THE WITNESS: Yes, sir.

THE COURT: You may proceed.

CROSS-EXAMINATION

BY MR. BERTOLLINI:

Q Good afternoon, Dr. Ullrich. My name is Simone Bertollini, I represent Fabio Gasperini. I want to ask you some questions and I'm going to conduct what is called cross-examination.

During the cross-examination I may ask you often questions that are called leading questions and you are expected to those leading questions to give only a short answer which will be yes, no or you're not sure.

Do you understand?

A Yes, sir.

Q Thank you. Dr. Ullrich, on what listening port do you keep your honeypots?

A My honeypots listen on a number of different ports. It almost changes daily, what ports they're listening on. It's a large number of ports.

Q What is the port that is most commonly attacked on your honeypots?

A These days, port 22, port 23.

Q The least?

A The least or the most?

Q The most.

A The most, 22 and 23.
Q The most?
A Yes.
Q What about port 80?
A Port 80 is attacked very much, too. Port 80, port 8080, all these ports associated with web servers. Over the last few months however, ports 22 and 23 have eclipsed these ports.
Q When you say in the last few months, what kind of time frame?
A Starting approximately November last year with a new botnet that was released back then that particularly scanned port 22, 23.
Q How many variances of Shellshock are you aware of?
A I don't have a clear number of that, but the attack was used very excessively. So, there are many, many different variances of this attack.
Q Isn't it true that the Shellshock attack targets any Linux-based device?
A Any Linux-based bot that exposes Bash. So, it does require, for example, a web application that exposes Bash.
Q When was the first Shellshock discovered?
A September 2014.
Q I'm talking about Shellshock not with respect to the QNAP devices.
Shellshock in general?

A I believe the vulnerability was announced in September 2014.
Q Isn't it true that you wrote a blog on your, posted on your website called: Shellshock a Collection of Exploits Seen in the Wild?
A Correct.
Q And that is dated September 29, 2014?
A Correct.
Q When you wrote this blog, how many types of Shellshocks had you seen by then?
A I don't recall the blog, but there were probably dozens. I don't think I listed them all in the blog.
Q The title of the blog is called -- would you like to see the blog, too?
A Sure.
THE COURT: Okay?
THE WITNESS: I do see the blog.
Q And it was authored by you; correct?
A Correct, yes.
Q By collection of exploits, did you mean any number it might be?
A Sorry, I didn't quite understand. So, any number of exploits?
Q What did you mean by collection?
A By collection, I meant that these were exploits that we

observed in our honeypots and that users, like we had in this case, reported to us.

Q Okay. So, with the word collection, what did you mean? Like, large number? Small number?

A In the blog it was a relatively small number, I believe.

Q Okay. And you say that you use Pastebin; correct?

A Sorry, did I use what?

Q Pastebin.

A Pastebin, yes, I do use Pastebin often.

Q And you have testified that Pastebin is used by security experts to share notes about vulnerabilities; correct?

A What I really said was that it's also used by attackers to share notes about exploits.

Q Isn't it true that you can use Pastebin to paste any kind of note?

A Correct.

Q How about college notes?

A Anything. Any text that you would like to paste, you can use for it.

Q So, Pastebin is not a tool that is used by someone that is investigating cyber crimes; correct?

A Correct. Pastebin is used by criminals and normal users.

Q You testified that you learned about the QNAP Shellshock vulnerability in December of 2014; correct?

A September. September. 9/2014.

Q About the QNAP?
A About the Shellshock vulnerability and QNAP shortly after. End of September?
Q Isn't it true that you wrote a blog on December 14th, 2014 called: Worm Back-Doors and Secures QNAP Network Storage Devices?
A Correct.
Q Are you familiar with that?
A Yes, I am.
Q What is a worm?
A A worm is self-propagating code. It's code that infects one system and then, once it infects the system, it reaches out and infects other systems.
Q Is that different from a virus?
A A virus, typically, is malicious code. It just infects one system and stops at this point. However, the two terms are often used exchangeable.
Q When you wrote this blog about the QNAP Shellshock vulnerability, did you think it was a serious threat?
A I'm sorry?
Q Did you think it was a serious threat?
A Yes, I thought it was a serious threat. That's why we posted about it.
Q Do you categorize on your blog Internet threats by level of dangerousness?

A Sometimes we do, but usually we don't. We do have something called INFOCON level, which we erase whenever there's a new threat available. We did initially erase our INFOCON when Shellshock was first released in September, but lowered it later after it became steady-state.
Q Okay. What is a threat level green?
A Green, as we usually define it, means the Internet is function as usual. So, there's a usual amount of activity and exploits. There's nothing unusual that provides special care.
Q Isn't it true that your blog about the QNAP vulnerability was tagged as a threat level green?
A Correct.
Q What would be the other threat levels in your blog?
A The highest we ever used was yellow, which is the second one up from green. We usually use that if there is a significant new vulnerability. At the point the QNAP worm was released, Shellshock was already known for a few months.
Q You say that during the direct examination that after you learned about the QNAP vulnerability in December -- I'm sorry.
MR. BERTOLLINI: Withdrawn.
Q You testified that around March of 2015 you got in contact with the FBI about it QNAP vulnerability; correct?
A Correct.
Q And you testified that you reviewed logs on your honeypots to check whether there were requests to your

honeypots regarding this vulnerability; correct?
A Correct.
Q What is the date of the log start that you produced?
A These were the logs that I displayed earlier and I believe the log was March 31st, but I can double-check this in the Exhibit.
Q So, is it fair to say that it was the end the March?
A Yes.
Q Okay. So, between the time that you wrote the article, December 14th, and end of March, what exactly did you do about investigating this worm?
A We pretty much set it aside because we saw it continued, but there was no significant change during that time.
Q So, during that time, three-month time frame, you didn't do anything because you didn't think it was a real threat; correct?
A It was a threat, but nothing we could do much about.
Q But you started investigating the end of March; correct?
A At the end of March I retrieved these logs based on the phone call, yes.
Q You testified that you retrieved the EMME script from the 23 server; correct?
A Correct.
Q When did you do that?
A I did that when I wrote the blog post. That would have

been in December.
Q Okay. So, you testified that when you wrote the blog, you downloaded EMME from 23; correct?
A Correct.
Q But isn't it true that you got the files of the actual worm on Pastebin?
A This was just the initial script, the test.sh script, yes.
Q So, you downloaded test.sh from Pastebin; correct?
A Correct.
Q Not from its source; correct?
A Correct.
Q Now, let's go back to the logs of your honeypots that started at the end of March.

Now, at the end of March, you have requests; correct?
A Correct.
Q And these requests mean to install the malware and try to infect the other device; correct?
A Yes.
Q Do you believe that at the end of March QNAP devices were infected by these worms?
A I believe so, yes.

(Continued on following page.)

BY MR. BERTOLLINI:
Q And you say that the host of this malware was the one in the 185 sever, correct?
A Sorry?
Q You say that the host of this malware was the server starting with 185, correct?
A Yes, whatever server was in the log.
Q Are you aware that the 185 server died on January 21, 2015?
A No, I'm not aware of this.
Q What happens if a QNAP device tries to download s0 from the 185 server on March 31?
A On March 31, the exploit would no longer work.
Q Isn't it the same as saying at end of March the infection was no longer active?
A Well, it was still spreading, it just couldn't download. So, there were still infected systems out there.
Q There were infected systems that would try to infect other systems commanding those systems to download s0 from 185?
A At which point it would no longer work.
Q Which no longer work.
A Right.
Q Now, you talk about -- you say you created DVD of the malware before coming here to court, correct?

