COURT OF APPEALS
DECISION
DATED AND FILED

January 11, 2024

Samuel A. Christensen
Clerk of Court of Appeals

Appeal No. 2022AP2051-CR **Cir. Ct. No. 2017CF2831**

STATE OF WISCONSIN **IN COURT OF APPEALS**
DISTRICT IV

STATE OF WISCONSIN,

PLAINTIFF-RESPONDENT,

V.

JACOB RICHARD BEYER,

DEFENDANT-APPELLANT.

APPEAL from a judgment of the circuit court for Dane County: MARIO WHITE, Judge. *Affirmed*.

Before Kloppenburg, P.J., Blanchard, and Nashold, JJ.

¶1 BLANCHARD, J. Jacob Beyer appeals a judgment of conviction for possession of child pornography following a bench trial. The State's trial evidence centered on one digital image of child pornography that police recovered from a device seized during a search of Beyer's residence that was authorized by a

search warrant. To support the State's application for the warrant, it relied on a different digital video recording of child pornography that an investigating agent stated he had downloaded from a "peer-to-peer" file-sharing network and that the agent linked to an Internet Protocol (IP) address associated with Beyer's residence. Beyer challenges two of the circuit court's pretrial rulings and the sufficiency of the evidence to support his conviction.

¶2 In challenging one pretrial ruling, Beyer argues that the circuit court erred in denying his request for an order requiring the State to allow Beyer's expert to forensically analyze the computer that the investigating agent used to obtain the recording from the peer-to-peer network. He contends that this ruling violated what he asserts is his constitutional right to access the State's investigative computer as part of his challenge to the warrant and the search of his residence. We assume without deciding that Beyer has a constitutional right to obtain evidence that is material and favorable to his suppression motion. We conclude that he fails to make the required showing that the discovery he seeks is material and favorable to the defense.

¶3 Regarding the other challenged pretrial ruling, Beyer argues that the circuit court erred in denying his motion to suppress evidence seized pursuant to the warrant because the warrant affidavit included false information and omitted references to material facts. We conclude that Beyer fails to demonstrate that the warrant affidavit contained false information or omitted information material to the probable cause analysis. In addition, Beyer more generally contends that the court erred in denying his suppression motion because the warrant lacked probable cause. We conclude that the affidavit provided sufficient evidence to establish probable cause for the seizure of devices in Beyer's residence and for the search of those devices for evidence of child pornography.

¶4 Separately, Beyer contends that there was not sufficient evidence at trial to support his conviction. We disagree.

¶5 Accordingly, we affirm.

BACKGROUND

Peer-to-peer Networks

¶6 This court has explained the general nature of peer-to-peer networks:

> [Peer-to-peer] file sharing is a means by which computer users share digital files with other users around the world. The only requirements to access a [peer-to-peer] file sharing network are that a user have an internet connection and [peer-to-peer] software ….
>
> [A] user must have an internet connection … requir[ing] the user to make his or her internet protocol (IP) address available, because without doing so, he or she cannot connect to other users on the network to share files. An IP address is a "unique address that identifies a device on the Internet."
>
> When a file is shared on a [peer-to-peer] network, [the file] is assigned a unique digital signature, known as a hash value. A hash value assigned to a file remains constant, even if the file name is changed. When a [peer-to-peer] user selects a file to download, the [peer-to-peer] software searches the [peer-to-peer] network for all users [who] have shared a file with the corresponding hash value. The [peer-to-peer] software then connects to those users to download the file. Law enforcement has compiled a list of hash values assigned to files of known child pornography. By using this list, [law enforcement is] able to search a [peer-to-peer] network and identify users who are sharing files of child pornography.

State v. Baric, 2018 WI App 63, ¶¶3-5, 384 Wis. 2d 359, 919 N.W.2d 221 (footnotes omitted); *see also* ***id.***, ¶21 & n.6 (the defendant "peer" who used a peer-to-peer network did "not have an objectively reasonable expectation of privacy in files ... publicly shared" through the network, even though shared files were

located on the defendant's electronic device, because the files were designated for sharing on the network).

Investigation

¶7 The pertinent facts here began on October 28, 2017, when a State agent was working with investigative software specially designed for use in a peer-to-peer network. The agent would later testify that he downloaded a file that was being shared by a single device associated with a particular IP address. The agent took note of the IP address. The file was a video recording constituting child pornography.

¶8 The agent identified and then subpoenaed the internet service provider that had assigned the IP address to a user, seeking information related to the IP address. The provider responded with Beyer's name and street address. We will refer to the facts we have just summarized as those involving "the peer-to-peer evidence" or "the peer-to-peer investigation."

¶9 Relying on the peer-to-peer evidence provided by the agent, a police detective applied for a search warrant for Beyer's residence. In the warrant affidavit, the detective averred to facts involving the agent's training and general experience in investigating the sharing of child pornography through peer-to-peer networks. This application was filed on December 6, 2017, and the circuit court issued the warrant on the same day.[1]

[1] The warrant was issued by the Hon. John Hyland.

¶10 Police executed the warrant at the residence on December 7 and at that time made contact with Beyer, who made statements to police that included the following. Beyer lived alone at the residence. He owned a desktop computer, used peer-to-peer software on the computer, and used this software to download child pornography, which he viewed regularly. Beyer had deleted some files that he downloaded through peer-to-peer file-sharing, but he identified for police the file path on his computer on which other downloaded files could be located.

¶11 Police seized Beyer's computer. They located child pornography on a hard drive. The prosecution charged ten counts of possession of child pornography in violation of WIS. STAT. § 948.12 (2021-22), based on ten images.[2] None of these counts was based on the video recording that the agent downloaded in the peer-to-peer investigation.

Procedural History

¶12 Beyer filed in the circuit court a "demand for additional discovery and inspection," purportedly based in part on the federal and Wisconsin constitutions. Beyer demanded that the State allow an expert retained by Beyer to access his seized devices. The circuit court ordered the prosecution to comply with this demand, which is not at issue in this appeal.

¶13 Beyer separately demanded, and filed a corresponding motion for, access to the computer and "software configuration" used by the State agent to

[2] All references to the Wisconsin Statutes are to the 2021-22 version unless otherwise noted.

identify the peer-to-peer evidence.[3] The State declined to voluntarily provide this access and the circuit court denied the motion.

¶14 Beyer moved to suppress evidence gathered pursuant to the search warrant, arguing that the warrant was not based on a showing of probable cause, that investigators relying on the warrant knew that it lacked probable cause, and that the warrant affidavit contained materially misleading information. As part of this motion, Beyer renewed his request for an order requiring the State to provide him with access to the State's investigative computer.

¶15 The circuit court held an evidentiary hearing on the motion to suppress. The State called as witnesses the agent who conducted the peer-to-peer investigation and the police detective who applied for the search warrant and led the execution of the warrant at Beyer's residence. As discussed further below, Beyer called two forensic computer analysts.

¶16 The circuit court denied the motion to suppress as well as Beyer's motion for reconsideration. The court conducted a "stipulated trial," but the resulting conviction was reversed by our supreme court based on analysis not pertinent to this appeal.[4] *See* ***State v. Beyer***, 2021 WI 59, ¶¶1-2, 28 n.12, 397 Wis. 2d 616, 960 N.W.2d 408.

[3] For ease of reference we generally shorthand Beyer's demand and motion as being for access to the State's investigative computer, recognizing that he sought access to all software systems and settings used by the agent as part of the peer-to-peer investigation.

