

*Vyacheslav Redkovsky v. State of Maryland*, No. 1478, Sept. Term 2017. Opinion filed on February 27, 2019, by Berger, J.

CRIMINAL LAW - SUFFICIENCY OF THE EVIDENCE – § 11-208(a)(4)(i) OF THE CRIMINAL LAW ARTICLE – DISTRIBUTION OF CHILD PORNOGRAPHY

A showing of specific intent is not required to sustain a conviction for distribution of child pornography under § 11-208(a)(4)(i) of the Criminal Law Article. Here, an appellant used a peer-to-peer file-sharing program which made files on his laptop available for others to download. Via this file-sharing program, videos depicting child pornography were transferred from appellant's computer to a law enforcement officer's computer. This evidence was sufficient to sustain appellant's conviction for distribution of child pornography.

Circuit Court for Washington County  
Case No.: 21-K-16-53003

REPORTED  
IN THE COURT OF SPECIAL APPEALS  
OF MARYLAND

No. 1478

September Term, 2017

---

VYACHESLAV REDKOVSKY

v.

STATE OF MARYLAND

---

Meredith,  
Berger,  
Kehoe,

JJ.

---

Opinion by Berger, J.

---

Filed: February 27, 2019

Pursuant to Maryland Uniform Electronic Legal  
Materials Act  
(§§ 10-1601 et seq. of the State Government Article) this document is authentic.



Suzanne C. Johnson, Clerk

A jury in the Circuit Court for Washington County convicted appellant, Vyacheslav Redkovsky, of four counts of distribution of child pornography and four counts of possession of child pornography. As to two of the distribution charges, the trial court sentenced appellant to consecutive ten-year sentences, with all but six years of each sentence suspended, and merged the remaining counts for sentencing purposes. On appeal, appellant challenges the sufficiency of the evidence to sustain his convictions.

We conclude that the evidence was sufficient and affirm the judgments of the trial court.

### **BACKGROUND**

Corporal Roger Schwarb of the Maryland State Police (“MSP”) testified that in February of 2016, he was assigned to the MSP division of the Internet Crimes Against Children Task Force (“Task Force”). In connection with his duties on the Task Force, Corporal Schwarb investigated internet child pornography on BitTorrent, a peer-to-peer file-sharing protocol.<sup>1</sup> BitTorrent allows users to download material, while also sharing material from the users’ files.

Corporal Schwarb explained the basic process for accessing a peer-to-peer network. First, a user must download a “client,” which is a free, publicly-available computer

---

<sup>1</sup> “BitTorrent” is defined as “[a] peer-to-peer file transfer protocol for sharing large amounts of data over the internet, in which each part of a file downloaded by a user is transferred to other users.” <https://en.oxforddictionaries.com/definition/bittorrent> (last visited February 13, 2019). According to Corporal Schwarb, “some businesses use it for document sharing. Some people may have heard of [] Napster back in the day where it was [used to] . . . download music.”

program. uTorrent is a popular client, which allows users to access the BitTorrent network. Corporal Schwarb explained that the client searches for files on the network by using a “torrent,” which is similar to a library “indexing card.”<sup>2</sup> A torrent contains text identifying the files associated with that torrent, including the number of files associated with that torrent, the size of the files and their location. The torrent does not contain any files or images; it only contains data with file descriptions. Each torrent is assigned a “hash,” which is a specific number, similar to an electronic “thumbprint.”<sup>3</sup> Once the user downloads a particular torrent, that torrent is saved in the user’s client.

Corporal Schwarb explained that, for example, a user who is interested in Lassie movies could search for a torrent using the term “Lassie,” and the user will receive a list of torrent files associated with that search term. The BitTorrent client then searches the peer-to-peer network to find the info hashes for files associated with that torrent. If there are “a hundred images of that torrent for Lassie, it will go out, you’ll get those hundred images,” and “[y]ou’ve essentially downloaded all the files associated with that torrent.”

---

<sup>2</sup> See Downloading With BitTorrent, <http://help.utorrent.com/customer/en/portal/articles/178825-downloading-with-bittorrent> (last visited February 13, 2019).

<sup>3</sup> See Downloading With BitTorrent, [http://help.utorrent.com/customer/en/portal/articles/179175-glossary?b\\_id=3883](http://help.utorrent.com/customer/en/portal/articles/179175-glossary?b_id=3883) (defining “Hash” as “[a] ‘fingerprint’ of data assumed to be unique to the data. Because of the assumed uniqueness of the data, it is used to verify that a piece of data is indeed uncorrupted (since the corrupted data’s hash would not match its expected hash)”) (last visited February 13, 2019).

