834

Wed, 6/23 9:10PM 1:02:29

SUMMARY KEYWORDS

phone, data, forensic, picture, messages, application, case, photo, recover, cell phone forensics, create, evidence, deleted, device, location, pull, record, information, searches, utilize

00:00

Hi, I'm Mark Dania with VISTA forensics and today we're going to be talking about cell phone forensics, a little about myself. I hold certifications in computer forensics, cell phone, forensics and sailor location technology. Those are the letters after my name. I have also testified as an expert witness over 30 times in state and federal court qualifying is a computer forensics expert, a cell phone forensics expert, a photo forensics expert, a video forensics expert and a digital forensics expert. And I teach continuing education and continuing legal education classes across the country every year, many of them and I've written a few books, which you'll see photos of at the end. But today, let's hop right in and begin talking about cell phone forensics. I like to begin this class with this falling case example. And the reason I like to do that is it has multiple forms of evidence that are used together holistically. So this includes call detail records. Now these are a super phone bill full of information that you don't get with a standard set of phone records. We will talk about that a little more in detail later in the class. But just to note, if you ever need the language for that type of information, we provide that for free, so feel free to contact me to get that this also has driver logs from a trucking company, and the cell phone data itself that had been recovered from the phone using forensic software. So in this particular case, a trucking accident occurred a truck driver hit a plaintiff's vehicle, we were retained by the Council for the trucking company. And in this case, we examined the opposing expert report and the evidence related to it. So the plaintiffs claim was that the drivers fatigue was the cause of the accident, and also that the driver was distracted at the time of the accident by using their cell phone. Now the claim that they were distracted by the use of the cell phone comes from the following. They said that the user was on the phone, using the application I Heart Radio contemporaneous to the time of the accident. The reason they said this is that there is an album cover created at the time of the accident. Now, if you've ever actually used the I Heart Radio application, you will know that when it switches from one artist, let's say Justin Bieber, in this case, to reanna, we see that photo there to fit switches, songs, and it's a different album, what changes automatically the album

cover. So we were able to prove based upon how this phone works and how the application works, that No, in fact, this driver was not on the phone utilizing this application, they did have iheart radio running. But the changing of the albums was an automated process of the application itself and had nothing to do with user activity. Therefore, this goes out the window that can't utilize this information is no good for their purposes. So following this, they attempt to take the driver's logs like we see here, coupled that with the phone records, and these this expert posing expert smashes all this data together to produce this. And this is the log of activity, whether he's driving whether he's sending messages or making voice calls. And he puts all that together to create this sleep analysis. So here's the claims by this expert that this driver could only have slept on Sunday, for example, for two hours and 23 minutes, an hour and 30 minutes and an hour and 16 minutes. So this odd kind of Faysal sleeping method. Obviously not very much sleep throughout the day and no gap of continuous sleep. But as with most things in forensics, the devil is in the details, especially with digital forensics. And what this expert failed to do was to remove incoming activity from his analysis. So what does this mean? This means that by removing that incoming analysis, you would have normal sleep schedules. Be here's why. When you go to sleep and you put your phone on the bedside table, are you receiving emails and sometimes text messages that you have to answer first thing when you get up and other important stuff? Yeah, it's happening all the time. But if you remove all that out, he had a normal sleep schedule. You're not awake when you're receiving all those. The only way you can attribute activity to someone is outgoing activity or activity that shows someone with a phone in their hand doing something. Incoming activity does not show that

05:00

Now when you're dealing with cell phones, they are unique. They are different than computer technology, they do share much in common with computers. But every time a new cell phone comes out, or a new model, a cell phone comes out, it has to be reverse engineer. So basically, we had to get the data off of it by forensic tool companies. We all remember a time when there was much less standardization than there is today. Luckily, today, we basically have the Android and the iPhone based systems, right? iOS and Android, we don't have 8000 different operating systems and models of phones, if you ever remember having to go find a charger for your old phone, where you had to go to a gas station when those big spinning kiosks, things and find the one charger that fit your device, it was quite challenging as compared to today. So that does create some complexity in that sense, in the sense that there's a lot of phones that come out. And there's lots of updates, and it's not as necessarily accessible as computer technology. However, today, there are so many phones that we can crack the passwords on in seconds and recover tremendous amounts of data, including deleted data that this is less of an issue than it used to be even a few years ago. Now phones do have some unique preservation issues. When you're collecting this data needs to be done correctly. For example, a phone first needs to be put inside a Faraday bag when you're going to collect the data. Why would we need to do this? Well, when

