Illinois Official Reports

Appellate Court

People v. Daigle, 2024 IL App (4th) 230015

Appellate Court Caption	THE PEOPLE OF THE STATE OF ILLINOIS, Plaintiff-Appellee, v. PATRICK DAIGLE, Defendant-Appellant.
District & No.	Fourth District No. 4-23-0015
Filed	May 21, 2024
Decision Under Review	Appeal from the Circuit Court of Winnebago County, No. 16-CF-796; the Hon. Brendan A. Maher, Judge, presiding.
Judgment	Affirmed.
Counsel on Appeal	Bradley C. Giglio, of Mevorah & Giglio Law Offices, of Bloomingdale, for appellant. J. Hanley, State's Attorney, of Rockford (Patrick Delfino, David J. Robinson, and Allison Paige Brooks, of State's Attorneys Appellate Prosecutor's Office, of counsel), for the People.
Panel	JUSTICE ZENOFF delivered the judgment of the court, with opinion. Justices Harris and Knecht concurred in the judgment and opinion.

OPINION

¶ 1 Following a bench trial, the trial court found defendant, Patrick Daigle, guilty of three counts of disseminating child pornography (720 ILCS 5/11-20.1(a)(2) (West 2014)). The court sentenced defendant to consecutive six-year prison terms on each of the three counts. On appeal, defendant argues (1) he should have been convicted of and sentenced on one count only, (2) the court erred in finding he knowingly disseminated child pornography, and (3) the court erred in admitting into evidence an exhibit containing three videos depicting child pornography. We affirm.

¶ 2 I. BACKGROUND

¶ 3 The bill of indictment charged defendant with three counts of disseminating child pornography involving individuals under the age of 13 on or about November 2, 2015. The indictment indicated the offenses required mandatory consecutive prison sentences.

¶ 4 A. The Trial Evidence

¶ 5 The matter proceeded to a bench trial in December 2021.

¶ 6 1. *Michael Bruns*

¶ 7 Michael Bruns, the State's first witness, testified as follows. In 2016, he worked for the Illinois Attorney General as part of the Internet Crimes Against Children Task Force System. Part of his training involved using technology to investigate peer-to-peer file-sharing websites, one of which was Gnutella. Bruns's software, which was used by investigators across the country, would search Gnutella to see which Internet Protocol (IP) addresses traded material known to be child pornography. When Bruns's software identified an IP address as potentially making child pornography available for download, his software would download the file. The software would identify and record the IP address, along with the date and time each file was downloaded.

¶ 8 According to Bruns, on November 2, 2015, his software downloaded three videos via Gnutella from a computer or device using the IP address 50.179.154.255. One video was a file ending in "7bze" that was titled "Pthc PedolandFrifam Black Mask 03.avi." In the course of his career, Bruns became familiar with the term "pthc," which stands for "[p]reteen hardcore." The second video was a file ending in "rxgf" that was titled "(Pthc)!!!NEW!!!MOV08828.avi." The third video was a file ending in "5fkn" that was titled "2012 private 7yr my sweet little bitch.mpg." Bruns viewed all three videos his software downloaded.

¶ 9 Bruns identified People's exhibit No. 3 as a disk containing the three videos his software downloaded. He testified this exhibit was a fair and accurate copy of those video files. When the prosecutor moved to admit People's exhibit No. 3 into evidence, defense counsel objected on the basis of lack of foundation. Before ruling on the objection, the trial court allowed defense counsel to question Bruns regarding the foundation for this exhibit.

¶ 10 Upon questioning by defense counsel, Bruns testified that the computer downloading these files was located in a "secure space in our office," which he believed at the time was located at 69 West Washington Street in Chicago. Although Bruns was not present when the files were downloaded, his software ran 24 hours a day, 7 days per week. Asked whether he brought "any

technological evidence to show that the image was downloaded on that particular day," Bruns responded he did not know and would have to "look through the information." Bruns added that every time the software downloaded a file, the software would record "all the information." Although the software downloaded the subject files on November 2, 2015, Bruns did not recall when he first took "possession" of the images; it could have been the same day, or it could have been a month later.

¶ 11 The prosecutor then asked Bruns additional questions relating to the foundation for People's exhibit No. 3. Bruns testified he received training on this software and had previously used it for hundreds of investigations. If the software and the computer attached to it were on and working correctly, it downloaded videos. According to Bruns, on November 2, 2015, his computer was functioning properly "when these images were downloaded."

¶ 12 Defense counsel then asked Bruns whether his computer was tested before November 2, 2015, to confirm it was in proper working order. Bruns responded that although the computer itself was not tested, if the computer operated, it would run the software just like any other software. Bruns was not aware of any date after November 2, 2015, when the computer was tested to determine whether it was working properly.

