assembler.

Q. Okay. What about the next one? What can you tell me about that?

MR. LEIDERMAN: I'm going to object, it calls for a narrative.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. Can you tell us what the difference is between the first one and the second one?

MR. LEIDERMAN: It also calls for a narrative, so objection.

THE COURT: Overruled.

THE WITNESS: So the difference between the first one and the second one, the first one was requesting the content of the home page. The second request is providing the look and feel for the home page.

BY MR. HEMESATH:

Q. Okay. How about the next one after that?

A. This request is providing the image that is specified on the home page and appears to be a favorite icon.

Q. What is the fav icon?

A. That would just be an image on the web page.

Q. Okay. And the next one after that?

A. Again, this is coming from the same IP --

MR. LEIDERMAN: I'm going to object, there's no question pending.

MR. HEMESATH: I'm sorry.

THE COURT: Sustained. Wait for a clear question.

BY MR. HEMESATH:

Q. What can you tell us about the difference between this entry and the previous entry?

A. This entry has the same IP address. The time is very similar. If you look at this entry and the prior entry, it's occurring approximately at the same time. And this is a request for another image, and the image is of the log-in button.

Q. When there are requests for images like that, you may have answered this previously, but is that a typical response when someone is accessing the Assembler system?

A. Yes.

Q. And is it they're just seeing pages coming across like you mentioned about the Google image?

A. Yes.

Q. Can we take a look at the next one.

Is this the same get image response that you were just previously referring to?

A. Yes.

Q. Could I see -- is that the next one?

And is that the same as the previous one with the get image?

A. Yes.

Q. And let's take a look at the next one.

All right. What about this one?

A. This one has the same IP address, the same date. And instead of getting the information, they're sending or uploading a post of information, and information is being posted to the log-in module, which would validate the username and password. And the results of that upload was successful because of the 200 number returned.

And this occurred on a Macintosh computer running Firefox, similar to the log entries above.

Q. All right. And then we have one more there, one more.

And what about this one?

A. This would just be another image file download.

Q. Someone accessed the system, is that correct, on January 2nd?

A. From this response, I cannot confirm that.

Q. Okay. What can you tell us about what a user from that IP address did with regard to the system on that day?

A. Referring to the bottom log entry or --

Q. The collective.

A. The collective.

So from the collective, a user went to the log-in page, the same as if you go to facebook.com. And then a user put a username and password in, similar as to how you would log into Facebook. And with the second to last or the next to last entry, that log entry shows that the log-in was successful when submitted because of the 200 code, which means the user logging into the page had submitted a username and password that was accepted.

Q. Okay. Can you tell what privileges that user might have had from looking at this?

A. No, I cannot.

Q. Okay. All right. Let's take a look at the last page. I like this page.

What can you tell us about the IP address and date on this page?

A. The IP address on this page differs from the prior exhibit, but it's similar to the IP address in earlier exhibits.

MR. HEMESATH: Could we take a look at 008 just to see that.

Q. So that's the same IP address?

A. Correct.

MR. HEMESATH: Okay. So let's go back to 10.

Q. And the date is?

A. The date is December 11th, 2010.

Q. Okay. And what can you tell us about the command that was transmitted on that day?

A. The command that was transmitted was an edit user command for a username of test1234. And that edit was successful, and the request came from a Macintosh computer running Firefox.

Q. Can you tell us specifically by looking at this what the edit was to that particular user on that day?

A. You cannot tell from this entry what the edit was.

Q. Why not?

A. To capture and log all of the information being submitted could, A, have potential impacts on privacy rights and, B, is not sustainable in an environment that receives a hundred to 200,000 requests a day. It would be too much information that would overload the system.

Q. Okay. Thank you very much. I appreciate your patience.

Mr. Kulesza, a personal question, but do you recall what your salary was while you were at the Tribune Company in December 2010?

A. In December of 2010, my salary was 105,000 a year.

Q. That was based on a 40-hour workweek?

A. Correct.

Q. During that period of time when you were responding to this, do you recall -- did you see what people were doing around you?

A.  Yes.

Q.  Co-workers?

A.  Yes.

Q.  What were they doing?

A.  The office I was located at in San Antonio, I observed Armando Caro on the phone with several individuals coordinating with others to respond to the incident.

Q.  Okay.  Anyone else that you were immediately around and could see with your own eyes?

A.  No.

MR. HEMESATH:  One moment, Your Honor.

(Government counsel conferring.)

MR. HEMESATH:  Okay.  Moving on.

Q.  Are you familiar with a concept known as IRC?

A.  Yes.

Q.  How are you familiar with IRC?

A.  I have used IRC in the past.

Q.  Okay.  How much have you used IRC in the past?

A.  I have used IRC to communicate with others on the Internet as well as configured my own IRC server for others to communicate on.

Q.  I see.

What does IRC stand for?

A.  Internet relay chat.

Q.  Okay.

MR. HEMESATH: Your Honor, if I may have one moment to confer with opposing counsel on something that might save us a little bit of time?

THE COURT: You may.

(Counsel conferring.)

MR. HEMESATH: Your Honor, pursuant to oral stipulation and understanding with defense counsel, the government moves Exhibit 605 into evidence.

THE COURT: All right. No objection, Mr. Leiderman?

MR. LEIDERMAN: No, he correctly stated the stipulation.

THE COURT: All right. 605 is admitted and may be displayed.

(GOVERNMENT'S EXHIBIT 605, IRC chat on 12/09/10, ADMITTED INTO EVIDENCE.)

MR. HEMESATH: All right. That's going to be a little hard to see. If we can just get this section.

Okay. And could I have you open your binder up to Exhibit 605 as well.

THE COURT: Just so you know, you've passed the 30-minute mark.

MR. HEMESATH: Oh, my apologies.

Could we take a look at the whole thing again, actually?

Q. Just looking at the form of what you see before you, can you tell what that is?

A. This is an IRC chat log.

Q. What distinguishing characteristics, if any, do you see that make you think that?

A. The characteristics that tell me it's an IRC log, if you look at the first entry of text where you see Evil Boat has kicked someone from #OperationPayback, those are all characteristics of IRC communication.

Q. Okay. So, in general, can you tell us why someone would seek to use IRC?

A. IRC is a form of communication. The difference between IRC and Facebook or Gmail is in an IRC you can own and operate the server for the communication. Versus communicating with someone on Facebook or Gmail, you're going through that third party that then could, ah, manage that communication.

Q. When you say manage, what do you mean by that?

A. That third party has the ability to review what you're sending on their servers and infrastructure.

Q. So if someone sets up their own IRC channel, who can review that content?

A. The only individuals that could review content would be the users connected to the IRC server, and they would only be able to see content within the channels they are joined. Or the -- the server administrator could turn on additional log-in to see communication.

Q. So someone like Facebook wouldn't be able to look at that communication, correct?

A. Correct.

Q. And who can set up one of these IRC channels?

A. Anyone with the technical proficiencies to do so.

Q. And you've set one up?

A. Correct.

MR. HEMESATH: So let's -- well, unfortunately we're stuck with this quality at this point. But could you go through -- we'll take one step at a time and make it a little easier to read. We'll just take a look at this part right here.

Right there would be great.

Q. Okay. So with regard to the first line, can you tell us what that first set of characters mean right here?

A. So the first part, the first portion of this log indicates the date and time that this message and the messaging following the text occurred.

Q. Okay. And on this first line, there appears to be an asterisk right after that date and time. Can you tell us what the asterisk means in this context?

A. The asterisk would mean one of two things. It's a message that was sent by the server or an event observed by the IRC software, and it was highlighted.

Q. Okay. And maybe that will become a little clearer after explaining the next line. So what can you tell us about what's going on on this next line?

A. So on this next line, you'll see again a date and time. And then you have a -- between the greater than, less than symbols, you have what would be referred to as a nickname or a user. This is the person that is sending a message. And then the following text would be the message that individual sent.

Q. Okay. So in this case, is it fair to say that a username odalfe or odalfe has sent a message consisting of exclamation point botnum?

A. Correct.

MR. HEMESATH: Okay. And let's open this up just a little bit here. Can you clear that, please. Let's look at -- okay.

Q. And based on what you said, is it fair to say that a P-A-U-L-L, paull is a username as well?

A. Correct.

Q. And amanikos; is that correct?

A. Correct.

Q. A username?

A. Correct.

Q. AEScracked is a user?

A. Correct.

Q. So in a typical IRC chat session, what would you expect to see in relation to what we're seeing here on this screen?

In other words, is this a typical IRC session as far as you can tell?

A. This would be a typical IRC session.

Q. And do you usually see graphics in IRC sessions?

A. No.

Q. When a user logs into an IRC channel, how is it that they come about on a username?

A. An individual would specify their username when they join an IRC server.

Q. So they can choose any username they want?

A. As long as it's not already in use.

Q. Is there any data about the user that appears when a user logs into the users of an IRC channel?

A. Yes.

Q. What information appears?

A. It would include either one of two things, one being their IP address, which was similar to their phone number; or, two, a name which, similar to caller ID, you would see the name of who is calling.

MR. HEMESATH: Could I get the whole page.

Q. What did -- is it possible to limit users in an IRC channel to only allow certain users in and not certain other users?

A. Yes.

Q. How do you do that?

A. You would set a key for the channel, which would mean you need a password to join the channel.

Q. Who's in charge of setting that key?

A. The first person that joins or creates the channel.

Q. Is it possible to create a channel without a key?

A. Yes.

Q. Are you familiar with the term "IRC logging"?

A. Yes.

Q. What does that mean?

A. IRC logging is generally a setting that IRC software -- it allows you to enable or disable and generally is enabled by default that logs all communications that occurs within an IRC channel.

Q. Is it fair to say it records whatever happens in the IRC log while that user that is running the log does that?

A. Yes.

Q. Does this appear to be an IRC log to you?

A. Yes.

Q. Could you tell me, other than logging, is there any other way that you know of to record what's going on in an IRC chat session?

A. Yes.

Q. What's that?

A. You could take a screenshot of the IRC session, and that would be an image in a point of time of what's being displayed by the IRC software.

MR. HEMESATH: One moment. I'm going to try to save a little more time.

(Counsel conferring.)

MR. HEMESATH: Your Honor, at this time, pursuant to the same understanding as with Exhibit 605, the government seeks to introduce -- the government moves into evidence Government's Exhibit 506.

THE COURT: No objection?

MR. LEIDERMAN: By stipulation.

THE COURT: All right. 506 is admitted as stipulated and may be published.

(GOVERNMENT'S EXHIBIT 506, screenshot of Keys computer, ADMITTED INTO EVIDENCE.)

THE COURT: This is a single page?

MR. HEMESATH: Yes.

THE COURT: All right.

MR. HEMESATH: Okay. Actually let's go all the way back out.

Q. So is this a fair representation of a screenshot from an IRC session?

A. Yes.

Q. What can you tell us about the form of this -- let me rephrase.

Why does this look different than the previous IRC sessions that we were looking at?

A. The previous IRC sessions were logs, which is a text representation of the communication occurring within the IRC channel. This is a screenshot, a capture of the IRC software as well as the communication occurring that was displayed to the user when this screenshot was made.

Q. So why would this look, for lack of a better term, fancier than a regular text representation?

A. This would be the software that an individual would use to communicate and talk with on an IRC server in an IRC channel.

Q. What would this section here tell us about this particular IRC chat?

A. This would show you the users or the nicknames that were in the IRC channel. So we have Chronom, SiteBot, AEScracked, which I believe is a name that was in a prior log, and the last one on the bottom, Sharpie, which appears to be the nickname of the user who is actually using this IRC software.

