IN THE COURT OF CRIMINAL APPEALS OF TENNESSEE
AT NASHVILLE
Assigned on Briefs October 8, 2013

STATE OF TENNESSEE v. JARED SCOTT AGUILAR

Appeal from the Circuit Court for Montgomery County
No. 41100542 Michael R. Jones, Judge

No. M2012-02611-CCA-R3-CD - Filed December 18, 2013

The defendant, Jared Scott Aguilar, appeals from his Montgomery County Circuit Court jury convictions of six counts of sexual exploitation of a minor, *see* T.C.A. § 39-17-1003(a)(1), claiming that the trial court erred by denying his motion to suppress evidence seized pursuant to a search warrant, that the evidence was insufficient to sustain two of the convictions, that the counts of the indictment are multiplicitous, and that the 10-year effective sentence is excessive. Discerning no error, we affirm the judgments of the trial court.

Tenn. R. App. P. 3; Judgments of the Circuit Court Affirmed

JAMES CURWOOD WITT, JR., J., delivered the opinion of the Court, in which ROBERT W. WEDEMEYER and ROGER A. PAGE, JJ., joined.

Roger E. Nell, District Public Defender; and Crystal L. Myers, Assistant District Public Defender, for the appellant, Jared Scott Aguilar.

Robert E. Cooper, Jr., Attorney General and Reporter; Kyle Hixson, Assistant Attorney General; John W. Carney, District Attorney General; and Dan Brollier, Assistant District Attorney General, for the appellee, State of Tennessee.

OPINION

A Montgomery County Circuit Court jury convicted the defendant of one count of knowingly possessing 100 or more images of child pornography, one count of knowingly possessing 50 or more images of child pornography, and four counts of knowingly possessing a single image of child pornography, all in violation of Code section 39-17-1003. *See* T.C.A. § 39-17-1003(a)(1), (b), (d) (2006). At trial, Montgomery County Sheriff's Office Investigator Mike Cereceres testified that as a member of the Internet Crimes Against

Children task force, he utilizes file sharing software and graphic search terms, techniques most often used by consumers of child pornography, to discover those viewing child pornography and sharing child pornography data, "whether it be in a video format, whether it be an image." He explained that file sharing software enables users "to share videos back and forth, to share PDFs, to share movies." He said, "[I]f I have all this stuff on my computer which I'm sharing, videos, pictures, it's there for the world to get. All they have to do is use the same software that I have, type in the title of what they want." He said that, in a typical case, after he observes a user's viewing or sharing child pornography, he "geolocate[s]" the user using the internet protocol ("IP") address of the computer used to view or share the images. He said that the "IP address . . . is essentially nothing more th[a]n like a house address except your computer gets assigned an address." If he ascertains that the computer is located in Montgomery County, he asks for a judicial subpoena to be sent to the internet service provider for that IP address in order to determine the name and address of the service subscriber and owner of the computer. After determining the owner and subscriber information, he conducts surveillance on the residence before requesting a search warrant. After obtaining a search warrant, he executes the warrant, most often at night.

Investigator Cereceres testified that in this case, while using file sharing software on January 9, 2011, he "ended up making a download off of the [d]efendant's computer. . . . [and] obtaining three images of child pornography." He said that the titles of the files indicated to him that they contained child pornography.[1] He viewed the files and confirmed that they did, in fact, contain child pornography. He said that each of the files had a different "secure hash algorithm" ("SHA"), which, he explained, is akin to fingerprints in that it renders individual files unique. He said, "No other file is going to have that same SHA one value." After viewing the downloaded files, he "geolocated" the IP address of the computer and determined that it was in Montgomery County. He then obtained a judicial subpoena that he sent to the internet service provider, and the service provider indicated that the IP address was registered to the defendant. He used the information gleaned during his investigation to obtain a warrant to search the defendant's residence and computer.

Investigator Cereceres said that when officers executed the search warrant at the defendant's residence on January 31, 2011, the defendant answered the door and indicated that he was alone. During the search, officers seized two laptop computers, and the defendant admitted ownership of one of the laptops. Upon questioning, the defendant acknowledged that he had used file sharing software, saying that he "was downloading movies like Twilight for his wife, and he's just made a lot of downloads of various things."

---

[1]The titles of the files obtained by Investigator Cereceres are, to say the least, vulgar. For this reason, and because the precise titles have no bearing on the outcome of this case, we will not repeat them here. Suffice it to say that the investigator's suspicions were well founded.

Investigator Cereceres said that the defendant also provided a written statement:

> "I have a program called FrostWire that I use to download music and movies. In the past when child pornography was accidently downloaded I deleted it immediately. While making mass downloads in the past I have downloaded various things that I am not interested in, and I deleted them as such.
>
> When my wife and I have friends over I'm usually the first to pass out. I leave my computer logged on in case anyone wants to use it. I have not had any issues with any friends in the past using my computer to download child porn or anything else that is illegal.
>
> I had a small party this past weekend to watch the probowl. . . . I enjoy inviting new soldiers to my house for various occasions to give them a sense of brotherhood.
>
> I have searched FrostWire for porn using such key words as little boy slash girl. I know it sounds suspicious; my intention was looking for jailbait. My understanding of jailbait is that it's a young girl, above the age of 18 that can pass for younger. I'm not interested in child porn in any way, shape or form.
>
> Let's see; a video that was downloaded by accident that involved two boys. I tried to delete it, but the computer said it was open in another program. I still have not been able to delete it. I searched hymen looking for virgins obviously over the age of 18. Carl David Hyman came up as pictures. I downloaded the page, and the pictures ended up being child porn. Again, I discarded them as something I wasn't interested in.
>
> When downloading movies I have hit preview and seen that it was child porn and stopped the download. These files are . . . in the incomplete section of the FrostWire folder. . . .
>
> I started using FrostWire when I got my computer in 2009. One day I accidently downloaded child porn. I was so shocked that I did delete it - - the image and uninstalled

> FrostWire. I reinstalled it thinking that I can just ignore anything like that that came up. I had done so by deleting anything that is child porn. I have also typed in church girls gone wild thinking it was innocent girls over the age of 18 that became sluts. I never tried it again when it turned out to be child porn. . . .