Corporal Schwarb's state computer used a software program specifically designed to allow law enforcement to operate undercover, searching BitTorrent for child pornography files located in Maryland.<sup>4</sup> On February 13, 2016, Corporal Schwarb's state computer generated a summary log identifying search results for a specific torrent associated with known child pornography info hashes. Three files associated with that torrent downloaded to the state computer from the IP address "24.170.239.94." Corporal Schwarb explained that the software program allows law enforcement to obtain a "single source download," from only one IP address at a time.<sup>5</sup> Corporal Schwarb viewed three of the downloaded files: [(1) "000015.mpg;" (2) "000018.avi" and (3) "000019.avi"], and observed that those files depicted child pornography.

On March 12, 2016, Corporal Schwarb's state computer's activity log identified an additional file, "!(PTHC)Composite01-fatherandhis12yotwinsdaughters-13m19s.avi," which had again downloaded to his computer from the IP address 24.170.239.94 via the BitTorrent network. Corporal Schwarb reviewed the March 12, 2016 video file and observed that it depicted child pornography. Corporal Schwarb copied to a CD the three video files downloaded to his computer on February 13, 2016 and the one video file downloaded on March 12, 2016 from the IP address 24.170.239.94. The four video files contained on the CD were played for the jury and admitted as evidence. The parties

---

<sup>4</sup> The software program also allows law enforcement to receive files from a peer-to-peer network without sharing files from the law enforcement computers.

<sup>5</sup> Typically, BitTorrent clients obtain portions of files from multiple sources at once.

stipulated that each of the four video files identified by Corporal Schwarb depicted someone under the age of 15 engaged in sexual conduct.

Corporal Schwarb testified that he researched the IP address 24.170.239.94 on the public website, American Registry for Internet Numbers (ARIN), and learned that the IP address 24.170.239.94 was registered to Antietam Cable. Corporal Schwarb sent a subpoena to Antietam Cable for the subscriber information associated with the IP address 24.170.239.94. Antietam Cable responded that the subscriber to the account for that IP address was Slava Redkovsky located at 1034 Mount Aetna Road, Hagerstown, Maryland.<sup>6</sup>

At 4:50 a.m. on April 6, 2016, Corporal Schwarb assisted members of the Task Force in the execution of a search warrant at 1034 Mount Aetna Road. Corporal Schwarb arrived at the residence and spoke with appellant in the driveway, as appellant prepared to leave for work. Appellant provided his house keys to the Task Force and the Task Force searched the home. Corporal Schwarb observed that there appeared to be only one person living in the house. Corporal Schwarb determined that appellant's WiFi network was secured, as it required a password to access the WiFi network. The Task Force seized a black Toshiba laptop and three hard drives from a custom built, "tricked out" computer tower.

---

<sup>6</sup> Elsewhere in the record, the account holder is identified as "Slavic" Redkovsky rather than "Slava" Redkovsky. Travis Knode, the lead network engineer for Antietam Cable, testified that, between February 23 and March 12, 2016, the IP address, "24.170.239.94" was linked to the cable modem located at 1034 Mount Aetna Road, Hagerstown, and the account holder for that address was Slavic Redkovsky. Knode defined an IP (Internet Protocol) address as "a 32-bit unique identifier for devices that need to route traffic on the Internet."

State Trooper First Class Chris Reid of the Task Force interviewed appellant at his residence immediately following the search. The audio-recording of the interview was played for the jury at trial. In the interview, appellant acknowledged to Trooper Reid that he had a password protected wireless internet cable service provided by Antietam Cable. Appellant stated that he had a custom desktop computer, which he built as “a hobby.” He also had two laptops: a broken HP laptop, which he was in the process of fixing, and a working Toshiba laptop. Appellant explained that he bought the laptops on eBay “super cheap,” and that he had tried to “fix them up.” According to appellant, he was the only person who had used the Toshiba laptop.

Appellant described himself as having “maybe a little more than average” knowledge of computers. Appellant stated that he understood a peer-to-peer file-sharing program to be one where “you like upload it to a server or something, and then if it’s on a server, somebody else can go on and download it.” Appellant stated that he understood that peer-to-peer file sharing involved sharing files with other people. Appellant indicated that he had heard of BitTorrent, but did not think that he had ever used it. Appellant acknowledged that he had used the uTorrent program on his Toshiba laptop and expected that uTorrent was probably still on that laptop.