Q. Okay. So what does it mean that Sharpie has a little bottom bubble or speech bubble above him?

If you don't know --

A. I don't know.

Q. Okay. What does the term "PM" mean in the IRC world?

A. PM is a private message.

Q. Okay. What do these two lines of text up here mean?

A. Those two lines of text would be one of two things, either, one, the channel or, two, the server, but it appears to be the channel.

Q. I see.

So there's two conversations going on?

A. Yes.

MR. HEMESATH: So let's clear that.

Q. And then looking at this part, just for clarity, what's going on in line 2 here? Not with regard to content, but could you tell us who is speaking and what's being done?

A. Correct.

For line 2, there is a nickname or user Sharpie that is sending a message that follows the colon.

Q. Got it.

And that can be seen by the whole chat room?

A. Correct.

MR. HEMESATH: Okay. And then we'll back off of that.

Q. And then to the extreme right, what do we have?

A. Those are times that these messages were occurring. And I would like to clarify on the prior question.

Q. Uh-huh.

MR. LEIDERMAN: Objection.

THE COURT: What's the objection?

MR. LEIDERMAN: The prior question has been asked and answered, and it tends to offer a narrative.

THE COURT: Fair enough.

MR. HEMESATH: I can ask my next question, which is with regard -- can we clear this screen?

Q. In addition to what you previously told us about the meaning of the words before the colon and after the colon, is there anything else that is relevant?

A. It was the question prior.

MR. LEIDERMAN: Objection, calls for a narrative.

THE COURT: Sustained.

MR. HEMESATH: Can we back out.

I'm sorry. I'm getting my questions, previous questions mixed up.

Q. What can you tell us about this number right here in relation to the information to the extreme -- to its corresponding left?

A. So that information there is the time the messages were sent.

Q. Okay. Has everything that you've been telling me in the last five minutes been completely explanatory?

A. Could you further elaborate?

THE COURT: Why don't you rephrase.

MR. HEMESATH: Okay.

THE COURT: If you can.

BY MR. HEMESATH:

Q. What, in addition to what you told me, would be relevant to the identity or time of the data here as shown?

MR. LEIDERMAN: Objection, vague and overbroad.

THE COURT: Relevance is not for this witness to decide, so you can ask a direct question.

BY MR. HEMESATH:

Q. What would you like to clarify that you previously indicated you would like to make a clarification about?

MR. LEIDERMAN: It's vague and overbroad for this witness to define relevance.

THE COURT: Well, this is clarification.

Do you have clearly in mind the question Mr. Hemesath is referencing in this question?

THE WITNESS: I'd like to clarify one of the answers on the prior question after having more exposure to the content displayed.

MR. HEMESATH: I think that's inherently relevant, Your Honor.

THE COURT: Well, we're not asking this witness to decide what's relevant, but I am going to allow him to clarify his answer, and it will be subject to cross.

So just very -- you were going to add something to an answer?

THE WITNESS: I was going to more appropriately answer the question based off of what I've seen with this evidence.

THE COURT: What was the question?

THE WITNESS: The question was regarding if the information being sent could be viewed by all users in the channel.

THE COURT: All right. So what is your answer to that?

THE WITNESS: No, it could not. It was a private communication.

THE COURT: All right. Mr. Hemesath.

MR. HEMESATH: So let's talk about that.

Q. What you're seeing on this particular screen, how can you -- was this a private communication?

A. Yes, it was.

Q. How can you tell whether it was a private communication?

A. By observing the username Sharpie being highlighted and the content being displayed with communication between Sharpie and AEScracked. This is a private communication between those two individuals.

Q. So fair to say because this was highlighted this was a private message?

A. Yes.

Q. Got it. Okay. Sorry about that.

Okay. And I'm not sure if we got it, but does this time to the extreme left correspond to the time this message was sent?

MR. LEIDERMAN: Objection, it's been asked and answered.

THE COURT: So withdrawn?

MR. HEMESATH: One moment.

Your Honor, no further questions.

THE COURT: All right. Mr. Leiderman?

MR. LEIDERMAN: Thank you, Your Honor. Just one second, please.

CROSS-EXAMINATION

BY MR. LEIDERMAN:

Q. Good morning, sir.

A. Good morning.

Q. I'm going to go a little bit out of order just because that's the way my notes are. If you're confused by it, please let me know, and we'll back track.

The first thing I want to ask you is, you went through I don't know how many logs but a lot of logs. You recall that, correct?

A. Yes.

Q. And most if not all of these logs had what I'm going to call a web address in them, assembler.tribuneinteractive.com; is that fair to say?

A. Yes.

Q. Is that what's called a front facing website?

A. Yes.

Q. And what is a front facing website?

A. A front facing website would be one available to users and displayed -- potentially exposed on the Internet to users.

Q. And I guess you say potentially because assembler.tribuneinteractive.com is not something that would typically come up in a Google search, for example?

A. Correct.

Q. But if someone were to type into their browser window assembler.tribuneinteractive.com, in fact that site would come up?

A. Yes.

Q. And what would a viewer see on that site?

A. A viewer would see a request for username and password.

Q. So this is not the site where you would see content on the Tribune Company -- on any Tribune Company property?

A. Correct.

Q. Did you meet with the government in connection with this case?

A. I spoke with them on the phone.

Q. Just once or twice?

A. I can't recall.

Q. Did you have a conference call -- did you have one conference call with and one conference call without Timothy Rodriguez on it?

A. I do believe I had a conference call at some point, but I can't recall the number of communications with the FBI.

Q. Okay. Well, were the conversations not just with the FBI, but with James Silver, Paul who just directed you, Mr. Hemesath, and Matt Segal?

A. I believe any communication was prior to the actual incident occurring.

Q. Prior to -- you spoke with the FBI prior to --

A. No, post the incident. So to clarify that, any communication with them occurred some time period after the incident had occurred.

Q. Okay. Does the -- were they recently, like within the last month or so?

A. These communications, yes.

Q. Okay. These two communications in specific?

A. Yes.

Q. And then there were other communications that were just you and the FBI?

A. Correct.

Q. And I'm just asking you with respect to these last two communications.

Was one -- it sounded like to you, if it refreshes your recollection, one in August and one in September?

A. Of this year?

Q. Yes.

A. Correct.

Q. And one was just about a week ago or just exactly a week ago?

A. Yes.

Q. And did you discuss your testimony with respect to this case?

A.  Yes.

Q.  Okay.  You do have a clear recollection of speaking with the government a week ago, right?

A.  Yes.

Q.  Going back to 2010, you were the -- did I get it right, you were the VP of engineering, security and architecture for the Tribune Company?

A.  Not in 2010.

Q.  What were you in 2010?  I'm sorry.  What was your job in 2010 with Tribune Company?

A.  I had two jobs in 2010, originally as a data architect and then as a principal security architect.

Q.  What does a data architect do?

A.  Business intelligence and data warehousing.

Q.  What does business intelligence mean?

A.  Looking at large amounts of information and trying to create simplified metrics to show value or characteristics of data you're looking at.

Q.  So essentially what you went through on the screen?

A.  Yes.

Q.  And you said you had another job, which I have forgotten?

A.  I was a principal security analyst or principal security architect in 2010.

Q.  What does that mean?

A.  I was primary for the security team in Tribune.

Q. So it was your job to respond to incidents like this?

A. Correct.

Q. And were there other incidents like the one we're talking about?

A. Not of this magnitude in 2010.

Q. Were there -- can you describe the typical smaller incident, if there was -- was there a typical smaller incident?

A. Yes.

Q. And what were those like? Can you describe them?

A. A security incident could be something as simple as an individual losing a phone or a laptop. It could be a conversation with HR understanding what websites an employee was visiting or something of more magnitude and impact such as a breach of confidential information or defacement of a website.

Q. You had defacement of websites prior to 2010?

A. I am not aware. I joined in 2010.

Q. Okay. Why did you mention defacement of a website?

A. That is in the classification of security incidents that could occur.

Q. Gotcha.

You said the largest incident was this Chippy 1337 incident?

A. Correct.

Q. And you were calling it Chippy leet?

A.  Correct.

Q.  And I think we already went over with Mr. Caro what leet is.  But just briefly can you tell us why you say leet as opposed to 1337?

A.  Because 1-3-3-7, 1337 is the numeric representation of the characters L-E-E-T.

Q.  Is L-E-E-T, is that also the name of a language?

A.  I'm not aware.

Q.  Do a lot of people that, let's say, hang around IRC use numbers in their nicknames as opposed to characters, numbers that correspond with characters?

A.  They can, yes.

Q.  For example, an A would be a 4 or a T would be a 7?

A.  Yes.

Q.  And you're not aware that that language is called leet; is that what you said?

A.  So if you're referring -- I believe the term might be leet speak.

Q.  Leet speak, yes.  That's what I'm asking about.

A.  Yes.

Q.  Okay.  So replacing a number with a -- just to summarize, what you said was replacing a letter with a number is leet speak?

A.  Yes.

Q.  That's because, quote/unquote, elite people use it?

A. I believe so, yes.

Q. All right. But in reality you don't have to be elite to use it, and in fact most users aren't elite in the computer or gaming field?

MR. HEMESATH: Objection, compound.

THE COURT: Sustained.

BY MR. LEIDERMAN:

Q. In fact to use it, you don't have to be elite; is that correct?

A. No.

Q. And is it true that a lot of the users aren't elite in the gaming field?

A. Correct.

MR. HEMESATH: Objection, relevance.

THE COURT: Overruled.

BY MR. LEIDERMAN:

Q. And is it true that a lot of users aren't elite in the computer programming field?

A. Correct.

Q. You said you started to triage the incident almost immediately?

A. Yes.

Q. Was it that day, December 14th, or December 14th the day of the defacement?

A. I believe so.

Q. And are you -- are you privy to the fact that the article in question was up for only 40 minutes?

A. Yes.

Q. Are you aware of who Chippy is?

A. No.

Q. And you did some Internet research on it?

A. Yes.

Q. Are you familiar with something called the urban dictionary?

A. Yes.

Q. Did it have an entry for Chippy 1337?

A. I'm not aware.

Q. What is the urban dictionary?

A. It's an online website where anyone can submit a definition for any word that they'd like to create as a common language.

Q. And would that have been one of the things you checked for Chippy 1337?

A. Not directly.

Q. What do you mean not directly? Perhaps through a Google search?

A. I would do Google first and see what becomes relevant.

Q. So as you sit there today, you don't know who Chippy is?

A. No.

MR. HEMESATH: Asked and answered.

THE COURT: Overruled.

BY MR. LEIDERMAN:

Q. Did you come to a conclusion about how someone could have accessed the L.A. Times content management system?

A. Yes.

Q. Were you able to lock that person out or that user out?

A. I was not responsible for locking the individuals out.

Q. Based on your review of the information, was that user locked out?

A. I believe there was multiple users that had to be locked out.

Q. You mentioned that the user could have possibly gotten in through brute force; is that correct?

A. I don't believe I mentioned brute force.

Q. I'm sorry. Not in direct here today, but in your interview a week ago with the government.

A. I believe that is one of the possible ways someone could compromise the system, yes.

Q. Can you explain what brute force is?

A. Brute force would be trying numerous username-password combinations and hoping to gain access.

Q. Guessing?

A. Yes.

Q. Was there an upgrade deployed in the system?

A. In reference to?

Q. Well, let's talk about the whole Tribune Company system to begin with.

MR. HEMESATH: Objection, vague as to time.

MR. LEIDERMAN: I'm talking --

THE COURT: Sustained.

MR. LEIDERMAN: I'm talking about in response to the December 14th incursion.