A Yes.
Q When did you give the DVD?
A On June 15.
Q 2017?
A 2017, yes.
Q You didn't create the DVD before?
A No, I did not.
Q And you said this is the first time that you testify in federal court concerning the script, correct?
A Correct.
Q So, you just testified that the Shellshock vulnerability for the unit was disclosed at the end of December 2014, correct?
A Correct.
Q So, in almost three years you did not testify in court about this specific malware?
A Correct. This is actually the first time I do testify in federal court.
Q Okay, so, first time you testify in federal court.

How many threats are going on in internet? How many kinds?

A That's a very difficult question to answer. I would say thousands, millions, depending what you consider a threat.
Q And about these thousands of threats or thousands upon thousands of threats you were never asked to testify in court,

correct?
A Correct.
Q Did you receive a subpoena to come here today to testify?
A No, I did not.
Q How much were you paid by the Government?
A I believe I'll be paid $70 for today, but I'm not sure.
Q You testified that each device has a unique IP address, correct?
A Correct.
Q What if your internet provider gives you dynamic address?
A If you use dynamic IP address, then this IP address keep changing. But at any point in time, you do have a specific IP address that is used to send traffic to your device.
Q Okay. So the IP address of a specific device changes all the time, correct?
A It may. It depends on the ISP.
Q If the ISP doesn't provide you with a stagnant IP, it can change, correct?
A Correct.
Q When the device reboots, you might get a different IP address, correct?
A Again, depends on the ISP. With many ISPs, a reboot will not trigger a new IP address; you actually have to connect a different device. Some ISPs change IP addresses daily. It varies from ISP to ISP.

Q What would happen if you executed the Shellshock virus on a Windows-based operating system?
A Typically, nothing will happen.
Q You testified when the script hits on outlogging.cgi, it attempts to execute, correct?
A Correct.
Q And on the log, you found 404 answers, let's call them answers.
A Correct.
Q 404 means--
A Answers, correct.
Q If you connect a QNAP device, it will give you 202, correct?
A Correct.
Q If you connect a patch QNAP, would it give you the 202 or the 404?
A It will give you a 200, actually.
Q 200?
A Yeah.
Q We had someone from QNAP, Inc., testifying this morning in court. And this person said that -- withdrawn.
You have a QNAP device, correct?
A Correct.
Q And you examine your own QNAP device, correct?
A Correct.

Q When you bought your device, were the SSH ports open or closed?
A On my particular device, they were closed.
Q All of them?
A Port 22 was not open and SSH was not enabled on this device.
Q The representative from QNAP testified this morning that all QNAP devices have 22 open.
MS. KOMATIREDDY: Objection, your Honor.
THE COURT: Sustained.
MR. BERTOLLINI: I respectfully request a sidebar, your Honor. This is cross-examination and I'm trying to ask the witness --
THE COURT: You want to have a discussion about it? Sustained. Move on.
Q In your particular QNAP, SSH 22 was closed?
A Right.
Q You testified that the script opened, created SSH 26, correct?
A Correct.
Q And you defined SSH 26 as a back door, correct?
A Correct.
Q So if a device, assuming that the device has an SSH open, is that a back door?
A No. SSH by itself is not a back door, but the running

SSH on Port 26 and then adding an account that allows the attacker to log in, that provides the back door.

Q But you say on your direct that SSH 26 itself is a back door, correct?

A Could be considered a back door as well because it's not the standard way of running SSH. So, that debates, for example, running SSH 22 in addition to 26.

Q I understand. But you say on direct SSH 26 is a back door. You say that, correct?

A Correct.

Q Now you're saying that SSH plus the extra files might be a back door, correct?

A Correct.

Q When you analyzed, this script you made notes, correct?

A I did.

Q What is cg.cgi?

A cg.cgi, I don't recall. I would have to look it up.

Q Would looking at a copy of your analysis refresh your memory?

A Yes, please.

Q Can you see the file?

THE COURT: You want to point where to on that document?

Q This is the first page of the analysis. Do you recognize it?

A I recognize it, yes. It's an annotated version.
Q The second page of the analysis, do you recognize it?
A Yes, I do.
Q Now, on Page 3 of the analysis --
A I do, yes.
Q Right --
A I see at the bottom gH.cgi.
Q Did you examine cg.cgi?
A Yes, and I believe -- I may be wrong here, but I believe there was an empty file. It had some HTML scripts in there. It was not really relevant.
Q But you say in your analysis right here --
A This is -- these are notes that I took when I write this particular script before actually looking at the CGI file.
Q So, you say gH.cgi is a CGI back door.
A These are notes that I took when I analyzed it before I actually verified what the file is.
Q How do you go through the gH.cgi as a back door?
A I didn't. I just took notes that I want to go back to this file to see what it is.
Q Okay.
A So, these notes are not accurate.
Q These notes are not accurate. Okay.
So, you testified that armgH.cgi is an IRC bot, correct?

A I said the CGI or the other one. Let me double-check which one it was.

Yeah, I believe it was the armgH.cgi.

Q ArmgH.cgi, you say, you believe is an IRC bot, correct?

A Yes.

Q And you say in your direct that you were talking to a server called IRC.org correct?

A Correct.

Q And this also will be on server 1927915327, correct?

A Correct.

Q And you say you examined this script in full, correct?

A Correct. Now, I want to clarify, it may have been the .cgi, not the armgH.cgi.

Q Say it again.

A It may be the file .cgi that you're talking about, not the file armgH.cgi, because I don't have a printout here of armgH.cgi with me. I only have a printout of .cgi. That's the file shown.

Q I'm actually in your notes right here. It include, it says, armgH is an IRC bot.

A ArmgH without .cgi. Again, these are notes that I took when I was investigating --

Q Notes.

THE COURT: What is the document that you showed the witness? Does it have a number?

MR. BERTOLLINI: This was a document not admitted into evidence.

THE COURT: That's fine.

MR. BERTOLLINI: It was provided to defense counsel with the discovery. And counsel relied upon these notes. The witness just testified that they are not accurate, for the record.

THE COURT: Here's the thing: I need to have the document identified with a number because it's part of the record. So, if you could give it a letter, like Defense A or Defense B, then we could make it part of the record of the case and it would go into the record even though it hasn't been admitted or placed before the jury.

MR. BERTOLLINI: I'd like to mark it for identification purposes as Defense Exhibit 1.

THE COURT: Use letters.

MR. BERTOLLINI: Defense Exhibit A.

THE COURT: Defense A for identification. Thank you. Let's move on.

(Defense Exhibit A so marked.)

Q You examine the script, you said, correct?

A Correct.

Q Did you examine the oro.org domain?

A I did not.

Q So, you don't know who this domain belong to, correct?

