UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN
GREEN BAY DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	Case No. CR 18-157
	)	Green Bay, Wisconsin
vs.	)	
	)	August 14, 2019
THOMAS J. OWENS,	)	1:35 p.m.
	)	
Defendant.	)	

TRANSCRIPT OF EVIDENTIARY HEARING
BEFORE THE HONORABLE WILLIAM C. GRIESBACH
UNITED STATES CHIEF DISTRICT JUDGE

APPEARANCES:

For the Plaintiff UNITED STATES OF AMERICA:	United States Dept of Justice (ED-WI) By: DANIEL R. HUMBLE Office of the US Attorney - 205 Doty St - Ste 301 Green Bay, WI 54301 Ph: 920-884-1066 Fax: 920-884-2997 Daniel.Humble@usdoj.gov
For the Defendant THOMAS J. OWENS: (Present)	Pruhs & Donovan SC By: CHRISTOPHER D. DONOVAN 757 N Broadway - Ste 401 Milwaukee, WI 53202 Ph: 414-221-1950 Fax: 414-221-1959 donovanc34@hotmail.com
U.S. Official Transcriber: Transcript Orders:	JOHN T. SCHINDHELM, RMR, CRR, WWW.JOHNSCHINDHELM.COM

Proceedings recorded by electronic recording,
transcript produced by computer aided transcription.

TRANSCRIPT OF PROCEEDINGS

Transcribed From Audio Recording

* * *

THE CLERK: The Court calls Case 18-CR-157, United
01:42 States of America vs. Thomas J. Owens for an evidentiary hearing. May I have the appearances, please?

MR. HUMBLE: Dan Humble for the Government, along with Misha Linsmayer (phonetic) from our office, Your Honor.

THE COURT: Good afternoon.

01:43 MR. DONOVAN: Attorney Chris Donovan appearing on behalf of Mr. Owens who is here in person on my right. And then, also to my immediate right is our expert, Peyton Engel.

THE COURT: Okay. Good afternoon.

So we have put this on for a hearing on the motion to
01:44 disclose investigative BitTorrent software and related documents. And the government has opposed the motion on the basis of the law enforcement privilege?

MR. HUMBLE: Yes, Your Honor.

THE COURT: Or investigation privilege?

01:45 And so the -- I guess, what do you -- Mr. Donovan, it's your motion, how would you plan on proceeding?

MR. DONOVAN: Your Honor, what I envision is I would call my expert. I think that we have at least the initial burden under Rule 16 to show that the requested material is
01:45 material to preparing our defense.

THE COURT: Uh-huh.

MR. DONOVAN: And then I think the burden on the law enforcement privilege would fall to the government, so they can, you know, carry that burden when they call their witness.

01:46 THE COURT: That sounds good. Go ahead. You may call your witness.

MR. DONOVAN: Do you want him up on the witness stand?

THE COURT: Oh, yeah.

MR. DONOVAN: Okay.

01:46 THE CLERK: Please raise your right hand.

Do you solemnly swear the testimony you are about to give today is the truth, the whole truth and nothing but the truth so help you God?

THE WITNESS: I do.

01:46 THE CLERK: Please state and spell your first and last name for the record.

THE WITNESS: My name is Peyton Engel, that's P-e-y-t-o-n, E-n-g-e-l.

THE COURT: Thank you, Mr. Engel.

01:48 Go ahead, Mr. Donovan, you may proceed.

MR. DONOVAN: Thank you, Your Honor.

PEYTON ENGEL, DEFENSE WITNESS, DULY SWORN

DIRECT EXAMINATION

BY MR. DONOVAN:

01:48 Q. Good afternoon, Mr. Engel. I just want to run through a few

background questions with you. Can you state your education background?

A. I have a bachelor's degree in Russian from Grinnell College, a master's in Russian literature from the University of Wisconsin-Madison, and a JD from the University of Wisconsin-Madison.

Q. And can you do a brief overview of your work history?

A. Yes. In about 1997, I went into the field of IT networking, the bottom having fallen out of the Russian literature market. And I specialized in computer security for about 16 years. And that included doing forensic investigations and incident response.

Q. And where do you work now?

A. I currently work for a law firm in Madison, Wisconsin that's called Hurley Burish.

Q. And can you just give a brief on overview, not necessarily maybe listing everything, but some examples of your certifications and continuing education in the computer field.

A. I routinely provide training. So I speak at conferences and at trainings, for example, for the state public defender, mostly regarding how to work with computer experts, how litigators should work with computer experts.

I maintain the CISSP -- that's Certified Information -- CISSP, Certified Information Systems Security Professional certification -- which is sort of a broad or a

generalist security certification but it's, for better or worse, one of the standard ones that people obtain in the field. It includes some requirements for forensics and incident response knowledge as well.

01:59 Q. Thank you. You mentioned that you train other professionals in this area, correct?

A. Yes.

Q. And so you've spoken at different conferences?

A. Yes.

01:59 Q. And do you also have some published works?

A. Yes.

Q. Can you give an example of a few of those?

A. The most recent one was an article on cell phone forensics and that appeared in The Champion, which is the National

01:59 Association of Criminal Defense Lawyers publication.

Q. And you've testified in court before?

A. Yes.

Q. And related to, again, computer issues?

A. Yes. I've appeared as an expert witness. This is my first

02:06 venture into federal court, but I've appeared as an expert at trial and at evidentiary hearings in a number of state court proceedings.

Q. Can you give a rough estimate?

A. My affidavit actually lists some specific ones. I've

02:06 probably appeared in 10 or so, 10 or 12. And then I've been an

expert in dozens more, but those haven't gone to trial.
Q. Okay, thank you. Okay. Have you also done some prior work for law enforcement before?
A. Once in a while. The most notable incident was -- well, never been deputized or anything like that, but in the course of my work I've assisted -- the FBI was the most notable, in an industrial espionage case down in Madison.
Q. So is it fair to say you've worked on both the defense side and law enforcement?
A. Yes, though heavily more on the defense side.
Q. Correct. Okay. Okay. Can you kind of explain what a peer-to-peer network is and how it operates?
A. Sure. A peer-to-peer -- well, the standard architecture on the internet is what's called a client server architecture. You have a centralized resource, say a website or something like that, that many people want to access. And so they'll use a client piece of software like a web browser to see the web server. And that shares this one central resource among many other users.

A peer-to-peer architecture is just a different arrangement. Instead of having one central resource, resources are distributed across the network and users share and consume on an as-needed basis.
Q. And to access a peer-to-peer network you have to download like a special type of software?

A. Yes. There's usually a peer-to-peer client software involved.

Q. Can you explain what open source software would be versus not open source?

02:10 A. Sure. Software is developed by programmers. And programmers write in a computer language. So, for example, C or Java. And that language is compiled -- the C or Java code itself is not what the computer runs. It's compiled and generated into an executable program for the computer. But that

02:11 code that the programmers write is called the source code.

Closed source software means it's not publicly accessible. Open source software means that the source code is available for others to review or potentially update and modify.

Q. So would most of these peer-to-peer programs be open source

02:13 software?

A. There's a variety. There are -- so, for example, at issue in this case is BitTorrent. There are both open and closed source BitTorrent clients.

Q. Okay. Now, is it your experience and knowledge that all

02:14 software is subject to having bugs or errors or malfunctions in it?

A. Yes. This is a universal truth. I mean, not all software has tons of bugs. Some is sounder than others. But sort of the gold standard for software bug-trimming would be avionics

02:16 software. And we've just recently seen the 737 Max disasters.

So it's a certainly heavily reviewed, heavily audited code that didn't function as expected.

Q. So even commercial products like Microsoft Word or Excel or other, you know, highly common programs have bugs and errors, correct?

A. Yes. And these are systems that are wildly deployed, you know, used by many, and there's a robust system for reporting issues and, you know, having them escalated and filtered through technical support. But I still get updates from Microsoft probably twice a month.

Q. Can you explain a little bit more about like how they're addressed? So, for example, is there things called "patches" that fix errors?

A. Right. A "patch" is a term for usually a small update to a piece of software. So there are patches. And then larger things might be called "service packs." These are basically usually small executable pieces of code that are delivered and they update some aspect of a piece of software that's been deployed out in the field.

Q. Now, do most programs also go through what's called "beta testing"?

A. Yes. Generally there's a beta phase before it's sent into full production.

Q. Could you explain what a beta test would be?

A. Sure. So a beta testing happens when people think the

software is pretty much done and more or less ready to deploy. They'll deploy it in a way that generally more sophisticated users who would be good at spotting issues and good at reporting the issues, have a chance to tinker with the software and to use
02:24 it and get the hang of it before it gets a general release.
Q. Is it kind of fair to say they kind of put it through its paces before it becomes generally used?
A. That's the idea of beta testing.
Q. And just to be clear, are most beta testers outside the
02:25 entity or the company that made the software?
A. That depends on the kind of software and who the eventual user base is. Probably in the world at large, yes, but for any given project it might be different.
Q. Now, can you describe briefly what the interface would look
02:25 like on a peer-to-peer program?
A. Well, it's usually a graphical user interface these days. There's a way of searching for -- let's restrict ourselves to peer-to-peer file sharing programs. There are other things out there, but there would be an interface for searching for the
02:26 type of file you want to find.
So, for example, if I want to download the latest Star Wars movie or something like that, there would be a place to type in what I'm searching for and a place to see results and select which ones I wanted to obtain.
02:26 Q. So there would be like a search bar that you could type in

like a text search, for example?
A. Yeah. I mean, something -- something like that is present somewhere along the way. Different clients will look different, but, yes, that functionality is there in one form or another.
02:27 Q. Can users also search by hash values if they would know the hash value of the particular file that they want?
A. It would be strange for a user to even understand what a hash value is. I have no -- I mean, there's no reason the software couldn't support that, but for someone to sit and enter
02:27 a 48-digit hexadecimal numbers -- I wouldn't think most users would do that.
Q. And maybe just to make sure everyone's on the same page, can you briefly explain what a hash value is?
A. Right. So a hash value, sometimes people call it the
02:28 "digital fingerprint" of a file. So suppose you have two files and you want to know if they're the same. Rather than go and bit-by-bit compare them, you can pass them each through a certain kind of mathematical function, called a "hash function," and you obtain a number. And if those two numbers are the same,
02:28 then the chances are astronomically small that the two files are different. And so a hash value is sort of a shorthand for identifying a file or a piece of a file.
Q. Now, you've reviewed the pleadings in this case, correct?
A. Yes. At least the initial ones.
02:29 Q. Including the government's response brief --

A. Yes.

Q. -- to our motion to compel?

Now, they raise this concern about if the program's turned over that, you know, hash tags could be manipulated to change and then they'd be harder to detect. Right? Do you remember -- do you recall that?

A. I do recall that.

Q. Okay. Now, why in your opinion would that be a red-herring argument?

A. For a couple of reasons. First, I presume, but do not know, that the database of known hash values is separate from the program itself. So one could look at the program without necessarily seeing the full list of things that it looks for.

Second, the government discloses hash values every time it applies for a search warrant. You see not only the hash value of the file that they say they've obtained, but also the file name that is associated with it. So it's not that any individual hash value is that big a secret.

Third, it's possible for anyone on the internet to go ahead and change a single bit in a file today without the software having been disclosed. And that would change the hash value and it would no longer trigger the automated alerts that the Torrential Downpour software generates.

That's something that could happen today for free and without any -- you know, without any need for knowledge of the

code base.

But fourth, that would actually reduce the ability to share or at least the ease with which people are sharing contraband materials on the internet because of all the hash
02:33 value changes -- values change. Then the Torrent clients won't know how to find the software for the images or movies or whatever it is they're downloading anymore because the whole thing is premised on a shared, you know, set of hash values.

So, yes, that could happen. But it doesn't seem to me
02:34 to be either a realistic possibility or one that would -- I mean, it would actually probably cut down on the sharing of child pornography on the internet.

Q. Now, you talked earlier about source code versus the program itself, right?

02:34 A. Yes.

Q. Can you explain what concerns there might be about turning over source code?

A. So the gold standard for understanding how a piece of software works is to review the source code. You get to see
02:34 pretty much everything it's capable of. And you can then see all of the inputs that it takes and all of the ways in which it gives output and all of the logic that it operates on. So the concern there would be that by knowing that, one would know something that couldn't otherwise be known.

02:36 So, for example, from time to time, and I believe in

this case, the government raises the concern that this kind of disclosure would impede future or ongoing investigations. So I can think of a couple ways that that might happen.

One is, that we know from reading the warrants here and in other cases, that RoundUp pretends to be sharing files in order not to get kicked off the network or throttled from being able to download files.

If it were the case that RoundUp always shared the same list of files, that might be a way of recognizing RoundUp and people who wanted to avoid being tagged by it would simply hang up the phone whenever something sharing those files connected.

Another thing might be that -- and this is hypothetical. I don't know this because I haven't had access to the source code. But another thing might be that if the system is designed so that -- to prevent law enforcement in one jurisdiction from accidentally investigating other users of RoundUp in another jurisdiction, maybe there's something about the way that it establishes its connection or operates -- or interacts with the systems it's investigating that could be recognized. That would be another sort of handshake signature that you could figure out this is RoundUp connecting to me and then hang up the phone again.

That would be -- those would be two ways that I can think of that would be potentially problematic.

Q. Now, those concerns wouldn't be raised if it was just getting access to the program and not the source code, correct?

A. Well, it would be less of a concern. It would sort of depend on how the program operates and what we'd be able to observe about it.

Q. Fair enough. I understand, again, you obviously don't have access to the program so you can't say for sure.

Okay. And I just want to clarify one thing. When you say RoundUp, you're using that interchangeably with Torrential Downpour?

A. Yes. I am sorry. That's a habit that I have. The investigative software, which is RoundUp-like, which is used on BitTorrent, is called "Torrential Downpour" from what I've read.

Q. Okay. So going back to peer-to-peer network I guess architecture. So it's a decentralized network, correct?

A. Yes.

Q. And this would be to allow sharing more efficiently and faster than if it was just in a centralized network?

A. Right. So the problem that the designers were attempting to solve was, how do we exchange large files that aren't hosted at some giant file repository like a Google Docs or something like that? How do we just trade large files on the internet?

And the issue is that when we purchase a connection to the internet from our internet service provider, whether it's AT&T or Comcast or whatever it is, the connection we get is

generally what's called asymmetrical. Meaning that we can download things much faster than we can upload them. Because the people who provision those circuits realize correctly that for most people's purposes that's the right way to do it. Most
02:46 people are much more interested in downloading things than they are in uploading things.

So you might get, say, from a Spectrum, Charter Spectrum account you might get 200 megabits downstream to your house so can watch Netflix on several TVs at once, but you might
02:46 only get, you know, 30 or 50 megabits upstream. So the problem is if -- let's say you and I want to exchange a file -- well, I want to get a file from you. I'm limited. Even though I can download things with blazing speed, I'm limited to getting the file by the fastest speed that you can upload. And so that
02:49 makes things crawl to a halt, and it also means you can't be sharing multiple files at once, et cetera.

So the insight of BitTorrent is, hey, why don't we chop the files up. Why don't we have the files stored on multiple systems around the internet, or at least realize that
02:49 they are stored in multiple systems around the internet, chop them up into segments, and I can grab one segment from system A, one segment from system B, one segment from system C, and then get the benefit of my fast bandwidth by being able to download from several sources at once and you get the file faster that
02:50 way.

Q. Can you describe briefly how computers connect to the internet and maybe also discuss what an IP address is?

A. Sure. So one of the hard problems in computing in the '70s was how do we get computers to talk to each other. And what came out of this, the sort of system that emerged and towers above all others today is what's called the "internet protocol." It's a series of rules or standards by which one communicates on the internet.

02:51

And one of the challenges that it solves is how do we route a message. So let's say we have a network that spans the nation or even the world, how do I get a message from one computer to another?

02:52

And so the way this is accomplished is via IP addresses and routing protocols. But for the purposes of this conversation, every machine that is connected to the internet is assigned or associated with at least one IP address.

02:53

And when we are -- you can think of -- as the machine sends messages across the internet, you can think of this as being like the send and return addresses on a mail envelope. It has a "destination" IP address, each message does, and a "sent from" IP address. And so that when the guy at the other end of the connection gets the message, he knows where to reply to.

