IN THE COURT OF CRIMINAL APPEALS OF TENNESSEE
AT NASHVILLE
Assigned on Briefs November 12, 2015

JARED S. AGUILAR v. STATE OF TENNESSEE

Appeal from the Circuit Court for Montgomery County
No. 41100542 Ross H. Hicks, Judge

No. M2015-00430-CCA-R3-PC – Filed December 30, 2015

Jared S. Aguilar ("the Petitioner") filed a Petition for Post-Conviction Relief alleging ineffective assistance of counsel. After a hearing, the post-conviction court denied relief. On appeal, the Petitioner argues that trial counsel rendered ineffective assistance of counsel when she (1) decided not to obtain the services of an expert witness for the defense without consulting the Petitioner and (2) ignored the Petitioner's specific request that she cross-examine the State's experts "on areas such as the contradicting of computer expert reports vs. the expert's in-court testimony and whether [the Petitioner's] estranged wife had 'set him up.'" Upon review of the record and applicable law, we affirm the judgment of the post-conviction court.

Tenn. R. App. P. 3 Appeal as of Right; Judgment of the Circuit Court Affirmed

ROBERT L. HOLLOWAY, JR., J., delivered the opinion of the Court, in which NORMA MCGEE OGLE and CAMILLE R. MCMULLEN, JJ., joined.

Gregory D. Smith, Clarksville, Tennessee, for the appellant, Jared S. Aguilar.

Herbert H. Slatery III, Attorney General and Reporter; Sophia S. Lee, Senior Counsel; John W. Carney, District Attorney General; and Daniel Brollier, Assistant District Attorney General, for the appellee, State of Tennessee.

OPINION

Trial

On direct appeal, this court summarized the facts presented at trial as follows:

A Montgomery County Circuit Court jury convicted [the Petitioner] 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. 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 Petitioner]. He used the information gleaned during his investigation to obtain a warrant to search [the Petitioner]'s residence and computer.

Investigator Cereceres said that when officers executed the search warrant at [the Petitioner]'s residence on January 31, 2011, [the Petitioner] answered the door and indicated that he was alone. During the search, officers seized two laptop computers, and [the Petitioner] admitted ownership of one of the laptops. Upon questioning, [the Petitioner] 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 Petitioner] 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 Petitioner] 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 Petitioner] had downloaded the files or how many times [the Petitioner] 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 Petitioner]'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 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 laptop, 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, it[']s 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 Petitioner]'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 Petitioner] 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 Petitioner]'s computer, [the Petitioner] "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 Petitioner]'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 Petitioner]. The user name for both accounts was "fun soldier zero one." Just before downloading child pornography, someone searched Craigslist 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 Petitioner] logged into the USAA website, and that data string indicated that [the Petitioner] "was conducting financial business on that website." Additionally, around the time of the child pornography downloads, [the Petitioner] logged into his accounts on You Tube and Facebook. Detective Levasseur found no evidence that any person other than [the Petitioner] had accessed the computer during those times.

Detective Levasseur 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 Petitioner]'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 Petitioner]'s computer were "recognized throughout the law-enforcement community . . . as being children underage." 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.

Detective Levasseur acknowledged that it was possible to unwittingly download child 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 Petitioner]'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 Petitioner]'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 Petitioner] elected not to testify and chose not to present any proof. Based upon the evidence presented by the State, the jury convicted [the Petitioner] as charged.

State v. Aguilar, 437 S.W.3d 889, 893-98 (Tenn. Crim. App. Dec. 18, 2013), perm. app. denied (Tenn. May 16, 2014) (footnotes omitted). This court affirmed the Petitioner's convictions on direct appeal. Id. at 909.

Post-Conviction Proceedings

In his Amended Petition for Post-Conviction Relief ("the Petition"), the Petitioner alleged that trial counsel "failed to fully, completely and adequately advise [the] Petitioner of his rights and options and to use witnesses that were available at the hearing but dismissed without consulting [the] Petitioner first. Further, [trial] counsel did not fully investigate and/or explain the options available prior to his original trial." He also asserted that "major tactical decisions on his case were not presented to [the] Petitioner so

that [the] Petitioner could make an informed and knowing decision on the path that his case should proceed which amounts to the denial of the effective assistance of counsel."

At a hearing on the Petition, the Petitioner testified that he believed trial counsel was ineffective because the Petitioner "didn't have an expert witness for the defense."[1] The Petitioner explained that he had discussed the possibility of an expert witness but trial counsel informed him that "such a witness would cost $125."[2] Trial counsel did not explain that he could receive funds for an expert witness, and the Petitioner stated that he thought that he would have to pay the $125 himself. The Petitioner stated that he had just been discharged from the military and he could not afford to pay for an expert witness. He stated that he was not aware "that the state would pick[ ]up any such costs." The Petitioner stated that, had he known he would not have had to pay for the expert witness, "[i]t would have changed the outcome [of his case] significantly."