you take that phone and you put it in a Faraday bag or a Faraday cage, what it does is it prevents that phone from receiving signals of any kind, whether it's wireless signals through a wireless network or through cellular signal, that means no new data can get in and no data can get out. Okay. And there's some important reasons for that. But this is a radio frequency shielded back and works on the same kind of idea in technologies, your microwave, right, you put your food in your microwave, and you cook the food and not your head as you're looking through the glass to see if that hot pocket is getting just the right temperature. So simply turning that phone on, can destroy data permanently. Right. And this is one of the reasons we want to put it in a Faraday bag and get that device in airplane mode. As soon as possible that is acceptable. To do that. You need to make sure that it's an airplane mode with wireless networking turned off though, because we all know you can get on a plane in airplane mode, and have the Wi Fi turned on these days. So you can access the internet, do messaging and so forth, that also needs to be done. But if we look at our two photos here, one, I've had this happen in actual cases, you can remotely wipe that phone, from your online accounts, you can go to your Apple account or your Google account and wipe your phone remotely in cases lost or stolen. Further, when you're dealing with less sophisticated phones, let's say your pay as you go phones, your flip phones. A lot of times it works on the conveyor belt type system as far as the data that exists on the phone. That means as new data comes in, you can delete the oldest data to make room for the new. Now what if you care about is that oldest data is potentially lost forever when this occurs, he may not be able to recover it that's highly problematic when you're trying to preserve evidence as an exact snapshot of how that data exists when it was collected. So what should happen, what should happen in almost every instance is that phones should be collected by whoever gets there first, whoever that first responder is, or whoever's there to collect the evidence. Under there's no concern a passcode lock, you just turned it off, or the passcode is known. Those are very acceptable. That's totally fine to do that. On many phones. Like I said, once again, we can crack the passwords on those anyway. However, in some instances, and this really applies to law enforcement only in every sense, it's the only place I've seen that utilized. And that's the following the phone is is taken out of a custodians hand or a suspects hand. And they're concerned about a passcode lock. So they just take that phone and they'll wigger their finger across it back and forth to keep it active. So it doesn't lock until it can be hooked up to forensic software. And the data can be collected from the phone. This is considered acceptable to do that. Once again, you're likely never to see this. It is rare for that to actually occur.

09:40

Now,

09:41

what we see happen quite often, however, is what I call phone forensics. This is where that first

responder, whoever they may be thumbed through the phone at the scene doing some forensics, right. The problem with some forensics is that a lot of times it has no accompanying doc mutation the person doing as no forensic training and no clue. There's a whole lot of problems with this. And we're going to talk about how to challenge manual examinations, which this is included in that later. But just know that this is highly problematic. The main reasons it is highly problematic in his report language was state is that when you're going through that phone with your thumb without any kind of forensic procedure in place, I later on as an opposing expert, or as the expert even on that same case, if someone had this before me, would not be able to tell us something was created, deleted or manipulated, intentionally or unintentionally through ineptitude. We don't have that perfect snapshot in time of data that we want. So as we get data from firms, there's different types of forensic acquisitions that can take place. One is a logical acquisition, this only gets still existing data sort of, okay. The reason I say that is it can recover deleted data, deleted data that's in logical space, when you hear logical space, this is just the the area of the file system on the phone that you have access to that's not deleted on that device. Okay. Logical space, still existing data, but you can recover deleted data. And the reason is, is because most applications on your phone work in a database type system. So what happens is that when the you tell the phone to delete something, and the phone automatically says to delete it, it doesn't actually delete it, it just marks that data and says, Don't show this to the user anymore. And it says potentially, when I need room to store more information, I can overwrite where that data lives in order to make more room. Now, you can simply recover that data from these databases and rebuild and recover messages, pictures, photos, videos, all types of different data that exists there voicemails, you name it, are in these database systems, so you can get deleted data, even if you do not get access to deleted space. There's also a filesystem acquisition now filesystem acquisition, we'll get more raw material, so to speak, you know, location type data, some other things, some other files that allow for some advanced analysis. And finally, there's the physical acquisition, this kind of gets everything right is getting all those logical files, and logical files, you can think about as the files in your filing cabinet, you can go open the filing cabinet, pull these files out, make copies of them, it gets deleted data. deleted data is different than your logical data deleted data inside of those databases, like we talked about in some senses. Once again, it works on the same principle, you delete a file and marks in the big database that keeps track of everything on the phone. And it says where that file exists, I can overwrite with new data when I need room, but it doesn't delete anything. So forensically, we just rebuild that and get it back, then it also has data recoverable from unallocated space. Now, let's say you delete a file, and the database entry related to it that we would normally use just to rebuild it quickly is gone. That means to get data out of unallocated space, you don't have a pointer to get there. So what you have to do in that sense, is you have to then use keywords and try to recover and carve out deleted files such as pictures, videos, messages, and so forth. And a lot of times, you can recover extensive deleted data from those places, it just takes a little more effort and work. Now, there's also chip off in j tag J. Tech stands for Joint Task Action Group, I won't bore you with the details. But more or less, here's the scenario on many phones that appear to be damaged. Beyond

recovery, like the phone you see here in this photo, we actually can recover the data from this. And the reason is, is that we can crack open the phone, pull the chip off and get the data that way. There's also other methods to get the data from things like this using that Joint Task action groups simply like you had an iPhone with a broken screen, you can't do the passcode. And maybe the charging port is broken. We can repair the phone to the extent where we can hook