02:53

So IP addresses are distributed more or less geographically. So we can -- by IP address, we can draw some inferences about where a system is located in the physical world

02:54

and which internet service provider allocates it. And this is what allows investigators, when they find an IP address that they think is associated with a crime, they can get an administrative subpoena or some other mechanism that compels the
02:54 relevant internet service provider to disclose the identity of the subscriber who was using that IP address at the time.
Q. Okay. So I'd like to talk a little bit about how BitTorrent's a little different than maybe perhaps other peer-to-peer programs. So you've talked about these little
02:55 pieces of a file. Would those be called "torrents"?
A. So a torrent -- at least the way I think of it is, there's a thing called a "torrent file" which is kind of like a recipe for obtaining and assembling a given set of contents.
So, again, let's use the example of the latest Star
02:56 Wars movie. It would list the -- for each segment of the file some directions for where to find that and how to, once you've got all the segments, how to assemble that into the finished product.
Q. And then -- so a torrent is basically a map that then helps
02:57 the computer receiving these different pieces to assemble them, correct?
A. Right. It tells you -- it's kinda like a recipe. It tells you what ingredients to get and how to put them together.
Q. Okay. And, again, BitTorrent is decentralized? There's no
02:57 central server or hierarchy, correct?

A. Yes.
Q. Okay. I'd like to talk now about Torrential Downpour, or what you call RoundUp, and how it modifies the normal BitTorrent program. Okay? So first off, Torrential Downpour is not open
02:58 source, correct?
A. Correct. The source code is secret.
Q. So, not publicly available from any other source, right?
A. Correct.
Q. Do you know anything about I guess the origin or who created
02:58 these programs?
A. There are publications available, some of them authored by the gentleman at the prosecution table, that describe its creation. It's a collaboration between law enforcement and some computer scientists.
02:59 Q. Okay.
A. I couldn't name them right off the top of my head.
Q. And that's fine. I'm not asking you to name them.
There's certain things we do know about Torrential Downpour that is different than the normal BitTorrent program,
02:59 correct?
A. Yes.
Q. Okay. Is one of the differences what's called single source downloading?
A. Yes. As I described earlier, the goal of BitTorrent was to
02:59 allow people to obtain files in pieces from multiple sources.

That was the point of it.

For law enforcement purposes, though, in order to prove that a user has the entirety of one file, it's necessary to get all of the segments from that one target computer. So
03:00 one of the things that RoundUp is designed to do is obtain an entire download from a single source.

So it's speaking the BitTorrent protocol, but doing so in a way that sort of subverts the purpose of it. It's not breaking any rules, but it's definitely doing something out of
03:01 the ordinary and deviating from the BitTorrent standard.

Q. And again, this isn't something a normal BitTorrent user would do or how it would operate.

A. It's not something a normal BitTorrent user would probably want to do, since it just makes things go more slowly. But,
03:01 yes, standard BitTorrent software would not be capable of doing this.

Q. Now, you mentioned earlier that it also might basically fake file share so it doesn't get throttled down on the network. Can you explain that a little bit more?

03:02 A. So one of the things that people quickly discovered when the BitTorrent standard was first developed is that people would do what's called "leaching." They would come and download a bunch of stuff, but they wouldn't be sharing anything. So they would be consuming BitTorrent resources but not contributing back.

03:02 So various efforts were made to force people to share

at least what they had downloaded, and maybe other things as well, so that they weren't just a drag on the network; so that they're contributing.

And so what you see is clients that aren't sharing anything won't get preferential treatment in terms of downloads. They won't get necessarily access. Their ability to download will be throttled.

Q. And why would law enforcement not want to be participating in the sharing?

A. Well, there are a couple of reasons. One would be, they don't want to commit any crimes.

The other one -- I mean, that's probably the major one. But they probably also want to appear as though at least from time to time they are sharing contraband because then they'll get more interesting connections inbound to them.

Q. And do you have any I guess speculation on how they could hold themselves out as sharing when they're not, in fact, sharing?

A. Oh, you simply respond to search queries saying, yeah, I've got this or -- you know, I don't know the exact dimensions of the protocol that they're speaking. You know, I don't know exactly what messages they're sending, but they can advertise what they've got.

Q. Now, another difference is, does Torrential Downpour run automatically?

A. Yes. We've learned -- well, automatically. Presumably a user launches it initially. So it's maybe not fully automated. But once it's on, it just sits and runs. It runs around the clock, unattended.

03:13 Q. And do we know how that actually is carried out or what means are used to do that, or is that something, again, that you don't know?

A. I mean, I presume, without firsthand knowledge, that it just sits in a lab somewhere and runs. It gets set up and launched

03:14 like any other process and it's left running and then people check on it from time to time to see what it's found.

Q. Okay. Does Torrential Downpour also generate special data logs?

A. Yes, it does.

03:14 Q. Now, how would we judge the reliability of those logs that's generated by the same program that we don't have access to?

A. I -- well, without access I have no objective way of judging the accuracy of the logs.

So, for example, I've seen log files and they

03:15 oftentimes will describe events that can be verified via other means; for example, in the context of a criminal case.

But what we don't know -- there's sort of confirmation bias here. What we don't know is how many log files are generated that don't result in prosecutions, or how many

03:15 warrants are executed that don't result -- based on those log

files that don't result in prosecutions. We don't have access to that information so there's -- we don't have a way of evaluating whether the system is accurate in general or not.

Q. Does this kind of maybe implicate that you'd have a false positive? Is there -- can you describe what a false positive might be in computer --

A. Sure. In testing -- in general, any time you have a test to look for a condition, there are two kinds of errors that you are worried about. One is a false positive result. In other words, the system, whatever it may be, falsely reports the condition exists. The other one is a false negative. The condition falsely reports -- or, I'm sorry, the test falsely reports that the condition does not exist.

And these are things which are tracked very carefully. For example, in medical testing, you know, you have a test which is 99 percent accurate for finding this kind of cancer. What they mean is there's 1 percent that they're getting either false positives or false negatives and, you know, giving a misdiagnosis potentially on that basis.

So here as well we know of times when the system has given positive alerts, but we only know the ones that resulted in prosecutions. So we don't know the false-positive rate or the false-negative rate of Torrential Downpour.

Q. And the logs themselves again don't shed any light on that, correct?

A. Right. They -- they report what the software reported. They're a record of what the software reported.

And there's -- the logs themselves, you know, purport to be accurate records of events that the software engaged in, but we have no way -- or at least I have no way of verifying their accuracy.

Other than, I will say, from time to time there are events in a log that can actually be correlated with records of events elsewhere or other sources of information.

Q. Well, let's talk about this case. So, for example, one way that this supposed single-source download could have been verified was that the image that the program said it downloaded was found later on Mr. Owens' computer, correct?

A. Correct.

Q. And in this case did that happen?

A. There was -- to my recollection there was an image that the Torrential Downpour reported a single source download of and that image was not found on any of the media seized.

Q. Is another difference between Torrential Downpour and the public version of the program is that Torrential Downpour can get information from target computers like, for example, the version that's being run of the program?

A. Torrential Downpour is a BitTorrent client in the sense that it speaks the BitTorrent protocol, but it's really a surveillance tool. It's designed for gathering information to

be used in prosecution, and so it makes records of all kinds of information that would be of no interest to the average BitTorrent user: IP addresses, software versions, segments of files and so forth.

03:25 All of that information is used to a greater or lesser extent by a BitTorrent client, but it's not exposed to the user. The user has no knowledge of it. The user just says, "ah, my file got here" and is happy with that.

So that's -- that's a difference between Torrential 03:25 Downpour and other BitTorrent software, is that the other BitTorrent software is designed for transferring files, Torrential Downpour is designed for supporting interdiction.

Q. Okay. Is there any other I guess major differences you're aware of that Torrential Downpour might have that the public 03:25 program doesn't?

A. I don't believe it's an issue in this case, but I have from time to time in warrant applications seen statements to the effect that Torrential Downpour is capable of tagging a target system.

03:30 So one of the other problems that can happen is in say a home network there might be multiple devices, tablets, phones, computers, these days thermostats, alarm systems, et cetera, that all use the internet for communications. And so one of the problems is, well, how do we know which of these devices was the 03:31 one that was on the BitTorrent network?

And so presumably this involves the placement in a log file somewhere of some piece of information that would be uniquely identifying the system as this is the one to which law enforcement connected. But I'm not aware of that being in play in this case.

Q. Would a tag, if it was placed on a target computer, possibly be in a nonshared portion of the target computer?

A. It would possibly be there, yes. I don't know the exact mechanism of tagging. But like I said, I assume it's probably in a log file somewhere.

Q. And again, without access to the program it's impossible to say.

A. A tag might be discernible, but, yes, it would be much easier to figure it out if we had access to the program.

Q. Okay. Okay. So, now, in this case you were hired by me, correct?

A. Correct.

Q. And you reviewed all the digital evidence that was made available by law enforcement.

A. Yes.

Q. And so did that include a mirror-image of the computer hard drive --

A. Yes.

Q. -- that was seized from the search warrant?

A. It did.

Q. And also was there several thumb drives?
A. Yes.
Q. Okay. And again, you also reviewed I think you said the pleadings, like the indictment?
03:33 A. Yes.
Q. And also the police reports.
A. Yes.
Q. And the search warrant, correct?
A. Yes.
03:33 Q. Okay. Now, after you reviewed all of this material did you have several questions that caused you concern?
A. One that I recall was that at least some of the single source downloads seemed to happen quite quickly. It's not rare to see single source downloads or logs of single source
03:34 downloads -- I've never seen the single source download itself -- but Torrential Downpour logs that describe single downloads that take hours, or even maybe span more than a day.
Here at least some of them -- and I don't recall the exact timeframes without refreshing my recollection, but some of
03:36 them were quite quick, on the order of less than a minute or maybe even seconds.
Q. And why would that be unusual?
A. Well, again, the nature of the single source download is that because you're downloading from a single source, you are
03:39 subject to whatever the upstream bandwidth limitations of that

source are. So that's why it sometimes takes a while to get files, because you're pulling it from a system that's only uploading very efficiently. It's maybe not the only consumer of that upstream bandwidth and, in any case, it's limited by that pipe size.

Q. Was another one of your concerns about what the search warrant meant when it said that law enforcement's investigative focus was directed to Mr. Owens' IP address?

A. Right. So search warrant applications derived from Torrential Downpour information are generally worded pretty obliquely, I assume in order to avoid divulging sensitive information about the software.

So I don't have any idea what it means to turn one's investigative focus, what actions that implies. I mean, presumably at any point in an investigation one's focus is somewhere, but I don't know what it means to turn one's investigative focus towards a certain IP address. I mean, obviously it means I've seen an alert and so I'm taking an interest in the IP address, but I don't know what actions the investigator takes.

I also don't know concretely, you know, in technical terms what it means to be associated with a certain hash value. That would be another -- you know, we just don't know precisely what it is that Torrential Downpour is basing its alerts on. We know the kind of stuff it is, but not exactly what.

Q. And, again, to be clear, this could have been the program by itself running automated that, you know, focused its investigation or, you know, thought that this target computer was associated with a torrent, not necessarily a person sitting there looking over it, correct?

A. Yeah. Based on what I have read in this case and in others, I think it's rare for someone to just sit there watching Torrential Downpour. What happens is they get a bunch of -- they come back in the morning, probably see a bunch of log files and then start digging on those.

Q. So in a sense, as far as the actual transactions that occur between Torrential Downpour and the remote client or the target computer, would it be fair to say that really the program's the only witness to what happened at that point.

A. Yeah, I think that's a good analogy. The process of identifying IP addresses in the language of the warrant associated with a piece of contraband and conducting the single source download is probably entirely automated and, you know, was done unattended by a human.

Q. Could the term "associated with a torrent" just means that the target computer says, hey, I have this torrent or this map to a file and not necessarily the file itself?

A. I assume it means either I have it or I want it, and I don't know for sure which.

Q. But, again, could it be that it doesn't necessarily have the

file; it's just saying that it has the information or the request for the file?

A. Oh, certainly. It might even be a false statement.

It's possible to imagine that someone, for example, Torrential Downpour might untruthfully advertise what they have.

Q. Okay. Did you also have concerns when the search warrant said that Mr. Owens' computer connected to law enforcement's computer and what that might mean?

A. Yeah, I would be curious to know exactly what that means and what caused it to do so.

Q. Okay.

MR. DONOVAN: And, Judge, I'm getting towards the end of my questions for Mr. Engel.

BY MR. DONOVAN:

Q. So I guess I'd like to kinda conclude with, you know, why you feel you need access to Torrential Downpour to answer all these questions or to answer some of these concerns in the case.

So would it be fair to say that you need access to the program to confirm whether Torrential Downpour actually conducted a single source download the way that it says it does?

A. Right. I don't think -- I mean, the time of that particular single source download has come and gone. But I don't have any way to verify how reliably Torrential Downpour conducts single source downloads. So that would be one of the things that I would want to observe is sort of, in a controlled environment,

does it reliably get all of a file from a single source when it reports that it's doing so.

Q. And this would be important because whether or not the entire file came from Mr. Owens' computer versus from multiple computers, would obviously bear on his intent or his knowledge of what occurred, correct?

A. I don't know so much knowledge as just actual possession. If someone has a piece of a file, that's different from having the whole file.

Q. And, again, that's, again, also maybe different from having just the torrent for the file.

A. Correct.

Q. Okay. Because, again, normal peer-to-peer protocol would be a download from multiple sources, not just one. So that would be pretty crucial to try to figure out.

A. Right. So presumably the authors of Torrential Downpour overrode that default behavior of the BitTorrent software. And the question is, did they do a perfect job of that or not.

Q. Okay. Are you also interested in knowing what network traffic is monitored to identify potential target computers?

A. Yes. I would be interested to know the specific sorts of messages that Torrential Downpour inspects.

We know that it discriminates between network messages that involve hash values that are related to contraband. In order to do that, it's gotta be looking at the pool of messages

in general and then it alerts on the ones that are presumably -- their hash values are in a database of known bad files.

But, so it's -- effectively it's looking at all of the traffic and then discriminating. It's only alerting on some of it.

Q. So correct me if I'm wrong, but it sounds like it could be doing like a dragnet search of all traffic across a peer-to-peer network, at least in maybe a certain geographic area, to then narrow down to what it thinks is contraband images or videos?

A. Right. In order to discriminate between contraband and noncontraband, it has to get all of the messages. It doesn't see all of the BitTorrent traffic in the entire world, but it certainly sees whatever is in its neighborhood and what it -- you know, whatever its peers are interacting with. And it then sifts through that to look for ones that are, you know, potentially bad.

Q. And this could maybe be important, for example, for raising Fourth Amendment concerns?

A. Well, one interesting question is, okay, there's this database of -- of known hash values. How do things get -- what's the process for adding things to that database? How rigorously are they vetted? Is the database --

I mean, it's also easily possible to imagine this database being used for discovering things other than child pornography. You could use it to look for hashes that are

associated with, say, recipes for bombs or things like that. It's not just a -- it's a Swiss army knife tool in the right hands.

And so, I mean, I'm not a criminal law practitioner so
03:57 I'll leave the Fourth Amendment arguing to you, but, yes, it seems to me that this is -- the fact that it looks at both legitimate and non-legitimate traffic in order to figure out what the non-legitimate traffic is, you know, that is -- that seems invasive to me. But, again, I'm -- that's not the part
03:58 I'm an expert on.

Q. Now, you also want to -- and we've talked about this a little bit already with the false positives, but you want to be able to have access to the program to test its accuracy and reliability in how it carries out its methods, correct?

03:58 A. Correct.

Q. All right. And this would be important because every software program has certain parameters and instructions that should be followed to make sure it's being used correctly.

A. Right. So the analogy I would make here is to say a radar
03:58 gun or a breathalyzer. These are tools that are used to establish probable cause to charge people with crimes or at least ordinance violations. And, but we know that they have to be calibrated a certain way and they have to be used correctly. And so defense attorneys routinely verify that that has been
03:59 done. You know, it is a defense in many cases if the equipment

was not operated correctly.

And we have no way of knowing what questions to even ask here, because we don't know how the software is set up, how the software is installed, what the correct way of operating the software is. Those are all things that are opaque to us. And so we don't have any way of evaluating or even properly questioning a prosecution witness about whether that took place in this case or not.

Q. Could you just describe briefly for the Court, if you were able to get access to the program, like what are some of the things that you might try to do or try to -- you know, what kind of tests might you run?

A. Well, one of them would be just what's called packet capturing or packet sniffing. I would attempt to watch from a nearby place on the network a single source download and see if indeed it all came from a single source. Probably do that a few times just to verify that it doesn't every so often grab a piece from elsewhere.