A I don't know that domain.
Q Have you visited this 192 bot server?
A No, I don't believe I visited that.
Q So, you have examined the script but you have not visited the source of the bot, correct?
A Correct.
Q Why is that?
A At that point, when I analyzed the script, it didn't really provide any additional value to me.
Q Are you familiar with Threatpost.com?
A Threatpost is a new site that posts about security news.
Q Is it a reliable source of news?
A It's reasonably reliable, yes.
Q Are you aware there was an article on September 15, 2014, that quoted you extensively on Shellshot vulnerability?
A Yes, I believe I've seen that article.
Q Would you like to see again to refresh your memory?
A Sure.
THE COURT: Well, was there a question? Why don't you ask him a question? If he doesn't remember, then you can show him the document.
MR. BERTOLLINI: Okay.
THE COURT: Do you remember the article?
THE WITNESS: I roughly remember it, but I would like to see it.

THE COURT: You'd like to see it.

What's the question?

Q The question is isn't it true that with respect to this bot net, you declare that: It is not a full-fledged command and control server in that it doesn't appear to send any commands, nor does it track the system, look for updates, from the bot. Right now, I don't think that is happening.

Is that accurate?

A It's probably accurate. That's what I said at the time. I don't remember the exact statement.

Q If this article came out on December 15 and in this article you're saying that these bots, these infected QNAP devices don't go anywhere, can these infected QNAP make any click through the botnet?

A This was a day or so after, yes, at that time it's very likely that the command control server was shut down.

Q So, by December 15, if there's no control banner, there's no click from the traffic device, correct?

A Correct.

Q You say during your direct examination that the Shellshock vulnerability won't harm QNAP device, correct?

A Correct.

Q Are you aware that many of the QNAP owners have not patched the device?

A Correct, many of them have not patched the device.

Did you say not patched or no patch?
Q Not patched.
A Correct, many of them have not patched.
Q So, the devices that were infected, you say that would be harmed, correct?
A Correct, yes.
Q But its owner perhaps didn't patch it, correct?
A Correct.
Q If your machine is broken, what do you do generally? Any machine; your car, your computer.
A Try to fix it.
Q Okay. So, if we had unpatched NAS devices, why wouldn't the owner fix them?
MS. KOMATIREDDY: Objection.
THE COURT: Sustained.
Q Can you explain in detail what kind of harm would the Shellshock cause the device?
A It will add additional lode to device because now it runs additional scripts on it, it will potentially add additional files, so it uses disc space. It may also steal data from a device which --
Q No, we're talking about the damage.
A I call that damage to my computer.
Q What is the size of the script?
A It's very small.

Q How small?
A A few kilobytes, maybe megabytes.
Q And how big is the QNAP hard drive?
A Usually in the terabyte range, so a thousand times larger.
Q How many of the Shellshock scripts can the QNAP host?
A The QNAP could host a lot of the Shellshock scripts, but the damage would be caused by additional files that may have been uploaded via the back door.
Q You testified at the end the script, the script erases the files, correct?
A Correct, some of the files; the initial test files, not all the files.
Q And it leaves the back door, correct?
A Correct.
Q What is the file size of the back door?
A The back door file size is small, but the damage that's caused by the back door --
Q That is not my question. What is the size of the back door?
A The size of the back door is, again, small. It's a few megabytes.
Q When a QNAP infected by this worm clicks or autoclicks, how many CPU resource does that click take?
A A very small number.

Q For how long is that CPU used?
A Milliseconds, fractions of a second.
Q Have you witnessed any control panel involving infected QNAP devices?
A Could you repeat the first part, please?
Q Have you witnessed any operating control panel involving infected QNAP devices?
A Contraband?
Q Control panel.
A Oh, control panel, sorry. No, I have not.
Q The Government showed you a picture of an IRC shot, correct?
A Correct.
Q Do you know what the host of that shot is?
A I know nothing about that other than what you saw in the screen shot.
Q You have not examined that host, correct?
A No.
Q Have you witnessed any control panel of IRC shots controlled by Fabio Gasperini?
A Actually, the first time I learned about your client was here, so no.
Q You talk about the files .64 and .32, correct?
A Correct.
Q Where do they connect?

A I did not really inspect those files in detail, I just analyzed them. They're substantially the same as the one on the ARM version of the malware. I inspected the ARM one because I had the device that ran it.
Q You testified that in order to figure out the password that was included and created in the infected QNAP, you used Hashcrack?
A Hashcat, C-A-T.
Q That's a software, correct?
A That's a software.
Q And it's used to decrypt or crack passwords, correct?
A Yes.
Q Is it illegal to have?
A It's legal to have.
Q It is legal?
A I'm not a lawyer, but I believe it's legal to own.

(Continued on next page.)

CROSS EXAMINATION
BY MR. BERTOLLINI: (Continuing)
Q Can a security expert view that software to test the vulnerability of its own passwords?
A Yes, that's how it has been commonly used.
Q Do you know the software called John the Ripper?
A Yes, that's a very similar piece of software.
Q Is that substantially similar to yours?
A I consider hashcat a more modern, faster version of John the Ripper, but it substantially --
Q But substantially the same?
A -- the same.
Q Okay. So using hashcat for research purposes does not make you a hacker; correct?
A Correct.
Q You say you have tested this worm on your own QNAP devices; correct?
A Correct.
Q And the Government showed you the screens as you ran the script on your device; correct?
A Yeah. Those screen shots were running the script against the device provided by the Government.
Q What is the name of the script that you analyzed? What is the file name?
A I started out with test.sh, which was the filed that we

retrieved from Pastebin.
Q Test?
A Test.
Q Have you examined S0?
A No, I believe I have not examined S0. Actually, I have looked at the file. I have not run it.
Q Have you examined S00.SH?
A No.
Q During your analysis of the script, you say that this script will download the EMME and CL scripts from the 23 server; correct?
A Correct.
Q And the EMME is used for the click counts; correct?
A Correct. It downloads banner ads.
Q Isn't it true that all these comments the EMME does can be done from the control panel?
A From which control panel?
Q The IRC control panel.
A Correct. And the screen shot you saw showed a wget from that control panel, yes.
Q If you were a hacker and you could control this auto clicks from the IRC control panel, wouldn't that be safer than running the EMME script?
A The problem may be that you have to actually be there to execute it while the script runs.

Q I'm asking you if clicking from the control panel would be more efficient and safer than running the EMME script?
A No, I think it is equivalent.
Q But the EMME script relies on two additional servers; correct, 23 and 178; correct?
A Correct.
Q If you control clicks from the control panel, you do not have to rely on such additional servers; correct?
A Yes, you do because otherwise the server would not connect to your control panel. It first has to download to the bots software to connect to your control panel.
Q What if you put those files within the same host of the control panel, then it is one server; correct?
A One server, yes.
Q Not three servers; correct?

