Witness: Lydell Wall

Date: 2004-08-03

Proceedings held August 3, 2004

Called by: People (prosecution)

Phase: Guilt

Examinations: Direct – David Harris

Day 1 of 4 for this witness

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

Source: https://pwc-sii.com/CourtDocs/Transcripts/Wall.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: Sir, can you tell is what your occupation is?

WALL: Yes. I'm a detective with the Stanislaus County Sheriff's Department. And I'm assigned to the Sacramento Valley High-Tech Crimes Task Force.

HARRIS: What is your assignment with the High-Tech Crimes Task Force?

WALL: I'm a computer examiner.

HARRIS: And to be a computer examiner, do you have any background, education, and training?

WALL: Yes. I have an approximately 640 hours of training pertaining to high technology investigations and computer examinations.

HARRIS: And this training, what kind of training is that?

WALL: Basically how to investigate technology-related crimes and methodology in how to extract data from computer systems that are seized as evidence.

HARRIS: Now, when you are talking about training, just to flesh this out a little bit more, is it something that you go to a class about, or is it something you just read about? How does that work?

WALL: Yes. Training is actually sanctioned by the California Commission of Peace Officers Standards and Training. And also attended training by the Search Group, the FBI, and specific software vendors. So it's Guidance Software and Access Data where I received certifications from those of completion of their courses.

HARRIS: Those last couple of courses, you are talking about software vendors. Are these products that you use as part your computer examinations?

WALL: Yes, it is.

HARRIS: Is it also referred to as forensic software?

WALL: Yes, it is.

HARRIS: And to use this, you actually go to the company, they provide you training and then certify you?

WALL: Yes, they do.

HARRIS: Now, have you also testified as an expert before?

WALL: Yes, I have. I have testified on three different occasions regarding technology crimes and computer examinations. And I have also been assigned as an Assistant Special Master by the Honorable Judge Humphreys of the Kern County Superior Court.

HARRIS: I'm going to direct your attention specifically in the case that you are here for. Were you asked by the Modesto Police Department to assist them in a forensic examination of some computers that have been seized from the defendant?

WALL: Yes, I was.

JUDGE: Are you going to offer him as an expert now?

HARRIS: Yes.

JUDGE: Do you want any voir dire?

GERAGOS: Is it detective?

WALL: Yes, it is.

GERAGOS: Did you say that you testified three times?

WALL: Yes.

GERAGOS: And in what courts?

WALL: In Stanislaus Superior Court. And I have testified in the Kern County Superior Court.

GERAGOS: And at all three occasions did you testify as an expert on forensic computers or computing forensics?

WALL: One of the cases was regarding a technology-related crime that did not involve computer forensics.

GERAGOS: Okay. When you say technology related crime, something that had to do with, what, an identity theft, or something like that?

WALL: It was a sexual predator that we arrested.

GERAGOS: So you were talking about, I guess, how you deal with an on-line situation?

WALL: Yes.

GERAGOS: Okay. And your expertise did not involve computer forensics in that case, correct?

WALL: That’s correct.

GERAGOS: The other two times was that one from Kern County?

WALL: No.

GERAGOS: That one was in Stanislaus?

WALL: That’s correct.

GERAGOS: And then the Kern County was on computer forensics?

WALL: Yes, it was.

GERAGOS: Was that in extracting the information from the computer?

WALL: Yes. I was assigned as an Assistant to the Special Master to deal strictly with the computers.

GERAGOS: Okay. Not one of those situations where a search is done, and then they image the computer, and then Special Master is supposed to take a look at it with you there?

WALL: Well, in this case it was not with the Special Master there. The judge gave me some leeway in that case, and I was able to examine the hard drives without the Special Master there.

GERAGOS: Okay. Did you end up testifying in that case?

WALL: The case is ongoing.

GERAGOS: So you have not testified?

WALL: I have testified regarding that case, but it's basically pretrial issues.

GERAGOS: Okay. So in terms of the actual issues of computer forensics, you haven't qualified as an expert and testified in a trial setting in that, on that case?

WALL: Not yet.

GERAGOS: Okay. So those are those two cases. There is yet a third case. Was that Stanislaus back again?

WALL: Yes.

GERAGOS: And did you testify in that case?

WALL: Yes.

GERAGOS: And was the testimony surrounding extracting information from a computer?

WALL: Yes. I had to deal with deleted files and assorted issues regarding computer forensics.

GERAGOS: Okay. And the testimony there, were you deemed to be an expert?

WALL: I don't think anyone specifically said that I was considered an expert. They stipulated to my knowledge regarding the computer use.

GERAGOS: Okay. And was that for a specific discrete issue in terms of deleted files, or something of that nature?