THE COURT: All right. You can answer.

THE WITNESS: The initial incident caused us to -- you know, going back to the house analogy, if someone breaks into the house, the first thing you're going to do is, one, see if anything has been stolen; two, make sure that there is still no one else inside, that you're not in harm's way; and, three, begin immediately trying to secure the house. So if they kick in the door, you're going to replace the door, you're going to lock it.

As far as upgrading, changing out your locks, putting in a security system, those activities take time and money to implement.

BY MR. LEIDERMAN:

Q. But they were done in this case?

A. Over a period of time, yes.

Q. Do you know what that period of time was; do you recall?

A. Somewhat generic, but this incident caused an awareness to executive leadership to put more investment in security.

Q. So finally the big bosses understood that you needed more security based upon this incident?

A. Yes.

Q. Sir, you can move that microphone closer to you if it would help. I notice you're leaning down each -- is that better?

A. Perfect. Thank you.

Q. Okay. So actually you never gave me a time frame. Did this take a week, a month, six months, a year?

A. Security is ongoing, but activity started to occur six months to a year after the incident.

Q. Still in response to the incident?

A. Correct.

Q. Can a nickname, IRC nickname, can it be used in different channels at the same time?

A. An IRC nickname is unique on the IRC server, but a nickname can be in multiple channels at the same time.

Q. And are different channels sometimes dedicated to different things?

A. They can be, yes.

Q. Some channels, for example, can be related to a particular game or gaming, and some of these channels that you're looking at can be related to some anonymous operation?

A. They could be, yes.

Q. Were these channels on the 2600 server? I'm sorry. Let me ask a foundational question.

Are you familiar with the 2600 server?

A. I'm familiar of 2600, the publication.

Q. Are you aware that they run an IRC server?

A. No, I'm not.

Q. Oh.

Do you know what server these chats were happening on?

A. No, I do not.

Q. During your investigation of this incident, you learned that nothing else was altered but the Chippy 1337 article, for lack of a better term on it?

A. Yes.

Q. So when you used the house analogy, you talked about immediate response. But in the long term essentially you built either an entire new house or at least large portions of a new house; is that fair to say?

A. Loosely, yes.

Q. I want to go back to those logs that you analyzed.

Is it fair to say that a web browser, the web browser that was used can be spoofed in those logs?

MR. HEMESATH: Objection, vague, foundation.

THE COURT: Sustained. You can ask a foundational question.

BY MR. LEIDERMAN:

Q. What is spoofing?

A. Spoofing would be altering the information being sent.

Q. And you recall in the web logs that you just reviewed, you said that there was something called Mozilla, which was a browser, and then the most common part of Mozilla was Firefox.

And then you found a Firefox in fact in some of the logs you --

MR. HEMESATH: Objection, compound.

THE COURT: Sustained.

BY MR. LEIDERMAN:

Q. Did you find the word Firefox in some of the logs that you looked at?

A. Yes.

Q. And what did Firefox mean to you?

A. Firefox meant the web browser that accessed the site.

Q. Could that be spoofed?

A. It could, yes.

Q. Meaning a different web browser could have been used, could have actually been used?

A. It could, yes.

Q. And you talked about Ms. Scholbrock's password being changed. Do you recall that?

A. Yes.

Q. And that when you examined those logs, it had Macintosh and Mozilla in it; is that fair to say?

A. Yes.

Q. And is it also fair to say that those password changes could have been made from any computer using Mozilla, presuming it's not spoofed, Mozilla and Macintosh, that version of Macintosh?

A. It was could only have been made from the IP address in the log, but the Mozilla and Macintosh could be spoofed.

Q. And in terms of the incursions themselves, none of them were done in the L.A. Times specific -- none of them were L.A. Times specific; is that fair to say?

MR. HEMESATH: Objection, vague.

THE COURT: Overruled. You can answer if you're able.

THE WITNESS: Are you referring to the incidents or IP addresses?

MR. LEIDERMAN: IP addresses and change of those logs that said test1234.

THE WITNESS: None of the requests appear to have come from any L.A. Times network addresses.

BY MR. LEIDERMAN:

Q. In your review of logs, did the names Kayla, Sabu and Sharpie come up?

A. Which logs?

Q. Did you review IRC logs in connection with this case other than the ones you just reviewed?

A. There were logs submitted by Tribune that were IRC logs, but not -- I don't recall those names coming up.

Q. It's been five years since you examined these?

A. Correct.

Q. You don't remember every nickname there was?

A. Correct.

Q. Lots of nicknames, sir?

A. Correct.

Q. And over the 15 years you've been using IRC, fair to say there are tons, scores of nicknames?

A. Correct.

Q. Presuming a nickname isn't already on an IRC server, can someone else use it?

You need a better question than that? I can rephrase.

A. It's technology. It's always complex.

Q. I get that. You want me to rephrase?

A. Please.

Q. Okay. Let's say the password -- let's say someone is using a nickname of 1234. Presuming that person isn't in IRC at that time, that they've logged out, can someone else use the nickname 1234?

A. It depends.

Q. Actually what does it depend on?

A. It depends if the IRC has services to protect nickname misuse.

Q. And do people call that service locking, locking the nickname?

A. It depends.

Q. Is that one of the things that people call it?

A. I haven't heard that specific term, but certain IRC services allow you to reserve nicknames, but it's not commonplace.

Q. Are you aware of whether or not the IRC that we're dealing with in this case allowed you to -- I'm going to use the word "lock" a password or reserve. You used the word "reserve"?

A. Typically if a nickname is reserved, it changes your nickname or kicks you off within 30 seconds to a minute if you're misusing it.

Q. What does misusing it mean? Oh, if someone else is using it?

A. Correct.

Q. Okay. The question is withdrawn, then. Well, no, it isn't. Sorry.

THE COURT: It's in the record.

MR. LEIDERMAN: Exactly.

Q. There's a line in the IRC logs you reviewed that said they were going to do something just for LULZ, L-U-L-Z.

Are you familiar with the term LULZ?

A. Yes.

Q. What does it mean?

A. That was a term used by Anonymous in most of their security breaches of various organizations.

Q. What does the term L-U-L-Z mean?

A. For laughs.

Q. Is it a kind of perversion of LOL?

A. Correct.

Q. And is it used just by Anonymous or is this a common Internet term, something that has grown into the lexicon?

A. I would say Anonymous made it more in the lexicon.

Q. But it existed before Anonymous became -- or even became a thing?

A. I'm sure it could have.

Q. Have you ever heard of the groups Internet Feds or LulzSec?

A. I've heard of LulzSec.

Q. Did you see in the logs you reviewed that they said Internet Feds?

A. I did.

Q. And I guess you're saying you don't know who Internet Feds are?

A. I'm not aware.

Q. Did you notice that a lot of the nicknames in Internet Feds matched the nicknames in LulzSec?

MR. HEMESATH: Your Honor, foundation and beyond the scope of direct. We didn't get into the content.

THE COURT: Sustained.

How much longer do you think you have on cross?

MR. LEIDERMAN: I have one more question, but I can't understand my own -- if I may have a second.

THE COURT: All right.

(Defendant conferring with his counsel.)

MR. LEIDERMAN: Okay. Seems I fooled myself.

Q. All right. The IRC times that you were talking about, do you recall that?

A. Yes.

Q. All right. Are those all in what you referred to earlier as GMT?

A. I could not tell in the IRC if they were GMT time.

Q. You'd have to see, for example, what you saw in the logs, which is minus or negative 800, negative 0800?

A. That's one way, yes.

Q. What's another way? What's another way that relates to IRC?

A. Regarding?

Q. What time these -- I want to know what actual time these comments were made in the IRC.

A. I cannot tell you whether or not the time is server or client based.

Q. If it was server based, it would be in GMT?

A. It depends.

Q. Oh, by the way, sir, let's go back a second.

What is GMT?

A. Greenwich mean time, which is the standard time that all time zones are keyed off of.

Q. It's the primary one --

A. Correct.

Q. -- of Greenwich, England?

A. Yep.

Q. And GMT minus 0800 is Pacific standard time?

A. I believe so, yes.

MR. LEIDERMAN: I don't have anything further.

THE COURT: All right. How much time would you need for redirect?

MR. HEMESATH: Maybe five minutes.

THE COURT: All right. Can we take the five minutes and then take our next break?

All right. I'm going to let you know when five minutes is up. This time you're standing in the way of a break.

MR. HEMESATH: I should have said ten.

THE COURT: Attorneys are at their best when they're required to condense, in my experience.

REDIRECT EXAMINATION

BY MR. HEMESATH:

Q. Mr. Leiderman asked you about your job and your response to incidents.

If you weren't responding to this incident, what would -- what else would you have been doing?

A. I would have been doing daily activities, such as working with other teams and ensuring they were developing secure software. You know, working with other teams in the organization to make sure they had security awareness.

Q. You weren't permitted to do nothing?

A. Correct.

Q. Mr. Leiderman asked you if there were any other defacements in 2010.

Are you aware of any other defacements of this magnitude throughout the entire time you were at Tribune?

A. Not of the same level of impact to the customer.

Q. And who do you define as the customer?

A. Any subscriber, any individual that would go to latimes.com to visit the website and read news articles.

Q. Mr. Leiderman asked you about whether the story was only up for 40 minutes, and you said that that was your understanding.

Do you have any knowledge about whether the mobile site was different or changed or how long that might have been different?

A. It's very possible the mobile site was changed.

Q. I don't want to ask you to speculate. If you don't know, then --

A. I'm not a hundred percent --

MR. LEIDERMAN: Move to strike the speculative answer.

THE COURT: There's no real answer, so just move on.

BY MR. HEMESATH:

Q. Mr. Leiderman asked you about brute force attacks.

What in the system protects against brute force attacks?

A. If an application is coded and designed to lock out an account after defining a number of attempts to log into the account with a given password.

Q. Was there any evidence of a brute force attack here?

A. No.

Q. Mr. Leiderman asked you about upgrades and about a period of time after which there were -- during which there might have been upgrades.

Do you know what upgrades were actually performed to your system?

A. I'm not aware of which upgrades were performed to Assembler.

Q. Other people were in charge of that?

A. Yes.

Q. What about beyond Assembler, to the system in general, any upgrades that you're aware of specifically?

A. The only upgrades I'm aware of are the upgrades to the security program to better protect all assets in the organization.

Q. And do you know how much those cost?

A. Anywhere between one to two million for upgrades that occurred in the year or two years prior.

Q. Okay. And one last question hopefully.

Mr. Leiderman asked you whether you were aware that anything else was altered in the content management system other than the story itself.

MR. LEIDERMAN: Objection, misstates the question I asked.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. Do you recall Mr. Leiderman's question with regard to whether anything else was changed?

A. Yes.

Q. And you answered nothing; is that correct?

A. Yes.

Q. How long did it take you to confirm that nothing else was changed?

A. There were other teams that confirmed it. Personally I wasn't involved in it.

THE COURT: So stop there.

MR. HEMESATH: Thank you. Nothing further.

THE COURT: All right. Let's go ahead and take our break. The attorneys can confer and see if we need to continue with this witness after the break. A 15-minute break or however much time you need as close as possible to that. Remember my admonitions as always. We'll see you when the break is over.

(Jury not present.)

THE COURT: You may step down. If they need you, be back in 15 minutes.

All right. Do you need more recross?

MR. LEIDERMAN: Oh, no. He can be excused.

THE COURT: You would agree, Mr. Hemesath?

MR. HEMESATH: Yes, Your Honor.

THE COURT: All right. Sir, you're excused. Thank you very much.

