[Cite as *State v. Wilkie*, 2017-Ohio-1487.]

IN THE COURT OF APPEALS OF OHIO
THIRD APPELLATE DISTRICT
AUGLAIZE COUNTY

STATE OF OHIO,

PLAINTIFF-APPELLEE, **CASE NO. 2-17-01**

v.

ERIC WILKIE, **O P I N I O N**

DEFENDANT-APPELLANT

Appeal from Auglaize County Common Pleas Court
Trial Court No. 2015-CR-133

Judgment Affirmed

Date of Decision: April 24, 2017

APPEARANCES:

***Nicole Rutter-Hirth* for Appellant**

***R. Andrew Augsburger* for Appellee**

SHAW, J.

{¶1} Defendant-appellant, Eric Wilkie ("Wilkie"), brings this appeal from the December 20, 2016, judgment of the Auglaize County Common Pleas Court sentencing Wilkie to an aggregate ten-year prison term after Wilkie pled no contest to, and was found guilty of, two counts of Pandering Obscenity Involving a Minor in violation of R.C. 2907.321(A)(2), both felonies of the second degree, three counts of Pandering Obscenity Involving a Minor in violation of R.C. 2907.321(A)(5), all felonies of the fourth degree, and sixteen counts of Pandering Sexually Oriented Material Involving a Minor in violation of R.C. 2907.322(A)(1), all felonies of the second degree. On appeal, Wilkie argues that the trial court erred by denying his motion to compel the government's software that was used to find Wilkie sharing child pornography and he argues that the trial court erred by denying his amended suppression motion, particularly without an additional hearing.

Relevant Facts and Procedural History

{¶2} On November 18, 2015, Wilkie was indicted in trial court case number 2015-CR-0133 for two counts of Pandering Obscenity Involving a Minor in violation of R.C. 2907.321(A)(2), both felonies of the second degree (Counts 1 and 3), and three counts of Pandering Obscenity Involving a Minor in violation of R.C. 2907.321(A)(5), all felonies of the fourth degree (Counts 2, 4, 5). A second indictment was filed against Wilkie on February 25, 2016, alleging sixteen counts

of Pandering Sexually Oriented Material Involving a Minor in violation of R.C. 2907.322(A)(1), all felonies of the second degree. The second indictment was originally assigned case number 2016-CR-0031; however, the two indictments against Wilkie were consolidated without objection and all filings were thereafter made in the 2015-CR-0133 file. Wilkie pled not guilty to the charges against him.

{¶3} The charges against Wilkie stemmed from allegations that Wilkie was publicly sharing child pornography through an online peer-to-peer ("P2P") file sharing program called Shareaza.[1] On multiple dates Detective Jeffrey Blackmore of the Van Wert Police Department was able to download suspected child pornography from an IP address linked to Wilkie and Detective Blackmore

[1] A thorough discussion of P2P file sharing is contained in *States v. Thomas*, D. Vt, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484, which was cited by the trial court in its entry denying Wilkie's suppression motion. It provides a general overview of P2P file sharing, which reads, in pertinent part:

> **Peer-to-peer file sharing is a popular means of obtaining and sharing files free of charge directly from other computer users who are connected to the Internet and who are also using peer-to-peer file sharing software. Peer-to-peer file sharing software is publicly available for download free of charge from the Internet and operates on a particular network which dictates to some extent how the file sharing will occur.** * * *
>
> **The file sharing software does not permit a user to access files that are not available for sharing. * * ***
>
> **File sharing occurs when one computer, identified by an Internet Protocol ("IP") address, initiates a search for a responsive file by indicating the term or terms that it seeks to find in the file's name. This is called a "query" and consists of key words such as "child," "pornography," or "child pornography." Law enforcement has identified a number of search terms commonly associated with child pornography. Other computers that are using the same file sharing software and connected to the Internet at the time will respond to the query with a "query hit message." A query hit message identifies the file or files available for sharing which have a word in the file name that matches the search word in the query. The query hit message will also contain additional information such as the IP addresses of the computers offering to share responsive files. * * ***

confirmed that the files he downloaded from Wilkie's IP address did, in fact, contain child pornography. Detective Blackmore passed this information onto Detective Douglas Burke of the Auglaize County Sheriff's Office. Detective Burke used this information to obtain a search warrant to search Wilkie's residence, where more child pornography was discovered on an external hard drive, leading to further charges against Wilkie. During the search of Wilkie's residence, Wilkie spoke with Detective Blackmore and Wilkie admitted to possessing child pornography.

