Witness: Kirk Stockham

Date: 2004-08-02

Proceedings held August 2, 2004

Called by: People (prosecution)

Phase: Guilt

Examinations: Direct – David Harris

Day 1 of 2 for this witness

Court: San Mateo County Superior Court, Redwood City (People v. Scott Peterson)

Source: https://pwc-sii.com/CourtDocs/Transcripts/Stockham-Trial.htm

Page/line: not available (source HTML has no page or line markers)

Text below is verbatim from the source page for this date only.

Direct Examination by David Harris

HARRIS: Mr. Stockham, did you used to work for the Modesto Police Department?

STOCKHAM: Yes.

HARRIS: And did you retire from them at some point in time?

STOCKHAM: Yes.

HARRIS: Approximately when did you retire?

STOCKHAM: Retired on May 1st of 03.

HARRIS: Prior to that, prior to your retirement, were you working in a particular assignment at the Modesto Police Department at the end of 2002 up until you retired?

STOCKHAM: Yes.

HARRIS: What is your assignment?

STOCKHAM: I was titled a Computer Forensic Investigator.

HARRIS: And what does a Computer Forensic Investigator to?

STOCKHAM: Just like a law enforcement oriented computer technician. We find data for field officers who come across computers that may be involved in cases.

HARRIS: As part of your assignment, do you have to receive any specialized training or education to be this computer forensic person?

STOCKHAM: Yes.

HARRIS: Could you tell us briefly about your background in computers?

STOCKHAM: I have been a computer hobbyist since 1989. My first case in computer forensics was 1994. My base education is two-year degree in police science, a Bachelors Degree in sociology, and some post-graduate work where I received a Masters Certificate in Computer Forensics. I am POST Certified by the state of California as a computer crimes examiner, which required several hours of classroom work over many months. I have taken many law enforcement courses, including investigating of internet crimes, exploitation of children, the search and seizure of computers that have taken place, use of the software that I will be testifying about today. And I have taught on similar subjects as an instructor.

HARRIS: Have you also testified as an expert in court?

STOCKHAM: Yes.

HARRIS: In the area of computer forensics?

STOCKHAM: Yes.

HARRIS: With that background in mind, I'm going to take you back to December 26th.

JUDGE: Do you have any voir dire as to his qualifications?

GERAGOS: Mr. Stockham, you have testified, qualified as an expert how many times?

STOCKHAM: Three times, and once on this case at the prelim.

GERAGOS: Three times. We talked at the preliminary hearing, correct?

STOCKHAM: Right. The Erica Frazier case in 99, Al Peacock case in 01 and 03, and the Stark case in Sacramento County Superior Court in 03, and this case in 03. So four total.

GERAGOS: Four total. Once including the preliminary hearing?

STOCKHAM: Yes.

GERAGOS: Once including the preliminary hearing?

STOCKHAM: Three times. Four including the preliminary hearing, yes.

GERAGOS: And your area of expertise is on forensic computers?

STOCKHAM: Forensic computers. Taking a look at computers, deciding what's on them, and when it was opened, setting up the computer for examination, doing so correctly. And we have had some data losses, so try to prevent that.

GERAGOS: And, in this case, is that what you did?

STOCKHAM: Yes. I help seize the computers, set them up for processing, and then look for data that might be relevant in the case.

GERAGOS: Thank you. I have nothing further.

JUDGE: Court will accept Mr. Stockham as a computer expert in computer forensics.

HARRIS: Thank you. Sir, taking you back to December 26th of 2002. Did you assist the Modesto Police Department while they served a search warrant in the area of collecting computers?

STOCKHAM: Yes.

HARRIS: The next day, did you also assist on December 27th of 2002 in seizing some additional computers?

STOCKHAM: Yes.

HARRIS: Like to have marked some photographs that have been shown to counsel.

JUDGE: Okay.

HARRIS: It would be a series of, appears to be eight photographs.

JUDGE: 174. How many have you got there?

HARRIS: Eight.

JUDGE: Eight. A through H.

HARRIS: I'm going to show you what's marked 174-A through H, have you take a look at these, see if you recognize what's depicted in the photographs.

STOCKHAM: Exhibit 174-A looks like the two laptop computers in the Peterson home. The Compaq Armada and the Dell Latitude laptops.

