**STATE OF MINNESOTA**
**IN COURT OF APPEALS**
**A16-0594**

State of Minnesota,
Respondent,

vs.

David Martin Arth,
Appellant.

**Filed July 3, 2017**
**Affirmed**
**Peterson, Judge**

Ramsey County District Court
File No. 62-CR-11-8857

Lori Swanson, Attorney General, St. Paul, Minnesota; and

John Choi, Ramsey County Attorney, Peter R. Marker, Assistant County Attorney, St. Paul, Minnesota (for respondent)

Cathryn Middlebrook, Chief Appellate Public Defender, Jessica Merz Godes, Assistant Public Defender, St. Paul, Minnesota (for appellant)

Considered and decided by Peterson, Presiding Judge; Cleary, Chief Judge; and Connolly, Judge.

**U N P U B L I S H E D  O P I N I O N**

**PETERSON**, Judge

In this appeal from convictions of multiple counts of possession of pornographic work involving minors, appellant argues that (1) the district court's suppression ruling must

be reversed because the search-warrant affidavit did not provide probable cause to believe that a computer identified as client ID DAAF7 would be found at his apartment on June 10, 2010; and (2) his convictions on counts 1 through 13 must be reversed because the state failed to prove that he knowingly possessed those images. We affirm.

## FACTS

Following execution of a search warrant at appellant David Martin Arth's residence and the seizure and forensic examination of a laptop computer, Arth was charged by amended complaint with 14 counts of possession of pornographic work involving a minor. Each of the charges involved a different minor identified by the National Center for Missing and Exploited Children (NCMEC).

One method for distributing child pornography is to use a peer-to-peer computer network that consists of multiple computers using the same network to share files. File-sharing software is publicly available for download under various product names, and users with file-sharing software can share files on a peer-to-peer network. To share files, the computers must have the file-sharing program open and must be connected to the Internet.

There are two classes of users on the network, peers and ultra peers. An ultra peer is a more powerful computer with a fast Internet connection, and it keeps track of which files each peer has. When a peer runs a keyword search, the ultra peer makes a direct connection between the requesting peer and other peers that have files that match the search terms.

Every computer file has a unique hash value, which is a DNA-like numeric signature. Some file-sharing programs record the Internet Protocol (IP) address of the

peers that possess a file. The IP address is a number assigned to an Internet subscriber. Some programs also record the global unique identifier (GUID), which is an alphanumeric identifier that is unique to a specific user profile on a particular computer. The IP address for a subscriber may change, sometimes frequently, but the GUID does not change.

Minneapolis Police Officer Dale Hanson is a computer forensic examiner and an investigator for the Internet Crimes Against Children (ICAC) Task Force. During an ICAC investigation in March 2009, Hanson used automated programs to search for child-pornography files on peer-to-peer networks. He learned that, on February 18, 2009, 11 known or suspected child-pornography files were on a computer with a GUID beginning with DAAF7 and an IP address ending in .139. On February 22, 2009, 12 known or suspected child-pornography files were on the same computer. On March 16, 2009, eight known or suspected child-pornography files were on the computer, and the IP address had changed to a number ending in .212. Hanson subpoenaed the subscriber information for the two IP addresses from Comcast, and Comcast provided Arth's name and an address for an apartment in St. Paul.

Hanson then referred the file to the Ramsey County Sheriff's Office. In January 2010, because the investigation had not progressed, the file was transferred to the Roseville Police Department. Hanson checked the status of the IP address ending in .212 and learned that it had last been active on the peer-to-peer network in May 2009, but the computer with the DAAF7 GUID was accessing child-pornography files on the network in May 2010.

Roseville Police Detective Maureen Sikorra became involved in the investigation in early 2010. Working with Hanson, Sikorra prepared an application, with a supporting

affidavit, for a warrant to search Arth's apartment. The affidavit contained information about Hanson's investigation. The affidavit also stated that Sikorra had confirmed that Arth still resided in the same apartment and that Arth had a 1983 fourth-degree criminal-sexual-conduct conviction.

The search warrant was issued and executed on June 10, 2010. At about 2:00 p.m., Sikorra and several other officers got a key from the apartment manager. After knocking on the door and announcing themselves as police offers, the officers used the key to enter and, as they entered, saw Arth naked. Arth claimed that he had been showering, but he was not wet and was not carrying a towel. A laptop computer with a solitaire game open was on a table. Forensic examination showed that it was the only time that the solitaire game had ever been played on the computer. During questioning later in the afternoon, Arth told Sikorra that child pornography would not be found on the computer.

Bureau of Criminal Apprehension Digital Forensic Specialist Shawn Hughes examined Arth's computer. The computer had one active user account, which required a log-in under the name David, and there was evidence that Arth had received e-mail on the computer at a Comcast e-mail address. The computer had programs capable of playing video files. The computer had been used to download multiple versions of LimeWire file-sharing software, and each version of the software matched the versions found on the computer Hanson used during his investigation. Search terms commonly used to access child pornography were recovered from the computer's browser history. The computer's registry, which tracks recently accessed files, showed that the computer was used to access child-pornography files less than one hour before the search warrant was executed.