WALL: Yes.

GERAGOS: Okay. And so that basically in these three situations you haven't qualified as an expert in any of those three; is that correct?

WALL: Well, no one specifically said we're qualifying you as an expert.

GERAGOS: You didn't do what Mr. Harris is doing, ask you the questions, offer you as an expert, have the judge find you to be an expert?

WALL: The judge did not say anything about me being an expert, no.

GERAGOS: I believe there is an insufficient foundation.

JUDGE: I think that's for the judge to decide. All right, based on his qualifications, I'm satisfied that he's a qualified has an expert in computer forensics, qualified to give an opinion. Go ahead.

HARRIS: Thank you.

HARRIS: Detective Stockham (sic), just to go back through this a little bit. Counsel was asking you about the other case dealing with this predator case.

GERAGOS: Could I just interrupt for a second? I think you misspoke. I think this is Wall, Detective Wall.

HARRIS: I'm sorry. Detective Wall, the predator that you were being asked about on line, is that basically referring to the internet?

WALL: Yes, it is.

HARRIS: As part of your background and experience, and in doing the High-Tech Crime Task Force, do you also learn how the internet works?

WALL: Yes.

HARRIS: And in that particular case, that was specifically the issue that you were dealing with?

WALL: That’s correct. Integral part of it goes hand-in-hand with computers.

HARRIS: Now, in this particular case, the investigation that you were asked to do, or the review you were asked to do by the Modesto Police Department, did it also cause you to look at certain internet usage?

WALL: Yes, it did.

HARRIS: And so that previous experience and background, that came to play when you did this examination?

WALL: Yes.

HARRIS: I want to go back through this. You were also asked about something else Mr. Geragos said about deleted information, or discrete areas of the computer. In that particular case, let me back up, just go to something the judge had asked of another witness. For a computer, if a person deletes something from their computer, so you are using the operating system, and hit delete, what happens to that information on the computer?

WALL: Well, in most cases that information never really goes away. The analogy I like to draw for people to clearly understand is, if you took the numbers off of your house, the house is still there, it's just the address is gone. Makes it more difficult to locate. So the data is still presently there, unless it is being overwritten by other data that's being allocated to that space. Most of the files, especially in large hard drives, are still going to be there.

HARRIS: Counsel was asking you about recovery of deleted information. Can you explain to us that process, what it is that you do forensically in one of your examinations to try and recover data that's been deleted?

JUDGE: Can I just ask one, this also applies to files, which is, you know, delete files, delete history?

WALL: There is several ways that operating systems can delete files. You can manually delete something by selecting that file and selecting the delete key.

JUDGE: And click it?

WALL: Yes. It goes into the recycle bin, we can delete from. There is, also the operating system can also delete things on its own, depending on the settings that you have through your Internet Browser.

JUDGE: Supposing you get, select options, the top of your computer, and you get delete file, delete history. Does that actually eliminate the website you were looking at?

WALL: No.

JUDGE: Is it still in the computer?

WALL: In most cases it is still there, your Honor.

JUDGE: Still retrievable?

WALL: Yes, sir.

JUDGE: Go ahead.

HARRIS: Detective, let's go back through this a little bit more. The, can you, I guess for look of a better term, can you give us a breakdown in lay person's terms, how does a computer actually work?

WALL: Well, computers are basically complex electronic filing cabinets, is the easiest term that I could come up with for that. They are large capacity storage systems consisting of a processor,

memory, a hard drive, or storage device, and input and output device, such as a keyboard and a mouse. And through a series of key strokes or other input methods, files are created and can be stored on computers; and, in the same way, they can be deleted as well.

HARRIS: We have heard the term being used, operating system. What is, in fact, an operating system?

WALL: Well, typically most people are familiar with the Windows operating system. Windows 95, Windows 98, more currently Windows XP.

HARRIS: And, again, what really are those things?

WALL: They are software devices that allow us to easily use our computers and interface with them so we can use them as that massive filing cabinet.

HARRIS: Now, you are talking about the address example. The analogy of when something is deleted from the computer. When you are using the operating system, to go back to what the judge was asking you, say, for example, you go on line on the internet, is that using this operating system?

WALL: Yes.

HARRIS: Now, so you are on the internet, and you go to a particular website, and you close down your computer, or leave the browser, what happens?

WALL: Well, a lot of things happen. When you go to a website, all of that information that's from that website actually gets put into a temporary internet file or a cache file. What happened is, the text and the images basically get separated. They are all there in that same filing area, but they don't stay together like you would typically see them in a web page, or if you printed them out. So the data is all there, and can be recovered.

