UNREPORTED

IN THE COURT OF SPECIAL APPEALS

OF MARYLAND

No. 1102

September Term, 2015

JARETT SAVOYE

v.

STATE OF MARYLAND

Graeff,
Kehoe,
Davis, Arrie W.
(Senior Judge, Specially Assigned),

JJ.

Opinion by Davis, J.

Filed: November 9, 2016

Appellant, Jarett Savoye, was tried and convicted by a jury in the Circuit Court for Baltimore County (Purpura, J.) of possessing child pornography. The court imposed a sentence of five years under the jurisdiction of the Maryland Department of Public Safety and Correctional Service. From the conviction and sentence, appellant filed the instant appeal, raising the following issues for our review, which we quote:

1. Did the trial court err in admitting hearsay records that were not authenticated?

2. Was the evidence insufficient to convict appellant?

FACTS AND LEGAL PROCEEDINGS

On December 18, 2012, Detective Josh Rees, a member of the Baltimore County Police Department assigned to the Crimes Against Children Unit, using a program installed on a computer at the Child Advocacy Center, downloaded from a free peer-to-peer ("P2P") file sharing network known as Ares Galaxy[1] an image titled !!!hothothot!!!tarapthcunknown79(2)(2).jpg, which depicted child pornography. Detective Rees explained that P2P networks enable file sharing, meaning individual computer users can share computer files directly with one another. He further explained that Ares, as part of its terms of service, has a default setting; downloaded files are stored in a specific directory on the user's computer so that other users can access the files to copy or download.

The user from whom Detective Rees downloaded the image was identified as ANON_6C2827DO@Ares. The user's Internet Protocol ("IP") address was identified as 108.40.39.208 and owned by Verizon. On February 20, 2013, Detective Rees obtained a

[1] Appellant's brief and trial transcripts spell the file sharing network as the "Aries."

grand jury subpoena and submitted it to Verizon, which disclosed that, from November 1**,** 2012, the IP address had been assigned to Walter R. Savoye,[2] age 86, at 901 Dogwood Hill Court, Towson, Maryland.

Three months later, on March 26, 2013, at 5:30 a.m., Detective Rees and several other officers executed a search warrant at the Dogwood Hill Court residence. They were "searching for anything that could be related to child pornography." Walter Savoye, Mary, his wife age 87, and appellant, their grandson, were home at the time. Detective Christopher Raut, a member of the Baltimore County Police Department assigned to the Police Crimes Against Children Unit, testified that he tested the Savoyes' wi-fi and determined that they used a "secure" network to access the internet. Following a preliminary forensic examination of three computers at the home, Mary Savoye's Acer laptop was seized. Detective Raut, although unable to observe any images, was "able to locate file titles consistent with that of child pornography and also some search terms that are currently used in [] locating child pornography from the internet and file sharing programs." No additional items related to the visual representation of child pornography were found at the home.

Mary Savoye testified that she kept her laptop in her room, but that she allowed appellant to use it from time to time. She relied on her two sons and husband, whom she described as computer experts, to help her when she encountered computer problems. Neither Mary Savoye nor her husband had ever seen images of a sexual nature on their

[2] Appellant's brief initially refers to the property owner as Walter Savage.

computers; nor were they familiar with P2P networks, file sharing or the Ares network. Both Mary and Walter Savoye testified that they had never used the laptop in question to access pornography.

Danna McAlister, a ten-year veteran of the Baltimore County Police Department's Digital Media Evidence Unit, was admitted as an expert in computer forensics. The following is her explication of the difference between allocated and unallocated space in the hard drive: Allocated space is where files that "you want [] go to . . . reside" and unallocated space is "where your deleted files go." She further explained that files may be disposed of in two ways: (1) by dragging the file to the recycle bin, where it remains until the recycle bin is emptied or (2) by right clicking delete, which removes the file from the file system completely, but leaves it in a "shredded" form in unallocated space. Deleting a file is one step further than placing the file in the recycle bin. A file that is deleted is "so far gone in unallocated space that it could only be recovered with . . . technical software." There are no "file paths" in unallocated space, so you cannot tell "where it comes from on the computer itself."