Investigator Cereceres acknowledged that a user could accidentally download child pornography, but he stated that an accidental download would be rare and that more than one accidental download to the same computer would be even more rare. He said that the search terms that the defendant admitted using were those most often used by individuals looking for child pornography and that, in his experience, those search terms were not indicative of a desire to view adult pornography.

During cross-examination, Investigator Cereceres said that he did not know when the defendant had downloaded the files or how many times the defendant had accessed those files. He explained that when using file sharing software, "if you click on one file, you're initiating that download of just the one file." He said that a file sharing software user can see what is on another computer "on a list." He maintained that "virus-wise or even someone hacking your e-mail wouldn't put a copious amount of child pornography on your computer."

During redirect examination, Investigator Cereceres said that the files observed via file sharing software would not automatically download after a search. Instead, he said, "[Y]ou have to choose to double click on it, or right click, you have to make that choice." He said that, because downloading the files required an intentional download, the presence of these files on the defendant's computer was indicative of an intentional decision to download child pornography. He said, "[G]oing online, you know, and to Google child pornography, it's not that easy to find unless you know what you're doing." He added that most internet search engines filter out child pornography even when illicit search terms are used and that he had "never seen" internet "pop ups" that downloaded child pornography onto a computer.

Dickson County Sheriff's Department Detective Scott Levasseur testified that he was "in charge of the computer forensics lab, cyber crime unit" and also assigned as an investigator for the district attorney's office and "to the FBI task force out of Nashville." He said that his primary duty in each of these roles was to perform forensic examinations of computers and other electronic equipment as an "electronic evidence collection specialist." He explained, "The job of a computer forensic examiner is to examine a device, find the evidence as it pertains to the case, preserve it and have it ready for display in a courtroom."

Detective Levasseur testified that Investigator Cereceres brought a laptop and some other pieces of evidence to be examined by Detective Levasseur. Only the laptop contained relevant evidence. He explained the process of forensic examination:

> We disconnect the battery supply, remove the hard drive. And then I take the hard drive out of the laptop and hook it up to a [write] blocker. And all a [write] blocker is is a physical device that allows me to copy the hard drive without writing anything to the hard drive, so I'm not making changes on that hard drive at all. And I copy the hard drive over onto one of the hard drives in the lab, so that I can work on it.
>
> And before that process starts, you were told about a hash value, well, we do an M-D hash on the hard drive and it hashes the whole hard drive, and it gives us one of them big long numbers, and then it copies it, and then it hashes the copy to make sure that it's the same number, so we've an exact - - an identical copy. And I did get an identical copy of the hard drive. After it's copied over and verified that it's identical, then I put the hard drive back in the lap top, and it goes into the evidence, and . . . I don't touch it again. I do all my work off of the image copy that I have.
>
> . . . [W]hat I do after I copy the hard drive and process it with my forensics software to get it indexed out, the first thing I go ahead and do is I search for child pornography. I actually go through and individually look at every picture that's on the computer that's live, or been deleted, or whatever and scan through them, and bookmark out. And bookmarking out just means set aside for later examination when I find files that I believe to be child porn. So I look for all the images and all the videos that could be child pornography and bookmark them and mark them for later examination.

Detective Levasseur said that he used "software that . . . indexes the entire hard drive and it separates all the files . . . . So it will put all the pictures in one location and all the videos in another location and all the word documents in another location." He explained that unallocated space on the hard drive is space "that's not being used but there's files there. Because when a file gets deleted . . . . [i]t doesn't actually go anywhere[], it's still in the same place it was physically on the hard drive but it's just being given a tag that hey, its been

deleted." He testified that although the "deleted" file remains on the computer until overwritten by another file, "it's not accessible to the user." Detective Levasseur explained that after his software indexed the files, he manually examined all the image files by viewing them as "thumbnail images" to determine if any contained child pornography. He said that he used his training and experience to make that determination, explaining, "I've seen millions [of images]. I've seen the same ones over and over and over. I'm pretty familiar with all the different series." He said that all child pornography collected during law enforcement investigations is sent to the National Center for Missing and Exploited Children, which places the images into a database. The agency then confirms which images actually contain minors.

Detective Levasseur testified that he located more than 160 images containing child pornography and six videos depicting child pornography on the defendant's laptop under the user account "Jared." He explained that the name of the computer was "Jared and Brittany" and that it contained two user accounts, one for "Jared" and one for "Brittany." He said that the "Jared" account had been used 2,521 times and the "Brittany" account had been used only 77 times. No child pornography was located under the "Brittany" profile. Detective Levasseur recalled that he found the pornographic images "in the owner's FrostWire save folder and unallocated space, which is free space, and the system volume information." Specifically, six child pornography videos came from the "FrostWire save folder." He explained, "Basically FrostWire is a file sharing program. It's the sister program to LimeWire." He said that once FrostWire has been added to the computer, when the user opens it, "it's set to hook to the Gnutella Network where everybody else with these programs, FrostWire, LimeWire, they're on the same network, it will start looking for other computers to connect to." He explained that the file name for child pornography images were "really, really long and very descriptive . . . . because the more descriptions . . . they can get the more hits they'll get when they're searching files. And they want to be specific about what they're getting." He said, "I have been doing this for a long time, you can't mistake the terms that they're using for child pornography for adult pornography. I mean, you just can't mistake it."

Detective Levasseur testified that during his forensic examination, he recovered some of the search terms that the defendant used in Google: "incest porn; jailbait girls; gay young boys porn; virgin porn; gay boys; jailbait porn; teen jailbait porn; caught my daughter giving head; caught my daughter having sex." He said that those search terms when used in Google may or may not return results that contain child pornography but when used in FrostWire or LimeWire would yield "child pornography in your search results." Detective Levasseur testified that before the images would appear on the defendant's computer, the defendant "had to type in a search term that's associated with child pornography, and you had to see your results, and then you have to double click on it, or single click on it, and click on

the download button to download it." His examination revealed that all of the files located in the "save folder" were downloaded between 2:58 p.m. on January 16 and 5:01 a.m. on January 17, 2011. His examination also showed that of the last eight movie files played by the defendant's computer, half depicted child pornography.