{¶4} On April 29, 2016, Wilkie filed an initial suppression motion, seeking to suppress the results of the search of his home on November 5, 2015, and the statements that he made on the day of the search.

{¶5} On June 30, 2016, a suppression hearing was held. At the hearing, Detective Jeffrey Blackmore of the Van Wert Police Department testified that he received training on how to use P2P file sharing programs and how to investigate those file sharing programs for individuals sharing child pornography. Detective Blackmore testified that utilizing a law enforcement-specific version of Shareaza called Shareaza Law Enforcement ("ShareazaLE"), he identified an IP address in St. Marys that had "child notable files shown in their file sharing database."[2] (June 30, 2016, Tr. at 16). Detective Blackmore testified that he initiated a "browse of

[2] Detective Blackmore explained that the "law enforcement version of the software" utilizes a database of known child pornography to search "the file sharing networks for any child sharing pornography" then it will identify the IP address where it is coming from. (June 30, 2016, Tr. at 14). He also testified that the law enforcement version will not allow file sharing; rather it only accepts downloads. (*Id*. at 31).

that person's file[s]" and that he then attempted to download the suspected child pornography files.

{¶6} Detective Blackmore testified that he downloaded five files of suspected child pornography between September 23rd and 24th of 2015 from the same IP address in St. Marys. Detective Blackmore testified that the five downloaded files did, in fact, contain child pornography. Detective Blackmore testified that he obtained a subpoena for Time Warner Cable to learn who was the subscriber attached to the IP address, and the address came back to 369 Northway Drive in St. Marys, Ohio, under a "nickname" shown as "Eric." The subscriber was Wilkie and the address was Wilkie's.

{¶7} Detective Blackmore testified that on October 18, 2015, he downloaded thirteen more suspected child pornography files from Wilkie's IP address. Detective Blackmore testified that the additional files he downloaded also contained child pornography.

{¶8} Detective Blackmore testified that he took his information to the Auglaize County Police Department and was placed in contact with Detective Donald Burke.[3] Detective Blackmore testified that he explained to Detective Burke what he had learned in his investigation, and that Detective Burke then used the information to obtain a search warrant to search Wilkie's residence.

[3] As St. Marys was in Auglaize County, Detective Blackmore sought out officers who had proper jurisdiction over the matter.

{¶9} Detective Blackmore testified that he was present when the search warrant was executed and that while he was at Wilkie's residence, he spoke with Wilkie. An audio recording of that conversation was played in open court.

{¶10} On the recording, Wilkie was explicitly informed that he was not under arrest and that he could leave at any time. Wilkie then readily admitted to having child pornography on his computer and that he had been convicted for Pandering Obscenity Involving a Minor in the past. Wilkie stated that he had a problem, that he viewed child pornography, and that he was a "collector," which is why he had all of the pornography. However, Wilkie stated that he had no desire to actually have sex with children. Nevertheless, Wilkie testified that he had viewed pornography with children as young as five or six.

{¶11} Detective Blackmore did testify that Wilkie told him that Wilkie thought he had "the share button off" on his Shareaza software. (June 30, 2016, Tr. at 31). However, Detective Blackmore emphasized when questioned by the trial court that he would not have been able to access Wilkie's files via ShareazaLE had Wilkie not been publicly file sharing them, or if Wilkie was not online. (*Id*. at 58).