McAlister testified that Detective Rees requested a forensic examination of the laptop's hard drive to recover any P2P program settings and child pornography. She first made a copy of the laptop's hard drive to avoid corrupting the original. She then used Encase, which is a specialized software program, to view images located within the file system (in allocated space) but found none. She found movie titles indicative of child pornography in the file system, but the "movies were not playable." Using Encase, she

then examined deleted files in unallocated space and was able to "carve out" fifty-six movies and three images depicting child pornography. Four images were displayed for the jury.

McAlister also ran an Internet Evidence Finder program ("IEF") on the hard drive and found internet searches for (1) "Ares," and (2) terms associated with child pornography, such as "pthc" and "ptsc," which mean preteen hard core and preteen soft core. She testified that the Ares program was not actively installed on the laptop when it was seized, but that remnants of it remained in the deleted, unallocated space on the laptop's hard drive. She added that the IEF report listed downloads to an Ares downloads folder, including the title, "!!!hothothot!!!tarapthcunknown79(2)(2).jpg," which the report indicated had been downloaded on December 18, 2012 at 6:41a.m.

McAlister also exported and examined the "thumbs DB files," which she explained are left in Windows folders that at one time contained images, using a digital investigations platform known as Forensic Toolkit (FTK). She testified, "No notable thumb nail files were located." She also searched for the term ANON 6C2827DO, but "no hits were received for that." After she submitted her report to Detective Rees, he submitted three "case enhancement requests." He asked her to look for appellant's email address, *i.e.*, jsavoye8l@gmail.com. McAlister testified, "There were emails but no[thing] notable." She subsequently used another forensics software known as "X-Ways,"[3] but "didn't find

[3] Appellant's brief refers to the forensic software as "x-waves" and the trial transcript refers to it as both "x-ways" and "x-waves."

anything notable" on the hard drive. She found no pictures, movies, written correspondence or "notable" emails on the hard drive tying appellant to his grandmother's laptop.

Konstantinos Dimitrelos, testifying on behalf of the defense as an expert in cyber forensics, explained that anything found in unallocated space "has no ownership, no creator, no create time, no name." He added that "anything we find in unallocated [space] is not attributed to anyone using that computer system." He further testified that data in unallocated space could only be accessed or recovered from the laptop by a person with "extensive training" and costly computer forensic tools. He testified that, in his expert opinion from a forensic perspective, "[t]here's no evidence that links [appellant] to being the one who downloaded, possessed or distributed child pornography."

The trial court permitted the State, over objection, to admit into evidence under the Business Records Exception to the Hearsay Rule, *i.e.*, Md. Rule 5-803(b)(6), a document from Verizon which contained identifying information about the IP address from which Detective Rees downloaded the image on December 18, 2012. The record was admitted without testimony of the custodian of records pursuant to Md. Rule 5-902(b).

Detective Rees testified that Verizon had responded to a grand jury subpoena by identifying "who that IP address was assigned to and the date and the time of the download." The following then ensued at the bench:

> [APPELLANT'S COUNSEL]: Your Honor, I know exactly [] where the State is going with this and I would make an objection to the—
>
> [THE COURT]: Okay. Well, I don't know where they're going so you got to give me a heads up.

[APPELLANT'S COUNSEL]: State's Exhibit number three, Your Honor, if the, purportedly the certified business records from the ISP, internet service provider.

[THE COURT]: From Verizon, okay.

[APPELLANT'S COUNSEL]: That would link it to my client (inaudible).

[THE COURT]: Well, would, it would link it to the owner of the, of the IP address.

[PROSECUTOR]: IP address.

[THE COURT]: Which would be the Savoyes.

[APPELLANT'S COUNSEL]: (inaudible).

[THE COURT]: Presumably, yeah.