I would also watch when the software generates an alert what traffic caused it to do that. That would -- those would be things that would help me understand what it's doing under the hood. And that's kind of the goal here.

Q. Now, would it matter where you did this testing or review, whether it was at, you know, your own facility, your office versus perhaps in a law enforcement office?

A. I have no, you know -- it would be more convenient at my office, but I have no, you know, principled objection to doing it elsewhere.

I would say that if it were at another facility, I'd probably want to schedule more than one visit because I assume I would spend a fair amount of time getting up to speed on just what -- how I would do the tests there. You know, what's available to me in terms of network ports or, you know, power outlets, you know, sort of mundane things like that. Also, just learning how to -- I've never seen the software. I don't know what it looks like. I don't know the first thing about how to launch it or do anything like that. So I'd need a little time to just get oriented, and then I'd also need time to do the tests.

So doing it at my leisure at my own facility would make that easier, but it's not impossible to do it elsewhere. I'd just need the requisite degree of access.

Q. Now, would you view it as a problem if this was done pursuant to a protective order where you can't disseminate or discuss or otherwise disclose the program to anybody else except for me?

A. No, I believe we've even proposed that.

Q. So you would obviously -- I mean, you're a practicing lawyer in Wisconsin, correct?

A. I am.

Q. You value your law license. You wouldn't do anything to violate an order, right?
A. I'd do my best to avoid that.
Q. Okay. Another reason that you might want access to the
04:03 program would be, again, to ensure that it -- when it identifies a computer as flagged for possessing a torrent, okay? That that is maybe different than an actual child pornography image or video, right?
A. Right. Now, this would be probably a dicey thing to test,
04:03 since I don't possess any child pornography and have no intention of doing so, so we'd probably have to set up some way of having a known, you know, safe file, you know, some dummy file that we could pretend was something, you know, that Torrential Downpour would alert on. So we'd want to see when
04:04 that file gets shared what is it that triggers Torrential Downpour to alert and do the log entries that it creates accurately reflect the condition that was present on the network.
Q. You mentioned earlier, but I just want to maybe clarify this
04:04 a little bit more. So it's virtually impossible for us as the defense to prepare any sort of cross-examination of government witnesses about how this program is used or whether it was used correctly or within the right parameters, right?
A. The best we have right now is what's in warrant applications
04:04 and then a few inferences we can draw from there.

There's a little bit of literature, you know, presentations that one can download, but there's really not much -- we don't have access to documentation about the system. We certainly don't have the source code. No one outside of law enforcement to my knowledge has seen a working copy of the software.

We get conceptually what it is, and we understand that a system could be built to do what it claims it does, we just have no way of verifying it. And that makes it hard to know what questions to ask, again, about whether the system was properly installed, was it properly operated, what network environment does it require in order to function correctly, did it have that at the time. These are all questions we don't -- since we don't know information about the guts of the system, we don't know what questions to ask. And we could ask a question, but we wouldn't know whether the answer was helpful or not.

Q. So would it be fair to say that your opinion is we are basically at the mercy of the government right now of what they say it does and doesn't do without independently verifying it?

A. Very much so. The -- we have nothing -- we just are -- we either take on faith what's in the warrant application or we don't.

Q. And so there's really been no -- again, as far as you're aware, and this is anywhere in the country -- any adversarial testing of this program.

A. I am not aware of any. There are a couple of competitors to Torrential Downpour also which are closely guarded. I'm aware of efforts in various courtrooms to get varying degrees of access to Torrential Downpour and other systems. I'm unaware of someone getting unrestricted access to do just sort of thorough testing.

Q. And lastly, would it be important to gain access to the program so that we can perhaps try to figure out why the file that the program said it downloaded twice over the course of two different days is not located on Mr. Owens' computer?

A. Well, what we could do -- I mean, we know that the program said it downloaded those things, and we know that the file was not present at the time when the computer was seized. We can think of a variety of explanations for why that might be the case. Inspecting the software would help us evaluate sort of which inferences are more plausible versus less plausible.

MR. DONOVAN: Your Honor, I believe I'm done. If I could just check my notes for a quick minute here to see if I missed anything.

(Brief pause.)

MR. DONOVAN: Your Honor, I have no further questions.

THE COURT: Okay. Mr. Humble?

CROSS-EXAMINATION

BY MR. HUMBLE:

Q. Mr. Engel, you mentioned your background and training. Have

you had any or received any training in BitTorrent file sharing for the networks?

A. Other than experiential testing, no.

Q. Okay. And you also mentioned that it sounds like what you learned you learned from reading the literature and also doing?

A. Yes. For better or worse, people of my vintage typically the courses weren't available at the time when we needed to learn things, so we had to just go do it.

Q. Okay. And you mentioned that some of the literature upon which you relied to teach yourself was authored by this gentleman sitting next to me; is that correct?

A. Yes. You have next to you one of the probably half dozen people in the world who knows most about the software.

Q. Okay. So if he helped teach you about what you know about BitTorrent, do you have reason to trust his -- distrust his expertise in this area with regard to BitTorrent Torrential Downpour or Torrential Downpour Receptor?

A. Curious question. I don't distrust him. No, I have no reason to distrust him. I mean, I don't think he's trying to fool anybody. I just don't have any objective way of verifying any of the facts in this case.

Q. But, again, what you've learned about this essentially, at least in part, you've learned from this gentleman. So you would rely on his expertise in what you're testifying to here today essentially.

A. In part, yes.
Q. And you referred to this in your -- in your affidavit as "RoundUp" and you clarified "Torrential Downpour." It's actually Torrential Downpour Receptor, were you aware of that?
04:15 A. I'm aware of that term as well.
Q. Can you tell the Court the difference between Torrential Downpour and Torrential Downpour Receptor?
A. Not with specificity I cannot.
Q. Okay. And when you had the opportunity to review the logs
04:15 and the imaging of the computer, you said that you never found this image that is alleged in the indictment; is that correct?
A. That image as far as I could tell was not present on the computer.
Q. And I said "image" and earlier you said "image," but
04:15 actually, more correctly, it's a movie.
A. Yes. Yes.
Q. Okay. So you didn't find this movie, but you did review the logs, correct?
A. Yes.
04:15 Q. And those logs did reflect that I believe there were 226 portions that made up the movie for lack -- I say "portions" for lack of a better term?
A. I'm taking your word for the number 226. But, yes, the movie was reflected in the logs.
04:17 Q. And this will probably be an exhibit soon, but this log

essentially shows all 226 portions of that movie are going into the computer of Mr. Owens; is that correct?

A. That log is a document that speaks for itself. I don't have a way of assessing its accuracy, but it has entries that appear to be what you describe.

Q. Do you have a way of proving inaccuracies in the log?

A. No.

Q. Okay. With regard to your review of the logs and the mirror imaging of Mr. Owens's computer, did you find evidence that that movie had been on Mr. Owens's computer?

A. I saw an indication that it may have been there, yes.

Q. And did you find indications that that particular movie with that particular hash value may have actually been on Mr. Owens's computer at different times throughout 2018, 2016, 2017?

A. I don't believe -- or at least I don't recall, sitting here today, seeing anything that gave me a sense of the time at which it may or may not have been there. I did find a reference to the file name, but that's all I recall finding.

Q. Okay. And in looking at, again, the evidence, the computer, the forensic evidence, were you able to establish essentially any evidence -- or did you observe any evidence that the file had been there prior to Mr. Owens's computer connecting with law enforcement?

A. Again, I don't recall what I saw being associated with a time. So I'm not -- one can always imagine a forensic analyst

smarter than oneself, so I'm not saying that there was definitively no such evidence. I just -- what I recall was seeing a reference to the file name and I did not recall that having any kind of timestamp on it.

04:19 Q. And in reviewing that information did you -- well, I'll just ask you: Do you know what program Mr. Owens used to establish peer-to-peer communication?

A. It's in my notes, but I don't recall if it was Micro-Torrent or what.

04:22 Q. Okay. And did you see any evidence when you were reviewing the forensic materials that Mr. Owens had downloaded a peer-to-peer program very close in time to when he connected with law enforcement?

A. There was peer-to-peer software installed. That would have

04:22 had a timestamp on it. I don't recall sitting here right now the proximity. I could refresh my recollection and I would -- I don't -- I don't have any reason to dispute it.

Q. Do you recall in reviewing that information that that particular movie with its 226 portions was -- that there was

04:23 evidence that it was on Mr. Owens's computer after he established contact with law enforcement?

A. Again, the evidence I saw for the existence of that file, I don't recall any time data associated with it. So, no, I don't. All I saw was the file name.

04:23 Q. Well, let me ask you this. If -- if there was evidence that

this particular movie was on Mr. Owens's computer prior to connecting with law enforcement, and there was -- and I'm just asking you to go with the question -- and there was evidence that this particular movie was on Mr. Owens's computer after
04:23 connecting with law enforcement, would that be pretty good evidence that that particular movie had been on Mr. Owens's computer?

A. If there was -- if there was evidence that the file was present before connecting with law enforcement and evidence that
04:23 the file was connected -- was present after connecting to law enforcement, would I infer that the file was present?

Q. Yes.

A. Yes. If the file was present it was present.

Q. So people can delete files, correct?

04:24 A. Correct.

Q. And you've been on other child pornography cases. You've testified you've done the research, looked at the forensics, correct?

A. Yes.

04:24 Q. Have you seen other instances where individuals who have contraband or child pornography have deleted the images after viewing them?

A. I have seen instances --

Well, let me answer it -- a two-part answer to that.
04:24 The short answer is, of course, people delete files from time to

time. And sometimes you'll find traces of files in unallocated space and those are presumably deleted files.

I am also aware of times when, as here, in the warrant application there's a report of a single source download of a file and we don't find it present on the target system when we go to analyze it. I don't know why that is. Deletion is one possible explanation, but another one would be a false positive.

Q. This is going to come across very crude, because it is crude, but it's a term that you may be familiar with and I'm going to ask you: Have you -- are you familiar with the term "pump and dump"?

A. No, I'm not.

Q. Not with regard to child pornography or the downloading of child pornography?

A. That is -- that's not one I've encountered.

Q. Okay. In reviewing the forensic evidence here in this particular case, was there a question in your mind that it was Mr. Owens's computer who initiated contact with law enforcement?

A. I don't know of a way from the forensic image to determine that. So it wasn't a question I particularly investigated because I had no idea how to investigate it.

So I -- I'm not sure what would cause a computer to connect to a law enforcement computer just in the abstract. So in that sense I wonder about it, but it was not something that I investigated.

Q. Are you familiar with the term "seeding"?
A. Yes.
Q. Could you describe for the Court what seeding is?
A. In broad terms it's advertising the presence of files so
04:27 that you can -- you're participating in the network and people
know that you've got either whole files or at least segments of
files that others might want.
Q. And seeding essentially -- well, sometimes, if not most
times, seeding is done by someone who already possesses an image
04:27 or a movie; isn't that correct?
A. My understanding -- yes. Yes, that's correct.
THE COURT: This is s-e-e-d-i-n-g?
MR. HUMBLE: Yes. Seeding as in -- S, yeah.
THE COURT: As in lawn seed.
04:27 MR. HUMBLE: Yes, correct.
BY MR. HUMBLE:
Q. So that seems counterintuitive. If someone already has the
movie, why are they offering it out to the world?
A. That's sort of the economic principle that's central to
04:27 BitTorrent. What one downloads one ought to offer for sharing.
And that's sort of how the BitTorrent network maintains itself
as an efficient distributor of files.
Q. So essentially that almost certainly is why the term is
called seeding. So you just keep distributing and distributing
04:28 and distributing because you're hoping it's going to come back

to you.
A. Not the same file, but --
Q. Not the same file, correct.
A. Yes.
04:28 Q. Same genre.
A. Well, genre even -- I think it's just bandwidth. I don't know that it discriminates by subject matter so much as just if you're not offering things, then you're kind of a jerk user of the system and you shouldn't get the benefit of it.
04:28 Q. Okay. And what is swarming?
A. Swarming is another feature of -- I think it was first in Gnutella. It's a way of boosting the performance of downloads of certain files. I'm afraid, sitting here right now, I can't go into much more detail than that. I don't recall exactly how
04:29 swarming works on BitTorrent.
MR. HUMBLE: I don't have any further questions, Your Honor.
THE COURT: Mr. Donovan?
MR. DONOVAN: Just a couple follow-up, Your Honor.
04:29 REDIRECT EXAMINATION
BY MR. DONOVAN:
Q. So, Mr. Humble asked you about how part of your knowledge and expertise of BitTorrent is based on the government's witness, correct?
04:29 A. Or documents authored by him. I've never met him before

today.

Q. Correct, I'm sorry. To be more precise, documents authored by him.

A. Yes.

04:29 Q. And again, I just wanted to clarify, there is no independent access to this program.

A. That's correct.

Q. And so anything that's known about this program is either what is chosen to be shared by its authors, including the

04:30 government witness, or that comes out through litigation.

A. Yes.

Q. Like, for example, in case decisions or, you know, opinions and orders, things like that.

A. Yes. And one can glean tidbits here and there from things

04:30 like warrant applications.

Q. So I guess my question -- you might be -- you know, where else could you go to learn about this? Other than perhaps publications by the government witness.

A. If I knew of another place I'd go there.

04:30 Q. Okay. The government asked you questions about whether you have any reason to doubt that the logs are inaccurate. Okay?

Again, why can't you assess the logs separate from the program?

A. Well, the log is just a text file. Sitting at my computer

04:31 with a Notepad application, I can make a text file that says

darned near anything. I don't think the government is generating false text files. That's not -- I'm not that much of a conspiracy theorist. But it seems to me antithetical to the idea of criminal defense that we should just take it at face
04:31 value. It seems that we should be able to do some investigation of the degree to which it accurately reflects the events that it's reported.

Q. Would it be fair to say that if there's problems within the program itself then there might be problems within the logs
04:31 themself?

A. Right. That's the old "computer garbage in/garbage out" theory. If the software does not function as designed, then there's no reason to expect that the logs would be better than the program itself.

04:32 Q. You testified that again you reviewed the forensic evidence available in this case personally.

A. Yes.

Q. And you found indications of perhaps the file name of the movie that was supposedly downloaded on Mr. Owens' computer.

04:32 A. Correct.

Q. But no actual file.

A. Correct.

Q. And I apologize, I forget, did you find any indications of a hash for that movie?

04:32 A. I did not.

Q. Okay. Now, part of these peer-to-peer programs would be, again, a search function where like a term could be entered, correct?
A. Yes.
04:32 Q. And so would that be part of a Torrent? So like could a search term or a function be part of a Torrent that might be on the computer? Meaning that, you know, it might say it's looking for or has information on it but, again, doesn't have the file itself?
04:33 A. Yes. One can find, for example, Torrent files on a computer, but not the -- not the movies or images or whatever that the torrent files would enable you to acquire.
Q. Okay. And so, again, you said one explanation could be, as you acknowledged, that the user deleted the file, right?
04:33 A. Yes.
Q. But another explanation could be, again, this idea of a false positive that perhaps Torrential Downpour reporting a single source download was just wrong; that there -- you know, it reports a download, but there never was a file there to
04:34 download from.
A. Correct.
Q. Okay.
MR. DONOVAN: I don't have any other questions, Your Honor.
04:34 THE COURT: Okay. Thank you, Mr. Engel. You can step

down.

(Witness excused at 2:44 p.m.)

THE COURT: How about a short break. Do you have -- I mean, are we in a rush because a witness has to catch something or get out of here or --

04:34

MR. ERDELY: 6:45.

MR. HUMBLE: We've got some time, Your Honor.

THE COURT: 6:45?

MR. HUMBLE: It's Green Bay, we can get him over there.

04:34

THE COURT: 20 minutes.

(Recess taken at 2:45 p.m., until 2:58 p.m.)

THE CLERK: Please raise your right hand.

Do you solemnly swear the testimony you are about to give is the truth, the whole truth and nothing but the truth so help you God?

07:17

THE WITNESS: I do.

THE COURT: Please state and spell your first and last name for the record.

THE WITNESS: Robert Erdely, E-r-d-e-l-y.

07:17

THE COURT: Thank you, Mr. Erdely.

Go ahead, Mr. Humble, you may proceed.

MR. HUMBLE: Thank you. May I approach the witness, Your Honor?

THE COURT: You may.

07:18

ROBERT ERDELY, GOVERNMENT WITNESS, DULY SWORN

DIRECT EXAMINATION

BY MR. HUMBLE:

Q. Mr. Erdely, I'm just going to hand you what's been marked as
07:18 Exhibit 1, can you just tell me what that is?

A. It's a copy of my CV.

(TRANSCRIBER NOTE: Mr. Humble not near a microphone.)

