Fox Rothschild Podcast

The Presumption of Innocence Podcast Series: Episode 3

The Science of Modern Digital Forensics

Featuring Matthew Adams of Fox Rothschild LLP and
Lacey Walker Jr, President of the Computer Forensic Practice LLC

Adams: Hi everyone, and welcome to "The Presumption of Innocence," a podcast brought to you by the White-Collar Criminal Defense and Regulatory Compliance Practice at Fox Rothschild. Today, I have the great fortune of being joined by my friend and special guest, Lacey Walker, Jr., who is the President of the Computer Forensics Practice LLC.

Lacey has many years of experience and a broad scope of expertise in connection with computer forensics investigations. Lacey is, to say the least, my go-to when it comes to computer forensics investigations.

Particularly today, we're going to talk about mobile forensics investigations. I want to present at the outset some staggering statistics that have been accumulated by Cisco in connection with their VNI Complete Forecast for 2021. Globally, Cisco predicts that IP traffic will grow threefold from 2016 to 2021, a compound annual growth of 24%. Something that I didn't even know existed: They predict that globally, IP traffic will reach 278.1 exabytes. That's not terabytes or gigabytes, but exabytes, per month in 2021, which is up from merely 96.1 exabytes per month in 2016. They also go on to predict that globally, internet traffic will grow 3.2-fold from 2016 to 2021 at a compounded annual growth rate of 26%.

What does that mean, and what is the impact of mobile devices on that? Just a staggering level of growth. Well, Cisco also says that global mobile was 7% of total IP traffic in 2016 and will increase to 17% of total IP traffic as of 2021. And obviously, some of the data from 2021 will be still analyzed and flow in here as we begin 2022.

As it relates to devices, Cisco says that globally, there will have been 27.1 billion network devices in 2021, up from 17.1 billion devices networked in 2016. As it relates to mobile-centric devices, Cisco also states in their forecast that globally, 43% of all network devices will be mobile connected as of 2021. They state that smartphones, in particular, there's about 6.2 billion in the world and accounting for approximately 23% of all networked devices as of 2021, compared to 3.6 billion devices and 21% of network devices in just 2016.

Now, Lacey, let's unpack that a little bit. That is just one staggering level of mobile connectivity. I know from working with you and working in a broad range of criminal defense and regulatory compliance matters that just about every case these days now has some sort of forensics component. But in particular, as it relates to mobile forensics against the backdrop of some of the statistics that I just read from that Cisco report, there is just this staggering amount of fluid data flying around in cyberspace. How can one possibly capture that, with such dramatic amounts of data like exabytes being talked about?

Walker: With regards to the mobile forensics, I've been doing this now for almost 20 years. If you look back at things 20 years ago, we had a few. The BlackBerry devices were big. The little handheld PDAs were also large about 20 years ago. But if you look at things today, everybody has a phone. Everybody has a tablet. A lot of people do a lot of work functions on those things as well as just personal things.

Adams: Everybody from sixth grade up has a phone.

Walker: Absolutely, absolutely. And, with that being said, it certainly makes the world a little bit more difficult with regards to getting your arms around where all the data is located, how to identify this data and preserve this data. So, from a computer forensics standpoint, we certainly come in, we help people identify where the information is located. iPhones, for example, you have a lot of information not only on the local device, but also you have it in the cloud itself. So, if we examine an iPhone, we also want to take a look at the cloud as well to see if there's any backup information there. One device can turn into two, three, four or five different avenues of things to look at with regards to mobile forensics.

Adams: Now in particular, we started talking about 20 years ago. 20 years ago, you had a PC that was plugged in. It required its own room and office and desk and cabinet. Then we kind of morphed into laptops. Now we have these devices that fit in our pockets, which have enough computing power – or perhaps more computing power – than the computers that launched the shuttle exploration to the moon.

Talk to us a little bit about the fluidity of that data and what that means from a perspective of examining the bits and bytes from a forensics perspective. This device can go with me anywhere now. It's not just simply something that has to sit in its own designated cabinet in a designated room at a designated location. Talk to us about the challenges that that fluidity provides. And then from a forensics perspective, how does that help us with investigations, or hurt us, as the case may be?

