IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

JARED SCOTT AGUILAR #508542,	)	
	)	
Petitioner,	)	
	)	**No. 3:16-cv-00779**
v.	)	
	)	**Senior Judge Nixon**
MIKE PARRIS,	)	
	)	
Respondent.	)	

MEMORANDUM

Petitioner Jared Scott Aguilar, a state prisoner serving an effective sentence of ten years for six counts of sexual exploitation of a minor, has filed a *pro se* petition under 28 U.S.C. § 2254 for the writ of habeas corpus. (ECF No. 1.) Respondent has filed an answer, along with a copy of portions of the state court record (ECF Nos. 26, 27), and Petitioner has filed a reply. (ECF No. 28.) For the reasons set forth below, the petition will be denied, and this action will be dismissed.

I. BACKGROUND AND PROCEDURAL HISTORY

On July 17, 2012, a Montgomery County jury found Petitioner guilty of six counts of sexual exploitation of a minor. (ECF No. 26-4, at 159–60.) The trial court entered judgment on August 30, 2012, imposing an effective ten year sentence to be served at 100%. (ECF No. 26-1, at 53–58.) Petitioner filed a motion for new trial, which was denied on November 13, 2012. (ECF No. 26-1, at 59–61.) Petitioner took a direct appeal, in which he asserted four claims for relief: trial court error in denying a motion to suppress evidence based on allegedly unconstitutional search and seizure; insufficient evidence to support convictions on Counts 1 and 2; unreasonable multiplication of charges in Counts 2–6; and abuse of discretion in application of sentence enhancement factors. (ECF No. 26-10.) The Tennessee Court of Criminal Appeals (TCCA) affirmed, and the Tennessee Supreme Court denied permission to

appeal. *State v. Aguilar*, 437 S.W.3d 889, 893 (Tenn. Ct. Crim. App. 2013), *app. denied* (Tenn. May 16, 2014) (ECF No. 26-12, 26-15, at 33).[1]

On September 19, 2014, Petitioner filed a *pro se* petition for post-conviction relief, which was followed by the appointment of counsel and the filing of an amended petition and an answer. (ECF No. 26-15, at 1–31, 46.) The post-conviction court held a hearing on February 12, 2015 (ECF No. 26-16), and entered an order denying relief on March 2, 2015. (ECF No. 26-15, at 47-49.) Petitioner again appealed, asserting ineffective assistance of counsel at trial. (ECF No. 26-20.) The TCCA affirmed the denial of relief, and the Tennessee Supreme Court denied permission to appeal on March 24, 2016. *Aguilar v. State*, No. M201500430CCAR3PC, 2015 WL 9581558 (Tenn. Ct. Crim. App. Dec. 30, 2015), *app. denied* (Tenn. Mar. 24, 2016) (ECF Nos. 26-23, 26-25).

Petitioner filed his *pro se* habeas corpus petition in this Court on April 25, 2016, and Respondent does not dispute that it was timely. (ECF Nos. 1, 27, at 2.) Respondent filed an answer to the petition on July 22, 2016, and has filed portions of the state court record. (ECF Nos. 26, 27.) Petitioner filed his reply on August 1, 2016. (ECF No. 28.)

II. STATEMENT OF FACTS

The TCCA summarized the facts of the case as follows:

> 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

[1] The Court notes that the document represented to be the order of denial in the record filed by Respondent actually pertains to Petitioner's later post-conviction proceedings, rather than his direct appeal. (See ECF Nos. 26, 26-14.) However, the direct appeal denial happens to be in the trial court's technical record in Petitioner's post-conviction action. (See ECF No. 26-15, at 33.)

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. FN1

> FN1 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.

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." 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.” FN2

> FN2 Again, the explicit titles of the videos are too vulgar to warrant mention in this opinion.

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. FN3

> FN3 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.

Detective Levasseur acknowledged that it was possible to unwittingly 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.

State v. Aguilar, 437 S.W.3d 889, 893–98 (Tenn. Ct. Crim. App. 2013).

IV. ISSUES PRESENTED FOR REVIEW

Petitioner raises three claims in his habeas petition:

1. The conviction was obtained by use of evidence gained pursuant to an unconstitutional search and seizure. (ECF No. 1, at 4, 7–13.)