So you testified that the EMME script download the file called agent PHP; correct?
A Yes.
Q And the agent PHP is the user agent screen; correct?
A Yes.
Q User agent screen is absolutely needed for the click?
A Correct.
Q So if the device did not download agent.php, it didn't click?
A The click probably did not count. It still clicked, but

the advertisement system would very easily be able to --
Q Disallow it?
A -- to disallow it.
Q I want to show you part of your script analysis here. Is this what you have been discussing during your direct examination?
A Correct. This is when I ran the script against the QNAP device.
THE COURT: Mr. Bertollini, do you have the exhibit number on that?
MR. BERTOLLINI: This is a Government Exhibit. It is Exhibit 203, page 6.
THE COURT: Fine. I just need it for the record. And it is in evidence. Go ahead.
Q So this is when this script executes; correct? It execute test of SH; correct?
A Correct.
Q And this is the part where he download the user agent's name?
A Correct.
Q I want to give this to you to show me something that I can't understand.
MR. BERTOLLINI: Can I approach the witness?
THE COURT: Well, you can show it to him.
MR. BERTOLLINI: Well, I needed to highlight

something.
A I can highlight on the screen here.
THE COURT: If you just point on the screen, you will get an arrow.
THE WITNESS: Okay. Thanks.
THE COURT: Go ahead.
Q Can you show me on this script here the part that downloads EMME and CL from the 23 server?
A This is not shown here on this screen shot.
Q It is not shown?
A No.
THE COURT: Is it somewhere else?
THE WITNESS: It was already downloaded. This is when I ran the script the second time.
Q So you analyzed this and you counting up parts?
A I didn't count off parts. These are just parts that didn't run here. This is also run in a laboratory, so --
Q So you are saying that the EMME script did not run in this instance?
A In this instance, it did not get downloaded. It ran, actually. It did not get downloaded.
Q So in this instance, it did not download EMME and CL. And you have a QNAP device; correct?
A Correct.
Q I am going to withdraw. You have a QNAP device?

A Correct.
Q And you say that the script will download EMME and CL; correct?
A Yes.
Q And you will execute the files?
A Uh-hum.
Q And the system will be cleaned up at the end, correct?
A Some of these files will be removed.
Q You just say that in your QNAP test the EMME script didn't execute; correct?
A I ran this test two weeks ago or three weeks ago in the lab for -- and --
Q You did not execute. Okay.
MS. KOMATIREDDY: Objection, Your Honor.
THE COURT: Sustained.
Please don't over speak the witness' answer. Go ahead.
Q Isn't it possible then that other QNAP devices downloaded the script and did not execute EMME or CL?
A It is possible that some were not able to download it. But we definitely observed that at the time that QNAP device downloaded.
Q So you are saying that it is possible that they didn't download or execute EMME; correct?
A Correct.

Q And if it didn't download or execute EMME, there is no click; correct.
A Correct. If the file is not available to them, then....
Q Let me ask you this, if you have a QNAP device and you open the shadow file, if the user request is not in the shadow file, what would you consider the QNAP? Infected or not infected?
A Well, if the QNAP user is not present in the shadow file then -- sorry, the request user is not present in the shadow file, it would not be infected by this particular bot.
Q Not be infected by this bot. And you say the malware created and opened SSH 26; correct?
A Correct.
Q So if you have a QNAP device that doesn't have that part open, would that QNAP be infected or not infected by this particular virus?
A It will probably not be infected.
THE COURT: Okay. We have reached five o'clock and we will break for the day and resume at 9:30 tomorrow morning. I am going to remind you about something I said at the beginning. You will hear it again and again. We are going to adjourn now for the day. Before we do, let me remind you that it is extremely important that you follow my instruction that you not discuss this case with anyone, not your family, friends, or business associates, and not your fellow jurors.

A Good morning.
Q Dr. Ullrich, yesterday you testified that to come to testify at this trial you were getting paid $70.
A Correct. I am being paid expenses.
May I make a correction to something I stated yesterday?
Q Let me give you a reminder so we don't waste time, when I ask you a leading question --
THE COURT: You already told him that. Keep going.
MR. BERTOLLINI: Okay.
Q When I ask you something, keep your answer as to my questions.
A Yes, sir.
Q So $70 a day or $07 total?
A I'm getting paid expenses. I don't know what the exact amount.
Q Okay. So you are not getting compensated?
A Correct.
Q You are getting reimbursed?
A Correct.
Q Is this your normal fee for such service?
A I've never done this before, so I don't have a normal fee, but it is less than I usually charge.
Q Okay. Do you charge the Government to do forensics examination of the script?

A No.
Q Is it normal for you not to charge for such service?
A I often do things like this without charging for it.
Q Yesterday you testified that you downloaded the EMME script directly from the 23 server; correct?
A Correct.
Q You also testified that you did not download the test.sh script from the 185 server; correct?
A Correct.
Q So now, from what IP address did you download the EMME script from the 23 server?
A I don't have the IP address in front of me, but I followed the instructions in the test.sh script.
Q What is the IP address that you generally use, do you know?
A Sorry?
Q What is the IP address that you generally use?
A I use the IP address in the test.sh script.
Q When you browse the internet, what IP address goes out from --
A So my personal IP address is what --
Q Your personal -- not the personal. The IP address that you used to download this QNAP.
A It probably was my home system that I typically used to investigate things like this.

Q And what is your home IP address?
MS. KOMATIREDDY: Objection, Your Honor.
THE COURT: Sustained.
Q Okay. So I don't have your IP address; correct?
A Correct.
Q So besides your word, I have no other way to verify that you actually downloaded the EMME script from 23; correct?
A Correct.
Q Because I cannot check your IP address with the server; correct?
A Correct.
Q Yesterday we talked about the differences between static IP address and dynamic IP address, do you remember?
A Yes, I do.
Q If you have a list of IP addresses, is there any way you know you can determine whether that particular -- whether one particular IP address is dynamic or static?
A There is no perfect way to determine this.
Q Is there any way you know to determine whether any IP address will respond to a QNAP device?
A At the time you see the IP address, it would possibly connect to the IP address.
MR. BERTOLLINI: I am moving to strike the answer.
Q I am asking do you know a way to determine whether a specific IP address is or is not a QNAP device?

A No, I do not.
Q You do not?
A Do not.
Q Yesterday you brought a QNAP device to court; correct?
A Correct.
Q Do you still have that with you?
A No, I do not. I believe it's in the bin behind you.
MR. BERTOLLINI: May I approach the witness with the QNAP device?
THE COURT: It is in evidence, is it not?
MS. KOMATIREDDY: It is. We have no objection.
THE COURT: Go ahead.
MR. BERTOLLINI: For the record, I'm handing the QNAP device to Dr. Ullrich.
THE COURT: And the exhibit number on that is what?
MS. KOMATIREDDY: 1B.
THE COURT: 1B. Thank you. Could you take it out of the box so we don't waste any time. Let's move on.
Q What QNAP model is that?
A TS-212E, as in echo.
Q TS-212E?
A Correct.
Q Tom?
A Tom, sierra, 212, echo.
Q What is the serial number on the device?

