COURT OF APPEALS OF VIRGINIA

Present: Judge McClanahan, Senior Judge Willis and Retired Judge Fitzpatrick[*]
Argued at Richmond, Virginia

KEITH ALAN ROSA

v. Record No. 0288-05-2

OPINION BY
JUDGE JOHANNA L. FITZPATRICK
APRIL 11, 2006

COMMONWEALTH OF VIRGINIA

FROM THE CIRCUIT COURT OF CHESTERFIELD COUNTY
Cleo E. Powell, Judge

Muriel-Theresa Pitney (Joseph W. Kaestner; Kaestner & Associates, P.C., on brief), for appellant.

Eugene Murphy, Senior Assistant Attorney General (Judith Williams Jagdmann, Attorney General, on brief), for appellee.

Keith Rosa (appellant) was convicted in a bench trial of ten counts of possessing sexually explicit visual material of a person less than eighteen years of age, in violation of Code § 18.2-374.1:1. Appellant contends that the trial court erred in denying his motion to suppress pictures found on his computer during a search of the computer. Appellant argues that the officer conducting the search unreasonably exceeded the scope of the search warrant by opening files that were labeled with picture extensions. Furthermore, appellant claims that the picture files were not in "plain view" because appellant had previously deleted them and they could only be viewed by the officer after he reconstructed them with a computer program. We hold that the officer acted reasonably in opening the picture files and that the deleted files were in plain view. Thus, we affirm the judgment of the trial court.

[*] Judge Fitzpatrick prepared and the Court adopted the opinion in this case prior to the effective date of her retirement on March 31, 2006.

I. BACKGROUND

We view the evidence in the light most favorable to the Commonwealth, the party prevailing below, regarding as true all credible evidence supporting the Commonwealth's position. Summerlin v. Commonwealth, 37 Va. App. 288, 294-95, 557 S.E.2d 731, 735 (2002).

On November 1, 2003, Catherine Jackson, a twenty-year-old student, received an e-mail from appellant. In response to this e-mail, Jackson sent appellant her screen name and the two began to have conversations over the internet concerning the distribution of drugs, alcohol, and various sexual acts. Jackson contacted the police about these discussions. The police pretended to be Jackson and arranged a meeting with appellant. When appellant arrived at the meeting, the police arrested him.

On November 10, 2003, Sergeant Adrienne Meador (Meador) obtained a search warrant for appellant's computer. The warrant authorized a search for "[e]lectronic processing and storage devices, computer and computer devices . . . bearing information on conversations had with University of Richmond student Catherine Jackson (aka sweetie3637) or any other conversations or files listing screenname KAROSA72 karosa@hotmail.com with any individuals." The search warrant was issued relative to the crimes of distribution of controlled substances, distribution of controlled substances in a school zone, and providing alcohol to a person less than twenty-one. The police executed the search warrant and seized appellant's computer and computer storage devices.

Meador delivered the computer to Officer Jeffrey Deem (Deem), who specializes in technology crimes. Deem examined the computer using a program called EnCase, which is designed to recover any data located on a hard drive, whether it is an active computer file or a previously deleted file. After appellant's hard drive was copied, Deem performed keyword searches with specific words related to the terms on the warrant, such as Catherine Jackson and sweetie3637. The search program allowed a search of the contents of files as well as the names of files. Although Deem testified that chat sessions would normally be saved as files with text extensions, he also opened files that did not have text extensions, such as picture, or jpeg files, after completing the keyword search. He noted that it was common practice to manually open picture files. The reason for doing this was that any text saved as a jpeg file would not be found by only conducting a word search, and it was possible to save a chat session as a jpeg file. Several chat sessions were in fact saved in jpeg files on appellant's computer. Deem stated that he could not determine whether a particular jpeg file fell within the scope of the search warrant until he opened it to see if it contained relevant information.

While Deem was opening jpeg files, he viewed an image that he believed to be child pornography. He immediately stopped opening picture files and applied for and received a second warrant that allowed him to specifically search for sexually explicit pictures of children. Appellant had deleted the files containing child pornography from his computer, and they were visible only when Deem re-created them using the EnCase program.

Appellant was indicted on ten counts of possessing sexually explicit visual material of a person less than eighteen years of age, in violation of Code § 18.2-374.1:1. Before trial, appellant moved to suppress the images recovered from his computer. At the hearing on the motion to suppress, appellant's expert, Bruce Thompson, testified that it was not necessary to view every picture file in order to determine whether it contained text. Thompson suggested that if all the picture files on appellant's computer were relabeled with text extensions, those containing text could be opened, while those containing pictures would be unreadable by the computer. The trial judge denied appellant's motion to suppress, finding that "I don't think it's unreasonable, if it can be disguised as a JPEG file when it's actually a chat room file or a text file and would not show up with the other searches, to then open the files to make sure that it is not a chat room or a text." Appellant was convicted in a bench trial on all ten counts of possessing child pornography.