Q. [Indiscernible]?

A. I did.

07:19 MR. HUMBLE: [Indiscernible].

MR. DONOVAN: No objection.

THE COURT: 1 is received.

(Exhibit 1 received in evidence.)

BY MR. HUMBLE:

07:19 Q. If you could go ahead and just inform the Court, what is your background, who is your employer, how long have you been employed, that kind of thing?

A. I worked for the Pennsylvania State Police until I retired in 2012. The last five years of that career I supervised the
07:20 Computer Crime Unit. And it was during my time with Computer Crime Unit that I worked on the development of these tools with the University.

And, April 2012 I retired and the very next day I started with the Indiana County Detectives Bureau where I kept
07:20 the same role — computer crime investigations, which is both the

investigative piece and the forensic analysis piece.

So as part of that and my time with Computer Crime Unit, I went through various trainings, conferences and such where I was able to acquire professional certifications. For
07:21 instance, the CISSP certification the defense expert was speaking of, I obtained that.

I'm a Microsoft certified systems engineer, a Cisco certified networking professional.

I went through the certification process for four --
07:25 four different certification processes for computer forensics. And, again, just the ongoing training day to day.

As it relates to peer-to-peer, much of my training came from the University, the researchers, the professors and Ph.D.'s that did the research into the network so I could learn
07:26 exactly how it operates.

Q. Okay. Just total, how many years have you been dealing in investigating computer crimes?

A. I started with the Computer Crime Unit October 1998 to present.

07:26 Q. Okay. And is it fair to say that now you split your time between investigations and training and testifying?

A. Correct. I do trainings for the Internet Crimes Against Children Task Force, for the FBI's Violent Crimes Task Force, their international task force. I've done a training for
07:27 Interpol and various different countries. I provided this

technology beyond the United States.

Q. So as you say, you've trained on BitTorrent and the investigative use of BitTorrent in other countries. How many countries use this investigative Torrential Downpour?

07:28 A. We last checked, over 60 countries used our investigative systems.

Q. And if you could just kind of describe for the judge when -- in defense affidavit and probably in your resume, it references Amherst is where this particular software was developed. Sounds

07:28 like you were in on the ground floor. Can you explain that to the Court?

A. Yes. Initially there was research done by a professor from University of Massachusetts Amherst, and a professor from Georgetown University. That was the initial discussions as to

07:29 where we move next as law enforcement for investigations.

After that, I worked, you know, day in and day out with the senior programmer at University of Massachusetts Amherst where we did the development of the software.

Q. So you didn't author the software.

07:29 A. No. I was part -- the development team was myself and the senior programmer from UMass.

There's a lot of back-end work that relate to other aspects and other networks that we investigate that I programmed in that area. I'm a Microsoft data -- Certified Database

07:29 Administrator, so I work with the databases and things like

that, as well as the actual individual testing of the software before it's deployed.

Q. Okay. So fair to say you're very familiar with Torrential Downpour.

07:30 A. Yes.

Q. Okay. And Torrential Downpour Receptor?

A. Yes, sir. Those are two separate programs. And this case relates to one, which is Torrential Downpour Receptor, specifically version 1.50.

07:30 Q. Okay. We've heard about the basics of BitTorrent from the defense expert. Is there anything that you want to clarify or put a little more focus on for the Court with regard to how that operates?

A. Just quickly a high-level -- I just want to make sure the

07:31 Court has a good understanding as to how things worked.

BitTorrent is different as was already described. One of the major differences is that the torrent file that we've heard about is a set of instructions on how to get the actual files that they describe.

07:31 Well, you have to search outside websites or get them from other people. The BitTorrent software, although it gives you a mechanism to type and search as described, I just wanted to clarify the BitTorrent file sharing network doesn't have a searching component built in. When I type in the little search

07:32 field in this program, which is my BitTorrent software,

typically what happens is a web browser just pops up and starts giving you your search results. Well, you could have skipped that whole step and just went to your web browser, opened up Google, and started searching that way.

07:32 So I just wanted to be clear that there is no mechanism to search by file name within the BitTorrent file sharing network. So that was a little bit different.

The second -- so after I get the instructions I search the internet and I find a torrent file that describes the

07:33 content I'm looking for. Then you load that torrent --

Q. Can I just stop you there?

A. Yes.

Q. We're talking in the abstract. What might one put into this to find the type of movie or image they are looking for?

07:33 A. "Jurassic Park movie torrent."

Q. Okay.

A. If I just use those four key words I would be presented with lots of sites that have these instruction files, these torrent files that would enable me to download Jurassic World or any of

07:34 the other new movies that are out there. But you have to start by finding these instructions outside of the BitTorrent file sharing network is my point.

Q. Okay. So now I found these websites, and I'm assuming the same holds for erotica or child pornography or any type of other

07:34 file?

A. Yes, sir.

Q. I found this, I found what I want, how do I go about getting it with the BitTorrent?

A. So now what happens is you load that torrent file into your
07:34 BitTorrent program. Much like if you wanted to open up a Word document. You can either double-click it and it will launch the program and load the Word file you were trying to view. Well, with BitTorrent it's similar, I can double-click the torrent file and, assuming there's an association between those two, it
07:35 just opens up my BitTorrent program and starts working.

Or you could have it already open and choose the drop-down file, open, and you just navigate to that torrent file which are the instructions. But in either case, once the torrent file, the instruction gets loaded into the program,
07:35 searching does happen. And what searching happens is, that now my computer, running a BitTorrent piece of software that has instructions loaded, it goes out to the BitTorrent network.

There's indexing that happens. So the BitTorrent network keeps track of who is associated with which torrent.
07:36 Because if I load a torrent, I need to find other people that have some or all of that material to share with me. I just started, I have nothing to share.

So the BitTorrent network does that all by itself. And it's just a search for a torrent that I've now loaded into
07:36 my program which is different than initially finding that

torrent. They are two separate things.

Q. So when you say it does it all by itself -- I guess that was a corny commercial where they said "set it and forget it"? I mean, is that what we're talking about? You've already told it what you want and you can just walk away and it's going to ask all of the people all over the world through the internet to give you pieces of what you want?

A. Correct. I load it into my program, assuming that all the [Indiscernible] are in place, it's going to learn a list of IP addresses that potentially -- that have shown this association, they've communicated on the BitTorrent network asking about the same torrent file. So they basically are matchmakers at this point. The BitTorrent network says this is the torrent you're looking for, I understand that, here's a list of 40 or 50 IP addresses that also show that association.

Well, at the point -- and this is very important -- at the point in time where my computer has interacted with the BitTorrent file sharing network and expressed interest in this torrent file, which is identified through caching like the Court has already heard, a very unique way to identify content.

So it will keep track of the fact that I asked that question. So my computer had -- my BitTorrent software, I loaded a torrent file into it, I've made an inquiry to the network, now the network knows about me. I have an association. And it could be me, Rob Erdely the law enforcement officer, or

any other BitTorrent user in the world.

So the next thing that happens is, I will start trying to connect people to get pieces of the file or files -- because it could be one file or many files described by a torrent -- and
07:39 hopefully get to connect to people. And at the point in time we connect, what happens with this BitTorrent file sharing network, there's some handshaking that goes on. It's just a computer term, but basically we're just gonna have a little conversation before we start creating data. And one of the very first things
07:39 that happens is, regardless of whether I initiated the connection to you or you initiated the connection to me, we first have to agree upon one thing: That we're talking about the same torrent.

And the torrent's identified through something called
07:39 an "info hash," but very simply it's a very, very, very unique way to identify it. It's more unique than DNA is to the human body. That's how unique it is.

So we agree we're talking about the same torrent. And then the next thing that happens is, both computers, regardless
07:40 of -- if I contacted you because I needed pieces of data, or if you contacted me because you needed pieces of data, in either case both sides are required to report, "These are the pieces I have to share," and the other side says, "These are the pieces I have to share."

07:40 Because BitTorrent is built on the premise it's a

tit-for-tat exchange. You're supposed to be able to give pieces of data to a person that is connected to you to download data, as well as receive. You're supposed to give and get, all through the same connection. And it's an automatic thing that
07:41 happens.

Q. Let me ask -- let me stop you there. Sorry.

Do I always need to go to 50 or 100 different people to get little pieces? Can I not just get the Jurassic Park movie I want from one person?

07:41 A. You could and do at times on the BitTorrent network using any software, not law enforcement, nothing specific. The network allows for the entire content to be downloaded from a single IP address.

But, it is true that you will speed up your download
07:42 times if you reach out to two, three, four, 10 or 20 different computers, because all of them could be giving you data at the same time.

But, just to put it in perspective, if I'm -- if I load a torrent into my BitTorrent program and I'm seeking to
07:42 download that material and there's only one person online that has it available at that moment in time, then the entire download happens from a single sharing computer. It's nothing unique to law enforcement software that downloads happen from a single sharing client.

07:43 Additionally, if you think about the person that had

to create this collection of data to share, no one else in the world has it. I'm creating this unique collection of files. So there's a process within your BitTorrent software to create that instruction file, that torrent file. So when I start sharing
07:43 that torrent file out and people want to start downloading it, there's only one person in the world that has that collection of files, me, the creator, until I start sharing it out.

So my point is, the fact that law enforcement does a download from a single sharing IP address is not unique to law
07:44 enforcement. It happens naturally on the BitTorrent file share network on a daily basis. So....

Q. So is that the conclusion of your overview of BitTorrent?

A. No. So then I just learned to go a step further. There was already a definition given for seeding and I just want to make
07:50 sure the Court understands exactly what seeding is.

So if I loaded a torrent into my BitTorrent software and I downloaded everything, now I have all the files that are described by that torrent file. I need nothing more. That's the moment in time you become a seed. If you are seeding a
07:50 torrent, you're in a position where you've -- you possess it all. And you're staying online for the purpose of continuing to seed the data, like a farmer in a field throwing seeds to grow his crops. Because a torrent and its associated data will only be available assuming there's enough BitTorrent programs online
07:50 around the world that have those pieces to share.

Well, so now that I have it all, this is the point that I'm trying to bring out, I am making myself --

(TRANSCRIBER NOTE: Witness moves away from microphone or microphone not functioning.)

07:51 -- available to anybody looking for that torrent and I will share the data for them. But it's important to understand this. I'm not just sitting here passively waiting for people to find their way through the internet to connect to my computer.

That certainly is one of the two possibilities.

07:51 Someone loads a torrent, they want to find a down -- someone to download it from, the BitTorrent network, the index tells them about my IP address, so they connect to me. And I'll give them the pieces they request.

Again, I don't need anything, I have everything, so

07:52 that whole tit for tat stage is gone, it's out the window. But there's another thing that happens, and a lot of people don't realize it [Indiscernible].

I don't just sit there as a seed on the BitTorrent network when I have everything and just sit passively waiting.

07:53 No. I created the index and look for people that are still in need of some of this material I have. I'm being overly helpful. I will make outbound connections from my computer -- when I say "I," I'm talking about the BitTorrent [Indiscernible] I apologize. I'm not trying to infer that the person

07:53 [Indiscernible] to make it happen. But the BitTorrent network,

I'm a seed, will continually query the network looking for new IP addresses that are in need of data. And I'm going to deliver it to them. I'm going to knock on the door and say, "I heard you need some of this data" and offer it up to them.

07:54 So it makes outbound connections to computers all around the world and it continues to share, and it didn't require that computer to reach into my BitTorrent software and make the request. I'm delivering it to you. It's home delivery so to speak.

07:55 Q. Okay. So when all this is happening, this happens automatically if the computer is on and connected to the internet?

A. Correct. As long as it's connected to the internet and it's running the BitTorrent software and until the person chooses to

07:55 stop the sharing or seeding process, it would continue operating that batch.

Q. And the handshake, the handshake takes place mutually, for lack of a better image, outside of each computer? I mean, no one's intruding each other's computer to go ahead and do that,

07:56 is it?

A. No, it's expected. The two computers have something called a TCP connection. It just -- think of it like a tunnel. There isn't a connection established or even a phone call. I pick up the phone and I dial your number and you have a phone, we have

07:56 an established connection, I can talk to you and you can talk to

me. That's what happens on BitTorrent.

So either I connect to the computer or the computer connects to me, but at that point we have this open line of communication. And again, the first thing that's gonna happen
07:57 is, we're going to agree that we both are talking about the same torrent. Because if we're not, the conversation's over. He could have stopped sharing. He could have stop [Indiscernible] seeding [Indiscernible].

The next thing that happens is handshake. And that's
07:58 where one BitTorrent program can talk to the other BitTorrent program and tell each other: I'm running a BitTorrent program called BitComet, and I could respond I'm running a BitTorrent program called UTorrent. Those are both real clients. So that's part of the handshake.

07:58 It's available to any program. As a matter of fact, the off-the-shelf, so to speak, clients tell you that. Or if there's a tab that says peers and you can see their IP address, you can see the version of software that they told us that they were running. It's part of the normal everyday communication,
07:59 that handshaking. It tells us what networking port they listed on, all those sorts of information.

Q. Okay. So Torrential Downpour Receptor, which is the program we're talking about here with regard to Mr. Owens, how does that differ from the BitTorrent -- or does it differ from the
08:00 BitTorrent that you just described?

A. Well, it's using just the functions I just described. Obviously we're law enforcement, that's not a surprise. But the way BitTorrent -- I'm sorry, Torrential Downpour Receptor works is that it searches for torrents files, the instructions, that 08:00 are known to law enforcement. And who is the person that decides whether it is something we search for or not? It's me.

And we learn that through the hashing of the files and comparing it to other [Indiscernible] location of files we know about, or at times I actually have to physically download the 08:01 file and look at them and say that's an eight-year-old, it's a sex offense, we're going to include this on the torrents that we investigate.

We do not listen in -- listen or monitor or try to discern one type of traffic from another. We simply search for 08:01 a torrent to learn the IP addresses of other -- others who have shown an association with that torrent, and we receive the search results relating to what IPs are present. We do not -- I don't even know how you would do that -- sit there and somehow sniff out or monitor all BitTorrent traffic. It's a 08:02 decentral -- decentralized network. That would be an incredibly difficult thing to do if it's possible at all.

We are just doing the same messages out that any BitTorrent program would give and receiving responses back. [Indiscernible] receptors you need, because all we're doing is 08:03 searching for torrents that relate to child exploitation and

then we sit there. We just sit. We're gonna sit and wait.

And because I searched for that torrent, remember, the BitTorrent file sharing network knows my IP address [Indiscernible], my law enforcement IP. And the BitTorrent
08:03 network is going to tell others about me. I'm just gonna sit and wait.

And that's what happened in this case. The suspect computer or the user's computer, however you want to define that, loaded a torrent into their BitTorrent program. The first
08:04 step happens where they inquire on the network [Indiscernible], what IPs might I connect to that also have an association with this torrent? And the suspect computer learns my law enforcement IP address and he, or she, connects to us.

That's analogous to the drug dealer driving his car to
08:04 the police station, going to the front desk and, any police officers here want to buy crack? Because that's what happened. The suspect computer arrived to law enforcement's computer, the TCP connection happens, we both agree that we're willing to talk about the same exact precise torrent, and now both sides, the
08:05 person that contacted the investigator and the investigator contacted the person who established the connection, we get to talk freely about that torrent. What pieces do you have to share, the law enforcement computer can ask the suspect computer, and vice versa.

08:06 So we're law enforcement, we do not share. And we

don't even have to lie. They ask us what pieces we have to share, we say zero. We have none. That's a completely acceptable message on the BitTorrent file sharing network. And then the sharing computer will tell us what pieces they have to share.

So here's what happened in this case as [Indiscernible] reading the law. The suspect computer was seeding. They had all the pieces. They didn't need anything from law enforcement. They connected to us through the overly helpful image sharing, like I previously described, and once we were connected we just started asking for the pieces of the data that the sharing client was making available. And all that gets memorialized in a log file by Torrential Downpour Receptor.

Q. Okay. And you've reviewed those log files prior to your testimony here today?

A. Yes, I have.

Q. And we've brought a couple with us?

A. Yes. The two in question that were two downloads of the same file spanning two different days.

Q. Okay.

MR. HUMBLE: May I approach, Your Honor?

THE COURT: You may.

MR. HUMBLE: And counsel has these.

BY MR. HUMBLE:

Q. Handing you what's been marked Exhibits 2 and 3, they seem

to be quite similar, could you explain to the Court what they are and why they're different?

