THE STATE OF NEW HAMPSHIRE
SUPREME COURT

No. 2023-0258

State of New Hampshire

v.

Roland Higgins

APPEAL PURSUANT TO RULE 7 FROM A JUDGMENT OF THE GRAFTON COUNTY SUPERIOR COURT

BRIEF FOR THE STATE OF NEW HAMPSHIRE

THE STATE OF NEW HAMPSHIRE

By Its Attorneys,

JOHN M. FORMELLA
ATTORNEY GENERAL

and

ANTHONY J. GALDIERI
SOLICITOR GENERAL

Audriana Mekula, Bar No. 270164
Assistant Attorney General
New Hampshire Department of Justice
Office of the Solicitor General
1 Granite Place South
Concord, NH 03301
(603) 271-1291

(Fifteen-minute oral argument requested)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

ISSUE PRESENTED

I. Was there sufficient evidence to support the defendant's convictions?

STATEMENT OF THE CASE

A Grafton County grand jury indicted the defendant with six felony counts of distribution of child sexual abuse images (CSAI) and sixteen felony counts of possession of CSAI. DAII[1] 2-23. The charges occurred on various dates between July 2017 and March 2018. *Id*. On September 30, 2022, following a two-day bench trial in August 2022, the trial court (*MacLeod*, J.) found the defendant guilty on all of the charges. V 8-12. On September 7, 2022, the defendant filed a motion to set aside the trial court's verdicts, to which the State objected. DAIII 121; SA 3. The trial court denied this motion in a written order on November 17, 2022. DAI 2-6.

On April 13, 2023, the trial court sentenced the defendant to four years to ten years stand committed on three of the distribution of CSAI convictions and eight of the possession of CSAI convictions. SA 5-70. On the remaining convictions, the defendant was sentenced to six years to twelve years in the state prison all suspended for ten years upon release. SA 71-125. This appeal followed.

---

[1] Citations to the record are as follows:
"DAI_" refers to the first volume of the defendant's appendix and page number;
"DAII_" refers to the second volume of the defendant's appendix and page number;
"DAIII_" refers to the third volume of the defendant's appendix and page number;
"DB_" refers to the defendant's brief and page number;
"SA_" refers to the State's appendix and page number;
"T_" refers to the trial transcript and page number; and
"V_" refers to the verdict hearing transcript and page number.

STATEMENT OF FACTS

At the time of trial, Indiana County Detective Gerhard Goodyear had been working in law enforcement since 1993 and had been a detective working in computer crimes for 12 years. T 27-28, 30. He primarily investigated crimes involving the "distribution and possession of child exploitive material via various peer-to-peer networks, such as 'BitTorrent, eMule, Freenet, and so on."' T 28. At trial, he was certified as an expert in the "BitTorrent network and investigative software" without objection. T 34.

Detective Goodyear explained that BitTorrent is a file sharing network through which users can download content or can send and receive content from other users. T 36-37. When a BitTorrent user is on the network, he can download "specific content he is interested in, and [he] then become[s] a source for that same content." T 38. This means that if a BitTorrent user downloads a certain file to a device, other BitTorrent users can download that same file from that user to their device. *Id*. This allows users to download content faster, and allows them to "share back out to other users who still need that content." T 38-39. Likewise, if there is more than one source for the content on BitTorrent, the network will take parts from all the sources to download the content faster. T 39.

BitTorrent utilizes a multi-step process to share files or content. *Id*. First, a user must download BitTorrent. T 40. Once the program is downloaded, a user must obtain a "torrent file." T 42. A torrent file is a set of instructions that defines downloadable content that the user can use to locate content he wishes to download on BitTorrent. *Id*. A torrent file is

necessary because "BitTorrent does not have the ability to search internally within the BitTorrent network for content," so the user needs to know specifically what to look for to download it on BitTorrent. *Id*. A torrent file contains seven pieces of information: a file name, a file path, the file's size, the number of pieces that make up the file, the sizes of the pieces, the "piece hash," which is a unique identifier like a digital fingerprint, and "whether the torrent is marked as either private or public." T 47.

To obtain a torrent file, a user can use his internet browser to search for an "indexing site" containing numerous torrent files. T 42. Once a user accesses an indexing site, he can search for specific content on the site using keywords. *Id*. To do so, the user types "one or more words which would describe the type of content that [he was] looking for" into a search bar. T 43. Each indexing site has different results. T 42. If a user wants to search for CSAI on an indexing site, he could search keywords such as "PTHC, which stands for pre-teen hard core; PTSC, which is pre-teen soft core; Belita; 6yo, 7yo, 8yo, which would generally indicate the age of the individual in [] the video." T 42-43.