II. ANALYSIS

Appellant first contends that the search of his computer became unreasonable when Deem opened his picture files. Appellant claims that while Deem acted appropriately by searching for keywords, any actions beyond that equated to a general search of the computer and exceeded the scope of the warrant. We disagree.

Appellant has the burden of showing that the trial court's denial of his suppression motion was reversible error. Murphy v. Commonwealth, 264 Va. 568, 573, 570 S.E.2d 836, 838 (2002). A claim that evidence was seized in violation of the Fourth Amendment presents "a mixed question of law and fact that we review de novo on appeal." Id.; see Ornelas v. United States, 517 U.S. 690, 696-97 (1996). This Court gives deference to the factual findings of the trial court, but will "independently determine whether the manner in which the evidence was obtained meets the requirements of the Fourth Amendment." Murphy, 264 Va. at 573, 570 S.E.2d at 838.

A search must be conducted in a reasonable manner. Wynne v. Commonwealth, 15 Va. App. 763, 766, 427 S.E.2d 228, 230 (1993). Additionally, the scope of a search is limited by the terms of the authorizing warrant. Kearney v. Commonwealth, 4 Va. App. 202, 204, 355 S.E.2d 897, 898 (1987). However, the scope of a search extends to every place where the object of the search may reasonably be found. Id. at 205, 355 S.E.2d at 899 (citing United States v. Ross, 456 U.S. 798, 820-21 (1982)).

While we have not previously addressed the issue, a number of courts have considered whether it is reasonable for an officer executing a search of a computer to open various types of computer files and to determine whether they fall within the purview of the warrant. They have concluded that such actions are reasonable. The Tenth Circuit, in United States v. Walser, 275 F.3d 981 (10th Cir. 2001), reviewed a suppression motion where an officer opened a file with an audio-visual extension while searching for evidence of drug transactions. Id. at 984-85. While the court stated that officers "cannot simply conduct a sweeping, comprehensive search of a computer's hard drive" because of the amount of private material potentially stored there, it found the search proper because the officer used a clear search methodology and obtained a second warrant as soon as he viewed images he believed fell outside of the scope of the first warrant. Id. at 986-87. See United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (where officer did not stop his search to obtain a second warrant after viewing images believed to be child pornography, the motion to suppress should have been granted).

United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999), dealt with a factual situation similar to the instant case. Officers searching for evidence of computer trespass opened jpeg files that contained pornographic images of children. Id. at 527. After viewing the images, the officers immediately obtained a second warrant. Id. at 528. That court noted that where it is not immediately apparent whether a document falls within the scope of the search warrant, an officer has the ability to examine the item to see if it falls within the warrant's purview. Id.; see Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (finding that in the course of a valid search "some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized"). The court then held, "[i]n searching for the items listed in the warrant, [the officer] was entitled to examine all of defendant's files to determine whether they contained items that fell within the scope of the warrant." Gray, 78 F. Supp. 2d at 529. Additionally, the court found that even though there may have been less invasive ways of conducting the search, "[t]he resolution of the motion to suppress *does not turn on whether [the officer] conducted the most technically advanced search* *possible, but on whether the search, as conducted was reasonable*." Id. at 529 n.8 (emphasis added).

United States v. Triumph Capital Group, Inc., 211 F.R.D. 31 (D. Conn. 2002), also reached the same conclusion. The court held that computer searches

> are technical and complex and cannot be limited to precise, specific steps *or only one permissible method.* Directories and files can be encrypted, hidden or misleadingly titled, stored in unusual formats, and commingled with unrelated and innocuous files that have no relation to the crimes under investigation. Descriptive file names or file extensions such as ".jpg" cannot be relied on to determine the type of file because a computer user can save a file with any name or extension he chooses. Thus, a person who wanted to hide textual data could save it in a manner that indicated it was a graphics or image file. For these reasons and as a practical matter, [the officer] acted reasonably and within the scope of the warrant by opening, screening and manually reviewing data and files in all areas of the hard drive, including image files.

Id. at 47 (emphasis added).

