STATE OF LOUISIANA
COURT OF APPEAL, THIRD CIRCUIT

KA 11-1209

STATE OF LOUISIANA

VERSUS

TIMOTHY ERIC DAIGLE

****

APPEAL FROM THE
NINTH JUDICIAL DISTRICT COURT
PARISH OF RAPIDES, NO. 295,729
HONORABLE THOMAS MARTIN YEAGER, DISTRICT JUDGE

****

BILLY HOWARD EZELL
JUDGE

****

Court composed of John D. Saunders, Marc T. Amy, and Billy Howard Ezell, Judges.

AFFIRMED.

James C. Downs
District Attorney
701 Murray Street
Alexandria, LA 71301
(318) 473-6650
COUNSEL FOR PLAINTIFF/APPELLEE:
State of Louisiana

George Lewis Higgins, III
P. O. Box 3370
Pineville, LA 71361-3370
(318) 473-4250
COUNSEL FOR DEFENDANT/APPELLANT:
Timothy Eric Daigle

Monique Yvette Metoyer
2729 Overton St.
Alexandria, LA 71301
(318) 473-6650
COUNSEL FOR PLAINTIFF/APPELLEE:
State of Louisiana

EZELL, Judge.

On June 13, 2011, Defendant, Timothy Eric Daigle, pled guilty to one count of pornography with juveniles, in violation of La.R.S. 14:81.1. As part of his plea bargain, Defendant received a two-year hard labor sentence without benefit of probation, parole, or suspension of sentence; Defendant was credited for time served; Defendant was required to register as a sex offender, and Defendant reserved the right to contest the trial court's ruling on his motions to suppress evidence under *State v. Crosby*, 338 So.2d 584 (La.1976).

The record shows that, prior to his guilty plea, Defendant filed a "Motion to Suppress Warrant and Incorporated Memorandum" on September 25, 2009. In his motion, Defendant contended that, contrary to law enforcement's assertion that the files were in "plain sight," the files were illegally seized from Defendant's home computer as Defendant's home computer neither broadcasted nor transmitted any information concerning the content of Defendant's hard drive. Further, the prosecution did not allege that any such transmission or broadcast occurred. Defendant additionally urged that the only way the files could be viewed was through the use of complex decryption software. Defendant continued that the title "secure hash algorithm values," SHA values, implied an expectation of privacy in addition to the encryption placed on the files. The presence of a firewall on Defendant's computer also added to his expectation of privacy.

On November 30, 2009, the trial court denied Defendant's motion to suppress:

> Mr. Daigle is present. *United States versus Stults*, *S-T-U-L-T-S*, it is cited as 575 Federal 3rd, 834, and it was filed August 14, 2009, It's United States District Court the 8th Circuit Court of Appeal in Nebraska.
>
> . . . .

> And, the case says, basically, that there is no expectation of privacy on your client's part in this case. He filed sharing information that was seized by the police. There was no expectation of privacy.
>
> Basically, it says, "as a result, although it was a jail matter, an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive the defendant's decision to install and use file sharing software, thereby opening his computer to anyone else with the same freely available program." So it discusses the same issues that we have in our case with Daigle. It is completely on point with the Daigle issue. And, based upon this decision and all the cases that it cites, I'm going to deny your Motion to Suppress the evidence that was seized from Mr. Daigle, that we previously have heard testimony on.

On April 12, 2010, the defense filed a "Supplemental Motion to Suppress and Incorporated Memorandum" with the trial court. In this supplemental motion, Defendant pointed out that Detective Chad Gremillion with the Louisiana State Police testified that he did not download any files but viewed the SHA-1 values for the file, which were available to the general public. Defendant claimed that Detective Gremillion viewed the SHA-1 values by using the Wyoming Tool Kit, which has access to a database of SHA-1 values that may be associated with child pornography.