By examining the file creation dates and the file modified dates of the child pornography files and comparing them with other "history files" on the computer created at the same time, Detective Levasseur discovered that someone had logged into a HotMail account and an account on a website called Ashley Madison at the same time that files containing child pornography were being downloaded by FrostWire. Detective Levasseur examined the profile picture for the Ashley Madison account and saw a picture of the defendant. The user name for both accounts was "fun soldier zero one." Just before downloading child pornography, someone searched Craig's List in the adult section for "woman for men, and man and woman for man" and just after the downloads, someone searched Google for "jailbait girls." During that same time, the defendant logged into the USAA website, and that data string indicated that the defendant "was conducting financial business on that website." Additionally, around the time of the child pornography downloads, the defendant logged into his accounts on You Tube and Facebook. Detective Levasseur found no evidence that any person other than the defendant had accessed the computer during those times.

Detective Levasseaur prepared a report of his findings and created a compact disc that contained his report and the child pornography images and videos that he found on the defendant's computer. Both the report and the compact disc were admitted into evidence, and each of the 167 images were displayed for the jury. Some of the images "were really small . . . thumbnails that were carved out of unallocated space, that had been deleted. Some of the bigger ones . . . . were live on the . . . shared folder." He explained that the images could not "go to unallocated space until they're live on the system first." The videos located on the defendant's computer were "recognized throughout the law-enforcement community . . . as being children underage."[2] The titles of each of the six videos clearly indicate that they contain images of child pornography, and, in fact, that the children in each video are being subjected to degrading and sometimes violent sexual abuse. Portions of each video were played for the jury.[3]

Detective Levasseur acknowledged that it was possible to unwittingly

---

[2]Again, the explicit titles of the videos are too vulgar to warrant mention in this opinion.

[3]Given the graphic nature of the videos, the trial court determined that only a portion should be shown in open court. The entirety of each video was made available for the jury to view during deliberations.

download chid pornography, explaining,

> [S]ometimes if . . . you're not paying attention and you click on the whole screen full of files and, say, download all at once, which nobody really ever does because it's too slow, . . . if you're searching for adult porn on a file sharing it is possible that child porn files will pop up and can accidently be downloaded.

He clarified, though, that in those cases, only a few child pornography files rather than hundreds would be found on the hard drive because "[y]ou're not going to keep making the same mistake over and over again." He said that in the case of accidental downloads, they are universally deleted quickly and not played in the media player or moved from folder to folder. Additionally, he said that search terms can establish whether a user was looking for adult pornography or child pornography. He stated definitively that the images on the defendant's computer did not come from "pop ups" during his surfing the internet. He explained, "The thing about it is if a pop up occurs I'm going to be able to tell if it was a pop up and that's where it came from, because they're . . . known as redirects. . . . it will show me that it's a redirect, show me the code on it."

During cross-examination, Detective Levasseur admitted that it was possible to download a computer generated image of child pornography, but he stated that in his opinion it was not difficult to tell the difference between the real images and the computer generated images. He acknowledged that he did not personally know any of the people depicted in the images or videos. Detective Levasseur said that there were 10 live images in the save folder on the defendant's laptop, and the rest were in the unallocated space, indicating that they had been deleted. He said that he could not tell whether the images had been downloaded individually or in a mass download. He added that even in a "mass download," "each download is an individual event" and that the selected files "don't come all together." The user account for "Brittany" was created on the same day as the videos were downloaded.

Upon redirect examination, Detective Levasseur clarified that even if the user wished to download several files at the same time, each individual file must be clicked. He said that only those files selected would be downloaded.

At the conclusion of this proof, the State rested. The defendant elected not to testify and chose not to present any proof. Based upon the evidence presented by the State, the jury convicted the defendant as charged. By special verdict form, the jury indicated that its verdict in count one covered "116 images or materials that include a minor engaged in

sexual activity. Exhibits one, two, nine through 120 and videos one and five," that its verdict in count two covered "57 images of materials that include a minor engaged in sexual activity, exhibits 121 through 177," and that its verdicts in the remaining four counts related to videos two, three, four, and six.

The defendant filed a timely but unsuccessful motion for new trial followed by a timely notice of appeal. In this appeal, the defendant challenges the denial of his motion to suppress, the sufficiency of the evidence for his convictions in counts one and two, the propriety of the multi-count indictment, and the application of three enhancement factors. We consider each claim in turn.

I. Motion to Suppress

The defendant contends that the trial court should have suppressed the evidence seized pursuant to the search warrant obtained by Investigator Cereceres because the warrant was not issued upon the application of the district attorney general as required by Code section 39-17-1007 and because the affidavit in support of the warrant did not contain sufficient facts to establish probable cause to search the defendant's residence. The State asserts that the defendant waived his challenge to the warrant on grounds that it was issued in violation of Code section 39-17-1007 and that the facts articulated by Investigator Cereceres in his affidavit provided probable cause to issue the warrant.

A trial court's factual findings on a motion to suppress are conclusive on appeal unless the evidence preponderates against them. *State v. Binette*, 33 S.W.3d 215, 217 (Tenn. 2000); *State v. Odom*, 928 S.W.2d 18, 23 (Tenn. 1996). Thus, questions of credibility, the weight and value of the evidence, and the resolution of conflicting evidence are matters entrusted to the trial judge, and this court must uphold a trial court's findings of fact unless the evidence in the record preponderates against them. *Odom*, 928 S.W.2d at 23; *see also* Tenn. R. App. P. 13(d). The application of the law to the facts, however, is reviewed de novo on appeal. *State v. Keith*, 978 S.W.2d 861, 864 (Tenn. 1998). We review the issue in the present appeal with these standards in mind.

When the defendant seeks suppression of evidence on the basis of a defective search warrant, he bears the burden of establishing, by a preponderance of the evidence, "the existence of a constitutional or statutory defect in the search warrant or the search conducted pursuant to the warrant." *State v. Henning*, 975 S.W.2d 290, 298 (Tenn. 1998) (citing *State v. Evans*, 815 S.W.2d 503, 505 (Tenn. 1991); *State v. Harmon*, 775 S.W.2d 583, 585-86 (Tenn. 1989)).