HARRIS: When you say the data is there and can be recovered, can you explain that process to us?

WALL: Well, the websites are there and can be recovered. When we use our forensic software to view this information, it's very similar to using your own Windows operating system. But, let's say, for example Windows Explorer if, you are familiar with that process, it is a graphical user interface that allows you to see files and folders on your computer, much in the same way that a normal user would see it in Windows. So our software allows us to view those files in the same way, except for the fact that files that are hidden by the operating system, we can see. The normal user can't, doesn't normally see those. Things that are in unallocated space we can access. So the normal user doesn't normally access the unallocated space of a computer.

HARRIS: What is unallocated space?

WALL: Well, there is basically two forms of space on a computer: Allocated space, which would be the space that you would normally access when you are using your computer, and then unallocated space. That's the things that get deleted. And when you fill your recycle bin, they go to unallocated space. When you select your Internet Browser to delete Temporary Internet Files, they get deleted in a different way, and go to the same area, unallocated space in the computer.

HARRIS: I want to go back to what you were talking about with that the address on your house. So just using that analogy, if we have the address for the house, that's the equivalent of a file. That means there is something, some address in the computer so you can find that house?

WALL: Actually the address of a house would be the equivalent of the name that, the file name. And that file name gets removed and is modified by the operating system. And, from there, we're able to shape our data mining, so to speak, to go after specific areas that are in unallocated space, that have been things that have been deleted, files that have been deleted.

HARRIS: Now, when you, if you take the address off of the house, or you change the name, or delete the name of this particular file, that's when it's assigned to this unallocated space?

WALL: That’s correct.

HARRIS: Is it still there, though?

WALL: Yes, it is. But it's available. The operating system recognizes that unallocated space as area that can then be written over with new data in allocated space.

HARRIS: You have used that term a couple of times about overwriting. What is that process?

WALL: Well, basically the computer decides what area, as new files are being created, decides what area that the new data is being written to. And it's data, as new files are being created, that information expands on the hard drive, that area of allocated space expands, and it starts taking up the unallocated space. It's a constant back and forth shifting of data that's occurring.

HARRIS: Again, kind of putting it in lay person's terms, the more you delete off of your computer, the more space that you have?

WALL: Available, that's correct.

HARRIS: Now, the data that you are deleting, though, is still there until it's overwritten?

WALL: That’s correct, because new files would then occupy that space.

HARRIS: To go back to what we were talking about in terms of the internet, you were saying that certain things happen when you go to the internet net. Does, unless you go in and delete this, does that internet information stay on your computer?

WALL: Yes, it does.

HARRIS: The judge asked, I think the term he used is, if you clear out, or hit your, delete your history, does the computer keep track of things that we do while we're on the computer?

WALL: Absolutely. It keeps track of almost everything that you do.

HARRIS: And how is that?

WALL: Well, every time that you access something like, let's say, for example, on the internet there are actually files that are created. If you view an image on a web page, that web page and its corresponding image that you are seeing gets cached or placed into the Temporary Internet Files, and a record of that is kept there until such time that that information from the Temporary Internet Files is either deleted or is, through the normal process, depending on settings of the Internet Browser, it rolls off into unallocated space.

HARRIS: And that's area where it can be reused by the computer?

WALL: That’s correct.

HARRIS: Now, if you are doing things in the computer, say, not the internet, does the computer keep track of that?

WALL: Yes, it does. Everything that the computer does, there is usually some type of a report or a log of it being that those transactions being conducted.

HARRIS: In the mechanical process of doing this, how the computer is doing this, can you explain to us what the computer does?

WALL: Well, there is, it's a pretty complex process, and I don't understand every aspect of the operating system that was designed, let's say, for example, by, in this case Windows. I don't know every little file that's created, or every issue that's created by the operating system. But there is a process that does occur where those files are saved and stored.

HARRIS: When you are talking about that, when these files are created and stored, does the computer name those files?

WALL: Yes. There is usually some type of naming convention that's associated with each file.

HARRIS: And does it give you some kind of indication as to either date and time as well?

WALL: That’s correct, it does.

HARRIS: So is that the process that you can go back, and when you do the forensic examinations, and try and figure out certain things that have been on the computer?

WALL: Yes. Specifically according to the date that it was either created or modified.

HARRIS: Now, in this particular case, the items that you were asked to look at by the Modesto Police Department, did you also deal with Detective Kirk Stockham?

WALL: Yes, I did.

HARRIS: And did he provide you with, for lack of a better term, it's been called either a cloned, or a mirrored, or forensic copies of hard drives?

WALL: Yes, he did.

HARRIS: And how many hard drives where you ultimately provided?