[4] The Hon. William Hanrahan presided over pertinent pretrial proceedings and the stipulated trial that followed. After remand from our supreme court, the Hon. Mario White presided over the trial to the court that is at issue in Beyer's challenge to the sufficiency of the evidence.

¶17 Following remand, the State pursued a single count of possession of child pornography in a trial to the court, based on the allegations relating to one digital image. The parties stipulated that the images underlying the nine other then-dismissed counts in the complaint could be admitted as other-acts evidence. *See* WIS. STAT. § 904.04(2) ("evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show that the person acted in conformity therewith," but can be "offered for other purposes"); ***State v. Sullivan***, 216 Wis. 2d 768, 772, 576 N.W.2d 30 (1998).

¶18 The circuit court found Beyer guilty and this appeal follows.

DISCUSSION

I. Motion to allow forensic analysis of the State's investigative computer

¶19 Beyer does not base an argument on his statutory criminal discovery rights under WIS. STAT. § 971.23(1), which enumerates categories of materials that a district attorney must disclose to a defendant. Instead, he relies exclusively on what he asserts are constitutional requirements to make what he acknowledges is a novel argument. The novel argument is that the circuit court violated his constitutional rights when it denied his request for an order allowing his expert to forensically analyze the computer that the agent used to allegedly detect the peer-to-peer evidence supporting the search warrant. Specifically Beyer directs us to due process-based rights referred to in case law as the right to access evidence and also to the right to present a "complete defense." *See* ***State v. Weissinger***, 2014 WI App 73, ¶8, 355 Wis. 2d 546, 851 N.W.2d 780 (due process requires that criminal defendants are given "'a meaningful opportunity to present a complete defense'" (quoting ***California v. Trombetta***, 467 U.S. 479, 485 (1984))).

¶20 Beyer contends that these rights entitle him to an order allowing his expert to access and analyze the State's investigative computer to pursue a potential ground for suppressing evidence obtained pursuant to the search warrant. That ground for suppression would be problems with the peer-to-peer investigation that Beyer anticipated would be revealed by his expert's analysis. To support this theory, Beyer relies on testimony by the investigating agent and the expert called by Beyer to the effect that there could be, at least in theory, circumstances in which the accuracy of the peer-to-peer investigative software could be called into question or in which it could be manipulated to create the false impression that a user of the computer had accessed a shared file. As we now proceed to explain, we assume without deciding that Beyer has a constitutional right to evidence that is material to a defense seeking to suppress evidence under the Fourth Amendment and, with that assumption, we reject his argument based on our conclusion that he fails to show that the discovery he seeks is material and favorable to the defense.[5]

¶21 To provide context for Beyer's novel constitutional argument we now review some orienting points of law.

¶22 Defendants in criminal cases do not have a general constitutional right to review all of the materials in the State's possession. *See* ***State v. Humphrey***, 107 Wis. 2d 107, 116 n.4, 318 N.W.2d 386, 391 (1982) ("'There is no general constitutional right to discovery in a criminal case, and ***Brady*** [***v.***

[5] In support of Beyer's argument on this issue, he cites to a per curiam opinion of this court. Under WIS. STAT. RULE 809.23(3), we disregard this citation and remind Beyer's counsel that we expect compliance with the rules of appellate procedure. *See* RULE 809.23(3)(a)-(b) (per curiams "may not be cited in any court of this state as precedent or authority, except to support a claim of claim preclusion, issue preclusion, or the law of the case").

Maryland, 373 U.S. 83 (1963)] did not create one'" (quoting ***Weatherford v. Bursey***, 429 U.S. 545, 559 (1977))). At the same time, defendants do have a right to obtain from the State "any favorable evidence 'material either to guilt or to punishment' that is in the State's possession." ***State v. Wayerski***, 2019 WI 11, ¶35, 385 Wis. 2d 344, 922 N.W.2d 468 (quoting ***Brady***, 373 U.S. at 87).

¶23 Another pertinent orienting principle is that some categories of defense motions to suppress prosecution trial evidence are based at least in part on the alleged lack of relevance or reliability of the evidence to prove the defendant's guilt, which may be contrasted with those suppression motions that seek to exclude potential trial evidence purely as a disincentive for unconstitutional police conduct. *See* ***State v. Felix***, 2012 WI 36, ¶30, 339 Wis. 2d 670, 811 N.W.2d 775 (the primary purpose of the exclusionary rule is to deter future unlawful police conduct). In the pure-deterrence situation there is often no issue about the relevance or reliability of the evidence for use at trial. In contrast, however, some motions to suppress are based, at least in part, on suppression theories of relevance or reliability. Examples include a claim that a confession is involuntary or that an out-of-court witness identification was improperly obtained. *See* ***Dickerson v. United States***, 530 U.S. 428, 432-33 (2000) (one constitutional basis for excluding involuntary confessions is the due process-related concern that they are inherently untrustworthy); ***State v. Roberson***, 2019 WI 102, ¶26, 389 Wis. 2d 190, 935 N.W.2d 813 (due process can restrict admission of identification evidence based on its lack of reliability).

¶24 With all of that context in mind, here Beyer sought evidence or information regarding the peer-to-peer investigation that does not directly relate to the evidence that the prosecution offered at trial to prove the single charged count of possession of child pornography. In other words, he does not make a developed

argument that he was not allowed to challenge unreliable or irrelevant trial evidence, or indeed that he was prohibited from challenging any trial evidence at all.[6] Instead, Beyer sought this evidence or information in an attempt to bolster his efforts to suppress evidence found on his seized computer following execution of the search warrant that was based on an alleged video recording that the prosecution did not offer as evidence at trial. In moving for a Fourth Amendment-based application of the exclusionary rule, Beyer sought suppression purely for the purpose of deterring police misconduct in obtaining the evidence, regardless of its reliability or relevance to the charged offense.

¶25 Yet Beyer relies on U.S. Supreme Court cases that address evidence that is at least potentially material to guilt or punishment based on the charged offenses. *See, e.g.*, ***Brady***, 373 U.S. at 87-88; ***United States v. Valenzuela-Bernal***, 458 U.S. 858, 867-70 (1982); ***Trombetta***, 467 U.S. at 488-89; *see also* ***Arizona v. Youngblood***, 488 U.S. 51, 55-56 (1988); note 13, *infra*. These "access to evidence" cases do not address a constitutional right of a criminal defendant to access evidence or information that is material only to an allegation in a challenged search warrant, and that is not based on the irrelevance or unreliability of that allegation to prove a charged crime at trial.

¶26 Similarly, Beyer fails to direct us to a Wisconsin opinion in which a defendant's due process rights have been extended to require circuit courts to

[6] In his reply brief on appeal, Beyer suggests that the computer access he seeks could also have value as a basis to impeach the agent at trial, but this argument is undeveloped. Left unanswered, for example, is how Beyer could have successfully impeached the agent regarding any aspect of the one image that was central at trial or the other images that the State relied on as other-acts evidence. Further, the argument comes too late, appearing for the first time in the reply brief.

order prosecutors to provide defendants with access to evidence or information that is not material to guilt or punishment. He cites to our decision in ***State v. Maday***, 179 Wis. 2d 346, 354, 507 N.W.2d 365 (Ct. App. 1993), in which we stated broadly that "pretrial discovery is a fundamental due process right." As Beyer acknowledges, however, the articulation of this discovery right in ***Maday*** involved, in the court's words, "nothing more than the right of the defendant to obtain access to evidence necessary to prepare his or her case *for trial*." ***Id.*** (emphasis added). In ***Maday***, we determined that, when the prosecution presents expert testimony regarding a victim's mental state, a defendant might be entitled to the psychological examination of an alleged victim in order to maintain "a level playing field" at trial. *See* ***id.*** at 357, 360-61. In sum, Beyer seeks what appears for purposes of Wisconsin law to be a novel extension of due process principles governing "access to evidence." Specifically, he seeks to extend these due process principles to evidence or information that relates exclusively to search warrant allegations when the evidence or information could potentially support a pretrial motion based on the Fourth Amendment to suppress evidence obtained through execution of the search warrant.