A. Code Section 39-17-1007

Code section 39-17-1007 provides, "No process except as otherwise provided shall be issued for the violation of §§ 39-17-1003 -- 39-17-1005 unless it is issued upon the application of the district attorney general of the district." T.C.A. § 39-17-1007. The defendant contends that the term "process" is broad enough to encompass a search warrant and that, as a result, the warrant in this case is invalid because it was not issued upon the application of the district attorney general. Unfortunately for the defendant, he did not present this claim in the trial court and, therefore, the claim is waived. *State v. Johnson*, 970 S.W.2d 500, 508 (Tenn. Crim. App. 1996) ("Issues raised for the first time on appeal are considered waived.").

B. Affidavit

The defendant contends that the affidavit filed by Investigator Cereceres in support of his application for a warrant to search the defendant's residence did not present sufficient facts to support the finding of probable cause.

Both the state and federal constitutions require probable cause as a prerequisite for the issuance of a search warrant. *See* U.S. Const. Amend. IV; Tenn. Const. art. 1, § 7. Probable cause for the issuance of a search warrant exists when, "given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place," which in this instance was the defendant's residence. *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332 (1983). "The sufficiency of a search warrant affidavit is to be determined from the allegations contained in the affidavit alone," *see Henning*, 975 S.W.2d at 297, when read "in a commonsense and practical manner," *see State v. Melson*, 638 S.W.2d 342, 357 (Tenn. 1982), and given their natural meaning and interpretation, *see State v. Smith*, 477 S.W.2d 6, 8 (Tenn. 1972).

In this case, Investigator Cereceres submitted a 27-page affidavit in support of his application for a warrant to search the defendant's residence. In that affidavit, Investigator Cereceres detailed his extensive training and experience in the investigation of internet crimes against children. He then provided a "glossary of terms" to familiarize the magistrate with the terminology used in this area of investigation and to define and explain each of these terms. Included in this glossary were definitions and explanations for the following terms: internet service provider, internet, IP address, Gnutella Network, peer-to-peer file sharing, Limewire, and SHA 1 Hash. Investigator Cereceres explained that peer-to-peer file sharing software "is designed to allow users to trade files through a worldwide network that is formed by linking computers together." He noted that he knew "from training and experience that peer to peer networks are frequently used in the receipt and distribution

of child pornography" and that the "Gnutella" network in particular "is being used to trade digital files, including still image and movie files, of child pornography." He explained the process for searching and downloading files within the peer-to-peer network.

Investigator Cereceres also provided background information on the use of the internet to traffic in child pornography as well as the common behaviors of the users and traffickers of child pornography. He provided significant detail in the area of child pornography trafficking via peer-to-peer file sharing, how such file sharing is routinely monitored by law enforcement personnel, and how child pornography files are identified within the file sharing networks. Investigator Cereceres observed that seizure of all computers and related electronic media is generally necessary to perform a thorough search for child pornography files. He explained that "the search of computers and retrieval of data from computer systems and related media, often require[] agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment."

Turning then to the specifics of this case, Investigator Cereceres stated:

> On 1/9/11, at approximately 05:58 CST, your affiant was using an internet file sharing program and observed a particular internet file sharing user located in Clarksville, TN. Said file sharing user was observed to have the following IP address: 70.156.27.128. The user with IP address 70.156.27.128 was observed to be in possession of files that contained images of minors engaged in sexual activity, in violation of T.C.A. 39-17-1003, Sexual Exploitation of Minor. The aforementioned files are more particularly described in Attachment C.[4]
>
> Your affiant searched the IP database Maxmind, which has been proven reliable by past searches. The Maxmind search resulted in the following information:
>
> IP address 70.156.27.128 is associated with a user located in Clarksville, TN. The internet service provider associated with that particular address is AT&T.
>
> On 1/25/11, your affiant obtained a judicial subpoena

[4]Again, the descriptions of these files, which are inordinately graphic, clearly suggest that they contain child pornography.

> issued by Judge Ray Grimes commanding AT&T to produce any and all records regarding the subscriber, or customer associated with the particularly described IP address 70.156.27.128 and deliver them to your affiant. . . . .

The information obtained from AT&T, which was scanned directly into the affidavit, provided that the IP address was associated with the account of Jared Aguilar at 1611 Bevard Road in Clarksville. The affidavit provided that Investigator Cerceres used "911 CAD" records obtained from the Montgomery County E-911 Center to confirm that Jared Aguilar was a resident of 1611 Bevard Road. Additionally, Investigator Cereceres examined driver's license records "and found that a Jared Aguilar lists his address as 1611 Bevard Rd." He also examined real estate records and learned that 1611 Bevard Road was owned by Jared Aguilar.

Although the defendant contends that the affidavit showed that Investigator Cereceres performed an illegal, warrantless search of the defendant's computer prior to obtaining the warrant, the record belies this statement. According to Investigator Cereceres's affidavit, when users are logged into file sharing software, the files on their computer are available for every other file sharing software user to view. Indeed, open sharing of files is precisely the purpose of the file sharing software. Faced with a nearly identical factual scenario, the Ninth Circuit Court of Appeals, in *United States v. Ganoe*, made the following observations and conclusions:

> Although as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive Ganoe's decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program. The crux of Ganoe's argument is that he simply did not know that others would be able to access files stored on his own computer. But he knew he had file-sharing software on his computer; indeed, he admitted that he used it -- he says to get music. Moreover, he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network. Ganoe thus opened up his download folder to the world, including Agent Rochford. To argue that Ganoe lacked the technical savvy or good sense to configure LimeWire to prevent access to his pornography files is like saying that he did not know enough to close his drapes. Having failed to demonstrate

> an expectation of privacy that society is prepared to accept as reasonable, Ganoe cannot invoke the protections of the Fourth Amendment.