HARRIS: 174-B.

STOCKHAM: 174-B is a repeat picture of those, two different angle.

HARRIS: 174-C?

STOCKHAM: 174-C is a closeup of the Compaq laptop in those pictures with the lid opened up.

HARRIS: All right. 174-D?

STOCKHAM: 174-D is a photograph of the Emerald Peterson workplace.

That's a picture of the IBM Thinkpad laptop and a Dell PC.

HARRIS: All right. 174-E?

STOCKHAM: 174-E is a closeup of the IBM Thinkpad that was on that desk, that work location.

HARRIS: 174-F?

STOCKHAM: 174 F is the IBM Thinkpad with the lid opened up.

HARRIS: 174-G?

STOCKHAM: 174-G is a closeup picture of the Dell PC under the desk at that workplace.

HARRIS: And 174-H?

STOCKHAM: 174-H is an another picture the Dell PC, closer up.

HARRIS: Do you recognize all of these items that are depicted in the photographs?

STOCKHAM: Yes.

HARRIS: Do those items, as they appear in the photographs, appear to be true and accurate depictions?

STOCKHAM: Yes.

HARRIS: I want to put up on the screen 174-A. I'm going to go through, you are talking about certain things. 174-A is this, does this depict the computers that you found on 12-26?

STOCKHAM: Yes.

HARRIS: There were two laptops there?

STOCKHAM: Yes.

HARRIS: Now, you were describing them somewhat different. Were they different brands?

STOCKHAM: Yes.

HARRIS: When you, from your point of view computer forensics when you collect a computer, do you do something to identify it?

STOCKHAM: Well, I do several things. I go brand names, and the photographs of course. I look at them, how they are connected. There is not much more except to look at the details of the actual case, label, serial numbers. Turn over and look at what's on the bottom, what's on top, what's on the sides.

HARRIS: When you do this examination, do you document this and transfer it at some point in time to something that you work on?

STOCKHAM: Well, there was a, we had a scribe who is writing things down as I talked about these things and the photographs were taken.

HARRIS: Well, let me just kind of skip forward a little bit. Do you make copies the hard drives of these computers?

STOCKHAM: Yes.

HARRIS: And without getting, we'll come back to that. But without getting too much into the details of how that's done, do you identify the copies of the hard drives in some particular fashion?

STOCKHAM: I see, when I use forensic software to look at the data on these PC's, I do file names, and I do a naming standard that helps me remember which laptop was which.

HARRIS: In this particular case were there ultimately five laptops that, computers that were recovered?

STOCKHAM: Yes.

HARRIS: And did you go through that file naming standard that you are referring to?

STOCKHAM: Yes.

HARRIS: Now, looking at these two computers in 174-A, what was the naming standard, as you went through this process, starting with these two particular computers?

STOCKHAM: One with the "Spain" sticker on it that was labeled in an abbreviated form "Compaq Laptop Home". And the other one was labeled "Dell Laptop Home".

HARRIS: And if anybody were to look at these hard drives, would that particular file information be kind of burned into a hard drive so you can tell which computer it came from?

STOCKHAM: It wouldn't be burned into a hard drive. But the copied files that I create would have those file names, and so another examiner could work with my work and do it very easily, and know what he's working with because of these file names.

HARRIS: Now, go back where we're at with necessary particular computers. You were telling us as you went along, you document kind of how they are. Looking at 174-B, is this the Dell laptop?

STOCKHAM: Yes.

HARRIS: You can also see a little bit up here in the upper corner, that other the Compaq laptop?

STOCKHAM: Yes, correct.

HARRIS: 174-C, does this depict the Compaq laptop that's now been opened?

STOCKHAM: Yes.

HARRIS: You are describing at the office at the warehouse that there were, actual term you used was workplace. 174-D, does this depict that office workplace as you first observed it?

STOCKHAM: Yes.

HARRIS: And you describe down here on the floor, this would be where the PC was at?

STOCKHAM: Yes.

HARRIS: And the item right here behind that piece of paper, that is the laptop?

STOCKHAM: Yes.

HARRIS: Showing you 174-E. And this, again, is that laptop with the paperwork cleared away?

STOCKHAM: Yes.

HARRIS: You describe this as the IBM Thinkpad?