¶27 Toward that end, Beyer directs us to persuasive authority from other jurisdictions. In particular, he cites one case as persuasive authority for the rule that the failure to disclose evidence or information material to a potential Fourth

Amendment-based suppression motion can violate a constitutional right.[7] *See* ***Biles v. United States***, 101 A.3d 1012, 1018-20 (D.C. 2014) ("the failure to disclose information material to a pretrial suppression ruling can implicate ***Brady***," including in the context of a suppression motion based on an allegation of an illegal search); *see also* ***United States v. Barton***, 995 F.2d 931, 935 (9th Cir. 1993) (holding that "due process principles announced in ***Brady*** and its progeny must be applied to a suppression hearing involving a challenge to the truthfulness of allegations in an affidavit for a search warrant" in order to "protect the right of privacy"). We assume without deciding that, consistent with the reasoning in these cases, Beyer's right to access evidence or information in the possession of the State and to prepare a defense includes the right to access evidence or information that could support an argument for an order based on the Fourth Amendment excluding the prosecution at trial from offering other evidence.

¶28 But Beyer concedes that applying the principles of case law such as ***Brady*** in this context requires that he show the following: the evidence he seeks is "favorable" and "material" to his defense. *See* ***Biles***, 101 A.3d at 1017; ***Wayerski***, 385 Wis. 2d 344, ¶35.[8] Thus, to establish materiality, Beyer must show that

[7] For persuasive authority, Beyer also relies on several federal court decisions that apply Federal Rule of Criminal Procedure 16, which addresses in pertinent part the obligations of federal prosecutors to disclose information to a defendant. *See* Fed. R. Crim. P. 16(a)(1). After the State argues that this federal rule allows access to evidence that is "material to preparing the defense" and that this is broader than any applicable constitutional or Wisconsin statutory discovery right, Beyer does not reply. This concedes for purposes of this appeal that authority interpreting Fed. R. Crim. P. 16 is not apt here. *See* ***State v. Dieter***, 2020 WI App 49, ¶10 n.3, 393 Wis. 2d 796, 948 N.W.2d 431.

[8] A third requirement to support a claim under ***Brady v. Maryland***, 373 U.S. 83 (1963), is that the evidence a defendant seeks was either willfully or inadvertently "suppressed" by the government. ***State v. Wayerski***, 2019 WI 11, ¶35, 385 Wis. 2d 344, 922 N.W.2d 468; *see also* ***Biles v. United States***, 101 A.3d 1012, 1017 (D.C. 2014). It is not disputed here that the State denied Beyer's request for access to the State's investigative computer.

disclosure of the evidence that he seeks would have created "'a reasonable probability'" of a different outcome at the suppression hearing. *See* ***Biles***, 101 A.3d at 1017 (citing ***United States v. Bagley***, 473 U.S. 667, 682 (1985)); ***Wayerski***, 385 Wis. 2d 344, ¶36 (citing ***Strickler v. Greene***, 527 U.S. 263, 281 (1999)).

¶29 Beyer argues that his expert's testimony at the suppression hearing establishes materiality, given the fact that the alleged peer-to-peer evidence was not found on his computer during or after the execution of the search warrant at his residence. More specifically, he contends that the testimony of his expert describes: a "well-documented … susceptibility" which is specific to the type of peer-to-peer network used by investigators; the "manner by which" an alleged "exploit"—that is, a flaw or vulnerability in the software used to access the peer-to-peer network—"could be used to manipulate files on the [peer-to-peer] network"; and "how the file that the State claims to have detected seems to have briefly appeared and then disappeared by either malfeasance or malfunction."

¶30 Beyer's primary expert, Nicholas Schiavo, testified in pertinent part:

> [I]n this particular [peer-to-peer network] program, there was a flaw in the program, and [the flaw] allowed [the program] to be exploited by any user with a web browser.
>
> ….
>
> Anybody [who] was aware of the exploit could go back to anybody sharing a file [on the network] and see anywhere on [the second person's] computer, add files, subtract files, delete files, move them around, and it would appear as if it all happened in the shared folder because the way it works is it allows the bad actor to designate anywhere on the computer as the shared folder and look around [on the hard drive of the computer] and then manipulate it.

Under this view, the alleged opportunity to take advantage of the vulnerability in the peer-to-peer network would have made it possible for a third party—in theory including the agent—to plant the peer-to-peer evidence in Beyer's shared folder without his knowledge. This opportunity to trick or mislead anyone who might later examine the system regarding who possessed a file would have been available during the time period when the investigating agent allegedly detected the peer-to-peer evidence in the shared folder of Beyer's computer.

¶31 Asked whether there was evidence that this vulnerability had in fact been used in this way with Beyer's software, Schiavo's response was to note that the peer-to-peer evidence was not found on Beyer's computer after the warrant was executed. Yet Schiavo also acknowledged another possibility. This is that the absence of the file could have been the result of Beyer, or another user, downloading the file through the network, later deleting it, and writing over the data in the file.[9] Schiavo further testified that, if he could access and analyze the State's investigative computer, he could rule in or out whether the State's computer could use the vulnerability to manipulate files on Beyer's computer. He also testified that it is possible that there could be evidence in the State's

[9] As a general matter, deleted files can be recovered from "unallocated space" on a hard drive unless the data in that space is written over by new data. *See* ***State v. Gralinski***, 2007 WI App 233, ¶¶8, 31, 306 Wis. 2d 101, 743 N.W.2d 448; ***United States v. Hill***, 750 F.3d 982, 987 n.6 (8th Cir. 2014) ("'Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder …. Such space is available to be written over to store new information.'" (quoting ***United States v. Flyer***, 633 F.3d 911, 918 (9th Cir. 2011); emphasis in ***Hill*** omitted)).

investigative computer logs that would show whether the vulnerability could have been used by some unknown third party.[10]

¶32 The agent who conducted the peer-to-peer investigation testified in pertinent part as follows. Both the peer-to-peer software used by Beyer and the law enforcement software used to investigate Beyer could be subject to "malware."[11] The agent also acknowledged the existence of the vulnerability described by Schiavo. But the agent further testified that he had never encountered a situation in which either malware or the vulnerability were the cause of a suspect's computer sharing child pornography on a peer-to-peer network.[12] The circuit court credited the agent's testimony, finding that there was "no … evidence or any suggestion" that the agent was "untruthful."

¶33 Bearing this background in mind, we conclude that, given the equivocal nature of Schiavo's testimony regarding mere "possibilities" regarding what information might be contained on the State's investigative computer, Beyer fails to establish a reasonable probability of a different outcome for his motion to

[10] Schiavo also made a reference to the software on the State's investigative computer also being subject to the same vulnerability. But he did not explain what bearing this could have on the agent's testimony that the peer-to-peer evidence was being made available through the shared folder on Beyer's computer.

