QUALIFICATIONS

(We want the expert to be seen as a credible witness and to state that he is in fact an expert in social media, file transfers, etc, so we can then later establish that the Box.com documents are not available to the general public).

Q: what company are you employed by?

A: ? company

Q: and what is your title at this company?

A: ? Examiner

Q: what roles do you perform as an ? examiner

A: I perform computer forensics and network security.

Q: so in your role you examine computers for forensic artifacts like communications, Internet history, system files, and so forth… is that correct?

A: yes that's correct.

Q: do you use forensic tools in the process of your examinations?

A: yes

Q: what forensic tools do you commonly use?

A: ? - EnCase, Forensic Tool Kit, Axiom

Q: and these forensic tools, they assist you in what way?

A: the speed of the process of an examination by parsing data, basically recovering different types of forensic data that I can use in the process of my examination without having to do everything by hand.

Q: so these tools allow you to be more efficient, to recover dozens, or hundreds, of different forensic artifacts?

A: yes

Q: so you would consider yourself an expert in social media applications, like Facebook and twitter?

A: in so far as the forensic artifacts it creates on computer systems and such yes I would.

Q: in the cases that you handle, is social media data commonly important?

A: yes, depending on the type of case it is.

Q: you would consider Internet history to be valuable in many cases as well, is that correct?

A: yes, Internet history is often a valuable source of evidence.

Q: with modern forensic tools, you can recover what people search for, in search engines like Google, Yahoo, and Bing, is that right?

A: yes, depending on if the data still exists in a way that is recoverable.

Q: and you would consider yourself an expert on how search engines work, at least in the data they leave behind on electronic devices, is that correct?

A: I wouldn't consider myself an expert in all the inner workings of a search engine, much of that is proprietary data. However, as to the data they leave on computer systems, I would, yes.

Q: and it would be safe to say that you have examined thousands of emails as a forensics expert given how common of an evidence source they are, is that correct?

A: yes, I've examined tens of thousands of emails at least.

Q: is it safe to say you would consider yourself an expert on email systems, at least the most common types such as Outlook, Gmail, Apple Mail, and so forth?

A: yes

Q: would you consider yourself an expert in cloud-based storage programs like Dropbox, ShareFile, and Box.com?

A: yes I would consider myself to have expertise in these services.

Q: and the forensic tools you use, they can recover data on computer systems and other devices related to these cloud-based storage applications like Dropbox, ShareFile, and Box.com, is that right?

A: yes that is right.

INTRODUCE EXHIBIT: EMAIL

Q: can you identify what the exhibit is for the court?

A: this is an email communication, dated September 22, 2015 at 2:43 PM, from Cesario, Thomas and to Rowe, Wesley.

Q: this email was sent by Thomas Cesario, correct?

A: yes that's correct

Q: and it was received by Wesley Rowe, correct?

A: yes

Q: and the sent time, as it sounds, is when the email was sent, is that right?

A: yes that's right

Q: what is the subject line say?

A: Subject: video

Q: and below that it has another line, what does that say?

A: Sensitivity: Confidential

Q: based on the demarcation of "Sensitivity: Confidential", would it be fair to say that Mr. Cesario intended this email to only be received by Mr. Rowe?

A: yes /or/ I cannot make a determination on what Mr. Cesario intended.

Q: what does confidential mean?

A: means to hold information in confidence, or securely between designated parties.

Q: modern email applications and services have security right?

A: yes they do

Q: and the security is designed so that people can have confidence that their emails are only going to be read by intended parties, is that correct?

A: yes that is correct

Q: if I sent you an email, I could have confidence that only you would receive it, is that right?

A: yes, as long as you type my email address correctly. The only other parties may be able to see it would be IT professionals who manage email for a company.

Q: if I sent you an email right now what it appear anywhere other than your inbox, like on the Internet or social media?

A: no it would not

Q: if I posted the email on a website, you could potentially find it then on the Internet though, is that right?

A: yes that's correct

Q: if I posted the email on Facebook for example, you could find it then, is that right?

A: yes that is correct.

Q: but simply sending an email from one party to another, with no posting or uploading anywhere else… That email is only contained in my mailbox and mail server, is that right?

A: yes, that email would only be contained in that mailbox/mail server.

Q: inside of this email there is a link to a Box.com account, is that correct?

A: yes

Q: can you read the link for the court?

A: https://nationwide.box.com/s/brajdu818uvivfxibbitld520ozx60ml

Q: would this be considered a URL, or universal resource locator?

A: yes it would

Q: what is a URL?

A: it is the address of a worldwide webpage, or in other words the address of a website or webpage.

Q: what does the acronym HTTP stand for?

A: hypertext transfer protocol

Q: and what is hypertext transfer protocol?

A: it is the foundation of data communication on the World Wide Web. It allows for information to be shared and located on the Internet, it is the language so to speak of the Internet.

Q: this link reads HTTPS at the beginning, is that right?

A: yes

Q: what does HTTPS stand for?

A: hypertext transfer protocol secure

Q: and this is commonly called HTTP over Transport Layer Security… Is that right?