¶ 13 The parties and the trial court then engaged in a lengthy discussion as to whether the State laid a foundation to admit People's exhibit No. 3 into evidence. The court ultimately admitted the exhibit, and the State continued its direct examination of Bruns.

¶ 14 Bruns testified that, in response to a subpoena, Comcast linked the IP address from which his software downloaded the three videos to a residence in Winnebago, Illinois. On March 24, 2016, police officers executed a search warrant at that residence, and defendant was inside. Bruns did not personally collect or examine any evidence at this residence. However, that same day, Bruns interviewed defendant. During the interview, Bruns showed defendant the three videos contained in People's exhibit No. 3, along with a printed still image taken from one video.

¶ 15 Without objection from the defense, the State introduced into evidence a typed statement defendant signed on March 24, 2016. Defendant made the following admissions. He currently lived at the residence police officers had searched. About a year ago, he started downloading child pornography. He downloaded "Frostwire" and started searching for child pornography. However, he did not initially get results, as he did not know proper search terms. After observing "what other people search for," he copied and pasted such search terms and started getting results. He would download about 20 to 60 videos at once, which would take a long time to download. He would then watch the videos "within the program." After "a day or a few days," he would reset his computer to the manufacturer's settings to "wipe all the videos." He had been doing this about once a month for the past year, and he would repeatedly "re-install Frostwire and do the same thing." The last time he did so was about two weeks prior to March 24, 2016. Defendant indicated he would only use the computer in the master bedroom, which was plugged into a television. He preferred videos of girls between the ages of 8 and 12 years old. He had "downloaded some of younger children but they really did not do much" for him. Defendant indicated he knew "Frostwire at install sets up a folder where it would download the videos too [*sic*]." However, defendant "really never opened the videos from the folder," but rather "would just view them with in [*sic*] the program." Defendant knew "that the program is a sharing program and you have to agree to share videos with other people." With respect to the three videos Bruns showed him during his questioning, defendant could not

remember having watched the first video. He said he downloaded a lot of videos, some of which he deleted without watching. The second video Bruns showed him looked "very familiar," but he "could not say for sure." Defendant remembered downloading and watching the third video Bruns showed him. Defendant acknowledged signing a screen shot taken from this video during the police interview. Defendant's written statement concluded by asserting he downloaded many of the videos he liked several times in between resetting his computer to the manufacturer's settings.

¶ 16 Without objection from the defense, the trial court admitted into evidence the still image defendant signed during his interview. The State concluded its direct examination of Bruns by playing in open court portions of the three videos contained in People's exhibit No. 3, which depicted child pornography.

¶ 17 On cross-examination, Bruns testified to the following most salient points. When his software downloaded the subject videos via Gnutella, the images stayed on his hard drive in a secure room. At some point, Bruns made a copy of these videos using a program he did not recall, and he gave that copy to the state's attorney's office. Bruns did not remember the specific format of the copy he provided to the state's attorney's office, but it probably would have been a compact disc. Bruns did not make a "log" documenting when he created this copy of the videos. He also did not know exactly how much time elapsed between when he made the copy and when he gave it to the state's attorney's office. Bruns believed, but was not sure, that the copy was kept in a secure office space until he gave it to the state's attorney's office. Bruns further testified that as part of his investigation, he did surveillance on defendant's residence and checked his background. Bruns never learned that anybody else lived at defendant's residence.

¶ 18 2. *Zeus Flores*

¶ 19 Zeus Flores was the State's second witness. He worked for the Illinois Attorney General as a computer evidence recovery technician supervisor. Without objection from the defense, the trial court recognized Flores as an expert in the field of digital forensics.

¶ 20 Flores testified that on March 24, 2016, he assisted in executing a search warrant at a residence in Winnebago. He provided "on scene triage assistance and examination assistance" regarding the devices found at the residence. One such device was an "eMachine desktop computer tower" connected to a television in the master bedroom. Flores removed the hard drive from that computer and did a "preview examination," which entailed connecting the hard drive to a write blocker that then connected to Flores's forensic workstation. The purpose of the write blocker was to prevent altering data on the hard drive. In conducting this examination, Flores used programs called "EnCase" and "C4All," which Flores asserted were commonly accepted by experts in the field.

¶ 21 During the preliminary examination of the hard drive located in the master bedroom of defendant's residence, Flores found "several videos of apparent child pornography in the unallocated space of the hard drive." Flores explained that unallocated space was "commonly referred to as deleted space," as a deleted file remains in unallocated space on the computer until it is overwritten. The State introduced into evidence both the computer found in the master bedroom of defendant's residence and the hard drive from that computer.