Defendant claimed that the State failed to establish probable cause because it relied solely on the information in that database, which was prohibited by the "Internet Crimes Against Children Data Network Access and Use Agreement," IDN, for the Wyoming Tool Kit. Further, the program did not vouch for the completeness or accuracy of the information contained in the "IDN." Despite this statement that the program could not guarantee the accuracy of the information, Detective Gremillion relied solely upon the database to establish probable cause. He did not actually view the files or consult with the source agency before taking action. Defendant urges, therefore, that "the warrant was not based upon proper probable cause."

On June 28, 2010, Defendant filed a "Second Supplemental Motion to Suppress" in open court. In this motion, the defense alleged that the ICAC, Internet Crimes Against Children, database only produced files possibly consistent with child pornography and that the database was not available to the public. Thus, the information contained in the affidavit supporting the warrant application was not true as the Wyoming Tool Kit and ICAC database are only available to members of law enforcement. Defendant argued that the trial court should not apply cases involving BearShare to the instant case because neither that program nor any other third-party peer sharing software was used in investigating Defendant. Defendant asserted he had an expectation of privacy because he had a binding contract with BearShare that limited file sharing access to other members.

On October 11, 2010, the district court denied Defendant's second supplemental motion to suppress. Then, on June 13, 2011, the district court clarified that it had denied relief on all of Defendant's motions to suppress. Defendant now appeals.

STATEMENT OF FACTS

The parties appeared for a pretrial discovery hearing on September 28, 2009. Defense counsel requested and received permission to proceed with the motion to suppress hearing as far as possible. Detective Chad Gremillion with the Louisiana State Police was called as the State's sole witness. Detective Gremillion was involved in investigating Defendant on October 2, 2008, when he began a peer to peer proactive investigation. During the investigation, Detective Gremillion identified an internet protocol, "IP," address, which was basically a telephone number, for a specific place where internet service was provided. Through information provided by the Wyoming Tool Kit, Detective Gremillion saw that the

IP address "had been seen" with SHA values that were consistent with child pornography.

Detective Gremillion explained that the Wyoming Tool Kit was a program designed by the Wyoming Department of Justice that ran on the Gnutella network. Software such as Limewire and BearShare also ran on the Gnutella network. The Wyoming Tool Kit identified IP addresses that had SHA values matching images previously identified as child pornography. Detective Gremillion described a SHA value as "a unique DNA fingerprint of a particular image." Every computer file was assigned either a SHA value or a MD5 value. The SHA value was an alphanumeric string of approximately sixteen characters. Different copies of the same file could not have different SHA values.

Detective Gremillion stated that, based on the information obtained from the Wyoming Tool Kit, he saw that the IP address 74.195.10.157 contained images with SHA values suspected to be child pornography. When Detective Gremillion checked, he discovered a SHA value and the filename "Daisy" that he recognized. Detective Gremillion revealed how he recognized the SHA value:

> Well, I remember them on the first three characters. For example, XQX, I know the XQX value is that of a 13-year-old girl performing oral sex on a male, and he then ejaculates into the juvenile[']s face. Well, the Daisy -- one of the Daisy series is 7 Foxtrot Foxtrot. I recognized the 7FF as being consistent with the Daisy series, which is a known series of images of child pornography, and it's known through the National Center for Missing and Exploited Children in Alexandria, Virginia.

After locating and recognizing the SHA value, Detective Gremillion ran it through the Wyoming Tool Kit. The Wyoming Tool Kit processed the image Detective Gremillion located and reported that it was a known or notable image of child pornography. Detective Gremillion next identified the person who used the IP address by using a subpoena duces tecum to get Suddenlink to reveal the physical location of the IP address at a specific time and date, which was "October 2, 2008, at 16:52 hours minus 0600." Suddenlink revealed that the IP address was assigned to a physical address on Series Street belonging to Defendant. Suddenlink was able to identify the owner of the modem because Defendant had either purchased or rented the modem from Suddenlink.