United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008), *cert. denied*, 556 U.S. 1202 (2009) (citations omitted). Like Ganoe, the defendant in this case installed file sharing software and thereby opened his computer to every other person using that same software. As a result, the defendant had no expectation of privacy in the files viewed by Investigator Cereceres using file sharing software. *See Ganoe*, 538 F.3d at 1127; *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009) ("We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking."); *see also United States v. Borowy*, 595 F.3d 1045 (9th Cir. 2010), *cert. denied*, ___ U.S. ___, 131 S. Ct. 795 (2010); *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), *cert. denied*, ___ U.S. ___, 131 S. Ct. 440 (2010).

The defendant also claims that Investigator Cereceres' affidavit failed to establish a nexus between the files observed by Investigator Cereceres and the defendant's residence. Again, the record does not support this argument. Investigator Cereceres' affidavit clearly outlined his extensive training and experience, defined all the relevant terms for the magistrate, and delineated the progress of his investigation from first observation to determination that the images he observed were located on a computer owned by the defendant inside a residence owned and occupied by the defendant. Investigator Cerceres noted that after viewing the files via the file sharing software, he identified the IP address of the computer that contained the files. He stated that he used a widely-accepted database to determine that the computer with that IP address was located in Clarksville. At that point, he applied for, and was granted, a judicial subpoena of the subscriber and owner information for the computer with that IP address. Information obtained from AT&T established that the defendant was the subscriber of the internet service for the computer with the identified IP address and that his residence was located in Clarksville. Investigator Cereceres confirmed that the defendant owned the property and resided at the address listed in the subscriber information provided by AT&T. This information, in our view, provided the magistrate with more than enough information to determine that probable cause existed to believe that the defendant possessed child pornography on his computer and that evidence of that possession could be uncovered in a search of the defendant's residence.

That Investigator Cereceres did not apply for the warrant until 19 days after he first observed the pornographic files on the defendant's computer does not alter our conclusion. Although the defendant did not challenge the warrant on grounds of staleness

in the trial court, he does so on appeal. As the State correctly points out, by failing to present a staleness challenge in the trial court, the defendant has waived our consideration of that issue. That being said, we conclude that the information contained in Investigator Cereceres' affidavit was sufficient to overcome any issue of staleness. A number of courts have observed that computer files containing child pornography, unlike other evidence that can be easily consumed or destroyed, are often hoarded and, even when not hoarded, remain on the user's computer even after deletion. For example, in *United States v. Estey*, the Eighth Circuit Court of Appeals observed,

> While Estey is correct to note there are outer limits to the use of such evidence, this case involves a search warrant issued five months after discovering information linking the defendant's residence with child pornography. This Court, and others, have held that evidence developed within several months of an application for a search warrant for a child pornography collection and related evidence is not stale.

United States v. Estey, 595 F.3d 836, 840 (8th Cir. 2010) (citing *United States v. Horn*, 187 F.3d 781, 786-87 (8th Cir 1999) (holding that warrant not stale three or four months after child pornography information was developed); *United States v. Davis*, 313 Fed. Appx. 672, 674 (4th Cir. 2009) (holding that information a year old is not stale as a matter of law in child pornography cases); *United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000) (holding that warrant not stale for child pornography based on six-month-old information); *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997) (warrant upheld for child pornography based on 10-month-old information). The Tenth Circuit Court of Appeals has explained,

> The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

Perrine, 518 F.3d at 1206 (citing *United States v. Riccardi*, 405 F.3d 852, 861 (10th Cir.

2005); *Hay*, 231 F.3d at 636; *United States v. Harvey*, 2 F.3d 1318, 1322-23 (3d Cir. 1993); *United States v. Koelling*, 992 F.2d 817, 823 (8th Cir. 1993); *United States v. Rabe*, 848 F.2d 994, 997 (9th Cir. 1988)).

Because Investigator Cereceres' affidavit provided sufficient information from which the magistrate could determine that probable cause existed to grant the search warrant, the trial court did not err by denying the defendant's motion to suppress.

II. Sufficiency

The defendant next contends that the evidence was insufficient to support his convictions in counts one and two, claiming that the State failed to establish that he actually possessed the images contained in the unallocated space on his computer. The State contends that the evidence was sufficient to support the convictions.

We review the defendant's challenge to the sufficiency of the evidence mindful that our standard of review is whether, after considering 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. Tenn. R. App. P. 13(e); *Jackson v. Virginia*, 443 U.S. 307, 324 (1979); *State v. Winters*, 137 S.W.3d 641, 654 (Tenn. Crim. App. 2003). "[D]irect and circumstantial evidence should be treated the same when weighing the sufficiency of such evidence." *State v. Dorantes*, 331 S.W.3d 370, 381 (Tenn. 2011).

When examining the sufficiency of the evidence, this court should neither re-weigh the evidence nor substitute its inferences for those drawn by the trier of fact. *Winters*, 137 S.W.3d at 655. Questions concerning the credibility of the witnesses, the weight and value of the evidence, as well as all factual issues raised by the evidence are resolved by the trier of fact. *State v. Cabbage*, 571 S.W.2d 832, 835 (Tenn. 1978). Significantly, this court must afford the State the strongest legitimate view of the evidence contained in the record as well as all reasonable and legitimate inferences which may be drawn from the evidence. *Id.*

Code section 39-17-1003, defining the offense of sexual exploitation of a minor, provides, "It is unlawful for any person to knowingly possess material that includes a minor engaged in . . . [s]exual activity; or [s]imulated sexual activity that is patently offensive." T.C.A. § 39-17-1003(a). "In a prosecution under this section, the state is not required to prove the actual identity or age of the minor." *Id.* § 39-17-1003(e). Code section 39-17-1003(c) provides that

> the trier of fact may consider the title, text, visual representation, Internet history, physical development of the person depicted, expert medical testimony, expert computer forensic testimony, and any other

> relevant evidence, in determining whether a person knowingly possessed the material, or in determining whether the material or image otherwise represents or depicts that a participant is a minor.

Id. § 39-17-1003(c).