2. Trial counsel was ineffective. (ECF No. 1, at 4, 14–15.)

3. There is insufficient evidence to support the convictions. (ECF No. 1, at 5, 16–17.)

V. STANDARD OF REVIEW

A. AEDPA Review on the Merits

The statutory authority of federal courts to issue habeas corpus relief for persons in state custody is provided by 28 U.S.C. § 2254, as amended by the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA"). A federal court may grant habeas relief to a state prisoner "only on the ground that he is in custody in violation of the Constitution or laws or treaties of the United States." 28 U.S .C. § 2254(a). Upon finding a constitutional error on habeas corpus review, a federal court may only grant relief if it finds that the error "had substantial and injurious effect or influence in determining the jury's verdict." *Brecht v. Abrahamson*, 507 U.S. 619, 637 (1993); *Peterson v. Warren*, 311 F. App'x 798, 803–04 (6th Cir. 2009).

AEDPA was enacted "to reduce delays in the execution of state and federal criminal sentences, particularly in capital cases . . . and 'to further the principles of comity, finality, and federalism.'" *Woodford*, 538 U.S. at 206 (quoting *Williams v. Taylor*, 529 U.S. 362, 436 (2000)). The requirements of AEDPA "create an independent, high standard to be met before a federal court may issue a writ of habeas corpus to set aside state-court rulings." *Uttecht v. Brown*, 551 U.S. 1, 10 (2007) (citations omitted). As the Supreme Court has explained, AEDPA's requirements reflect "the view that habeas corpus is a 'guard against extreme malfunctions in the state criminal justice systems,' not a substitute for ordinary error correction through appeal." *Harrington v. Richter*, 562 U.S. 86, 102–03 (2011) (quoting *Jackson v. Virginia*, 443 U.S. 307, 332 n.5 (1979)). Where state courts have ruled on a claim, AEDPA imposes "a substantially higher threshold" for obtaining relief than a de novo review of whether the state court's determination was incorrect. *Schriro v. Landrigan*, 550 U.S. 465, 473 (2007) (citing *Williams v. Taylor*, 529 U.S. 362, 410 (2000)).

Specifically, a federal court may not grant habeas relief on a claim rejected on the merits in state court unless the state decision was "contrary to, or involved an unreasonable application

of, clearly established Federal law, as determined by the Supreme Court of the United States," or "was based on an unreasonable determination of the facts in light of the evidence presented in the State court proceeding." 28 U.S.C. § 2254(d)(1) and (d)(2). A state court's legal decision is "contrary to" clearly established federal law under § 2254(d)(1) "if the state court arrives at a conclusion opposite to that reached by [the Supreme] Court on a question of law or if the state court decides a case differently than [the Supreme] Court has on a set of materially indistinguishable facts." *Williams v. Taylor*, 529 U.S. 362, 412–13 (2000). An "unreasonable application" occurs when "the state court identifies the correct legal principle from [the Supreme] Court's decisions but unreasonably applies that principle to the facts of the prisoner's case." *Id.* at 413. A state court decision is not unreasonable under this standard simply because the federal court concludes that the decision is erroneous or incorrect. *Id.* at 411. Rather, the federal court must determine that the state court's decision applies federal law in an objectively unreasonable manner. *Id.* at 410–12.

Similarly, a district court on habeas review may not find a state court factual determination to be unreasonable under § 2254(d)(2) simply because it disagrees with the determination; rather, the determination must be "'objectively unreasonable' in light of the evidence presented in the state court proceedings.'" *Young v. Hofbauer*, 52 F. App'x 234, 236 (6th Cir. 2002). "A state court decision involves 'an unreasonable determination of the facts in light of the evidence presented in the State court proceeding' only if it is shown that the state court's presumptively correct factual findings are rebutted by 'clear and convincing evidence' and do not have support in the record." *Matthews v. Ishee*, 486 F.3d 883, 889 (6th Cir. 2007) (quoting § 2254(d)(2) and (e)(1)); *but see McMullan v. Booker*, 761 F.3d 662, 670 and n.3 (6th Cir. 2014) (observing that the Supreme Court has not clarified the relationship between (d)(2) and (e)(1) and the panel did not read *Matthews* to take a clear position on a circuit split about whether clear and convincing rebutting evidence is required for a petitioner to survive (d)(2)).

Moreover, under § 2254(d)(2), "it is not enough for the petitioner to show some unreasonable determination of fact; rather, the petitioner must show that the resulting state court decision was 'based on' that unreasonable determination." *Rice v. White*, 660 F.3d 242, 250 (6th Cir. 2011).

Thus the standard set forth in 28 U.S.C. § 2254(d) for granting relief on a claim rejected on the merits by a state court "is a 'difficult to meet' and 'highly deferential standard for evaluating state-court rulings, which demands that state-court decisions be given the benefit of the doubt.'" *Cullen v. Pinholster*, 563 U.S. 170, 181 (2011) (quoting *Harrington*, 562 U.S. at 102, and *Woodford v. Visciotti*, 537 U.S. 19, 24 (2002) (per curiam)). The petitioner carries the burden of proof. *Pinholster*, 563 U.S. at 181.