[APPELLANT'S COUNSEL]: For this to come in, it would have to come in as a certified business record (inaudible).

[THE COURT]: Okay.

[APPELLANT'S COUNSEL]: The State's certification is dated today.

[PROSECUTOR]: But the information was provided—

[THE COURT]: The information that's in the records.

[PROSECUTOR]: Was provided in discovery back in two thousand and whatever.

[THE COURT]: And we're in the, and the information that's in the records does it not indicate who the owner was on the date in question?

[PROSECUTOR]: It does. It does.

[THE COURT]: Okay.

[PROSECUTOR]: (inaudible).

[THE COURT]: So what difference does it make that, I mean, the certification should have today's date on it.

[APPELLANT'S COUNSEL]: Well, no, the certification, Your Honor, should have the date that it was compiled by the custodian of records, Your Honor, and in this case, it is unclear that the custodian of records who signed that today was the custodian of records that assembled that information. I would refer to *Shpigel* v. *White,* 357 Md. 117 from 1999, which goes into depth about how the custodian of records—

[THE COURT]: Okay. Now, the certification I have indicates that the attached, it's only a one page record, is true and accurate, created from information maintained by Verizon in the actual course of business, that it's Verizon's ordinary practice to maintain such records and that the records are made contemporaneously with the transaction and events stated. Now, it indicates that, okay, that the IP address was in use on the date of the subpoena and the date of the sub, the date that the subpoena was the, whatever it is, the date in question, Ms. Dever [*i.e.*, the prosecutor], yes or—

[PROSECUTOR]: Yes.

* * *

[THE COURT]: Okay, So what's your problem with this?

[APPELLANT'S COUNSEL]: Your Honor, I'm attacking the self-authenticating nature of this document, Your Honor. The document itself I have no qualms—

[THE COURT]: Well, hold on a sec, you got this in discovery, right?

[APPELLANT'S COUNSEL]: The second page, no argument, Your Honor. The first—

[THE COURT]: Okay. I had a question, I want an answer to it. You got it in discovery, yes or no?

[APPELLANT'S COUNSEL]: The second page, yes.

[THE COURT]: Yes, okay. Okay. The first page, which is the certification, that was more recently, I would assume updated for purposes of trial, correct?

[PROSECUTOR]: Correct.

[THE COURT]: Okay. Okay and your problem with it is what?

[APPELLANT'S COUNSEL]: The original provided in discovery, Your Honor, had a blank certificate from the custodian of records, Your Honor.

[THE COURT]: Okay.

[APPELLANT'S COUNSEL]: Today—

[THE COURT]: That's not unusual.

[APPELLANT'S COUNSEL]: —this—

[THE COURT]: Because they're, that, they were responding to a subpoena—

[PROSECUTOR]: Correct.

[THE COURT]:—as opposed to certifying it for trial, that's why. Okay.

[APPELLANT'S COUNSEL]: Today, the State is going to, I'm assuming, attempt to introduce this document as a self-authenticating record pursuant to both to the hearsay rule—

[PROSECUTOR]: As a business record.

[THE COURT]: It's a business record.

[APPELLANT'S COUNSEL]: But it's self-authenticating, Your Honor, there's no one from Verizon here to testify.

[PROSECUTOR]: I had given notice that the State intended to put all documents into evidence as business documents. That, I mean, that goes in our initial discovery so.

[THE COURT]: Right, I understand that, but it's a, it's, it's a business record.

* * *

[APPELLANT'S COUNSEL]: And my argument, Your Honor, is that in order for the document to be self-authenticating, I agree that it is a business record, but for it to be admitted without the presence, the physical presence of the custodian of records, Maryland Code Annotated, Courts & Judicial Procedures 10-101, *et. al.*, need to be complied with, Your Honor, both for the notice requirements of the certificate—

* * *

. . . The rule that would cover this—

[THE COURT]: It's an evidentiary rule.