14:40

it up to forensic tools to get the data back in that fashion also. Now even talking about forensic acquisitions, in general forensic acquisitions require a lower level of expertise and you might think, about 80% of phones are pretty easy to get the data off of using these very advanced for In the tools that are available today, but 20% are significantly more difficult. But where are the real expertise comes in as an analysis. This requires the real skills, right? It's not like just hitting a button, the forensicator Pro find all the evidence or playing a video game, it is complex. It's complex, because you need to understand all the hundreds and 1000s of types of forensic artifacts that can be recovered from the phone, what the data means, and especially how the timeline works, because times in electronic devices don't work the way you think they should work many times, in my opinion, if anyone's going to talk about the time something was created, or modified, or whatever else on an electronic device, they should have to qualify as an expert to give that opinion because it's simply too complicated to to testify to as a fact witness. Here's an example of analysis. This is a deleted file, we're looking at it from a forensics program. And I can look at this and see a JFIF at the top, and I know this is a picture, I would grab that select it drag all the way down real far where you can't see, grab what's called the footer. parse this out correctly. And what you have is the picture here is you see, so we see that's a recovered deleted photo picture of this, this nice view that you see there, the beautiful clouds and the cityscape. And that's what would recover by rebuilding this by hand. Another example is from the case that we did a few years ago, one of our examiners was the first of my knowledge to ever do this is that there was communications between two parties, a lady and a doctor. And it was claimed that the doctor did inappropriate communications with this lady. and in this situation, we had heard devices only. So we had a phone for iPhone, or iPad, or Mac, desktop or Mac laptop, and iPod Touch. And she's switching between all these devices in different applications to chat. And it's a very complicated time when we pull all of it. And there's gaps, though there's gaps in the communication that don't seem to make sense for us to be able to truly show that there was no wrongdoing by this doctor. And what we were able to discover was that there was communications inside of the application words of friends. Now, if you're familiar with words, with friends, this is a game you can play with anybody all over the world where you play Scrabble back and forth, basically, but it has chat functionality. Well, this isn't necessarily parsed by forensic software. So this database had to be rebuilt by hand, we're able to recover that information, put it into the extensive timeline of all the other communication and show conclusively that on the messaging, there was no evidence whatsoever of inappropriate communication. Now, as far as it

goes with recovering data from phones, the last resort that we use as forensic examiners is a manual examination. On the flip side, it's possible that this is the most common type that you see, this is our last option. But regardless of whether this is what you're doing yourself, or you have a custodian doing to self collect some messages, or you receive it from a client. Or if we're doing it, it should follow forensic best practices, one, so you can protect yourself from an opposing expert who could challenge it. And we have challenged these types of examinations many times. We'll talk about that later. But right now let's talk about how it should be done and how the appropriate means are to actually perform a manual examination. So what is it first of all right? Well, you've got a external video camera and external camera. And you set it up like you see in this here.

19:07

And what you're trying to do is take pictures of the screen itself from the phone as you manipulate the phone. So you're going through the messages, you're going through the pictures and taking pictures with that separate camera. You never want to do screenshots from a phone by clicking the home and lock button on the iPhone, you're creating new data, which is overriding other data, you're causing a lot of other issues as far as the integrity of the data on the device, always want to use a separate camera to do that. But here's the important parts. One, you got to take those pictures. And the second thing is that you need to have that video recorded your entire process of examination from the time you pull it out of evidence. So the whole process of taking the pictures until the end when you put it back away. The reason is that this is your verification that you have not created, deleted or manipulated anything on that intentionally or unintentionally. Remember that when we're doing the other forms of acquisition that physical, logical and file system, now we're using forensic tools that give us these mathematical algorithms are run against the data that we can prove that this data has not been tampered with. And that isn't good, and so forth. You can't do that. If you don't do it, right. And the only verification you have if you don't do that is the video. So you got to have a video, absolutely have to have a video when you're dealing with a manual examination. All right, now, let's shift gears. And let's look at some of the types of data that can actually be recovered from these phones from within forensic software. What we see here is an example of location data. This is wireless networking. So you see Google Play YouTube, those are the applications that are being utilized. While connected to a wireless network. Where the name of the wireless network we have some other very valuable information. But we need to understand is that these are typically today on modern phones, geo located to with with latitude and longitude coordinates associated with the wireless router your phone saw. So for example, you are riding through a neighborhood riding through town and your phone's popping up asking, Hey, would you like to join this network? Depending on your phone, not only is he recording the fact whether you connected to one of those is potentially recording that you saw a network even if you never connected to it. So you go to McDonald's and a pops up? Would you like to join the network and you say, no, it could still record the fact that you saw

that network. The average broadcast range of a wireless router like in your home, how long how far it will reach out and connect those about 150 feet. So that's this gets you very good granular location data to about 150 foot radius, where you can put someone at a particular date and time. So it's excellent for location data. There's also so much location data, even related to your health applications, your wearable technology that gets sucked into the phone to your steps, so on and so forth. If you have Uber if you have these other applications that are pulling application information that can be recovered from the phone as well. So use your imagination will show a few examples of this. But there's so much I can no, there's no possible way I can show it all of you in an hour long class. But here's an example of those wireless routers. And as you see here, this is from an actual case, some murder case. And on that left side, you see all those yellow pins. That is where the suspect drove up through those streets, went to the crime scene, committed an act. And then left on the right side, each one of those is a wireless router at a person's home, that their phone saw timestamp in geo located putting them all over that location area when they're not supposed to be there. You also have location data from Google Maps. So you have the timestamp the geolocation data, where you were searching to go, you have location data being recovered from multiple sources on the phone itself. This includes seeing cell towers, and different types of harvest data, the wireless networks like we're talking about and GPS coordinates. Now remember your phone today, if you have a modern smartphone has a GPS chip in it. That's why you can utilize it like you would an old TomTom you put in your car. It's better than that in reality, because it's using not only GPS, but other forms of location information. So it's extremely accurate when you get GPS location details is much, much more accurate than the type of information you'd get from a call detail record, for example, which we'll talk about later. But that GPS location data is fantastic and very, very accurate.