Once a user searches for certain keywords, a "list of available options" appears on the indexing site and the user can choose "which one of those descriptions or files best describes what it is that they're looking for." T 43-44. Then the user can choose which torrent files to download. T 44.

Once a user selects a torrent file, he can either download it directly from the indexing site, or he can copy and paste a URL into BitTorrent to download the torrent file from another user on BitTorrent. T 45.

If a user copies a URL of a torrent file and pastes it into BitTorrent, BitTorrent "will attempt to find other users who may have that torrent, and it will download that torrent directly from that user, and have it displayed within the download screen." T 46. However, this file will not download to the user's device until the user "actually selects download" or "okay[s]' the actual download of the specific content. *Id*.

The torrent files accessed through an indexing site do not usually contain the actual content; they simply contain instructions on how to find the content on BitTorrent or another program similar to BitTorrent. T 47. Some torrents contain multiple files and certain torrents can contain over 50,000 files. T 48. As such, downloading one torrent means that a user may download a multitude of files in many formats. *Id*. Likewise, a torrent containing CSAI could contain more than one file of CSAI. *Id*. If a user wanted to download a torrent with multiple files, the user could select which specific files in that torrent to download, or could download all of the files in the torrent. T 80, 100-01.

To download a file to a user's device from BitTorrent, data must be exchanged from other users to the user seeking to download the file. T 47. For this to occur, all the users must have "the same torrent" that has the same hash, or unique identifier, loaded into BitTorrent. T 47-48. This is necessary because each torrent breaks up the file or files it contains into equally sized pieces. T 49. When a user begins downloading a file from other users' torrents, the user receives each piece from multiple user's torrents. *Id*. For example, if a user wanted to download an image on BitTorrent, and three other users had the same image, the user downloading the image "would actually connect to each of [the other three users] and

download individual pieces [of the image] from any one of those three [users] . . . .” T 39.

Once pieces are downloaded onto a user’s device through BitTorrent, BitTorrent confirms that the pieces it downloaded from other users match the hash value for the pieces the download user requested. T 50. Once hash values are verified as being the same, “that piece becomes available to share back out onto the network to other users who may need that same content, or that same piece.” T 50-51. Sometimes, when pieces are downloaded, they do not contain the entire file, but contain enough of the file for a user to see what the file is. T 51-52. Even if the file download is not complete, the file still may be recognizable if enough of it was downloaded. T 52-53.

Investigators use the hash value of a file as the file’s digital fingerprint to differentiate it from other files. T 54. BitTorrent’s hashing uses alphanumeric characters to differentiate each file and create a “one in about 1.4 quindecillion, which would be one followed by 48 trillion zeros” chance that two files would have the same hash value. *Id*. According to the detective, this means that it is “computationally infeasible, really, for two different files to calculate the same hash value.” *Id*.

To find the proper pieces to download from other users based on hash values, BitTorrent “will reach out to various, what are referred to as indices, looking for IP addresses and ports that are associated with that specific torrent as identified by its info hash.” T 57. If there is a direct match, BitTorrent downloads the matching pieces from the users whose information it has stored on its network. T 58. These downloads can only occur if the other user from whom the pieces are being downloaded has

saved the file "somewhere on a device that was connected to whatever device that is running" the BitTorrent program. T 63-64. Likewise, the user's IP address, port, and hash value for the sought-after file are also stored on BitTorrent as a source for that file. T 58. If BitTorrent tried to download a file from a source that no longer had the file, the download would not occur. T 59.

Investigative software exists to search networks like BitTorrent. T 60-61. One example is Torrential Downpour, which investigators use to search for CSAI on BitTorrent. *Id*. Torrential Downpour is only able to download content that is stored on a user's device or is "actively being shared and being made available" by a user on BitTorrent. *Id*.

To successfully download content to BitTorrent, a user takes multiple "affirmative actions." T 44. Specifically, the user takes affirmative action when he: (1) searches for certain keywords in an indexing site to find CSAI, T 45-46; (2) clicks on a torrent file to download its contents, T 46; (3) cancels a download while it is in progress, T 106; (4) saves the content that was downloaded from BitTorrent onto the user's device, T 63-64; and (5) shares the downloaded content beyond the default sharing that already occurs on BitTorrent. T 64. Additionally, programs like BitTorrent are file-sharing programs, meaning that "users are expected to give in order to get content." T 83. Likewise, a user agrees through the licensing agreement for BitTorrent that other users can download content from the user without the user's knowledge or permission. T 105.