STOCKHAM: Yes.

HARRIS: Was that assigned an evidence number as well?

STOCKHAM: Probably, but I'm not sure. I wasn't doing that.

HARRIS: Do you see at the top of the photograph placards?

STOCKHAM: Yeah. The yellow placards, the tents that were propped, that could be evidence.

HARRIS: This was given a placard of 103, at least in that photograph?

STOCKHAM: Yes.

HARRIS: Looking at 174-F, before the placard is there, this is, again, the IBM Thinkpad in an open condition?

STOCKHAM: Yes.

HARRIS: 174-G, how did you describe this again?

STOCKHAM: The Dell Work PC.

HARRIS: And is there an, in terms of your examination, is there a difference between desktop or computer like this, and a notebook or laptop?

STOCKHAM: In what respect? On what I have to do?

HARRIS: Yes. Is there any difference?

STOCKHAM: Yes. The hard drives are usually different sizes. The one in the PC is usually larger than the mini hard drives in the laptop.

HARRIS: Looking at 174-H, is that same computer with placards there now?

STOCKHAM: Yes.

HARRIS: Now, to go back to this naming convention. So that we're clear about this, there were two laptops that were found at the house?

STOCKHAM: Correct.

HARRIS: How did you describe each of those?

STOCKHAM: The Compaq Laptop Home. I better check my report on that one.

HARRIS: Did you write a report?

STOCKHAM: Yes.

HARRIS: And if you were to look at your report, would that help you recall specifically what you said?

STOCKHAM: Yes.

HARRIS: Please do. Having looked at your report now, can you go through and walk us through how you named each of these computers?

STOCKHAM: It's the same as before. It's an abbreviated form, where you can easily tell from the file name that "Dell Laptop Home" is the Dell laptop.

And the "Compaq Laptop Home", number two, is the one with the Spanish banner sticker on it.

HARRIS: Now, so you collect these computers from where you find them at the, with the search warrant, what do you then do?

STOCKHAM: I take them to the Modesto Police Department and use my computer forensics lab to start the process of seeing what's on the computers.

HARRIS: Walk us through that. What do you do?

STOCKHAM: Okay. With three laptops, I examined the laptops. I take more photographs of what I'm doing. And I find out where the hard drives are, remove them from the laptops.

HARRIS: Hold on. You say you take the hard drives out of the laptops?

STOCKHAM: Yes. Most laptops allow you to do a fairly harmless disassembly of that part of the computer. The hard drive slips or slides in, depending how it's fastened to the circuitry. These were fairly easy. Once they were out of their cases, I had to take off the framing for the cartridge and expose the actual laptop and the pin connectors. Then I would hook that up to my computer forensic machines and make forensic copies of the laptop hard drives.

HARRIS: What's the forensic copy?

STOCKHAM: A forensic copy is a, like a bitstream copy where no data is lost. It's actually a very good clone of a hard drive. If done with forensic software, it catches the first byte of the hard drive, the last byte, and copies everything in between.

HARRIS: Let me they just back up. You are using a bunch of different terms. What is a bitstream?

STOCKHAM: Well, computer data is zeroes and ones on bits of data. You can copy a hard drive without affecting the original drive. You can actually do a copy that is so perfect of the original that you can do your examination on the copy and leave the original intact so there is no damage done. Because we never know if these hard drives are in good repair or not. So the first hurdle to protect the original drive is to copy it as a perfectly forensic copy. And once that's done, we can put the original hard drive aside for the defense experts later, or for recopying, and we can kind of do a free-for-all examination of the copied drives what malfunction or mistakes wouldn't affect the original hard drive. It's the first hurdle we like to get over.

HARRIS: Why is it that you actually go in and take these hard drives out of the computer?

STOCKHAM: Well, to make sure they work, they are in good condition, they are not cracked, dented. To make sure we can hear them when they turn on, to see if they overheat or not. Just a total examination process to make sure those things are working properly for that copy.

HARRIS: You mentioned something about forensic software. What is that?

STOCKHAM: We, in this case we used a forensic software program called EnCase by Guidance Software. And I also useda copying program called SnapBack by Columbia Data Products. And with that software, they are designed to forensically copy where there is no alteration of the original drive and still give you a good copy. And it's been tested by me, and backed up by the manufacturers.