24:05

Here's some more examples of location data that have been extracted by cell Brite forensic software. And you have latitude and longitude coordinates and the applications that you were using at the time during those different sessions. So as we go along, we can also see user accounts. Now if you've ever had a case where someone says I only have one email, I only have one application that I use, and you examine the phone and you see they have multiple email accounts, they have 20 or 30 different social media applications that they utilize. We can absolutely recover that a lot of times many times with their friends lists their communications and so forth, as well as potentially the passwords for each one of those. So this gives you a lot of information on additional areas of potential interest to subpoena to get additional data so forth, a really excellent source to kind of see the full holistic approach to all the forms of evidence that you could get if you wanted

25:07

to.

25:10

Now searches searches obviously are extremely important in every kind of case, what a person is searching for is invaluable information. We see here a few different examples. And what I really want you to see is like in the Play Store in our image on the left, these are applications that someone's looking for fake text prank pranks on your phone voice changes that have become important later, we look at some case examples. But we can see the applications are looking for. If we go to YouTube, you can see what they're searching for inside of YouTube as well. Now remember, YouTube is the video repository of all human knowledge these days, you want to learn how to fix your car, how to build a deck, how to feed your turtle, cage, whatever, you can learn it on YouTube, including forensic case examples that we have, how to behead your girlfriend, literally a search before someone beheaded their girlfriend. We've also seen a case that I did, which was an embezzlement case, the lady literally Search For how long will I go to jail for stealing X amount of dollars from the company I worked for. And it was the same amount of money that she was accused to his stolen, literally search for a sign of YouTube. So we also obviously have you look in the bottom right Chrome, Safari, any of your normal browsing applications, it's going to recover those searches as well what you're typing into the search bar. But in general, think like this, if a program has a search bar, regardless of the program, it could be the Facebook search bar, the safari search bar, anywhere, there's a search bar if you're searching inside of that as the high probability that that is going to be recorded by your phone. And it's also highly probable that we can recover the deleted searches that are on that phone as well. One quick example of the value of these searches, we worked a case we were retained by the Council representing the trucking company, young lady had hit a 18 Wheeler. upon impact, she did die. But when we examined her phone, we were able to see that at the exact moment of impact. She was searching for the obituary of a friend right before impact mean literally, the moment before and back, she was on the phone and distracted. There's also internet history. Now here's just another example of some of the Google searches alone that were recovered. Internet history, even a short session of maybe a minute can create dozens of records that are all timestamp because it's not just one page that the internet's pulling down is pulling down a lot of different information when you do that. So we can see with great detail what someone's doing on the phone, when they access the Internet through a browsing application, such as like a Safari or Chrome. Okay. Quick case example of how that's valuable. This is a trucking case as well, where the truck drivers driving down the road. And he's in Facebook. And he clicks on a link inside of Facebook that kicks him out to a web browser. And in the web browser is a game and the game is what nationality Should I really be based upon my favorite pizza toppings or something like that? And he starts answering the questions one by one and we can see all of this in the internet history and when he hits to see his final results to find out what nationality he should truly be a plow, sir, an intersection harming a whole lot of people causing some severe bodily damage and obviously

property damage as well. All right, now, let's look at call logs. No surprise that call logs are valuable and that they can be recovered from a phone I'm sure you assume that are ready. Now a few things to note everywhere we see that red X is a deleted recovered entry from the call logs. And further what I really want you to see is the very bottom call, which I've kind of blown out to a bigger picture on the left. You see this call the duration of it last for 000000 seconds. So what is this? If you've ever accidentally called someone than hung up that call is long enough to record the fact that you made the call on your phone on your actual phone itself. But that call did not last long enough to create a record anywhere else. It did not last long enough to create a record in your phone bill or call Detail Report. So if you need to know if someone had a phone in their hand Adam ticular date and time The only place you're going to get that information for this is from the phone itself, you're not going to get that from any kind of subpoenaed record didn't last long enough to connect to the cellular network.