By its express terms, Section 2254(d)'s constrained standard of review only applies to claims that were "adjudicated on the merits" in the state court proceeding, including instances where the state court rules against the petitioner in a summary opinion that rejects all claims without discussion, or an opinion that addresses some claims but does not expressly address all the federal claims presented. *Johnson v. Williams*, 133 S. Ct. 1088, 1096 (2013); *Harrington v. Richter*, 562 U.S. at 98–99; *Clinkscale v. Carter*, 375 F.3d 430, 436 (6th Cir. 2004). Where a claim has not been adjudicated on the merits in state court but is still subject to federal review despite the bars of exhaustion and default, "federal habeas review is not subject to the deferential standard that applies under AEDPA. . . . Instead, the claim is reviewed *de novo*." *Moritz v. Lafler*, 525 F. App'x 277, 282 (6th Cir. 2013) (quoting *Cone v. Bell*, 556 U.S. 449, 472 (2009)); *accord Bies v. Sheldon*, 775 F.3d 386, 395–96 (6th Cir. 2014) ("Because Bies' *Brady* claim was never 'adjudicated on the merits in State court proceedings,' the limitations imposed by § 2254(d) do not apply, and we review the claim de novo.").

B. Exhaustion and Procedural Default

1. Exhaustion

28 U.S.C. §§ 2254(b) and (c) provide that a federal court may not grant a writ of habeas

corpus on behalf of a state prisoner unless, with certain exceptions, the prisoner has presented the same claim sought to be redressed in a federal habeas court to the state courts. *Cullen v. Pinholster*, 563 U.S. at 182. The petitioner must "fairly present"[2] each claim at all levels of state court review, up to and including the state's highest court on discretionary review, *Baldwin v. Reese*, 541 U.S. 27, 29 (2004), except where the state has explicitly disavowed state supreme court review as an available state remedy. *O'Sullivan v. Boerckel*, 526 U.S. 838, 847–48 (1999). Tennessee Supreme Court Rule 39 eliminated the need to seek review in that court in order to "be deemed to have exhausted all available state remedies." *Adams v. Holland*, 330 F.3d 398, 402 (6th Cir. 2003), *cert. denied*, 541 U.S. 956 (2004); *see also Smith v. Morgan*, 371 F. App'x 575, 579 (6th Cir. 2010) ("*Adams* not only requires the federal courts to ensure that the state courts have the first opportunity to review and evaluate legal claims ... but also mandates that the federal courts respect the duly-promulgated rule of the Tennessee Supreme Court that recognizes the law and policy-making function of that court and the court's desire not to be entangled in the business of simple error correction").

This rule has been interpreted by the Supreme Court as one of total exhaustion. *Rose v. Lundy*, 455 U.S. 509 (1982). Thus, each and every claim set forth in the federal habeas corpus petition must have been presented to the state appellate court. *Picard v. Connor*, 404 U.S. 270 (1971); *see also Pillette v. Foltz*, 824 F.2d 494, 496 (6th Cir. 1987) (exhaustion "generally entails fairly presenting the legal and factual substance of every claim to all levels of state court review"). Moreover, the substance of the claim must have been presented as a federal constitutional claim. *Gray v. Netherland*, 518 U.S. 152, 162–63 (1996). Fair presentation requires that the state courts be given the opportunity to see both the factual and legal basis for each claim. *Wagner v. Smith*, 581 F.3d 410, 414 (6th Cir. 2009). For the claim to be exhausted,

[2] For a claim to be exhausted, "[i]t is not enough that all the facts necessary to support the federal claim were before the state courts or that a somewhat similar state-law claim was made." *Anderson v. Harless*, 459 U.S. 4, 6 (1982) (per curiam) (internal citation omitted). Nor is it enough to make a general appeal to a broad constitutional guarantee. *Gray v. Netherland*, 518 U.S. 152, 163 (1996).

it must be presented to the state courts as a federal constitutional issue, not merely as an issue arising under state law. *Koontz v. Glossa*, 731 F.2d 365, 369 (6th Cir. 1984). Specifically, in determining whether a petitioner "fairly presented" a federal constitutional claim to the state courts, federal courts should consider whether the petitioner: (1) phrased the federal claim in terms of the pertinent constitutional law or in terms sufficiently particular to allege a denial of the specific constitutional right in question; (2) relied upon federal cases employing the constitutional analysis in question; 3) relied upon state cases employing the federal constitutional analysis in question; or (4) alleged "facts well within the mainstream of [the pertinent] constitutional law." *Hicks v. Straub*, 377 F.3d 538, 553 (6th Cir. 2004) (quoting *McMeans v. Brigano*, 228 F.3d 674, 681 (6th Cir. 2000)). Moreover, the claim must be presented to the state courts under the same legal theory in which it is later presented in federal court. *Wong v. Money*, 142 F.3d 313, 322 (6th Cir. 1998). It cannot rest on a legal theory that is separate and distinct from the one previously considered and rejected in state court. *Id.* This does not mean that the applicant must recite "chapter and verse" of constitutional law, but the applicant is required to make a specific showing of the alleged claim. *Wagner*, 581 F.3d at 414.