¶ 22 Flores removed this hard drive from defendant's residence and stored it at the attorney general's office. On March 25, 2016, Flores created a "forensic image" of the hard drive, which

was a copy of the data on it. The purpose of doing this was so he could conduct his work using a copy of the hard drive's data rather than the original hard drive. Flores used "hashing" to confirm the data was intact. He explained a hash is an alphanumeric string identifying data like a fingerprint. If a copy's hash value matches the original's, "you know that you're dealing with the same data." Flores confirmed the hash value of the forensic image he created in this case was a "100 percent match." Flores did not do any additional work with respect to the investigation in this case.

¶ 23 On cross-examination, Flores testified there was no child pornography found on other devices recovered from defendant's residence. Flores never located e-mails or other correspondence from defendant transmitting child pornography to third parties. Flores testified he was aware of two copies that were made of the hard drive taken from the computer in defendant's master bedroom: (1) the copy Flores made on March 25, 2016, and (2) a copy that Flores's coworker, Steven Strahm, made for himself at some point. According to Flores, an encrypted version of the copy he made was ultimately given to defendant's expert, Warren Daniel. Defendant's hard drive stayed in the lab at all times until defendant's trial. However, Flores had no specific documentation regarding who accessed the hard drive within the lab.

¶ 24 Flores further testified on cross-examination that although the most common way a file could end up in a computer's unallocated space would be if it were deleted, a file could also end up there when an operating system is overwritten. Additionally, pictures contained on websites could also be in unallocated space. Absent other "artifacts" providing further context, there would be no way to determine whether a person specifically sought out a particular image found in a computer's unallocated space. If a file were deleted, that file would no longer be accessible to a peer-to-peer application.

¶ 25 The most relevant point elicited on redirect examination was that if someone were able to download a file through a peer-to-peer network, that means the file was *not* deleted on the originating computer. In other words, that file would be "present and allocated on the source" at the time of the download. Flores also testified that the attorney general's office's lab was located in a secure facility guarded with swipe cards. Only forensic examiners had access to the area where digital electronics were stored. According to Flores, if someone restored a computer to the manufacturer's settings, areas of the drive that were untouched could have remanent information located in unallocated space. It is "hit and miss" as to which portions of unallocated space get overwritten when new items are saved.

¶ 26 3. *Steven Strahm*

¶ 27 Strahm was the State's final witness. He worked as a senior digital forensic examiner with the attorney general's office. Defendant did not object to the trial court recognizing Strahm as an expert in digital forensics.

¶ 28 Strahm testified that, on July 19, 2017, he was assigned to conduct a forensic examination of the hard drive taken from the computer found in the master bedroom of defendant's residence. This hard drive had been stored in the attorney general's office's secure lab, which was accessible only to forensic examiners and the bureau chief. Using a program called "Encase 7," Strahm made a forensic image (copy) of the hard drive. He confirmed its hash value matched both the original hard drive and the copy previously made by Flores.

¶ 29 Strahm explained it is not always possible to recover deleted files, which may be partially or completely overwritten. If a file cannot be retrieved, there are programs that can allow him

to uncover some information about the file, such as its name or where it was originally stored on the computer. In this case, Strahm was able to locate items "of interest" in the unallocated space of the hard drive. For the majority of the videos he located, he was able to recover full video files, some of which were slightly corrupted but still viewable. (Those videos were not the basis for defendant's charges.)

¶ 30 Strahm also located on this hard drive "artifacts related to a program called FrostWire," which was a program allowing users to "upload or download files via a peer-to-peer network." Specifically, in FrostWire's property file, which was located in the hard drive's unallocated space, Strahm saw a file created on "Monday, November 2nd, 00:15:17 CST 2015." Strahm believed this information corresponded to when Bruns accessed files. Strahm also noticed the IP address FrostWire was using at the time was 50.179.154.255, matching the IP address from which the search warrant indicated Bruns downloaded files.

¶ 31 Strahm also recovered information from this hard drive's Internet Explorer main history relating to certain FrostWire files that "had previously existed" but "may have been deleted." Specifically, there was information relating to video files entitled (1) "(pthc)!!!NEW!!!MOV08828.avi," (2) "2012private7yrmysweetlittlebitch.mpg," and (3) "(pthc)pedolandfrifamblackmask03.avi." Although Strahm identified "file paths" for these videos, the actual videos were not still on the hard drive. Strahm determined these file paths had been stored in a saved folder associated with FrostWire. From this information, Strahm concluded that, at some point, files by these names were "accessed by Windows Explorer" on this hard drive.

¶ 32 Strahm also located "artifacts" in the hard drive's unallocated space, indicating FrostWire version 4.2.18 had been installed at some point. (In other portions of Strahm's testimony, this was referred to as version 4.21.8.) The "creation date" on the hard drive for this installation file was October 30, 2015, at 9:11 p.m. The reason this information was of interest to Strahm is that versions of FrostWire preceding version 5 had access to the Gnutella network, whereas later versions did not. Strahm found indications on the hard drive that someone searched for websites that could allow a person to download old versions of FrostWire. Strahm also found indications that either FrostWire or LimeWire had been used to conduct searches on this hard drive for items containing the acronym "pthc."