[APPELLANT'S COUNSEL]: —would be 5–803(b)(6).

(Emphasis added). Appellant's counsel further argued that the State had not complied with the notice requirement and that the certificate mandated by Md. Rule 5–902(b)(A)(i)-(ii) had not been previously provided. The court overruled the objection and subsequently permitted the State to introduce into evidence the Verizon report over defense counsel's renewed objection. Appellant was ultimately convicted of possessing child pornography and the instant appeal followed.

DISCUSSION

A. Business Record Hearsay Exception

Appellant contends that the trial court erred in permitting the State to introduce a document from Verizon ("the document") which contained identifying information about the IP address from which Detective Rees downloaded the illicit material in question because it was not properly authenticated and, according to appellant, was inadmissible hearsay, not covered under the business records exception. Specifically, appellant asserts that the accompanying certificate "did not comply with the certification requirements of Rule 5–902."

The State first responds that appellant has failed to preserve the issue because appellant's counsel objected to the introduction of the document on the grounds that the document presented at trial was not the same document received in discovery, where the

document had been accompanied by a certification without a date. The State asserts that appellant is making a new argument concerning the inadequacy of the business record certification because it was not signed under "penalties of perjury." The State also asserts that, to the extent that appellant's argument has been preserved when admitted at trial, the document was accompanied by a certificate from the Verizon custodian of records attesting that the document was made and kept in the ordinary course of business. Accordingly, the State maintains, the trial court did not err in admitting the business record and we should affirm.

"Under the Maryland Rules, hearsay must be excluded as evidence at trial unless it falls within an exception to the hearsay rule. Thus, a trial court's decision to admit or exclude hearsay ordinarily is an issue of law and . . . we review decisions of law *de novo*." *Hall v. Univ. of Maryland Med. Sys. Corp.*, 398 Md. 67, 83 (2007) (citing MD. RULE 5–802.8).

"Whether hearsay evidence is admissible under an exception to the hearsay rule, on the other hand, may involve both legal and factual findings. In that situation, we review the court's legal conclusions *de novo*, but we scrutinize its factual conclusions only for clear error." *Baker v. State*, 223 Md. App. 750, 760 (2015) (citations omitted).

An out-of-court statement, offered as evidence to prove the truth of the matter asserted, constitutes hearsay and is generally inadmissible. MD. RULE 5–801(c). There are certain exceptions to the hearsay rule, where hearsay statements are not excluded, *per se*, even though the declarant is available as a witness. MD. RULE 5–803. One such exception,

governed by Md. Rule 5–803(b)(6), is for "Records of Regularly Conducted Business Activity," also known as the "Business Records Exception," which provides:

> A memorandum, report, record, or data compilation of acts, events, conditions, opinions, or diagnoses if (A) it was made at or near the time of the act, event, or condition, or the rendition of the diagnosis, (B) it was made by a person with knowledge or from information transmitted by a person with knowledge, (C) it was made and kept in the course of a regularly conducted business activity, and (D) the regular practice of that business was to make and keep the memorandum, report, record, or data compilation. A record of this kind may be excluded if the source of information or the method or circumstances of the preparation of the record indicate that the information in the record lacks trustworthiness. In this paragraph, "business" includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

"To admit evidence under the business records exception to the hearsay rule, the proponent of the evidence must lay a proper foundation." *Baker*, 223 Md. App. at 764. *See State v. Bryant*, 361 Md. 420, 428 (2000) ("Proper certification, under Rule 5-902(a)(11), establishes a *prima facie* foundation for the business records exception."). The custodian of the records does not have to testify; the documents may be "self-authenticating." Md. Rule 5–902(b)(1) outlines the procedure for self-authenticating certified records of regularly conducted business activity.