To explain why he thought an expert would have been helpful to his case, the Petitioner stated that the "sharing feature" on FrostWire could be disabled if the user does not want others to have access to the user's files. According to the Petitioner, if someone disables the sharing feature, the "share folder is empty." The Petitioner claimed that the sharing feature on his file sharing program was disabled and that was why "they didn't find anything in [the Petitioner's] share folder." Consequently, the Petitioner claimed that Investigator Cereceres "did not do the investigation that he claim[ed] to have done, because he claimed to have downloaded directly from [the Petitioner's] share folder." The Petitioner stated that trial counsel did not cross-examine Investigator Cereceres about the Petitioner's empty share folder. The Petitioner brought this discrepancy to trial counsel's attention after Investigator Cereceres had been excused as a witness, but trial counsel told the Petitioner that Investigator Cereceres would not testify again.

The Petitioner also noted that Detective Levasseur testified that he found items in the Petitioner's share folder, and the Petitioner claimed that such testimony contradicted both Investigator Cereceres' testimony and Detective Levasseur's own report.[3] The Petitioner asked trial counsel to ask Detective Levasseur "if you could access files without it being in the share folder," but trial counsel did not ask the detective that question. The Petitioner asserted that a defense expert witness could have said that there was nothing in the Petitioner's share folder and that "this investigation [was] impossible

[1] It is not clear from this portion of the Petitioner's testimony what type of expert witness he felt should have been called. However, by examining the rest of the Petitioner's testimony and his brief on appeal, it appears the Petitioner believes trial counsel should have retained a computer expert to assist in his defense.

[2] The Petitioner did not know whether the $125 was a flat fee or an hourly rate.

[3] Detective Levasseur's report is not included in the record on this appeal.

because there's nothing in the share folder." The Petitioner admitted that Detective Levasseur contradicted himself, but the Petitioner noted "there's nothing to contradict him directly."

The Petitioner stated that he wanted to present a theory of defense that his now-ex-wife was working with the detective "from day one" in order to get retribution against the Petitioner because he was cheating on her. The Petitioner told trial counsel about this theory, but trial counsel refused to use such a defense.

The Petitioner acknowledged that he did not tell trial counsel that he wanted to proceed to trial, as opposed to taking a plea, until four days before the trial was scheduled to start. The Petitioner said that he did not "really discuss" trial strategy with trial counsel. However, he stated, "I had already come up with what I had thought was a pretty solid defense, and I asked [trial counsel] can we just look at the evidence, and [trial counsel] cut me off and just said 'I'll see you Monday.'" The Petitioner explained that he wanted to highlight that both he and his wife shared the computer, and the Petitioner "was trying to figure out how you can say it's one person and not the other." The Petitioner admitted that he had given a statement to police in which he admitted to downloading pornography off of FrostWire, but he maintained that he did not intentionally download child pornography but "it had come up by accident several times . . . during my downloading."

The Petitioner also noted that, in the fifteen days after his ex-wife's log-in had been created on their shared computer, she had logged in seventy-seven times. The Petitioner believed that an expert witness could also help support the Petitioner's theory of defense because the expert could have looked at the date and time the Petitioner's ex-wife's log-in had been created and calculated that she logged into the computer five times a day. The Petitioner said he thought that evidence was significant because "it shows two people had access to the computer but only one was ever questioned, only one was ever looked at. I mean, my wife, in my—in my opinion, was the embodiment of reasonable doubt."

Trial counsel testified that she discussed the possibility of a computer expert with the Petitioner and informed the Petitioner that they "could try to find an expert to look over everything . . . ." Trial counsel also told the Petitioner that the state would provide funds for an expert. However, no expert was hired for the defense. Trial counsel explained that she spoke with Detective Levasseur and met with Investigator Cereceres at his office for over two hours. Investigator Cereceres showed trial counsel a copy of what they had found on the Petitioner's computer and "walked [trial counsel] through" the evidence from beginning to end. In that meeting, trial counsel was able to see what was found on the computer and how the files were stored and determine if she needed to hire an expert witness. Trial counsel "questioned [Investigator Cereceres] thoroughly on . . .