In this case, the indictment alleged that the defendant knowingly possessed images containing child pornography between January 1, 2009, and January 31, 2011. The evidence adduced at trial established that Detective Levasseur discovered 167 images and six videos depicting children engaged in sexual activity on the defendant's laptop. He testified that the vast majority of the images were found in the unallocated space on the defendant's computer, indicating that the files had been deleted. He explained, however, that the images "can't go to unallocated space until they're live on the system first." To be "live on the system," the files would have to be manually downloaded by the user. Both Detective Levasseur and Investigator Cereceres testified that although it was theoretically possible to inadvertently download child pornography, the sheer volume of images on the defendant's computer belied an accidental download argument in this case. The defendant's internet search history, as discovered by Detective Levasseur, as well as the defendant's own admitted search inquiries, evinced that he knowingly sought out child pornography. The explicit file names attached to each of the images clearly indicates that the files contain child pornography. That the defendant could not have accessed the files in the unallocated space at the time of Detective Levasseur's examination did not negate the fact that the presence of the files in that space indicated that they had been manually and individually downloaded onto the defendant's computer and that they were, within the time frame provided in the indictment, "live on the system." The evidence sufficiently established that the defendant knowingly possessed each of the images admitted into evidence.

The defendant also complains that the evidence was insufficient because the image in exhibit 20 "is indistinguishable," and, as such, the State failed to establish that the image depicted a minor engaged in sexual activity. Even if we excised that image from the proof, however, the State still presented sufficient proof that the defendant possessed more than 100 images of child pornography in count one.

The defendant contends that the evidence failed to establish that some of the images, and specifically that exhibit 142 in particular, depicted actual minors. Seizing on Detective Levasseur's admission that computer generated images that appear to be child pornography but do not contain actual minors exist, the defendant contends that the State failed to meet its burden. This argument completely ignores the vast majority of the proof introduced by the State. The search terms utilized by the defendant along with the extraordinarily descriptive and explicit titles of the files strongly suggest that the files contain

actual minors engaged in sexual activity. *See* T.C.A. § 39-17-1003(c) (permitting the trier of fact to infer from the title, text, and internet history that an image depicts an actual minor). Furthermore, although Detective Levasseur admitted that computer generated images existed, he testified that they are easily distinguishable from actual child pornography. Finally, and perhaps most importantly, the jury viewed each image and video, many if not most of which depict very young children, first hand and rationally concluded that each depicted an actual minor engaged in sexual activity. The defendant's argument is without merit.

Finally, the defendant argues that the evidence was insufficient to support his convictions because many of the files contained duplicate images. Specifically he notes that 22 of the images that fall within the purview of count one and 15 of the images that fall within the purview of count two are duplicate images. He argues that because the "statute punishes possession of images not computer files," he cannot be convicted under separate counts for possessing the same image more than once "even if it is contained in separate computer files."

The defendant's characterization of Code section 39-17-1003 is not entirely accurate. As indicated, that statute prohibits the possession of "material that includes a minor engaged in . . . [s]exual activity; or . . . [s]imulated sexual activity that is patently offensive." T.C.A. § 39-17-1003(a). "A person possessing material that violates subsection (a) may be charged in a separate count for each individual image, picture, drawing, photograph, motion picture film, videocassette tape, or other pictorial representation. . . ." *Id.* § 39-17-1003(b). Code section 39-17-1002 provides:

> "Material" means:
>
> (A) Any picture, drawing, photograph, undeveloped film or film negative, motion picture film, videocassette tape or other pictorial representation;
>
> (B) Any statue, figure, theatrical production or electrical reproduction;
>
> (C) Any image stored on a computer hard drive, a computer disk of any type, or any other medium designed to store information for later retrieval; or
>
> (D) Any image transmitted to a computer or other electronic media or video screen, by telephone line, cable, satellite transmission, or other method that is capable of further

> transmission, manipulation, storage or accessing, even if not stored or saved at the time of transmission[.]

Id. § 39-17-1002(2). The statute does not define the term "image" as it is used in subsections (C) and (D). The defendant does not urge that a specific definition be given to the term, but he appears to equate "image" with pictorial representation. To evaluate this issue, we are guided by some well-settled principles of statutory construction.

The most basic principle of statutory construction is "'to ascertain and give effect to the legislative intent without unduly restricting or expanding a statute's coverage beyond its intended scope.'" *Houghton v. Aramark Educ. Res., Inc.*, 90 S.W.3d 676, 678 (Tenn. 2002) (quoting *Owens v. State*, 908 S.W.2d 923, 926 (Tenn. 1995)). "Legislative intent is determined 'from the natural and ordinary meaning of the statutory language within the context of the entire statute without any forced or subtle construction that would extend or limit the statute's meaning.'" *Osborn v. Marr*, 127 S.W.3d 737, 740 (Tenn. 2004) (quoting *State v. Flemming*, 19 S.W.3d 195, 197 (Tenn. 2000)). "When the statutory language is clear and unambiguous, we apply the plain language in its normal and accepted use." *Boarman v. Jaynes*, 109 S.W.3d 286, 291 (Tenn. 2003) (citing *State v. Nelson*, 23 S.W.3d 270, 271 (Tenn. 2000)). "It is only when a statute is ambiguous that we may reference the broader statutory scheme, the history of the legislation, or other sources." *In re Estate of Davis*, 308 S.W.3d 832, 837 (Tenn. 2010) (citing *Parks v. Tenn. Mun. League Risk Mgmt. Pool*, 974 S.W.2d 677, 679 (Tenn. 1998)). "Further, the language of a statute cannot be considered in a vacuum, but 'should be construed, if practicable, so that its component parts are consistent and reasonable.'" *In re Estate of Tanner*, 295 S.W.3d 610, 614 (Tenn. 2009) (quoting *Marsh v. Henderson*, 424 S.W.2d 193, 196 (Tenn. 1968)). This court must also "presume that . . . the General Assembly 'did not intend an absurdity.'" *Lee Med., Inc.*, 312 S.W.3d at 527 (quoting *Fletcher v. State*, 951 S.W.2d 378, 382 (Tenn. 1997)).