A The serial number is Q144B08947.
Q Q144, B like boy, 08947?
A Correct.
Q When did you purchase this device?
A I did not purchase the device. It was provided to me by the Government.
Q When did the Government provide you with the QNAP device?
A About a month ago.
Q And you say you examined the device; correct?
A Correct.
Q What firmware does the device had?
A It came without any firmware installed. I installed the last firmware that was vulnerable to the Shellshock exploit.
Q What version is that?
A I forgot what the version number is.
Q Okay. At the SANS Institute, do you have QNAP devices?
A Yes.
Q What brand?
A I do have two QNAP devices. I have AllReady Net, Netgear device. We probably have a number of additional devices, but these are the ones that I am familiar with.
Q Do you keep them behind or outside the firewall?
A Behind the firewall.
Q Why do you do that?
A Because of vulnerabilities like Shellshock, in order to

protect them.
Q So it is safer, if not advisable, to put them behind a firewall?
A Correct.
Q Are you in charge of those QNAP devices at SANS?
A I'm in charge of the two QNAP devices, yes.
Q Are you aware that by default SSH port 22 of this device is open?
A Yes, and I misstated this yesterday. I would like to correct this. SSH is open. And on this device, SSH was open as well. This is how I obtained these screen shots of the modified files.
Q So yesterday you say that the ports were closed and now you are saying that the SSH port is open?
A It's open.
Q Which one?
A Port 22.
Q 22. Is there any difference between -- would there be any difference between any of the available SSH ports?
A Difference in?
Q For example, something you can do with the port that you cannot do with another or you can do the same things --
A SSH may listen on all ports.
THE COURT: For the jury and me, what does that mean?

THE WITNESS: What this means is you can configure SSH, the service that will accept connections on various ports. A port is an additional address, like a floor number that you use to connect to the device. If the IP address is the street address, then the port is the floor number that you use to connect to it.

Q Do you know who invented the Shellshock vulnerability?

A I don't recall.

Q Do you know if defendant invented the Shellshock vulnerability?

A I'm sorry.

Q Do you know if defendant --

A I don't believe he invented.

Q He didn't invent.

Let me ask you this, you said that the script opens port 26; correct?

A Correct.

Q Why will there be a need to open an SSH port if the device comes to the port already open?

A For example, in order to evade firewall rules that may block access to port 22, also, in case the administrator turns off SH on port 22 to harden the device, port 26 would still be open.

Q I understand, but the ports are closed by default. So I'm not sure I'm following your point.

If the ports are closed, they are not vulnerable, are they?
A Ports on a firewall in front of the device or under the device.
Q So you are saying that if a firewall is set up to block port 22, why would you set such firewall in such a way, like why would you set your firewall only to block port 22?
A Port 22 is a very commonly attacked port because services like SSH are listening on this port.
Q Why wouldn't you put all the ports behind the firewall, as you do?
A It's convenience by the administrator. Sometimes applications need certain ports, so administrators are careful not to block any brick fire ports.
Q And you say that you put your QNAP behind the firewall?
A I do, yes.
Q Okay. Does the QNAP have a CC count?
A I don't believe it has a CC count file by default.
Q Can you watch satellite TV from a QNAP?
A No. QNAPs can be used to stream video but not satellite TV.
Q Yes or no?
A No.
Q Can you watch cable TV from QNAP, yes or no?
A No.

Q Yesterday you say that within the EMME script you found a file called CL; correct?
A Correct.
Q And you say that the CL steals users and passwords the way that the satellite would do; correct?
A Correct.
Q So what happens if CL gets into a QNAP, what kind of user and password would the virus steal?
A If the virus is not pressing, then it will not steal any users and passwords.
Q So if the file related to the cable or the satellite is not in the QNAP, it will not take it?
A Correct.
Q And did you just say that you can't watch cable or satellite directly from the QNAP?
A Correct.
Q Yesterday you also talk about port scanning. Do you remember?
A I probably did, yeah.
Q Now, when you do a port scanning, does the software access any ports?
A It depends on how the port scan is configured, but typically it does access a large number of ports.
Q When you do the ports scan, does the software scanning the internet enter into any port? Does it access any port,

the scanner?
A Yes, it may access any port. That's up to the user to configure.
Q So you're saying that it is called a scanner but it actually intrudes ports?
A It connects to the port and checks if there is a response coming back.
Q So it connects to the port? It doesn't access the port?
A Correct.
Q And when it connects to the port, does it damage it or not?
A No. Typically it does not damage it.
Q Is it illegal to scan the internet in your expert opinion?
A I'm not a lawyer, but I don't believe it is.
Q When the script is run in the QNAP device, it executes a number of comments; correct?
A Correct.
Q These comments change the VNS; correct?
A Correct.
Q Creates the port on SSH 26; correct?
A Correct.
Q And installs the backdoor?
A Yes.
Q It patches?

A Yes.
Q It reboots, or first it erases the file and then it reboots; correct?
A It sort of happens at the same time.
Q So now during this process, does the script take anything at all from the QNAP?
A It only retrieves information about the system configuration in order to run.
Q So what configuration -- what, for example --
A What processor is running --
Q What processor. Okay. So it may have an arm-based processor or an --
THE COURT: You can't speak at the same time. One question and then an answer. Go ahead, please.
Q It might have an arm-based architecture?
A Correct.
Q Or it might have an I-686 architecture; correct?
A Yes, sir.
Q I am going to bring your attention to your notes that I showed you yesterday.
MR. BERTOLLINI: Your Honor, I would like to mark the notes as Defendant's Exhibit B for identification purposes.
THE COURT: I'm sorry, the notes, how many pages are there of these notes?

MR. BERTOLLINI: Six pages.

THE COURT: Does the Government know what six pages we are talking about?

MS. KOMATIREDDY: We are just waiting for it to come up on the screen.

MR. BERTOLLINI: I can describe it.

THE COURT: Just show it to the Government. We are making some changes on the screens right now.

Q Before we look at your notes again, yesterday you talk about the backdoor; correct?

A Correct.

Q And the backdoor is exo.cgi; correct?

A Correct. I believe the file is originally named armgH.cgi, but they were renamed into exo.cgi.

Q Yes. That's what you --

A That's why I called the notes the web backdoor.

Q And if that -- if the specific QNAP were to have the I-686 architecture, it would be gh.cgi; correct?

A Correct. There are different names for different architectures.

Q Okay. Now, I want to show you your notes.

THE COURT: Are these in evidence?

MS. KOMATIREDDY: No, Your Honor.

THE COURT: Okay.

Q So here we have -- one second. Page 1, we have right

here armgH.cgi?
A I do not see anything.
THE COURT: How is that? Do you have it?
THE WITNESS: Got it.
Q Do you see it now?
A I do see the notes now. Let me see if I see -- okay.
Q ArmgH.cgi, this would be the file of the backdoor if the QNAP were to have the arm-based architecture; correct?
A Correct.
Q In your notes here you put the armgH is an IRC bot; correct?
A Actually, the .cgi is the IRC bot. The armgH is not the IRC bots.
Q Yesterday you say that these notes were wrong?
A These notes are notes I took while I was investigating the final reporting.
Q So while investigating --
THE COURT: He has to finish before you start and you have to finish before he starts. That's the way it works, because the court reporter can't take down what you are both saying at the same time. It is a physical impossibility. That much I know. Everybody has to cooperate and the jury is not going to hear everything.
Let's continue.
Q Okay. When you were investigating this, you figured that

armgH was an IRC bot; correct?

A Can you point -- that was my assumption at the time, yes.

(Continued on following page.)