Walker: Sure. Certainly, with the mobile devices, like you said, you could take them pretty much anywhere, everywhere. You can have a meeting sitting in your backyard or outside in the parking lot. So, there's a lot of places where you can travel to and actually have your devices.

From a forensics standpoint, obviously, there's a lot of information stored locally on the device. From a forensic image standpoint, we can look at text messages, we can look at social media apps: WhatsApp, Snapchat, Facebook, for example. With a forensic image of a cell phone, basically, we're getting a snapshot in time of what's stored locally on the device.

Adams: Location data?

Walker: Correct. Location data is actually a very important thing on mobile devices. For example, any time a picture is taken, specifically with an iPhone, there's geographical location hidden inside of that picture. So, buried within all the metadata, there are basically coordinates of where that actual picture was taken. In addition to that, any time your cell phone accesses a cell tower, I can geographically locate where you were at any point in time on your cell phone. I've had several cases where that bit of information was very critical in identifying where a particular person was located from a cell tower point of view.

With regards to pictures…there's one particular case where there was a party and one person saying they weren't there and that they received the picture from someone else. But the picture metadata showed it was taken from their particular device, and I was able to identify the coordinates of when and where that picture was taken. So, there's a lot of information that is stored on the local device that can certainly help out or in some instances, hurt, with regards to forensics.

Adams: Yeah, I mean, I was reading in recent news about the use of certain messaging apps — which we'll get to in a few minutes — being a central focus in the case of a prominent securities regulator against a prominent investment bank. In an effort of certain traders to subvert certain compliance controls that were placed around their messaging systems, they were using certain commercially available apps in an effort to try to fly under the regulators' radar when discussing certain trading activity, resulting in an enormous fine.

We'll talk in a little bit about how that might come to bear and some of the hallmarks of an investigation when you start looking into those types of apps. But let's talk at a broad perspective for a moment, and start literally with the differences between the types of phones and mobile devices that we have on the market, this moment here in the present day, and some of the challenges that you, as a forensic investigator, might face based on that. I'm talking the differences between sort of the Apple iOS platform and an Android device. So, break it down for us. What are the primary challenges that you face when dealing with those two principal types of devices that are available on the market today?

Walker: With the Apple devices and Android devices, there certainly are a lot of challenges out there. For example, we'll start with the Apple iPhone. Past history has shown…I believe there were a couple of terrorist events where the government was actually trying to gain access to a phone in order to identify some information. Apple, to say the least, is a very secure platform. They work on security a lot, in a sense where they try to encrypt a lot of things. So, it certainly makes a computer forensics examination of an iPhone a little bit more difficult with all the security features that an Apple iPhone would have.

Androids: You have the Samsung platform, you have the Windows phones…it's a different level of security. But if I had to compare the two, I would say it's probably more challenging with the Apple iPhones than with the Android devices. There's a lot of products out there available to forensics people like myself that can actually get around a lot of the security. But in the grand scheme of things, certainly within the past 10 years, I see more issues with the Apple products than I would with the Android-based devices. With Apple, if you ever look at your iPhone, you're always seeing, "Hey, there's an update today." Well, every time there's an update, guess what? The forensics people will have to update their forensic software in order to operate and be able to interact with these devices. So, sometimes it's kind of hard to stay ahead of the curve with regards to these devices, whether it is the Apple iPhone or an Android device. Though, I've had instances where we got a forensic image, but we weren't able to parse it until a month or two later once the forensic software has actually caught up. So, you do run into those challenges along the way, and certainly if someone has updated their phone recently or prior to an investigation.

Adams: Now, in the traditional concept of digital forensics, we talk a lot about the ability to potentially restore deleted data and what is and is not recoverable. The classic example that I've

always been told and — sort of a guiding premise behind some of my work in the early days of digital forensics with the more static environment outside of the mobile platforms that we're talking about today — was that once you delete something, that goes into unallocated slack space and then when the device needs that memory, it overrides it. So, for a period of time, it is conceivable that something which a user may believe is deleted may in fact not actually be deleted and is recoverable.