When asked by Trooper Reid if he ever looked up pornography, appellant responded: “Uh, I can’t say that I haven’t, but not on a file sharing program.” Appellant stated that he typically “would just Google for [pornography].” Appellant indicated to Trooper Reid that he did not expect that the Task Force would find any pornography on his laptop. Trooper Reid asked appellant if the Task Force would find any child pornography

on appellant's computer, and he responded, "Gee, I hope not." According to appellant, he "didn't have any of that stuff on [his] computer" and "[didn't] want anything to do with child porn."

Steven Gibson, a computer forensic analyst with the Department of Homeland Security Investigations, testified as an expert in computer forensics and data analysis. Gibson assisted in the execution of the search warrant at 1034 Mount Aetna Road by previewing devices to identify items of evidentiary value. On or about April 13, 2016, Gibson conducted a forensic analysis on multiple devices seized from appellant's residence, including a Toshiba laptop computer. Gibson observed that the peer-to-peer filing-sharing program, uTorrent, was installed on the Toshiba laptop and remained in active use. The most recent recorded logon date for the Toshiba laptop was April 6, 2016. In the course of Gibson's forensic analysis of the Toshiba laptop, he did not find any file names or visual images that matched the March 12, 2016 video provided to him by Corporal Schwarb. Gibson's findings were recorded in a forensic report, and the State introduced that report in evidence.

One year later, on or about April 18, 2017, Gibson conducted a subsequent analysis of the Toshiba laptop using GriFi Analyze, a digital imaging software tool, which had not previously been available to him. Using the four video files provided by Corporal Schwarb, Gibson searched the Toshiba laptop using a "hashset" from the info hashes and the file names, but found no filenames on the Toshiba laptop matching the filenames of the four video files identified by Corporal Schwarb.

In May of 2017, Gibson conducted a visual search of the files on the Toshiba laptop's thumbcache,<sup>7</sup> which is a hidden folder where users can view thumbnail-size images of their videos. Gibson identified three thumbcache images that matched images from the three video files downloaded on February 13, 2016 by Corporal Schwarb. Gibson took a "screen shot of it for comparison view so [one] can see the exact frame where the thumb cache image is matching to that exact frame of the video." The three "screenshot" images were admitted in evidence at trial.

In the course of his visual file search, Gibson also discovered a complete video file located in the "unallocated" space of the Toshiba laptop, which matched the fourth video downloaded by Corporal Schwarb on March 12, 2016. Gibson explained that the unallocated space is the area containing deleted files that have been emptied from the computer's "trash can." Gibson was unable to determine when the video on the Toshiba laptop was created or whether it had ever been viewed; he could only determine that someone had deleted it. Gibson explained that deleted files may be recovered from a computer so long as they have not been overwritten.

## **DISCUSSION**

Appellant contends that the evidence against him was insufficient to support his convictions for distribution of child pornography because he did not "actively transfer or

---

<sup>7</sup> According to Gibson, "[a] thumbcache is basically a marker to help you find images and videos quicker on your computer," by showing "a small picture" of the contents of the file. Once a particular folder is opened, a thumbcache is created from an image contained within that file.

distribute the videos to the State's computer and did not knowingly make the videos available for download[.]” Appellant is not challenging the sufficiency of the evidence as to his convictions for possession of child pornography. The State argues that appellant's claim is not preserved because he failed to raise before the trial court the argument that he now advances on appeal. Alternatively, if the argument was preserved, the State contends that there was sufficient evidence to show that appellant knowingly distributed child pornography by making the video files available for other users of the file-sharing network to download.

### **Preservation**

The State contends that appellant's argument for acquittal was limited to “arguing that there was insufficient evidence that it was *he* who distributed the child pornography files to the State's computer.” (Emphasis added). At the close of the State's case, the appellant moved for judgment of acquittal arguing:

Your Honor, at this time, I make a motion for judgment of acquittal, specifically with counts one through four - distribution. The legal definition says distribution is to transfer possession. I would argue that the State has not met [its] burden of showing that [appellant] transferred possession to the State. And I'd ask the [c]ourt to grant the motion.

The prosecutor responded:

Your Honor, at this point, the State has shown that [appellant] has transferred possession. He transferred digital files to Corporal Schwarb. The showing that it was indeed [appellant] in this particular matter is the fact that the files in question linked back to [appellant's] IP address.