Users may use VPNs, or virtual private networks, to shield their IP addresses from other users or from law enforcement on a file-sharing program. T 91. A VPN shields a user's IP address by "directing traffic"

through the VPN server and not the user's IP address. *Id*. Once a VPN is turned off or disconnected, however, the user's IP address is then visible on the program. T 91-92. To identify the owner of an IP address, an investigator relies on subscriber information from a service provider that "will detail exactly where the business or residence is at that the IP address was assigned to." T 93.

Detective Goodyear said that, in his experience, users downloading CSAI often download it, view it, or "do[] whatever business they're doing with it," and then delete it, knowing that they can "get it again anytime they want to essentially very quickly." T 110.

Lieutenant Fredric James of the Grafton County Sheriff's Office was trained in 2017 on using Torrential Downpour to search BitTorrent for CSAI. T 114-15. After he completed the three-to-four-day training, he received the Torrential Downpour software, which he downloaded onto an "undercover computer" that was password protected at the sheriff's office in a private, secured office. T 115-16. The lieutenant installed and began using this software in July 2017. T 116. When he began using it, he monitored his "own cases and the region of New Hampshire." *Id*. The lieutenant explained that he limited his searches to New Hampshire so that he would have jurisdiction over any contraband he found. *Id*.

On July 17, 2017, the lieutenant noticed "activity involving an IP address that geolocated to Lebanon, New Hampshire where [he] was able to successfully download at least one file [] of interest." T 117. This IP address was 76.118.42.20. *Id*. Torrential Downpour downloaded multiple images or videos of CSAI from this IP address from July 2017 to November 2017. T 118. As a result, the lieutenant sought a grand jury

subpoena for the IP address's subscriber information. T 118. That information identified the subscriber as the defendant. *Id*. The lieutenant continued monitoring the defendant's IP address on Torrential Downpour. T 120-21. The IP address downloaded "erotica" in December 2017, January 2018, and February 2018, and child sexual abuse material in February 2018. T 121.

The lieutenant explained that Torrential Downpour showed the lieutenant the "info hash, the date and time of the connection, how many pieces may be associated with that file, and as well as how many pieces" for each downloaded or partially downloaded image from the defendant's IP address. T 120. The lieutenant viewed all of the downloads and saw "child erotica," or lewd images of children, and "child sexual abuse material which was the sexual assault on minors whereas some of the images portrayed maybe a five-to-seven-year-old being sexually assaulted by an adult male." T 119. Other images showed a child's genitalia as the focal point of the image. T 120. In other images, "there would be two youth, probably early teenage years, who were manually stimulating each other's genitalia." *Id*.

In February 2018, the lieutenant attempted to execute a search warrant at the defendant's home. T 121. However, when he attempted to execute the warrant, the defendant was not home. T 121. The lieutenant reapplied for a search warrant in March 2018 for the defendant's home and executed that search warrant on March 26, 2018. T 121-22. When he executed the warrant, the defendant's wife was home and she told the lieutenant that the defendant was at work at Keene State College. T 122.

The lieutenant and Trooper Kelly Wardner drove to Keene State College and spoke with the defendant in his office. *Id*. During this conversation, the defendant told the investigators that "he had been struggling with [] paraphilia, being an interest in young girls specifically 12 to 18 years of age for a lengthy period of time and that he had used BitTorrent to view some of this content, but he was looking for the legal content and not the illegal content." *Id*. At that point, the investigators asked the defendant if he would drive himself to the Keene Police Department to continue speaking with them. T 123. He agreed, and the investigators audio and video recorded the defendant's interview at the police department. *Id*. This two-hour interview was admitted as a full exhibit. T 123-24; SA 126-94.

During the interview, the defendant said that he was a "risk-taker," an "intellectual," and was "curious . . . to see what it is that's out there." SA 127. He admitted that he was "stuck as an adolescent . . . sexually speaking." SA 147. He also said that he had talked to "shrinks" and they told him he had "paraphilia," which he later explained meant that he was attracted "to the beauty the loveliness the purity" of child erotica. SA 137-38, 164.

The defendant then told the police about a website he had found called BTKU that he described as "dangerous," because someone could search on this website for "PHC," or "PTH," which the defendant said was an acronym for "pedo . . . hard core," and that the website would provide "page after page of" CSAI with children who are as young as three years old. SA 139-40.

The defendant also told the police about using BitTorrent to download content overnight. SA 143. He said that sometimes he would download files overnight and he would not know what he had downloaded until it was finished, and he opened the file. *Id*. He said if he opened a file that he did not want, he would "delete it" and it would go "straight in the trash." *Id*. He told the investigators that he stayed away from files named ten-year-old or twelve-year-old, but would sometimes download a file named "Russian model." *Id*. He denied searching for pre-teen hard core files on BitTorrent. SA 171. He admitted that he used a European website and a Japanese website to look at pictures of "teenage models." SA 141.