{¶12} Detective Burke was the next witness to testify at the suppression hearing. He testified that Detective Blackmore came to him with the information he had and Detective Burke used it to obtain a search warrant. The search warrant itself was introduced into evidence, and it contained brief descriptions of five of the

files that had been downloaded from Wilkie's IP address. The warrant briefly explained how Detective Blackmore's investigation had proceeded and how it had led to Wilkie. The State rested after Detective Burke testified.

{¶13} Wilkie then testified on his own behalf. Wilkie testified that despite what was played on the audio of his interview he did not feel he was free to leave on the day of the search when he spoke with Detective Blackmore; however, Wilkie did admit that he was told he was free to leave. The hearing then concluded and the matter was submitted to the trial court.

{¶14} On July 12, 2016, another hearing was held wherein Wilkie notified the trial court that he had hired private counsel and wanted to replace his current court-appointed counsel. The trial court allowed Wilkie to substitute his counsel. Wilkie's new counsel then indicated that he wanted to supplement the original suppression motion. Specifically, Wilkie's new counsel indicated that he wanted to obtain an expert to show how the software the government was using to detect Wilkie purportedly sharing child pornography operated differently than it was portrayed by the government at the prior suppression hearing. Wilkie's new counsel also indicated that he may make an argument challenging the warrant itself under *Franks v. Delaware*, 438 U.S. 154, 155-156 (1978) (if a "substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if

the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request."). The trial court gave Wilkie time to secure an expert and set the matter for further hearing.

{¶15} On July 29, 2016, the trial court held further hearing on the suppression motion. At the hearing, the trial court heard arguments from the parties, but took no new evidence. The defense indicated that it had secured an expert but it needed access to a "mirror image" of Wilkie's computer for its expert to analyze in order to attempt to show that the government's software initially searched beyond what Wilkie had shared publicly in Shareaza. The defense indicated that if the government had searched Wilkie's private files, the initial search locating Wilkie would be illegal. The defense also indicated that it wanted to challenge the affidavit for the search warrant pursuant to *Franks v. Delaware*.

{¶16} The trial court ordered the State to provide the defense with a mirror image of Wilkie's computer for the defense's expert to analyze, and the trial court also ordered Wilkie's counsel to amend his motion to suppress to reflect the new suppression arguments that were being raised, particularly once his expert had analyzed Wilkie's mirrored computer.

{¶17} Consistent with the trial court's order, on September 12, 2016, Wilkie filed his supplemental motion to suppress and a motion for access to the government's ShareazaLE software. In his motion, which was filed after his expert

had analyzed the mirror image of Wilkie's computer, Wilkie argued that he now needed access to the ShareazaLE software program to establish that the government searched the non-shared files on his computer and that the government thus conducted an illegal search of his computer. Wilkie argued that while the State's officers had testified that the ShareazaLE software only searched his publicly shared files, the officers were not qualified to render such opinions.

{¶18} Further, Wilkie argued that the affidavit for the search warrant was insufficient because it did not contain a sufficient explanation of the software the government used to detect Wilkie, and that because law enforcement did not own the software, the State could not meet its burden to demonstrate that the files obtained from Wilkie's IP address were in a shared space. As a separate argument, Wilkie argued that the affidavit did not specify what software was used by law enforcement.

{¶19} Attached to Wilkie's supplemental suppression motion, and what was essentially a motion to compel access to the government's software, was a copy of Wilkie's expert's report. The report, from Tami Loehrs, indicated that Loehrs had analyzed the mirrored copy of Wilkie's computer, but *not* the external hard drive due to time constraints. The report contained the following executive summary.

> **None of the files identified during the undercover investigation were found on the computer. Although text fragments were recovered from unallocated space indicating the files or portions of the files existed at one time, I am unable to determine the**

> **content of the files, the state the files were in (completed, partial, corrupted) or whether the files were publicly available. As such, I am unable to corroborate the details set forth in Det. Blackmore's Affidavit with the forensic evidence from Mr. Wilkie's computer and the issues regarding law enforcement's proprietary software remain unanswered.**

(Doc. No. 96, Ex. 1, p. 3).