2. Procedural Default

The procedural default doctrine is ancillary to the exhaustion requirement. *See Edwards v. Carpenter*, 529 U.S. 446 (2000) (noting the interplay between the exhaustion rule and the procedural default doctrine). If the state court decides a claim on an independent and adequate state ground, such as a procedural rule prohibiting the state court from reaching the merits of the constitutional claim, a petitioner ordinarily is barred from seeking federal habeas review. *Wainwright v. Sykes*, 433 U.S. 72, 81–82 (1977); *see also Walker v. Martin*, 562 U.S. 307, 315 (2011) ("A federal habeas court will not review a claim rejected by a state court if the decision of the state court rests on a state law ground that is independent of the federal question and

adequate to support the judgment"); *Coleman v. Thompson*, 501 U.S. 722 (1991) (same).[3] If a claim has never been presented to the state courts, but a state court remedy is no longer available (e.g., when an applicable statute of limitations bars a claim), then the claim is technically exhausted, but procedurally barred. *Coleman*, 501 U.S. at 731–32; *see also Hicks v. Straub*, 377 F.3d 538, 551 (6th Cir. 2004) (the procedural default doctrine prevents circumvention of the exhaustion doctrine).

If a claim is procedurally defaulted, "federal habeas review of the claim is barred unless the prisoner can demonstrate cause for the default and actual prejudice as a result of the alleged violation of federal law, or demonstrate that failure to consider the claims will result in fundamental miscarriage of justice." *Coleman*, 501 U.S. at 750. The burden of showing cause and prejudice to excuse defaulted claims is on the habeas petitioner. *Lucas v. O'Dea*, 179 F.3d 412, 418 (6th Cir. 1999) (citing *Coleman*, 501 U.S. at 754).

A petitioner seeking to overcome procedural default must establish prejudice as well as cause. To establish prejudice, a petitioner must demonstrate that the constitutional error "worked to his actual and substantial disadvantage." *Perkins v. LeCureux*, 58 F.3d 214, 219 (6th Cir. 1995) (quoting *United States v. Frady*, 456 U.S. 152, 170 (1982)); *see also Ambrose v. Booker*, 684 F.3d 638, 649 (6th Cir. 2012) (finding that "having shown cause, petitioners must show actual prejudice to excuse their default"). "When a petitioner fails to establish cause to excuse a procedural default, a court does not need to address the issue of prejudice." *Simpson v. Jones*, 238 F.3d 399, 409 (6th Cir. 2000). Likewise, if a petitioner cannot establish prejudice, the question of cause is immaterial.

[3] "The state-law ground may be a substantive rule dispositive of the case, or a procedural barrier to adjudication of the claim on the merits." *Walker*, 562 U.S. at 315. A state rule is an "adequate" procedural ground if it is "firmly established and regularly followed." *Id*. (quoting *Beard v. Kindler*, 558 U.S. 53, 60–61 (2009)). "A discretionary state procedural rule ... can serve as an adequate ground to bar federal habeas review ... even if the appropriate exercise of discretion may permit consideration of a federal claim in some cases but not others." *Id*. at 1128 (quoting *Kindler*, 558 U.S. at 60–61) (internal citations & quotation marks omitted).

Because the cause and prejudice standard is not a perfect safeguard against fundamental miscarriages of justice, the United States Supreme Court has recognized a narrow exception to the cause requirement where a constitutional violation has "probably resulted" in the conviction of one who is "actually innocent" of the substantive offense. *Dretke v. Haley*, 541 U.S. 386, 392 (2004) (citing *Murray*, 477 U.S. at 495–96); *accord Lundgren v. Mitchell*, 440 F.3d 754, 764 (6th Cir. 2006).

VI. ANALYSIS AND DISCUSSION

A. Claim 1

Petitioner claims that the affidavit supporting the warrant to search and seize his computers contained insufficient facts to establish probable cause. He also claims that it conflicted with the evidence established at trial in a way that indicates the affiant misrepresented how he discovered the pornography on Petitioner's computer, and that he actually discovered the pornography through some other – illegal – means.