The defendant then explained how someone could use BitTorrent to download large files by accessing the content in "small packets" from "anywhere." SA 143-44. He said that meant that if he had part of a file, that part could be taken from his device to download the file for another user. SA 144-45. He also explained that on BitTorrent, searching for a keyword was not the same as downloading content. SA 150. He explained that after he searched for something, he would then scroll through an index and select something to download. SA 151. He also admitted that he had a VPN that he tried to use all the time, but that he did not always connect to it. SA 165-67.

The defendant said that some content on BitTorrent is "godawful," and that he did not look for that content "except for once in a while" when he was "curious." SA 144. When the investigators asked the defendant about "the worst" content he had seen on BitTorrent, the defendant answered that the worst he had seen was "a big fat hairy probably Russian guy um having intercourse with a very young kid." SA 152. He also said

that he is only interested in viewing clothed teenage models in erotic positions. SA 160-61.

Near the end of the interview, the defendant said that if he had done "something wrong, it was a mistake," and told the investigators that if they found anything illegal, he would "certainly regret it hugely, but it[] wasn't [his] intention to get it or keep it." SA 188. He also said that he "certainly did not want to keep anything that was incriminating." SA 189.

Police seized numerous devices from the defendant's home, including two "Mac Mini PC[s]." T 130-31. Nashua Police Detective Peter LaRoche, who was certified at trial as an expert in digital forensics, forensically examined these two devices. T 130-31, 171. One of the devices had two accounts associated with it: "Roland Higgins" and "R Higgins." T 178. Under the "R Higgins" account, the detective found vacation photographs of the defendant and the defendant's employment documents. T 179. Under this account, the detective also saw that BitTorrent and uTorrent were downloaded onto the device. T 179-80.

The detective saw "several hundred" torrent files with "names that were consistent with child exploitation files" and "related to child sexual abuse material" on the "R Higgins" account. T 180. Some of these file names included "Pre-Teen Hard Core," "12-year-old," "15-year-old," and some from a "series" of "Russian electronic magazine[s] that featured child erotica, anywhere from preteen girls to single digits, like, eight, nine-year-old females, and that ranged from anywhere from in bathing suits, to lingeries, to nude." T 181. The detective explained that these were terms he was "familiar with because we see them often in cases like this, and they're

included in key word search term lists that we run. And there were other names [he] was familiar with from seeing in other cases." *Id*.

The detective ran this device through Griffeye Analyze, which is software that searches through images and videos stored on a device for certain hashes "of known images of child exploitation, child sexual abuse material, [and] even exploitative animation." T 183-84. The hashes are entered into the software's database by law enforcement, so the detective's search was not exhaustive. T 184-85. When it locates images or videos matching a known hash, it categorizes the content into either category one, which is illegal content, or category two, which is "maybe illegal" content. T 185. This content is then reviewed by an investigator to determine whether the content is illegal to possess. *Id*. On this device, Griffeye categorized eight files as category one content. *Id*. The detective manually looked at each file that the software categorized on this device and looked at content that the software flagged but did not categorize. T 194.

On the other device, the detective found two accounts: "R Higgins" and "RLH." T 186. He also found that BitTorrent was installed on this device. *Id*. The detective ran this device through Griffeye as well. T 186. That software found "significantly more images" on the second device. *Id*. Six images were classified by the program as category one, and a "significant amount" of content was classified as category two. *Id*. The detective also manually looked at each file that the software categorized on this device and looked at content that the software flagged but did not categorize. T 194. This content was located under the "R Higgins" account. T 187. After reviewing files on both devices, the file times showed that many of the files on both devices had been accessed. T 197. After

completing his forensic examinations, the detective wrote "forensic examination reports." *Id*.

Lieutenant James reviewed some of the content that was stored on these devices and reviewed Detective LaRoche's forensic examination reports for the two Mac Minis. T 132. On the Mac Mini that had a significant amount of category two content, Lieutenant James found the charged images and videos. *Id*. The other Mac Mini had some images that could have been charged, "but not in large volume." T 134. The lieutenant said that he viewed all the images and videos that the defendant was charged with possessing and that they matched the descriptions in the indictments. T 147-50; DAII 8-23.