30:12

And obviously, messaging messaging is of huge importance in so many cases. A few things to note here, one everywhere you see next is a recovered deleted message. You see how the parties all the names are in red. That is because this user had deleted their address book entirely. However, we recover the address book, we're able to rebuild it back to the numbers they were associated with. So we knew what every number was named by this user. If you've ever had a list of 234, or 500, phone numbers, you got to figure out who's who at the zoo without a name already associated with it, it can be extremely frustrating and time consuming. So we have all that information. To our right, let's look at the analyzed data section. And really a couple things really to note. One were you see I messages, we have 28,000 if you look at the bottom, you see SMS messages about 13,000 SMS messages or short message service messages. These are transmitted via the sailor system in such a way where they can create a record of being sent or received in a call Detail Report or phone bill. So you may have a record of that without ever having the phone. However, I messages like your kik messages, your skype messages or any data based data based messaging application will not create a record you can get an A phone bill or call detail record. The only way you'll know that these messages were transmitted back and forth is to recover it from the phone, perhaps the iCloud account or something like that. But you're not going to get it in the subpoenaed record. Okay. So that's 20,000 of these messages. That's even more than the SMS messages down there. If you've got an iPhone, the green messages that come in, those are SMS, the blue ones are iMessage. That is data transfer. So no record anywhere else but the phone. This is particularly important because younger generations are much more likely to use Instagram or other applications to do their communication and chatting and not standard text messaging, ultimately, which means to get a full comprehensive view of all the messaging usually have to get the actual phone itself. So we also have installed applications to know what someone has installed on the phone can be very valuable, too. I'll give you a quick example of that. We worked a case where a gentleman was accused of putting a GoPro webcam in a lady's

dressing room. Now we got his phone, he said I never did that. I was not my phone, whatever. We examine the phone Sure enough, there's no evidence of that GoPro application. However, we recovered artifacts of the installed application related to a GoPro able to recover that and then link up that specific installation has as of been connected to that specific camera in the dressing room. So conclusive evidence there that that had actually been connected at some point to that very camera the

33:32
phone had.

33:35
Also pictures, pictures are of great value. Obviously, for many reasons, a few things I want you to know from this photo. Look at that first picture, we can see that the camera making model or an LG Electronics, bm 670. So the making model will be the phone that took the photo, we have the capture time Now pay attention to this. If you have a photo and you see the created time that is not necessarily when that photo was taken is probably not when the photo was taken, okay? that relates to the file system that the device The photo was on. Okay, so if you copy that to a computer or phone or other things like that, there's lots of exceptions. But the date that it's comes to exist somewhere else is the created date. It's not the date that it was taken, you have to look at the metadata and metadata is data about data like metacognition is thinking about faking it special data inside of a file that you can access using the right tools to see particular information about a file. So the capture time is the actual time that that photo was taken the capture time, not the creative time you got to get that from the metadata. We also see that the latitude and longitude are inside of this photo too and the metadata. This allows us to geo locate where this picture was taken at a particular time. Most photos and most cameras, whether you go buy a DSLR camera or digital camera or you buy anything else will have that capability. Now, the reason being is so that when you go look at your trips or whatever else, these fancy applications like Amazon photos can can show you where you were and all this other neat information. So you can, you can look back in your memories and so forth. Another thing to note is that second picture, the Samsung sphc, may 20 took that picture. Now, let's say that that second picture, someone's trying to say, look at this, I took a picture of this, look what happened? Well, we'd look at this and say, No, you have LG Electronics Vm 670. Phone, you didn't take this picture. Plus, there's no capture to capture time or latitude and longitude. This was probably in this case pulled from the internet. And now you're trying to pass it off as a picture you actually took. So the ability to authenticate photos, the other lot of capabilities that can be done doing that, utilizing cell phone forensics and pulling this information. Now we also have powering events. Now there's even more events in this available today events that allow you to see when the phone was held up and down when was held long ways you can see the phone was was turned on. screen was

powered on screen was powered off, if you hooked up bluetooth headset and so forth. And when that occurred, lots of information like that. And powering events is just one example of that. The reason I showed this is perhaps you want to know that after that phone has been in possession of someone, if it was powered on and off a bunch of times and looked at and mean touched and so forth. Yes, we absolutely can't see evidence of that from forensic analysis of the phone. We can also things like notes, and the last modification times on that and you can see recover deleted notes. And here's one of my favorite examples of a forensic artifact. And that's the user dictionary also called the dynamic dictionary on the phone. What matters about this is that these are unique words. So you're typing on your phone, and you put in a word, and it tries to autocorrect your word new and you tell it No, don't correct my word. I meant to type in this, okay, don't don't fix what I typed. If you tell it that it will remember your words. So it doesn't have to keep trying to correct you every time. So what does that mean? It means you can attribute the content of that word and the typing of it in and in saving into the phone and in essence, to a user to the person who has that phone to that custodian, potentially right. And those words are often things like names, slang locations, know things that don't have particularized spelling like you'd find in a dictionary. So very, very helpful as far as showing user attribution.

38:09

And as quickly, I know, you probably know this, you can go to your my Google account right now. And you can see that Google is absolutely watching everywhere you go like this, even if you don't necessarily have location put into place. This isn't using it for location purposes, this is just driving around. And it's also recording what you ask it. So if you ask it fast med Urgent Care Apex North Carolina and not only records that you asked it that it has a snippet of your voice saying it. So all that is in there as well. Now, there's nothing better than electronic devices creating for creating extensive timeline activity, the ability to have all that information in a timeline that can be sorted and filtered and examined. Nothing better than electronic devices because they create so much data and so much timeline information. interpreted correctly, this timeline information is extremely useful. Now, imagine this, you get a cell phone forensics report and you try to print it out, it's probably gonna be 10,000 pages. And then inside those 10,000 pages, you got messages and one pile emails and one pile of voicemails, and another pile and so forth. Right. Now, you're going to have to try to string together to create a timeline by looking through all those different ones and cutting them out putting them on poster board or something which I've seen people do. Or you can recover and get this timeline and this can be produced to you by a forensic examiner actually, most forensic examiners who have the right tools and capabilities and expertise, such as our lab are able to provide you a mini version of forensic software that allow you to parse and search and do all this on your own. We have little guides to do that that are super, super valuable. So I say all that to say this. If opposing counsel or the opposing side will only give you a print out or like a PDF version of all this data, you probably want to ask for in a different way, because you can absolutely get it in a much more manageable fashion than having to deal with it like that. So