BY MR. BERTOLLINI:
Q And on what basis did you make that assumption?
A I typically look at strings in a file. I may have also uploaded it to a site called VirusTotal that does a quick analysis of the file.
Q Yesterday you said that you did not examine the back door, correct?
A I did not examine in detail the armgH file. I probably just did that, I uploaded it to the -- to VirusTotal.
Q So how did you later determine that armgH is not an IRC bot?
A Based on the report I got from VirusTotal and based on strings, it did not appear to be an IRC bot.
Q So you wrote the note before running the file through the software?
A Correct, I wrote these notes as I was reading this file.
Q Okay. So, if someone is now using that software, he might be likely to believe it is an IRC bot as you did.
A Sorry?
Q If someone is now running the file with the same software, he might be inclined to believe at first impression that that's IRC bot.
A That's possible, yes.
Q Let's move on to Page 3 of the same analysis. You have here gH.cgi, correct?

A Correct.
Q And that would be the file that the script will use if the QNAP was based on an IC86 architecture, correct?
A Correct.
Q When you were analyzing the script, you determine that this was a CGI factor, didn't you?
A Correct, I did.
Q And yesterday you say that this determination was wrong, turned out to be wrong.
A I believe that statement was wrong. I believe this was the CGI back door.
Q So, yesterday you testified that these notes were wrong and today you're testifying that these are actually right.
A They're wrong in parts. The earlier part was wrong. This part I believe is right.
Q So, what do you currently believe of armgH, is that an IRC bot or a back door?
A I believe armgH is the back door.
Q Okay. Is it true that armgH and gH contain binary language pointing to the 192 server which goes to ppolloo.org?
A I don't recall.
Q Okay. Let me refresh.
MR. BERTOLLINI: I actually left some of my notes there.
THE COURT: Please.

(Pause in proceedings.)
Q Here I have armgH and gH.cgi and I would like to show you both, okay?
A Okay.
THE COURT: This document, is it in evidence?
MR. BERTOLLINI: It's not in evidence, your Honor. I would like to mark armgH as Defendant Exhibit C for identification purposes, and I would like to mark gH Defendant Exhibit -- 4?
THE COURT: D.
MR. BERTOLLINI: I'm sorry, D.
THE COURT: That's fine.
(Defendant's Exhibits C and D so marked.)
MR. BERTOLLINI: Your Honor, I believe it would be more efficient if I deliver this personally after I show counsel because this machine I don't think will zoom enough.
THE COURT: You want to show it to the witness?
MR. BERTOLLINI: And to the Government.
THE COURT: Yes, you can show it to the Government. There are two; C and D, whatever they are. And then you can approach the witness and question him.
Can we remove the hardware now? Are we done with that?
MR. BERTOLLINI: We're done with it.
THE COURT: Just put it down on the floor for now.

Thank you, thank you very much.
Q Okay. You already testified that you didn't examine armgH or gH.cgi in depth, correct?
A Correct.
Q And I handed you two sheets of paper.
A Correct.
Q That reflects -- that is what -- can you describe what that is in a few words?
A This is a printout of the binary code. It does include some text.
Q Okay. What does the text say on the binary language?
A The text is the manual page showed yesterday that gives these IRC bots instructions, a list of instructions that could be used for the IRC bot.
Q So, what is the difference that you see from those two papers with respect to the instruction from the IRC bot?
A It's a little bit hard to read, but I don't see a substantial difference glancing at it.
Q Fair enough. Okay. So, you just say -- well, let's recap.

Yesterday you say that your notes on Page 3 regarding gH.cgi being a back door were wrong. Today you rectify and say they were right, that's a back door. Now you have just said that those two papers, gH and armgH, both contain binary language connecting to an IRC bot, correct?

A Correct.
Q So, how's that a back door if it contains binary language instructing a bot?
A A bot is a back door.
Q So, what you're saying now is that the IRC chat is a back door?
A IRC chat is back door that allows remote access to the system.
Q So, what you're saying essentially is that the IRC bot and back door are synonymous?
A They're similar. IRC bot is back door plus more. There's more that you can do than just the back door with IRC bot.
Q But you say right now those are essentially similar one to another?
A Correct, I do.
MR. BERTOLLINI: May I confer one moment with my client?
THE COURT: Of course.
Q So, yesterday you were discussing about dark web; do you remember?
A Yes, I do.
Q And you also testified that you have observed negotiations online on this dark web website, correct?
A Correct.

Q Have you ever witnessed the negotiation or the sale of IP addresses?
A IP addresses are usually not sold but systems connected to those IP addresses.
Q I ask you the IP address by itself, at least the IP address, is that marketable?
A It's marketable, but that's not something you would market on dark web; that's something you would buy and sell officially.
Q So, I'm assuming, based on your answer, that you have never observed any negotiation or sale of IP address lists; correct?
A IP address list as in lists of vulnerable systems?
Q As a list in general, a list of IPs.
A A list of IPs? No. They have to have some meaning or value.
Q You have not seen that negotiation?
THE COURT: He hadn't finished his answer.
You may finish your answer.
A I have not seen the sale of meaningless IP list.
Q Let's go back to the difference between a static and a dynamic IP. If you have a dynamic IP and your system reboots, are you going to get different IP or not?
A Not necessarily. It depends on the ISP.
Q Not necessarily.

What if you get a new IP? What part of the IP address changes?
A The entire IP address may change.
Q The entire.
A Again, that depends on how your ISP configures the network.
Q Not just the last of the four, five or the last two, you're saying all of it.
A Not only the last part may change, but anything may change.
THE COURT: "ISP" means?
THE WITNESS: Internet service provider.
THE COURT: Okay.
Q So, you say often it changes only the final five, correct?
A Correct.
Q You mean the fourth of the four parts or the third and fourth parts?
A The third and fourth is very common.
Q Very common, correct?
A Correct.
Q Let's go back for a second to the CL file. How, if anything, is that related to clicks or click fraud?
A CL is not related to click fraud.
Q Yesterday, you also testified with respect to the user

agent, saying that if a device clicks on an advertisement without a user agent's name, that click will be invalid, correct?

A Correct.

Q And you say that you're familiar with pay per click in a line advertisement, correct?

A Correct.

Q In your opinion, what would the advertiser believe, if anything, if the advertiser gets multiple clicks from the same advertiser without a user agent's name?

MS. KOMATIREDDY: Objection.

MR. BERTOLLINI: He say his answer.

THE COURT: Can you answer that question?

THE WITNESS: I can.

THE COURT: Go ahead.

A An advertiser will expect a limited number of clicks without a user agent, based on search engines and similar tools. But there's usually a threshold. And once that threshold is exceeded, the account is considered fraudulent.

THE COURT: Next?

Q So, if you have four simultaneous clicks without a user agent, what would happen, if anything, in your opinion?

A Four different clicks would probably not trigger that threshold yet. It's too small.

Q I say four simultaneous clicks from the same address.

A Still, I would think four simultaneous clicks from the same IP address would probably not raise an alarm. In particular in this case, there was additional parameter that identified the IP address as --

Q As the --

THE COURT: He has to finish the answer before there's another question. Go ahead.

A In this particular case, the different banners were identified with different position codes --

MR. BERTOLLINI: Your Honor, it's not responsive.

THE COURT: Excuse me. I have to hear the answer before I can rule on your objection. So, I want to hear the answer. I don't want part of the answer and then you interfere with the answer and then I have to ask him to answer it again so that you can then make your objection. That's three extra steps.