We'll let the jury know that the government can be ready with its next witness in 15 minutes.

MR. SEGAL: Your Honor, would you like the witness to be on the stand when the jury comes in?

THE COURT: That's fine.

MR. SEGAL: Okay.

(Recess taken.)

(Jury not present.)

THE CLERK: Come to order. Court is back in session.

THE COURT: All right. Let's bring the jury in.

(Jury present.)

THE COURT: Welcome back, Ladies and Gentlemen. You may be seated.

The government is ready to call its next witness.

We excused, Mr. Kulesza. Am I saying that right, Kulesza? He has been excused.

The government's next witness.

MR. SEGAL: Your Honor, the United States calls Mr. Tim Rodriguez.

THE COURT: All right.

THE CLERK: Mr. Rodriguez, please come forward. I need to take your photograph this afternoon. If you can stand with your back against the wall facing me. Thank you.

All right. Step into the witness stand behind you, remain standing and raise your right hand.

TIMOTHY RODRIGUEZ, GOVERNMENT'S WITNESS, SWORN

THE WITNESS: I do.

THE CLERK: Thank you. You may be seated.

THE WITNESS: Thank you.

THE CLERK: Will you please say and spell your first and last name for the record.

THE WITNESS: Sure. Timothy P. Rodriguez. T-I-M-O-T-H-Y, R-O-D-R-I-G-U-E-Z.

THE COURT: All right. You may proceed. We have until 1:00 today.

MR. SEGAL: Thank you, Your Honor. We're hoping to do this witness and one more.

THE COURT: All right.

DIRECT EXAMINATION

BY MR. SEGAL:

Q. Good afternoon, Mr. Rodriguez.

A. Good afternoon.

Q. In what line of work are you?

A. I do security and forensics.

Q. And for how long have you been doing that?

A. About 18 to 20 years.

Q. What was the training you had before you actually started working in the area?

A. There was a lot of on-the-job training, and I'm a certified system and network auditor. So I have a lot of certifications from a lot of other vendors for security firewalls, networking and things of that nature.

Q. Okay. You want to just briefly walk us through your career up to January of 2011?

A. Okay.

Q. But slowly.

A. So I worked at a number of different institutions, hospitals, insurance agencies, other medical centers and banks. And I started doing -- I started on the help desk and worked my way up to server support, and from there I started doing networking. After I left networking, I started doing security, and I do security now full-time at my current employer. But I've worked, once again, at different hospitals, medical organizations, insurance agencies and banks.

Q. Okay. Are you at Tribune now?

A. No, sir, I'm not.

Q. Okay. In January -- have you ever worked at Tribune?

A. Yes, I did.

Q. What was your first day?

A. Well, my first day was actually handling the information for this case, going to group --

Q. Wait, wait.

What day was your first day?

A. January 3rd, 2010.

Q. Okay. And into what title were you hired into? What were you supposed to do?

A. So what I was supposed to do was -- we had green-fielded the whole security team, so my job there was to backfill the security position that had a lot of different roles and responsibilities, one of them being investigating things like compromises and incidents.

Q. Okay. And I know it's not usually what we ask people, but when you were hired in, at what salary were you hired?

A. I believe it was at 101K a year.

Q. Okay. A 52-week year?

A. Yes, sir.

Q. And a 40-hour normal workweek?

A. Yes.

Q. Okay. So January 3rd, 2011, who was your supervisor?

THE COURT: That wasn't -- that wasn't his testimony.

BY MR. SEGAL:

Q. What was your first day at Tribune?

A. January 3rd, 2011, I believe.

THE COURT: All right. I think he said 2010 before.

MR. EKELAND: He did.

THE COURT: Are you certain about -- what is the date when you started?

THE WITNESS: I'm sorry. It was 2011.

THE COURT: All right.

MR. SEGAL: We -- this will become clear.

Q. Which is true, did you have a slip of the tongue that I heard wrong or --

A. Yes, I did, a slip of the tongue. Sorry. I apologize.

Q. All right. So on January 3rd, 2011, who was your boss?

A. I worked for Armando Caro. He was a technical director.

Q. All right. And first day on the job, to what project did he assign you?

A. He assigned me to look into the incident where Chippy leet had defaced one of our websites on some of the bylines.

Q. What were you trying to -- on January 3rd, what were you instructed to assess?

A. Well, I was instructed to assess where the break-in happened, if the break-in was continual, and if the perpetrator was still inside the Tribune systems.

Q. How important was it to assess how the break-in happened?

A. It was critical to assess how the break-in happened because the way the break-in happened is germane to the rest of the opportunity that the person who perpetrated this act would have access to all other systems or, in fact, have access to a system where they can jump off and attack other Tribune systems.

Q. How important was it to assess whether they were still in the system?

A. That's very -- that was extremely important because they could alter other bylines, they could alter other Tribune systems and make it so that we would not be able to detect that they were there.

Q. They could do it so that what?

A. They could -- what they could do is they could jump off to other systems, so they could delete logs so that we wouldn't know what systems they were, create user accounts and then use those accounts to garner other Tribune Media sites and/or financial information.

Q. When you say creating user accounts, is there a security term or shorthand for that kind of conduct?

A. Yes.

Q. What is it?

A. Back doors.

Q. Okay. So my next question, how important was it to assess whether there were any more back doors?

A. That was critical because an open back door would not only give them access to resources now but resources in the future, and they could pull down other information unbeknownst to us.

Q. I want to ask you what other systems at Tribune you were concerned about. Can you name some of them, please?

A. Sure.

Other than the Assembler system, we were concerned with our LDAP systems, if they could get in there and tamper with those.

Q. And what was the LDAP system?

A. The LDAP system is the authentication system you use when you log in.

Q. Okay. What other systems?

A. We have financial systems that were on the same network. We have other websites which we host other papers called the Red Eye, the Chicago Tribune, the actual newspaper itself. And then they could jump off and attack some of the different TV and radio stations that we had.

Q. What in your business did the plates mean?

A. What the plates are is --

Q. Do you want to move the microphone away from you or down a little bit. That might be -- there you go.

A. What the plates are is if you could -- if you could alter the plates --

MR. LEIDERMAN: I'm going to object. Altering plates is speculative.

THE COURT: Sustained.

MR. LEIDERMAN: And move to strike.

THE COURT: That answer is stricken. Rephrase the question and -- or at least restate the question. He's not answering the question.

MR. SEGAL: Okay. Yes, Your Honor. Thank you.

Q. What were the plates?

A. The plates, when a newspaper prints out a -- when a newspaper prints out the daily newspaper, what the plates are is a -- it's like a set of printing instructions so that you can print out thousands of copies of a newspaper. If there is an error in that thousands of copies, we have wasted paper, we wasted circulation. And if the paper went out, then it's technically inaccurate, and it would have to be corrected.

Q. All right. And in 2010 -- or I'm sorry --

MR. LEIDERMAN: I'm going to object again as irrelevant.

THE COURT: Overruled.

BY MR. SEGAL:

Q. In 2011, was there a relationship between the plates and your computer network?

A. Yes, they were directly connected.

Q. Okay. Explain that, please.

A. So you could get on a computer network, alter the plates where you can actually change stories and change information before it went out to print, thereby causing, you know, untold thousands of dollars of damage or millions.

Q. So what did you want to assess with regard to the computers that controlled the plates?

A.  We wanted to make sure that the computers were -- were not hacked and didn't have back doors or accounts that were recently changed or changed so that an opportunity to deface them could happen.

Q.  You discussed also financial systems.  What kinds of financial systems did Tribune use?

A.  We took information for circulation of newspapers and subscriptions through credit cards, online checks and things of that nature.

Q.  Okay.  And what was important for you to assess with regard to those financial systems?

A.  Once again that they weren't hacked, computer accounts weren't changed, and no back doors were put in any of the systems.

Q.  All right.  So let me ask you what you did.  What did you do to assess what was going on on the LDAP system with regard to further back doors?

A.  So what we did is we had the system administrators check the accounts.  There's a number of accounts on the LDAP system, so what we did is we checked each account for one verified user and made sure that password wasn't changed within the scope of 30 days prior or post to the incursion happening.

Q.  What did you do on the financial systems to assess the integrity of your systems?

A.  Basically the same thing.  And then what we do is we look through the logs, and we made sure that anyone who accessed the systems were inside Tribune and had a legitimate reason. And then, once again, we looked through back door accounts, any account that was changed or created in the last 30 to 60 days.

Q. And what did you do on the systems that controlled the plates to assess the integrity of your system?

A. We performed the same functions. We checked to make sure that all the IDs were valid on the plates. We removed IDs of people who were actually terminated, who were no longer working at the company. And we just did a check on the system files to make sure that they were -- they were correct and unaltered.

Q. Were you -- the things we've been talking about, were you personally involved in those things?

A. Some of them, yes. Some of system administrators -- I didn't have access to any of the systems as per my role. The system administrators actually performed the duties and the tasks and correlates into the hours that they performed these duties and tasks. My job was to create a CSIRT process, a computer security emergency --

Q. No, go ahead, you were explaining CSIRT. Go ahead.

A. A computer security emergency process so that they could understand what the responsibilities were, what they had to check and to communicate with me just in case there was another back door or another system that I wasn't aware of so we could put that in focus.

Q. Okay. So you're directing this cast of characters out there?

A. Yes. And they would deliver the data to me after they actually solved it. And they sent me the data so that I could analyze it and submit it as evidence to an electronic CD.

Q. Were there any other systems that you performed damage assessment on?

A. Well, the number of systems we performed was quite large. Tribune doesn't work with one computer, one server. There's many servers that, ah, correspond to our web presence on the Internet. There's literally hundreds of servers with thousands of pages and archives and things of that nature. So that was a very monumental task within itself.

Once again, the financial systems had many servers that housed that data, and then the plates. There's a small amount of data on the plates, but there's a lot of access that goes to that. So we had to check each computer that accessed the server that controlled the plates.

Q. Okay. So now just asking you about your job alone, the hours that you spent at $102,000 a year, how much time did you spend on the tasks that we just described?

A. I spent 50 hours.

Q. Okay. Did you do -- what did you do to keep track of the the time that you spent?

A. I -- every time we had a conference call or I met with system administrators or managers, I just -- I just copied down that time as I was taught to do on a sheet of paper, which unfortunately I don't have, and I tabulated out the information.

And then I went to each person --

Q. Wait. Just -- no, not them. Just you, please.

A. Sorry.

Q. You gotta remember that. So -- but we'll go to that.

MR. SEGAL: Let's look at Government Exhibit 306. That's that big piece of paper that is taped up there in front of you. For identification only, Your Honor. I've told the defense that I don't intend to offer this into evidence.

THE COURT: All right.

BY MR. SEGAL:

Q. Do you see that?

A. Yes, sir.

Q. What is that?

A. This is a list of the functional titles, names, preventive hours, software code, redesign hours, analysis and investigative hours, the total hours, their hourly wage, and what the total is from all categories from left to right.

Q. Okay. You said that you were directing people to do things as part of your job. Can you look down the name field there and identify who among them were people that you directed to do things?

A. Sure.

Tom Comings was one of the people that helped me actually discover who -- what ID was used to change the byline.

Let's see.

Craig Hancock and Sabrina Downard, they actually reviewed the LDAP logs to find specific time and date when that person was, ah, authorized with that garnished credential.

Greg Noth, Brandon Zylstra and Jason Potkanski actually did a lot of -- did a lot of analysis and investigative hours to look through not only the Assembler system, but everything that connected with P2P.