speaking of timeline data, this is a timeline example. That's very, very helpful. So look on this particular report, and this from an actual case, it's obviously been redacted. But if you move down, you'll see in that kind of pinkish text where it says picture picture picture, okay. What's happening in this is that this is an examination of a plaintiff's phone, we were retained by the counsel for the trucking company, to examine to plan his phone. And what's occurring here is that he's got his phone in his hand while he's driving down the road. And he's taking pictures of a pill bottle, and is the seat next to him in the passenger seat, trying to upload those photos to his pharmacy application so that it will refill his prescription, the first picture is blurry. That second picture three seconds later is also blurry. Then this third picture, one second after that, he takes it perfectly clear. However, the problem when he takes that picture, is that he goes on to the back of the 18 Wheeler and is decapitated. But we were able to show that distraction user attribution activity at the time of the accident. Now let's talk about challenging the evidence. And as promised, we're going to start with manual examinations. The reason we're covering this is that they're rarely performed correctly. Remember, the phone used to be isolated from networks, these video verification the entire process, we need complete documentation truly, to have a robust analysis that is done correctly.

42:01
First of all,

42:05
here's some examples. Just massive waves that I've written. Here's the short of it. Anyone who is touching a phone with their fingers is performing a manual examination. Okay? If that's what you're doing, you're not using a forensic tool. It is a manual examination, and therefore it needs to be treated with the highest integrity according to digital forensics best practices and industry standards. Remember, it needs to be isolated from the cellular network. We talked about that already? How would you know from a picture if you received in discovery if that phone had been isolated from the cellular network, or from networks entirely? It's not difficult just look at it. If you see bars of any kind, it's probably not right, if you see connected to a Wi Fi, or to a sailor from the pictures. That's evidence right there. It was not isolated from the sailor or wireless networks, okay.

43:01
So

43:03
one of the best ways to deal with this is to actually utilize industry standards from really excellent

sources. So fear, for example, we see the National Institute for Standards and Technology, you can use this as an exhibit use this as in quarter use, this is a part of an affidavit or whatever, saying you got to isolate it from cellular networks. This is Wayne Janssen, Rick airs from nest nest is super important. If this is not a proven methodology or a tool many times government agents can't use it until they do really, really an important group there. We also have Ethan Casey and Benjamin Turnbull. This is their book digital evidence and computer crime, the third edition, they say the same thing got isolated. And from my book, digital forensics for legal professionals got isolated from the sailor networks. Similarly, with video verification, you have to have that entire video from the time is pull out of evidence storage, the whole examination to put it away, that's your only way to verify it once again. So you have to have that that's in accordance with best practices. Nest says it as you see here. And there are guidelines on cell phone forensics. Once again, and Egan Casey and Benjamin Turnbull's book, they say the same thing, it should be videotaped. And then we say the same thing in our book, digital forensics for legal professional. So there's industry consensus on the way it needs to be done. So the question is, is why is such a big deal other than just the simple verification process, being able to have something to show you didn't change anything? What if that's really that not that high on your priority list? Well, I would argue that potentially it should be and the reason is, is that fake messages are real, and creating pictures or screenshots of text messages. It's just not enough. reason is, is that they can be faked easily quickly. And they really require a low level of technical sophistication, especially today, there's so many advanced ways to do this. applications that allow you to do this. I here's one example. Here's a website you can go to. And on this website, you can put who the message is from who gets to your battery percentage who your carrier is, like Verizon or at&t, you put all that in there, the actual what you want it to say. And you can create all these fake messages, right? Like you see a number 6000 there, if we go through the whole process that looks absolutely real. Now you get their message and you save it to your phone, I then email it or text it to you and say, Look what this person said to me. And it looks absolutely real, just like a real screenshot on the phone, but it's completely fake. You could also simply change the name, right? And we can't have the underlying data related to these names. Because all we have is a picture we don't have the phone itself. So you the change we need to Louise. And it looks like Luis and all these messages when in reality it was Rene may Bernays, your friend and you want to incriminate the creepy guy down the street or something, you just change the name. on an iPhone, you still have this capability, you can turn off the automatic clock settings and then you can set the time manually yourself. This allows you to send a message and make it look like it came in at some bizarre time like October 16 2005. I could do that today. Now, remember that as we look at this,