The lieutenant explained that the distribution of CSAI charges were based on the single source downloads that Torrential Downpour found and downloaded from the defendant's IP address. T 135-36. Torrential Downpour tracked not only the content of the downloads, but also tracked the date and time of the downloads, the file's "info hash," how many pieces were associated with each file, what pieces were actually downloaded, and whether the download was complete or incomplete. T 137. The lieutenant then organized this information into logs for each file that the defendant was charged with downloading. T 138-39. These logs were admitted at trial as a full exhibit. T

The logs showed that on July 18, 2017, Torrential Downpour downloaded from the defendant one complete image that was contained within a torrent folder titled "Asian girls Yuli Tetemi (phonetic) nine-year-old." T 140-42. The lieutenant said that the image he saw in this download matched the description in the indictment. *Id*.; DAII 2. The logs also

showed that, on August 16, 2017, Torrential Downpour downloaded from the defendant two videos, both of which were incomplete downloads, meaning that while watching the videos, the screen would periodically go black and then return to the video. T 143-44. The lieutenant watched the two videos and said they matched the descriptions in the indictments. *Id.*; DAII 3-4. The logs also showed that on September 18, 2017, Torrential Downpour downloaded from the defendant two complete images. T 144-45. The lieutenant saw both images and they matched the descriptions in the indictments. *Id.*; DAII 5-6. The logs also showed that on January 19, 2018, Torrential Downpour downloaded from the defendant a complete video that the lieutenant watched that matched the description in the indictment. T 146.; DAII 7.

The parties stipulated that the images and videos described in the indictments were CSAI and agreed that the charged images and videos could be admitted as full exhibits. T 146-47; DAII 24.

After the State rested, the defendant moved to dismiss all of the charges. T 200. Relative to the distribution charges, the defendant argued that the State had not proven that the defendant knowingly possessed the CSAI, nor did the State prove that the defendant knowingly exchanged or transferred the CSAI. T 201. Relative to the possession charges, the defendant argued that the State did not prove that the defendant knowingly possessed the specific images, nor did the State prove that the defendant knew that the images were "that of a child engaging in sexually explicit activity." T 201-02.

The State objected, arguing that, for the distribution charges, the State presented sufficient evidence that the defendant had an in-depth

understanding of how BitTorrent worked and that the trial court could infer that the defendant knew he was taking affirmative steps to find, download, and save the charged images. T 202-06. The State also argued that Torrential Downpour would not have been able to download the charged images and videos from the defendant's BitTorrent account if the content had been deleted, renamed, or moved. T 204.

The State also argued that it presented sufficient evidence of the possession charge because the defendant admitted in his police interview to having seen "some pretty terrible stuff out there," and admitted to deleting images that he would re-download to view again. T 206. The trial court took the motion to dismiss under advisement and allowed the parties to make closing arguments. T 200, 207.

On September 30, 2022, the trial court held a hearing on its verdict. The trial court found the defendant guilty on all 22 charges. V 8-12. In issuing its verdict, the trial court found that RSA 649-A:3 did not define possession, exchange, distribution, or transfer. V 4-5. To define these terms, the trial court relied on Black's Law Dictionary. *Id*. Black's Law Dictionary defined possession as "the fact of having or holding property in one's person – or in one's power, rather, or the exercise of dominion over the property," constructive possession as "control and dominion over property without actual possession or custody of it;" distribution as "to apportion, to divide among several, to deliver, to distribute;" and transfer as "any mode of dispensing or parting with an asset or an interest in an asset, including a gift, et cetera." *Id*.

The trial court found no New Hampshire cases defining the exchange or transfer of CSAI pursuant to RSA 649-A:3. V 5. The trial

court relied on a First Circuit Court of Appeals case, *United States v. Chiaradio*, 684 F.3d 265 (1st Cir. 2012), to define distribution of CSAI. V 5-6. In that case, as the trial court found, the defendant had downloaded a peer-to-peer sharing program called LimeWire onto his home computer. V 5. A federal agent, using a program similar to Torrential Downpour, downloaded CSAI from the defendant's computer that he had accessed and shared using LimeWire. *Id*. The First Circuit held that there was sufficient evidence supporting the defendant's distribution conviction because the defendant consciously made files available for others to download. V 6. The trial court also noted that the First Circuit held that distribution's plain meaning was "the act or process of apportioning or giving out." *Id*.

The trial court then found the defendant guilty of the distribution charges because "the evidence is convincing to the Court beyond a reasonable doubt that, in fact, [the defendant] did know" that he downloaded CSAI. V 7. "And he certainly took affirmative steps to download these images onto his machine with a program that allowed others, without his knowledge or any further action on his part, to remove such images from his machine." *Id*. The trial court also found that the defendant "clearly [knew] that he had the BitTorrent program on his computer and in so many words that he clearly understood how it functioned." V 8.