> Testimony of authenticity as a condition precedent to admissibility is not required as to the original or a duplicate of a record of regularly conducted business activity, within the scope of Rule 5–803(b)(6) that has been certified pursuant to subsection (b)(2) of this Rule, provided that *at least ten days prior to the commencement of the proceeding in which the record will be offered into evidence*, (A) the proponent (i) notifies the adverse party of the proponent's intention to authenticate the record under this subsection and (ii) makes a copy of the certificate and record available to the adverse party and (B) the adverse party has not filed within five days after service of the proponent's notice written objection on the ground that the sources of information or the method or circumstances of preparation indicate lack of trustworthiness.

(Emphasis supplied). Furthermore, subsection (b)(2) provides a form of certification that must be "substantially" followed in order for the business record to be admitted as self-authenticating.

In the case *sub judice*, we first examine whether appellant has preserved, for our review, the issue of whether the trial court erred by admitting into evidence a self-authenticating business record where, during discovery, the document was accompanied by an undated certification and, at trial, the certification does not expressly state that it was signed "under penalties of perjury" as provided for in Md. Rule 5–902(b)(2). The State would have us decline review, arguing that appellant, at trial, only objected to the undated certification, making a "new" argument on appeal concerning the "under of penalties of perjury" language missing from the certification and any review of the issue should be constrained to the certification's date. We agree with the State that, at trial, appellant focused on the undated certification from discovery and the dated document at trial. During a colloquy with the court, appellant expressly states that they received the document years prior in discovery. The contention, according to appellant, concerning the date is that, because appellant did not have the 'dated' certification before, despite possessing the identical document, he did not have adequate notice of its use as evidence at trial. Furthermore, when the Assistant State's Attorney, during the same colloquy, stated that notice was given that all documents provided in discovery were intended to be put into evidence as business records, appellant did not contest or refute this assertion. Nor does appellant contend, at trial, that the certification is defective in any other regard. We hold

that the document was offered well beyond the ten days prior to the commencement requirement under Md. Rule 5–902(b)(1) and appellant had notice concerning the document's use, as a business record, as evidence by the State.

Accordingly, we hold that appellant has not preserved the issue presented in his appellate brief for our review. First, the only discrepancy that appellant notes between the certification from the document during discovery and the document presented at trial is the date. If appellant objected to the missing language, *i.e.* "under penalties of perjury," he should have filed a written objection "within five days after service of the proponent's notice . . . on the ground that the sources of information or the method or circumstances of preparation indicate lack of trustworthiness," as required under Md. Rule 5–902(b)(1)(B). Second, appellant failed to make an objection on the record regarding the issue. A review of the trial transcript illustrates that appellant did not mention once the missing language, "under penalties of perjury." Although making this argument at trial may not cure the failure to file the written objection, as required under the Md. Rule 5–902, it certainly reinforces the State's argument that appellant has not preserved this issue for our review.

Assuming, *arguendo*, that appellant has preserved this issue for our review, his argument nevertheless fails. His contention, on appeal, is that the trial court erred by admitting into evidence the document as a business record exception to the hearsay rule because the certification lacked the language "under the penalties of perjury." Md. Rule 5–902(b)(2) requires that the form of certification be *substantially* complied with. The certification accompanying the document, at trial, expressly states: "I, Jason Craumer,

being *duly sworn, depose and say* . . . ." Being "duly sworn" indicates that the custodian made an oath before an officer authorized to administer oaths in accordance with the law, per Md. Rule 1–304.

Therefore, we hold, if appellant's argument was preserved for our review, the document's custodian at Verizon substantially complied with Md. Rule 5–902(b) and we, therefore, affirm the trial court's admittance of the document into evidence as a business record.

B. Sufficiency of the Evidence

Appellant contends that "the laptop's file system did not contain child pornography" nor did the "recycle bin" of the laptop. Appellant further contends that "[t]he prohibited material had at some unspecified point been deleted" evinced from the fact that "[i]t could only be accessed from unallocated hard drive space by using specialized computer forensic software." Appellant asserts that the State, "among other things, . . . was required to prove that he 'knowingly possess[ed] and intentional retain[ed]' the prohibited material. It failed to do so here."

