STATE OF LOUISIANA

COURT OF APPEAL

FIRST CIRCUIT

NO. 2012 KA 0826

STATE OF LOUISIANA

VERSUS

LEVI DUNHAM

Judgment Rendered: December 21, 2012

* * * * * * * *

Appealed from the
23rd Judicial District Court
In and for the Parish of Ascension
State of Louisiana
Case No. 26,284

The Honorable Thomas J. Kliebert, Jr., Judge Presiding

* * * * * * * *

Ricky L. Babin
District Attorney
Donaldsonville, Louisiana

Counsel for Plaintiff/Appellee
State of Louisiana

Donald D. Candell
Assistant District Attorney
Gonzales, Louisiana

Jarrett P. Ambeau
Gonzales, Louisiana

Counsel for Defendant/Appellant
Levi Dunham

* * * * * * * *

BEFORE: CARTER, C. J., GUIDRY, AND GAIDRY, JJ.

GAIDRY, J.

The defendant, Levi Dunham, was charged by bill of information with seventeen counts of pornography involving juveniles, a violation of La. R.S. 14:81.1A(3) (prior to amendment by 2010 La. Acts No. 516, § 1). He pled not guilty and filed a motion to suppress. After a hearing, the district court denied his motion to suppress. Following a jury trial, the defendant was found guilty of eight counts of pornography involving juveniles.[1] The defendant was sentenced to thirty months at hard labor without the benefit of probation, parole, or suspension of sentence for each count, to be served concurrently. He now appeals, arguing that the use of technology unavailable to the public to search his computer constituted an illegal, warrantless search. For the following reasons, we affirm the defendant's convictions and sentences.

FACTS

Trooper Jared Sandifer with the Louisiana State Police became involved in an investigation of the defendant on July 19, 2009, while using peer-to-peer file sharing software called "GNU Watch." Tpr. Sandifer testified that GNU Watch searches for internet protocol ("IP") addresses that are sharing files with a known secure hash algorithm ("SHA") value, which he described as being "like a thumbprint" for a video or image. He used GNU Watch to search LimeWire, a peer-to-peer file sharing software system, for files with SHA values indicative of child pornography. According to Tpr. Sandifer, if such files were not in LimeWire or another peer-to-peer file sharing software system, GNU Watch would not detect them. He also opined that if the files were not in the LimeWire user's "shared" folder, GNU Watch would not detect them.

[1] Counts 8 and 10-16 were quashed pursuant to the defendant's motion, and the state dismissed count 6.

Through the information obtained by GNU Watch, Tpr. Sandifer saw that IP address 68.11.192.222 had files with SHA values that were consistent with child pornography. Based on this information, Tpr. Sandifer had a court ordered subpoena issued to Cox Communications, Inc., and determined that the IP address belonged to the defendant's wife. He then obtained a search warrant, and he and a group of other officers and detectives executed the search warrant at the defendant's residence. Tpr. Sandifer found a laptop computer in the residence and seized it after the defendant stated that it belonged to him. Tpr. Sandifer conducted an examination of the files on the computer and discovered that it contained images of child pornography.

The computer was then transported to the Louisiana State Police headquarters and a forensic examination was conducted by Trooper Dwight Herson, an expert in the field of forensic computer examination. Tpr. Herson testified that he was provided with a list of files that Tpr. Sandifer saw on the defendant's computer and was able to locate all of those files. When asked whether a LimeWire user would have access to the SHA value of a file on the program without the use of special police software, he responded that programs are available to obtain the SHA value of a file once the file has been transferred from LimeWire. According to Tpr. Herson, although it is not normal practice, a user could access the SHA value of a file once the user has the file.

DISCUSSION

The defendant argues that the Louisiana State Police's use of the "Wyoming Tool Kit" or GNU Watch software to search his personal computer was an illegal, warrantless search because the software is not readily available for public use. In support of his argument, the defendant

contends that SHA values are not available to the general public and special software was required to obtain the value and compare it to other known files. He also argues that LimeWire shares parts of files, rather than whole files, and that SHA values cannot be obtained from the fragments available on LimeWire through publicly available software.

When a district court denies a motion to suppress, factual and credibility determinations should not be reversed in the absence of a clear abuse of the district court's discretion, i.e., unless such ruling is not supported by the evidence. See *State v. Green*, 94-0887 (La. 5/22/95), 655 So.2d 272, 280-81. However, a district court's legal findings are subject to a *de novo* standard of review. See *State v. Hunt*, 2009-1589 (La. 12/1/09), 25 So.3d 746, 751.