A: yes

Q: HTTPS provides authentication of a website and its associated Web server that a person is communicating with, is that right?

A: yes that is correct, it means that the connection you have a secure with the website you are sending and receiving data from.

Q: so if I log into my bank account online, I would see HTTPS at the beginning of the web address, is that correct?

A: yes

Q: this secure connection, it has bidirectional encryption between a client and a server, is that right?

A: yes that is correct.

Q: what is encryption?

A: usually it is a mathematical algorithm that turns plain text, or what you could read with normal language, into a cipher, or in other words unintelligible data that you cannot read without the encryption key.

Q: are you familiar with what is commonly referred to as a man-in-the-middle cyber attack?

A: yes

Q: what is a man-in-the-middle attack?

A: it is a cyber attack used to either collect information while it is in transit from one party to another that is unencrypted.

Q: so this type of attack is used to eavesdrop or tamper with communications between parties, the fair to say?

A: yes

Q: in this case we see that the link contains HTTPS, the secure part of this protects against men in the middle attacks, is that correct?

A: yes that is correct

Q: so the secure tunnel if you will, this would prevent someone from snatching this web address to this Box.com account while it is in transit from one party to another, is that right?

A: yes that is correct

Q: and based upon your examination, you have no reason to believe that some sort of hacker got this information, is that right?

A: correct, I've seen no evidence that a hacker got this information.

Q: so just to clarify, this link represents a secure connection, with safeguards in place to protect it from hackers or unintended access, is that correct?

A: yes it does have security measures in place via HTTPS

Q: email is commonly encrypted as well, isn't that correct?

A: sometimes… In many cases it is but not always.

Q: most email applications have some form of security to protect your email as it is in transit from one party to another, so that isn't subject to a man in the middle attack as we discussed?

A: that is correct, most email applications have security.

Q: do you have any reason to believe that this email between Mr. Cesario and Mr. Rowe was somehow intercepted by a hacker or other malicious party?

A: I didn't do an examination for that, but no I don't.

Q: so to your knowledge, this email was transmitted as intended, from one party to another and not intercepted in any form or fashion that would make it available to anyone on the Internet?

A: that is correct

LIKE PUTTING DATA ON SOCIAL MEDIA

Q: there's been some discussion that receiving this email as a part of discovery is like posting confidential information directly onto social media websites like Facebook, are you familiar with that?

A: yes (?)

Q: if I put this web address, https://nationwide.box.com/s/brajdu818uvivfxibbitld520ozx60ml , into the search box on Facebook, would a search return as a result that would allow me to get to this link?

A: No *(If Yes - I did not test for that but it is possible - if he answers like this for any of the following questions just hammer him on the fact that he did perform a simple test of searching for this web address and the most simplest of forms ((on Facebook, Google, etc.) - And in with the question "you didn't consider it to be relevant whether or not you could locate this with a simple search on Facebook/Google.etc?", "as an expert, do your normally come to expert conclusions with no forensic examination?"))*

Q: if I search for this web address on Google, would it allow me to get to this link?

A: No

Q: if I search for this web address on Bing, would it allow me to get to this link?

A: No

Q: if I search for this web address on Yahoo, would it allow me to get to this link?

A: No

Q: if I search for this web address on Twitter, what it allow me to get to this link?

A: No

Q: if I copied and pasted this address directly into the address bar of a browser, it would allow me to get to this link, isn't that correct?

A: yes it is

Q: and this is the only way I would reasonably get to this web address isn't that correct?

A: yes that is correct

Q: so to be clear, searching for this link within the search bar for Google, Bing, Yahoo or other search engines would not allow me to actually get to this link, isn't that correct?

A: yes that's correct.

Q: and also, to clarify, if I put this link address into the search box and Twitter, MySpace, or Facebook it would not return a result that would allow me to get to this link, isn't that correct?

A: Yes that is correct, it would not work.

Q: in your examination did you locate any evidence whatsoever that this link was available to the general public on social media?

A: No

Q: in your examination did you locate any evidence whatsoever that this link was available to the general public by searching the Internet?

A: No

Q: as a forensics expert you deal in bits and bytes, hexadecimal and other technical forms of numbers, is that correct?

A: yes

Q: did you determine what the mathematical probability of someone accidentally, or unintentionally finding this link would be?

A: No I did not.

Q: the long list of letters and numbers at the end of this link, brajdu818uvivfxibbitld520ozx60ml, that's a unique series of numbers and letters associated with a particular link, isn't it?

A: yes it is

Q: if two different links had the same numbers as a part of the URL, or web address, it would go to the same exact place wouldn't it?

A: yes

Q: and if I changed even one of these letters or numbers, this link wouldn't work, would it?

A: no it would not

MATHEMATICAL CHANCE OF STUMBLING UPON THIS VIA SEARCHING

David to do the numbers part here

Q: since you can't find this link via search box for Google or via social media search boxes on sites like Facebook, you would have to take the first part of this URL, assuming you knew that in the first place, which is: https://nationwide.box.com/s/ … And then try random combinations of 32 alphanumeric characters to find this address, isn't that right?

A: Yes

END