Furthermore, that didn't stop. It also further went to the fact that not only did it link to his IP address, but a device that

he readily identified as being his own. I - - indicated he was the only occupant, didn't frequently have visitors. It was his laptop. There were no other - there were no other - - there would be anticipated no other users of it. Had either one of the videos saved - - still saved on his particular device as well - - or artifacts, in other words, thumb[.]cache indicative of the other three files.

Following counsel's arguments, the court ruled: "Your motion is denied, counsel."

Pursuant to Maryland Rule 4-324 (a), a criminal defendant who moves for judgment of acquittal must "state with particularity all reasons why the motion should be granted[.]" and "is not entitled to appellate review of reasons stated for the first time on appeal." *Starr v. State*, 405 Md. 293, 302 (2008) (citations omitted). Thus, "the issue of sufficiency of the evidence is not preserved when [the defendant]'s motion for judgment of acquittal is on a ground different than that set forth on appeal." *Mulley v. State*, 228 Md. App. 364, 388-89 (2016) (citations omitted). We have recognized, however, that a motion for judgment of acquittal may be sufficient to preserve an issue where the acquittal argument generally includes the issue raised on appeal. *See Williams v. State*, 173 Md. App. 161, 168 (2007) (finding that defendant's argument in support of acquittal that he was not in possession of a rental car that he was charged with failing to return, was sufficient to preserve his challenge that he lacked the required element of intent); *Shand v. State*, 103 Md. App. 465, 488-89 (1995) (defendant's argument that proof as to the elements of assault was lacking sufficiently preserved challenge for review); *aff'd on other grounds*, 341 Md. 661 (1996).

Appellant's argument in support of his motion for acquittal challenged the State's evidence relating to the element of transferring possession. The State argues that

appellant's argument was confined to challenging the evidence as to his identity as the source of the child pornography sent to the State's computer. We disagree. It was the prosecutor who addressed the sufficiency of the evidence linking appellant to the laptop and IP address. The State's argument on that point did not limit the scope of appellant's motion. We, therefore, conclude that appellant's argument challenging the element of transferring possession, though general, sufficiently encompassed the argument he raises on appeal: that the evidence was insufficient to establish that he transferred possession of child pornography files via the peer-to-peer file-sharing network. Appellant's argument in support of his motion for judgment of acquittal was sufficient to preserve his claim for appellate review.

### **Sufficiency of the Evidence**

We review a challenge to the sufficiency of the evidence to determine “whether, after viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.” *Grimm v. State*, 447 Md. 482, 494-95 (2016) (quoting *Cox v. State*, 421 Md. 630, 656-57 (2011)); accord *Jackson v. Virginia*, 443 U.S. 307, 319 (1979). “Because the fact-finder possesses the unique opportunity to view the evidence and to observe first-hand the demeanor and to assess the credibility of witnesses during their live testimony, we do not re-weigh the credibility of witnesses or attempt to resolve any conflicts in the evidence.” *Tracy v. State*, 423 Md. 1, 12 (2011) (citation omitted).

“[T]he question is not whether the [trier of fact] could have made other inferences from the evidence or even refused to draw an inference, but whether the inference [it] did

make was supported by the evidence.” *State v. Suddith*, 379 Md. 425, 437 (2004) (citation and internal quotation marks omitted). We, therefore, “defer to any reasonable inferences a jury could have drawn in reaching its verdict, and determine whether there is sufficient evidence to support those inferences.” *Lindsey v. State*, 235 Md. App. 299, 311, *cert. denied*, 458 Md. 593 (2018).

Appellant was convicted of violating Md. Code (1985, 2012 Repl. Vol.), Criminal Law Article, § 11-207(a)(4)(i), which prohibits an individual from knowingly distributing or possessing, with the intent to distribute any matter, visual representation, or performance that depicts a minor engaged in sexual conduct. For purposes of that section, “knowingly” is defined as “having knowledge of the character and contents of the matter,” § 11-201(c), and “distribute” means to “transfer possession.” § 11-201(b).

Appellant contends that § 11-207(a)(4)(i) requires that the State establish that he had the specific intent to deliberately and intentionally distribute child pornography. Appellant argues that the State failed to carry its burden of showing specific intent because it failed to demonstrate that he “actively” transferred or distributed child pornography to the State’s computer and knowingly made those videos available for download. The State responds that a showing of specific intent is not required to sustain a conviction under § 11-207(a)(4)(i) because “knowingly,” as used in that statute is defined in § 11-201(c). Though proof of specific intent was not required, the State submits that in this case, the evidence established that appellant had specific intent to distribute the child pornography videos because he admitted that he understood that the file-sharing program that he

installed on his laptop shared his files with other users on the network and made those files available for download.