[11] Malware is "a malicious program designed to do harm to a computer or its user." *See* ***State v. Gratz***, No. 2021AP1281-CR, unpublished slip op. ¶18 (WI App Oct. 13, 2022).

[12] The agent testified that he had been involved in "at least" 25 investigations related to the use of peer-to-peer networks and child pornography.

suppress if he were given access to the computer. The argument is heavily speculative, depending on a series of "what ifs."[13]

¶34 Beyer argues that failing to grant him access to the State's investigative computer—when the State used peer-to-peer-based evidence to obtain a search warrant but then did not use that evidence to support a criminal charge against him—renders "inscrutable" the process the State used to secure the search warrant. Absent a showing of a potential violation of his rights, however, this and related arguments that Beyer makes amount to potential policy concerns that do not show a reversible error based on any statute or constitutional provision.

[13] Although Beyer invokes in general terms the right to access evidence noted in ***Trombetta***, he does not cite to the Supreme Court's related decision in ***Youngblood***. That is, Beyer does not make the alternative argument that this case is analogous to the ***Youngblood*** scenario, in which a defendant seeks evidence to which the defendant lacks access due to government destruction of, or failure to preserve, the evidence. *See* ***State v. Weissinger***, 2014 WI App 73, ¶10, 355 Wis. 2d 546, 851 N.W.2d 780 (discussing ***Arizona v. Youngblood***, 488 U.S. 51, 55-56 (1988)). Under this line of cases, the defendant can carry his or her burden by showing that unavailable evidence is merely "'potentially useful.'" *See* ***id.*** (quoted source omitted). However, even putting aside his failure to raise such an argument in this appeal, to the extent it may be implied in arguments that he does make, he has the following problem. Even if the ***Youngblood*** test would apply in this context, a defendant who cannot show that the evidence sought is "apparently exculpatory" must show that "the police … act[ed] in bad faith by failing to preserve evidence that is potentially exculpatory." ***Id.*** "Bad faith can only be shown if '(1) the officers were aware of the potentially exculpatory value or usefulness of the evidence they failed to preserve [or by analogy here, grant access to]; and (2) the officers acted with official animus or made a conscious effort to suppress exculpatory evidence.'" ***Id.*** (quoted source omitted; emphasis in ***Weissinger***). The expert testimony presented by Beyer at the motion hearing does not establish that the evidence sought is apparently exculpatory—Schiavo could not testify to a problem he would find in his analysis, but instead provided only vague speculation. Nor did Schiavo's testimony establish the required showings for "bad faith" in this context because, to repeat, the testimony merely demonstrates the existence of various exculpatory possibilities for how the file shared from Beyer's computer could have gotten there. Moreover, the circuit court found that the agent was credible in his testimony that he had not encountered a problem with malware or the vulnerability when using the investigative computer on numerous occasions.

II. Suppression Motion

¶35 Beyer makes two arguments in support of the proposition that the circuit court erred in denying his motion to suppress evidence recovered pursuant to the search warrant.

¶36 He contends that the warrant was invalid because the supporting affidavit contained deliberately misleading information and omitted relevant information. On that issue, for reasons explained below, we conclude that Beyer fails to meet his burden under ***Franks*** to show that material in the warrant application should be "set to the side," or that material information was omitted. *See* ***State v. Manuel***, 213 Wis. 2d 308, 313, 570 N.W.2d 601 (Ct. App. 1997) (probable cause analysis under ***Franks*** "'set[s] to one side'" warrant application's "'false material[s]'" (quoting ***Franks v. Delaware***, 438 U.S. 154, 155-56 (1978))).

¶37 Beyer also contends that the warrant affidavit failed to state probable cause sufficient to support the issuance of the warrant for a search of Beyer's residence for child pornography. On that issue, as separately explained below, we conclude that the application established probable cause.[14]

¶38 Before explaining our conclusions further, we first make a preliminary point about what Beyer is not arguing on appeal. Beyer does not argue staleness. That is, he does not base an argument on the passage of time between the agent's identification of the peer-to-peer evidence and either the application for, or the execution of, the warrant. The interval here was a little over

[14] Because we conclude that the warrant affidavit established probable cause, we do not reach the parties' arguments regarding whether the good faith exception applies to prevent the suppression of the evidence obtained in connection with the execution of the warrant.

one month (late October to early December 2017), as measured either from either the date of application or the date of execution, and Beyer does not argue that this was too long. *See* ***State v. Gralinski***, 2007 WI App 233, ¶¶4-7, 30-31, 306 Wis. 2d 101, 743 N.W.2d 448 (two-and-a-half-year delay between defendant's use of credit card to access a website containing child pornography and execution of warrant did not render probable cause stale because of the tendency of individuals interested in child pornography to retain it and the potential for authorities to recover deleted images). Rather, we interpret Beyer's probable cause arguments to rest on the proposition that the affidavit did not establish a sufficient likelihood that police would discover child pornography on any device found in Beyer's residence for the following specific reason: there was not sufficient evidence that Beyer possessed and then would retain on a device in his possession, through the time of the search, the particular child pornography identified by the agent.

Additional Background

¶39 Many of the detective's averments in the warrant affidavit were based on the asserted training and experience of the investigating agent, as related to the detective. The averments included the following:

> [I]ndividuals who have an interest in child pornography or child sexual exploitation tend to retain any images or videos they obtain that depict such activity or maintain their interest in such depictions so that it can reasonably be expected that similar evidence of that sexual interest in children or interest in child sexual exploitation will be found in their computer(s) or other digital devices or storage media, or found in other forms in their private places. The possession, or apparent possession, of sexually explicit depictions of children, like those described in this affidavit, is consistent with a sexual interest in children or an interest in the sexual exploitation of children.

¶40 During the agent's testimony at the suppression motion hearing, the prosecutor asked how common it is that a file containing alleged child pornography that has been observed through a peer-to-peer network is not then found during the execution of a subsequent search warrant at a place associated with the observed file. The agent was also asked for his general observations regarding the typical habits of individuals who view and collect child pornography. The agent answered:

> There's been a majority of cases where we went to do the search warrant—So, [from] the time … we get the download to the time we do the warrant, between that timeframe, the sooner we do it, the more likelihood we're going to find that file, but if we're doing search warrants 30 days, 60 days, 90 days down the road and they happen to delete that file or do something with that file, then it's more likely we're not going to find it.
>
> ….
>
> Every target we deal with is different. Some people will keep [a file containing child pornography] in a downloads folder. They'll download it, go back and view it later. After they view it, they will save it somewhere else. They'll delete it. Some people watch it right away and after watching, delete it. Sometimes they'll back it up on other devices to watch later. They'll categorize. Every person we deal with has a different way they categorize or do something with it after they download it.

¶41 Later in the hearing, the circuit court asked the agent about the averment in the affidavit regarding "individuals who have an interest in child pornography," leading to the following testimony by the agent:

> So we deal with two different types of offenders, or multiple different types, but the most common we deal with is we have collectors, and we have the people that are going to view right away and delete it. So we never know what kind of offender we're going to have at the time of the warrant.
>
> ….