46:37
this is

46:38

one of my old email addresses. And my current cell phone number. And I'm having a conversation with myself. Hello, how are you? I'm doing fine. Was it raining today? Yes, cats and dogs? Did you remember an umbrella? Unfortunately, no. I'm doing this with one phone in my hand. And I'm able to do this because I simply made my phone number named fake contacts on my phone. And my email address is another contact under Lars Daniel my name. And I'm able to do this because they're both utilizing my iMessage account to send messages because you can send I message communications from your email or phone number. And it looks absolutely real. I take those I screenshot those or I take pictures of them, I provide them to whoever and it looks exactly like I did it. Now, let's look at a real case example of bring this home. In this case, the defendant, our client in this case had been accused by his ex girlfriend of threatening her and he'd been arrested and sitting in jail for six months, we're going to let the police report and there is some language I will I will PG and as I read it. But if the language bothers you just close your eyes through this section and you can hear me narrate on gun. So what happened was from the actual law enforcement report, now the victim has a 50 b order on the defendant that states he cannot contact her via phone or text. The defendant sent a text to the victim stating that he was going to her place of work with a gun to cause death or bodily injury. Now, would that point to these other defendants guilt, he's violated the 50 B or twice in the past stated on text that he is aware of the police and will go after her threatening her life. He said You're so dumb, I don't care about a restraining order, ma'am. I don't get the care in the world about the law, do whatever I want. Because you can't call the police. You're in big trouble. And I get off work tonight and come into your house, you better watch out a lot and take my guns right? And never be seen again. normal stuff that couples say to each other right. So what's the evidence of the crime? What did she provide the law enforcement she provided these pictures of text messages. So we look at this do you see a name on these messages? No, my we see. I'm not sure what to do with this. I don't have April 9. I don't have a year on that either. So there's already issues here. But if we see, I'm glad everyone at beefin thinks you're an unpleasant person. You know, it twists, lots of stories, all kinds of stuff like that nasty things said back and forth. And then we have photos of the text messages on the girlfriend's phone. These are allegedly texts after being served a restraining order for 2015. Now, if you note Do you have an electronic date on this? You don't right? We have very little information. We just have these text messages that have been sent. You're so dumb, all that stuff we talked about I don't even care in the world about the law. You deserve to be hit. If you're this lacking in mental furniture. The police don't care up here and I've got a lawyer in my family which always works right always. That's the best answer. I've got a lawyer in my family. But here's where we really had a good break in this case.

49:59

Sheila He begins to use a new phone. So we have a phone number Finally, right? Obviously, I've redacted the last four numbers, but we've got a phone number. And it says I don't care. If you

block my number you can't report this one who is this? I'm not stupid. Just know you can't hurt my feelings anymore. Please don't contact me. Okay, just know when you're dead. You don't have a story. I find you unpleasant. Right? So that's the general gist of the conversation. Well, we have that phone number. So now, we can take that phone number. And we can find out who belongs to right. So we get that phone number we see it belongs to go text me We assist the attorney and getting subpoena language set out. For the subscriber information from go texts mean, here's what comes back. The username is Jake, this Nate k 3816. We see when it was signed up, was created. We have his email address, Jake, the snake at tahu calm now, if I had a roomful of you, I'd ask you please raise your hand if you have a talku.com email account? And your answer will be no because tahu.com does not exist. That's obviously a fake email account. Or you can also see not verified a specified by user in the text. Now you create an account somewhere, that tells you click on the link inside the email we just sent you to verify your real person. That's how you do that. That didn't happen here. Also, it didn't happen via text messages you see via phone number. But a couple important things. One is we have the IP address when the number was assigned to this application gives you a phone number, we have the IP address that will give us some location information. And we have the device ID. The device ID is unique to the phone you carry not your account, not you but to the physical piece of hardware that you have.

51:50
So

51:53
the IP address that we saw there, we can look at that and we can find out a belongs to Verizon. His phone is on sprint. So for him to have done this, he would have gone out and had to have gotten an entirely new account with a different carrier. first piece of information there. So did he really get a new number? Can we find out what we do? We then send a subpoena to Verizon to find out who had that IP address at that date. And time it turns out she had that IP addresses that date and time not him. And second, the device ID was her phone, not his phone. So she faked all these messages. And because of her fake messages, he was in jail for six months he was released upon the conclusion of this investigation. So fake message or real pictures or screenshots. And messages are not enough. There's lots of ways to create fake ones. So got a few case examples. In this particular case, example, you've got a a rather sophisticated gang that steals high high end vehicle. So if you're elderly or infirm, you pull up to the gas station, they hit you on the head with a blackjack, they steal your car, only if you have a really nice car only really nice cars, they drive it down to the harbor or whatever, and they put it on a big boat, and they send it to China and sell it for an exorbitant amount of money. That's what they were doing. Okay, excuse my lack of medical terminology. It's not my area of expertise. So they're stealing all these books in this guy's like, Yes, I love to bite people on the head, I love to steal cars. But I didn't have a gun. And they're