How does that work in a mobile environment?

Walker: Well, that's a very interesting question. If we could rewind and go back, let's say, maybe a couple of years ago, a lot of what you said could actually correlate to the mobile device. For example, with the iPhones: If someone deleted the text message, we can forensically go in and a large percent of the time we can actually recover that deleted content. But as things progressed, software writers will update their code. They want to make the phone faster and smarter. Apple, for example, has actually changed how they store the text messages. Now, if something was deleted, the likelihood of recovery has gone down because the databases of where this information stored is basically overwritten a lot sooner, a lot quicker, in order to actually make the device run a little bit faster.

Adams: Is that due in large part to how much functionality these devices now have on the various processes that they can run simultaneously, for example?

Walker: Absolutely. You can see it with every new release of iPhone. They always say something is faster. Something is stronger. Something is more robust. Well, to get that level of speed, that level of having every little gadget on your phone, things would have to change on the back end. So, if they can minimize unused space, such as deleted content, and make your phone run faster, that's where they attack it in order to make your device run more efficiently.

Adams: Is there a correlation between the memory size of the device and the probability of success in recovering deleted information?

Walker: Nowadays, the answer to that is no. The way that the databases on iPhones and the Android devices are stored, the databases themselves are updated in somewhat real time now. It's done in the fashion that you want to have your devices run a little bit faster. You want to be able to access your data much quicker. They update things real time nowadays versus yesteryear when things stood there for a while and a forensics person could actually come in and retrieve and recover a lot of stuff. So, with the newer, better products, you trade off the ability to recover and retrieve that type of information from the past.

Adams: Now, modern mobile devices, to me at least, seem tethered in some respects to a parallel cloud universe where some of the data backs up to a cloud for lack of a more sophisticated way of saying it. How does that impact a mobile digital forensics investigation?

Walker: Sure, absolutely. Sort of piggybacking off of what we were just talking about, the deleted data, we always take a look to see, “Hey, is there a backup somewhere?” Sometimes people forget that they had backed up a device and we have a backup from last year or last month. Well, we can look at that backup and then identify any content that was deleted. So, with the Apple devices, you have the iCloud account. With the Android devices, it depends on the

device you have. For example, Samsung has a backup. Google Drive is also a backup avenue for Android devices. So, there's a lot of data up there in the cloud that, with some of the phones by default, will backup to these cloud repositories.

From a forensic standpoint, we don't limit it to just the phone. We want to see what else is out there in the cloud because a lot of time, there's a lot of rich information that's out there in the cloud world.

Adams: I would imagine that the cloud can somewhat keep you honest as it relates to something that may have been deleted off of the mobile device itself.

Walker: Absolutely. You know, I always advise clients, with regards to that; we want to attack things from multiple sides. So not just the physical phone itself. So, the cloud … I have a snapshot in time of your phone. I can then compare it to what you currently have and sort of identify what's there, what's not there. Also, in addition to that, we advise people, “Hey, if you think text messages were deleted, well, you can send a subpoena to the phone providers.” They may not have the actual text messages. They would have information with regards to messages being sent and received. So, from that standpoint, you could do a correlation with regards to timestamps of when messages were sent and received, and then review what you actually have from your forensic image to sort of say, “Hey, yeah, there were 10 messages that were deleted.” I don't have any image, but the phone records which were provided by an independent source, i.e., the phone provider, can sort of provide that additional information to fill in the blanks.

Adams: I remember being involved in a pretty large investigation with you back several years ago where we had to do a timeline analysis of USB drive access based upon some allegations of mass data theft from a more static digital environment, and I was fairly astonished about the ability of some of your forensic software to correlate various streams of data like you're talking about. I'd imagine with the mobile device and the comparison to the cloud, that's not you doing that manually. There's some software helping you, correct?

Walker: Yeah, absolutely. There's just so much data out there, as you had said in the beginning. To manually go through and do that it would certainly take months, if not years, depending on the usage of the device. So forensic software, it's pretty smart with regards to doing, as you said, the timeline analysis and filling in the blanks … doing comparisons between forensic images and actual content you get from a phone provider. So thankfully, the software has been able to stand up to the test of time, and improve over time, to make our job a little bit easier.