If you keep interrupting the answer, you have to stop asking the questions and sit down. So, let him finish his answer and then you can make your objection, and I'll rule on the objection.

Please, finish your answer.

THE WITNESS: Yes, sir.

A Four distinct clicks from one IP address at the same time typically do not raise to the limit where an advertiser would consider the account fraudulent. In this particular case, the

advertisements were labeled with different position codes which would identify them as distinct, different ads on that page.

MR. BERTOLLINI: Move to strike the answer as not responsive.

THE COURT: Overruled. Next question.

Q When was click fraud invented, as far as you know?

MS. KOMATIREDDY: Objection.

THE COURT: You may answer.

A I do not know when it was invented, but I believe it was invented as long ago as advertisements were invented.

THE COURT: You mean internet advertisements?

THE WITNESS: Internet advertisements.

Q You said yesterday that there's a difference between a visualization of an ad and a click, correct?

A Correct.

Q You also testified that some companies will pay you just for visualization while some others will pay you just for the click, correct?

A Correct.

Q You also testified that Google only pays you when you click, correct?

A Correct.

Q Have you ever worked for a company called JuiceADV?

A No, I have not.

Q So you have no idea whether they will pay an advertiser for visualizations only, correct?
A I do not know.
Q How much is a click paid on average to a site owner?
A Anywhere between a few cents and a couple of dollars.
Q From the advertiser?
A To the website that displays the advertisements, yes.
Q What's the average, in your opinion?
A Ten cents is probably fair average.
Q Do you know if companies protect themselves from click fraud?
A Yes, they do.
Q Do you know if an advertiser will need a valid IP address to validate a click?
A Yes, they do.
Q How about the user agent's name?
A Typically, user agent's name is used as part of that validation, yes.
Q How about internet history?
A That usually affects as well, yes.
Q Does an advertisement monitor the IP location of the clicks?
A The IP location could affect whether it's considered fraud and also affect the money being paid.
Q The advertiser monitor the click-through rate?

A Yes, they do.
Q And mobile phone click-through rate?
A Mobile click-through rates are in the one to five percent range.
Q Meaning that every 100 visits on average is only two clicks, correct?
A Correct.
Q Does an advertiser need cookies to verify validity of a click?
A Yes, cookies are used as part of that.
Q Yesterday, you testified with respect to the EMME.
A Yes, I remember.
Q You testified that the script, when it runs, IT downloads the banners four times, correct?
A It attempts to download banners four times, I believe is what I said. The last version fails on QNAP devices, the last of the four times fail.
Q After the script downloads the banners, how many clicks, if any, does EMME?
A This should not trigger any clicks, it will just trigger exposures.
Q What you're saying, in other words, is that the EMME script only views the banner correct?
A Correct.
Q It does not click on the banner, correct?

A Correct.
Q And if you're advertising with an advertisement company that does not pay for visualization, it means that you get zero, correct?
A Correct.
Q You also testified that if you have a botnet, you can enter such commands to direct all the connected affected QNAP devices to click specific site, correct?
A Correct, I did.
Q Let's assume that we have a botnet with 500 QNAP infected devices. And let's assume that the owner of that botnet enters to the command to have them click. In that case, how many clicks would the referring website get?
A The referring website would get these 500 clicks.
Q And what would be the time frame between these 500 clicks?
A This will happen very fast; within seconds.
Q And how would the advertisement company validate 500 clicks made in a matter of seconds?
A I do not know how an advertisement company would validate it, but they should be able to deal with that speed.
Q I'm not talking about the speed, I'm talking about the volume. Wouldn't that be a little suspicious, to have 500 clicks in a matter of second?
A Yes, that would be suspicious.

Q And unless -- withdrawn.

You just testified that normal click-through rate for a site will be two percent, correct?

A Correct.

Q That would mean that if you have 500 real clicks, you will have to have 500 per 50 times to stay in two percent click-through rate, correct?

A Correct.

Q So, unless the website makes -- 500 per 50 is 25,000, correct?

A Yes, I believe so.

Q So, unless the domain makes 25,000 visits, those 500 botnet clicks will go well above the two percent normal click-through rate.

A Yes, sir.

Q Now, if you are using a botnet to make these clicks and you're using the EMME script, would the QNAP infected device show or attempt to fabricate cookies?

A No, there was no evidence that cookies are fabricated.

Q So, in other words, these 500 hypothetical clicks would all have no cookies, correct?

In other words, it would mean that to the advertisers' point of view -- advertisement company's point of view, these 500 persons or bots -- not real person -- making the clicks will have to visit the referring site directly,

correct?
A Could you repeat?
Q Okay. From the advertisement company's point of view, looking at these 500 clicks may almost seem fantasy, as you say. These clicks would all come without cookies you say, correct?
A Correct.
Q Without browsing history, correct?
A Correct.
Q So, in other words, just to explain the jury, it would look like these 500 computers just clicked directly on the browser's bar, they refer the website, correct?
A Correct.
Q Without a Google search.
A Without first downloading the banner.
Q Without downloading the banner, okay, but with or without a Google search?
A A Google search is really not related to this.
Q It's not related. So, these 500 computers affected going to the referred website with the advertisement will go there without going to a Google search or a search engine search, correct?
A Correct. These advertisements are totally unrelated to search engines.
Q How would advertisement company validate such clicks?

A The advertisement company would not have the cookie to validate the click.

MR. BERTOLLINI: Your Honor, may I propose a quick recess?

THE COURT: No.

MR. BERTOLLINI: Okay.

Q Yesterday, with respect to the botnet and its potential capabilities, you testified about websites being potentially flooded by bot advertise, correct?

A Correct.

Q Have you witnessed any operating botnet making such flooding attacks?

A Yes, I have.

Q And the attacks that you witnessed were coming from botnet operated by Defendant?

A No, I did not.

Q So, yesterday you were more explaining what a botnet can do, correct?

A Correct.

Q Rather than explaining whether Defendant ever had a botnet, correct?

A Correct.

Q Yesterday, with respect to the script and with respect to the file that remains in the infected QNAP device, you testified that a file named .cgi remains in the system,

correct?
A During a test of our maintenance system, yes.
Q .cgi?
A Correct.
Q So, let's assume we have a QNAP that does not have .cgi. Will that QNAP be infected or not infected?
A It would not be infected by this particular bot.
Q You just said from this particular version?
A Correct.
Q Because there are, in your opinion, different versions of this, correct?
A There are many different versions.
Q Many different versions.

Yesterday, you testified that you have not witnessed an operating IRC botnet of QNAP devices, correct?
A Correct.
Q If the QNAP device infected with the files do not connect with an IRC chat, what do they do?
A They just sit there and try to connect, but that's it.
Q They don't click, do they?
A They don't click.

MR. BERTOLLINI: Can I confer one moment, your Honor?

THE COURT: Yes, you may.

(Pause in proceedings.)

MR. BERTOLLINI: I have no further questions for this witness, your Honor.

THE COURT: Very well.

MR. BERTOLLINI: Thank you.

THE COURT: Redirect.

MS. KOMATIREDDY: Your Honor, if I may approach the witness with a binder of exhibits.

THE COURT: Sure. Are these exhibits that are in evidence?

MS. KOMATIREDDY: Yes, your Honor.

THE COURT: All right. Yes.