¶ 33 On cross-examination, Strahm testified that although he can say Windows Explorer accessed video files by certain names on this hard drive at some point, he did not know the content of those files or whether they were ever opened. He also did not know when such files were accessed or whether those files existed on the subject computer on November 2, 2015. Furthermore, Strahm's records indicated FrostWire was deleted from this hard drive by the time he analyzed it and files associated with FrostWire were last accessed prior to November 2, 2015. All versions of FrostWire had been deleted prior to November 2, 2015.

¶ 34 Strahm also testified on cross-examination that he checked and confirmed aspects of his own work in 2019, after receiving a report prepared by Daniel. Specifically, Daniel had indicated in his report he did not find FrostWire on the subject hard drive. In response to this report, Strahm confirmed FrostWire was indeed on the hard drive. According to Strahm, the hash value of the copy of the hard drive provided to Daniel matched the actual hard drive, which meant they were identical.

¶ 35 On cross-examination, Strahm further testified that the IP and "Mac" addresses identified in this case were linked to defendant's residence, not to any specific device. Although Strahm

could not say whether the "computer he retrieved" was the actual device from which defendant obtained "these images," as far as he was aware, the device he analyzed was the only one found to "have FrostWire on it with these file names."

¶ 36 On redirect examination, Strahm clarified that Windows 7 by default documents the time a file was created, rather than when it was last accessed. Thus, Strahm could tell the "three video files" found on defendant's hard drive (*i.e.*, the three file paths) were created on October 30, 2015, but he could not say when they were last accessed. Nor could Strahm say when those files were either deleted or moved into unallocated space on the device. Strahm explained the same was true with respect to the FrostWire files he found. Specifically, there was an installation file for FrostWire version 4.21.8 created on October 30, 2015, but Strahm could not tell when that file was run. Strahm did not believe that knowing the internal IP and Mac address for the specific device he was analyzing would have been relevant to his investigation.

¶ 37 4. *Warren Daniel*

¶ 38 After the trial court denied defendant's motion for a directed finding of not guilty, Daniel testified for the defense.

¶ 39 Daniel was the chief executive officer of a company called Commercial Level Simulations. He testified his company specialized in various types of digital products, including cybersecurity, forensics, and eDiscovery. He also had some experience advising law enforcement in connection with child pornography cases. After extensive testimony and argument regarding Daniel's qualifications, the trial court allowed him to testify as an expert without formally being recognized as one. The court indicated it would evaluate Daniel's "credibility on the specific issues in this case."

¶ 40 Daniel primarily testified in generalities about how important it was to maintain a proper chain of custody for digital evidence to ensure the authenticity of the data. Daniel also testified that, "[d]epending on the BitTorrent application" and the default setting of a program, it was possible to use peer-to-peer programs and not share files. More specific to the present case, according to Daniel, the Mac addresses of the hard drive and the computer tower he analyzed did not match the Mac address listed in Comcast's letter in response to a subpoena. If Daniel had personally conducted the law enforcement investigation in this case, he would have removed all digital devices from defendant's residence for examination to avoid the possibility of losing information about which devices were connected to the network.

¶ 41 At the conclusion of Daniel's direct examination, defendant personally confirmed on the record that he agreed with his counsel's strategy not to question Daniel further about the contents of his report specific to the facts of this case.

¶ 42 On cross-examination, Daniel testified defendant was identified as the subscriber for the Comcast account associated with the residence in Winnebago that the police searched. On redirect examination, Daniel said he could not "independently verify the connection between that IP address and that address."

¶ 43 After hearing closing arguments, the trial court took the matter under advisement.

¶ 44 B. The Trial Court's Findings

¶ 45 On January 20, 2022, the trial court issued a written "bench trial verdict," finding defendant guilty of all three charges. The ruling was comprehensive and lengthy, and we will highlight only a few salient points.

¶ 46 The trial court deemed Bruns, Flores, and Strahm credible, and their testimony was "not substantially impeached," "effectively challenged," or "rebutted" on cross-examination. The court found that Daniel testified primarily without reference to the specific facts of this case, so his opinions were "not particularly helpful." It was "not entirely clear" to the court how the testimony about Mac addresses was intended to contradict or impeach the State's witnesses. Daniel's testimony "did not undermine, impeach or otherwise call into serious question any aspect of the State's case in chief."

¶ 47 The trial court explained the State established a proper chain of custody with respect to both the original and copies of the hard drive that was removed from the master bedroom of defendant's residence. Among the points the court mentioned on this issue were (1) Flores and Strahm testified credibly that the computer and hard drive were stored in a secured location and (2) the risk of evidence tampering or accidental substitution was "highly improbable."