unallocated space, deleted files, where things were moved from shared files, how they were downloaded from share drives, and [Investigator Cereceres] thoroughly walked [trial counsel] though every part of that as preparation for [trial]." Additionally, trial counsel consulted with Charles Bloodworth, another attorney in her office who was very knowledgeable about computers, about the computer investigation and asked him to help with the hearing on the Petitioner's motion to suppress prior to trial. Mr. Bloodworth litigated the issue about the Petitioner's file sharing capability and whether the State should have been able to get a search warrant based upon the police investigation at the hearing for the motion to suppress.[4]

Based on her conversations with Detective Levasseur, Investigator Cereceres, and Mr. Bloodworth, and after consulting with the Petitioner, trial counsel "didn't think that [a computer expert] would offer any benefit." Trial counsel acknowledged that she made the decision not to hire an expert witness. Trial counsel recalled speaking with the Petitioner about the decision not to hire an expert, but she could not remember the exact conversation she had with the Petitioner. Trial counsel could not remember whether the Petitioner agreed with her conclusion not to hire an expert witness. Trial counsel also could not recall whether she had any discussions with the Petitioner about the Petitioner's share folder being blocked by disabling the file sharing feature.

Trial counsel stated that the trial was scheduled to begin in June or July, but trial counsel announced that the Petitioner was accepting a plea agreement in March. However, trial counsel said she was prepared for trial when the Petitioner decided not to accept the plea on the eve of the scheduled trial date. Trial counsel explained that she did not ask for a continuance because she had already spoken to all of the witnesses involved before the March date and that she had spoken with the Petitioner numerous times, so there was no need for a continuance. Trial counsel stated that she cross-examined both Investigator Cereceres and Detective Levasseur. However, she did not recall having any discussions with the Petitioner about a blocked share file.

On cross-examination, trial counsel explained that she gave the Petitioner a note pad and pencil to write down questions for her during the trial. Trial counsel read the Petitioner's notes and took them into consideration when she cross-examined witnesses. Trial counsel stated that she did not ask every question the Petitioner posed, but she noted that the Petitioner had "a good amount of computer knowledge" and she tried to accommodate his requests with her cross-examination. Additionally, trial counsel stated

[4] In the hearing on the motion to suppress, Mr. Bloodworth argued that the application for the search warrant of the Petitioner's home was insufficient and, consequently, that the warrant should not have been issued. There was no discussion as to whether the Petitioner's file sharing capability was disabled on his computer.

that she cross-examined the witnesses at trial about whether other people in the Petitioner's home could have downloaded the files.

In regard to her decision not to hire an expert witness, trial counsel stated that she scoured the case files and looked for a way to challenge the evidence. However, the evidence showed that the images were downloaded within a twenty-four-hour window, and during that time: the Petitioner was signed into the computer as himself; he signed into an Ashley Madison account using his password; he signed into his email; and he signed into his banking account in order to conduct some financial business.

Trial counsel stated that she had numerous meetings with the Petitioner and that she listened to all of the Petitioner's suggestions for defense theories. Trial counsel also said, "I argued everything at trial from mass downloaded to zip files, to the wife being home[,] to not being home, to the pornography not being recognized individuals. I mean, I think if it was out there I think I threw it out there." Trial counsel did not recall the Petitioner's theory—that his wife had colluded with police in order to frame the Petitioner—being so well-formed prior to trial. Prior to trial, the Petitioner simply told trial counsel that his ex-wife and "other people" lived in the home, and trial counsel stated that she did cross-examine the witnesses about other people being in the house. Trial counsel acknowledged that it would be reasonable to conclude that the Petitioner's wife would have known the passwords to the Petitioner's accounts, and trial counsel stated that she brought out that possibility at trial.

Investigator Cereceres testified that computers using FrostWire could share files with one another via the share folder. Investigator Cereceres acknowledged that even though the program's default setting allowed sharing, the Petitioner could disable the sharing function. Based on Investigator Cereceres' experience, he believed that the Petitioner's sharing function was enabled because "otherwise it wouldn't share at all." Investigator Cereceres explained that, in the course of his investigation, he would search for key words indicating child pornography and the FrostWire software would pull results from all over the world and would give Investigator Cereceres a geographical location of where the image was found. Investigator Cereceres then downloaded the images, and he was able to get the IP address of the computer from where the images were downloaded. After that, Investigator Cereceres was able to subpoena records from the internet carrier in order to get the address where the computer could be located. As such, Investigator Cereceres said that there was no need to work with the Petitioner's wife to get access to the Petitioner's computer. Investigator Cereceres did not recall speaking with the Petitioner's wife about this case. On cross-examination, Investigator Cereceres confirmed that he conducted a search for child pornography and found files that he was able to trace back to the computer that was at the Petitioner's house.