Regarding the possession convictions, the trial court found that RSA 626:1 "was applicable." V 9. The trial court noted that RSA 626:1 provides that "[a]ll crimes require conduct that includes a voluntary act or the voluntary admission to perform an act . . . [and] the possession is a voluntary act if the possessor knowingly provided or received the thing

possessed or was aware of his control thereof for a sufficient period of time to be able to terminate his possession." *Id*. The trial court then cited *State v. Clark*, 158 N.H. 13 (2008), for the proposition that "images that were downloaded to a computer affirmatively done so by the defendant [] constitute[] a voluntary act." V 9-10.

The trial court also found that the defendant

> made some very incriminating and damaging statements in his interview with the police. He also made various denials, which given the totality of the evidence, I do not find to be credible, regarding his knowledge of what he was looking at and when he was looking at, particularly in light of the testimony of Detective James as to the number of images downloaded onto the County's – sheriff's department's computer, for which the defendant was not charged, as well as the number of images recovered by Detective LaRoche, for which the defendant also was not charged.

V 10.

On October 7, 2022, the defendant filed a motion to set aside the verdicts, arguing that the State had not proven all of the elements beyond a reasonable doubt. DAII 121. On October 18, 2022, the State objected to the defendant's motion to set aside the verdicts. SA 3.

On November 17, 2022, the trial court denied the defendant's motion to set aside the verdicts. DAI 2-6. The trial court found that the defendant had argued in his motion that the State had failed to prove that the defendant "knew or was aware that the child pornographic images identified in the 16 possession indictments and the 6 distribution indictments were contained within his computer files on the dates the State claims, and thus the State failed to prove that the defendant knowingly committed the criminal acts alleged." DAI 3.

The trial court found that, to prove the defendant knowingly possessed CSAI, the State had to prove that the defendant knowingly exerted some control over the CSAI. *Id*. The trial court found that the State presented sufficient evidence that the defendant knowingly possessed the CSAI on his devices "because it proved that the defendant caused the specific images at issue to be downloaded to his computer and was aware of the same, and thus that he knowingly possessed those images as charged." DAI 3-4. To support this conclusion, the trial court relied on "each evidentiary fact and item in the context of all the evidence presented and not in isolation," including the defendant's police interview in which he said that "the images were readily assessable [sic] to him via a software system he had installed for that purpose on his computer." D I 4. The trial court further found that the CSAI stored on the defendant's computer was not accidental or inadvertent, but that the defendant "intentionally made use of the software he installed in his computer to knowingly reach out on the internet and acquire the images identified by the State." *Id*. The trial court also found that the defendant viewed the images was "not dispositive given the evidence of his intentional acquiring and control of the images." *Id*.

The trial court also noted that the dates of the offenses were not essential elements that the State had to prove for either the possession or the distribution of CSAI charges. *Id*.

Regarding the distribution of CSAI charges, the trial court found that the State presented "probative and persuasive evidence that the defendant knowingly distributed" CSAI. DAI 5. The State proved that the defendant "knowingly installed a software program in his computer which he was aware was designed specifically for the purpose of searching the internet,

including other computers with the same software, and downloading to his computer various items which he knew included [CSAI] as well as lawful content including so-called child erotica." *Id*. It found that the State also proved that the defendant knew that the same software program "permitted other users with the same software to remotely access his computer files at any time without his permission or knowledge and download its contents, including [CSAI]." *Id*.

SUMMARY OF THE ARGUMENT

The State presented sufficient evidence that the defendant distributed and possessed CSAI. Regarding the distribution charges, the State presented sufficient evidence that the defendant exchanged or transferred CSAI six times because the defendant consciously made the CSAI available for others to take, download, or access through a peer-to-peer sharing network, and the CSAI was downloaded by an investigator using that network. Specifically, the State proved that the defendant knew that BitTorrent was a peer-to-peer sharing network, and knew that what he downloaded and saved to his devices using BitTorrent could be downloaded by other users. The State also proved that the defendant knew he had CSAI saved on his devices based on the incriminating statements he made during his police interview. Based on the evidence as a whole, the State also disproved any rational inferences from the evidence associated with innocence.

Regarding the possession charges, the State presented sufficient evidence that the defendant exercised control over the CSAI investigators found on his devices. This Court has held that in a possession of CSAI case, "[t]he relevant inquiry thus becomes whether the defendant knowingly possessed the images, in that he exerted some control over them, or whether the presence of the images on his computer was merely inadvertent. This inquiry is a question of fact." *Clark*, 158 N.H. at 20 (citations omitted). The State presented sufficient evidence that the defendant had a substantial amount of CSAI on his devices, that some of the files had names indicative of containing CSAI, that some of the files stored on the defendant's devices

had been accessed, that the defendant was interested in viewing images of teenage models, and that he desired specifically to view twelve-year-old girls. The defendant also admitted to viewing CSAI that he downloaded from BitTorrent and subsequently deleted. Because the State proved that the defendant controlled the CSAI found on his devices, the State did not need to prove that the defendant accessed or viewed the sixteen charged images.