¶ 48 The trial court wrote that, after it took the case under advisement, it reviewed *in camera* the three video files admitted as People's exhibit No. 3. The court described the contents of those videos, the details of which are not relevant to this appeal other than to note they depicted child pornography.

¶ 49 The trial court explained defendant admitted he resided at the subject residence in Winnebago, and there was no evidence suggesting anyone else lived there. The court also found defendant admitted (1) knowing the nature and character of the videos he downloaded, (2) intending to download such videos, and (3) knowing FrostWire was a sharing program that required him, as part of the terms of service, to agree to share videos with other people.

¶ 50 C. Posttrial Motion, Sentencing, and Notice of Appeal

¶ 51 Defendant filed a motion for a new trial, arguing (1) the trial court erroneously admitted People's exhibit No. 3 into evidence and (2) the State failed to prove him guilty beyond a reasonable doubt. The court denied this motion.

¶ 52 The sentencing range for each of the three counts was 6 to 30 years' imprisonment, with mandatory consecutive sentencing. 720 ILCS 5/11-20.1(c-5) (West 2014); 730 ILCS 5/5-4.5-25(a), 5-8-4(d)(2.5) (West 2014). The State sought the minimum sentence of 18 years in prison. Raising an argument about the appropriate unit of prosecution, defense counsel asked the trial court to sentence defendant to the minimum prison term on only one of the three counts (six years in prison), as the evidence did not show whether the three videos were "separate downloads, separately acquired." The court rejected defense counsel's argument and sentenced defendant to 18 years in prison, which it determined was the minimum possible sentence.

¶ 53 Defendant filed a motion to reconsider his sentence, citing *People v. McSwain*, 2012 IL App (4th) 100619, in support of his argument that he should not be convicted of and sentenced for three separate offenses. The trial court denied this motion. In determining defendant committed three separate acts of disseminating child pornography, the court reasoned (1) the three videos involved different children; (2) unlike in *McSwain*, this case involved

dissemination of child pornography, not mere possession; and (3) defendant admitted he knew he was making child pornography available for download.

¶ 54 Defendant filed a timely notice of appeal.

¶ 55 II. ANALYSIS

¶ 56 On appeal, defendant challenges (1) whether the trial court erred in entering more than one conviction and sentencing him on multiple counts of disseminating child pornography, (2) whether the State proved beyond a reasonable doubt he knowingly disseminated child pornography, and (3) whether the court erred by admitting People's exhibit No. 3 into evidence. For the sake of the most logical analysis, we will address the sufficiency of the evidence, then defendant's evidentiary challenge, and then the sentencing issue.

¶ 57 A. Sufficiency of the Evidence

¶ 58 Defendant argues the State failed to prove he disseminated child pornography, as there was no proof he knew of the possibility that others could obtain such images from either him or his computer. Defendant also asserts the evidence did not show he "took any action to make the images available." According to defendant, he "is no more guilty of dissemination [than] if he had the images in the backseat of his car (knowingly or unknowingly) and someone broke into his car and took them from him."

¶ 59 "When a court reviews the sufficiency of the evidence, it must ask 'whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.' " (Emphasis in original.) *People v. Phillips*, 215 Ill. 2d 554, 569-70 (2005) (quoting *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). "We will reverse a criminal conviction only if the evidence was so unreasonable, improbable, or unsatisfactory as to create a reasonable doubt of the defendant's guilt." *People v. Gumila*, 2012 IL App (2d) 110761, ¶ 61.

¶ 60 Section 11-20.1(a)(2) of the Criminal Code of 2012 (Code) provides, in relevant portion, that a person commits child pornography who,

> "with the knowledge of the nature or content thereof, *** disseminates *** any film, videotape, photograph or other similar visual reproduction or depiction by computer of any child *** whom the person knows or reasonably should know to be under the age of 18 *** engaged in any activity described in subparagraphs (i) through (vii) of paragraph (1) of this subsection." 720 ILCS 5/11-20.1(a)(2) (West 2014).

The statute defines "disseminate" as "(i) to sell, distribute, exchange or transfer possession, whether with or without consideration or (ii) to make a depiction by computer available for distribution or downloading through the facilities of any telecommunications network or through any other means of transferring computer programs or data to a computer." 720 ILCS 5/11-20.1(f)(1) (West 2014).

¶ 61 Defendant does not dispute that the three videos at issue depicted child pornography. He also does not appear to dispute in this section of his brief that the State proved he possessed those videos. Rather, he challenges whether the State proved he knowingly disseminated them.