Q. And that's Greg Noth, Brandon Zylstra, Z-Y-L-S-T-R-A, and Jason Potkanski, P-O-T-K-A-N-S-K-I?

A. Yes, sir.

Q. Okay. Anybody else?

A. The software development team consisted of Joe Bezouska --

Q. Okay. If the software development team is upgrading, I'm not interested in that. Have you moved to upgrades now?

A. No. What they were doing is they were redesigning the way this code was accessed, and there were some vulnerabilities that they actually addressed that at the time we didn't -- we didn't know whether they used those or not to -- we didn't know if they garnished the system ID until a little bit later.

Q. Okay. So still part of your incident response?

A. Yes.

Q. Okay. Who are they?

A. Joe Bezouska, Casey Conor, and Brian Heusinkveld.

Q. Okay.

MR. SEGAL: I'll give the Reporter the list.

THE COURT REPORTER: Thank you.

MR. SEGAL: Okay. Thank you.

Q. Now how many hours are recorded here for you?

A. There is 50 analysis and investigative hours recorded for me.

Q. And we went -- we approached this first, but can you tell the jury, please, how your notes were accumulated and got to that number on this document?

A. Okay. So every meeting we had with either each one of these people or specific teams to find out what systems Assembler connected to, web searches that we actually had to -- or the web blogs we had to analyze to get this, and then how many other systems that they actually looked through to make sure credentials, A, weren't changed or that a specific credential was not present on that system.

Q. Okay. And then you took that time and recorded it in a note, right?

A. Yes.

Q. And -- all right.

In 2011, how late in 2011 were you still trying to figure out the extent of the damage to the integrity of your systems?

A. I think I have noticed in the case log --

MR. LEIDERMAN: Your Honor, I'm going to object to the characterization of damage.

THE COURT: Sustained.

BY MR. SEGAL:

Q. How late in 2011 were you still assessing the integrity of your systems?

A. I don't have the exhibit, the report. I have -- I have the exact date, and I want to be exact with it.

Q. Would it refresh your recollection --

A. It's been almost five years, so --

Q. Is there a document that would refresh your recollection?

A. Ah, yes. It is the report that I submitted for the incident.

MR. SEGAL: May I have a moment, Your Honor? I gotta go find that exhibit number.

THE COURT: You may.

Can you move on to another set of questions?

MR. SEGAL: Yes, I can, Your Honor. While that's going on, I'm going to move on and approach it at the end of the exam.

Q. Do you remember in what month it was, yes or no?

A. Yes, I believe it was either at the end of January or the beginning of February.

Q. Okay. After that, after that was over, did Tribune Company take any measures to upgrade its systems?

A. Yes. We discovered that there was a lot of systems that needed to be upgraded.

Q. The answer to that is yes?

A. Yes.

Q. Okay. We've used an analogy about a break-in to a house, and the initial response is kind of seeing if they're still there, if there are back doors and that kind of thing. And the upgrade is putting in a security system or installing a new and stronger door, that kind of thing.

Are you comfortable with that analogy?

A. Yes.

Q. Okay. So if I understand you correctly, your 40 hours -- I'm sorry -- your 50 hours until whatever time --

MR. SEGAL: And I have the document here. I'm going to refresh recollection with Defense Exhibit P.

THE COURT: All right. That's in a separate binder behind you.

MR. SEGAL: May I approach, Your Honor?

THE COURT: Well, can you open the binder? Let's see if you can find it quickly. Is there a number that corresponds?

MR. SEGAL: Yes. It's behind tab 16, Mr. Rodriguez.

THE COURT: All right. You may ask about the document. You've found that? It appears to be quite a few pages.

MR. SEGAL: Yes.

Q. If you look at that, can you tell about how --

THE COURT: What's the question?

MR. SEGAL: The question is, in what month was he finished assessing the integrity of the systems? If you can tell from this report.

THE WITNESS: Yes. It was January 25th before I started sending information to Agent John Cauthen.

MR. SEGAL: January. Okay.

Q. Now, after that, I want to ask you how important was it to Tribune Company to upgrade and make sure this couldn't happen again even once you'd re-secured the system?

A. Well, I think that that's critical to make sure that this couldn't be appropriated again from either another individual or another set of individuals. Because we were -- we're an active target because they were a large media company. So usually hackers like to target the larger media companies.

Q. Okay. How much did management approve upgrading your systems to secure against a future attack?

A. We planned, we developed, and we brought in technologies that can help us detect and prevent these types of breaches.

Q. Do you recall about how much money was spent?

A. It was in excess of $450,000, I believe.

MR. LEIDERMAN: I'm going to object. This is the wrong witness. It's beyond the scope. It calls for implied hearsay.

THE COURT: Well, the jury shall disregard that answer for now. If you can lay more of a foundation.

BY MR. SEGAL:

Q. What was your involvement in upgrading the system?

A. We specked out --

Q. Well, it's you, it's not we.

A. I'm sorry.

Q. You individually. And if it's not you, then that's the truthful and adequate answer, just whatever it is.

A. What I did was I performed some penetration and an application testing process. I not approved, I recommended to my boss, Armando and Dylan, that we purchase this type of solution so we could run these. We bought -- I recommended, because I tested an event gathering system called Nitro that gathered logs so we can actually see if this was happening again through not only those systems, but other systems as well, and they were very expensive.

If you put all those systems together, I think they were --

THE COURT: Well, wait for the next question.

MR. SEGAL: Okay.

Q. Now do you -- in that process, when you were personally engaged in it, did you see prices for those applications?

A. Retail prices, yes.

Q. Okay.

THE COURT: He recommended.

MR. SEGAL: Oh, sure.

THE COURT: So --

MR. SEGAL: I'll close it up.

Q. Were your recommendations followed?

A. Yes.

Q. Okay. And did you see, as part of your job, the prices -- what were the retail prices that you saw?

MR. LEIDERMAN: I'm going to object to the retail prices if he doesn't know what Tribune Company paid.

THE COURT: Sustained.

BY MR. SEGAL:

Q. Do you know what Tribune Company paid?

A. I didn't see the itemized list of appropriation, no.

Q. Okay. In your job in IT, when you recommended the purchase, how much of an expenditure in your view was merited?

MR. LEIDERMAN: I'm going to object, that calls for speculation.

THE COURT: Sustained.

MR. SEGAL: That's all, Your Honor. Thank you.

THE COURT: All right. Mr. Leiderman?

MR. LEIDERMAN: Thank you, Your Honor.

## CROSS-EXAMINATION

BY MR. LEIDERMAN:

Q. Can someone from inside the L.A. Times or can someone from inside the Tribune Company content management system change the plates from a -- change the plates?

A. From the CMS system?

Q. From the CMS.

A. Not --

MR. SEGAL: Vague as to time, Your Honor.

THE COURT: Hold on one second. Clarify the time frame.

MR. LEIDERMAN: Well, how about ever from the CMS.

THE COURT: All right.

BY MR. LEIDERMAN:

Q. Could someone ever from that CMS change -- you referred to them as plates -- the plates from which the L.A. Times print edition is published?

A. From the actual system itself or from outside? I don't understand the question.

Q. From the -- from the CMS system.

A. If you're on the CMS system and have access to the plates, you can change it.

Q. Okay. What part of the CMS system had access to the plates?

A. The physical servers. You can actually log into the plates from the physical servers.

Q. Okay. Who had access to that?

A. To the servers or --

Q. To -- these are the L.A. Times physical servers?

A. Yes.

Q. So you'd have to have an L.A. Times user and pass to get into those?

A. Yes, sir.

Q. And those are specific L.A. Times users and passes?

A. Yes.

Q. Couldn't be just a general Trib Co user and pass?

A. I'm not sure if Trib Co had access to those systems.

Q. Do you believe they did have access to those systems in December of 2010?

A. I'm not sure if Trib Co had access to the plates at that time.

Q. Could any user, for example someone sitting at Fox 40, a television affiliate, change the plates from the L.A. Times if they just had regular access to the CMS?

A. The CMS doesn't have direct access. The system -- if you had access to the CMS systems or from Fox 40, you had a user ID and password that can get into the system with the plates, yes, you can.

Q. So anyone in Tribune with access to the CMS can get into the plates? Because that's not what I understood you to say previously. You said they had to have access to the L.A. Times server.

A. Because when you say access to the CMS, there's different types of access. It would be like if I had access to my e-mail system from here, if I could access e-mail. That's different than me having system access to the e-mail, a user ID and password that can actually log into the system. Those are two different things.

Q. Right.

That's special access, correct?

A. Yes.

Q. That's where I was trying to go.

MR. LEIDERMAN: Thank you.

THE COURT: Are you done?

MR. LEIDERMAN: I'm done.

THE COURT: All right. Mr. Segal, any redirect?

REDIRECT EXAMINATION

BY MR. SEGAL:

Q. When you came on -- when you began your assessment, what did you know about the level of access that the hackers had acquired?

A. Initially I didn't assume anything. We started looking at different systems, and that's when we found the access from that garnished credential. So basically if they had garnished a credential on one system, they could have garnished a credential on any other system that that system had access to or that credential had access to.

Q. And that's why you checked those other systems?

A. Yes, sir.

MR. SEGAL: Thank you.

THE COURT: Anything further, Mr. Leiderman?

MR. LEIDERMAN: No, nothing further.

THE COURT: Is this witness excused, Mr. Segal?

MR. SEGAL: Yes, Your Honor.

THE COURT: Mr. Leiderman?

MR. LEIDERMAN: Yes.

THE COURT: All right. You may step down, sir. You're excused.

THE WITNESS: Thank you.

THE COURT: All right. Next witness.

If you want to stretch, you may. Who's your next witness?

MR. HEMESATH: The government calls Samantha Cohen.

THE COURT: All right. Do you believe she'll take the rest of today?

MR. SEGAL: That's our plan.

THE COURT: But you have someone else lined up if we have additional time?

MR. SEGAL: Yes.

THE COURT: All right. Very good. Innocent questions.

MR. LEIDERMAN: Ask the questions slowly, right?

THE CLERK: Ma'am, please come forward. I need to take your photograph. If you can stand here with your back against the wall facing me. Thank you.

Thank you. Step into the witness stand behind you, remain standing, and raise your right hand.

SAM COHEN, GOVERNMENT'S WITNESS, SWORN

THE WITNESS: I do.

THE CLERK: Thank you. You may be seated. Will you please say and spell your first and last name for the record.

THE WITNESS: My name is Sam Cohen, C-O-H-E-N.

THE COURT: You may proceed.

DIRECT EXAMINATION

BY MR. HEMESATH:

Q. Good afternoon.

A. Thank you.

Q. Ms. Cohen, have you ever gone by another name?

A. Yes. My maiden name is Sam Scholbrock.

Q. Scholbrock.

What is your profession?

A. Right now I'm the executive producer of digital and social media at ABC 10. So I'm a journalist who works online.

Q. A journalist that works online.

How long have you been in that position at that station?

A. Since March, so about seven months.

Q. So that's where you currently work. Where have you worked in the past?

A. Before that, I worked at Fox 40 here in Sacramento.

Q. Fox 40, the television station?

A.  Yes.
Q.  When did you start with Fox 40?
A.  Ah, I started working for Fox 40 in August of 2009.
Q.  Do you recall what your title was at that point in August of 2009?
A.  I was a senior producer for their morning show at that time.
Q.  Was that always your title while you were at Fox 40?
A.  No.  In 2010, I became the executive producer of digital content.
Q.  What about before you worked at Fox 40, what did you do?
A.  Before Fox 40, I worked at a TV station in Salt Lake City, Utah.
Q.  What were you doing for them?
A.  I produced newscasts.
Q.  And before that?
A.  Before that, I worked for a TV station in Milwaukee, Wisconsin, producing newscasts.
Q.  Okay.  Before that?
A.  Before that, I was in college.
Q.  In college.
    And where did you go college?
A.  I went to college at Northwestern University in Chicago.
Q.  And what was your major there?
A.  Broadcast journalism.