> [W]e put the collector portion in [the affidavit] because when people do download files, people back up their stuff, whether they back it up on another hard drive or whatever they do with it, and people [who] are going to collect it[,] and don't want family members or people living with them to find it or whatever the circumstances [are,] will take that and move it to another location.… [N]ot every single target we deal with is a collector, but there's a high likelihood that they are.

¶42 On cross examination, the agent acknowledged that his viewing of the video recording that he downloaded from Beyer's shared folder on the peer-to-peer network did not indicate how the file got into that folder (*e.g.*, whether Beyer caused the video recording to be in the folder), nor did it indicate whether Beyer had viewed the file. In a related vein, the agent testified that he did not know at the time of the peer-to-peer investigation, based on the peer-to-peer evidence alone, whether Beyer was in fact a "collector" who was likely to retain the file.

¶43 The circuit court initially expressed skepticism over the reliability of the investigative software and the strength of the averments in the warrant affidavit tying Beyer individually to a likelihood of retaining child pornography. However, the court denied Beyer's motion and clarified with the ultimate conclusion that, in light of the testimony presented at the hearing, peer-to-peer evidence established "a reasonable likelihood" that the shared file would be found on Beyer's computer. The court noted that there were a lot "opportunit[ies]" and "possibilities" for the observed file to be disposed of in a way that would result in its no longer being found on Beyer's computer from the time of the execution of the warrant onward, but that it was nonetheless "a reasonable assumption to make that this video that was observed was still in the possession of the party" who shared it.

Franks/Mann

¶44 In ***Franks***, 438 U.S. at 155-56, the United States Supreme Court stated:

> [If] the defendant makes 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. In the event that at that hearing the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit's false material set to one side, the affidavit's remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.

¶45 Through ***Mann*** and its progeny, Wisconsin courts have extended this proposition to allow a defendant "to impeach a warrant affidavit if a material fact has been omitted from it and if the omission is the equivalent of a deliberate falsehood or reckless disregard for the truth." ***State v. Fischer***, 147 Wis. 2d 694, 701, 433 N.W.2d 647 (Ct. App. 1988) (citing ***State v. Mann***, 123 Wis. 2d 375, 388, 367 N.W.2d 209 (1985)). "[T]o prove reckless disregard for the truth, the defendant must prove that the affiant in fact entertained serious doubts as to the truth of the allegations or had obvious reasons to doubt the veracity of the allegations." ***State v. Anderson***, 138 Wis. 2d 451, 463, 406 N.W.2d 398 (1987).

¶46 Our supreme court has noted that, to make the substantial preliminary showing described in the passage from ***Franks*** just quoted, defendants must provide "'allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to

be false; and they should be accompanied by a statement of supporting reasons.'" ***Anderson***, 138 Wis. 2d at 462 (quoting ***Franks***, 438 U.S. at 171). Whether a circuit court has correctly determined that a defendant has met the defendant's burden to make the substantial preliminary showing is reviewed de novo. *See* ***Manuel***, 213 Wis. 2d at 315 (Circuit court's "denial of a defendant's motion for a ***Franks*** hearing is subject to de novo review.").

¶47 Here, in filing his motion to suppress, Beyer took the general position that the warrant was not based on sufficient probable cause (an issue that we address separately below), and made one argument relying on ***Franks*** and identified specific averments in the warrant affidavit that he contended were problematic. As reflected in the additional background above, Beyer's counsel and the circuit court both questioned the agent regarding the nature and accuracy of specific averments in the affidavit, which occurred without an objection by the prosecution that Beyer had not made a preliminary showing needed to adduce evidence on the topic.

¶48 In a brief, puzzling footnote, the State now asserts that the evidentiary hearing on Beyer's motion to suppress was not a hearing on his ***Franks***/***Mann*** argument. From this the State may mean to suggest that he failed to make the required showing for a hearing. However, the State's argument on this point is undeveloped for at least the reason that it fails to address the content of Beyer's motion. Beyer's briefing on appeal does not address the topic at all. In the absence of developed arguments on this topic, we assume without deciding in Beyer's favor that he made the "preliminary showing" needed for a hearing on his ***Franks*** claim.

¶49 Turning to the substance of the ***Franks*/*Mann*** issues here, because it involves the application of constitutional principles to a particular case, we address it as "a question of constitutional fact." *See* ***State v. Dearborn***, 2010 WI 84, ¶13, 327 Wis. 2d 252, 786 N.W.2d 97. Under this approach, "[w]e accept the circuit court's findings of fact unless they are clearly erroneous" and apply "constitutional principles to those facts" de novo. ***Id.***

¶50 We conclude that Beyer's argument fails because it is premised on alleged conflicts between the detective's affidavit and the agent's suppression hearing testimony and Beyer fails to show a conflict.[15] Having failed to identify a conflict between the affidavit (or any other evidence) and the agent's testimony, Beyer does not show by a preponderance of the evidence that the agent (and presumably by extension, the affiant-detective) had "serious doubts as to the truth of the allegations or had obvious reasons to doubt the veracity of the allegations." *See* ***Anderson***, 138 Wis. 2d at 463.

¶51 Beyer characterizes the agent as having testified at the suppression hearing that "a significant percentage" of persons who possess child pornography are "actually not collectors" and that this contradicts averments in the warrant affidavit. We do not think that this is an accurate characterization of the agent's testimony when it is considered as whole. When all of the testimony is taken into account, not just isolated references, we fail to see any contradiction between the

[15] Beyer's ***Franks*** argument is at times difficult to track. He does not directly analyze the text of the averments at issue but instead offers unexplained characterizations of the affidavit. Similarly, Beyer makes sweeping characterizations about the investigative agent's testimony and what it reveals regarding the warrant affidavit, but he fails to support these characterizations by providing detailed comparisons between the averments and the testimony. As a result, his repeated assertions that there are inaccuracies, omissions, or misrepresentations in the affidavit go unsupported. Nonetheless, we address Beyer's argument as best we understand it.

warrant affidavit and the testimony, or even any tension. As summarized above, the agent testified that child pornography possessors do different things with contraband files, including different things involving retention, transfer, or deletion. As the agent eventually explained his views, "not every single target we deal with is a collector [of child pornography], but there's a high likelihood that they are." Consistent with this, the pertinent averment in the warrant affidavit states "individuals who have an interest in child pornography or child sexual exploitation *tend to* retain any images or videos they obtain that depict such activity." (Emphasis added.)

¶52 It is true, as Beyer emphasizes, that one of the possibilities raised in the agent's testimony—that a possessor of child pornography could download but then (irrecoverably) delete a contraband file—is not explicitly noted in the affidavit. The degree to which the possible recoverability of deleted data, *see* note 8, *supra,* might reasonably be considered to be a matter of common knowledge among the computer-using judiciary is unclear to us. But regardless of what would be reasonable for a warrant-issuing judge to infer, we disagree with Beyer that the averments in the affidavit are rendered sufficiently misleading under ***Franks*** and ***Mann*** by the failure to more explicitly account for the (non-recoverable) deletion of contraband. Again, the challenged feature of the affidavit speaks only in terms of tendencies, including a specific averment about what "can reasonably be expected." Beyer essentially argues that it is "the equivalent of a deliberate falsehood or reckless disregard for truth" when an affiant does not flesh out any and all alternative reasonable inferences that evidence of a crime might not be found in the place identified in the affidavit—even when those alternative inferences are implied by the affidavit's use of terms indicating less-than-certain probabilities and tendencies that the evidence is there. This would create a new

legal standard. *See* ***Fischer***, 147 Wis. 2d at 701; ***Gralinski***, 306 Wis. 2d 101, ¶25 (warrant-issuing judge may draw reasonable inferences; the test is "'whether the inference drawn is *a* reasonable one'" and "'not whether the inference drawn is the *only* reasonable inference'" (quoting ***State v. Ward***, 2000 WI 3, ¶30, 231 Wis. 2d 723, 604 N.W.2d 517) (emphasis added in ***Gralinski***)).