¶ 62 We hold the evidence was sufficient to sustain defendant's convictions. Bruns testified that on November 2, 2015, his computer software searched a file-sharing network called Gnutella and downloaded three videos depicting child pornography from a particular IP address. Bruns

then learned this IP address was associated with defendant's residence and Comcast account. Upon searching the unallocated space of the hard drive of a computer found in the master bedroom of defendant's residence, Strahm located file paths corresponding to the names of the videos Bruns's software had downloaded. Those file paths indicated the files had been stored in a saved folder associated with FrostWire. Strahm also found indications that an old version of FrostWire, capable of using the Gnutella network, had once been on defendant's hard drive. This evidence provided sufficient proof of the *actus reus* of disseminating child pornography, as defendant made material constituting child pornography "available for distribution or downloading" via a computer program. 720 ILCS 5/11-20.1(f)(1) (West 2014).

¶ 63 With respect to the *mens rea* for the crime, the statute requires a person to disseminate child pornography with "knowledge of the nature or content thereof." 720 ILCS 5/11-20.1(a)(2) (West 2014). Defendant admitted during his police interview he knew the videos he routinely downloaded depicted minors engaged in sexual activities. Thus, he clearly had knowledge of the nature or content of the material at issue. Without offering any analysis or citing authority, defendant assumes the statute also requires knowing dissemination. The State does not dispute defendant's assumption. At any rate, the evidence showed defendant knowingly disseminated child pornography. Among defendant's admissions were (1) he remembered downloading and watching at least one of the three videos at issue and (2) he knew FrostWire was "a sharing program and you have to agree to share videos with other people." Bruns testified his software downloaded three videos depicting child pornography from an IP address linked to defendant's Comcast account and residence. From defendant's admissions, a reasonable fact finder could determine defendant knew he was making child pornography available for distribution or downloading by using FrostWire to acquire child pornography.

¶ 64 In challenging his convictions, defendant mentions that (1) there was no specific correspondence showing him transmitting child pornography, (2) there was no evidence he placed the subject videos in a "shared folder" on his computer that was viewable to others, and (3) the actual videos were not on his computer when the State's witnesses examined it. However, defendant fails to mention his own statements to the police, including his admission he knew the program he used to acquire child pornography required him to agree to share videos with other people. Additionally, Flores testified that if someone were able to download a file through a peer-to-peer network, that means the file was *not* deleted on the originating computer. In other words, according to Flores, that file would be "present and allocated on the source" at the time of the download. Thus, the evidence supported an inference that defendant deleted the subject videos from his computer—thus relegating them to the unallocated space of his hard drive—sometime *after* Bruns downloaded those videos from him. Defendant's analogy about somebody breaking into his car to steal his child pornography is inconsistent with the evidence presented.

¶ 65 The only authority defendant cites in this section of his brief is a case affirming three defendants' convictions for dispensing narcotics. See *People v. Savage*, 84 Ill. App. 2d 73, 78 (1967). This case is irrelevant to our analysis of the sufficiency of the evidence.

¶ 66 B. People's Exhibit No. 3

¶ 67 Defendant also argues the trial court erred by admitting into evidence People's exhibit No. 3 (the three videos depicting child pornography), as the State failed to lay a proper

foundation. According to defendant, the State (1) "failed to provide sufficient evidence of how the images were acquired" and (2) "failed to provide a chain of custody of the images or any other acceptable form of authentication and identification to show that the images acquired Nov. 2, 2015 were in fact the same images presented to the court on December 13, 2021." Defendant explains why he believes the various factors discussed in *People v. Taylor*, 2011 IL 110067, pertaining to the "silent witness theory" did not justify admission of People's exhibit No. 3.

¶ 68 The State responds that Bruns's positive identification of the three videos provided a sufficient foundation for People's exhibit No. 3. The State maintains that because defendant did not present any evidence of tampering, the prosecution was required to establish only a probability that no tampering occurred. Additionally, the State proposes any gaps in the chain of custody went to the weight of the evidence, not its admissibility. According to the State, "[t]he fact that [Bruns's] computer successfully downloaded child pornography from defendant's IP address showed that the police computer was functioning and that Bruns knew how to operate it."

¶ 69 A reviewing court will not disturb a trial court's decision to admit evidence absent an abuse of discretion. *People v. Brand*, 2021 IL 125945, ¶ 36. "An abuse of discretion occurs when the trial court's decision is arbitrary, fanciful, or unreasonable or when no reasonable person would agree with the trial court's position." *Brand*, 2021 IL 125945, ¶ 36.

¶ 70 "The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Ill. R. Evid. 901(a) (eff. Sept. 17, 2019). Among the ways a party may authenticate an item is to introduce (1) "[t]estimony that a matter is what it is claimed to be" or (2) evidence regarding the "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics of an item, including those that apply to the source of an electronic communication, taken in conjunction with the circumstances." Ill. R. Evid. 901(b)(1), (4), (eff. Sept. 17, 2019).

