CITY OF PORTLAND
INDEPENDENT POLICE BUREAU
Confidential Taped Statement
IPR Investigator Eric Berry

Interview Date: **11/14/2016**
IPR #: **2016-B-0030**
IPR File Name: **16b0030-Brillhart, Joel interview**
Complainant: **Portland Police Bureau**

Interviewed: **Joel Brillhart**

BERRY: This is IPR investigator ERIC BERRY. Today's date is Monday, November 14th, 2016. The time is approximately 10:08. I'm present in the IPR interview room for the interview with JOEL BRILLHART related to 2016-B-0030 and 2016-B-0014. Mr. BRILLHART, are you aware that I am recording our conversation?
BRILLHART: I am now.
BERRY: Excellent, thank you very much. Will you briefly describe your experience extracting material from cell phones?
BRILLHART: So, I retired from the FBI in 2009. I was a special agent for 23 years, the last five of which I was assigned to the Northwest Regional Computer Forensic Lab where I processed digital evidence to include cell phones. So, I was a certified forensic examiner, cell phone examiner and then I retired in like I said in 2009. I went to Iraq for a year where I processed digital evidence for the US Army -
BERRY: My gosh.
BRILLHART: - and then returned and have been doing the same type of work but as a consultant both criminal and civil cases on both sides.
BERRY: It seems like there's been a remarkable evolution over the time that you were with the Bureau in terms of cell phone technology. They are a lot fancier than they used to be.
BRILLHART: Exactly, and they contain a lot more data than they once did and they are more prevalent in all of the cases that I work on now.
BERRY: Absolutely. And were you hired by the City to extract some material from some City cell phones?
BRILLHART: Yes, I was.
BERRY: Okay, and I'm just cribbing off your report, but it looks like it was Captain RODRIGUES, former Chief O'DEA, former Assistant Chief MODICA and then a retired Lieutenant TERRY KRUGER.
BRILLHART: Those are the four names -
BERRY: Yeah.
BRILLHART: - their positions are not all there present
BERRY: All right. I mentioned being a layman, can you briefly tell me what a forensic extraction is?
BRILLHART: Yes, so I used for these four exams the primary forensic tool, which is a tool in the sense that it is either a piece of software or hardware that has the program on it that extracts the data. So, the tool that I used was I believe Cellebrite for all of them and then for some of them I think I used oxygen – oxygen, I am drawing a blank right now.
BERRY: I got it there if you want to refer.
BRILLHART: - I think I used it down here - oxygen forensic extractor. So, those were the tools that I used. So, for Cellebrite there is both a physical extraction done with or not a physical extraction, an extraction done with a piece of hardware called the Cellebrite Touch. So, that basically connects to the cell phone and then depending upon what the file system on the cell phone is, these cases – three of them were IOS devices, which are Apple cell phones and then the other was an Android operating system. Depending

upon what access those file systems allow to the various applications that are on the phone determines the type of data that is extracted. So, Cellebrite will extract as much of the data as the operating system allows it to. So, it's not like a computer where you get access to – physical access like to the hard drive.
BERRY: Mm-hm.
BRILLHART: So, you can take a hard drive out of a computer and basically create a forensic image of every bit – from the very first bit to the very last bit on the hard driver. So, you're getting all of the data. And in the phones, the phone types of extractions in some instances you can get a physical extraction –
BERRY: Mm-hm.
BRILLHART: On older iPhones and on jailbroken iPhones and/or certain Android phones. These – all of these particular phones we weren't able to get a – or I wasn't able to get a physical extraction. There is no tool that is out there that will allow that.
BERRY: Mm-hm.
BRILLHART: So, you aren't able to recover as much deleted data as you would if you were able to get a physical extraction. In this particular case, I believe I did logical and file system extractions and then the Cellebrite has another portion of the software that's called Physical Analyzer that takes this extraction and it's just a group of files and then it parses them so that you can read the text messages in the format that I provided to the client -
BERRY: Yeah.
BRILLHART: - in the spreadsheet format or PDF. And the same with chats. And it containerizes files such as images, text files, database files, things like that. And for those database files, it can parse and it can recognize and then it puts that data in a format that is readable by us very easily. Almost of all of the data that's on the phone is kept in database files. So, and not all of them are able to be parsed by the forensic tools.
BERRY: That's really interesting. The only other – the previous forensic images I've reviewed have all been of computer drives.
BRILLHART: Yes -
BERRY: I didn't realize -
BRILLHART: - totally different.
BERRY: - yeah that there was such a difference between the phone -
BRILLHART: Yeah.
BERRY: So, in terms of your ability to extract deleted data -
BRILLHART: Mm-hm.
BERRY: - it sounds like it's really limited by not being able to do a physical extraction.
BRILLHART: Yeah, it's limited by the operating system of the phone primarily and if you're not able to get a physical extraction, all – not all of the deleted data is going to get recovered. Obviously, we've recovered various deleted data that's recovered because much like on a computer when a file is deleted –
BERRY: Mm-hm.
BRILLHART: - the file itself isn't like immediately removed – just the pointers to that file, much like on a computer. So, as I mentioned, everything is in databases. So, when you delete like a text message from the database, the entire database isn't wiped away. Otherwise, all the other messages would go with it.
BERRY: Right.
BRILLHART: Only just a portion of that database is – was removed and it's there for a while, but the phone operating systems have a process called vacuuming where they will periodically – it removes portions of that database file -