Based on the information he had obtained, Detective Gremillion applied for a search warrant. Detective Gremillion said, when he checked out the shared computer folders, he listed the three partial filenames that matched those on the Wyoming Tool Kit printout in the search warrant application: (1) PTHC5, "preteen hard core five," The Daughter is Waiting; (2) Rape, Incest, My Daughter's Five, YRcont.; and (3) Daisy-012-084-12-year Old Underage. On November 4, 2008, the Ninth Judicial District Court issued a search warrant in the case. Detective Gremillion, along with a group of other officers and Detectives, executed a search warrant at Defendant's residence on November 4, 2008, at approximately 17:29 hours. Detective Gremillion seized several computers. Detective Gremillion conducted an examination of the files on one computer and discovered that it contained images of child pornography.

Detective Gremillion explained peer-to-peer investigation. A peer-to-peer investigation involved files shared between peers. When either Limewire or BearShare was downloaded, depending on the version downloaded, the party downloading the software had the opportunity to share files with peers who had also opted to share, or the party downloading the software could have selected the option that would keep his or her files private. The software was free.

Detective Gremillion was not sure how many child pornography images were discovered during the preview of Defendant's computer. In such cases, Detective Gremillion customarily stopped looking after the first image was found.

The first image was sufficient to establish probable cause to arrest. Detective Gremillion did not remember which image he found on Defendant's computer, but he was certain it was child pornography

Detective Gremillion testified that, after completing the preview, Detective Gremillion transported the computer to the Louisiana State Police where he conducted a forensic examination of the item. This was accomplished by removing the hard drive, attaching it to a device that prevented additional files from being added to the hard drive, and processing the hard drive using "access data forensic tool kit Version 1.81." Detective Gremillion copied Defendant's hard drive and used the software to go through every sector of the computer and categorize all of the files into different categories. The categories allowed the investigator to see what was contained on the hard drive. Using this investigation technique, Detective Gremillion located the Daisy series of child pornography on Defendant's computer. Detective Gremillion explained the type of images contained in the Daisy series:

> Daisy series is a series of young, um, prepubescent females that are engaged in sexual positions. They have bows in their hair. They are naked; their legs are spread wide open with their genitalia exposed. They appear to me to be, uh, somewhat prepubescent or they do appear to be pubescent, um, and they are put in sexual positions and at the bottom there is a little title down there that has Daisy, and most of the time their file names are Daisy, uh, as in one of the cases here, it would be like Daisy-012-084, and it appears to be about a 12-year-old, underage, female engaged in sexual[ly] explicit positions.

Sometimes the file names described the contents of the images.

Detective Gremillion related that his investigation revealed eighteen photographs and two videos of child pornography. He bookmarked those files and put them in his report, which was kept with the original case file. The hard drive was then put back into evidence.

Detective Gremillion advanced that the contents of shared folders were in plain view because Defendant would have needed to enable file sharing on the computer. Detective Gremillion did not remember the files having any sort of encryption when he ran his forensic analysis of the hard drive. If decryption had been required, Detective Gremillion would have had to decrypt the file by typing in keywords. The files were not protected by a firewall because they were in a shared folder, which allowed anyone access as long as they had the same capabilities on their computer

On cross-examination, Detective Gremillion stated that the exact SHA values of the files he saw prior to the execution of the search warrant were in the discovery materials. The IP address belonged to Defendant and was assigned to his address. The peer-to-peer investigation did not specifically target Defendant; Detective Gremillion did not know the IP address belonged to Defendant. The file sharing software provided a list of regional IP addresses in the area; Detective Gremillion looked at Defendant's IP address because it was located within his jurisdiction.