Likewise, the State disproved any rational conclusions consistent with innocence based on the fact-finder's determination that the defendant largely incriminated himself based on his own statements, that the fact-finder did not believe the defendant's denials of possessing CSAI, and based on the other evidence admitted at trial.

Accordingly, this Court should affirm the defendant's convictions.

ARGUMENT

I. THERE WAS SUFFICIENT EVIDENCE TO CONVICT THE DEFENDANT OF DISTRIBUTION AND POSSESSION OF CSAI.

A. Standard of Review.

"When considering a challenge to the sufficiency of the evidence, '[this Court] objectively review[s] the record to determine whether any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt … considering all the evidence and all reasonable inferences therefrom in the light most favorable to the state.'" *State v. Saunders*, 164 N.H. 342, 351 (2012) (quotations and citation omitted). "The defendant bears the burden of proving that the evidence was insufficient to prove the guilt." *State v. Seibel*, 174 N.H. 440, 445 (2021) (citing *State v. Saintil-Brown*, 172 N.H. 110, 117 (2019)).

When the evidence presented at trial includes both direct and circumstantial evidence, this Court will "uphold the verdict unless no rational trier of fact could have found guilt beyond a reasonable doubt." *Seibel*, 174. N.H. at 445. "Further, the trier may draw reasonable inferences from facts proved and also inferences from facts found as a result of other inferences, provided they can be reasonably drawn therefrom." *State v. Sanborn*, 168 N.H. 400, 412-13 (2015) (quotation omitted).

This Court reviews a challenge to the sufficiency of the evidence *de novo* because it raises a claim of legal error. *Saintil-Brown*, 172 N.H. at 117. In reviewing the evidence, this Court assesses "each evidentiary item

in the context of all the evidence, and not in isolation." *Id.* (citing *State v. Craig*, 167 N.H. 361, 369 (2015)).

"Direct evidence is evidence which, if accepted as true, directly proves the fact for which it is offered, without the need for the factfinder to draw any inferences." *State v. Kelley*, 159 N.H. 449, 454 (2009) (quotations and citation omitted). Direct evidence includes "the testimony of a person who claims to have personal knowledge of facts about the crime charged such as an eyewitness." *State v. Newcomb*, 140 N.H. 72, 80 (1995).

"Circumstantial evidence, to be sufficient to convict, must exclude all rational conclusions other than the guilt of the defendant in a case where there is *only* circumstantial evidence to support the conviction." *Newcomb*, 140 N.H. at 80 (quotations and citation omitted) (emphasis added). "Facts may be proved by circumstantial evidence, and [t]he law makes no distinction between direct evidence of a fact and evidence of circumstances from which the existence of a fact may be inferred." *Id*. at 81 (quotations and citation omitted). "A defendant's intent often must be proved by circumstantial evidence and may be inferred from the defendant's conduct under all the circumstances." *State v. Vincelette*, 172 N.H. 350, 354 (2019).

B. The State Presented Sufficient Evidence That The Defendant Distributed CSAI.

To find the defendant guilty of the six distribution of CSAI charges, the State had to prove beyond a reasonable doubt that the defendant knowingly "exchanged or otherwise transferred a visual representation of a child under the age of eighteen years engaged in sexually explicit conduct," using "IP Address 76.118.42.20 registered to Comcast Cable using the

BitTorrent file sharing software." DAII 2-7; RSA 649-A:3-a, I(a). The State also had to prove that the defendant exchanged or transferred the CSAI described in each indictment. *Id*. At trial, the parties stipulated that the images or videos described in the six distribution charges were CSAI as defined by RSA 649-A:2 and that IP address 76.118.42.20 "was assigned to [the defendant]." DAII 24; T 4-5. Thus, the State only needed to prove that the defendant knowingly exchanged or transferred the CSAI described in each indictment.

As the trial court found, RSA 649-A does not define "distribution," "exchange," or "transfer." This requires this Court to engage in statutory interpretation. This Court reviews questions of statutory interpretation *de novo*. *State v. Proctor*, 171 N.H. 800, 805 (2019). This Court first looks to the language of the statute itself and, if possible, construes that language according to its plain and ordinary meaning. *Id*. This Court interprets a statute in the context of the overall statutory scheme and not in isolation. *Id*.