The State responds that appellant has failed to preserve this claim for our review. However, even if preserved, the State argues that, although the prohibited image had been deleted and was not "immediately accessible," it was still on the laptop's hard drive and had been made available, *via* the Ares network for file sharing. Therefore, the State maintains, if preserved, the evidence presented was sufficient to sustain appellant's

conviction for possession of child pornography and we should affirm the lower court's ruling.

> It is well settled that appellate review of the sufficiency of the evidence in a criminal case tried by a jury is predicated on the refusal of the trial court to grant a motion for judgment of acquittal. Maryland Rule 4–324 requires a defendant to state with *particularity* all the reasons why the motion [for judgment of acquittal] should be granted. This means that a defendant must argue precisely the ways in which the evidence should be found wanting and the particular elements of the crime as to which the evidence is deficient. The issue of sufficiency of evidence is not preserved when appellant's motion for judgment of acquittal is on a ground different than that set forth on appeal.

Poole v. State, 207 Md. App. 614, 632–33 (2012) (Emphasis supplied) (quotations and citations omitted). *See also Hobby v. State*, 436 Md. 526, 540 (2014) (quoting *Anthony v. State*, 117 Md. App. 119, 126 (1997) (Emphasis supplied) ("[A]ppellate review of sufficiency of evidence is available only when the defendant moves for judgment of acquittal at the close of all the evidence and argues *precisely* the ways in which the evidence is lacking."); *Montgomery v. State*, 206 Md. App. 357, 385 (2012) (Emphasis supplied) (citation omitted) ("[A] motion which merely asserts that the evidence is insufficient to support a conviction, without *specifying* the deficiency, does not comply with [Maryland] Rule [4–324(a),] and thus does not preserve the issue of sufficiency for appellate review.").

We agree with the State that, in the instant case, appellant has failed to argue that the issue has been preserved. At the end of the State's case, appellant's trial counsel, when asked by the court if he wanted to be heard, stated that he wanted to make a motion for judgment of acquittal. The following colloquy occurred regarding the possession of child pornography:

> [APPELLANT'S COUNSEL]: Yes, Your Honor. Looking at the third count, the child pornography possession, Your Honor, that requires both the knowing possession of it and the—
>
> [THE COURT]: Right. We're at the end of the State's case, this is not the end of all of the evidence. The evid, it's been generated, so I'll deny your Motion on that . . . .
>
> At the close of all the evidence, the following brief colloquy occurred:
>
> [THE COURT]: Okay. Let's get the jurors.
>
> [APPELLANT'S COUNSEL]: Your Honor, I have, I'd like to renew my Motion for Judgement of Acquittal.
>
> [THE COURT]: Go ahead, you can go get them awhile. Denied.
>
> [APPELLANT'S COUNSEL]: Thank you.

As the preceding excerpts clearly illustrate, appellant's trial counsel provided no specific, particularized grounds for his Motion for Judgment of Acquittal. Accordingly, the issue of sufficiency of evidence has not been preserved for our review.

Assuming, *arguendo*, that the issue has been preserved for our review, in determining whether the evidence presented was sufficient to support the conviction, we must determine "whether 'any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt' when the evidence is presented in the light most favorable to the State." *Bible v. State*, 411 Md. 138, 156 (2009) (quoting *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). We are required to "'give deference to all reasonable inferences [that] the fact-finder draws, regardless of whether [we] would have chosen a different inference.'" *Bible*, 411 Md. at 156 (quoting *State v. Suddith*, 379 Md. 425, 430 (2004)).

Md. Code Ann., Crim. Law ("C.L.") § 11–208(a) provides that

> (a) A person may not knowingly possess and intentionally retain a film, videotape, photograph, or other visual representation showing an actual child under the age of 16 years:
>
> (1) engaged as a subject of sadomasochistic abuse;
>
> (2) engaged in sexual conduct; or
>
> (3) in a state of sexual excitement.