¶53 In a variation on this argument, Beyer asserts that the investigative agent testified that there was "no reason to believe" that Beyer was a "collector" of child pornography based on the peer-to-peer evidence. Beyer contends that this contradicts the "reckless[] impli[cation]" of the warrant affidavit that he (or whoever allegedly accessed the file) is a "collector." Again here, Beyer fails to identify an inaccuracy or omission of pertinent information in the affidavit, in part by ignoring the common sense implications of an apparently demonstrated interest by a computer user in the possession of child pornography. The affidavit makes the general averment that individuals with an interest in child pornography tend to retain in some form the contraband that they obtain (or, as Beyer largely ignores, perhaps obtain *new* items of contraband consistent with their demonstrated interest). But the affidavit does not stop there. It further avers the individualized facts, based on the peer-to-peer investigation, that give rise to the reasonable inference that someone, through Beyer's IP address, obtained and shared child pornography. Combining these averments, it was not a reckless implication to infer that Beyer, or someone using a device in, or associated with, his residence on the peer-to-peer network, was a person interested in child pornography, even if the agent could not know this with certainty. Beyer's attacks on these points are all based on his undeveloped characterizations of the agent's testimony and speculation regarding the investigative software through arguments that we have already rejected.

¶54 Beyer emphasizes that the circuit court at various points during the suppression hearing expressed reservations regarding averments in the warrant affidavit and the agent's testimony. It is true that the court, in the course of a dialog with the prosecutor, expressed the view that some of the agent's testimony at the hearing regarding the potential for a suspect to *not* retain child pornography "would have been helpful" to the warrant-issuing judge. And, at another point the court expressed doubt that the sharing of a single file through a peer-to-peer network could be enough to support the inference that Beyer was a person who "has an interest in child pornography." But the court did not make any factual finding that would undermine the court's ultimate conclusion that the warrant affidavit supported a reasonable inference that evidence of possession of child pornography would be found through a search of devices located in Beyer's residence. We agree with that conclusion.

Probable Cause

¶55 We have explained the following regarding our review of whether probable cause exists to support the issuance of a search warrant:

> A search warrant "may issue only upon a finding of probable cause by a neutral and detached magistrate." [***Ward***, 231 Wis. 2d 723, ¶21] (citation omitted). The probable cause test is one of common sense. ***Id.***, ¶23. The task of the court is to decide "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." ***Id.*** (citation omitted). In reviewing that determination, we accord the warrant-issuing court great deference. ***Id.***, ¶22. Our duty is to ensure that the court had a substantial basis for concluding that probable cause existed. *See* ***State v. DeSmidt***, 155 Wis. 2d 119, 133, 454 N.W.2d 780 (1990).

State v. Kilgore, 2016 WI App 47, ¶39, 370 Wis. 2d 198, 882 N.W.2d 493. As part of this review, "the warrant judge may draw reasonable inferences from the evidence presented in the affidavit." ***State v. Multaler***, 2002 WI 35, ¶8, 252 Wis. 2d 54, 643 N.W.2d 437; ***Gralinski***, 306 Wis. 2d 101, ¶25.

¶56 To clarify, the case law just quoted refers to "contraband *or* evidence of a crime," but these two categories are of course not mutually exclusive. Many items could constitute both contraband (in this case, an image constituting child pornography) and also evidence of a crime (crimes involving the intentional creation, transfer, or possession of child pornography).

¶57 Beyer contends that the averments of the warrant affidavit were insufficient to establish probable cause that evidence would be found on one or more devices in his residence that could support a finding that he knowingly accessed or possessed child pornography. *See* WIS. STAT. § 948.12(1m) (requiring that possession or access be knowing); ***State v. Mercer***, 2010 WI App 47, ¶16, 324 Wis. 2d 506, 782 N.W.2d 125 (noting that possession in this context is defined as "exercis[ing] control"). Specifically, Beyer contends that averments that someone merely shared a single file of child pornography from his IP address does not establish probable cause that he knowingly obtained or shared the file, or more generally that he was someone "likely to retain [child] pornography." We conclude that the averments were sufficient to support a reasonable inference that Beyer or someone else using his device was a person interested in child pornography such that it was further reasonable to infer that the observed

contraband or other evidence relevant to a child pornography-related crime could be found on a device in Beyer's residence.[16]

¶58 Moreover, Beyer's argument is premised on the inaccurate notion that probable cause in this context must necessarily include proof that Beyer (or any other individual) had engaged in conduct that satisfied each element that the State would need to prove at trial to obtain a conviction. That is not the standard in general, and here there was evidence of child pornography which is contraband. Therefore, the issue is whether the affidavit provided a sufficient basis to conclude that evidence of a child-pornography-related offense would be found in the residence, regardless whether the conduct or knowledge of Beyer or anyone else might meet all of the elements of the offense of the possession of child pornography. *See* ***Kilgore***, 370 Wis. 2d 198, ¶39 ("The task of the court is to decide 'whether … there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" (quoted source omitted)); ***State v. Hughes***, 2000 WI 24, ¶20, 233 Wis. 2d 280, 607 N.W.2d 621 (distinguishing probable cause to search for evidence of a crime in a particular place from probable cause to arrest an individual, which naturally requires proof "that a particular suspect has committed a crime"). Here, investigators sought a warrant allowing them to search Beyer's residence for child pornography, based on the averred existence of a device that was used by someone to share child pornography, and based on evidence that the device was associated with Beyer's

[16] The affidavit avers the following based on the agent's training and experience regarding the peer-to-peer network at issue in this case: "Typically, once the … network peer has downloaded part of a file or files, that file is saved into the peer[']s … 'shared' file folder (based on the typical default settings of the [peer-to-peer network] client software programs) so that [the file] is immediately available for [sharing] with other users on the network."

residence. Under the circumstances, it was reasonable to infer that child pornography, or other evidence related to child pornography, would still be present on a device located in the residence.

¶59 On a similar point to one we have addressed above, Beyer repeatedly asserts that "nothing" in the warrant affidavit links him to the tendency of those interested in child pornography to retain child pornography. As part of this argument he cites to federal case law as persuasive authority for the proposition that the inference that someone has likely retained child pornography, or is likely obtaining new child pornography, "depends on the preliminary finding that the suspect is a person 'interested in' images of child pornography." *See* ***United States v. Raymonda***, 780 F.3d 105, 114 (2d Cir. 2015) ("The 'alleged "proclivities" of collectors of child pornography' … 'are only relevant if there is probable cause to believe that [a given defendant] *is* such a collector.'" (quoted source omitted; emphasis added in ***Raymonda***). This persuasive authority cautions against making this inference based on "a single incident of possession or receipt" without proof of additional "circumstances suggesting that [the individual] had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection." *See* ***id.*** at 115. Thus, for example, the federal court stated that there was probable cause that a defendant was interested in child pornography based on a single instance of downloading a file that the defendant then distributed to others. *See* ***id.*** (citing ***United States v. Seiver***, 692 F.3d 774, 775-77 (7th Cir. 2012)). But, in contrast, there was not probable cause when a defendant "opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files." ***Id.*** at 117.