The title of the act indicates that its purpose is to protect children from the ravages of sexual exploitation via child pornography. *See* T.C.A. § 39-17-1001 ("This part shall be known and may be cited as the 'Tennessee Protection of Children Against Sexual Exploitation Act of 1990.'"). The Sentencing Commission comments to Code section 39-17-1001 inform us that "[t]his part punishes persons involved in child pornography." *Id.*, Sentencing Comm'n Comments. Code section 39-17-1003(b) provides that the State may institute a separate charge for "each individual image, picture, drawing, photograph, motion picture film, videocassette tape, or other pictorial representation." *Id.* § 39-17-1003(b). Nothing in the statute requires that each image be unique or original to be counted. Given that the purpose of the statute is to punish and prevent the possession of child pornography, it is our view that the legislature intended that every image, whether duplicate or not, be

subject to a separate charge or subject to counting for purposes of aggregating the number of images for sentence enhancement.

The three federal circuit courts of appeal to address a similarly operating federal sentencing guideline would agree.[5] In *United States v. Price*, the Fourth Circuit Court of Appeals, rejected the "uniqueness requirement" urged by Price and held "that any image without regard to its originality should be counted when applying this enhancement so long as that image depicts child pornography and is relevant to the underlying conviction." *United States v. Price*, 711 F.3d 455, 459 (4th Cir. 2013). Similarly, the Sixth Circuit Court of Appeals has held "that duplicate visual depictions, digital or otherwise, should each be counted separately for purposes of this enhancement," *United States v. McNerney*, 636 F.3d 772, 779 (6th Cir. 2011), and the Eighth Circuit Court of Appeals has ruled that each image "is to be counted under § 2G2.2(b)(7), regardless of whether or not it is a duplicate," *United States v. Sampson*, 606 F.3d 505, 510 (8th Cir. 2010). In *Sampson*, the court, discussing the unique and "'viral' nature of digital forms of child pornography," observed,

> "In contrast to wheat or marijuana, the supply of electronic images of child pornography has a viral character: every time one user downloads an image, he simultaneously produces a duplicate version of that image. Transfers of wheat or marijuana merely subdivide an existing cache; transfers of digital pornography, on the other hand, multiply the existing supply of the commodity, so that even if the initial possessor's holdings are destroyed, subsequent possessors may further propagate the images. This means that each new possessor increases the available supply of pornographic images."

Sampson, 606 F.3d at 510 (quoting *United States v. Sullivan*, 451 F.3d 884, 891 (D.C. Cir. 2006)). The *Sampson* court noted that "[t]he distribution of duplicate images increases the

---

[5]The guideline in question provides the following sentence enhancements for a conviction of trafficking in child pornography:

> If the offense involved--
> (A) at least 10 images, but fewer than 150, increase by 2 levels;
> (B) at least 150 images, but fewer than 300, increase by 3 levels;
> (C) at least 300 images, but fewer than 600, increase by 4 levels; and
> (D) 600 or more images, increase by 5 levels.

18 U.S.C.S. Appx § 2G2.2(b)(7).

supply and availability of child pornography just as the distribution of unique images does. Both types of distribution compound the effect of an original act of sexual exploitation of a child by increasing the quantity and thus the availability of the image." *Id.* In this case, the defendant's obtaining and possessing duplicate images similarly compounded the original act of sexual exploitation perpetrated to obtain the original image.

Turning to the facts of this case, Detective Levasseur testified that each of the image files discovered on the defendant's computer bore a secure hash algorithm that differentiated those files from all other files. Investigator Cereceres explained that the secure hash algorithm operated in the same manner as a fingerprint to identify and distinguish one computer file from another. The evidence clearly established that each of the files required an individual, manual download, evincing a separate act and intent by the defendant. We conclude that this evidence established that even though the depictions within each file may have been visually similar or even the same, they constituted separate images for purposes of Code section 39-17-1003.

III. Multiplicity

The defendant next contends that "[c]ounts 2-6 ought to have been dismissed as they are an unreasonable multiplication of charges in violation of the due process guarantees of both the federal and [s]tate constitutions." Specifically, he claims that Code section 39-17-1003 permits only a single aggregation of images rather than the multiple aggregation used in this case. The State contends that the charges are expressly authorized by Code section 39-17-1003.

Both the federal and state constitutions protect an accused from being "twice put in jeopardy of life or limb" for "the same offence." U.S. Const. Amend. V; Tenn. Const. art. 1, sec. 10. The state and federal provisions, which are quite similar in verbiage, have been given identical interpretations. *See State v. Waterhouse*, 8 Tenn. (1 Mart. & Yer.) 278, 284 (1827) ("[W]e did not feel ourselves warranted in giving [the double jeopardy provision of the state constitution] a construction different from that given to the constitution of the United States, by the tribunal possessing the power, (and of pre-eminent qualifications) to fix the construction of that instrument."). The United States Supreme Court has observed of the double jeopardy clause:

> Our cases have recognized that the Clause embodies two vitally important interests. The first is the 'deeply ingrained' principle that 'the State with all its resources and power should not be allowed to make repeated attempts to convict an individual for an alleged offense, thereby subjecting him to embarrassment,

> expense and ordeal and compelling him to live in a continuing state of anxiety and insecurity, as well as enhancing the possibility that even though innocent he may be found guilty.' The second interest is the preservation of 'the finality of judgments.'

Yeager v. United States, — U.S. —, 129 S. Ct. 2360, 2365-66 (2009) (citations omitted). To these ends, our state supreme court has "noted many times, three fundamental principles underlie double jeopardy: (1) protection against a second prosecution after an acquittal; (2) protection against a second prosecution after conviction; and (3) protection against multiple punishments for the same offense." *State v. Denton*, 938 S.W.2d 373, 378 (Tenn. 1996), *overruled on other grounds by State v. Watkins*, 362 S.W.3d 530, 533 (Tenn. 2012), (citing *Whalen v. United States*, 445 U.S. 684, 688 (1980); *United States v. Wilson*, 420 U.S. 332, 343 (1975); *North Carolina v. Pearce*, 395 U.S. 711, 717 (1969)). "Multiplicity concerns the division of conduct into discrete offenses, creating several offenses out of a single offense." *State v. Phillips*, 924 S.W.2d 662, 665 (Tenn. 1996).