{¶20} The defense also filed a document titled "Affidavit of Tami Loehrs," in an attempt to support its motion to compel, though the "affidavit" was unsworn. The "affidavit" indicated that by the time Wilkie's computer had been seized from his residence, the operating system had been reinstalled and the files of child pornography identified during the undercover investigation were not found. (Doc. No. 100). Loehrs' "affidavit" indicated that she wanted to recreate Wilkie's computer as closely as possible to what it would have been at the time of Detective Blackmore's undercover investigation, and then use the government's software to see if it was searching beyond what Wilkie was publicly sharing—or at least had the capability to do so.

{¶21} The State opposed Wilkie's supplemental suppression motion and his motion to compel the government's software, arguing that the trial court had already heard evidence that Detective Blackmore used the law enforcement software to download child pornography files from Wilkie's *shared* space on Shareaza and that Wilkie's expert indicated in her own report that she could not contradict that testimony. Further, the State argued that *Wilkie* was attempting a "fishing

expedition," and that under *United States v. Pirosko*, 787 F.3d 358 (6th Cir.2015), it was not an abuse of discretion to deny such a request. *Pirosko* at 367 ("allowing Pirosko access [to the government's software] without any evidence of error would needlessly expose the government's enforcement tools to examination and pointlessly drag out the course of litigation.").

{¶22} In his reply, Wilkie argued it was the *government's* burden to show that the child pornography files were downloaded from his shared space, and the government had not met that burden simply through the testimony of Detective Blackmore. Wilkie maintained that Detective Blackmore was not even qualified to render an opinion that the software only searched Wilkie's shared space, despite his training.

{¶23} On October 26, 2016, the trial court filed its entry on the matter. The trial court denied Wilkie's original suppression motion, his renewed suppression motion, and his request to compel the government's software. The trial court made findings of fact, including that the defense expert's statement was unsworn and it did not qualify as an affidavit. Nevertheless, the trial court stated that there was sufficient evidence before it to determine the issues without allowing the defense expert to have access to the government's software program or have a further hearing on the matter.

{¶24} Based on the evidence presented at the suppression hearing, the trial court found that the search warrant was supported by probable cause and that there was no intentional or reckless misstatement in it that was false or misleading pursuant to *Franks*. Thus the trial court found that the search warrant was valid; however, the trial court added that even if the warrant was not valid the police conduct was still supported under the good-faith exception to the exclusionary rule pursuant to *United States v. Leon*, 468 U.S. 897, which held that, "The Fourth Amendment exclusionary rule should not be applied so as to bar the use * * * of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be invalid." *Leon* at syllabus. The trial court further found that additional discovery would not change the existence of good-faith in this case or the applicability of the good-faith exception.

{¶25} Following the trial court's denial of Wilkie's motion to compel and his suppression motion, Wilkie entered no contest pleas to all counts against him. After a factual narrative related to the charges was presented to the trial court, Wilkie was found guilty of all counts against him and he was sentenced to aggregate ten-year prison term. A judgment entry memorializing Wilkie's sentence was filed on December 20, 2016. It is from this judgment that Wilkie appeals, asserting the following assignments of error for our review.

Assignment of Error No. 1
The trial court erred in denying the Motions to Suppress.

Assignment of Error No. 2
The trial court erred in denying the request for access to the government software.

{¶26} For ease of discussion, we elect to address the assignments of error out of the order in which they were raised.

Second Assignment of Error

{¶27} In Wilkie's second assignment of error, he argues that the trial court erred in denying his motion to compel access to the government's ShareazaLE software. Specifically, Wilkie argues that an analysis of the software was relevant to the motion to suppress and to the trial, that defense had shown good cause to request access to the software as the software could potentially show that an illegal search occurred, and that the trial court improperly found that Detective Blackmore's testimony and the defense expert's report were consistent.