A. Well, this is two different investigative sessions. Every investigative session -- every time we accept a connection from
08:08 a person -- a person's computer, it gets compartmentalized in its own folder. It lives all by itself.

And on two different dates, the same IP address connected to the law enforcement computer, possessing all of the content in complete possession of this movie file, and offered
08:09 to share it because that computer was, quote-unquote, seeding.

And that's what happened in these cases. And the reason there's two log files is because the first investigation began on May 21st, 2018. The download happened quite quickly, as the Court's already heard. And then the next day on May
08:09 22nd, the early-morning hours of May 22nd, that computer still had that material to share and was still offering to share it to the world. Just fortunate for law enforcement that that computer chose to connect to law enforcement's instance of the BitTorrent piece of the file.

08:10 MR. HUMBLE: May I approach again, Your Honor? I'm sorry.

THE COURT: You may.

BY MR. HUMBLE:

Q. I'm going to hand you exact duplicates of what you have
10:25 there so the Court has a copy and [Indiscernible].

A. Thank you.

Q. And obviously these are detailed logs. So I don't want you necessarily to dwell on each line, but there's highlighted portions.

10:25 Could you explain for the Court the significance of the highlighted sections, why you chose to highlight those and what that essentially means with regard to the program and the memorialization of the program?

A. Sure. And so just for the sake of being on the same log at
10:25 the same time, let's just describe a download dated May 21st, 2018.

Q. Which will be Exhibit 2.

A. Which is Exhibit -- I don't have -- yeah.

Q. You don't have that.

10:26 A. Okay, Exhibit 2. So if we all look at that one, then I can explain the highlighted portion.

So on May 20th of -- the first highlighted portion on page 1, it says, "Remote client at IP address 104.11.97.37 has connected to us."

10:26 Again, there's two possibilities why some BitTorrent computer would connect to us. That's either, A, he's seeking to find pieces he's yet missing, but he'd still share what he had, or he's seeding. I have it all, I want to be overly helpful, I'm going to give this data freely to anyone on the BitTorrent
10:27 file share.

So I know that a computer is connected to me, but I'm not really sure why until we start communicating. So the second highlighted area, "info hash sent by remote client."

So the computer that connected to us has to tell us why are you even talking to me. Well, I'm talking to you about a very specific torrent, and that has a hash value, it's called an info hash, uniquely identifying that torrent. There can be no duplicate. It's the same -- the odds are astronomical, it's one -- it's two to the hundred and sixtieth power, or one in 1.4 quindecillion, which is one with 48 trailing numbers. It's a very, very large number.

Q. So that number that begins 0833, that is the hash value?

A. That's the info hash.

Q. Info hash?

A. It's the hash of the information, the instructions unique to that torrent. And that's going to be the only payload or content it could describe is that file that it was meant to help you download.

Q. And that second highlighted portion appears to be occurring at essentially the same exact time as the initial connection?

A. Yes, it happens. We're talking about computers. It happens very, very quickly. Right.

Q. Okay. So what's that next highlighted portion mean?

A. The next thing that happens is, handshake data. And this is where the computer that is connected to us is telling us more

information.

Now, we know the torrent that they connected to us about, but in the extended handshake it's telling us things like they're listening port. So if we ever wanted to connect back to them, you need to know not only just an IP address but also a networking port. So P equals and then you see a number, that's their networking port.

REQQ, that sands for request Qs. It tells us how many pieces are we -- I'm sorry, how many packets are we permitted to ask for at any given moment in time. If it's included, we're supposed to abide by that value and we do. And you'll see that here in a minute.

It tells us the version of software they're running. This is something they offered to us in the extended handshake. It's given to any BitTorrent client, not just us.

And then it actually tells us our IP address, your IP. That means they're detailing in the handshake who they connected to. Just so there's no misunderstanding, I meant to connect to -- whatever IP address was listed. That would have been the law enforcement officer.

And then the next highlighted portion is why I know it was seeding and needed no data from law enforcement or it would even think to ask for any data from law enforcement or any other BitTorrent client, because the next section says remote client has all 226 pieces. You have to download 226 pieces of data

before you would be in possession of the entire movie file.
Q. And I'm sorry to interrupt, but you'd have to -- based on what you previously said, you'd have to do that 50 pieces -- 50 packets at a time?
10:34 A. 50 packets at a time is how you have to request them, yes.
Q. Okay.
A. So, and just to put it in context, that's about 50 -- just over 50 megabytes. So it's actually a small file as far as movies go on BitTorrent. 50 megabytes is not that large.
10:46 There's hundreds of megabytes of data that's shared in a single movie file.
Q. So here we've been talking about abstract kind of strings of alphanumeric -- alphanumeric strings, it looks like in the next highlighted portion we're actually start talking about the
10:47 movie's name that you would see on the computer?
A. Correct. Now, it's inside of the torrent. The instruction files knows how to name it. It takes the name of the creator. Whoever first shared this content on the BitTorrent file sharing network, it takes that name.
10:48 Q. Okay.
A. And the file name is -- and it's long, I don't know -- it's on everyone's sheet of paper. 022 Asian-VPHC. It appears in the quotes. That's the file name.
Q. Okay.
10:49 A. And then the downloads begin in the next highlighted

section, it says, "Sent 50 requests." Well, that's because of the extended handshake. The sharing client that came to us to share child pornography said you're allowed to ask for 50 packets at a time. So that's what we did. We asked for 50 packets.

10:56

And then we started asking for the packets and they get received, line by line. I've requested a packet, it's received. I requested a packet, it's received. Had to happen 226 times before the investigator would have the entire payload. So....

10:57

Q. And are -- on the next -- geez, I don't know how many pages, 17 pages long -- in the next series of pages, is that what you're detailing, that each piece going up to 226 --

A. Correct.

10:57

Q. -- this log reflects that it's been successfully received?

A. Correct, yeah. And it's just a couple minutes is all that it took. And then you don't see any more highlighting until page 11 of 17.

So, to put it in context, a computer on the BitTorrent

11:30

file sharing network came to us and we agreed we're willing to talk about the same info hash, the same form.

We asked for pieces of data. Now, you notice in the extended handshake it never told us 226, did it? It didn't say anything about 226 pieces or even the file name of this file.

11:31

It's because both ends of the communication has this instruction

file. It's required. Without a torrent file, you can't download on the BitTorrent network. You can't just, you know, wander around on someone's computer and say I think I want to download that. It just doesn't work that way.

11:32 It only works because we have the same instructions file. And also included --

So, well, let me back up. So for the -- for the sharing computer to say I have piece zero through piece 225, which is 226 pieces, tells me right away he's got the torrent,

11:32 he has to have the torrent, because I have my copy and sure enough, there's 226 pieces. Either that or it was a really good guess.

But now I named the file like the instructions says, but I've downloaded those 226 pieces. And where I'm going is,

11:33 on page 11 where that highlighting [Indiscernible], that's a hashing that happens on every piece of data shared. And it comes up with that fingerprint, digital fingerprint as the defense expert described. It's actually a SHA-1 hash. Secure hashing algorithm version 1 hash is what BitTorrent uses.

11:33 And it calculates the hash value, the signature for all 226 pieces. And so now what happens is, we are going to compare those hash values and make sure it matches what is in the instruction file of the torrent.

We had data set, we calculated the fingerprint, we

11:35 look inside the torrent and it matches. I got the right piece

of data. It has to be the right piece of data.

So for it to not -- for the computer that connected to us offering to share this torrent file to have guessed that it's 226 pieces and responded to our 226 requests for data, have that
11:36 computer give us that data and then match 226 SHA-1 hash values is inconceivable. The computer had to be in possession of that file and the instruction file, the torrent file, for what I described to have just happened. It's an impossibility. The computer had to have had it.

11:36 Q. And to be clear, that computer came to you. So Mr. Owens came to you.

A. Correct. And when you say "you," you mean the investigator --

Q. I mean the investigator, I'm sorry.

11:37 A. But, yes, the investigator running our software -- just because we searched for the torrent, like any other BitTorrent program searches for download candidates, that was enough to make us associated with the torrent that suspects were any computer on the BitTorrent network comes to law enforcement's
11:37 version just the same way they would go to any other BitTorrent program [Indiscernible]: Bitcom, uTorrent, Sherazel (phonetic), there's a ton of them out there.

Q. And that was Exhibit 2. Exhibit 3 we don't really probably need you to walk through, but why are there two exhibits? This
11:38 one reflects a date of May 22nd.

A. Yes. It was -- the Torrential Downpour Receptor is configured by the end-user and you can specify what IPs you'd like to investigate.

For instance, if I was a law enforcement officer at a university and I knew all of the University's IP addresses, I could say just -- I want to investigate any of these IPs.

And with Torrential Downpour Receptor, if any computer having that IP address comes to me offering to sell me drugs in my analogy, or give me child pornography, then I would accept that connection. I don't care about people in Russia or Spain or France coming to my computer, I care about people in my jurisdiction.

Or, the other possibility in the configuration, is I specify by geographic region. And I think the Court's already heard some of that through the defense expert. But it's publicly available. You can go to lots of places on the internet and you punch in an IP address and it will approximate what city and state that that IP is being used in. And that's just an effort for law enforcement to try to do investigations in their primary jurisdiction and not poaching in someone else's, so to speak.

Q. And so you reviewed the defense expert's affidavit.

A. Yes.

Q. And in there, in paragraph 24 essentially he asked what does it mean to direct investigative focus. Is that what you're

saying, this program directs the investigative focus by saying I want to do this in Wisconsin, or I want to do it in northeast Wisconsin, or this particular series of IP addresses?

A. Yes. It's user configurable. And it does run -- I

10:57 configure it, I launch it, and it's set to investigate people in Wisconsin. And it's ignoring all the other connection attempts to us.

If I have a connection attempt from an IP address and it approximates the location as being in Spain, I just refuse

10:58 that connection. I'm only accepting connections from the Wisconsin area, if that's how I configured it. And that's how you direct your investigative focus to a particular region, by their IP addresses, or straight up with their IP address if I knew that range off the [Indiscernible].

11:01 Q. And are those the settings that the investigator would be able to essentially input?

A. That, a license, their name. Things of that nature. But there is no setting that would enable them to -- enable a feature that would be harmful or would make the software not

11:02 work properly.

Q. Or I want to go after this particular person or just white males in a certain area, those aren't variables that this program allows?

A. No, it's geographic region or IP address. And then you can

11:03 further restrict it. Although I'm sort of the gatekeeper as it

relates to what torrents do the systems seek out on the network.

I can't define what's illegal in every state in the U.S., let alone every country in the world. I include torrents to be investigated that presumably would have some violation somewhere. It relates to child exploitation.

For instance, I could include pictures and movies of 17-year-olds engaged in sex, which is child pornography federally and child pornography in Pennsylvania, where I'm from; but in Connecticut, it's 16 or under.

So the onus is on the investigator to look at what's downloaded and determine, yes, this violates our statute, [Indiscernible]. But we don't just sit there and sniff and listen to every piece of BitTorrent communication and try to discern as the defense expert --

And, you know, obviously he hasn't seen the software, but we aren't sitting there sniffing on the network or listening and trying to discern this is child pornography and this is not. No. We have the torrent. We're like every other BitTorrent client. We reach out to the index, the matchmaker as I described it earlier, and they provide us with IPs. That's it.

There's no listening for movie files, for anything else; it's just the predesignated torrents in the system. We're very refined. We're not searching for everything, we're looking for a very specific subset of data.

Q. And to be clear, in this particular case Mr. Owens came to

law enforcement.

A. Correct. But let me just say that if he had come to law enforcement and it wasn't one of the torrents we had chosen to investigate, it would have ended there as well. Because we're not going to talk to a person about it.

The other configuration I was leading towards -- and, sorry, that was a little long-winded -- is that the end-user, if they download material and they determine this is not violating my statute in Connecticut, because it has to be under 16, they have a mechanism to exclude those in future investigations. So they can further refine it even more than the work that I've done trying to identify the torrents leading to be investigated by law enforcement.

Q. Okay. You had the opportunity to view the imaging of Mr. Owens's computer I believe yesterday in my office, correct?

A. Yes.

Q. Okay. And I'll ask you what I asked the defense expert, did you find any artifacts or evidence that this particular file had been on Mr. Owens' computer?

A. Yes. The torrent which points to a file, yes, that both the torrent and the file was on the system in -- excuse me -- in three different areas.

Q. Okay. And did you print off basically information that would reflect that that we can show to the Court and provide to counsel?

A. Yes, I did.

MR. HUMBLE: May I approach, Your Honor?

THE COURT: You may, uh-huh.

BY MR. HUMBLE:

11:10 Q. I've handed you what have been marked Exhibits 4, 5 and 6. Could you just identify those and tell the Court what they are?

A. Yes. These are just one portion of the forensic analysis.

4 relates to installed programs.

5 relates to torrent files.

11:11 6 relates to MRUs, or most recently used entries, from the registry.

Q. Okay. And did you create these?

A. I created this printout, but the forensic -- it was part of the forensic [Indiscernible].

11:11 Q. Sorry, that was imprecise. You created the images.

A. Yes.

Q. And that captures what you're trying to show here?

A. Yes.

Q. Okay. I'm going to switch those out, those duplicates, so 11:12 that the Court can follow along.

Now, I guess start with the first one which I believe is No. 4?

A. Correct. So --

Q. Sorry. Could you just explain the significance of why 11:12 that's highlighted and what that reflects?

A. Yes. But before I get there, I just want to go back to this log file where the computer that connected to the law enforcement reported what software they were running. And they reported it as being BitComet Version 1.50, which was highlighted in yellow in those two exhibits we just went through.

So the first thing I would look at would be to see if there is a BitTorrent -- BitComet program installed, and sure enough, BitComet Version 1.50 was installed. And coincidentally, or not coincidentally, it was installed on May 20th at 9:07 -- I don't have my glasses on, I believe that's right -- p.m.

So that's the date, the day before the investigation happened. So the user of this computer installed BitComet Version 1.50 the day before the investigation happened and was memorialized in these logs. So that's the first -- that would be Exhibit 4.

MR. DONOVAN: Your Honor, if I may, I would like to interpose an objection. I think this is getting a little far afield of the relevance of this hearing which is whether or not we should have access to the program.

It sounds to me like he's trying to establish guilt based on he had the program on this date, it was installed on a certain date, then I guess there was, you know, torrents downloaded.

It just seems like this is kind of far afield of where we should be for today.

MR. HUMBLE: Except, Your Honor, that the defense expert places great significance on the fact that he did not find that particular file on the defendant's computer or in multimedia. So I think it is certainly relevant that there was strong evidence, which he also testified he did not find necessarily, to show that this was there both before and after law enforcement had any interaction with Mr. Owens's computer.

11:16 THE COURT: Overruled. And I assume we'll get to the law enforcement privilege later. But this is kind of the preliminary steps of how it works, as I understand it. And it's -- I see this as testimony intended to show that the defense is not in need of the software or the computer -- the other materials sought. Now, that's arguable, I agree, and certainly you'll be able to cross-examine and argue on that. But at this point I think this testimony is relevant, so overruled.

BY MR. HUMBLE:

11:17 Q. Okay. So, now, essentially he -- if this reflects that [Indiscernible] the tool that was used to knock on law enforcement's computer essentially and say I'm gonna give you this, that's reflected on No. 4?

A. Correct. Because the file wasn't found, the next thing I want to know as a forensic expert, okay, if it isn't there

today, deletion being a common thing we all do, let's show whether or not it was there during the investigation, which is what this was meant to do. So the software reported to law enforcement was installed the day before the investigation took place. That's the relevance of that exhibit.

Q. And how about Exhibit 5, what's the relevance of --

A. 5 is the torrent file named by its info hash. So if you looked at the detailed log with the highlights that we went through, remembering the first step is to agree that we're talking about the same torrent file, that's step number 1. Because if we can't agree that it's the same torrent, I'm done talking to you.

If you look at the entry on Exhibit 5, the longest cell, it starts "Partition 4 Microsoft NTFS." But if you look at the next row down all the way to the end, you see a string of numbers and letters, 0833, and then at the end it ends in 3C0, I believe.

If you marry that up with the log, that's the exact same info hash. So there's a date and time affixed to that. May 20th at 9:29. So we're talking 22 minutes after he installed BitComet -- he or she, the user of the computer -- 20-some minutes later the torrent was downloaded and loaded into BitComet. Why do I know that? Because the path of where that torrent was found would only get there if you loaded the torrent into the BitTorrent program. Otherwise it would just be sitting

in my downloads directory or on my desktop or someplace I chose to save it. That's a hidden directory for applications to store data they're using. So I know he downloaded the torrent and loaded it into BitComet for it to be there.