BERRY: Mm-hm.
BRILLHART: - that contains deleted files. And it removes them and then once they are gone, you know, once they have been removed by the operating system, then the forensic tools can't get to them any more unless you have a physical image and then, you know, there is a potential for more recovered deleted data.
BERRY: Interesting. So, I suppose the operating system of the phone is just doing that because of the limited file space available on a phone?
BRILLHART: As far as doing what?
BERRY: Well, just going through and vacuuming.
BRILLHART: Yeah, that's all – you know, I don't know that anybody knows when that process takes place -
BERRY: Yeah.
BRILLHART: - other than the developers.
BERRY: Right.
BRILLHART: But it is a function of sq-like database files, which are the predominant make-up of the databases that are on phones.
BERRY: Yeah. That's really interesting. Well now, I mentioned specifically there's a deleted exchange I hope to ask you about and I've got – right here I'll refer you to this the Captain RODRIGUES end of it.
BRILLHART: Okay.
BERRY: I mentioned I don't have right now a copy of the O'DEA end of it.
BRILLHART: Yeah, I think I went and looked at that.
BERRY: Yeah.
BRILLHART: And then sent you an email regarding that.
BERRY: Yeah, and you've got – I've got a copy of that email here. Essentially it sounds like – what you told me is that there was some indication that former Chief O'DEA and Captain RODRIGUES exchanged text messages on May 20th?
BRILLHART: Yes.
BERRY: Yeah, okay, and in your work you weren't able to actually recover the content of the messages that they exchanged?
BRILLHART: No, only an indicator that the messages were there at one point.
BERRY: Okay, and recognizing that I put you in a difficult position not having the O'DEA material available, are you able to describe the sequence of messages? Who messaged who first? Or can you -
BRILLHART: No, you wouldn't even be able to tell. One – where you would be able to get that information is from the phone billing records.
BERRY: Mm-hm.
BRILLHART: So, they would have the time stamps much like this because they would have both sides of it, so that conversation could have been 20 messages. It could have been 4 or 8, whatever. But the phone billing records should have both sides -
BERRY: Mm-hm.
BRILLHART: - for each party, so you would be able to see an indication of how many messages were exchanged between the two. You won't get the content, but you will get -
BERRY: Yeah.
BRILLHART: - you will get the back-up. Another place where you could potentially get the content would be if there was a computer that either of these phones were synced to.
BERRY: Synced to.

BRILLHART: - there would be a [unintelligible] back-up file on there.
BERRY: Okay.
BRILLHART: And that's typically a source of golden little nuggets.
BERRY: I can imagine, yeah.
BRILLHART: Because a lot of time it is unbeknownst to the user. You know, they, they backed it up and then they don't realize that it's continuing to get synced when they connect their phone.
BERRY: That's interesting. Well and I just – revealing, continuing to reveal my ignorance of this process.
BRILLHART: No.
BERRY: In your report here, you mentioned doing some images of two Verizon SIM cards. You noted that neither contained any text messages.
BRILLHART: Yeah.
BERRY: I'm just wondering is that typical?
BRILLHART: Yeah.
BERRY: Is the SIM card not going to have text messages?
BRILLHART: Older SIMs do, newer SIMs. I haven't encountered a newer SIM card that has any messages on it for quite some time.
BERRY: Okay, and just generally we've had occasion to review now a lot of text message exchanges between City employees, here and there I've noted that there will be a gap of some amount of days or weeks between messages being sent. In the work that you did, would – if someone had deleted particular messages in an exchange, would there be some indication that there was a message there even if they -
BRILLHART: Only if – I mean only if the iPhone [unintelligible], you know, had it, but this iPhone [unintelligible] you're not going to get all of the messages. So, it may not even by all of the outgoing messages. It's what, you know, is recovered at that – by the software at that point. So, those gaps, you know, if you see text messages going back and forth between two individuals and then you have a gap of a month, I mean either they were out of touch with each other or there's – and that's a pattern.
BERRY: Mm-hm.
BRILLHART: I mean, that's – I would think that there's – or text message have been deleted. You know, but that's pure speculation.
BERRY: Yeah.
BRILLHART: But the only – I mean again you just look at the billing records and you can – your billing records and say hey there are all these text messages going back and forth but yet there's none on the phone any more. That's -
BERRY: Makes sense. So, you have a great deal of experience doing this work. As you did this particular job for the City, did anything stand out as unusual or notable?
BRILLHART: No, you know, because I don't – I didn't – I wasn't requested to like analyze the data, do any type of analysis like that. I was – it was a very limited scope in that I was asked to – I believe it was just communications. So, that's what I pulled off. Either chat – I think telephone calls and SMS.
BERRY: You've been generous in your time in coming in today. Is there anything you want to add to our conversation or anything you think we should make note of?
BRILLHART: No. I mean, if you have any – well, if anything pops up in the future just give me a buzz.
BERRY: Absolutely, I'll do that. DEIRDRE do you have anything you want to add?
PEREZ: I just have one. Does the amount of time between the extraction and when a person may have deleted the text messages have an impact on the record?

BRILLHART: Nah. Which is odd. You know, in some instances you can delete the data, a few hours later process the phone and it's not there, but yet there's a text message deleted from a month ago that's recovered.
BERRY: That is so strange. I have always wondered about that.
BRILLHART: Yeah, yeah, and I don't have any – you know, it's just that – it's the – you know phones are very volatile in that the data is moved around a lot like that and so it's just -
PEREZ: Kind of random.
BRILLHART: Yeah, it's very random.
BERRY: Excellent. Well, Mr. BRILLHART, thank you so much for your time.
BRILLHART: Any time.
BERRY: The time is approximately 10:21.

16b0030trs-Brillhart, Joel interview – IPR
Transcribed 11/15/2016 @ 3:30 p.m. Cathy Daley