The Court of Appeals of Indiana also refused to limit police searches to a particular type of file extension. Frasier v. State, 794 N.E.2d 449, 465 (Ind. Ct. App. 2003). The court remarked, "[t]he case before us is a case in which ambiguously labeled files were located on the hard drive and the officer had to 'open' each file before discovering its contents." Id. The court approved of the officer's actions in opening files to determine whether they contained relevant material and obtaining a warrant as soon as the officer viewed material which he suspected fell outside of the scope of the original warrant. Id.[1]

[1] See also United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) ("Computer records searches are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy."); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (disregarding file extensions when conducting a computer search "makes sense, as the user is free to name a file anything").

Commentators addressing the issue have reached the same conclusion. See Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 Miss. L.J. 193, 210 (2005) ("the more sound approach" is to allow officers to scan

We agree with the reasoning of these cases. In a search for tangible documents, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Andresen, 427 U.S. at 482 n.11. That principle applies equally to searches for electronic files. Moreover, a lawful search extends "to the entire area in which the object of the search may be found." Kearney, 4 Va. App. at 205, 355 S.E.2d at 899 (quoting Ross, 456 U.S. at 820). Therefore, officers may glance at files with various extensions in order to ascertain whether or not the files fall within the purview of the warrant. See Gray, 78 F. Supp. 2d at 528; Frasier, 794 N.E.2d at 465. Because file extensions may be misleading and may not give accurate descriptions of the material contained in the file, limiting the scope of a search to a particular file extension is an irrational restraint on the discretion of the searching officer. See Triumph Capital Group, Inc., 211 F.R.D. at 47; State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000).

Thus, the pictures obtained in this case were properly admitted. After performing a keyword search, the officer glanced at the picture files to determine whether they fell within the scope of the search warrant. The officer testified that he commonly opened picture files when conducting a computer search, because any text saved in a picture file would not be found simply by using a word search. Indeed, a number of chat sessions were located in picture files on appellant's computer. Once the officer viewed the image he believed to be child pornography, he immediately obtained a second warrant.[2] As a result the officer acted properly in opening

all documents, regardless of their file extension); David J. S. Ziff, Note, Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant, 105 Colum. L. Rev. 841, 863 (2005) (an officer's authority to search a defendant's computer "should not be limited to files with names or types that indicate the category of information authorized for seizure by the warrant").

[2] The fact that a less intrusive means of searching existed does not alter our conclusion. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995); Hogan v. Commonwealth, 15 Va. App. 355, 364, 423 S.E.2d 841, 847 (1992). The overriding question is one of

files with various extensions in order to ascertain if they contained relevant material, and the trial court did not err in denying the motion to suppress.

Appellant also contends that the computer files were not in "plain view" because they were deleted files and could only be viewed after they had been re-created using computer software. We disagree.

As noted earlier, the officer was entitled to examine all of appellant's files to determine whether they contained items that fell within the scope of the initial warrant. During the proper execution of that warrant the officer viewed pornographic images and immediately applied for a second warrant to cover the seizure of those additional items. We find no error in this procedure.

The fact that appellant had attempted to delete these files is of no moment. Deleted files have consistently been treated no differently than intact files. United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) (analogizing deleted files to a coded message or a torn ransom note); Commonwealth v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991) (likening such files to a diary written in code). The court in Copenhefer explained, "[a]ppellant's unsuccessful attempt to delete documents or files from his computer did not create a legally protected expectation of privacy which would have required a second warrant before the prosecution applied technology to elicit the content of files buried in the memory of the computer." Copenhefer, 587 A.2d at 1356. Here, Deem took the even more rigorous route of obtaining a second warrant.

The picture files at issue were saved on unallocated space. Deem testified that "unallocated space on a computer is that area of the computer where files have been in the past,

reasonableness, El-Amin v. Commonwealth, 269 Va. 15, 20, 607 S.E.2d 115, 117 (2005), and here the officer acted reasonably in opening the jpeg files to determine whether or not they contained relevant material. Although appellant's expert testified that another alternative existed, "as computer technology changes so rapidly, it would be unreasonable to require the [police] to know of, and use, only the most advanced computer searching techniques." Gray, 78 F. Supp. 2d at 529 n.8.

the area is available to be used again, but the files haven't been deleted." After appellant deleted the files, he probably would not be able to view them again: "once they are deleted, the computer is not going to through its normal interface recognize that that data is still there. I mean, I couldn't pull up Windows Explorer and say I want a file in an unallocated space."

The warrant authorized a search of all "electronic processing and storage devices, computer and computer devices, [and] external storage devices" and did not limit the search to any specific area of the computer. Deem, therefore, was permitted to look in any section of the computer that might contain the objects of the search, including deleted files that had been re-created. The deleted files are not entitled to additional protection simply because appellant attempted to erase them. See Copenhefer, 587 A.2d at 1356.

For the foregoing reasons, we affirm the judgment of the trial court.

Affirmed.