¶ 71 In *Taylor*, our supreme court addressed what is known as the " 'silent witness' theory" in the context of authenticating surveillance footage, where there was no eyewitness to the events depicted. *Taylor*, 2011 IL 110067, ¶ 1. Pursuant to this theory, "a witness need not testify to the accuracy of the image depicted in the photographic or videotape evidence if the accuracy of the process that produced the evidence is established with an adequate foundation." *Taylor*, 2011 IL 110067, ¶ 32. The court then identified a nonexhaustive list of factors that "may be considered when determining whether the process by which a surveillance videotape was produced was reliable." *Taylor*, 2011 IL 110067, ¶ 35.

¶ 72 Unlike in *Taylor*, the purpose of the State seeking to admit People's exhibit No. 3 into evidence was *not* to prove the accuracy of the events recorded in that exhibit. Notably, in a prosecution for disseminating child pornography, laying the foundation for the admission of images does not require the State to show the images fairly and accurately depicted events that occurred. *People v. Thomann*, 197 Ill. App. 3d 488, 497 (1990). Moreover, there was no audio or video recording purportedly depicting defendant disseminating child pornography. Thus, contrary to what defendant contends, the silent witness theory is not instructive here.

¶ 73 Instead, to lay a foundation for admitting People's exhibit No. 3 into evidence, the State had to demonstrate this exhibit accurately depicted the videos Bruns's computer downloaded from an IP address linked to defendant. See *Thomann*, 197 Ill. App. 3d at 498 ("All the State

must show as a foundation is that the tape introduced into evidence is the tape [the investigator] received from the defendant and that this tape has not been altered in any fashion since then."). The State met its burden to establish this foundation. Bruns testified his computer software continuously searched a file-sharing network to identify files known to depict child pornography. Upon identifying such files, Bruns's software would download them automatically. Bruns explained that on November 2, 2015, his software downloaded files he later viewed and determined depicted child pornography. Bruns also testified he learned from Comcast that the IP address from which his software downloaded these files was associated with defendant's account and residence. Bruns testified that People's exhibit No. 3 was a disk containing the three videos his software downloaded. He also testified this exhibit was a fair and accurate copy of those video files. The State's evidence supported a conclusion that People's exhibit No. 3 was "what its proponent claims" (Ill. R. Evid. 901(a) (eff. Sept. 17, 2019))—*i.e.*, child pornography that Bruns's software downloaded from defendant's computer. Accordingly, the trial court did not abuse its discretion by admitting this exhibit into evidence.

¶ 74 Defendant identifies numerous purported deficiencies in the foundation for People's exhibit No. 3. For example, he mentions his witness, Daniel, testified about the importance of maintaining a chain of custody. However, chain of custody was *not* a foundational requirement for admitting People's exhibit No. 3 into evidence, as Bruns identified the videos as being the ones he observed during his investigation. See *People v. Schubert*, 136 Ill. App. 3d 348, 355 (1985) ("A proper foundation for the admission of an exhibit may be laid either through identification by a witness, or through establishment of a chain of possession, and it is not necessary to require both methods."). The trial court also reasonably discounted Daniel's testimony as being mere generalities, unrelated to the specific facts of this case.

¶ 75 Defendant also mentions Bruns did not identify the "machine" he used to acquire the subject videos. It is not clear what further specificity defendant believes was required to establish the foundation. For example, defendant does not cite any authority indicating it matters for purposes of laying a foundation whether Bruns's computer was manufactured by Dell or Apple. Defendant further notes Bruns did not regularly test his computer. But as Bruns testified, his computer was clearly functioning on November 2, 2015, as his device was able to download videos. Defendant cites no authority suggesting the lack of regular testing undermines the foundation for People's exhibit No. 3 under the circumstances of this case.

¶ 76 Moreover, defendant notes Bruns could not remember when he acquired the videos. However, Bruns testified his software automatically downloaded the subject videos on November 2, 2015. Although Bruns could not remember exactly when he viewed those videos, he positively identified People's exhibit No. 3 as containing the videos he viewed. Defendant does not cite authority indicating it makes a difference for purposes of laying a foundation whether Bruns viewed the videos an hour, a day, a week, or a month after his software downloaded them.

¶ 77 Defendant also notes Bruns could not remember certain details about his process of making a copy of the videos for the state's attorney's office. Again, these facts do not undermine the foundation for People's exhibit No. 3, as Bruns identified this exhibit as a fair and accurate copy of the videos his software downloaded. A duplicate of a recording "is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the

original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." Ill. R. Evid. 1003 (eff. Jan. 1, 2011). Neither of those exceptions applied here.

¶ 78 Finally, defendant claims aspects of Strahm's testimony revealed faults in the foundation for People's exhibit No. 3. These contentions are unpersuasive. No portion of Strahm's testimony cast doubt on Bruns's assertion that People's exhibit No. 3 was a fair and accurate copy of the three videos his software downloaded.