On direct appeal, the TCCA rejected Petitioner's claim that the affidavit was insufficient to establish probable cause:

> 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 (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. FN4

FN4 Again, the descriptions of these files, which are inordinately graphic, clearly suggest that they contain child pornography.

> 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 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*, 131 S.Ct. 795 (2010); *United States v. Perrine*, 518 F.3d 1196 (10th Cir. 2008), *cert. denied*, 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) [additional citations omitted]). 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) [additional citations omitted]).][4]
>
> 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.

State v. Aguilar, 437 S.W.3d 889, 899–902 (Tenn. Ct. Crim. App. 2013) (ECF No. 26-12, at 10–15.)

Petitioner does not dispute that the state court applied the proper federal standard to this claim. He simply disagrees with its conclusion. Although the affidavit could certainly have contained more details, such as what type of file sharing software Petitioner appeared to be using, the state court reasonably found that it contained sufficient facts to establish probable cause to believe that Petitioner was in possession of child pornography. Those facts include the location and ownership of the IP address that Cereceres discovered through an internet file sharing program to possess several images of minors engaged in sexual activity, and the graphic titles and descriptions of those image files. This Court, like the state court, will not repeat those lurid titles or descriptions, but a review of the investigator's list of them leaves no room for doubt that they depict child pornography. (See ECF No. 1-1, at 27.)

[4] The preceding paragraph does not appear in the version of the TCCA opinion available on Westlaw, being replaced by the notice "[text omitted for publication]." *See Aguilar*, 437 S.W.3d at 902. It does appear in the original version of the opinion available in this Court's record at ECF No. 26-12.

At the hearing on the motion to suppress, Petitioner's counsel argued that the affidavit was so scarce on detail about this particular investigation that it left open the possibility that Cereceres acquired access to Petitioner's files illegally:

> The officer has already been inside the computer he states as the defendant's computer. He does not say that it was with the knowledge and consent of the defendant. He does not say it was using a file sharing program open to the world. He does not say if he hacked his way in. He does not say if he guessed the password. He does not say if he used the penetration of the firewall by the internet port to get through the central processing unit and have access to this hard drive. All he says is I was using a file sharing program.

(ECF No. 26-2, at 22–23.) But this argument overlooks the fact that the statement "your affiant was using an internet file sharing program" was prefaced by several pages of detailed background explanation about peer-to-peer file sharing networks, the whole purpose of which is "to allow users to trade digital files through a worldwide network that is formed by linking computers together," the programs, including "Bearshare, Limewire, Frostwire, Shareaza and Phex," that are used to access those networks, and how users locate and access the desired digital files on other users' computers within the network. (ECF No. 1-1, at 2–13.) The unmistakable import of the affidavit, therefore, is that Cereceres used a file sharing program to discover that Petitioner had child pornography on his computer that was accessible on a peer-to-peer file sharing network. That this assertion was allegedly unsupported by evidence at trial months later is irrelevant to the state court's probable cause analysis at the suppression hearing, which was limited to the "four corners" of the affidavit.[5] *See United States v. Brown*, 828 F.3d 375, 381 (6th Cir. 2016) ("The review of the sufficiency of the evidence supporting probable cause is limited to the information presented in the four corners of the affidavit."); *State v. Alberts*, 354 S.W.3d 320, 323 (Tenn. Ct. Crim. App. 2011) ("Tennessee law is clear that in determining whether or not probable cause supported issuance of a search warrant only the information contained within the four corners of the affidavit may be considered.").

[5] Notably, Petitioner never asserted in state court that affidavit used to obtain a search warrant contained knowingly false statements in violation of *Franks v. Delaware*, 438 U.S. 154 (1978), or that he was entitled to a *Franks* hearing to develop such a claim.

Accordingly, the state court's determination that the warrant was supported by probable cause was not unreasonable, and this claim will be denied on the merits.

Petitioner also claims that the application for the search warrant was invalid because it was signed by an assistant district attorney rather than the district attorney general, as Petitioner claims Tennessee law requires. (ECF No. 1, at 10–13.) But the TCCA refused to consider this claim on direct appeal, finding that Petitioner had waived it by failing to raise it in the trial court. *State v. Aguilar*, 437 S.W.3d 889, 899 (Tenn. Ct. Crim. App. 2013) ("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. Ct. Crim. App. 1996) ('Issues raised for the first time on appeal are considered waived.')"). The Sixth Circuit has repeatedly held that that "Tennessee's waiver rule, T.C.A. § 40–30–206(g), which provides that claims not raised in a prior proceeding are barred, constitutes an adequate and independent state-law rule precluding habeas relief." *Hutchison v. Bell*, 303 F.3d 720, 738 (6th Cir. 2002). Accordingly, this portion of the claim is procedurally defaulted and not subject to review on habeas.