Child-pornography images and videos were recovered from the computer. The "my-videos" directory contained a child-rape video that showed an adult male attempting to vaginally penetrate a prepubescent female.

Hughes testified that deleted files may exist in unallocated space on a computer without being associated with an existing file on the computer and that carving technology enables the recovery of some deleted files from unallocated space. Using the carving technology, Hughes recovered 115 child-pornography images and 18 child-pornography video files from Arth's computer.

The NCMEC determined that 14 files, including the child-rape video, contained child victims whose identities and ages were verifiable by law enforcement. Count 14 was based on the child-rape video. The other 13 counts were based on videos recovered from unallocated space that contained identifiable child victims.

Arth testified that he had slept very late and had just finished showering and drying off when the police entered his apartment to execute the search warrant. Arth testified that he was "sick" that he was accused of possessing child pornography and that he told Sikorra that he had no Internet access for one year. Arth claimed that he had on occasion seen child-pornography files on his computer when downloading music files, but he denied downloading the child-pornography files and claimed that he immediately deleted the files. He claimed that he first noticed child-pornography files on his computer in 2009. Arth suggested that friends could have used his computer to access the child-pornography files. He speculated that the files may have gotten onto his computer via a software bug or that they may have been planted by the police.

The jury found Arth guilty as charged. This appeal followed sentencing.

## D E C I S I O N

### I.

When reviewing the decision to issue a search warrant, a reviewing court's role is limited to evaluating whether the district court had a "substantial basis" for concluding that probable cause existed. *State v. Jenkins*, 782 N.W.2d 211, 22-23 (Minn. 2010) (quotation omitted). When reviewing the district court's probable-cause determination made in connection with issuing a search warrant, the reviewing court affords the district court's probable-cause determination great deference. *State v. Rochefort*, 631 N.W.2d 802, 804 (Minn. 2001). The resolution of doubtful cases should be largely determined by the preference accorded to warrants. *State v. Harris*, 589 N.W.2d 782, 791 (Minn. 1999).

> Probable cause should be determined under a "totality of the circumstances" test: The task of the [district court] is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before [the court], including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.

*State v. Wiley*, 366 N.W.2d 265, 268 (Minn. 1985) (quoting *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332 (1983)). "[A] collection of pieces of information that would not be substantial alone can combine to create sufficient probable cause." *State v. Jones*, 678 N.W.2d 1, 11 (Minn. 2004).

Arth argues that "[t]he warrant to search [his] residence lacked probable cause because the supporting affidavit did not provide a substantial basis for believing a computer

identified as client ID 'DAAF7' would be found there on June 10, 2010." "Probable cause not only requires that the evidence sought likely exists, but also that there is a fair probability that the evidence will be found at the specific site to be searched." *State v. Yarbrough*, 841 N.W.2d 619, 622 (Minn. 2014). A "direct connection, or nexus, between the alleged crime and the particular place to be searched" is required. *State v. Souto*, 578 N.W.2d 744, 747 (Minn. 1998). Direct observation of the evidence at the place to be searched is not necessary to establish this nexus and can instead be inferred from the totality of the circumstances. *Yarbrough*, 841 N.W.2d at 622.

Relevant factors to consider include the type of crime, the nature of the items sought, the extent of the suspect's opportunity for concealment, and normal inferences as to where the suspect would usually keep the items. *Id.* at 623. "[T]he proof must be of facts so closely related to the time of the issue of the warrant as to justify a finding of probable cause." *Souto*, 578 N.W.2d at 750. But "[t]he passage of time is less significant when the activity is of an ongoing, protracted nature." *State v. King*, 690 N.W.2d 397, 401 (Minn. App. 2005), *review denied* (Minn. Mar. 29, 2005).

Arth acknowledges that the search-warrant application may have provided probable cause to believe that the computer with GUID DAAF7 would be found at his residence in March 2009, when Hanson downloaded child-pornography files from the computer and learned that Arth was the subscriber with the IP address ending in .212. But he argues that the warrant application did not establish a connection between the computer and his residence when the warrant was executed in June 2010.

Although the .212 IP address was last online in June 2009, the computer with GUID DAAF7 continued to access and download child pornography in May 2010. The computer had been placed behind a firewall device and was reporting only its internal IP address to the peer-to-peer network. The supporting affidavit for the search warrant stated that child-pornography collectors "often maintain their collections, in a digital or electronic format, in a safe, secure, and private environment, such as a computer and/or surrounding area;" that "[c]ollectors highly value their collections and often maintain them for several years;" and that "[c]ollectors frequently keep their collection close by, usually at their residence to enable them to easily view the collection."