The Petitioner was recalled and responded to Investigator Cereceres' testimony, stating:

> . . . [H]e said it himself that you can't—you can't access someone's files unless it's in a share folder. If it's not in that share folder then you can't access that. And as—as it says, both in the published report by the State's expert witness and also as it states in the record, there was nothing ever found in my share folder; there's no way that he could have done the investigation that he claims to have done if there was nothing in the share folder.

The Petitioner maintained that the sharing function on his computer was disabled.

In the order denying post-conviction relief, the post-conviction court noted that both the Petitioner and trial counsel testified that they had "some discussion or conversation about the possibility of using an expert witness" and that trial counsel decided not to call an expert witness after a thorough discussion with the State's experts and Mr. Bloodworth. The post-conviction court also stated:

> [The Petitioner] insists that had [trial counsel] retained and called an expert to testify, the expert would have refuted the testimony of the State's experts on these issues. However, [the Petitioner] has presented nothing but argument to support his position. He has yet to produce any evidence other than his own testimony to contradict the State's experts. Not only is he unable to show that an expert would say what [the Petitioner] says the expert would say, there is no showing that such an expert even exists.

Additionally, the post-conviction court found that "all of [the issues about the search of the computer and other people accessing the computer] were adequately addressed by [the Petitioner's] counsel at the suppression hearing or during the course of the trial." This timely appeal followed.

Analysis

On appeal, the Petitioner argues that trial counsel rendered ineffective assistance of counsel when she (1) decided not to obtain the services of an expert witness for the defense without consulting the Petitioner; and (2) ignored the Petitioner's specific requests that she cross-examine the State's expert witnesses "on areas such as the contradicting of computer expert reports vs. the expert's in-court testimony and whether [the Petitioner's] estranged wife had 'set him up.'"

In order to prevail on a petition for post-conviction relief, a petitioner must prove all factual allegations by clear and convincing evidence. Jaco v. State, 120 S.W.3d 828, 830 (Tenn. 2003). Post-conviction relief cases often present mixed questions of law and fact. See Fields v. State, 40 S.W.3d 450, 458 (Tenn. 2001). Appellate courts are bound by the post-conviction court's factual findings unless the evidence preponderates against such findings. Kendrick v. State, 454 S.W.3d 450, 457 (Tenn. 2015). When reviewing the post-conviction court's factual findings, this court does not reweigh the evidence or substitute its own inferences for those drawn by the post-conviction court. Id.; Fields, 40 S.W.3d at 456 (citing Henley v. State, 960 S.W.2d 572, 578 (Tenn. 1997)). Additionally, "questions concerning the credibility of the witnesses, the weight and value to be given their testimony, and the factual issues raised by the evidence are to be resolved by the [post-conviction court]." Fields, 40 S.W.3d at 456 (citing Henley, 960 S.W.2d at 579); see also Kendrick, 454 S.W.3d at 457. The trial court's conclusions of law and application of the law to factual findings are reviewed de novo with no presumption of correctness. Kendrick, 454 S.W.3d at 457.

The right to effective assistance of counsel is safeguarded by the Constitutions of both the United States and the State of Tennessee. U.S. Const. amend. VI; Tenn. Const. art. I, § 9. In order to receive post-conviction relief for ineffective assistance of counsel, a petitioner must prove two factors: (1) that counsel's performance was deficient; and (2) that the deficiency prejudiced the defense. Strickland v. Washington, 466 U.S. 668, 687 (1984); see State v. Taylor, 968 S.W.2d 900, 905 (Tenn. Crim. App. 1997) (stating that the same standard for ineffective assistance of counsel applies in both federal and Tennessee cases). Both factors must be proven in order for the court to grant post-conviction relief. Strickland, 466 U.S. at 687; Henley, 960 S.W.2d at 580; Goad v. State, 938 S.W.2d 363, 370 (Tenn. 1996). Accordingly, if we determine that either factor is not satisfied, there is no need to consider the other factor. Finch v. State, 226 S.W.3d 307, 316 (Tenn. 2007) (citing Carpenter v. State, 126 S.W.3d 879, 886 (Tenn. 2004)). Additionally, review of counsel's performance "requires that every effort be made to eliminate the distorting effects of hindsight, to reconstruct the circumstances of counsel's challenged conduct, and to evaluate the conduct from counsel's perspective at the time." Strickland, 466 U.S. at 689; see also Henley, 960 S.W.2d at 579. We will not second-guess a reasonable trial strategy, and we will not grant relief based on a sound, yet ultimately unsuccessful, tactical decision. Granderson v. State, 197 S.W.3d 782, 790 (Tenn. Crim. App. 2006).