Mr. Bertollini, you want to take your exhibits back, please.

MS. KOMATIREDDY: We will be referring to Defense Exhibit D.

THE COURT: You can hold on, then.

MR. BERTOLLINI: Yes, can I move to admit them later on or move to admit them right before we excuse the witness?

THE COURT: I think you should move to admit them now since they were part of your cross-examination.

Which exhibits are you talking about.

MR. BERTOLLINI: Yesterday I showed him A, B and today I showed him C and D.

THE COURT: Is there any objection to these exhibits?

MS. KOMATIREDDY: There is, your Honor, as to A and B; not C and D, the scripts currently in counsel's possession.

THE COURT: I don't have A and B in my possession so I wouldn't be able to rule on that. I'll review them at break.

As to C and D, there's no objection?

MS. KOMATIREDDY: No, your Honor.

THE COURT: Defense Exhibits C and D are received in evidence. As to Exhibits A and B, I will rule after reviewing the exhibits at some point, okay?

(Defendant's Exhibits C and D so marked.)

THE COURT: So, let's have redirect now. Thank you.

REDIRECT EXAMINATION

BY MS. KOMATIREDDY:

Q Dr. Ullrich, what are cookies?

A Cookies are identifiers that websites send to a client so they can reidentify the client when the client comes back to a particular website.

Q The scripts that you analyzed yesterday, test and the others, do they have anything to do with cookies?

A There were no cookies used.

Q You were asked on cross-examination about the CL file and whether it was related to click fraud. What was your answer on that?

A It's not related to click fraud.

explode or melt down or become in any obvious way broken. It still ran and it still fulfilled its functions.
Q What did happen?
A What happened was that the confidentiality, really, of the information on the device was put at risk by installing these back-doors.
Q And to what extent was it put at risk?
A Other attackers could now, for example, come in and connect the device, download any files on the device. They could delete or encrypt these files.
Q What type of access did the attacker have to the victim computer?
A The attacker with the request account had full access to the victim's computer.
Q That's complete control over the data on the computer?
A Correct.
Q Also known as root access?
A Correct.
Q So, the system was totally compromised?
A That is correct.
MS. KOMATIREDDY: No further questions.
THE COURT: Re-cross.
RECROSS-EXAMINATION
BY MR. BERTOLLINI:
Q You just testified that other attackers could go back in

and potentially steal information to the device; correct?
A That is possible, yes.
Q Other attackers, you say; correct?
A I said other attackers, but also includes the original.
Q So yesterday you testified that this script installs the QNAP patch from its original QNAP website; correct?
A Correct.
Q After the device downloads and execute the patch, can anyone exploit the QNAP Shellshock vulnerability?
A No.
Q You just testified that there may be instances where the script is downloaded but not fully executed.

You just say that; correct?

A Correct.
Q What is the timeframe for execution of this script?
A Seconds.
Q What are the odds that within seconds it does not fully execute?

MS. KOMATIREDDY: Objection.

THE COURT: You may answer.

A There's a low probability that this will happen.
Q Low or very low?
A Very low.
Q Thank you.

And you just testified the back-door comes in a

variety of formats, depending on the architecture of the QNAP; correct?
A Correct.
Q Isn't it true that no matter what the architecture of the QNAP is, his old files will be renamed to exo.cgi?
A I do not exactly recall.
Q So, you don't know what is the name of the back-door as it appears after the scripts execute?
A I do not recall it right now.
Q Would looking at the notes of the script help you refresh your memory?
A Sure.
(Exhibit published to jury.)
THE COURT: What is the Exhibit number?
MR. BERTOLLINI: This, Your Honor, is...
THE WITNESS: There is a Government's Exhibit.
MS. KOMATIREDDY: It is not in evidence, Your Honor.
MR. BERTOLLINI: I would like to mark it as Defendant's Exhibit E for identification purposes.
THE COURT: Well, let's just show it to the witness and maybe you can get your answer.
(Pause in the proceedings.)
MR. BERTOLLINI: Exhibit E for defendant for identification purposes.
THE COURT: Okay, you can show it to the witness.

MR. BERTOLLINI: Okay.
Q So, let's look at the -- I'm sorry.
Your note here, which based on architecture?
A Correct.
Q That's what you testified before; correct?
A Yes.
Q ArmgH is one version; correct?
A Correct.
Q And what does happen, if anything to armgH -- isn't it true --
MR. BERTOLLINI: Withdrawn.
Q Isn't it true that armgH becomes exo.cgi?
A Can you scroll up a little bit? I'm sorry.
Yeah, but I'm pretty sure that the second-to-last line you see the rename to exo.cgi.
And then the line after that, it's actually being copied to .exo.cgi.
Q So it does rename to .cgi?
A Yes.
Q Let's look at page 3 when we talk about gH.cgi.
You just testified there is another variance of the QNAP; correct?
A Correct.
Q But in particular, this particular version will operate on I686 architecture based QNAP devices; correct?

A Correct.
Q What happens, if anything, to gH?
A Its later renamed to .exo.cgi and copied to exo.cgi.
Q So, it's basically the same process, isn't it?
A Correct.
Q You also discussed, and this is my last line, about agent.php; correct?
A I did.
Q You say that if the device downloaded agent.php, it got to be involved with the EMME script; correct?
A Involved, with?
Q EMME?
A M?
THE COURT: E-M-M-E.
A EMME, yes, that's correct, yes, sir.
Q Are you saying that agent.php can only be identified with EMME script?
A It is possible that other scripts will load the same file, but I have not observed any other scripts that access that file.
Q What is agent.php? Is that a BIOS?
A Agent.php is a web service that provides a user agent. So, all it does is it provides a string.
Q Is it illegal to have?
A No.

Q It is not illegal to have.

You are saying agent.php is illegal to have?

MS. KOMATIREDDY: Objection, Your Honor.

THE COURT: I'm sorry. One moment.

(Pause in the proceedings.)

THE COURT: Can you rephrase the question?

MR. BERTOLLINI: Yes.

Q Is the file, agent.php, a legal file to possess?

MS. KOMATIREDDY: Objection.

THE COURT: Sustained.

Q Isn't it true that you can use agent.php on old browsers to simulate a new browser?

A Most browsers allow you to adjust the user agent. You would not necessarily use agent.php but another method to accomplish the same thing.

(Continued on following page.)

RECROSS EXAMINATION
BY MR. BERTOLLINI: (Continuing)
Q Can you use agent.PHP to accomplish the same method?
A With wget, yes.
Q So I'm assuming I have been on the computer and I want to browse to agent and it only accepts Mozilla, my computer does not accept Mozilla as an installment, can I use agent PHP on my other browser?
A You would not use agent.PHP, but you would use a technique that's essentially identical to that.
Q Okay. I will use something identical.
A Yes.
MR. BERTOLLINI: No further questions, Your Honor.
THE COURT: Anything else?
MS. KOMATIREDDY: Not from the Government.
THE COURT: All right. The witness is excused. You may stand down. Watch your step.
(Witness excused.)
MS. KOMATIREDDY: If I may retrieve the exhibits, Your Honor.
THE COURT: Yes, please.
MR. BERTOLLINI: Your Honor, I have the other exhibit.
THE COURT: All right. This would be a convenient time to take our morning break.