11:22 Q. And what is the --

A. And that's the day before the investigation, to put it in perspective, May 20th at 9:29 p.m.

Q. Okay. And the next exhibit, what is the significance of that?

11:22 A. Well, this is most recently used. And when you touch files and you access files, it will keep a record of that. And on May 22nd, a file with the exact same file name as the one sent from the suspect computer to the law enforcement computer, is there. And that's dated May 22nd at 1:38 a.m.

11:23 So the second investigation occurred on May 22nd at 3 a.m. So it's just an hours apart. It's still there so it's being shared all the way from the 20th, when he started downloading it, through the 22nd when the second undercover session happened.

11:23 And I also note that in the exhibit where the torrent was found, this -- there was more than one instance of him having that torrent. There was one that dated all the way back to January of 2016. And so what we are seeing more and more -- because I still do investigations beyond the development aspect

11:24 of my position -- more and more with the speed of the internet

and the efficiency of BitTorrent, not everyone keeps every file they download. They download it, they look at it, and at some point in time after that they delete it because it's so easy to get it again.

11:24 And there's -- there's a reference to that same torrent file all the way back to January of 2016. So that makes me fall on the side of the fence that these files were getting deleted as opposed to it was never there. It was clearly there. That's what these forensic artifacts show.

11:25 Q. And correct me if I'm wrong, the log that we went through previously, that's what law enforcement has -- receives, correct?

A. Right. This is the memorialization of the events that took place during the investigation made by Torrential Downpour

11:25 Receptor.

Q. And 4, 5, 6 were taken from the image -- the imaging of the defendant's computer.

A. Yes, that's correct. That's a seized device.

Q. So these aren't married -- these are two opposite ends

11:25 essentially matching up.

A. Correct. Everything's lining up.

And I could have stopped just by reading this log. There is no way that a computer at that IP address didn't possess that data, to be able to give me 226 pieces that match

11:26 the right hash file. The computer had to be in possession of

that data to send it, and this just further confirms it.

Q. Okay. So let's get to law enforcement privilege then.

What's the harm in allowing testing to occur with regard to Torrential Downpour Receptor?

11:27 A. Well, it has access. In order to run it you have to have a license, first of all. That license is controlled by the system I'm the administrator of.

And when you have a license to the software, it's designed to download child pornography. And so you put in a

11:29 license and you specify an IP address or geographic region, child pornography will be downloaded, because people will arrive to our computer and offer to share child pornography with us. So it exposes each and every torrent file we're investigating.

Again, to know the info hash of these torrents could

11:29 be harmful to law enforcement because if that gets out -- although, you know, people can promise never to release it, you can't un-ring the bell. Once it's out it's done. We have to start from scratch.

It's taken eight years to amass what we have here

11:29 today. At least eight. I can't remember the exact days when we started, but it was at least eight years to get where we are today.

It exposes the files we investigate and their hash [Indiscernible].

11:30 It exposes law enforcement contact information of

investigators who are investigating individual IP addresses. These are active investigation.

It exposes the IP address -- other IP addresses associated with the torrents that we investigate. So, in other words, these have yet to be investigated. There are just so many people on BitTorrent sharing child pornography, we cannot get to them all. I've trained personally hundreds, maybe upwards towards a thousand investigators, and we can't come close to getting all the people sharing child pornography on the BitTorrent file sharing network. And I'm not even talking about all the other areas that we can investigate.

So -- and finally, I mean, aspects of the system, you're basically dropping a civilian in the mix of a raid briefing. These are -- the system is designed to connect law enforcement officers that have similar investigations based on their IP addresses, they're in some stage of investigation, the system alerts them of that, and you're dropping a civilian in the middle of a raid briefing. If you're taking something technology and trying to relate it to something real world, it would be an equivalent.

Q. Were you saying raid, r-a-i-d briefing?

A. Raid like a search warrant.

Q. Okay.

A. Is what I was referring to.

Q. Okay. So, let me ask you, with regard -- in your opinion,

as someone who helped develop this program and obviously has a lot of familiarity with it, is Torrential Downpour Receptor so different from other BitTorrent programs that there is a strong need for the defense to have this before they could
11:41 cross-examine somebody on the operations of this particular BitTorrent?

A. The only point of confusion that I could see the defense expert having, which he now has the answer to, was why a computer would connect to us. He gave a definition of seeding.
11:41 And I don't know that he had a full understanding of what seeding actually was.

But now with that question answered, this is -- this is BitTorrent talk. This is not Torrential Downpour Receptor talk. I mean, anyone should be able to look at this and see
11:42 that data was sent and it matches the corresponding hash [Indiscernible]. The defense expert has the ability to look at the torrent which is part of discovery, open it up and see all of the hash values of all those 226 pieces, see that they were verified, could even take the original file and hash those
11:44 individual segments to make sure that they do, in fact, belong to that file, none of which requires our software.

This is -- this is a law enforcement BitTorrent piece of software that, yes, employs the ability to download from a single IP address as opposed to from multiples. Well, that's
11:45 law enforcement being more restrictive on itself.

I could get it really fast, but I'm willing to wait. But it's not something unique to law enforcement software. A download from a single sharing IP happen all the time.

So I don't believe that there is a need to confirm it when we've detailed it as specifically as we have. This is all information, as the defense expert said, that any BitTorrent client would know. But whether or not it chooses to display it to the user, and certainly probably wouldn't memorialize it to a log file like this, but it is to aid the prosecution, but it's also letting the defense expert know exactly what happened at what moment in time.

And he can confirm these things through the forensic analysis, as I did. I spent 10 or 15 minutes and found these three items. There's probably much more on there that I didn't look at, and to have the torrent file and the data, that should be sufficient.

Q. In your expert opinion, if there had been a bug or a glitch in the software, would that be reflected in the things that you've reviewed prior to your testimony here today?

A. Yes. I mean, I would get the bug reports. I would know if there was a bug report. If people are continually downloading files and they didn't come from the sharing computer, I would know to seek that out.

But it's a very simple process. As the defense expert said, the IP addresses have a source and destination IP right in

every packet of data. It's not hard to discern where it came from. And we just memorialize that in this document.

And, again, that IP address came to us. Just like if you visit a web page, that web server knows your IP address immediately. Well, the suspect computer came to us. We documented the IP address, we allowed the communication to happen, and then we received the data they wanted to share with us.

Q. Would you -- based on your knowledge of Torrential Downpour Receptor, would you describe it as bug-ridden or buggy as I guess software people say?

A. No. Early on in its early stages of development we had the source code looked at, and there was one issue -- and this is eight years ago -- where we weren't accounting for long file names that exceeded 260 -- or the path and file name to exceed 260 characters, that was fixed, and that was the end of the bugs as it relates to downloading.

BitTorrent is a very, very light-weight small protocol. A BitTorrent program like BitTorrent or uTorrent are like a couple megabytes. It's the size of a single picture. It's not a ton of code that could be bug-ridden like the defense expert's example of an operating system or Microsoft Word that are millions of lines of codes. We're talking about 2 megabytes of programming.

So, but that was fixed eight or more years ago, the

long file name issue, and all that would have done was shut the program down. It wouldn't have collected erroneous information.

And the fact that BitTorrent relies on SHA-1 hashing, which is extremely accurate, you're not going to get the false positives because we're confirming the data through hashing, the same thing forensic examiners use to confirm I'm working from an exact duplicate of the hard drive seized. We rely on it day in and day out. Well, BitTorrent does as well. And through hashing, short of SHA-1 hashing failing, which is very, very accurate, you're not going to get a [Indiscernible] false positive.

MR. HUMBLE: Judge, I don't have any further questions.

THE COURT: Mr. Donovan?

MR. HUMBLE: Could I just ask that those exhibits be received, Your Honor?

THE COURT: 1 through 6 received.

I take it there's no objection.

MR. DONOVAN: Well, Your Honor, I mean, we didn't see Exhibits 4, 5 and 6 before today, but, I mean, no objection as far as --

THE COURT: I don't think they existed before today. It sounds like they were run off today. Is that right, Mr. --

MR. HUMBLE: Was it this morning or last night? Last night perhaps.

THE WITNESS: To be clear, this is the forensic report of the forensic examiner. This is the material that was --

MR. HUMBLE: Yeah, it's been provided, just not the exhibit --

11:54 THE COURT: Okay.

MR. DONOVAN: Your Honor, we don't deny that the forensic material was provided, but, I mean, it's large. It's very voluminous. And we did not see these exact references until today.

11:54 THE COURT: Yeah. But you had access to the hard drive or the computer --

MR. DONOVAN: Correct, yes.

THE COURT: -- evidence from which this was taken.

I'll overrule the objection and 1 through 6 are

11:55 received.

(Exhibits 1-6 received in evidence.)

MR. DONOVAN: Thank you.

CROSS-EXAMINATION

BY MR. DONOVAN:

11:57 Q. Good afternoon. Getting towards the evening here shortly.

Okay. So you have testified that you were part of the original development for all of these types of programs, correct?

A. Yes.

11:57 Q. And it's been kind of an evolution from probably -- I don't

know if Gnutella was maybe the first iteration all the way up through now BitTorrent. Right?

A. There are many file-sharing networks that we have investigative tools for.

11:59 Q. Can you I guess more precisely describe your role? Because you said you didn't do any of the actual programming, correct?

A. I didn't write Torrential Downpour Receptor, the program being used. I did programming on the back end and testing of the software. But with the other tools there are programming

11:59 elements that I did participate in, it's just not with Torrential Downpour Receptor. The physical program sitting on the investigator's computer, how it logged search results and things like that I was involved.

Q. Okay. How long did the development take of Torrential

11:59 Downpour?

A. From the point in time where we first talked about it at the University of Massachusetts to releasing the first version, it was well over a year. Maybe more.

Q. And maybe this is a good time, can you explain the

12:00 difference between Torrential Downpour and Torrential Downpour Receptor?

A. Torrential Downpour wasn't used in this case and it doesn't sit and wait for suspect computers to arrive to our computer. It's the complete opposite of that.

12:00 So Receptor sits and listens passively for people

coming and knocking on our door asking to share torrents that we know that involve child exploitative material.

Torrential Downpour makes outbound connections trying to connect to somebody that may or may not be sharing child pornography.

That's the big difference. We sit passively and wait for the suspect to come to us.

Q. Is the only way you know which one was used in this case is from reviewing the logs? Or did you talk directly to the law enforcement officers who ran this?

A. Well, the log certainly tells us -- that's the whole purpose of putting on the first line the software that's used. But beyond that, through networking I can tell that.

In the extended handshake he tells us what his listing port is. So if I were to connect to him, I would connect into that port. I know we're getting kind of technical. But you can see at the top, he connected to us because it's an outbound port. There's a specific range of ports. Of the 65,000 ports -- there's more than 65,000 ports available to use -- there's a set of ports set aside just for making outbound connections.

So it's proof that the suspect computer connected to us. The networking ports alone tell you that. And the software that we indicate we were using at the top of the log indicate that. That's the only functionality it has, is to receive an

inbound connection which triggers an investigation.
Q. But, again, you would agree that the logs are a subset of the program, correct?
A. The --
12:03 Q. They're generated by the program.
A. They're generated by the program, I agree with that.
Q. And so the information that comes from the program dictates what's on the logs.
A. Correct.
12:03 Q. In other words, the logs aren't an independent check or verification of anything, it's a subset of the program that we're talking about.
A. Correct. The computer comes to us, we see the IP address, we memorialize it in the log. Correct. Which is Windows,
12:04 actually.
Q. What language is Torrential Downpour Receptor written in?
A. C#.
Q. Okay. And so obviously this involved, you know, computer scientists and software developers and other people besides
12:06 yourself to put it together, correct?
A. Me and one guy, Brian Lang.
Q. Okay. Oh, just the two of you.
A. Yes. And it's not -- it was written by the ground up from the university. It was not a modified version of an existing
12:07 program. So that was incorrect information the Court had heard.

It was written by the University of Massachusetts Amherst. And the team of developers beyond the initial research is me and that one individual.

Q. Okay. Now, you've reviewed the pleadings in this case, right?

A. Yes. Well, I've read the defense expert's report/affidavit.

Q. Did you read any of the motions filed by either me or the government?

A. I did not. They were already filed and done before I even had communicated with the office. I don't believe I -- I did have a copy of the police officers' report. I never had a copy of the search warrant. And then obviously I have the two detailed logs.

Q. So, sir, are you aware that the government has said that basically the investigator in this case accessed BitTorrent like a normal or average user of the program? I'm talking about the normal BitTorrent program, not the law enforcement program.

A. Can you repeat that? I don't want to --

Q. Are you aware that the government's characterized law enforcement's use of BitTorrent here as a normal or average user?

A. I am now, I wasn't before. But I don't feel that that's inaccurate.

Q. You don't feel that's inaccurate.

A. No, we follow the protocol. And just like any other program

can receive an inbound connection and download any or all of that data, we did the exact same thing except we memorialize the data and we don't share.

Q. Well, there's -- I mean, there's a lot of other things that the program does the public version doesn't, right?

A. (No response.)

Q. And I can give examples.

A. Okay.

Q. Would you agree that, again, it does single source downloads?

A. Correct. The general public does that as well.

Q. And I understand you testified that that could also happen in the public if there was only one computer sharing this one file that could be a single source, but your program doesn't even when there's multiple sources available which would be contrary to the normal protocol, right?

A. Our program I'm sure it happens every time, but it happens naturally every day on the internet.

Q. But yours insures it only happens on single source downloads.

A. Right.

Q. Right? It wouldn't do any good to get multi-source downloads and then try to figure out who to attribute this to, right?

A. That would be counterproductive. It would add a burden to

law enforcement.

Q. And your program -- and I think you testified earlier that it doesn't fake file share, it just says it has no pieces to share, right?

01:09 A. Because we have no pieces to share we appropriately say we have no pieces to share.

Because the computer -- since we're employing a single source download, every piece of data we have received came from the computer that connected to us. So there is no need for us

01:09 to ever share any data back because everything we have came from the sharing computer.

Q. Well, I understand, too, you don't want to share contraband, correct?

A. Correct.

01:10 Q. Okay. How do you then -- so the program does something to stay on the BitTorrent network and not get kicked off, right?

A. That doesn't exist. And I don't -- I'm not sure what the defense expert was talking about.

Q. Well, have you heard the term "throttling" before?

01:10 A. Yes, you can throttle. That's not being kicked off the network.

Q. Oh.

A. So, in other words, there are incentives. If you share, if you employ that tit-for-tat exchange, so I'm giving pieces as

01:11 I'm getting pieces, you're -- the allocated bandwidth you're

given is increased. So I might get that file a little quicker.

But, to not share, I'm still able to download and I'm not kicked off the network and I'm not fake file sharing.

Q. Okay. I'm sorry, I don't mean to be imprecise. I didn't mean to say kicked off the network. But you could get throttled if you're not sharing, right?

A. You could receive your downloads slower than other BitTorrent clients.

Q. But here you testified that based on the logs these downloads actually occurred pretty quickly.

A. Correct. Because the client didn't need any pieces for us. The tit-for-tat exchange was gone. That, on top of the fact it was an AT&T U-verse connection, which has a large amount of upload bandwidth which is the one exception. AT&T U-verse and Verizon Fios have huge upstream bandwidths. So what the defense expert was describing really doesn't apply because the connections are so fast. But it's only a 15-megabyte movie, so I expect it to happen fairly quickly with the speed of the internet today.

Q. So just to be clear, is your testimony that the program does not do anything to stay on the network that an average user couldn't do? To avoid being throttled or --

A. I don't even understand what you mean by on the network. Because you're on the network every time you load a torrent file into your program. You don't get kicked off. A user can choose

to share the data with you slower. And, yes, that is part of the incentive scheme for this give-to-get scenario on BitTorrent. But it doesn't preclude you from getting everything without sharing one single bit of data, which happens naturally every day on the network.

Q. So does Torrential Downpour do anything to avoid throttling? I shouldn't say kicked off. Avoid throttling for not sharing.

A. No. We properly say we have nothing to share at the beginning of the session. And then if ever we're asked again, if we handshake again, which happens sometimes, we would report what pieces we did have to share.