B. Claim 2

Petitioner next claims that his trial counsel was ineffective for failing to retain and present the testimony of a computer expert who "would have been able to better explain the 'share folder' mystery" – i.e., Petitioner's claim that Cereceres must have lied about how he found child pornography on his computer, because Petitioner did not have anything in his Frostwire "share folder." Petitioner claims to have disabled the sharing capability in Frostwire on his computer, and alleges that the fact that forensic examination of his computer found child pornography only in other locations (Frostware "save" folder, unallocated space (deleted files) and system volume information) confirms that he was not sharing files and refutes Cereceres' affidavit and testimony to the contrary. He alleges that counsel had led him to believe that he would have to

pay for an expert with his own funds, and that she blamed his eleventh-hour decision to go to trial for needing to rely solely on the prosecution's expert at trial.

All federal claims of ineffective assistance of counsel are subject to the highly deferential two-prong standard of *Strickland v. Washington*, 466 U.S. 668 (1984), which asks: (1) whether counsel was deficient in representing the defendant; and (2) whether counsel's alleged deficiency prejudiced the defense so as to deprive the defendant of a fair trial. *Id.* at 687. To meet the first prong, a petitioner must establish that his attorney's representation "fell below an objective standard of reasonableness." *Id.* at 688. In assessing counsel's performance, a reviewing court must be highly deferential and avoid the "second-guess[ing of] counsel's assistance . . . , [as] it is all too easy for a court, examining counsel's defense after it has proved unsuccessful, to conclude that a particular act or omission of counsel was unreasonable." *Strickland*, 466 U.S. at 689. The court must determine whether, under the circumstances, counsel's allegedly unreasonable acts or omissions "were outside the wide range of professionally competent assistance." *Id.* at 690. In order to avoid "the distorting effects of hindsight," a reviewing "court must indulge a strong presumption that counsel's conduct falls within the wide range of reasonable professional assistance; that is, the defendant must overcome the presumption that . . . the challenged action 'might be considered sound trial strategy.'" *Id.* at 689 (citation omitted).

The "prejudice" component of the claim "focuses on the question of whether counsel's deficient performance renders the result of the trial unreliable or the proceeding fundamentally unfair." *Lockhart v. Fretwell*, 506 U.S. 364, 372 (1993). Prejudice, under *Strickland*, requires showing that "there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different." *Strickland*, 466 U.S. at 694. "A reasonable probability is a probability sufficient to undermine confidence in the outcome." *Id.* The Supreme Court has further explained the *Strickland* prejudice requirement as follows:

> In assessing prejudice under *Strickland*, the question is not whether a court can be certain counsel's performance had no effect on the outcome or whether it is possible a reasonable doubt might have been established if counsel acted differently. Instead, *Strickland* asks whether it is "reasonably likely" the result would have been different. This does not require a showing that counsel's actions "more likely than not altered the outcome," but the difference between *Strickland*'s prejudice standard and a more-probable-than-not standard is slight and matters "only in the rarest case." The likelihood of a different result must be substantial, not just conceivable.

Harrington v. Richter, 562 U.S. 86, 111–12 (2011) (internal citations omitted). "[A] court need not determine whether counsel's performance was deficient before examining the prejudice suffered by the defendant as a result of the alleged deficiencies. . . . If it is easier to dispose of an ineffectiveness claim on the ground of lack of sufficient prejudice, which we expect will often be so, that course should be followed." *Strickland*, 466 U.S. at 697.

As discussed above, however, federal habeas relief may not be granted on an exhausted claim under 28 U.S.C. § 2254 unless the petitioner shows that the earlier state court's decision "was contrary to" federal law then clearly established in the holdings of the United States Supreme Court, § 2254(d)(1); *Williams v. Taylor*, 529 U.S. 362, 412 (2000); or that it "involved an unreasonable application of" such law, § 2254(d)(1); or that it "was based on an unreasonable determination of the facts" in light of the record before the state court, § 2254(d)(2). Thus, when an exhausted claim of ineffective assistance of counsel is raised in a federal habeas petition, the question to be resolved is not whether the petitioner's counsel was ineffective. Rather, "[t]he pivotal question is whether the state court's application of the *Strickland* standard was unreasonable." *Harrington v. Richter*, 562 U.S. at 101. As the Supreme Court clarified in *Harrington*,

> This is different from asking whether defense counsel's performance fell below *Strickland*'s standard. Were that the inquiry, the analysis would be no different than if, for example, this Court were adjudicating a *Strickland* claim on direct review of a criminal conviction in a United States district court. Under AEDPA, though, it is a necessary premise that the two questions are different. For purposes of § 2254(d)(1), an unreasonable application of federal law is different from an incorrect application of federal law. A state court must be granted a

> deference and latitude that are not in operation when the case involves review under the *Strickland* standard itself.