¶60 Beyer's argument and related reliance on federal precedent essentially ignore the results of the peer-to-peer investigation here. To repeat, the evidence showed that a device registered to Beyer's IP address and associated with his residential address was observed sharing a video recording containing child pornography on the network from a file located on the device. This ties Beyer's residence in a direct manner to the averment regarding those interested in child pornography. *See* ***Gralinski***, 306 Wis. 2d 101, ¶30 & n.5 (submission of defendant's credit card information with other detailed information to website that contained child pornography sufficient to support inference that defendant was interested in child pornography). It is true that there are alternative inferences that could explain this evidence. For example, the peer-to-peer evidence is also consistent with the following: someone used Beyer's device to download the observed file, believing it to be something other than child pornography, resulting in its automatic but brief placement in the shared folder, before this person deleted the file and overwrote its data, thus cutting off its availability as soon as the downloader realized what the file was.[17] But the warrant-issuing judge was not required to draw these inferences. The evidence was also consistent with someone downloading the file in order to view it and then failing to delete the file from the computer after it was evident that the file contained child pornography.

¶61 Beyer argues that it would produce an absurd result to weigh the averment in the affidavit regarding the tendency of child pornography possessors to retain contraband in favor of probable cause under the circumstances here.

[17] Consistent with this potential theory, while the warrant affidavit avers that the name given to the file containing child pornography might be reasonably inferred to refer to a sexual act, the file name did not self-evidently distinguish between an unlawful portrayal of sex involving a child and a sex act portrayed in lawful adult pornography.

Specifically, he contends that "[i]f the detection of a single file" shared on a peer-to-peer network can render an individual, in the words of the warrant, "a person interested in child pornography" and thus someone likely to retain child pornography, then it would be "an absolute certainty" that probable cause is established in all such cases, regardless of other relevant facts. Beyer does not make clear what other relevant facts he is referring to that could render such an affidavit insufficient. In any case, however, Beyer fails to persuade us that recognizing the reasonable inferences available to the warrant-issuing judge here based on the warrant affidavit foreshadows unreasonable results in future cases.

¶62 In a similar vein, Beyer notes other kinds of evidence that the affidavit could have averred that would have created a *stronger* case for probable cause. For example, he notes that the download of the peer-to-peer evidence by the State investigative computer consisted of a connection lasting only two to three minutes, and also contends that follow-up monitoring of activity by his device on the peer-to-peer network by authorities might have provided necessary additional information. It is possible that in another case, given all of the allegations presented, a reviewing judge might consider the absence of follow-up of some kind to be a factor weighing against probable cause. But these arguments, in conjunction with other arguments that we reject, do not show that the specific affidavit here did not provide the circuit court with a "substantial basis" to conclude that there was probable cause. *See* ***Kilgore***, 370 Wis. 2d 198, ¶39.

III. Sufficiency of the evidence

¶63 To convict Beyer of possession of child pornography, the State needed to prove the following beyond a reasonable doubt: Beyer knew that he either possessed a recording or "accessed a recording in any way with intent to

view it"; the recording depicted a child engaged in sexually explicit conduct; Beyer knew or reasonably should have known that the recording contained depictions of a person engaged in actual or simulated sexually explicit conduct; and Beyer knew or should have known that the person depicted in the recording engaged in sexually explicit conduct was under the age of 18 years. *See* WIS JI—CRIMINAL 2146A (July 2020); WIS. STAT. § 948.12.

¶64 There was no dispute at trial that the specific image that the prosecution relied on as the basis for the single charge ("Image One") depicted a child who had been subjected to posing in a sexually explicit manner qualifying as "engag[ing] in sexually explicit conduct" for purposes of WIS. STAT. § 948.12. *See* WIS. STAT. § 948.01(7) (defining "sexually explicit conduct" to include "[l]ewd exhibition of intimate parts"). Moreover, at least as argued on appeal, there is no dispute that the evidence is sufficient to show that Beyer possessed Image One—its file was downloaded to the hard drive of his computer approximately two months before the execution of the search warrant, where it remained saved without being deleted. *See* ***Mercer***, 324 Wis. 2d 506, ¶¶15-16 (possession for purposes of § 948.12 can be established when a person "'knowingly had actual physical control'" of contraband or it is "'in an area over which the person has control and the person intends to exercise control over'" it (quoting WIS JI—CRIMINAL 2146A (May 2007))).

¶65 Instead, Beyer's argument at trial, which he essentially renews on appeal, is that the evidence failed to show beyond a reasonable doubt that Beyer's possession of Image One was knowing in the ways required by WIS. STAT. § 948.12. That is, Beyer contends that the evidence was insufficient to prove that his possession of Image One was the knowing possession of child pornography.

We now provide pertinent background and explain why we conclude that sufficient evidence was presented to sustain Beyer's conviction.

¶66 "This court independently reviews whether the evidence was sufficient to sustain the jury verdict, 'but in so doing, we view the evidence most favorably to sustaining the conviction.'" ***State v. Hibbard***, 2022 WI App 53, ¶9, 404 Wis. 2d 668, 982 N.W.2d 105 (quoting ***State v. Hanson***, 2012 WI 4, ¶15, 338 Wis. 2d 243, 808 N.W.2d 390), *review denied*, 2023 WI 29, ¶9; *see also* ***Gauthier v. State***, 28 Wis. 2d 412, 416, 137 N.W.2d 101 (1965) ("As the burden of proof is the same whether the trial is to the court or to a jury, the test to be applied to determine the sufficiency of the evidence is the same."). "Evidence is insufficient to support a conviction only if, viewed most favorably to the State, it 'is so insufficient in probative value and force that it can be said as a matter of law that no trier of fact, acting reasonably, could have found guilt beyond a reasonable doubt.'" ***Hibbard***, 404 Wis. 2d 668, ¶9 (quoting ***State v. Poellinger***, 153 Wis. 2d 493, 501, 451 N.W.2d 752 (1990)).

Additional Background

¶67 A State-employed forensic computer analyst testified in pertinent part as follows. She examined a hard drive that was removed from a computer seized from Beyer's apartment and determined that it contained child pornography. The detective who led the execution of the warrant reviewed some of these images and selected ten that the prosecution agreed to use as the basis for charges. Image One was one of the ten images. Image One had a "file created" date of September 9, 2017, signifying that this was when the file was first created on Beyer's computer. Data on the file also included fields for "last accessed" and "entry modified," which exactly matched the time of the "file created" field. The

analyst "interpret[ed]" these matching times to mean that the file "was on the computer, opened, but not necessarily modified or … saved additionally." Based on the timing of the download of Image One by the user of Beyer's computer, it appeared to have been downloaded in conjunction with five other images from the same file shared on the peer-to-peer network—all six images were downloaded within approximately 26 seconds. However, unlike Image One, the other five images in the set had "last accessed" times that varied from the images' "file created" times.[18]

¶68 The circuit court found that the five other downloaded images each contained child pornography of the same kind as Image One—one or two children subjected to posing in a sexually explicit manner.

¶69 On cross examination, the analyst testified that she could not determine from the file data alone whether Beyer was aware that Image One was downloaded to his hard drive.