Again, the sharing client gave us every piece we possess. There is no need for him to ever request that back from us. So this whole tit-for-tat exchange and the throttling, as you put it, of the bandwidth doesn't really come into play in this case specifically because they were seeding. They had all of the content. There is no need to throttle data. Its purpose in life when it's seeding is sharing the data proactively out to the network to keep that data alive on the BitTorrent network. So throttling really isn't in play when there's a seed.

Q. Is it ever in play, though? I mean, it's not in play in this case, but can it ever be in play that you get throttled?

A. Oh, absolutely. Again, if I never share a piece of data, which we don't, I will never benefit from added bandwidth from the sharing client.

Additionally, clients at times, depending on -- there's so many variables to go into, but depending on how popular the torrent is, they could actually share with me for a period of time and then disconnect from me. And then later, as any BitTorrent client would, you can reconnect and ask for additional pieces. Again, I'm in the same situation.

Q. So I'm not trying to belabor this, but, again, not in this case, but does Torrential Downpour Receptor ever do anything to not get throttled in general to be able to keep up fast --

A. No.

Q. -- and do what it wants to do?

A. To the contrary. We get throttled is what I'm trying to say. We didn't here because --

Q. Okay.

A. -- he was seeding. But there is no secret mechanism to keep us getting data faster than we deserve to get it. It doesn't exist. And I wasn't trying to avoid the answer --

Q. Okay. It's fine. I apologize. I probably wasn't being precise enough.

Torrential Downpour Receptor again generates these specialized data logs that you've talked about which the normal program doesn't do, correct?

A. Correct.

Q. Okay.

A. It's information known by the programs, but there would be

no purpose for BitComet to write out a log like this.
Q. And it conducts searches against the hash library, you've talked about, right?
A. (No response.)
01:19 Q. Again -- in other words, you have a set of hash values that you are looking for torrents that report having an association with them, correct?
A. Correct. We're searching for a torrent exactly like any other program out there. As soon as a torrent gets loaded into
01:19 BitComet, which is the program in question here, it actually searches for download candidates.
And that's what we do. We physically load a torrent into Torrential Downpour Receptor, and then it searches the network for download candidates. It's exactly the same.
01:20 Q. Now, to be clear -- to be clear, when you say "we" it's actually you. You maintain control exclusively of the database, or library, whatever you want to call it, of all these hash values you're looking for, right?
A. What torrents we search for I'm in control over. What is
01:20 being searched for by the investigator is an actual torrent file being loaded into Torrential Downpour Receptor like any other program. We're just excluding the commercial movies and the commercial music and the illegal, you know, copyrighted programs that are traded on BitTorrent and we're only focusing on child
01:21 exploitation material.

Q. Again, that you decide on, correct?
A. I decide on what is to be searched for. The investigator decides on what to use as probable cause for a charge.
Q. Okay.
01:21 A. And they make suggestions. They will submit torrents to me to be evaluated to be included into our system.
Q. Can you describe a little bit about how the program is set up by someone who's got a license and is trained to do this?
A. Sure. It has an installer file just like any other program. 01:21 You double-click an installer file. It will ask you some questions. Some questions already have answers to them. But it will ask you to input your name. There are options to put in your email address. But you have to have a license number to run it or else it won't function.
01:22 So we control who has a license. So if the software gets out there it's nonfunctional without the license, it will do nothing.
You will specify with Receptor what geographic region you'd like to investigate. Or you could express it by the 01:22 physical IP address or a range of IP addresses, which is the trigger to the program to decide whether to, as the investigator put I think, direct his investigative focus towards a particular IP or not. It's based on his settings. He's told the computer investigate these IPs or just investigate people in Wisconsin as 01:23 opposed to anywhere in the world.

And there are settings regarding how long should we wait for the download to complete. Because we're not gonna wait forever. And so we can just stop the investigation after a predetermined period of time. The default I think is four hours.

Q. And this program can run automatically, right, after it's set up and configured?

A. Correct. You're going to configure it and set it up and it's going to search for torrents and receive those inbound connections automatically. The logs get written out automatically as well.

Q. So does the investigator typically just check the results like every day, every week, every month? Like how does that work?

A. Well, I can't speak for every investigator, but on every shift of my work I check my logs.

Q. Okay. Okay. So going back to the logs that have been introduced as Exhibits -- I believe 2 and 3, how do those logs, for example, like establish by themselves that Torrential Downpour Receptor doesn't invade, for example, the shared space of a computer?

A. Well, it basically comes down to -- well, first the suspect computer comes to [Indiscernible]. That's the first piece.

The second piece is just to understand BitTorrent, if you understand the BitTorrent set of rules that have to be

followed and how it functions, it's -- what you're describing is impossible.

I can't -- if I wanted to download -- excuse me, I'm sorry.

01:25 If I wanted to download a file from some unshared location on the computer, I can't even do that because both the sharing computer and the investigating computer -- or in another way I could say that as any two BitTorrent programs -- would require that you have the exact same torrent file.

01:26 I can't -- there's no function within BitComet, which is what was used on the suspect computer in this case, there is no ability to download anything. We can only receive what the sharing computer permits us to get.

Q. So is your answer that the program just can't do it and,

01:27 therefore, that's why it's not on the logs? Is that --

A. It's -- yeah. Not even BitComet. Any BitTorrent program on this planet require a torrent file on both sides with that really unique identifier. I have no way to know where these files are on the suspect computer, let alone create a torrent

01:28 file, load it into his BitTorrent program, just so that I could then investigate him with our BitTorrent software. There's just no mechanism. You'd have to show that there was a flaw in BitComet at Version 1.50 that allowed some crazy intrusion like you're describing, but that doesn't exist.

01:29 Q. Are there any other types of logs generated besides what's

been entered as exhibits or is that the comprehensive log?
A. This is the comprehensive log. There's also a net -- a netstat. Because for reasons just like this, there's a Windows program that will record TCP connections.

01:29 And earlier as I was describing how the suspect computer connected to the law enforcement computer, it was through something called a TCP connection. And Windows has a utility that will track all of the TCP connections between my computer and other computers. So we run this netstat program,
01:30 this windows program that has nothing to do with us and our development, to confirm, to give corroborative evidence that, yes, this other program came to the same conclusion as us that there was an active TCP connection between us and the suspect computer.

01:31 So there's the netstat log. There's a summary log which is just less verbose than the detailed log. There is the torrent info.txt file which gives you all of the information inside of the torrent that is used to calculate that unique identifier, that info hash I spoke of.

01:32 There's two XML files that contain data and I don't remember them off -- the names off the top of my head. Those XML files are just data that help us evaluate the case more quickly.

It's the same data that you're finding in the detailed
01:32 log in other areas. We have a program that helps us parse

through that and realize information. So that's what those XML files are for. And then you have the actual downloaded material which is in a download directory.

So that's the output of the software, all those items.

01:33 Q. Are there any other either libraries or software packages that the program relies upon or uses?

A. No. Actually there's no libraries. Everything was written from the ground up. There was a point in time I think he was using an open source library, but he ceased using that years

01:34 ago.

Q. So is it like -- I mean, I'm not trying to be too basic here, but is it literally like one file, the program? Like one application file? Or does it have associated files with it?

A. Yeah. I mean, you're gonna install a program and it's one

01:34 file to start the installation, but it's just not a single file that makes it work. There's configuration files and such.

For instance, when you're inputting the settings on who you want to investigate, that has to be stored somewhere. There's other associated files [Indiscernible].

01:35 Q. Okay. Is Torrential Downpour Receptor actively maintained?

A. Yes. It's worked on and maintained by the University, who is the owner of the software. It still exists. And, you know, there may be features we want added to it. That programmer is still available to accommodate law enforcement requests.

01:36 Q. How about like, are there patches done to it occasionally?

A. Oh, there's new versions released to implement new features that we want to make law enforcement's job easier in evaluating the case. There's so many people on BitTorrent sharing child pornography that we want to try to get the most egregious stuff
01:37 first. Those are the changes that are being made in the new release.
Q. Is it your testimony that there's really only been one bug with this program since the time it was developed?
A. That's the only bug that I know of that relates to single
01:37 source downloading, and it was reviewed -- it was the long file names, which was handled.
Q. Who found that or who reviewed that?
A. Before the FBI would let the -- their agents use the software, which we had already bought through a grant, and they
01:38 did an independent validation of the method in which we do single source downloading to confirm that we don't share, which obviously law enforcement can't become part of the problem, and that it does employ properly as [Indiscernible].
Q. I don't know suppose that FBI validation is publicly
01:39 available.
A. No. I mean, the purpose of them doing it was to permit the agents to use the software we developed. And now they've abandoned their own programs and just use the whole [Indiscernible] that make --
01:40 Q. But again, that's not something that we can look at, that

validation.
A. I don't have it. I've read it once, and that's why I know that was the bug that was seen and fixed immediately. And, again, I'm the administrator of the entire system still to this
01:41 day. It's housed by the Pennsylvania State Police in a computer center and I would receive those bug reports. I don't know of any other bug that would affect [Indiscernible].
Q. So you're the only person that would get reported to if there was a problem?
01:41 A. Me or the developer. If any other instructor would receive it, it has to come to me eventually, or the programmer.
Q. So how often typically is it updated?
A. The version that's current -- I don't think there was any release in the last six, eight, ten months maybe. There may be
01:42 some years where there were a couple releases. Because we, again, they're feature enhancements, not changing the method in which we single source download. But we may want to be able to flag the most egregious torrent as opposed to torrents that have pictures of kids modeling adult lingerie or something like that.
01:42 Q. Well, that would just be more updating the hash database, right?
A. No, that's updating the program and how you look at it.
Q. Okay.
A. How you look at the data.
01:43 Q. What type of network connectivity does it require?

A. It uses TCP communication for the file transfers.

TCP, Your Honor, is transmission control protocol. And it's, again, that type of internet traffic that I compared to like a phone call. You dial a number, you say hello, hello. There's error correction, all kinds of things.

Some of the indexing that BitTorrent uses also uses UDP packets, which are connectionless packets. And that's for once you load the torrent, so that you can get those IPs of people associated with the torrent. That comes via UDP depending on which index you're connecting to. So it uses both TCP and UDP networking.

Q. Do you test to determine whether it's operating correctly from time to time?

A. Yes. You test it at the conclusion of every class with the students. I test it before the release of the software. There's a validation process.

Q. So you've done that testing in the past. You say you do it every class that you teach?

A. Yeah, at the conclusion of the class we go through a process. Because it's automated the end-user in the class, we'll go through a validation process.

So, for instance, if we're gonna rely upon a log as the basis to get a subpoena for a subscriber or eventually a search warrant, then that investigator needs to trust that the logs' dates and times are correct.

So we have a computer that's sharing content and a computer that is investigating. And we show both screens. And as -- as events happened we confirm that the dates and times in the log are correct. We confirm that the IP address purported in the log is correct. Because we're controlling both sides of the communication, so we know the sharing computer's IP and the investigating computer's IP.

We verify that it properly weights out the info hash of the torrent in question, and that it dates and timestamps appropriately throughout that log.

And then, finally, it calculates the MD5 and SHA-1 hash at the conclusion of the transfer.

Q. So in this training or this validation testing you just described, you're controlling both computers, correct?

A. Correct.

Q. Are you actually transferring child pornography or is it just a benign file of something else?

A. It's a benign file.

Q. So why couldn't that be done for the defense?

A. Well, it exposes all those other things to our system.

Again, once you have a license to our software, you see active investigations, you see contact information for the investigators, you would learn all of our hash values, all the info hashes of the torrents. But it is possible to set up a torrent with data that is not child pornographic, but it takes

my involvement.
Q. Well, in fact, so you've done that before for the defense counsel, right?
A. Done what?
03:14 Q. A demonstration or a validation testing.
A. I've done demonstrations. But when I do demonstrations I can just actually -- I can actually just transfer child pornography. In my test I run the system, I actually download [Indiscernible] log. I don't have to show them the movie file
03:15 that gets downloaded. But additionally, we have offered a validation test -- although it's in-house, we've offered a validation test I think for [Indiscernible].
Q. So you have offered some access before to defense counsel, right?
03:16 A. Not to the software. A validation test which is documented.
The whole process, like I describe to our students, we'll test the software so they can be comfortable with the dates and times, the logs, what's logged. There's a whole validation process. And just like the students would see, both
03:18 the sharing computer and the investigating computer, we do that with video screen recording. So visually you can see that the software is connected to the sharing computer. The logs are shown. And so you can verify the dates and times are accurate. And then, finally, there's a packet capture.
03:18 As the defense brought out, that can be used to prove

single source downloading, which is the only thing that I saw other than the questions he had in his report was more of a what-if scenario, what if it was downloaded from someone else.

So that's the only thing I really saw in his report
03:19 that was any question as to the reliability of our software short of not finding a file, but clearly it was there.

So that packet capture is proof of single source downloading as your own expert said.

Q. But you've never let anybody do a packet capture, you never
03:20 let anyone have hands on the program. The most you've ever done is let them just watch your demonstration controlled on both ends from you.

A. Correct.

Q. Or by you.

03:20 A. It's documented in such a way it couldn't be altered. Hash values of all the elements of the tests are recorded and seen visually and memorialized [Indiscernible].

Q. Has the government asked you to be able to do that here today, you know, in this case?

03:21 A. No, the government never -- again, I got involved in this case I think after the motion -- the pending responses or motions were filed. It's only been a couple weeks that I've been involved in the case.

Q. All right. So when you do a single source download from the
03:22 IP address that you identify as a target computer, okay? Do you

know how long at that point that the source computer had that file?

A. No. If you had search results, a history recorded, you could have an idea of about how long. But normal BitTorrent communication, no, would not tell you that.

Q. And you didn't know -- you wouldn't know where they got it from, where the source computer might have gotten it from in the first place, right?

A. No. No. I mean, that's true with file sharing as a whole --

Q. Okay.

A. -- across the board, yeah.

Q. So it could have been downloaded by that source computer as a single file or it could have been downloaded in a batch. I think you testified earlier that you can download, you know, multiple files at one time, right?

A. Yes. Some torrents describe one file, as it was in this case, or it could be dozens or more.

Q. So it could be a situation where a user of a computer is downloading dozens of files, a whole batch of files and, you know, maybe one of it or some of it's child pornography, the rest is legal material.

A. That's certainly possible. That's the whole purpose -- that's why we get search warrants and do an interview.

Q. Right.

A. Because we'll never know that before the search warrant and -- we're dealing with the internet here.

Q. So I think you testified earlier -- so you say that it doesn't sniff data across the network in total, but you must be doing some sort of narrowing-down or winnowing process that only gets you what you're looking for which means by definition you're excluding other things, right?

A. No. I have a torrent. Although I'm the gatekeeper of all the torrents, each investigator has a physical torrent. They load it into a physical BitTorrent program, Torrential Downpour Receptor. It searches for download candidates and then it receives search results.

Done. That's it. But that's every BitTorrent client. That's different than saying like with a wiretap, a phone wiretap, you're listening to all conversations in and out. With a packet capture, as the defense expert described, that's listening to all the communication on a wire.

Here we are searching, issuing a search request to find IPs and receiving results and recording it. That's it. It's not like we're listening on the internet for any time any BitTorrent communication happens and I can somehow magically discern one from the other. That's not at all what happens. We just search and receive results. That's it.

MR. DONOVAN: Your Honor, if I could have one minute to consult with my expert.

(Brief pause.)

MR. DONOVAN: Your Honor, I don't have any further questions.

THE COURT: Mr. Humble, anything else?

03:38 MR. HUMBLE: No, Your Honor.

EXAMINATION

BY THE COURT:

Q. Mr. Erdely, you said that one of the concerns about allowing an expert to share or look at some of these things is that it

03:38 would expose hash values?

A. Correct. It would expose -- it's taken years to amass the instruction files, those torrent files that law enforcement are seeking out. If any of that --

Q. Aren't those -- I thought those were publicly available.

03:39 A. They are publicly available. They're not -- but what the public doesn't know is what areas we, law enforcement, exist in. We're looking for these 500,000, 2,000 torrents. To put that out there would give them the key to not get caught. We'd have to start from scratch.

03:39 Q. Okay. So you don't want them to know what you're looking for.