Detective Gremillion testified that the Wyoming Tool Kit was made for law enforcement, and it was for use by law enforcement only. Detective Gremillion explained that the statements he made in his warrant affidavit concerning his remaining in areas only available to the general public and his use of peer to peer file sharing software available to the general public were correct:

> Because I was operating on the Gnutella network. The Gnutella network is free and available to you . . . at anytime you can download B[ear]Share or Limewire and you can access the internet at anytime.
>
> Q. Right, but what allowed you to target this address is not available to the general public, is it?
>
> A Yes, sir, it is. I can download . . . a program called PHEX, type in a key wor[d] and from there get . . . candidates who are sharing

> files. This so happen[s] to be that the Wyoming Tool Kit has made it easier for investigators to regionally locate . . . suspects in their area.
>
> Q Did you use the software that was available to the public in this investigation?
>
> A Yes, sir, the backbone of this is Limewire or B[ear]Share.
>
> . . . .
>
> . . . I did not have PHEX running that I believe.

However, the Wyoming Tool Kit that Detective Gremillion used in this investigation was not available to the general public.

Detective Gremillion thought that it was not necessary to penetrate a computer to obtain shared files. Instead, once the user gave permission for the file to be shared, the information became part of the world wide web. However, the files would have been physically stored on Defendant's computer. By sharing the files, Defendant opened the door for them to be seen by anyone walking by. Detective Gremillion still would have been able to see the files and their contents without using the Wyoming Tool Kit; the program only made it easier to look at the files. By enabling file sharing software on his computer, Defendant made it possible for Detective Gremillion, any other law enforcement officer in the country, and any other person in the world to connect to Defendant's computer and copy his shared files.

Detective Gremillion related the process of the search:

> Q Tell . . . the Judge, just how it works. You're sitting at your computer, what magic button do you press?
>
> A You click on the Wyoming Tool Kit icon on your computer.
>
> . . . .
>
> A It runs, then you open up . . . another program, called Gnu Watch, which is inside the tool kit . . . .
>
> A . . . and operates within the tool kit, I guess . . . .

A . . . simultaneously . . . .

A . . . and that in turn goes out and searches for internet protocol addresses . . . .

A . . . that have been seen with titles and SHA values . . . .

A . . . that are consistent with child pornography.

Detective Gremillion knew that the IP address had been seen with known images of child pornography because the software developers had developed the program to see files being shared between computers through accessible internet points, and the program identified the SHA values as those consistent with images known in the jurisdiction as child pornography.

Detective Gremillion clarified that he did not physically download the files and view them; instead, he relied upon the files' SHA values. Detective Gremillion did not use a search warrant to discover the IP address connected to the files; the software provided the information. Detective Gremillion then input the IP address into the system, and the software listed all of the files that have been seen at the IP address. Detective Gremillion reiterated that he used a subpoena duces tecum to link the IP address to its user.

Detective Gremillion said that the history he had of Defendant's IP address began on September 22, 2008. He conducted the investigation on October 2, 2008. Then, when the warrant issued on November 4, 2008, he conducted the search on the same date. Detective Gremillion said that one could not use filenames to determine whether images were pornographic because filenames could be changed. The process of identifying pornographic images used SHA values because they could not be altered

On redirect examination, Detective Gremillion agreed that, when he initially went into the peer-to-peer file sharing program, he was in Limewire. The Gnutella network ran LimeWire, BearShare, and a couple of other programs. The programs Detective Gremillion used, Wyoming Tool Kit and Gnu Watch, only ran on the Gnutella network. The file sharing between Defendant and Detective Gremillion occurred through a network that allowed anyone else with the same file sharing capabilities to share the same information. Detective Gremillion used the Wyoming Took Kit to substantiate that the shared files were child pornography.

On June 28, 2010, the parties again appeared in reference to a supplemental motion to suppress. At that hearing, the defense introduced into evidence a terms of use agreement for BearShare and for the Wyoming Tool Kit. The defense then stipulated that, at all times during the investigation, Defendant was under contract with BearShare.

ERRORS PATENT

In accordance with La.Code Crim.P. art. 920, all appeals are reviewed for errors patent of the face of the record. After reviewing the record, we find there are no errors patent.