Id. (internal quotation marks and citation omitted).

Reviewing this claim on appeal from the denial of post-conviction relief, the TCCA identified and discussed the applicable *Strickland* standard and rejected the claim on its merits:

> First, the Petitioner claims that trial counsel was ineffective for deciding not to obtain the services of a computer expert without consulting the Petitioner. The Petitioner appears to argue that he was prejudiced by the combination of "the short time frame between the final decision to go forward with trial and [trial counsel's] *sua sponte* decision to forego any defense expert" (emphasis in original). However, there is no indication that trial counsel made the decision to "forego any expert defense" after the Petitioner informed her that he wanted to proceed to trial. Trial counsel testified that she decided not to obtain a computer expert after she thoroughly discussed the matter with Investigator Cereceres, Mr. Bloodworth, and the Petitioner. Additionally, trial counsel testified that she had interviewed all the witnesses before the March trial date where she announced that the Petitioner would accept a plea and that she was ready for trial when the Petitioner decided to reject the plea. Accordingly, there is no factual basis for the Petitioner's contention that trial counsel decided not to obtain a computer expert only after the Petitioner informed her that he wanted to proceed to trial. The Petitioner has failed to show that the "short timeframe" resulted in prejudice.
>
> Further, the Petitioner cannot establish prejudice by trial counsel's decision not to hire an expert because he failed to present any evidence of what a defense expert would have said if called to testify. This court has long held that "[w]hen a petitioner contends that trial counsel failed to discover, interview, or present witnesses in support of his defense, these witnesses should be presented by the petitioner at the evidentiary hearing." *Black v. State*, 794 S.W.2d 752, 757–58 (Tenn. Crim. App. 1990). The Petitioner cannot establish that he was prejudiced unless he can produce a material witness who "(a) could have been found by reasonable investigation and (b) would have testified favorably in support of his defense if called." *Id.* Neither this court nor the post-conviction court can speculate as to whether an expert witness who supported the Petitioner's theory existed, what such a witness may have said if presented, or how that witness may have responded to a rigorous cross-examination. See id. Accordingly, the Petitioner has failed to establish that he was prejudiced by trial counsel's alleged deficiencies.

Aguilar v. State, No. M201500430CCAR3PC, 2015 WL 9581558, at *10–11 (Tenn. Ct. Crim. App. Dec. 30, 2015), *app. denied* (Mar. 24, 2016).

This conclusion accurately summarizes trial counsel's post-conviction hearing testimony. To elaborate, counsel testified that she interviewed Cereceres for hours about his investigation,

as well as meeting with Detective Levasseur, and that after going through the evidence with them and discussing it with Petitioner, she made the strategic decision that a computer expert would not "offer any benefit." (ECF No. 26-16, at 28.) She did not recall any indication from Petitioner, either before or during trial, that he had disabled Frostwire sharing, and testified unequivocally that she told Petitioner that the state would provide funds for an expert if they chose to use one. (ECF No. 26-16, at 27, 29, 34.) She further testified that her meetings with Cereceres, Levasseur and other witnesses took place prior to a March court appearance in the case, so she did not need additional time to prepare when Petitioner later decided to go to trial. (ECF No. 26-16, at 32.)

Petitioner's post-conviction testimony that his sharing was disabled so there was nothing publicly accessible on his computer (ECF No. 26-16, at 16–17, 55) was contradicted by Cereceres' testimony that Petitioner's computer must have had sharing enabled for the files Cereceres accessed to be shared. (ECF No. 26-16, at 48.) Cereceres expressly denied working with Petitioner's ex-wife to gain access to his computer, because "there wasn't a need to." (ECF No. 26-16, at 49–50.) Petitioner argues that the discovery of illegal images in locations other than a Frostwire "share" folder on his computer after it was seized supports his testimony and proves that he had disabled his sharing function. But as Petitioner himself argued in state court in support of his staleness claim, 22 days passed between Cereceres' investigation and the seizure of Petitioner's computer, and image media is "highly mobile" and "susceptible to not being in one place very long." (ECF No. 26-10, at 26.) Proof at trial established that during those 22 days, Petitioner continued to access the file-sharing network and to control and make changes to his files, including downloading at least six child pornography videos. (ECF No. 26-4, at 91, 115.) The location of files on his computer at the time it was seized is not, therefore, persuasive evidence of the file organization or functionality of the computer on the date of Cereceres' investigation. In the absence of any other evidence

to support his claim, it was not unreasonable for the state court to credit the testimony of counsel and the investigator over the Petitioner's.