WALL: I started off with four, but a fifth one was added.

HARRIS: And these four, were they named by Detective Stockham?

WALL: Yes, they were.

HARRIS: And did he have what, I think you used the term earlier, some type of naming convention for those?

WALL: Yes, he did.

HARRIS: Do you recall what the naming conventions for these hard drives were?

WALL: Yes. One of them was "Dell Laptop Home 1". There was another, and I would have to refer to my report to make sure that I'm getting them all correct.

HARRIS: Let me ask you that. As part of the process of doing this for the Modesto Police Department, did you write a report?

WALL: Yes, I did.

HARRIS: And if you were to look at your report, would that help you refresh your memory as to the specifics?

WALL: Yes, it would.

HARRIS: All right.

WALL: Okay. Compaq Laptop Home 2; Dell Work PC 4; IBM Laptop Work 3; and Dell Laptop Home 1.

HARRIS: You indicated that there was an additional one that came in later. What was that one named?

WALL: That one was labeled Sotec Laptop.

HARRIS: When you received these particular hard drives for examination, these were forensic copies, so they are kind of duplicate copies of the originals?

WALL: That’s correct.

HARRIS: And did you start to go through this process, let me back up for a second. When we're talking about they are hard drives, what does that really mean?

WALL: Well, basically it's the storage device for a computer which, most people are familiar with the terminology of a hard drive. What Detective, or Officer Stockham did was create a set of image files using EnCase forensic software. And those were the set of files that he gave to me. Each one of those that were labeled by their naming convention were given to me on a hard drive. For me to be able to analyze it requires for me to use a hard drive with those bitstream image copies, the image files on them, to be able to conduct the analysis with the software that we use.

HARRIS: Now, as you said, most people are kind of familiar with hard drives at this point in time. When we're talking about hard drives, did these hard drives have a particular size?

WALL: Yes. I don't remember the exact size, but there was a total of, I think it was a little over 84 gigabytes total between all five hard drives.

HARRIS: What does that mean?

WALL: Well, the storage space that's available is measured in a lot of different formats. First came out in megabytes, you know, smaller, the older computers was smaller, the drive space was. Now we're into hard drive sizes that exceed 250 gigabytes of storage space. It's a lot of space.

HARRIS: When we are talking around, you said 80 gigabytes?

WALL: Yeah. Approximately 84 was the

HARRIS: In terms of data storage, or what you have to look at, is that a lot or a little?

WALL: That's a lot.

HARRIS: Can you give us some idea or estimate of how big that is?

WALL: Well, a typical floppy disk, most people would be familiar with that. Quite a few document files can be contained on one floppy disk. That's 1.44 megabytes of space. I don't know the exact number, and it would depend greatly on the size of the document. But if you multiply that times what is available on 84 gigabytes, which is, a gigabyte is a thousand megabytes, you have the potential for a lot of data storage on one of those, on a single hard drive.

HARRIS: Now, as you were talking about this being part of EnCase software and the use. What is EnCase software?

WALL: EnCase Forensic Software is actually a software product that was developed by Guidance Software that would enable examiners, like myself, to be able to safely view the files and operating system and the folder structure on the computers that we're examining. So basically we're able to look at that data without changing any of the evidence files. So everything remains exactly the same as when the file was, when the image files were created, when bitstream copy was made.

HARRIS: Let's just go back, make sure I understand that. So you start with this kind of cloned copy. It's a duplicate of the original?

WALL: That’s correct.

HARRIS: When you examine it, does your examination change anything?

WALL: Absolutely not.

HARRIS: So when you find something on this cloned or mirrored copy, forensic copy, you get to look and see what was on the original computer kind of in the pristine state?

WALL: That’s correct. That is also fully duplicateable as well.

HARRIS: You were talking about, with the EnCase software, say you go into the forensic copy, you find something in the unallocated, or something that's been deleted, how do you go through and recover that?

WALL: Well, there is several processes that the software allows us to do. There is specific scripts that we can run that are provided by the company, that we can say recover all web page documents. And it will automatically run a script, and it will go through the computer, through the unallocated space and extract all that data out for us. So it's pretty much an automated process.

HARRIS: And did you go through that process in this particular case?

WALL: Yes, I did.

HARRIS: What kind of these automated processes did you do?

WALL: There is quite a few of them. You can do them for key words, for searching anything in a computer for specific, key words, which is probably one of the most common processes. You can extract image files, you can shape your search to go after just about any type of, any type of data that's on the computer.

HARRIS: Let back up to the second one you mentioned about searching for image files. What is the process of doing that?