Appellant cites *Chow v. State*, 393 Md. 431 (2006), in support of his argument that in order to sustain a conviction under § 11-207(a)(4)(i), the State was required to show that he had the specific intent to knowingly distribute child pornography. In *Chow*, the Court of Appeals determined that

[t]he sale of handguns is not itself illegal. It is the manner of the sale or rental, etc., that may make it illegal. The phrase used here “knowingly participates in the illegal sale . . .” contemplates that the actor must know that he or she is committing an “illegal sale.” We find this to be indicative of a *mens rea* requirement of specific intent for violations of § 449(f).

*Chow*, 393 Md. at 471.

Appellant contends that the Court’s application of “knowingly” in *Chow* applies equally to the application of “knowingly” under § 11-207(a)(4)(i). Specifically, he contends that § 11-207(a)(4)(i) requires proof that he knew that he was distributing child pornography when he downloaded the peer-to-peer file-sharing network which allowed his computer files to be accessed and downloaded by other users. As the State points out, in *Chow*, the Court of Appeals defined “knowingly” in the context of a firearms statute for which there was no statutory definition of the term. Here, unlike *Chow*, “knowingly” is defined by statute in § 11-201(c), and that definition does not require a showing of specific intent.

While no reported Maryland decision has addressed the question of whether the use of peer-to-peer file-sharing networks which allow users to obtain and download child

pornography files from another user's computer constitutes knowing distribution under § 11-207(a)(4)(i), both parties note that many state and federal courts have upheld convictions for distribution of child pornography where the evidence was sufficient to show that the defendant shared child pornography files using a peer-to-peer file-sharing network with the understanding that the network permitted others to download files from the defendant's computer.

In *United States v. Shaffer*, 472 F.3d 1219, 1223 (10th Cir. 2007), the defendant challenged the sufficiency of the evidence supporting his conviction for distribution of child pornography under a federal statute which made it unlawful “for a person knowingly to distribute child pornography by any means, including by computer.” In that case, the defendant used a peer-to-peer network to download images of child pornography to his computer and store them in a shared folder accessible to other network users. *Id.* at 1220-21. Similar to the argument raised by appellant here, Shaffer argued that he was not guilty of distribution because he did not “actively” or “personally” transfer possession of the files to another, but rather, he was “only a passive participant in the process.” *Id.* Concluding that the defendant had distributed child pornography in the sense of “transferring” it to others, then-Judge Gorsuch explained:

[Though the defendant] may not have actively pushed pornography on [other users of the peer-to-peer file-sharing network], ... he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items. It is something akin to the owner of a self-serve gas station. The owner may not be present at the station, and there may be no attendant present at all. And neither the owner nor his or her agents may ever pump gas. But the owner has a roadside sign letting all passersby know that,

if they choose, they can stop and fill their cars for themselves, paying at the pump by credit card. Just because the operation is self-serve, or ... [as defendant suggests], passive, we do not doubt for a moment that the gas station owner is in the business of “distributing,” “delivering,” “transferring[,]” or “dispensing” gasoline; the *raison d’être* of owning a gas station is to do just that. So, too, a reasonable jury could find that [the defendant] welcomed people to his computer and was quite happy to let them take child pornography from it.

*Id.* at 1223-24.

The majority of federal circuit courts have followed the Tenth Circuit’s reasoning and sustained convictions for distribution of child pornography where the defendant understood the purpose of a peer-to-peer file-sharing network and used that network to download and share child pornography with other users. *See United States v. Ryan*, 885 F.3d 449, 452-53 (7th Cir. 2018) (evidence that the defendant had a “sophisticated understanding of computers and software” and that he knew that child pornography files on his computer were accessible to others via a peer-to-peer file-sharing program was sufficient to sustain his conviction for knowingly distributing child pornography); *United States v. Stitz*, 877 F.3d 533, 538 (4th Cir. 2017) (“where files have been downloaded from a defendant’s shared folder, use of a peer-to-peer file-sharing program constitutes ‘distribution’” [under federal law]); *United States v. Richardson*, 713 F.3d 232, 236 (5th Cir. 2013) (“we conclude that downloading images and videos containing child pornography from a peer-to-peer computer network and storing them in a shared folder accessible to other users on the network amounts to distribution under [federal law]”); *United States v. Budziak*, 697 F.3d 1105, 1109 (9th Cir. 2012) (evidence was sufficient to support conviction for distributing child pornography where “the defendant