{¶28} We review a trial court's decision on a motion to compel discovery under an abuse of discretion standard. *See State v. Victor*, 6th Dist. Sandusky No. S-12-009, 2013-Ohio-2255, ¶ 5; *see also State ex rel. The V Companies et al., v. Marshall*, 81 Ohio St.3d 467, 469, 1998-Ohio-329. An abuse of discretion constitutes a decision that is arbitrary, unreasonable, or unconscionable. *Blakemore v. Blakemore*, 5 Ohio St.3d 217, 219 (1983).

{¶29} In this case, Wilkie's original counsel filed a suppression motion and a full hearing was held on it. At that hearing, Detective Blackmore testified that he used a law enforcement specific version of Shareaza, called ShareazaLE, to identify users sharing suspected child pornography. Detective Blackmore clearly testified as to how the ShareazaLE software worked, how it identified Wilkie's IP address as having possible child pornography that was publicly shared, and how Detective Blackmore downloaded the suspected child pornography from what he later learned was Wilkie's IP address. Detective Blackmore testified that the ShareazaLE software did not search the private spaces of Wilkie's computer, only the publicly shared files.

{¶30} After the hearing, Wilkie obtained new counsel and his new attorney indicated that he wanted to obtain an expert to dispute Detective Blackmore's claims that ShareazaLE only searched Wilkie's publicly shared files. To do this, the expert initially needed access to a mirrored copy of Wilkie's computer to analyze it. The trial court granted Wilkie's request for access to the mirrored copy of Wilkie's computer for analysis and when the analysis of Wilkie's computer was not able to corroborate or discount Detective Blackmore's testimony, Wilkie requested access to the ShareazaLE software in an attempt to show that it did not operate as Detective Blackmore claimed at the suppression hearing. The trial court denied Wilkie's request.

{¶31} In our review of the trial court's decision, we note at the outset that Wilkie has never produced any evidence at all that the ShareazaLE software used to detect Wilkie sharing suspected child pornography operated in any fashion other than what Detective Blackmore testified to. The best Wilkie could suggest to undermine Detective Blackmore's testimony was that Wilkie "thought" he had turned sharing off on his computer. Otherwise, Wilkie is only able to offer the unsworn statement of his expert that it was *possible* that if she examined the government's software it *may* operate differently than Detective Blackmore's testimony.

{¶32} An argument similar to Wilkie's was made to the Sixth Circuit Court of Appeals in *United States v. Pirosko*, 787 F.3d 358 (6th Cir.2015). *Pirosko* was another case that dealt with child pornography being shared via P2P software, and the Sixth Circuit affirmed a trial court's decision denying a defendant's motion to compel access to the government's software, ShareazaLE. The *Pirosko* court reasoned, *inter alia*, that although the government should not be given "a blank check to operate its file-sharing detection software sans scrutiny," it was "important for the defendant to produce some evidence of government wrongdoing" before going to the lengths to turn over the software. *Pirosko* at 366. The *Pirosko* court reasoned that "allowing [a defendant] access without any evidence of error would needlessly expose the government's enforcement tools to examination and

pointlessly drag out the course of litigation."[4] *Id*. at 367. *But see U.S. v. Budziak*, 697 F.3d 1105 (9th Cir.2012) (remanding a case to the trial court, under distinguishable facts, to determine whether disclosure of the government's software would have led to a different outcome in the case).

{¶33} Here, Wilkie produced no actual evidence that the government's software operated in any manner other than what was testified to by Detective Blackmore. The trial court granted Wilkie some leeway in an attempt to establish a defense by allowing him to have an expert analyze the mirrored copy of his computer. Wilkie's expert was ultimately unable to dispute Detective Blackmore's claims, and we cannot find that the trial court abused its discretion in denying a motion to compel further discovery on the matter. Therefore, Wilkie's second assignment of error is overruled.

First Assignment of Error

{¶34} In Wilkie's first assignment of error, he argues that the trial court erred in denying his motion for a *Franks* hearing, and that the trial court erred in denying his motion to suppress, particularly without holding an additional hearing on the matter. We will address each issue in turn.