WALL: Well, it's the same. In the allocated space, we can see them freely, just like the user would. So we can go through files and folders and look where image files are contained. We can also sort specific data and say I want to see a specific type of image file format. Let's say, for example, a JPEG image, which is a very common image file. It's, the file extension is dot J-P-G. I can then sort every file using forensic software to let me see only the file extension that shows those image files. And then I can sort by date and organize them, and be able to see exactly where they are resident on the computer.

HARRIS: When you run these searches, do you just do this one hard drive at a time?

WALL: No. It can be done one hard drive at a time. But, in this case, I loaded all four hard drives, that was with the exception of the Sotec laptop. I ran this process on them simultaneously.

HARRIS: Does that speed up the process?

WALL: Yes, it does.

HARRIS: We now, so you run this across the four hard drives that you have, other than the Sotec. What do you get?

WALL: Well, depending on what data you ask for, you can get web pages, images, document files. Just whatever you are particularly looking for.

E-mail. Just depends on what you ask for.

HARRIS: What I'm basically getting to, what, you kind of get a large amount of data?

WALL: Yes. You do get a large amount of files that are extracted.

HARRIS: Now, let's go through that again. Since we're talking computer stuff here, when we are talking about data or file, is that terms that are interchangeable?

WALL: Yes.

HARRIS: Now, if you have data that is out there in the unallocated space, it's been deleted, do you have to name that to recover it?

WALL: Actually, depending on the process, well, the short question is, no, you don't have to name it.

HARRIS: If you wanted to recover that, how do you do that?

WALL: You ask it to search for a specific file extension. So if you are looking for web page documents, you would ask it for HTM, or HTML documents. It would extract all the document data A lot of these files don't have file names, because most of them are deleted from the drive. So the file naming convention doesn't stay with that file and web page documents. So the software assigns a numerical file name to it so it has some way of bringing it out to your computer so you can see it.

HARRIS: As part of the process of doing this investigation, were you actively involved in what the Modesto Police Department was doing, or were you assisting them as they asked?

WALL: They would ask me for a specific task to be done, and I would do it. I wasn't privy to their investigation information. And I was pretty much working in the background.

HARRIS: So as part of this process, I want to talk about that. Would they give you certain information to look for to see if you could find it on the computers?

WALL: Yes. They were interested in specific dates. And they were also interested in specific keywords to be looked at to see if they could be associated with any files that might have been created.

HARRIS: Were you asked to also go through and see if you could, if there were any e-mails on these computers?

WALL: Yes, I was.

HARRIS: And did you, were you asked to see if you could go through and find out if there had been any internet usage besides e-mails?

WALL: Yes.

HARRIS: Basic things of that nature, is that what they were asking you to do?

WALL: Yes. And specific dates.

HARRIS: You mentioned dates. I want to go through this process, and then have some documents that we're going to need to have marked, judge. And they are quite a few of them. So

JUDGE: Okay. Next one is 177.

HARRIS: I don't need to have this marked at this point in time. Since we're getting close to the end, I don't know if, I'll ask a few more questions, then,

JUDGE: Why don't you ask an few more questions, then we'll take the recess, then we'll mark these things tomorrow morning.

HARRIS: All right. And at some point in time, did the Modesto Police Department, as part of your search looking at these four computers, ask to see if you came across anything that dealt with going to either the San Francisco Bay, or to bay charts, or things of that nature?

WALL: Yes, it did.

HARRIS: And did you search across these computers?

WALL: Yes, I did.

HARRIS: What, if anything, did you find?

WALL: Well, I found specific information relating to fishing sites, maps, and charts. I also located information on boat want ads, and variety of information associated with fishing.

HARRIS: Now, this information about fishing, or boats, or the Bay, boats or the Bay, you did this kind of search that you are talking about, you put in the search all four computers?

WALL: That’s correct.

HARRIS: They would search for the active, or the files that you can see, and then the unallocated files that you couldn't see?

WALL: That’s correct.

HARRIS: When was the first time, or what file date did you find for these particular searches?

WALL: The first instance that I found was an allocated space, conducting the searches, was on December the 7th.

HARRIS: You say unallocated space?

WALL: In allocated space.

JUDGE: Allocated.

HARRIS: This is something that was still there, still visible on the computer?

WALL: That’s correct. That was December 7th, 2002.

HARRIS: Did you look to find out what that particular document was?

WALL: Yes.

HARRIS: What document was that?

WALL: That was a want ad pertaining to boat sales.

HARRIS: So the first time you found anything dealing with fishing, or boating, or the Bay, was on December 7th, of these want ads?

WALL: That’s correct.

HARRIS: Judge, we are going to have a number of things marked. I don't know. It's going to take some time.

<evening recess>