Q. What year did you graduate?

A. 2004.

Q. Thank you.

So while you were at Fox 40, what was your name?

A. My name changed while I was at Fox 40. When I was originally hired, my name was Sam Scholbrock. And when I got married, my legal name changed to Sam Cohen.

With the Tribune system, they didn't allow you to change your log-in once you were in the system, so many of my company -- the log-in for my computer -- the log-in for all of the company systems remained S. Scholbrock even though legally my name had changed.

Q. So do you remember what your log-in was during that initial period of time at Fox 40?

A. My whole time at Fox 40 my log-in was S. Scholbrock.

Q. S. Scholbrock.

Did that ever change at any point, a variation on S. Scholbrock?

A. At one point in time I had a new log-in created for me that was S. Scholbrock 2.

Q. Now speaking of log-ins -- well, a little foundation.

Do you know someone by the name of Matthew Keys?

A. I do.

Q. Do you see him sitting in this courtroom here today?

A. I do.

Q. Could you describe some article of his clothing that he's wearing that would distinguish him in the courtroom?

A. He's wearing a black suit coat and glasses.

Q. Okay.

MR. HEMESATH: Your Honor, may the record reflect Ms. Cohen is identifying Matthew Keys?

THE COURT: Who's on this witness?

MR. JAFFE: No objection, Your Honor.

THE COURT: All right. The record shall so reflect.

BY MR. HEMESATH:

Q. So you knew Matthew Keys.

Did you happen to know what his log-in was?

A. I wouldn't be able to -- I don't. Sorry. I don't remember.

Q. So when you started in two thousand -- I'm sorry. When did you say you started at Fox 40?

A. 2009.

Q. 2009. You said you were senior producer.

What were the circumstances of your title changing from senior producer to did you say director of social media?

A. Executive producer.

Q. Executive producer of social media.

A. When I was senior producer in the summer of 2010, the executive producer of the morning show left, she got another job. I was considering that position, and in conversations with Brandon Mercer, who was my boss at the time, we talked about an opportunity of me becoming executive producer of the digital side of things where I would be working with Matthew Keys.

We had had one, maybe two conversations about this. At one point in time, Brandon Mercer approached me and asked if I would make that change immediately, so I switched in October of 2010.

Q. October of 2010.

So previous to that moment in time, had you worked with Matthew Keys?

A. I worked with him. I contributed to the website. I worked on the morning show, and I would occasionally write stories and post them to our website.

Q. During that period of time preceding your new title, how would you characterize your working relationship with Matthew Keys?

A. I considered it friendly. We weren't -- socially outside of work, we didn't keep in touch, but at work we were friendly.

Q. Would you describe your contact as daily, weekly, occasionally?

A. Daily. Our shifts overlapped. I came in in the early morning, and Matthew came in in the late morning or afternoons.

Q. Did you have occasion to notice whether or not he was good at computers?

A. I considered him to be good at computers.

Q. So you knew --

MR. JAFFE: Objection, speculation.

THE COURT: Sustained.

MR. JAFFE: Move to strike.

THE COURT: The jury shall disregard that answer. You can ask a more focused question, if you're able.

BY MR. HEMESATH:

Q. What in particular did you observe with regard to Matthew Keys and computers?

A. I knew he knew our CMS platform, the P2P, really well.

MR. JAFFE: Objection, no foundation.

THE COURT: I'd sustain that.

MR. JAFFE: Lack of personal knowledge.

THE COURT: Again, the jury shall disregard. If you want to lay a foundation, you may.

BY MR. HEMESATH:

Q. In your work with Matthew Keys, did you have occasion to observe his familiarity with computers?

A. Yes.

Q. And what did you observe with regard to Matthew Keys and computers in particular with regard to the CMS system?

THE COURT: Well, that's where you need to lay some foundation.

BY MR. HEMESATH:

Q. Did you see Matthew Keys access the CMS system?

A. Yes.

Q. Under what circumstances were those?

A. It was his job.

Q. Were you looking over his shoulder? Were you helping him? Was he helping you?

A. Ah, both. He trained me on the system, and it was his job to be posting content through the system. So that's the program he used every day when he came in.

Q. So in that context, were you able to observe his facility or not with that system?

A. Yes.

Q. So can you think of any examples of his expertise with that system?

MR. JAFFE: Objection.

THE COURT: Just yes or no.

THE WITNESS: Yes.

BY MR. HEMESATH:

Q. Could you now tell us about those examples.

THE COURT: Well, that calls for a narrative.

BY MR. HEMESATH:

Q. Specifically what would Matthew Keys be doing that would have allowed you to observe his expertise?

A. He was the --

MR. JAFFE: Objection.

THE COURT: What's the objection?

MR. JAFFE: Calls for a narrative.

THE COURT: Well, can you focus this a bit?

MR. HEMESATH: I think she's about to narrow it. I've asked her specifically examples of what she's talking about.

THE COURT: How many examples --

MR. JAFFE: Your Honor, that's a narrative. The question assumes expertise that's not in evidence.

MR. HEMESATH: I'm certainly not asking for expertise.

MR. JAFFE: That was the question, Your Honor.

THE COURT: This is a lay witness. This is not an expert.

MR. JAFFE: Examples --

THE COURT: Just pose a new question.

BY MR. HEMESATH:

Q. Have you ever obtained help with CMS from anyone at Fox 40?

A. Yes.

Q. Was one of those people ever Matthew Keys?

A. Yes.

Q. Can you tell me about that instance of getting help from Matthew Keys?

A. He trained me on the CMS system. He also was our station's administrator, so he would assist with passwords and log-in issues. He trained new employees when they started.

THE COURT: All right. Next question.

BY MR. HEMESATH:

Q. Is Matthew Keys working at Fox 40 today?

A. He is not.

Q. All right. Do you know why he's not working at Fox 40?

THE COURT: Just yes or no.

THE WITNESS: Yes.

BY MR. HEMESATH:

Q. What did you observe directly with regard to his not working at Fox 40 any more?

A. I observed the day before --

MR. JAFFE: Objection, calls for a narrative.

THE COURT: Overruled.

THE WITNESS: I observed the day before he stopped showing up to work that he got into a verbal argument with our current news director, Brandon Mercer.

BY MR. HEMESATH:

Q. Did you overhear that conversation?

A. I did. I was sitting in a control room that had glass windows with the newsroom at the time.

Q. Was it a loud conversation?

A. It was.

Q. What happened with regard to your position immediately following that argument?

MR. JAFFE: Objection, assumes facts not in evidence.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. Did anything happen with regard to your position in December of 2010?

A. Not in December.

Q. Oh, you know what -- I'm sorry -- in October of 2010.

A. Yes.

Q. Did your position change?

A. Yes.

Q. Was it before or after this altercation that you witnessed with Matthew Keys?

A. Immediately after.

Q. So what were the circumstance of your change in position immediately after that altercation?

A. Immediately after that altercation, my news director came up to me and told me that my switch to dealing and managing our digital properties was immediate.

Q. Did you consider that a replacement of Matthew Keys?

A. No. In the context that I had talked to Brandon Mercer about the position, it would have been managing Matthew and managing the web team.

Q. Did Matthew Keys ever come back to work after that?

A. He did not.

Q. Do you recall what you did with regard to your position or rather -- let me ask it more directly.

As of that moment, what did you do? What were your job duties?

THE COURT: Which moment?

MR. HEMESATH: The moment that you were appointed with this new title in October of 2010.

THE WITNESS: I would manage the website and the station's social media accounts.

BY MR. HEMESATH:

Q. Is that something that Matthew Keys had done before?

A. Yes.

Q. Were you able immediately to manage -- did the station have Facebook and Twitter accounts?

A. Yes, they did.

Q. Were you able to immediately manage those accounts?

MR. JAFFE: Objection as to relevance.

THE COURT: Overruled.

THE WITNESS: No. There was an issue immediately following the altercation at work and Matthew's departure that stopped us from managing the social media --

MR. JAFFE: That was a yes or no question.

THE COURT: I'll leave the answer, but --

MR. HEMESATH: I'll just restate the question.

Q. Why weren't you able to manage those accounts immediately?

A. We were not able -- we did not have admin access to the station's Facebook or Twitter accounts. When we came into work Friday morning, we couldn't log in, we couldn't manage those accounts.

Q. So were the passwords working?

A. They were not.

MR. HEMESATH: If you could turn in your binder in front of you to Exhibit 112. It's a tab.

I'm sorry. Is that the right binder? I think that's -- you might want to put that binder behind you. It's the binder that says government.

THE WITNESS: Okay.

MR. HEMESATH: And if you wouldn't mind taking a look at page 6 of that and reviewing the document from that page in reverse order.

THE WITNESS: Okay.

BY MR. HEMESATH:

Q. Do you recognize this document?

A. Yes.

Q. What is this document?

A. It's an e-mail thread between myself and somebody with support in Chicago.

Q. And how do you recognize the document?

A. I recognize that that was my signature on my e-mail thread. Ah, the gentleman I was sending the e-mails to, I remember having this conversation with him.

Q. Okay.

MR. HEMESATH: Your Honor, at this time the government moves 112 into evidence.

THE COURT: That's six pages?

MR. HEMESATH: Yes.

MR. JAFFE: To the extent that the government is introducing this for any truth of any of the statements, the defense objects on hearsay grounds.

THE COURT: Response?

MR. HEMESATH: The government does not intend to offer this for truth.

THE COURT: All right.

MR. HEMESATH: Except with regard to Ms. Scholbrock.

MR. JAFFE: Including statements contained by the witness.

MR. HEMESATH: I'll retract that. She can testify as --

THE COURT: Elicit some more testimony before you attempt to offer it. You may elicit more testimony.

MR. HEMESATH: Okay.

Q. So turning to the last page.

A. Okay.

Q. On December 6th, do you recall having trouble with your password on December 6th?

MR. JAFFE: Objection as to relevance.

THE COURT: Overruled.

THE WITNESS: Yes.

BY MR. HEMESATH:

Q. What was your password trouble?

A. I could not log into our CMS system.

Q. Why would that be important to you?

A. That's how I did my job.

Q. You had to have CMS to do your job?

A. I had to be able to log in to the CMS to do my job.

Q. Could you explain why that would be the case.

A. Ah, I managed the website, so in order to post a story on our website, in order to move stories around on the website, I had to be able to log in to our CMS.

Q. So what did you do as a result of that problem with your password?

A. When I had issues with my password, I e-mailed our corporate support.

Q. Okay. And was someone at corporate support that you e-mailed by the name of Ryan Pollyea?

A. Yes.

Q. And did he respond?

A. He did.

Q. What did he tell you?

A. He -- we went through a pattern of resetting my password.

MR. JAFFE: Objection, calls for hearsay.

THE COURT: Sustained.

MR. JAFFE: Move to strike.

THE COURT: Well, there wasn't much of an answer out, so no need.

BY MR. HEMESATH:

Q. Ms. Cohen, as part of your day-to-day business there at Fox 40, did you send e-mail?

A. Yes.

Q. And did you receive e-mail?

A. Yes.

Q. And did you use e-mail to get your job done?

A. Yes.

Q. And to your knowledge, were these e-mails automatically stored in Outlook in the course of your communication?

A. Yes.

Q. And did that happen at the time that it occurred?

A. Yes.

MR. HEMESATH: Your Honor, at this time the government moves this into evidence, and specifically under the business record exception to the hearsay rule.