Adams: Talk to me a second about phone service provider data. I guess it's probably broader than just phones. It's probably mobile device service provider data. How can that be useful in a forensics investigation?

Walker: One of the things we had just mentioned, for example, is the text messages. A lot of phone providers — Verizon, AT&T, whoever is servicing phones — will have records of when messages are sent and received. They may not have the content, but they will have that additional information. In addition to that, we spoke earlier about cell tower information. They will also have that information as well. You'll see this a lot on missing person cases and things of

that nature where, “Hey, let's check the cell tower signals so we can identify where the person was last located.” So, all that information is stored with the phone provider.

For example, with Apple, iMessages aren't “with” the Verizons or AT&Ts of the world. They’re actually stored at Apple. The iMessage content is sort of a separate text message application, if you will, and Apple would have that type of information stored. So you have to think outside of the box, not just the Verizons of the world, but sometimes device-specific people would also contain useful information with regards to the phone.

Adams: It seems to me that there are lots of custodians of potentially useful information along the path, just by virtue of the fact that the device is mobile. Because, like you said, you have the provider who's giving you the connectivity. You have, potentially, the company that makes the operating system and some of the gears that make the device work. And then you have other separate third-party potential applications that would be running in that environment, all coalescing around potentially relevant issues in the investigation.

Walker: Absolutely. It gets kind of complicated with regards to, “What data do we need? Where do we need to get it from?”

I remember a case not less than a month ago where counsel had to subpoena six different individuals with regards to getting information related to an iPhone. The WhatsApp messaging is by the WhatsApp people. The iMessages were with Apple. The phone provider has the SMS messages. You can just look there, that's three alone that could actually be pretty useful with regards to the text messaging itself. We didn't even touch on the other apps. You have the Facebooks of the world, the Snapchats… a whole large universe of other applications that are out there that haven't even scratched the surface yet.

Adams: It seems to me that you have to be more of a detective now with the way that mobile devices work, perhaps than you used to have to be with those computers I talked about that stood in their own box in their own room. Now, you have to be looking for three and four different levels removed from the actual device itself.

Walker: Absolutely. In comparison to computers, mobile devices and tablets certainly have evolved with regards to where the information is located and what additional information is out there. There was just a traditional computer. Yeah, things update over time, but the forensic software can sort of stay ahead of the curve as well as a forensic practitioner. We know what to look for in a Windows operating system or an Apple operating system, whereas every day there are thousands, if not millions, of new applications that are being developed and provided to users to use out there. Sometimes, it's kind of hard to stay ahead of the curve with regards to all these different applications that are out there.

Adams: Inquiring minds want to know: End-to-end encryption for messaging apps. Can it be broken? Does it work? Are messages in those end-to-end encryption apps are actually more secure?

Walker: That's a very tricky question and a very loaded question. It all comes down to: It depends. It depends on the device itself. Recently, I was doing a case with WhatsApp, which has actual end-to-end encryption. The WhatsApp data was actually uploaded to the cloud, and

all that data is encrypted. All the forensic software in the world right now currently cannot access and pass that information because WhatsApp has recently changed how they handle the encryption. It's one of those things that we spoke about earlier where, yeah, we have the data, but we can't actually tell you what the data is until the software is updated. Sometimes it will take months for a forensic software provider to update its software so that you can interact with it with the new encryption. There are always backdoors with regards to encryption. There's certainly a lot of tricks that we use in the field with regards to gaining access to some of this encrypted information.

So, to answer your question: Yes, encryption is a huge problem. There certainly are ways or workarounds in order to gain access. It certainly has made our job a lot more difficult, but, there's a way in methodology for everything. But there are newer applications out there that I can honestly say, right now we're waiting for the forensic software to catch up to.

Adams: I remember reading about a high-profile case in which the end-to-end encryption application was utilized for messages in question. But unbeknownst to the people communicating, logs of those communications were being created, generated and stored in a way that was completely accessible and essentially undermined the entire intention of using the encrypted app. So, talk to me about that.