claiming he had a gun at the time of the commission of these felonies because of this photo on his phone. Because they have a date and time is contemporaneous to the time around when some of these actions occurred. Now we see the capture time we have the creative modified access all that good stuff really want you to see is the model. The model the very far bottom is this is an iPhone four s that took the picture of this gun. Now. For phones that our guy has, he's got two phones, but they're both iPhone four, not iPhone for us, so that his phones didn't take that picture. Second, we recovered these text messages that law enforcement did not recover. where he's talking to his friend Walter, I got you download Spartan soldier Tommy Lee at the end and then lots of sins, these photos of this firearm to him. Walter is on different continent wealth waters in Africa. So this gun is not in the United States. And if you pull the metadata from those photos, you can see even more information like that. So the information, the data that really tells the story devils in the detail Details once again, like we have talked about already. So our final conclusions, these images also exists in the DCM folder on the phone. They were taken with the four s metaphor. It's not his phone that took those pictures. Here's another example of this was a person who was supposed to have content that he was not supposed to have. In this particular case, this was a contraband case involving images of children. This is a firefighter. He is about 20 years old like that, talking to a girl who's 16, she had claimed through this application they were chatting on to be older than that. Here's some short what happens, mom finds her phone, mom gets concerned, the chat says she sees she contacts law enforcement, law enforcement gets involved, they take the girl's phone, they begin to impersonate her to try to get a meet up, they do get a meet up. The defendant in this case shows up with movie tickets. And that's it to the movie theater, he doesn't show up with flowers, condoms in a box of chocolates or something. So that was good in that first sense for him. But in second, really, they had no way to make a case of solicitation or anything like that. So what they did is that they scoured that phone for some photos, and they found a few photos that she sent to him. And they charged him with possession of child pornography. Now, intention to receive possession of child pornography.

56:39

Here's the thing, when it comes to that, and this is all I had to do in the case, this is my whole part was simply the technology explanation. Because he never solicited the pictures, he never asked for pictures. That was been part of this case. Did he intend to possess the contraband? That's the question. Now if I send you an email, can you stop it? No, you're going to get it unless you previously blocked me say anything, if I sent you a text message, or sent you a photo via text message, you're going to get a new way to stop it. So what matters is there an intention to do anything with it to preserve it.

57:18

So

57:21
in this case, all this

57:24
fun text, everything we're seeing here basically explains the following. If I send you a message, you're either gonna have preview on or off, what you're going to get is this, you're going to see that I sent you a message or that you have a little picture of the message and then I send it on your phone either way, you can do nothing about it. For you to intentionally preserve that data, all you have to do is unlock your phone, hit the share, modify button, select the photo and save it to your images, right, you'd have to do something like that to show a command and control these messages. If similar case, were all saved in the library, SMS parts way down in this folder, which is the automatic location where they're saved. To my understanding, he didn't even know they were in there. So there's those photos there. From the actual forensics report by law enforcement, we can see that all the images are there. They offered him a plea of non sexual child child endangerment, no registrated loses job or anything out based on the outcome of this case, this analysis was was a critical part in this one because it was so technology heavy. Remember to we're not limited to only getting data from the actual cell phone itself. If you have a phone and you're backing it up to the iCloud or whatever cloud service your your particular model has associated with it, we can use those credentials and pull the data directly from the cloud in a forensically sound manner. We can also get data from local backups. So for example, if you have an iPhone hook into iTunes, and pull the data from that to backup your phone, that's just like having the cell phone in many regards. A lot of data is saved in those backups. Sometimes those backups are better than the actual phone itself. For example, it's been a year since an incident occurred, we need to know what happened on your phone a year previous if you have a backup contemporaneous to that time, the data may be better, more relevant for what's contained in that backup than the actual phone. And also this is great if the phone goes missing or such things too. That is also synced between devices. Remember, Apple sells you all these different things and they don't allow AI messages to be used on any device but Apple products that's one of their main selling points to keep you in their ecosystem. They want you to have all their products and keep buying their stuff to so they can make money. So if you have an iPhone and it's sinking as messages to your computer, To your iPad, just because the phone is lost doesn't mean you can't get all the messages back from the computer or the iPad. quick example of how this actually works in real life. I worked on a case i was i was brought in by the board, who runs a particular bank, there were concerns about an employee. And an email had gone out from an employee's email account to these VIPs, and CEOs of really, really important organizations. Inside the picture, it had a, it was an inside the the message was a picture of his genitalia. So he said I didn't do it, I was hacked all this stuff, I go to examine his devices, which he did turn over after a little bit of process. But his phone had gone missing. His work laptop had had anti forensics run against it and had completely wiped it. And his other laptop that he had, he had actually run a eraser

program on it. But these eraser programs want to get rid of stuff they think you don't want now if you have a backup of an iTunes phone, a phone and iTunes, deleting iTunes doesn't get rid of the back of the backups way deep down in the file system, and you had to know how to get there to find it. So I was able to pull that and recover it, rebuild it and see the data. Unable to see what had occurred is that he had sent actually sent out a picture of his genitalia from this device. And instead of hitting the picture for his or the contact for his mistress, he had the contact list for this this group of people from his work really important people and accidently did that. So I'm not sure if his if his employment status stole that location of you just as a nickname or something now, but those data sinking in the ecosystem of devices is very, very valuable. Finally, remember that your your pods, your players, your Kindles, your your your touches, things like that. They're all just cell phones without cellular service. In many instances, we absolutely can get data from those just like we could a cell phone. Well, I appreciate your time today. If you have any questions, feel free to contact me directly. There's my email and my cell phone number. There's a few bucks you can potentially check out if you'd like to. I appreciate your time. Have a great day.