MR. JAFFE: The objection remains. This is inadmissible hearsay. It does not fit into that exception, Your Honor.

THE COURT: Any reason to distrust the representation that these are copies of e-mails?

MR. JAFFE: They're not regularly within the course of business as required for that exception.

THE COURT: Well, the objection is overruled up to -- as to the December 2010 e-mails?

MR. HEMESATH: Correct, Your Honor.

THE COURT: So essentially pages 2 through 6, the bottom of page 1, if you redact before any publication.

MR. HEMESATH: I could take a moment to redact that, Your Honor, if --

THE COURT: Or you can work with whatever else -- the other pages for now.

MR. HEMESATH: Well, let me ask the defense, would they prefer redaction or an admonition to the jury to not consider that top part?

MR. JAFFE: The top part of page 1?

MR. HEMESATH: Yes.

MR. JAFFE: The direction, the direction is acceptable to redact.

THE COURT: All right. Then 112 is admitted, the bottom of page 1 through page 6. To the extent the government displays the first page with some e-mails at the top, I would just instruct the government not to enlarge those --

MR. HEMESATH: Yes.

THE COURT: -- at this point.

And the jury shall disregard them if it can read them.

(GOVERNMENT'S EXHIBIT 112, e-mail series, ADMITTED INTO EVIDENCE.)

MR. HEMESATH: May I have Exhibit 112, page 6.

Q. So this is the e-mail that you sent to someone at IT indicating your password wasn't working?

A. Correct.

Q. Did this strike you as unusual at that time?

A. It did.

Q. Why was it unusual?

A. I didn't understand why my password wasn't working, especially since it had recently worked for me after resetting it earlier.

Q. Okay. Let's look at the whole page again.

And you said that Ryan Pollyea was someone you communicated with?

A. Yes.

Q. And did he assign you a new password?

A. Yes, he did.

Q. And he tested it?

A. Yes, he did.

MR. HEMESATH: Okay. Could we have page 5. It runs over to the next page.

Oh, I'm sorry. Let's go back to page 6.

Q. So do you recall sending this e-mail?

A. Yes.

Q. And what were you attempting to communicate with that e-mail?

A. I was frustrated that initially the new password he sent me appeared to work. Unfortunately it suddenly stopped working when I was in the middle of trying to do something, so I was frustrated. Ah, I reached out to Ryan to see if he would help.

Q. What did you mean when you said that you lied?

A. I initially sent him an e-mail saying thanks, and then I logged in with the initial -- the password he had sent me initially. It appeared to work, and I had sent him an e-mail that said thanks, I'm sure something to the effect of thank you for your help, it's working. But I lied about it working, and I sent him another e-mail.

Q. I see. Okay. Now let's look at page 5.

So did Ryan respond to you?

A. He did.

Q. What did he say?

A. He reset the password. At this point I think he and I both realized that I was having this issue, and it was not a widespread issue within the Tribune system at that time.

Q. I see.

And when he says Assembler or P2P, what does that -- what did that mean to you?

A. Assembler and P2P were our CMS systems. Assembler was an older version of it we still had access to. P2P is the platform we were using.

Q. I see. Okay. So let's clear that.

And then you responded to Ryan with -- let's go right there. And here what are you attempting to communicate to Ryan?

A. He wanted to double-check how I was resetting my password. His question about are you resetting it in Assembler or P2P, I was clarifying that I reset it in P2P. And I told him I went to the tab user management, I searched for my name, and then there is a button you would push to reset the password.

Umm, I -- at this point in the day, I remember feeling frustrated that I couldn't get my job done.

MR. JAFFE: Strike as nonresponsive.

THE COURT: Sustained. The jury shall disregard the answer from the start of the last sentence forward.

Next question.

BY MR. HEMESATH:

Q. At this point in the day, could you get your job done?

A. I could not.

Q. And how did that make you feel?

A. Frustrated.

Q. So could we look at the next chunk above here.

So was Ryan Pollyea able to help you out in his next response?

A. Basically his next response was just assuring me that he was having somebody take a look at it. I don't know if I would necessarily say it was helpful. It was just letting me know they were having someone look at it.

Q. Okay. Let's go to page 4.

So then what happened?

A. The password that he had sent me a day or two before stopped working.

Q. This is the new one that he sent you in the previous e-mail indicated by TXOW 8439?

A. Correct.

Q. And so when that happened to you, what were you doing? Does that e-mail indicate?

A. I was logged into P2P, our CMS system at the time. TIVID used the same credentials, it was related to our CMS, and I was logged in at the time.

Q. What is TIVID?

A. TIVID is a -- it was where we managed our videos within the -- it was a program that helped us manage the videos that went on our website.

Q. Okay. So now you appear to say, to get work done today, I'm going to re-log-in under Scholbrock 2. Can you tell me what you mean Scholbrock 2, S. Scholbrock 2?

A. When I was having issues with my password, when we noticed that the initial user password that he had sent me with ABCD, when that wasn't working, he had assigned me to a different log-in. He thought maybe there might be something wrong with my first log-in, so he set up a second one, S. Scholbrock 2.

Q. Do you recall whether you were changing your own passwords from some external IP address at this time?

A. I would have been changing them at work.

Q. At work only?

A. Uh-huh.

MR. HEMESATH: Could we go to the next page. There's just a little bit more to this e-mail. I'm sorry. Page 5. Okay. And then there was a little more.

Q. You reported some other incident having to do with P2P; is that correct?

A. Yes.

Q. All right. Page 4, please.

So what did Ryan do in response to that?

A. He just reassured me that they were looking into it. Ah, he was also with corporate IT, and I had reached out on a separate issue of headlines disappearing to the main corporate help e-mail. Marquez was the one who responded back, and so I was making sure that Ryan knew Marquez was also looking into issues.

And then he was just reassuring me to use the alternate S. Scholbrock 2 account, and he would follow up with me if he found anything.

Q. Okay. Let's take a look at the next chunk above.

So you had more e-mail correspondence with Ryan Pollyea. What was the next bit of correspondence about?

A. I was having more issues. The secondary account, S. Scholbrock 2 was now coming up as authentication failed with invalid user-password combination. I couldn't log in with my secondary account. I still couldn't log in with my primary account.

Q. And let's take a look at the previous page or 003.

That happened on December 8th at about -- do you recall it being about 11:40 a.m. in the morning?

A. Yeah.

Q. It was a long time ago.

A. I was going to say I'm sure it was in the morning.

Q. Once again, were you able to get your work done while this was going on?

A. No.

Q. What was Ryan Pollyea's response to you now?

MR. JAFFE: Your Honor, move to strike the portions from Ryan Pollyea to the extent that the government relies on this hearsay exception. There's been no foundation for it.

THE COURT: I'd sustain that. I think as to this witness, it's present sense impression.

MR. HEMESATH: So are you objecting to what's on the screen right now?

MR. JAFFE: That's correct.

MR. HEMESATH: Okay.

Q. So do you recall getting a new password for Scholbrock 2?

A. Yes.

Q. And did that work for a while?

A. For a while.

Q. And what did you think that your problem might be?

A. I honestly didn't know what the problem was.

Q. Did you think it might be your fault?

A. Initially I thought it was my fault, but I didn't -- I just didn't have an understanding of what was happening. I didn't know.

Q. Take a look at page 2.

So with regard to an e-mail that you sent on December 14th, what happened there?

A. My passwords for S. Scholbrock and S. Scholbrock 2 were not working again.

Q. Were you able to do your work?

A. No.

Q. Okay. Let's do this here.

Did you send any more to Ryan Pollyea?

A. Yes.

Q. What was that?

A. I wanted to let him know that at the same time this was happening, there were other things going on in our station, and they were e-mails being sent to some viewers of our station that seemed to be, umm, threatening or harassing at the same time that I had these password problems.

Some of my co-workers knew that I was having these password problems.

MR. JAFFE: Objection, move to strike.

THE COURT: Overruled.

MR. HEMESATH: Go ahead.

THE WITNESS: They knew I was having these passwords problems because I couldn't get my work done, and they -- as I say in the e-mail there, they're a little bit more conspiracy theory-ish, and they started to combine the harassing e-mails issue with my log-in issues.

MR. JAFFE: Move to strike.

THE COURT: Overruled.

Are we trying to get this witness done today? I don't know if it's possible at this point. I'm just --

MR. HEMESATH: It depends on cross. I think I need another seven minutes.

THE COURT: All right.

MR. HEMESATH: Actually I should say 14, I guess.

THE COURT: Why don't you aim for 5:00 in case there is a chance -- well, if there is a chance of concluding reasonably --

MR. HEMESATH: Yes.

THE COURT: -- with this witness today.

MR. HEMESATH: Okay.

Q. What did super user access mean to you?

A. If you were a super user, you had the ability to manipulate or touch more content on the CMS system Tribune wide, ah, touch the content or some of the users, see different users. It was a higher level being able to -- to be able to touch some of the content in the CMS.

Q. Do you --

MR. HEMESATH: I'm going to consult with defense counsel.

(Counsel conferring.)

MR. HEMESATH: Could you look at Exhibit 505.

THE WITNESS: Okay.

BY MR. HEMESATH:

Q. Do you recognize those lines?

A. I do.

Q. How do you recognize them?

A. When you logged into our CMS, that's how you would access different levels, different places within the CMS.

MR. HEMESATH: Okay. So at this time, I would just like to mark that for identification and note her response.

THE COURT: It's identified as 505.

MR. HEMESATH: 505, yes.

THE COURT: All right. I think the record makes that clear.

MR. HEMESATH: Uh-huh. So let's get into the e-mails that you were just talking about with regard to the other things that you were mentioning that was going on in the newsroom.

Q. What was going on in the newsroom at about that time?

A. In December 2010, we as a station, Fox 40, were running a contest through our Facebook page. People signed up to our -- signed up to our system, and they could be entered to win an iPad.

After some time of running the contest, in early December some people who had signed up for the contest started getting e-mails. Ah --

MR. JAFFE: Objection, this evidence is irrelevant, Your Honor.

THE COURT: Sustained.

MR. HEMESATH: Your Honor, is this the Cancer Man objection?

MR. JAFFE: Yes.

THE COURT: It's also -- let's ask some focused questions to structure this.

BY MR. HEMESATH:

Q. What were those e-mails about, do you recall, the e-mails to viewers?

A. The e-mails --

MR. JAFFE: Objection, there's been no foundation laid for this line of testimony.

THE COURT: It's a yes or no initially.

THE WITNESS: Can you ask the question again?

MR. HEMESATH: Yes.

Q. Do you recall that there were a series of e-mails that were from a moniker Cancer Man?

A. Yes.

MR. JAFFE: Objection, no foundation laid for the personal knowledge of the witness.

THE COURT: Overruled.

BY MR. HEMESATH:

Q. Do you recall those e-mails?

A. Yes.

Q. Do you recall similar e-mails around the same time that were purportedly sent to viewers from a moniker Fox Mulder?

A. Yes.

Q. Same question, Walter Skinner?

A. Yes.

Q. Okay. So what was your reaction to those e-mails being sent to viewers?

MR. JAFFE: Objection, no personal knowledge.

THE COURT: You can lay a further foundation.

BY MR. HEMESATH:

Q. What did you know about those e-mails?

A. I was contacted by people who had gotten the e-mails. They forwarded them to me.

Q. And so what was your reaction to the fact that people were forwarding e-mails --

MR. JAFFE: Objection, not relevant.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. What was the content of those e-mails that were being sent to viewers?

MR. JAFFE: Objection.