[4] In *Pirosoko*, the government argued strongly for "privilege" and the Sixth Circuit applied a "balancing approach, weighing the government's concerns against the needs articulated by Pirosko." *Pirosko* at 365.

Franks Hearing

{¶35} Wilkie first argues that the trial court erred by failing to hold a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978), after he alleged in his supplemental suppression motion that the affidavit used to secure a search warrant was insufficient and that the affidavit contained at least one misstatement.

{¶36} In order to secure a *Franks* hearing, courts have held that a defendant must make a " 'substantial preliminary showing' that a deliberate falsehood or statement made with reckless disregard for the truth was included in the warrant affidavit and the statement was necessary to the judge's finding of probable cause." *United States v. Falso*, 544 F.3d 110, 125 (2d Cir.2008), quoting *Franks*, 438 U.S. 154, 155–56, 170–71. A search warrant affiant "does not *necessarily* act with 'reckless disregard for the truth' simply because he or she omits certain evidence that a reviewing court, in its judgment, considers to be 'clearly critical.' " (Emphasis sic) *United States v. Rajaratnam*, 719 F.3d 139, 154 (2d Cir.2013). "Rather, the reviewing court must be presented with credible and probative evidence that the omission of information" in a search warrant application "was 'designed to mislead' or was 'made in reckless disregard of whether [it] would mislead.' " *Id.* quoting *United States v. Awadallah*, 349 F.3d 42, 68-69 (2d Cir.2003).

{¶37} To prove reckless disregard for the truth, a defendant must show that the affiant entertained serious doubts as to the truth of his allegations. Because

states of mind must be proved circumstantially, a factfinder may infer reckless disregard from circumstances evincing obvious reasons to doubt the veracity of the allegations. *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir.2001); *States v. Thomas*, D. Vermont, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97, 2013 WL 6000484.

{¶38} In this case, the affidavit presented to obtain the search warrant stated, in pertinent part, as follows.

> **Affiant states he is a Detective with the Auglaize County Sheriff's Office * * *[.] Affiant states he has become familiar with the investigation of Det. Jeffrey Blackmore of the Van Wert Police Department.**
>
> **Det. Blackmore states that he is part of [a] task force that is involved in the [sic] investigating the trading and file sharing of child porn. During one investigation Det. Blackmore was contacted by an individual out of St. Marys, Auglaize County, Ohio. The first occurrence occurred on September 24, 2015. At that time, Det. Blackmore received five video files. The file name [sic] has a name "Webcam Omegle PTHC 2015 Sister Brother lick suck + dog GREAT!!!.avi." Within this the [sic] first video shows a pre-pubescent girl who removes her pants and is naked from the waist down, and an adult male who is wearing a mask. The girl then removes the male's pants. The male has an erection and attempts to penetrate the girl's vagina from behind and then from the front.**
>
> * * * [The affidavit then similarly describes four of the other downloaded videos containing "pre-pubescent" or "young" girls engaging in sexual acts.] * * *
>
> **On October 14, 2015, Det. Blackmore prepared a subpoena for Time Warner Cable requesting subscriber information for the IP address associated with the files that were sent to him on September 24, 2015. The IP address 184.58.67.84 came back to Eric Wilkie who resides at 369 Northway Dr., St. Marys, Auglaize**

> **County, Ohio[.] * * * Affiant states Eric Wilkie was convicted of Pandering Obscenity Involving a Minor in 1993.**
>
> **Det. Blackmore than [sic] used software available to law enforcement to track "Child Notable" computer files. These Child Notable computer files include known files that have been traded or shared on the internet that involve cases of child pornography. In searching the IP address for Eric Wilkie there are at least 67 incidents of that IP address accessing Child Notable files. He also accessed 3 child erotic files, 6 age difficult files, and 3 beastiality. These Child Notable files all have unique filed [sic] numbers that are unique just to that file. The files being shared with Det. Blackmore have the individual's nickname as "Eric".**
>
> **On October 18, 2015, Det. Blackmore received 13 more files from "Eric" from the IP address that is associated with * * * [Wilkie's residence]. All 13 videos show either pre-pubescent girls or girls between the age of 12 to 14 years of age in different states of nudity and having different forms of sexual contact or conduct.**

(June 30, 2016, Suppression Hrg., State's Ex. 1).