The state court's conclusion that Petitioner did not establish that he was prejudiced by counsel's performance with regard to the computer evidence was neither unreasonable nor contrary to federal law. Accordingly, this claim fails on its merits.

C. Claim 3

Finally, Petitioner claims that there was insufficient evidence to prove that he was the person who downloaded the child pornography files, as opposed to his wife. On direct appeal, Petitioner challenged the sufficiency of the evidence on four distinct bases: (1) the state had not proven that Petitioner has "possession" of files that had been deleted and were in unallocated space and inaccessible to him; (2) the state had not proven that one indistinguishable image depicted a minor engaged in sexual activity; (3) the state had not proved that the images were of real people (as opposed to manufactured images) under the age of 18; and (4) the state had not proven that Petitioner possessed the requisite number of images to support two of the counts against him, because many of the files contained duplicates of other images already counted. (ECF No. 26-10, at 28-33.) He did not include on direct appeal any claim that there was insufficient evidence to establish that he was the party responsible for the presence of the images on his computer.

Accordingly, if this claim is exhausted in any form, it is limited to Petitioner's post-conviction claim that trial counsel was ineffective for failing to pursue a theory at trial that Petitioner's "estranged wife had 'set him up.'" (ECF No. 26-20, at 14.) The TCCA rejected that claim:

> Likewise, the Petitioner has failed to show that trial counsel was deficient for failing to cross-examine the State's witnesses about the theory that the Petitioner's ex-wife colluded with police in order to frame the Petitioner. Trial counsel testified that, prior to trial, the Petitioner simply told her that his ex-wife and other people were living in the home and had access to the computer. Trial counsel did not hear the details of his theory that his ex-wife colluded with police

> until the post-conviction hearing. Nevertheless, Investigator Cereceres testified that he did not need to work with the Petitioner's ex-wife in order to conduct his investigation and that he did not recall ever speaking with the Petitioner's ex-wife. Moreover, during trial counsel's cross-examination, Detective Levasseur admitted that the Petitioner's ex-wife could have logged into the computer under the Petitioner's name and that she could have known the Petitioner's passwords to access his email and banking account. Trial counsel was not deficient for failing to ask whether the Petitioner's ex-wife colluded with police to frame the Petitioner. The Petitioner is not entitled to relief.

Aguilar v. State, No. M201500430CCAR3PC, 2015 WL 9581558, at *12 (Tenn. Ct. Crim. App. Dec. 30, 2015), *app. denied* (Mar. 24, 2016).

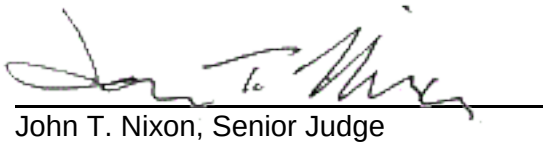
In addition to the trial testimony that the state court accurately recounted above, counsel also elicited testimony at trial from Levasseur that the name of the computer in question was "Jared and Brittany," and that a user profile for Brittany, Petitioner's then-wife, had been created and accessed the same day that some of the videos were downloaded. (ECF No. 26-4, at 118.) But Levasseur also testified that contemporaneous to the download of child pornography files from Frostwire, while logged into the computer under the user profile "Jared," the user also: logged into an email account with the user name "Jared_A_1990"; logged into a messaging account with the name "fun soldier 01"; logged into an Ashley Madison account, also with username "fun soldier 01" and a photo of Petitioner from Petitioner's own picture folder on the computer; ran several searches on the "adult" section of Craig's List; searched Google for "jailbait girls"; logged in and conducted financial business at USAA.com; accessed Petitioner's YouTube account; and accessed Petitioner's Facebook account. (ECF No. 26-3, at 116; ECF No. 26-4, at 95–96.) These undisputed facts constitute sufficient evidence for the jury to conclude that Petitioner was the user who downloaded the child pornography, and Petitioner has not demonstrated what more counsel could have done to rebut them, beyond forcing Levasseur to acknowledge that it was possible that Petitioner's wife knew the passwords to his accounts.

Petitioner has not established that the state court's rejection of this claim was contrary to or an unreasonable application of federal law. The claim will be denied.

VII. CONCLUSION

For the reasons set forth above, the petition for the writ of habeas corpus will be denied, and this case will be dismissed.

An appropriate Order shall enter.



John T. Nixon, Senior Judge
United States District Court