At the trial of a motion to suppress, the burden of proof is on the defendant to prove the ground of his motion. La. Code Crim. P. art. 703D. The defendant also has the obligation of designating the transcript of the hearing of the motion to suppress for the record on appeal. See La. Code Crim. P. art. 914.1. The transcript of that hearing is not in the record before us. However, in determining whether the ruling on defendant's motion to suppress was correct, we are not limited to the evidence adduced at the hearing on the motion. We may consider all pertinent evidence given at the trial of the case. *State v. Chopin*, 372 So.2d 1222, n. 2 (La. 1979).

The Fourth Amendment to the United States Constitution protects individuals from "unreasonable searches and seizures." Similarly, Louisiana Constitution Article 1, Section 5 provides, "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy." Whether the Fourth Amendment protects an individual from a warrantless search rests on

whether the individual can demonstrate a reasonable expectation of privacy against government intrusion. See *Katz v. United States*, 389 U.S. 347, 350, 88 S.Ct. 507, 510, 19 L.Ed.2d 576 (1967). Only individuals who actually enjoy the reasonable expectation of privacy have standing to challenge the validity of a government search. See *Rakas v. Illinois*, 439 U.S. 128, 132, 99 S.Ct. 421, 424, 58 L.Ed.2d 387 (1978).

The issues presented in the defendant's brief were recently addressed by the Third Circuit in a factually similar case, *State v. Daigle*, 2011-1209 (La. App. 3d Cir. 5/2/12), 93 So.3d 657. In *Daigle*, Louisiana State Police detectives conducted an investigation using the Wyoming Tool Kit and discovered the defendant's IP address was seen with SHA values consistent with child pornography. At trial, the detectives explained that the Wyoming Tool Kit was designed by the Wyoming Department of Justice and ran on the Gnutella network. According to the detectives, 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. *Daigle*, 93 So.3d at 659-60. The detectives used GNU Watch in addition to the Wyoming Tool Kit, and testified that both programs only ran on the Gnutella network. *Id.* at 663. Citing several recent federal court decisions, the court found that in applying for a search warrant, the detective did not violate any reasonable expectation of privacy on defendant's part by using software available only to law enforcement to identify defendant's IP address as having SHA values that might be associated with images of child pornography. It explained:

> 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 Lime[W]ire, Morpheus, BearShare, or Shareaza. See *United States v. Gabel*, 2010 WL 3927697 (S.D. Fla. 2010); *United States v. Stults*, 575 F.3d 834, 842 (8th Cir. 2009), cert. denied, ___U.S.___, 130 S.Ct. 1309, 175 L.Ed.2d 1093 (2010); *U.S. v. Ganoe*, 538 F.3d 1117 (9th Cir. 2008), cert. denied, __U.S.__, 129 S.Ct. 2037, 173 L.Ed.2d 1122 (2009) . . . . 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 3927697; *United States v. Borowy*, 595 F.3d 1045 (9th Cir. 2010) [per curiam], cert. denied, __U.S.__, 131 S.Ct. 795, 178 L.Ed.2d 553 (2010).

Daigle, 93 So.3d at 665.

We agree with third circuit's reasoning and find that Tpr. Sandifer did not violate the defendant's right to privacy by using GNU Watch to examine the SHA values for files the defendant had already elected to freely share with other LimeWire users. Moreover, the defendant offered no evidence at trial in support of his assertion that publicly available programs are unable to obtain the SHA values of files on LimeWire, and the record does not support that argument. Therefore, the defendant's arguments related to the alleged violation of his right of privacy are without merit.

The defendant also argues that there are misrepresentations in the search warrant regarding the technology used in obtaining evidence in support of the warrant and whether that technology was publicly available, such that the evidence used against him should have been suppressed. As noted above, under La. Code Crim. P. art. 703D, the defense has the burden of proving that the search warrant was invalid. Although the search warrant application was attached to the motion to suppress, it was never introduced into evidence. It was the defendant's obligation to designate the transcript of the hearing on the motion to suppress for the record. See La. Code Crim. P. art. 914.1. We are unable to review that hearing because the defendant

failed to designate that transcript for the record. From our review of the trial transcript and the minutes from the hearing on the motion to suppress, it appears that at no point in the proceedings did the defendant introduce the search warrant or the search warrant application into evidence. The only information properly before us concerning the warrant is that gleaned from Tpr. Sandifer's trial testimony, wherein he asserts that there are programs available to the public that can be downloaded to view the information that he was able to view using the special software. As there is no search warrant or search warrant application properly before us, the defendant failed to prove both that there were any false statements contained therein and, consequently, that the search warrant was issued without probable cause. Therefore, defendant's arguments related to misrepresentations in the search warrant are without merit. See *Daigle*, 93 So.3d at 666. Accordingly, we find no error in the district court's denial of the defendant's motion to suppress.

AFFIRMED.