Md. Code Ann., C.L. § 11–201(c) defines "knowingly" as "having knowledge of the character and content of the matter.

The Criminal Law Article does not define "possession," for purposes of § 11–201; however, this Court in *McIntyre v. State*, 168 Md. App. 504 (2006), adopted the analysis of possession of a controlled dangerous substance to inform our analysis of the sufficiency of the evidence in child pornography possession cases. Although *McIntyre* concerned physical evidence of child pornography, *i.e.*, computer disks, the *McIntyre* possession analysis is also appropriate in the case *sub judice*.

> In drug cases, the factors to be considered in determining whether the defendant had possession are as follows:
>
> > 1) [The] proximity between the defendant and the contraband, 2) the fact that the contraband was within the view or otherwise within the knowledge of the defendant, 3) ownership or some possessory right in the premises or the automobile in which the contraband is found, or 4) the presence of circumstances from which a reasonable inference could be drawn that the defendant was participating with others in the mutual use and enjoyment of the contraband.

McIntyre, 168 Md. App. at 521 (quoting *Folk v. State*, 11 Md. App. 508, 518 (1971)). Furthermore, "[w]e have said that '[p]ossession [of controlled dangerous substances] need

not be immediate and direct but may be constructive.' The fact that [items] were not found on the person of the defendant does not prevent the inference that the defendant had possession and control of those [items]." *Id.* (quoting *Archie v. State*, 161 Md. App. 226, 244–45 (2005)).

In the instant case, appellant does not dispute the presence, prior to its deletion, of child pornography on the laptop. Essentially, appellant argues that, because the material had been deleted and was not readily accessible by him, he was not in possession of child pornography and that the State failed in its burden to present evidence that would support his conviction under § 11–208(a) beyond a reasonable doubt. We disagree.

We note a paraphrasing of the enumerated list of evidence included in the State's brief:

> 1. Three people had access to the laptop—appellant, his 87-year-old grandmother Mary, and his 86-year-old grandfather Walter.
>
> 2. Mary and Walter Savoye's use of the laptop was limited.
>
> 3. Neither Mary nor Walter Savoye were familiar with P2P networks, file sharing or the Ares Galaxy network. Neither Mary nor Walter Savoye had ever seen any pornography on the laptop and both testified that they had never used the laptop to access pornography.
>
> 4. Appellant had access to the laptop and used it on occasion.
>
> 5. Detective Rees downloaded an image on December 18, 2012, depicting child pornography using the Ares P2P network which required users to enable the sharing of files, storing them in specific directories so other users could access them.
>
> 6. The user from whom Detective Rees downloaded the image used an IP address that was owned by Verizon and assigned to its customer, Walter Savoye.

> 7. A search of the Savoye residence revealed that they used a "secure" network to access the internet, "meaning that no outsiders could use their network for accessing the internet," and that the image downloaded by Detective Rees was found on Mary Savoye's Acer laptop, along with other images and movie clips later determined to depict child pornography.
>
> 8. Although the image had been deleted, police were able to use forensic software to confirm that the same image downloaded by Detective Rees on December 18, 2012 was in the unallocated space on the laptop.

Appellant's argument focuses on "current possession" of the illicit material; that the image was deleted and he could not access it. Appellant fails to acknowledge, however, that at least one image from the laptop depicting child pornography was available to Ares users on December 18, 2012, when Detective Rees was able to download the image, thereby establishing that, on at least one occasion, appellant was in possession of child pornography. In that context, a jury could have determined that the *Folk* factors of possession of a controlled dangerous substance, as cited in *McIntyre*, *supra*, were sufficiently established, beyond a reasonable doubt, by the evidence presented.

Accordingly, we hold that the issue has not been preserved for our review; however, even if it had been, there was sufficient evidence to convict appellant of possession of child pornography.

JUDGMENT OF THE CIRCUIT COURT OF BALTIMORE COUNTY AFFIRMED; COSTS TO BE PAID BY APPELLANT.