HARRIS: So you make the these forensic copies or, I think the term you also used is a clone?

STOCKHAM: That's another term.

HARRIS: When you use the software, you make these copies, do you do something to identify the clone copy so that you can always tell which computer or which hard drive it's a copy of?

STOCKHAM: Yes. The EnCase software allows you to file naming standards or labels, as I have testified previously. And once you do that, the EnCase copy files can be stored on my hard drives, and I can sift through the data and see what those computers have.

HARRIS: When you go through, let's look the process, do it in reverse, since we have in photograph up there. 174-H, the Dell PC. You have the H. Did you do the same thing with the laptop, do with the laptops, did you do the same thing you do with the PC?

STOCKHAM: PCs are easier, because they have a larger hard drive with a standard ribbon cable connected. We simply take off the cover or backing, whatever we need in this case. We took off the cover, and I searched the frame area for the hard drive unit. I disconnected it. This is all with power off, of course. And I have to undo some screws. I take the hard drive out and connect it to my forensic PCs in my lab and make that forensic copy of that PC hard drive.

HARRIS: You keep talking about a forensic PC in your lab. Again, tell us what that means.

STOCKHAM: These are computers that have features that we like to make forensic software work properly. And they are computers that allow us to hook up other hard drives and other devices to them so we can get the lab work to get these copies done and the data reviewed. We actually use these machines where we put the forensic copies to actually look for data from these copied hard drives.

HARRIS: Going back to starting to talk about how you use that file naming forensic copying with this particular computer 104, and in photograph 174-H. This is the Dell PC. What was the name you that gave it?

STOCKHAM: Okay. That file name on those copy files was "Dell Work PC 4".

HARRIS: And that's something that stayed with that cloned hard drive after you created it?

STOCKHAM: Yes. The EnCase software allows the streamlining of this process, allows this file naming standard that keeps things straight on whatever computer we are calling it. It sure helps.

HARRIS: Going back through the other computer at the warehouse, in 174-E, that was evidence 103, IBM Thinkpad. Was the file naming standard that was given as part of that clone copy?

STOCKHAM: Okay. I called that copy file process the "IBM Laptop Work 3".

HARRIS: And you talked about that if somebody else looks at it they can tell where it's coming from. Not being a computer kind of person, when you put this up on your computer, can you see actually a label, or some type of file name there that tells you which hard drive this is from?

STOCKHAM: Yes. The actual forensic copied files have that name that I assigned to it. So there is, I just don't lose track of what file goes with what PC that is seized out in the field.

HARRIS: Going back to the house. Do it with this 174-C, the Compaq laptop from the house.

STOCKHAM: Yes.

HARRIS: What was the file name standard that you applied to this particular computer?

STOCKHAM: Okay. That's "Compaq Laptop Home 2".

HARRIS: Again that's on always on that copy?

STOCKHAM: Yes, it will stick with that file for the duration of the examination, yes.

HARRIS: And the Dell laptop at the house?

STOCKHAM: That would be "Dell Laptop Home 1".

HARRIS: Were you also given a computer, SOTEC computer by Detective Kipp Loving?

STOCKHAM: Yes. Yes, I went to the Turlock office of the Task Force on about February 24th of 03, and he had that laptop.

HARRIS: Did you go through the same process and make a forensic copy of that laptop hard drive?

STOCKHAM: Yes. We did some other steps for the convenience of the defendant. But that was the same thing.

JUDGE: How many computers were there?

STOCKHAM: Five total, sir.

JUDGE: Five total computers. Okay where were they indicated?

STOCKHAM: Two in the Peterson home?

JUDGE: Three in the warehouse.

STOCKHAM: Two. Two in the warehouse, and the fifth one I didn't. Some other detective did, and I got it from him.

JUDGE: Okay. All right. Just want to make sure.

HARRIS: All five of the computers, did you use this naming standard and make forensic copies of the hard drive?

STOCKHAM: Yes. The fifth computer had a brand name that was kind of unusual, SOTEK, S-O-T-E-K, so I used that as the file naming standard for that image.

HARRIS: Now, we already, we're talking about at some point in time, you retired. When you retired, did the work that you were doing on this particular case, was that transferred to another detective?

STOCKHAM: Yes.