As to the first prong of the Strickland analysis, "counsel's performance is effective if the advice given or the services rendered are within the range of competence demanded of attorneys in criminal cases." Henley, 960 S.W.2d at 579 (citing Baxter v. Rose, 523 S.W.2d 930, 936 (Tenn. 1975)); see also Goad, 938 S.W.2d at 369. In order to prove that counsel was deficient, the petitioner must demonstrate "that counsel's acts or omissions

were so serious as to fall below an objective standard of reasonableness under prevailing professional norms." Goad, 938 S.W.2d at 369 (citing Strickland, 466 U.S. at 688); see also Baxter, 523 S.W.2d at 936.

Even if counsel's performance is deficient, the deficiency must have resulted in prejudice to the defense. Goad, 938 S.W.2d at 370. Therefore, under the second prong of the Strickland analysis, the petitioner "must show that there is a reasonable probability that, but for counsel's unprofessional errors, the result of the proceeding would have been different. A reasonable probability is a probability sufficient to undermine confidence in the outcome." Id. (quoting Strickland, 466 U.S. at 694) (internal quotation marks omitted).

Failure to Obtain an Expert Witness

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.

In his reply brief, the Petitioner notes that Tennessee Supreme Court Rule 13 section 5(a)(2) bars state funding for expert witnesses in non-capital post-conviction proceedings and argues that mandating an indigent person to present expert testimony at the post-conviction hearing violates due process. This issue is raised for the first time on appeal. "Issues not raised by the petitioner in the lower court[] cannot be raised for the first time on appeal." Bobby Taylor v. State, No. M2008-00335-CCA-R3-PC, 2009 WL 2047331, at *2 (Tenn. Crim. App. July 14, 2009) (citing Cauthern v. State, 145 S.W.3d 571, 599 (Tenn. Crim. App. 2004)). To the extent that the Petitioner raises a new due process claim, such claim is not properly before this court. To the extent that the Petitioner raises his due process claim to explain why he did not present a witness at the post-conviction hearing to establish prejudice, his arguments are unpersuasive. The Petitioner correctly states that Tennessee Supreme Court Rule 13 section 5(a)(2) bars state funding for an expert witness in this case. However, we are unable to determine whether the Petitioner suffered prejudice from trial counsel's alleged failure to obtain an expert witness without credible testimony of what such an expert could have said. See Black, 794 S.W.2d at 757-58.

Failure to Properly Cross-Examine Witnesses

Second, the Petitioner argues that trial counsel failed to cross-examine the State's witnesses "on areas such as the contradicting of computer expert reports vs. the expert's in-court testimony and whether [the Petitioner's] estranged wife has 'set him up.'" It is unclear whether the Petitioner asserts that the State's witnesses should have been cross-examined with their own reports or with reports from other computer experts. However, the trial transcripts reflect that trial counsel did question Detective Levasseur about his own report on cross-examination. Additionally, we note that no expert reports—from either the State's witnesses or other experts—are included in the record on this appeal. Therefore, we are unable to determine whether the Petitioner was prejudiced by the failure to use any such reports during cross-examination.

The Petitioner also insists that the State's witnesses contradicted each other as to whether the Petitioner's file sharing function was disabled, and he provides citations to the trial transcript which purportedly illustrate the contradictory testimony. However, the Petitioner's citations do not include any discussion about whether the Petitioner's file sharing function was disabled. The Petitioner does not explain how the witnesses' testimony contradicted each other, and we are unable to find any contradictions between

the two testimonies in the citations provided.[5] The Petitioner has failed to prove that trial counsel was deficient in her cross-examination of the State's witnesses about alleged discrepancies in their testimony.

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.

Conclusion

For the aforementioned reasons, the judgment of the post-conviction court is affirmed.

_____

ROBERT L. HOLLOWAY, JR., JUDGE

[5] The Petitioner cites to portions of Investigator Cereceres' testimony wherein he explained that FrostWire utilizes a "save folder" and an "incomplete folder" when downloading files from the file sharing system. Investigator Cereceres noted that he found files in the "unallocated space" on the Petitioner's hard drive that "definitely were downloaded from the [file sharing system]." The Petitioner also cites to a portion of Detective Levasseur's testimony wherein he stated that he found several files in the "unallocated space" of the Petitioner's hard drive and some files in the Petitioner's "share folder." Detective Levasseur explained that the files found in the "unallocated space" had been deleted and were not accessible without forensic equipment but that such files "can't go to unallocated space until they're live on the system first."