THE COURT: Overruled. You may describe generally if you're able.

THE WITNESS: The e-mails harassed the person about the contest being fake and about the reputation of Fox 40.

BY MR. HEMESATH:

Q. Did you know who was sending those e-mails at that time?

A. I did not.

Q. Did the fact -- okay.

You've stated previously you have knowledge of CMS and how to access content on the CMS?

A. Yes.

Q. Are you aware of whether or not e-mail lists are available for downloading on the CMS?

A. I am not aware how to download an e-mail list from the CMS. I never had a reason to.

Q. So the question is not whether or not you know how to, but do you know whether e-mail lists are available on the CMS?

MR. JAFFE: Asked and answered.

THE COURT: Sustained.

BY MR. HEMESATH:

Q. To your knowledge, has anyone else based on your personal knowledge downloaded e-mail lists from the CMS?

MR. JAFFE: Objection as to relevance.

THE COURT: Answer yes or no.

THE WITNESS: No.

BY MR. HEMESATH:

Q. Are you -- with regard to what you testified earlier to with regard to the contest, are you aware of an e-mail list having been generated as a result of that contest consisting of customer e-mails?

A. We could access their e-mails.

MR. JAFFE: Nonresponsive.

MR. HEMESATH: So let's start --

THE COURT: That answer is stricken.

BY MR. HEMESATH:

Q. Let's start with are you aware of that contest?

A. Yes.

Q. Were you able to access that e-mail list?

A. Yes.

Q. How were you able to access that e-mail list?

A. When I logged into the CMS, I could click on a tab for UGC, user generated content, and search for a name of someone who had registered or entered for the contest.

Q. Okay.

MR. HEMESATH: Just one moment, Your Honor.

(Government counsel conferring.)

BY MR. HEMESATH:

Q. Do you recall, with regard to your testimony that you just gave, whether e-mail addresses that would have been generated as a result of the contest, whether they would have existed on the CMS?

MR. JAFFE: Asked and answered.

THE COURT: Overruled. Just answer yes or no.

THE WITNESS: Yes.

BY MR. HEMESATH:

Q. Ms. Cohen, do you recall how much money -- how much your salary was during that period of time?

A. In December of 2010, I made $50,000.

Q. Do you recall how much of your work time it would have consumed to -- in reaction to not having your password to the CMS?

MR. JAFFE: Objection as to relevance.

THE COURT: Overruled.

THE WITNESS: I would say about five working days.

BY MR. HEMESATH:

Q. So could you elaborate on that a little bit why you wouldn't have been able to do your job for five working days?

A. So my job is to post content and rearrange the content on our station's website. And if I can't log into the system, I can't do that.

I also worked with the video that our station produced, and if I couldn't log into the CMS, I couldn't touch that video. I couldn't -- I couldn't do my job.

Q. So what did you do instead?

A. I assisted some of the other writers in our newsroom. I worked with corporate on trying to reset my password. Ah, I also dealt with people who entered our contest and were contacting us about these e-mails they were receiving. So I would e-mail them back or try to work with them and did customer service. That's how I saw the e-mails.

Q. So how much working time would you say you were not able to perform that was part of your job or that was your job as a result of not being able to access CMS in hours?

A. Ah, sorry. A lot. There was -- I mean, it was a week of resetting my password, and all I could do is just sit at my desk and twiddle my thumbs.

MR. JAFFE: Nonresponsive.

THE COURT: Overruled.

THE WITNESS: About 40 hours.

MR. HEMESATH: About 40 hours? Okay.

Q. And that was your salary. You were assigned a 40-hour workweek?

A. Yes.

Q. Okay.

MR. HEMESATH: Could we -- and this will be the last for -- Exhibit 505.

THE WITNESS: Okay.

MR. HEMESATH: Could we have Exhibit 505?

MR. SEGAL: It's not in evidence.

THE COURT: It's not been admitted.

MR. HEMESATH: I'm sorry. We discussed this earlier.

Q. You said you recognized these lines; is that correct?

A. Yes.

Q. Okay. And how do you recognize them?

A. Within the CMS, these are places that you could click on to -- it was different abilities that you had, so things that you were able to do. You could edit things, delete things. So these were credentials assigned to somebody.

Q. Did you use these URLs a lot?

A. I wouldn't necessarily use the URLs, but I knew they were there. I saw them a lot.

MR. HEMESATH: Your Honor, at this time the government moves Exhibit 505 into evidence.

THE COURT: Any objection?

MR. JAFFE: Objection as to relevance and hearsay.

THE COURT: Well, I'm going to defer a decision allowing further testimony to be elicited. But we have come to 1:30, and so we will continue with this witness tomorrow morning. So we'll adjourn for the day. Thank you so much for your service. I know it's a long day even though we're done at this time.

So tomorrow our schedule will be the same, 8:30 to 1:30. Please remember all of my admonitions. Don't research the case in any way. Don't look up definitions in any kind of dictionary online or otherwise. Don't talk with anyone about the case. Don't think about its ultimate conclusion. Your consideration comes only once you have deliberated, discussed the case with your fellow jurors. And if anyone attempts to contact you, please let me know in the morning.

Have a good afternoon. We'll see you tomorrow morning. Thank you.

(Jury not present.)

THE COURT: You may step down. If you can be back in your seat at 8:30. All right? Thank you.

All right. Who are your witnesses for tomorrow once you're done with Ms. Cohen?

MR. HEMESATH: It will be very briefly --

MR. LEIDERMAN: No one believes you at this point.

MR. HEMESATH: I know my credibility is shot, but I will make my best efforts to make it short. And then I believe we have --

MR. SEGAL: We've got to do some thinking. We may cut some witnesses out depending on some of the things that happened today. For this, I don't mind sending an e-mail to the Court and to counsel both saying who our witnesses are tomorrow, but we need to kind of circle around and see if we can strip it down a little bit.

We're certainly calling Jason Jedlinski. We may be calling Russ Schmidt, but all he did was image the seized Macintosh computer. That could be avoided by stipulation. That will be brief or stipulated. And then we have to do some thinking about whether we want to call Jerry Del Core and two people who received e-mails whose names I can't remember right now. And then the last witness will be John Cauthen.

THE COURT: How long will Agent Cauthen take on direct?

MR. SEGAL: A long time, hours.

THE COURT: Well, how many?

MR. SILVER: If it turns out -- the government still intends to seek to use snippets of the recorded conversation.

(Government counsel conferring.)

MR. SEGAL: We'll figure it out. So part of the answer to that in part turns on the Court's determination of this motion in limine regarding the completeness doctrine.

THE COURT: That was my next question. Can you provide me at this point the revised power point and the complete set of excerpts?

MR. SILVER: Mr. Ekeland and I are going to meet right now to discuss the latest version of the power point, and so we should be able to provide that to the Court hopefully today.

MR. EKELAND: Later today.

THE COURT: All right. You can e-mail that to Ms. Schultz.

And on the complete set of excerpts?

MR. HEMESATH: Your Honor, I think we've provided that. And based on what has happened in the testimony, I believe we seek to add one more excerpt.

THE COURT: So when can I get that?

MR. HEMESATH: And so I think we can get it in the next hour or so.

THE COURT: All right. So also e-mail that to Ms. Schultz and make certain the defense has it.

Those will all be used only with Agent Cauthen?

MR. SILVER: That's correct, Your Honor.

THE COURT: So Agent Cauthen may start tomorrow?

MR. SILVER: Not impossible.

THE COURT: All right. And then you do have the original of the handwritten statement. I've never seen a good copy of that.

MR. SILVER: Yes.

THE COURT: It's in the binders? Okay.

MR. HEMESATH: Yes.

THE COURT: Ms. Schultz can just show it to me tomorrow morning before we come in. I just want a chance to eyeball it before -- you've had a chance to inspect the original?

MR. EKELAND: I believe we've got them.

MR. HEMESATH: We produced a copy of the original. You can take a look at --

MR. LEIDERMAN: I was able to see a copy. We were able to read it.

MR. SEGAL: They have a legible copy, but the original is -- is it in the courtroom or is it --

THE COURT: All right. I just --

MR. LEIDERMAN: Your Honor, does the Court have the complete copy of the transcript of Mr. Keys' testimony, the 86 pages that compliments the excerpts?

THE COURT: I thought I had the complete --

MR. LEIDERMAN: I thought so, too.

THE COURT: -- the complete set, but with the excerpts identified within it.

So that -- but I haven't reviewed it because I'm waiting to know the final set of excerpts the government plans to --

MR. HEMESATH: In addition, Your Honor, I believe that we've also produced to the defense and to the Court a copy of just the excerpts, but we want to add one more to that.

MR. EKELAND: Yeah, we received -- we haven't gotten the one with the addition you're talking about, but we did receive the excerpts. And then there's a complete --

THE COURT: I only want -- at this point, I need the complete transcript with the excerpts clearly identified.

MR. SEGAL: Got it. Okay.

MR. EKELAND: There was a complete copy of the transcript in the defense exhibit binder, too, Your Honor.

MR. SEGAL: No, but I understand what you need. You need --

MR. LEIDERMAN: I understand what the Court needs.

MR. SEGAL: -- from us a document that has everything with each snippet identified by government exhibit number what that snippet is so that we can argue that that's complete and not misrepresenting.

THE COURT: Right. So it sounds to me like we can argue that on a break tomorrow before Agent Cauthen testifies. I don't know when you want to use that with him, but we have to argue it before you can use it, just so that's clear.

In terms of the government's estimate currently, we'll still wrap up by Monday at some point?

MR. SEGAL: The way things are going, I think it's possible, yeah.

THE COURT: And then does the defense know at this point -- you aren't required to answer me. Do you know if you're going to put on evidence?

MR. LEIDERMAN: Well, if the people are just -- oh, in our case? No, we're not. I thought -- I went to the cross-examination.

THE COURT: No. At this point, no case in defense planned?

MR. LEIDERMAN: No, no case in chief. No.

THE COURT: All right.

MR. SEGAL: Something to think about now that will probably come up in the Cauthen testimony is -- sorry.

The defense has made exhibits out of these plea agreements and -- the plea agreement and an indictment of this person whose Internet nickname comes up a little bit. And we made a motion on this, and it's been represented that that stuff is not going to be offered without first flagging it for the Court because we have a lot of objections as reflected in our motion in limine.

THE COURT: Is there a current plan to offer those exhibits?

MR. EKELAND: Only if the government opens the door on it.

THE COURT: Do you believe the government has opened the door at this point?

MR. LEIDERMAN: They don't sound like they're about to.

THE COURT: All right. I don't think it's an issue at this point in time. All right.

MR. EKELAND: We'll flag it for the Court, Your Honor, if we do.

THE COURT: All right. So we'll look for some e-mails today of the final power point and the excerpts in context, and then we'll see you at 8:30.

At some point tomorrow, I'll provide you with a working set of proposed instructions and a verdict form, and then we'll start working in earnest on those Monday during breaks and perhaps after we take a short break at 1:30 on Monday. So they'll be ready hopefully by Tuesday on the assumption that there's a pretty good chance this goes to the jury on Tuesday.

All right?

MR. SEGAL: There's a good chance of that, yeah.

THE COURT: All right. Anything else?

MR. EKELAND: No, Your Honor, nothing for the defense.

THE COURT: All right. See you tomorrow morning.

MR. EKELAND: Thank you, Your Honor.

MR. JAFFE: Thank you, Your Honor.

THE CLERK: Court is in recess.

(Proceedings were adjourned at 1:37 p.m.)

---o0o---

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/ Kathy L. Swinhart
KATHY L. SWINHART, CSR #10150