DISCUSSION

Defendant argues, "The court committed reversible error when it failed to grant defendant's Motion to Suppress Evidence." Defendant urges that the search warrant was invalid because it was based on inaccurate and invalid information and that, as a result, all evidence seized as a result of the search should have been suppressed under the fruit of the poisonous tree doctrine. Defendant asserts that the trial court utilized the wrong standard for determining whether the evidence should be suppressed. Defendant asks this court to review the issue under the de novo standard of review. The State responds that this assignment of error is totally without merit.

Defendant next claims that he had an expectation of privacy in the SHA values for his files as SHA means Secure Hash Algorithm. By its very name, it implies an expectation of privacy. Moreover, Defendant had an expectation of privacy because his files were encrypted and firewall-protected. Defendant equates Detective Gremillion's viewing the SHA values for his files to a law enforcement officer climbing a fence to look inside someone's window. Defendant distinguishes the instant case from recent cases involving privacy issues where law enforcement used BearShare because the Louisiana State Police did not use BearShare. Defendant entered into a binding contract with BearShare. As part of the contract, only BearShare members had access to file sharing.

The State responds that Defendant's failure to select the option to prevent BearShare from sharing his files demonstrates that Defendant lacked a reasonable expectation of privacy. Therefore, there could be no violation of Defendant's Fourth Amendment rights.

Defendant claims that there was no probable cause to issue the search warrant. Defendant states that his arrest was based upon law enforcement's observation of files on a computer, which was linked to an unidentified modem bearing an unidentified media access control address linked to an internet protocol address that was, in turn, linked to Defendant's address. Defendant contends that the files were not discovered through "plain sight." Instead, the files were illegally seized when law enforcement extracted them from Defendant's home computer. In support of his contention, Defendant points out that his home computer did not broadcast or transmit any information about the content of its hard drive. Defendant equates the prosecution's argument that the information was available to anyone in the general public with peer-to-peer software to a claim that anyone with lock picks could unlock Defendant's front door.

Defendant further alleges that Detective Gremillion could not determine the content of a file by looking at SHA-1 values as SHA-1 values are made up of groups of numbers and letters that cannot be construed as obvious evidence. Defendant maintains that, although Detective Gremillion cross-referenced the SHA-1 values with those contained in a database of SHA-1 values that may be associated with child pornography, Detective Gremillion failed to establish probable cause because he relied solely on the word of those who privately maintained a database of values that *possibly could* be associated with child pornography. Defendant continues that the "Internet Crimes Against Children Data Network Access and Use Agreement" specifically prohibits arrests and searches based solely on the information contained in the "IDN" and requires that all data in the "IDN" be verified with the source agency prior to its use in any enforcement actions. As such, Detective Gremillion's reliance upon the Wyoming ICAC Task Force's national database, without viewing the files or consulting with the source agency, was inadequate to establish probable cause.

Defendant adds that the four points presented by the State in its application for a search warrant have all been proven to be inaccurate: (1) Detective Gremillion used a peer to peer file sharing program; (2) the program was free; (3) the program was readily available to the public; and (4) law enforcement downloaded a file from a shared folder on Defendant's computer. The Wyoming Tool Kit used by the Louisiana State Police was not a peer to peer file sharing program. The Wyoming Tool Kit does not allow file sharing at all. Thus, it could not be used to download or access any shared folders on Defendant's computer. Further, Detective Gremillion stated he never saw or opened any files from Defendant's computer. Also, the Wyoming Tool Kit is not free as it is a SHA-1 sniffing program that costs several thousand dollars. Additionally, the Wyoming

Tool Kit is not readily available to the public; one must be a sanctioned law enforcement officer before being allowed to use the program. Finally, Detective Gremillion admitted at the hearing that he had never downloaded any files from Defendant's computer and that he never had any peer to peer software installed.