{¶39} On appeal Wilkie argues that the affidavit contained materially false statements and that it was insufficient. In support of his position, Wilkie contends that his expert, Tami Loehrs, presented an "affidavit" that stated that the law enforcement software actually searched the private areas of Wilkie's computer rather than the public areas, that Wilkie never "contacted" Detective Blackmore as the warrant affidavit stated, making the word "contacted" a material misstatement, and that the affidavit did not adequately describe the software used by the government.

{¶40} First, Wilkie's expert's unsworn affidavit does not go so far as to claim that the law enforcement software actually searched the private areas of Wilkie's computer to download the suspected child pornography in this case. Rather, the expert merely stated that it was theoretically possible that upon examining the government's software she could find that the government's software had such a capability. This is far from the definite statement Wilkie claims exists in the unsworn affidavit of his expert. To the contrary, the only evidence in the record, presented by Detective Blackmore, was that Wilkie's public files were searched using ShareazaLE.

{¶41} Second, as to Wilkie's claims that there was misleading information in the search warrant affidavit, we note that while the word "contacted" in the affidavit is perhaps inexact, it is not wholly inaccurate given that the law enforcement software searches for people who are actively sharing "child notable" files and the software informs the police officer when a user has been identified as sharing those files. Thus it may be inexact to state that Wilkie "contacted" Detective Blackmore when really the software was notifying Detective Blackmore that Wilkie's IP address was sharing suspect files, but being inexact does not remotely rise to the level of a *Franks* issue, and it would not defeat probable cause here.

{¶42} Third, although Wilkie argues that the affidavit was insufficient because it did not thoroughly describe the software used in this case, Wilkie ignores

the fact that a search warrant only needs to establish probable cause. The Sixth Circuit Court of Appeals considered essentially the exact same issue raised by Wilkie in this assignment of error and rejected it in *United States v. Schumacher*, 611 Fed.Appx. 337, 341 (2015), *cert. denied*, 136 S.Ct. 434 (2015). In *Schumacher*, the Sixth Circuit cited language that "probable cause [for a warrant] does not require scientific certainty." *Schumacher* quoting *United States v. Chiaradio*, 684 F.3d 265, 278-79 (1st Cir.2012). The Sixth Circuit was persuaded by the argument that the defendant "provide[d] no precedent holding that a court must assess the reliability of investigative software used to support a search warrant's affidavit before finding that probable cause for the warrant exists." *Id*. at 341. Ultimately the Sixth Circuit affirmed the trial court's refusal to hold a *Franks* hearing where the defendant was claiming that the warrant lacked probable cause because it failed to establish the scientific reliability of the government's software. We find *Schumacher* persuasive here.

{¶43} In sum, Wilkie has shown no indication that the officers provided material false statements or that they were reckless in that regard. Based on the record before us we cannot find that the trial court erred in declining to hold a *Franks* hearing. Wilkie's arguments related to *Franks* are thus not well-taken.

Suppression

{¶44} Appellate review of a motion to suppress presents a mixed question of law and fact. *State v. Burnside*, 100 Ohio St.3d 152, 2003-Ohio-5372, ¶ 8 (2003). When considering a motion to suppress, the trial court assumes the role of trier of fact and is therefore in the best position to resolve factual questions and evaluate the credibility of witnesses. *Id*. citing *State v. Mills*, 62 Ohio St.3d 357, 366 (1992). Consequently, an appellate court must accept the trial court's findings of fact if they are supported by competent, credible evidence. *Burnside* at ¶ 8 citing *State v. Fanning*, 1 Ohio St.3d 19 (1982). Accepting these facts as true, the appellate court must then independently determine, without deference to the conclusion of the trial court, whether the facts satisfy the applicable legal standard. *Burnside* at ¶ 8.