¶70 Turning to the testimony of the detective who led the execution of the warrant, this included the following. Beyer was at the apartment when police executed the warrant and he was detained while a search of the apartment for electronic devices was conducted. The detective recorded an interview of Beyer while he was detained. A portion of the interview was played at trial.

[18] The analyst was explicitly examined at trial about only one of the images besides Image One, but the analyst relied on a police report that was prepared based on her on-site analysis of the ten images that formed the basis for the original charges. The defense later relied on each of the other images besides Image One, specifically to note that they had "file created" data that varied from their "last accessed" and "last modified" entries. This report further indicated that four of five images downloaded with Image One showed the same child as shown in Image One, and each of the images appeared to show one or both of the same two children.

¶71 During the interview, Beyer said all of the following. Beyer lived alone at the residence that was associated with the IP address provided in the peer-to-peer investigation. For "[a] few years" he had been using a peer-to-peer network to download child pornography onto his computer. More specifically, he had been "working through" a "list" of peer-to-peer files on a particular website as a means of finding child pornography on the peer-to-peer network without making use of search terms. It was a "good estimate" that he viewed child pornography weekly. Although Beyer was primarily interested in obtaining and viewing "[o]lder teenagers," he would receive images that included younger children—files depicting children in "the toddler age range" were "quite common" for him to see. The first time he ever downloaded child pornography, which occurred years before the interview, he downloaded a file from the peer-to-peer network that had content that he "wasn't expecting," in that it depicted "[i]ndividuals that clearly looked younger" than he expected to see.

¶72 At trial, the defense did not present evidence and Beyer did not testify.

¶73 In making its findings, the circuit court noted that Image One was found on a hard drive retrieved from Beyer's computer, which was located in an apartment occupied solely by Beyer. The court further found that, although there was some testimony that the image was "maybe … downloaded automatically or inadvertently," there was "no evidence that [Image One] was placed there by someone" other than Beyer. The court appeared to further credit testimony that Image One was downloaded as part of a set including other images, all to the same folder on Beyer's hard drive, with some depicting the same child as in Image One. The court further found that images accompanying Image One "certainly … were viewed," and themselves contained child pornography. The court reasoned that

this supported the finding, beyond a reasonable doubt, that Beyer also viewed Image One, or alternatively, "accessed" the image.

Analysis

¶74 To repeat, Beyer argues that there is insufficient evidence to show that he knew during any relevant time period what was depicted in Image One. Beyer bases this in large part on the fact that Image One's "last accessed" and "last modified" data exactly matched the time at which Image One was first saved to Beyer's hard drive, which he apparently contends supports a finding that he did not open Image One. Beyer couples this proposition with what he asserts is evidence supporting the inference that he unexpectedly downloaded child pornography at a pertinent time period. The resulting argument is that he could not have been certain what was contained in Image One without first opening it, and the evidence does not support a reasonable inference that he did open it. However, as we now explain, Beyer's argument fails to account for other evidence on which the circuit court as factfinder could reasonably rely to conclude one of the following two alternative possibilities: that Beyer knew by viewing Image One that it depicted child pornography after it was downloaded to his computer and retained by him; or, that Beyer knew or should have known that Image One was child pornography based on his background knowledge in obtaining child pornography and having viewed the images downloaded along with Image One before retaining it.[19]

[19] Because we conclude that there was sufficient evidence to establish Beyer had the requisite knowledge for a conviction based on the reasons explained in the text, we do not address the State's alternative argument that there was sufficient evidence to convict him based on his "access[ing]" Image One "in any way" that demonstrated "the intent to view" it.

¶75 The testimony of the analyst who interpreted pertinent dates and times is significant. She testified that the matching "file created," "last accessed," and "last modified" dates and times meant that the file "was on the computer, *opened*, but not necessarily modified or … saved additionally." (Emphasis added.) This amply supports the circuit court's finding that Beyer viewed Image One and therefore knew what it depicted and retained it thereafter. Beyer heavily relies on what amounts to contrary inferences regarding how the Image One data could be interpreted, but he fails to develop a supported argument that the court as factfinder could not credit the analyst's testimony that the file was "opened."

¶76 Further, even beyond the analyst's testimony, there was evidence to support the inference that Beyer either viewed or in any case should have known what was contained in Image One, which he retained after he or someone else downloaded it. As noted above, Image One was downloaded as part of a set of images, each of which depicted one or two children who had been subjected to posing in a sexually explicit manner. And, each of the images accompanying Image One had "last accessed" times that support the inference that they were viewed by a user of the computer after they were downloaded.[20] Then there were Beyer's admissions to police, which could be reasonably interpreted to establish that his exclusive means of obtaining child pornography at the time was from a website familiar to him. This provided relevant context reinforcing the inference that, if Beyer knew one image in the set was child pornography, then all of the images were. Beyer's admission regarding the use of this site also undermines his

[20] The analyst testified that sometimes a computer's own processes, independent of a user's input, will cause "last accessed" data to change, which could support the inference that it was not Beyer opening any of the files that caused their "last accessed" data to change. But the circuit court as factfinder was not required to draw the inference that this in fact occurred.

emphasis on appeal regarding the lack of evidence that he used search terms demonstrating that he specifically obtained Image One as part of a deliberate search for child pornography. Moreover, as noted by the circuit court, there was no evidence to corroborate mere possibilities that someone could have remotely accessed Beyer's computer to in some manner plant this set of images on Beyer's hard drive, nor evidence that someone planted images by going directly onto his computer, which was located in an apartment that he said had been solely occupied by him.

¶77 Although unclear, Beyer's briefing suggests that he takes the position that the only reasonable view of the evidence was that he could not have known the content of Image One without opening it. This appears to be based on his statements to police that he sometimes viewed pornography depicting adults, as opposed to child pornography, and that he sometimes did not expect to see what he encountered in a particular downloaded file. However, viewing the evidence through the light most favorable to the verdict, there are other reasonable interpretations of Beyer's statements to police. *See* ***Hibbard***, 404 Wis. 2d 668, ¶9. As to the adult sexual images versus child pornography topic, the factfinder was free to interpret Beyer's detailed explanation regarding how he obtained child pornography as his exclusive means of getting such materials, which occurred entirely separately from however he obtained adult pornography. As to the "not expecting" topics, Beyer's reference may be reasonably interpreted to mean that this occurred when he *first began* looking at child pornography, and not that it occurred during what he described as his more recent, deliberate obtaining of child pornography from a list of peer-to-peer files on a specific website.

¶78 In his reply brief on appeal, Beyer makes an argument that is difficult to follow. He asserts that the circuit court deemed as other acts evidence

Beyer's admissions to downloading and viewing child pornography that did not specifically include reference to Image One. He further asserts that the court could have relied on these admissions regarding other images only for an improper propensity purpose, namely, to conclude that Beyer viewed Image One in conformity with the character trait of desiring to view child pornography. If one ignores the propensity-based value of this purported other-acts evidence, Beyer's argument apparently continues, there was insufficient evidence that Beyer viewed Image One. This argument is undeveloped on several levels, but it is sufficient to make the following point. Beyer does not provide a reason to think that the court considered any aspect of his admissions for an improper propensity purpose, as opposed to considering the admissions for proper purposes, including those allowed under WIS. STAT. § 904.04(2)(a).

CONCLUSION

¶79 For all of these reasons, we affirm the judgment of conviction.

By the Court.—Judgment affirmed.

Not recommended for publication in the official reports.