Defendant contends that the affidavit submitted by the Louisiana State Police in support of the search warrant is also inaccurate as it contains a statement that, "No software other than 'peer to peer' file sharing software available to the general public, was used over the internet in order to come into contact with the possessors/distributors computer." Defendant urges that Addendum A of the ICAC Collaboration Portal requires verification by a source agency before the data could be used in enforcement actions and all users must agree to adhere to the ICAC Data Network Access and Use Agreement. Because the information supplied to the judge issuing the warrant was inaccurate, the search warrant was illegally obtained and invalid.

The prosecution replies that Detective Gremillion used the Wyoming Tool Kit in addition to the peer to peer investigation and SHA value identification. The Wyoming Tool Kit was used to identify the IP addresses that have SHA image values that match those identified as child pornography. The State continues that SHA values constitute the unique identifiers for particular images, and the SHA values cannot be changed. Detective Gremillion testified that the Wyoming Tool Kit has a program that runs on the Gnutella network and that some of the software programs on the network are Limewire and BearShare. Under those software programs, those participating have an opportunity to either share or not share files with others. Defendant did not select the option to prevent sharing. A forensic search of Defendant's computer verified the presence of child pornography.

This court has determined that the proper standard of review for examining mixed questions of fact and law on a motion to suppress is abuse of discretion:

> When a trial court rules on a defendant's motion to suppress, the appellate court must look at the totality of the evidence presented at the hearing on the motion to suppress. The appellate court should not overturn a trial court's ruling, unless the trial court's conclusions are not supported by the evidence, or there exists an internal inconsistency in the testimony of the witnesses, or there was a palpable or obvious abuse of discretion.

State v. Bargeman, 98-617, p. 5 (La.App. 3 Cir. 10/28/98), 721 So.2d 964, 967, *writ denied*, 99-33 (La. 5/28/99), 743 So.2d 658. The defendant bears the burden of proving the inadmissibility of evidence seized with a warrant. La.Code Crim.P. art. 703(D).

Federal courts have examined the issues presented in Defendant's appeal and have determined that defendants have no Fourth Amendment privacy rights in computer files that they have shared on file sharing networks such as Gnutella regardless of whether the defendants have logged onto the Gnutella network through clients such as Limewire, Morpheus, BearShare, or Shareaza. *See U.S. v. Gabel*, 2010 WL 3927697 (S.D. Fla. 2010); *U.S. v. Stults*, 575 F.3d 834 (8th Cir. 2009), *cert. denied*, ___U.S.___, 130 S.Ct. 1309 (2010); *U.S. v. Ganoe*, 538 F.3d 1117 (9th Cir. 2008), *cert. denied*, ___U.S.___, 129 S.Ct. 2037 (2009); *U.S. v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), *cert. denied*, ___ U.S. ___, 131 S.Ct. 440 (2010). This is equally true if the investigating law enforcement officer uses software specially modified to screen for child pornography, such as ShareazaLE or the Wyoming Tool Kit, provided that the software has no greater access to the defendants' computer files than that available to any other Gnutella client. *Gabel*, 2010 WL 392697; *U.S. v. Borowy*, 595 F.3d 1045 (9th Cir. 2010), *cert. denied*, ___U.S. ___, 131 S.Ct. 795 (2010).

Accordingly, Defendant’s argument that Detective Gremillion violated his right to privacy by using the Wyoming Tool Kit to examine the SHA values for files Defendant had already elected to freely share with other BearShare clients is without merit.

Furthermore, under La.Code Crim.P. art. 703(D), the defense had the burden of proving that the search warrant in the instant case was invalid. At no point in the proceedings contained in the record did the defense admit the search warrant, the search warrant application, or the warrant affidavit into evidence. Thus, they are not part of the record before this court. The only information concerning the warrant is that gleaned from Detective Gremillion’s testimony, wherein he asserts that his statements in the warrant affidavit were accurate and true. Therefore, as there is no search warrant, search warrant application, or search warrant affidavit in the record, Defendant failed to prove both that there were any false statements contained therein and, consequently, that the search warrant was issued without probable cause.

CONCLUSION

Defendant’s conviction is affirmed.

AFFIRMED.