A. Correct.

Q. The other thing is, now, Exhibits 2 and 3, the logs, are essentially downloads of the exact same video?

03:39 A. Yes, sir. That computer was online sharing it over two

days.
Q. Why -- I thought -- you know, if you put out the request, why does it pull in from the same person twice?
A. And actually you can -- there are settings to avoid that.
03:40 If you downloaded the whole torrent from somebody --
Q. Yeah.
A. -- in our software you can say don't try to download again. But, I believe your question is more about why would -- why would the same computer come to us to be overly helpful and
03:46 share the whole file with us the second time when they had just done it the day before. Is that summarizing --
Q. Yes. And your initial log says we don't have any of it.
A. Right.
Q. But by that time, the time the second download happens, you
03:47 have it all.
A. Right. But that's a whole other investigative session. So, to remember, and we haven't really talked about it in this hearing much, IPs are dynamic. They change. I could have one IP address today and another IP address tomorrow. There is
03:47 nothing that is going to enable me to know, even though it's the same IP address, a day later. I don't know for certain it's the same individual.
Q. Okay.
A. They're dynamic and can change daily or even hourly.
03:48 Q. Now, we just have the logs that came from the IP address of

the defendant. In this same investigative session is it likely that this search or this -- not so much a search, but they received -- after inputting this torrent, this hash value -- received a number of other hits as well where there were other individuals now that they followed up on?

A. Yes. So the software isn't going to just sit there and investigate one person at a time.

Q. Right.

A. There are different programming threads that you could have multiple investigations going on at any given time. So, for instance, I could have through my web browser five tabs open with five different web pages.

Q. Uh-huh.

A. But tab 5 doesn't somehow get mixed up with tab 1. I see MSN here, I see CNN there.

Same concept. And Windows controls that. It's not even -- if there was an error in that, you would need to go to Microsoft and say why aren't you controlling your TCP connection.

Q. Yeah.

A. But it's separate tunnels, so to speak, separate TCP connections, so one would never get mixed up with another one or Windows is failing.

Q. And then lastly, I think you've covered this, but you said you had that bug maybe eight years ago or whatever and the

result of it was it just didn't work. It wasn't that it gave false information, it just doesn't work. Is that --

A. Right. It would just cause the program to stop working because -- to put it in context, Windows allows for, you know, the folder, all the folders and sub folders and the file name can't exceed 260 characters.

Q. Uh-huh.

A. So the programmer said, okay, we're gonna limit it to 260 characters. That's what Windows says. But the problem is other operating systems like a UNIX or Linux environment or Mac can have even longer extensions, so we had to account for that.

So programmatically they're accounting for the fact that some of these paths and file names could exceed 260, which doesn't make Windows happy, but we had to account for it because BitTorrent is not just unique to a Windows computer, it runs on Mac and Linux and all these other operating systems.

But that was the extent of the bug. And you're right, Your Honor, it would just shut the program down. It didn't collect false information or give us false negatives or positives, it just shut down. So that's a case I will never investigate.

THE COURT: Okay. Any follow-up?

MR. HUMBLE: No, Your Honor.

THE COURT: All right.

MR. DONOVAN: I do have just a little follow-up based

on some of these questions and answers. And I appreciate it, Your Honor.

FURTHER CROSS-EXAMINATION

BY MR. DONOVAN:

03:54 Q. You would agree that an info hash is different than a hash value for a file, correct?

A. It is certainly different.

Q. So the info hash is just saying, hey, I've got this information and you want it or vice versa, and we're going to

03:54 now have this handshake and hookup, right?

A. Well, it's more specific than a file hash. I just want to be clear. Info hash is different. It's a hash with information. But the information in hashes are the file names, the file sizes, the SHA-1 hash of every piece. So indirectly

03:58 the info hash actually defines the material being traded, whether that be one file or 100 files. So it's better than a file hash.

Q. Okay. So that's -- so an info hash is different than a file hash, right?

03:59 A. Yes.

Q. And then a file hash is different than the file itself, right?

A. It's the fingerprint or signature of the data.

Q. But it's not the thumb, it's the thumb's fingerprint, right?

03:59 So it's not the same thing.

A. (No audible response.)
Q. So, in other words, if you can get a file hash, does that give you the file?
A. No. The file hashing is a unidirectional thing.
04:00 Q. It's an algorithm, right?
A. Right.
Q. It's a 40-digit hexadecimal whatever, it's not the file itself, correct?
A. Correct.
04:00 Q. Okay.
A. The hash points to the file.
Q. Now, I think you testified earlier and correct me if I'm wrong, the name of the file is inside the torrent, right?
A. Yes. And the [Indiscernible].
04:02 Q. Okay. And so, for example, like on Exhibit I believe it was -- let me just make sure I'm getting this one right.
So on Exhibit 5 I believe, where it says "torrent file fragments," right?
A. Yeah.
04:02 Q. And it has the -- you know, the name right there under the name column.
A. Yes.
Q. Starting, you know, "022Asian," okay?
A. Yes.
04:02 Q. And then in the source column it's got the hash file

torrent, right?
A. It's -- basically what it's done is it's named the torrent by its info hash.
Q. Right. So that name is inside, like you said, the hash. It's part of the information that's in the hash file.
A. It's part of the information in the hash, so, yes.
Q. But again, that's not the file itself.
A. That is not the file --
Q. And you don't contest again that the file that supposedly was downloaded here two days in a row wasn't recovered later, right?
A. I don't contest that. Although the other exhibit shows it was there, the MRU. That's the file, that's not the torrent.
Most recently used, which was Exhibit 6, show you that file name including its extension. That's when you open the file in a video player, for instance. And that was on May 22nd, after the first investigation and just before the second investigation. MRU is the file.
Q. Yeah. Gotcha. Now, you talked about false positives. You would agree that just because a false positive might be rare, it's not impossible, right?
A. Well, statistically speaking it's 1 and 1.4 quindecillion or two to the 160th power.
Q. That's of two hash values not matching, that's not the same thing as whether or not there might be a false positive in a

software, which is a type of malfunction or bug in the software, correct?

A. Right.

Q. So I'm not asking the odds of two hash values matching, which I understand is an impossibly high number, I'm saying that just because a false positive might be rare within this program that we don't have access to, doesn't mean it's impossible.

A. (No audible response.)

Q. And I can --

A. There's so many areas a false positive could be, you'd need to define that further. Because the data we receive as hashed, it's impossible -- or at least two to the 160th power that that is not the data that belongs to the torrent.

Q. Let me put it -- can I put it this way? Okay. So you have these hash values which are indicators of the file on the computer, right?

A. Are we -- the info hash of a torrent, is that what we're talking about?

Q. Or the torrent. The torrent is not the file itself, it's an indicator of the file, right?

A. It's the instructions to download file.

Q. Okay. And we also have like this, you know, again most recently used whatever with, you know, the extension, right? But again, it's not the file itself.

A. That's the file itself was touched which caused an entry,

MRU entry.
Q. But an MRU entry is not the file.
A. No, no, no, you're right.
Q. Okay.
04:09 A. It's just proof that the file was there.
Q. And you've speculated that the reason the file isn't there and only these indicators are there is because perhaps it was deleted, right?
A. Correct.
04:10 Q. And that's possible. It's also possible it was a false positive; that the program reported the file as being there and it really wasn't. I'm not asking again about hash matches or -- I'm saying is that possible?
A. It's not possible because the detailed log -- there's no way
04:11 he could have sent us 226 pieces with the corresponding hash values unless it was present at that moment in time on his computer. So this, I say, no, it's impossible.
Q. I'd like to ask you a hypothetical. Okay? Let's say the Torrential Downpour Receptor, just like every other computer
04:12 program, whether it's Windows, Microsoft Excel, you name it, whatever, has a bug in it. And I understand you said there was only one. Let's say it has a bug in it, okay? And it's not performing properly. Those log files are generated from the program, correct?
04:12 A. Correct.

Q. So if there was a problem with the program there could also be a problem with those log files.
A. I don't -- I agree that if there's a problem with the program it could affect the log file. But what it couldn't do
04:12 is make 226 pieces match. There's no possibility that the computer at that IP address didn't possess that whole file because he shared 226 matching pieces. It's not a possibility.
Q. But the log files which says it matched 226 pieces, fair?
A. It is what it says, yes.
04:16 Q. Okay.
A. And so we would have had to get wrong and have it match 226 times. It's just inconceivable to me. I don't know how to better answer your question. I apologize.
Q. I guess my final question would be: So a false positive is
04:17 possible.
A. Anything's possible. But statistically speaking, I don't believe it happened here.
Q. I understand.
MR. DONOVAN: I don't have any other questions,
04:17 Your Honor.
THE COURT: All right. Thank you, Mr. Erdely.
THE DEFENDANT: Thank you, Your Honor.
(Witness excused at 4:42 p.m.)
THE COURT: Mr. Donovan, what would you like to do?
04:20 MR. DONOVAN: Well, Your Honor, I'm kinda torn.

Obviously I think this is complicated stuff. I think we've learned a lot today. I know my expert whispered to me that he's learned a lot today. So I think we might have some of our questions answered, but not all of them.

04:20 THE COURT: I'm -- you know, when you have an expert like Mr. Erdely come in, I don't get this stuff much, I don't think the government wants to produce him over and over and over, so it probably makes sense for me to write something. And if I'm going to write something on this, I think you should tell
04:21 me what you -- your position after hearing the evidence.

MR. DONOVAN: Well, and that's what I was getting towards, is I'm -- I think I'm leaning towards I'd like to get the transcripts, have some time to review those, I guess do a follow-up, you know, brief or, you know, position.

04:22 THE COURT: Transcripts? Can't you give me something faster? I mean, this case has been --

MR. DONOVAN: I know.

THE COURT: This is an 18 -- when was this filed, back in July of last year? And there were a lot of delays in getting
04:22 you as much as we did get. Then you got an expert.

MR. DONOVAN: I understand, Your Honor. And I do appreciate the Court's patience with this case because, again, at least from my perspective, this has been complicated and difficult to work through even with the expert because, again,
04:23 we have an asymmetry of information here trying to figure out

what's going on.

THE COURT: What makes this case unique? I mean, we have all these child pornography cases. Is it just that he's charged with distribution and the files he was charged with
04:23 distributing weren't found on the -- the files themselves were no longer -- or not found on his computer?

MR. DONOVAN: I think that's exactly right. I think what the big difference we have here is that they're pretty convinced that it must be because it was deleted. Okay?
04:24 We're --

THE COURT: There were a lot of files that were on the computer, correct? I mean, there's possession charges here.

MR. DONOVAN: Yes, later. Yes. Count 2 relates to the search warrant and the stuff that came from the search
04:26 warrant. That's a simple possession charge. Has no mandatory minimum.

Count 1 relates only to these two downloads from Torrential Downpour Receptor. And that's what was not located on the media. And so --

04:27 THE COURT: Did you know that there was -- 4, 5 and 6 showed that it was on the -- or at least there's pretty good evidence that --

MR. DONOVAN: Well, again, these are artifacts. You know, these are indicators, these aren't the files. I mean,
04:27 this is -- this is what I was trying to get on my rebuttal

questions there.

THE COURT: Yeah.

MR. DONOVAN: 4, 5 and 6 show things taken from the system through a -- basically a forensic program, right? And they're indicators of the file, they're not the file. I don't think it's being disputed here and I think he even admitted on --

04:27

THE COURT: So I guess my question is: Is this more a question of the search or are we beyond that now and this is a question of just your ability to assert your defense and --

04:28

MR. DONOVAN: I think it's two things. I think, one, it's the ability to properly prepare for trial, should there be a trial here, of the government witness who ran this program and says that these things were downloaded because, again, they're not later recovered, okay?

04:28

So the only evidence that the government's going to present about that is what this program did and what it supposedly observed and downloaded and generated logs about and all of that. That's how they're going to prove Count 1.

04:28

They're not going to prove Count 1 because it was located later on his computer. Count 1 is a distribution charge that carries a five-year minimum, so that's obviously the one that we're more concerned about.

And, I would also mention, Your Honor, what happened in Count 1 during this program running is the sole basis of the

04:29

search warrant that is then later used to form the basis of Count 2, to go get the warrant executed, locate whatever they locate and then charge possession.

So I think it relates more directly to Count 1, and I think that's what makes this case more unique than other cases where they do later recover the file or whatever. But it also does impact Count 2. And it impacts it on I think several levels, but definitely preparing for trial and cross-examining the government --

04:30 THE COURT: Are you suggesting that the program actually puts child pornography on the defendant's computer?

MR. DONOVAN: No. I don't think we have any indication of that. I'm not going to advance that. I asked a couple questions about that.

04:30 Again, I think the question for Count 1 is could this be a false positive, which is why it's not there when they go back later to look, versus he deleted it.

THE COURT: So even if it's a false positive, let's say, it's still probable cause.

04:31 MR. DONOVAN: Yes.

THE COURT: So --

MR. DONOVAN: So in that case it could still support Count 2. But then it would not support Count 1 because that would mean that it was never there. Count 1 is that he, on a 04:31 specific date, distributed this specific file.

THE COURT: Well, they'd still get to a jury on Count 1 because they'd certainly be able to argue from the logs and the search of the computer, the mirrored computer, the data they have there; that he actually possessed it, he just deleted it.

04:31

MR. DONOVAN: Yes, I think that could get to the jury. That could be arguable. That's where we're handicapped because we don't have access to this program and can't question its reliability, accuracy. I mean, this is the problem. Everything, with all due respect to the government witness, is --

04:31

THE COURT: Okay. Let's say it takes a week to get a transcript. When will I see your brief?

MR. DONOVAN: Well, Your Honor, I'm on vacation from August 23rd until September 2nd, so I think that's the day before Labor Day. I mean, I'll do it as fast as I can after that, but my, you know --

04:32

THE COURT: Okay. So how about September 10th. 15th?

MR. DONOVAN: Sure. I'm assuming that the transcript hopefully comes through.

04:32

THE COURT: September 15th for your brief, Mr. Humble?

MR. HUMBLE: Whatever you'd like, Judge.

I'll just say, we were told -- and I know it's on the recordings -- repeatedly when we were having these continued -- what am I -- adjournments to --

04:32

THE COURT: Status conferences.

MR. HUMBLE: Correct. -- that this was dispositive; that there wasn't going to be a trial. I understand --

THE COURT: This motion would be dispositive.

04:33 MR. HUMBLE: I understand things change.

THE COURT: Yeah.

MR. HUMBLE: But it was repeatedly asserted by counsel that this was dispositive, that there wasn't going to be a trial, but this was the issue that we were basically going to

04:33 battle out. Now that's not what I'm hearing. So....

THE COURT: Well, my sense is if he's -- if the motion's denied am I likely to see a -- then it's probably not a trial.

MR. DONOVAN: Well, that's exactly what I meant when I

04:33 said dispositive before. Obviously if we don't get this, that changes things drastically I think from our perspective and then it probably -- yeah, I don't know at that point how we could effectively even prepare for trial. If it's granted, then that would be a different story because then we could actually maybe

04:34 get even further answers than what we've gotten so far.

THE COURT: Yeah. 30 days after his. And the sooner the better. And then if you want to reply, 10 days later, Mr. Donovan.

MR. DONOVAN: Okay.

04:34 THE COURT: And I appreciate this is delayed, but I

take it there's been compliance. There's no noncompliance with conditions of bail as with most of these cases?

MR. DONOVAN: Correct, he's been --

THE COURT: And frankly I -- you know, this is very unusual. If the government needs to go through this on every child pornography case, that's -- we're going to see far fewer. You can't -- and the government has made the effort of calling an expert who frankly is acknowledged as the expert on this program. So I think since they've made that record I'll try and give you something that will have some value.

MR. DONOVAN: Thank you. I would just note September 15th's a Sunday. Can we do September 16th which is Monday?

THE COURT: Sure. Any day I selected that is a weekend, take the next day.

MR. DONOVAN: Okay, thank you.

THE COURT: All right. Anything else today?

MR. HUMBLE: Not from the government.

THE COURT: All right. Thank you, all.

MR. HUMBLE: Thank you.

UNIDENTIFIED SPEAKER: Thank you, Your Honor.

(Hearing adjourned at 4:49:46 p.m.)

* * *

C E R T I F I C A T E

I, JOHN T. SCHINDHELM, RMR, CRR, Official Court Reporter and Transcriptionist for the United States District Court for the Eastern District of Wisconsin, do hereby certify that the foregoing pages are a true and accurate transcription of the audio file provided in the aforementioned matter to the best of my skill and ability.

Signed and Certified August 30, 2019.

/s/John T. Schindhelm

John T. Schindhelm

John T. Schindhelm, RPR, RMR, CRR
United States Official Reporter
517 E Wisconsin Ave., Rm 236,
Milwaukee, WI 53202
Website: WWW.JOHNSCHINDHELM.COM

I N D E X

*****

E X H I B I T S