The supporting affidavit showed that (1) the IP address known to officers in March 2009 connected the computer with GUID DAAF7 to Arth as the account holder and to his apartment address, (2) the same computer was still being used to download child pornography in May 2010, and (3) Arth still resided at the same address. Given the nature of the child-pornography crime, this information supports an inference that Arth was continuing to use the computer at his residence to collect child pornography but was attempting to conceal his activity. Considering the totality of the circumstances, the information in the warrant application and supporting affidavit was sufficient to support the district court's probable-cause determination. *See State v. Brennan*, 674 N.W.2d 200, 206-07 (Minn. App. 2004) (concluding that, due to the expected use and storage of child pornography as described in the warrant application, sufficient nexus existed to support a warrant to search the suspect's home, even though discovery of child pornography had been limited to his work computer).

## II.

Arth concedes that the evidence was sufficient to support his conviction of count 14. He argues that the evidence was insufficient to prove that he knowingly possessed the other 13 videos on or about June 10, 2010, the timeframe stated in the complaint.

When considering a claim of insufficient evidence, this court conducts "a painstaking analysis of the record to determine whether the evidence, when viewed in a light most favorable to the conviction," was sufficient to allow the fact-finder to reach the verdict that it reached. *State v. Caine*, 746 N.W.2d 339, 356 (Minn. 2008) (quotation omitted). We must assume that the fact-finder believed the state's witnesses and disbelieved any contrary evidence. *State v. Porte*, 832 N.W.2d 303, 309 (Minn. App. 2013), *review denied* (Minn. June 16, 2015). We will not disturb the verdict if the fact-finder, acting with due regard for the presumption of innocence and the requirement of proof beyond a reasonable doubt, could reasonably conclude that the defendant was guilty of the crime charged. *Bernhardt v. State*, 684 N.W.2d 465, 476-77 (Minn. 2004).

Knowledge is an element of possession of a pornographic work involving a minor. Minn. Stat. § 617.247, subd. 4(a) (2008); *State v. McCauley*, 820 N.W.2d 577, 586 (Minn. App. 2012), *review denied* (Minn. Oct. 24, 2012). To prove a knowing violation of a statutory provision, the state must prove that the defendant knew at the time of the offense that his conduct violated the provision. *State v. Watkins*, 840 N.W.2d 21, 30 (Minn. 2013). Knowledge is generally proved by circumstantial evidence. *State v. Ali*, 775 N.W.2d 914, 919 (Minn. App. 2009), *review denied* (Minn. Feb. 16, 2010). We apply an elevated, two-step process when reviewing a conviction based on circumstantial evidence. *State v.*

*Nelson*, 812 N.W.2d 184, 188 (Minn. App. 2012). "The first step is to identify the circumstances proved." *State v. Silvernail*, 831 N.W.2d 594, 598 (Minn. 2013). In doing so, we "defer to the [fact-finder's] acceptance of the proof of these circumstances and rejection of evidence in the record that conflicted with the circumstances proved by the State." *Id.* at 598-99 (quotation omitted). Second, we "examine independently the reasonableness of all inferences that might be drawn from the circumstances proved" to "determine whether the circumstances proved are consistent with guilt and inconsistent with any rational hypothesis other than guilt, not simply whether the inferences that point to guilt are reasonable." *Id.* at 599 (quotations omitted). "We give no deference to the factfinder's choice between reasonable inferences." *Id.* (quotation omitted).

Although the evidence does not directly show when the 13 videos were deleted, it does show that they were deleted at some point. The evidence also shows that the computer was used at Arth's address to collect child pornography during 2009. LimeWire file-sharing software that was periodically updated was used with the computer to acquire the files and to search files using search terms commonly used to access child pornography. *See United States v. Ramos*, 685 F.3d 120, 132 (2d Cir. 2012) (holding that defendant's possession of child pornography was shown by evidence that he searched for and downloaded the files using the Internet and later attempted to delete temporary files and browser history from computer); *United States v. Bass*, 411 F.3d 1198, 1201-02 (10th Cir. 2005) (holding that jury could reasonably infer that defendant's efforts to sanitize his computer of downloaded child pornography files showed knowing possession of the files).

Also, the computer's registry showed that the computer was accessing child-pornography files less than one hour before the search warrant was executed. Arth did not answer the door when the officers repeatedly knocked and announced their presence. Arth was naked when the officers entered his apartment, and his claim that he had just showered was inconsistent with his appearance. The computer was open to the only solitaire game that had ever been played on it. This evidence is inconsistent with any rational hypothesis other than that Arth was deleting the child-pornography files while the officers waited for him to answer the door and opened the solitaire software for the first time to conceal his activity.

Viewing the evidence in the light most favorable to the conviction, as we must, the evidence was sufficient to prove that Arth knowingly possessed the 13 videos on June 10, 2010.

**Affirmed.**