Walker: Yes, certainly. I recall that particular case and a lot of people … you've got to read the fine print with regards to how these applications work. Yes, in the end, it's encrypted. However, a lot of times information is stored somewhere else, unbeknownst to those individuals, and can be accessed by either subpoena or forensic practitioner in order to circumvent the actual end-to-end encryption. A lot of times, we get cases where the WhatsApp information, for example ... if it's stored on an Android device, it's a little bit more secure; if it's stored on an iPhone device, there are a lot of applications out there that could break that encryption and allow us to parse out that information and review what content is in there. A lot of times this information is backed up to the cloud, and people don't realize when they back up information to the cloud, sometimes it's not encrypted. What's encrypted on your phone may not be encrypted in your backup. Those are certainly areas that we take a look at with regards to being a computer forensics practitioner in order to get around the issues of encryption.

Adams: What is the most typical thing that you pull out from a mobile forensics investigation? What are you most frequently looking for in connection with those types of investigations?

Walker: It really varies. Each case is a little bit different. A lot of times people just want to see the communications. So, we have the various text messages, WhatsApp messages. There's a whole other community of different messaging applications that people use with regards to communicating with each other, and they think that, "Hey, if I use this particular app, it's not going to be found on my phone or it's stored somewhere else." And unbeknownst to them, we can actually see that communication and we're able to get that data. The majority of the investigations that we get, it's more or less the communications that play a significant role. Outside of that, certainly, phone call logs are very important and crucial. And, actually, web browsing history. Believe it or not, people do a lot of things on the internet and with the forensics of these devices, we can actually analyze and see what the person was looking at on their device at certain periods of time.

So, those are probably the three main areas that we touch on in investigations. Overall, I think the communications part of it is the probably the higher profile with regards to these types of investigations.

Adams: Well, I know that you and I have been working together long enough that we've seen the evolution into these devices and some of the new types of data that we've brought to bear to use in various cases. Again, I said from the outset that it's really the exception these days where there is not a mobile forensics component to the evidence in a particular case, and not the rule. It's virtually every case where we're seeing these types of issues come to play.

What's next in mobile forensics? Where do you see the field going? Where do you see the evidentiary value evolving? What's next?

Walker: You'll see a good trend of…there's applications out there that can sort of mimic cell phones. So, for example, Google Phone is actually a phone application that you can use on your iPhone or your Android device. You can make phone calls, you can make text messaging, you can access it from a computer. So basically, it's making your mobile phone even more accessible, even if you don't have your mobile phone itself. I think that would be more of the trend: More accessibility.

In addition to that, you have the smartwatches that have played a significant role as well with regards to forensics. We get a lot of information off the smartwatches that people aren't aware of. If you delete something on one thing, unless, say, your watch wasn't on, we can pull your smartwatch and we can actually get that type of information as well.

The more difficult things that we're seeing… the trend that's going now, again, it's going to be more of the encryption, more of the software being updated and the lack of the forensic software actually being able to keep ahead of the curve. You're always going to be maybe a step or two behind because, obviously, there's a lot of testing of these new applications, and making sure that we can actually access and view content. So, just trying to keep up with the curve, is the trend that you're seeing now, especially these devices getting new operating systems, the latest and greatest, and increasing the speed of these devices.

Adams: Well, from someone who loves to use digital evidence in my cases – and you know that because you've testified at trial with me, and we've had certainly some interesting experiences together – what I'm hearing from you is that there's more potential sources developing virtually every day of digital evidence out there. As this big concept of big data evolves, we're going to have more and more buckets of potential evidence. I guess the converse of that is something that I often tell my clients is, if you're not willing to see whatever you're writing in your digital world as Exhibit A in a court filing, you shouldn't write it.

Walker: I agree with that. I always know if I talk to kids in the community and stuff, I always tell them, "Hey, if you don't want your mother to read what you have on there, don't put it on your device."

Adams: Well, Lacey, I can't thank you enough for joining us today, and I think we could probably spend all day talking about this subject. There's a lot to unpack, for sure. I look forward

to having you potentially back when we have some new developments. Thanks for the great overview today, and thanks everyone for joining us on “The Presumption of Innocence.”