maintained child pornography in a shared folder, knew that doing so would allow others to download it, and another person actually downloaded it”); *United States v. Chiaradio*, 684 F.3d 265, 282 (1st Cir. 2012) (“[w]hen an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred”); *United States v. Collins*, 642 F.3d 654, 656-657 (8th Cir. 2011) (evidence that defendant was “knowledgeable about computers” and had a peer-to-peer file-sharing program on his computer with stored images of child pornography supported his conviction for attempting to knowingly distribute child pornography).

Many state courts have also upheld distribution of child pornography convictions in cases involving distribution via peer-to-peer networks. In *State v. Lyon*, 9 A.3d 596, 597 (N.J. Sup. Ct. App. Div. 2010), the trial court found that the defendant’s passive participation in a peer-to-peer file-sharing program where child pornography was downloaded from his computer, did not constitute offering and distributing child pornography under the New Jersey statute. On appeal, the New Jersey appellate court rejected “defendant’s omission and passive conduct argument.” *Id.* at 603. The appellate court determined that the term “knowingly,” which was not defined in the New Jersey distribution statute, was intended by that state’s legislature to include the conduct of using a file sharing network to “provide and offer child pornography he possessed in his shared folder.” *Id.* at 602-603. See also *People v. Rowe*, 318 P.3d 57, 61 (finding that evidence that defendant knowingly stored sexually exploitative photos and videos of children in a shared folder on a peer-to-peer file-sharing network for others to download was sufficient to support conviction for sexual exploitation of a child by “offering” sexually exploitative

material), *cert. denied*, 2013 WL 4008636 (Colo. 2013); *Maddox v. State*, 816 S.E.2d 796, 802 (Ga. Ct. App. 2018) (evidence was sufficient to sustain conviction for distribution of child pornography where defendant admitted that he stored child pornography in his computer's shared folder and that the purpose of the file-sharing program that he downloaded was to share his files with other users); *State v. Tremaine*, 315 S.W.3d 769, 772 (Mo. Ct. App. 2010) (finding that evidence was sufficient for jury to find that the defendant offered to disseminate child pornography where he used a peer-to-peer file-sharing network in a way that made child pornography files available "for widespread sharing" over the network, and he invited others to download those items from him); *Wenger v. State*, 292 S.W.3d 191, 200 (Tex. App. 2009) (evidence that defendant used a file sharing program, which he understood shared files from his computer with other users, was sufficient to support conviction for knowingly "disseminating" child pornography); *Kelley v. Commonwealth*, 771 S.E.2d 672, 675 (Va. 2015) (finding that evidence that defendant's use of peer-to-peer file-sharing network and understanding that the program enabled other users to download his files supported conviction for knowing distribution of child pornography).

In this case, appellant was a savvy computer user who, as a hobby, repaired broken computers and built a customized desktop computer with multiple hard drives. Appellant admitted downloading and installing the client, uTorrent, required for using a peer-to-peer file-sharing network. Appellant indicated that he understood that peer-to-peer file-sharing programs worked by uploading files from one computer and making them available for others to download.

The evidence demonstrated that four child pornography videos downloaded to Corporal Schwarb's state computer from a single source: the appellant's IP address. The State presented forensic evidence showing that images identified in three thumbcaches on appellant's Toshiba laptop matched still shot images of the three video files downloaded on February 13, 2016 from appellant's IP address to Corporal Schwarb's computer. A fourth video file, located in the unallotted space on the Toshiba laptop, matched the child pornography video downloaded on March 12, 2016, from appellant's IP address to Corporal Schwarb's computer.

Viewing the evidence in the light most favorable to the State, we conclude that the evidence was sufficient for a jury to reasonably find that, based on appellant's understanding of the peer-to-peer file-sharing programs, and his use of the uTorrent client which made files on his Toshiba laptop available for other users to download, appellant knowingly transferred four videos depicting child pornography to Corporal Schwarb's state computer. Accordingly, the evidence was sufficient to support the appellant's convictions for distribution of child pornography.

**JUDGMENT OF THE CIRCUIT COURT  
FOR WASHINGTON COUNTY  
AFFIRMED. COSTS TO BE PAID BY  
APPELLANT.**