¶ 79 The State provided a proper foundation for People's exhibit No. 3. All of defendant's points are challenges to the weight to be attributed to this exhibit, not barriers to its admissibility.

¶ 80 C. Unit of Prosecution

¶ 81 Defendant also argues the trial court erred by entering more than one conviction and sentencing him on three counts of disseminating child pornography, as the State failed to prove he committed three separate offenses. Specifically, defendant proposes that to justify three convictions, the State was required to prove Bruns acquired the videos from defendant via "three separate downloads." In presenting this argument, defendant relies on *McSwain*. In *McSwain*, this court held that the appropriate unit of prosecution was ambiguous in the 2008 version of the child pornography statute. *McSwain*, 2012 IL App (4th) 100619, ¶ 59. Thus, where the defendant in *McSwain* simultaneously possessed multiple images of the same minor that were sent to him in a single e-mail, he could be sentenced only on one count of child pornography. *McSwain*, 2012 IL App (4th) 100619, ¶ 64.

¶ 82 The State responds that the legislature subsequently amended the child pornography statute to specify the appropriate unit of prosecution. The State further notes that even before this amendment went into effect in 2014, the Second District determined *McSwain* did not apply where a defendant simultaneously possessed multiple images of different children. *People v. Murphy*, 2013 IL App (2d) 120068, ¶ 10.

¶ 83 "The unit of prosecution of an offense refers to what act or course of conduct the legislature has prohibited for purposes of a single conviction and sentence." *People v. Hartfield*, 2022 IL 126729, ¶ 67. In other words, the question focuses on "determining how many times the same offense has been committed in a particular course of conduct." *Hartfield*, 2022 IL 126729, ¶ 73. "Determining the unit of prosecution is a question of statutory interpretation." *Hartfield*, 2022 IL 126729, ¶ 68. Courts must "look[ ] to the language of the statute to determine what precisely has been prohibited by the legislature and in what unit of time, actions, or instances that crime is committed once." *Hartfield*, 2022 IL 126729, ¶ 83. The controlling factor is "the unambiguous intent of the legislature." *Hartfield*, 2022 IL 126729, ¶ 83. If the legislature does not indicate the unit of prosecution, courts must resolve any doubt "against construing the statute as supporting multiple instances of the same offense based on the exact same act." *Hartfield*, 2022 IL 126729, ¶ 83. We review the trial court's ruling *de novo*. *People v. Sedelsky*, 2013 IL App (2d) 111042, ¶ 13.

¶ 84 As noted above, section 11-20.1(a)(2) of the Code provides, in relevant portion, that a person commits child pornography who,

> "with the knowledge of the nature or content thereof, *** disseminates *** any film, videotape, photograph or other similar visual reproduction or depiction by computer of any child *** whom the person knows or reasonably should know to be under the age

> of 18 *** engaged in any activity described in subparagraphs (i) through (vii) of paragraph (1) of this subsection." 720 ILCS 5/11-20.1(a)(2) (West 2014).

The statute defines "disseminate" as "(i) to sell, distribute, exchange or transfer possession, whether with or without consideration or (ii) to make a depiction by computer available for distribution or downloading through the facilities of any telecommunications network or through any other means of transferring computer programs or data to a computer." 720 ILCS 5/11-20.1(f)(1) (West 2014). Since January 1, 2014, the statute has stated:

> "The possession of each individual film, videotape, photograph, or other similar visual reproduction or depiction by computer in violation of this Section constitutes a single and separate violation. This subsection (a-5) does not apply to multiple copies of the same film, videotape, photograph, or other similar visual reproduction or depiction by computer that are identical to each other." Pub. Act 98-437 (eff. Jan. 1, 2014) (adding 720 ILCS 5/11-20.1(a-5)).

¶ 85 We hold that the trial court properly entered three convictions and sentenced defendant on three counts of disseminating child pornography. As an initial matter, *McSwain* is distinguishable, as the evidence here consisted of three separate videos depicting three different children. Additionally, before defendant committed the charged offenses in November 2015, the legislature amended the child pornography statute to clarify that possession of each distinct film constitutes a separate violation of the statute. 720 ILCS 5/11-20.1(a-5) (West 2014). Indeed, in *Hartfield*, our supreme court cited this statute as an example of where the legislature had clearly defined the unit of prosecution. *Hartfield*, 2022 IL 126729, ¶ 87. Although section 11-20.1(a-5) references the unit of prosecution for "possession" of child pornography, the definition of "disseminate" includes the exchange or transfer of possession of child pornography. Thus, under the plain language of the statute, defendant's actions constituted three separate acts of dissemination. Defendant's unit-of-prosecution challenge lacks merit.

¶ 86 III. CONCLUSION

¶ 87 For the reasons stated, we affirm the trial court's judgment.

¶ 88 Affirmed.