HARRIS: Was that detective Lydell Wall?

STOCKHAM: Yes.

HARRIS: He is also a member of the High-Tech Task Force?

STOCKHAM: Yes.

HARRIS: And as part of transitioning, did you make sure that he knew which particular hard drives he was looking at?

STOCKHAM: Yes. I explained the file naming system that I used to identify these four laptops, yes.

HARRIS: So he would be able, from your explanation and what was on those copies, he would be able to look at it say which computer it came from?

STOCKHAM: Right. He's been one of my students, and he knows the EnCase software. He could actually take my work which I gave to him on one large hard drive and see in those file names, he would know this data came from the Dell Laptop Home, or the ones from work, just by using the EnCase software with that file naming standard.

HARRIS: Now, after you do all that, maybe it's not after. At some point in time, besides doing what you were doing with the hard drives in this particular case, did either a Community Service Officer or an ID Technician talk to you about having a problem recovering some photographs?

STOCKHAM: Yes.

HARRIS: And was this some type of flash drive that they wanted you to look at?

STOCKHAM: It was a Sony Memory Stick.

HARRIS: And what is that?

STOCKHAM: Can I show you one?

HARRIS: If you have one with you.

STOCKHAM: Yes. A Sony Memory Stick. This goes into some very high resolution cameras that our Modesto Police ID Technician use. It's a Sony Cyber Shot with a very long lens on it. A 5.1 megabyte camera. They store the pictures digitally, electronically, on these Memory Sticks. Plug into the camera, and they put them in and out as they record pictures, and put them into a server network for safekeeping.

HARRIS: Did they indicate something that happened to one of those particular disks and ask you to look at it?

STOCKHAM: Yes. Technician, first name is Joy. I'm at a loss on her last name. The tall, blonde-haired technician.

HARRIS: Could that be Joy Smith?

STOCKHAM: That's it. That's, I haven't seen her in many, many months.

HARRIS: Did, after you talked to technician Joy Smith, did you start, or did you look at that Memory Stick?

STOCKHAM: Well, as part of my help calls service with the Modesto Police Department, I was also the network manager. And a lot of the MPD users used me as the go-to person on computer problems. This was no exception. Joy called me to try to fix her problem. She told me that she couldn't find the pictures that should be recorded on the Memory Stick. It was a hundred twenty-eight megabyte Memory Stick. And after questioning her and getting a description of what may have happened, I looked at it, looked at the camera, asked some more questions, and just decided to do a forensic analysis on the Memory Stick in my lab.

HARRIS: How do you do a forensic analysis of the Memory Stick?

STOCKHAM: Well, I borrowed Joy's card reading device, and that's a slotted device that you plug them into on her computer. Comes the pictures that she took. That didn't happen with her, so I borrowed that device, took the actual Memory Stick into my lab, and used the EnCase software again, as in this case, to look at the data that is resting on the stick. And there it was. I saw the data. But there had been some corruption. The photos, some of them seemed to still be there as I viewed the Memory Stick, but there seemed to be a loss of the index data that tells the computer where these pictures are on the Memory Stick. Once these are lost, the computer acts like they are not there.

HARRIS: Maybe I need to go back to just real basics. Does the computer, either the disk, or the laptops, or the PCs, do they need an operating system to work?

STOCKHAM: Well, they need a low level or high level formatting, but not necessarily always an operating system.

HARRIS: You are talking about an index was missing, or was corrupted?

STOCKHAM: Right.

HARRIS: What does that mean?

STOCKHAM: In this case, well, in all cases, computers need to find computer files that use many, some kind of indexing, something put there by software, some kind of an operating system by a manufacturer. And that is data just like the digital picture data. And if that indexing or table of contents is gone or corrupted, the computer looks for it to find the pictures. And if it's not there, it simply tells the user it's not there with some kind of a warning message, some kind of an error message.

HARRIS: Now, is it actually gone, is it just that the computer can't find it?

STOCKHAM: Well, if the table of contents or the indexing numbers are gone, and that corruption didn't go far enough in the Memory Stick, I could be able to see the photos if they are still there, unerased, or not overwritten, depending what kind of damage was done by Joy.

JUDGE: At this point I think we should call it a day.

HARRIS: All right.

<evening recess>