{¶45} Wilkie next argues that the trial court erred in failing to suppress the evidence against him and, at the very least, that the trial court erred by failing to hold an additional hearing on his supplemental suppression motion. More specifically, Wilkie argues that a warrantless search took place when Detective Blackmore downloaded the suspected child pornography from Wilkie. He contends that the government did not establish that the files were downloaded from the shared

space on his computer.[5]

{¶46} Contrary to Wilkie's arguments, Detective Blackmore testified that the software he used only searched shared files and that Wilkie was, in fact, sharing suspected child pornography. The trial court found that Detective Blackmore's testimony was not disputed as Wilkie's expert could not actually discount Detective Blackmore's testimony; rather, she could only state that text fragments of the files that Detective Blackmore downloaded from Wilkie were recovered on Wilkie's computer, but she could not determine whether they were in a shared space. The trial court's conclusion that the only actual evidence in the record was that Detective Blackmore downloaded the files from Wilkie's shared space was correct, and thus we cannot find that the trial court erred in denying Wilkie's suppression motion.

{¶47} Finally, we note that Wilkie seems to place a lot of emphasis on the fact that when his computer was searched in November of 2015, the files Detective Blackmore downloaded from it in September and October of 2015 were no longer

[5] It is fairly well-settled that there is no expectation of privacy in files shared over a P2P network. Various state and federal courts have held that "a defendant's utilization of a peer-to-peer file-sharing program [such as Shareaza] that allows other public users of such software to access the shared files on that defendant's computer negates any reasonable expectation of privacy in those shared files." *United States v. Dennis*, N.D. Georgia No. 3:13-cr-10-TCB, 2014 WL 1908734, *7, citing *United States v. Norman*, 448 F. App'x 895, 897 (11th Cir.2011); *see also Louisiana v. Daigle*, 93 So.3d 657, 665 (La. App.2012) citing, *inter alia*, *United States v. Gabel*, 2010 WL 3927697 (S.D.Fla.2010); *Oregon v. Holland*, 355 P.3d 194 (Or.App.2015). "This is equally true if the investigating law enforcement officer uses software specially modified to screen for child pornography, such as ShareazaLE * * * provided that the software has no greater access to the defendants' computer files than that available to any other Gnutella client." *Daigle*, citing *Gabel* and *United States v. Borowy*, 595 F.3d 1045 (9th Cir.2010).

Notably, some courts have extended this to "situations where a defendant may not have knowingly enabled the sharing feature, or even where he affirmatively attempted to opt out." *Dennis, supra*, citing *United States v. Borowy*, 595 F.3d 1045, 1048 (9th Cir.2010).

on the computer. However, it was weeks after Detective Blackmore's initial download from Wilkie's computer that Wilkie's computer was searched, so the files simply could have been deleted. This seems particularly true given that Wilkie recorded most of his pornography onto the external hard drive—an external hard drive that his expert did not analyze according to her report. Notwithstanding that point, Wilkie's expert indicated that Wilkie's operating system had been reinstalled on his computer and the prior files were essentially gone, but even with the entire operating system reinstalled, Wilkie's expert was still able to find *traces* of some of the files Detective Blackmore purportedly downloaded from Wilkie, meaning that they likely had been present, at least in some capacity.[6]

{¶48} Based on the evidence presented, we cannot find that the trial court erred in denying Wilkie's suppression motion. Similarly, we cannot find that there was any necessity for an additional hearing, particularly given that we previously determined that the trial court did not abuse its discretion in denying Wilkie's motion to compel. Therefore, Wilkie's first assignment of error is overruled.

[6] Many of Wilkie's arguments in his brief to this court and at the trial court level seem to focus more on the weight and credibility that should be given to the officers and the evidence against Wilkie, not the admissibility.

Conclusion

{¶49} For the foregoing reasons Wilkie's assignments of error are overruled and the judgment of the Auglaize County Common Pleas Court is affirmed.

Judgment Affirmed

PRESTON, P.J. and ZIMMERMAN, J., concur.

/jlr