Of primary importance when considering a claim of multiplicity is legislative intent regarding cumulative punishment. *Watkins*, 362 S.W.3d at 542 ("Legislative intent with respect to punishment remains the focus of the analysis when a defendant in a single prosecution relies upon the Double Jeopardy Clause's protection against multiple punishments."). Noting that "[t]he Double Jeopardy Clause does not limit the legislative authority to define criminal offenses and to prescribe punishments," the supreme court observed that "in single prosecution cases, the double jeopardy prohibition against multiple punishments functions to prevent prosecutors and courts from exceeding the punishment legislatively authorized." *Id.* (citation omitted). Our supreme court has observed that the legislature sets the unit of prosecution and, in doing so, establishes "the minimum unit of conduct that may be prosecuted as a separate offense." *Id.* at 554. Accordingly, we must first "determine 'what the legislature intended to be a single unit of conduct for purposes of a single conviction and punishment.'" *Id.* at 543.

Citing *State v. Pickett*, the defendant asserts that the State unfairly aggregated the images in this case "in order to exponentially increase the potential punishment." In *Pickett*, our supreme court deemed 10 of the 11 images possessed by Pickett multiplicitous because the State did not "distinguish the offenses by showing that the crimes were separated by time or location or by otherwise demonstrating that Pickett formed a new intent as to each image" or establish "that our legislature intended cumulative punishment." *State v. Pickett*, 211 S.W.3d 696, 706 (Tenn. 2007). Importantly, *Pickett* involved interpretation of a former version of Code section 39-17-1003. In 2005, the legislature amended Code section 39-17-1003 by adding the following provision, "Where the number of materials possessed is greater

than fifty (50), the person may be charged in a single count to enhance the class of offense under subsection (d)." T.C.A. § 39-17-1003(b). Noting this change in the law, other panels of this court have determined that multiple aggregation of offenses as was done in this case is permissible under Code section 39-17-1003. *See State v. David Wayne Phillips*, No. M2011-01920-CCA-R3-CD, slip op. at 9 (Tenn. Crim. App., Nashville, July 13, 2012) ("[W]e conclude that section 39-17-1003 allows charges to be brought by the State in the manner utilized in this case. The Defendant's convictions are not multiplicitous."); *State v. Walter Jude Dec*, No. M2009-01141-CCA-R3-CD, slip op. at 8 (Tenn. Crim. App., Nashville, July 30, 2010) ("Under the plain language of Tennessee Code Annotated section 39-17-1003(b), the State has discretion as to whether each image results in a separate count of an indictment or whether a number of images are grouped into a single count. Thus, the manner in which the defendant was indicted was permitted by the statute. Accordingly, we conclude that the counts of the presentment are not multiplicitous . . . ."). We see no reason to depart from the holdings in *David Wayne Phillips* or *Walter Jude Dec*. Consequently, because the defendant's convictions in this case are permitted by the terms of Code section 39-17-1003, they are not multiplicitous.

IV. Sentencing

Finally, the defendant asserts that the trial court abused its discretion in imposing the 10-year effective sentence by misapplying three enhancement factors. He argues that the effective sentence should be modified to a term less than 10 years. The State contends that trial court did not misapply the enhancement factors and that, even if it had, the misapplication would not warrant modification of the defendant's sentence.

"[A]lthough the statutory language continues to describe appellate review as de novo with a presumption of correctness," the 2005 revisions to the Sentencing Act "effectively abrogated the de novo standard of appellate review." *State v. Bise*, 380 S.W.3d 682, 707 (Tenn. 2012). Observing that a change in our standard of review was necessary to comport with the holdings of the United States Supreme Court, our supreme court "adopt[ed] an abuse of discretion standard of review, granting a presumption of reasonableness to within-range sentencing decisions that reflect a proper application of the purposes and principles of our Sentencing Act." *Id.*

Despite the new standard of review, trial courts must still consider the principles of sentencing enumerated in Code section 40-35-210(b), *see Bise*, 380 S.W.3d at 698 n.33 (citing T.C.A. § 40-35-210(b)), 706 n.41, and must, as required by statute, the consider "[t]he potential or lack of potential for the rehabilitation or treatment of the defendant . . . in determining the sentence alternative or length of a term to be imposed." *Id.* § 40-35-103(5). The court cautioned that, despite the wide discretion afforded the trial court

under the revised Sentencing Act, trial courts are "still required under the 2005 amendments to 'place on the record, either orally or in writing, what enhancement or mitigating factors were considered, if any, as well as the reasons for the sentence, in order to ensure fair and consistent sentencing.'" *Bise* at 706 n.41 (citing T.C.A. § 40-35-210(e)).

Here, the trial court applied enhancement factors (3), that the offense involved more than one victim; (4) that a victim of the offense was particularly vulnerable because of age; and (7) that the offense was committed to gratify the defendant's desire for pleasure or excitement. *See* T.C.A. § 40-35-114(3), (4), (7). The court determined that factor three was entitled to the greatest weight, observing, "The videos are just beyond description. Those persons were certainly being victimized physically." The court concluded that factors (4) and (7) were entitled to less weight. In mitigation, the trial court noted the defendant's service in the Army and his efforts at rehabilitation while on bond pending trial. The court then imposed a 10-year sentence for the defendant's conviction in count one, a four-year sentence for the conviction in count two, and three-year sentences for each of the remaining convictions. Noting that the State had not established a sustained intent to violate the law, that the defendant had no criminal history, and that the 10-year sentence in count one had a 100 percent service requirement, the trial court ordered that all of the sentences be served concurrently.

In our view, the trial court did not misapply any of the enhancement factors. As the trial court noted, many of the images and videos included more than one child, and the videos in particular depicted the egregious sexual assault of more than one child. Additionally, as the trial court correctly noted, many of the children depicted in the more than 160 images discovered on the defendant's computer were very young. Finally, the defendant's search history, as discovered by Detective Levasseur, evinced the defendant's intent to satisfy his desire for pleasure or excitement. The record more than justified the 10-year sentence.

Conclusion

The trial court did not err by denying the defendant's motion to suppress evidence seized pursuant to the search warrant in this case. The evidence was sufficient to support each of the defendant's convictions, and none of the convictions was multiplicitous. The 10-year sentence was warranted under the circumstances of this case. Accordingly, the judgments of the trial court are affirmed.

_____

JAMES CURWOOD WITT, JR., JUDGE