While the definitions of distribute, exchange, and transfer in the context of RSA 649-A:3-a are matters of first impression for this Court, other courts have defined these terms based on their plain and ordinary meaning as they relate to the distribution of CSAI. The First Circuit has held that "[w]hen an individual consciously makes files available for others to take and those files are in fact taken, distribution has occurred." *Chiaradio*, 684 F.3d at 282. The Tenth Circuit Court of Appeals has held, citing Black's Law Dictionary, that distribute means "1. To apportion; to divide among several. 2. To arrange by class or order. 3. To deliver. 4. To spread out; to disperse." *United States v. Shaffer*, 472. F.3d 1219, 1223 (10th Cir. 2007). It also held that the defendant distributed CSAI because,

while he did not "actively push[] [CSAI] on users. . . . he freely allowed them access to his computerized stash of images and videos and openly invited them to take, or download, those items." *Id*.

The Fifth Circuit Court of Appeals has held that "downloading images and videos containing [CSAI] from a peer-to-peer computer network and storing them in a shared folder accessible to other users on the network amounts to distribution." *United States v. Richardson*, 713 F.3d 232, 236 (5th Cir. 2013). In *United States v. Husmann*, 765, F.3d 169 (3rd Cir. 2014), a case cited by the defendant, the Third Circuit Court of Appeals held that a conviction for distributing CSAI can be sustained if the State proves that the defendant placed CSAI in a "shared computer folder, available for other users of a file sharing network," if "another person actually downloaded or obtained the images stored in the shared folder." *Husmann*, 765 F.3d at 170.

The Fourth Circuit Court of Appeals held not only that "[s]everal of our sister circuits subsequently adopted the Tenth Circuit's interpretation [in *Shaffer*] and held that where files have been downloaded from the defendant's collection of [CSAI], use of a file-sharing program constitutes distribution," but also that "[n]one of our sister circuits have rejected the Tenth Circuit's position." *United States v. Stitz*, 877 F.3d 533, 538 (4th Cir. 2017). Indeed, in the six years since *Stitz*, no court has rejected the Tenth Circuit's position.

Thus, in the context of RSA 649-A:3, I(a), this Court should hold that the plain and ordinary meaning of "exchange" or "transfer," as used in the State's indictment, occurs when a defendant consciously makes CSAI

available for others to take, download, or access, and that taking, downloading, or accessing has in fact occurred.

Based on this meaning of "exchange" and "transfer," the State offered sufficient evidence that the defendant knowingly distributed CSAI six times. Specifically, the State presented sufficient evidence that the defendant understood what BitTorrent was and how it worked. He also admitted that he understood that if he had a file and someone else had a file and a third person wanted to download that file, "BitTorrent will say I'm gonna take ah part A from her, part B from, from him, part C from me and it'll just that small piece will go from each computer that has that image or that file or that game or that program and then BitTorrent will [] reassemble them." SA 144-45.

The State also proved that the BitTorrent was downloaded on the defendant's two Mac minis that had both charged and uncharged CSAI, and that the defendant had images or videos of CSAI saved on his computer, which is how Torrential Downpour was able to download the charged CSAI from the defendant's computer.

The defendant argues that there was insufficient evidence supporting his distribution convictions because the State did not prove beyond a reasonable doubt that "the defendant actually opened or viewed the charged images," or that the defendant "knew the nature of contents of the computer files," nor did the State prove beyond a reasonable doubt that the defendant knew that the CSAI was "being downloaded by another person." DB 35-38. The defendant largely relies on *United States v. Dillingham* to support these arguments. *Id*.

In *United States v. Dillingham*, the defendant was charged, in part, with distributing CSAI based on two sets of CSAI that investigators uploaded from the defendant's computer using uTorrent. 320 F.Supp. 3d 809, 812 (E.D. Va. May 29, 2018). Between June 16 2016 and June 24, 2016, investigators accessed and uploaded the CSAI described in the charge using "a law enforcement version of BitTorrent software." *Id*. at 813. When investigators seized the defendant's device, they located the CSAI in the distribution charge on the device's hard drive, and found that these images were downloaded to the defendant's computer and subsequently moved to "Trash." *Id*. at 814. The court found that the only direct evidence that the charged CSAI was on the defendant's computer in June 2016 was "the fact that [an FBI agent] was able to upload them," not that the defendant had actually opened the files. *Id*. at 816. The court also found that the defendant believed that files he downloaded through uTorrent could only be accessed by other users "'if [a user] allow[ed] that to happen." *Id*. at 817.

Despite these facts, the court held that the government introduced sufficient evidence of distribution because the government established that the defendant knew in June 2016 that "files on his computer downloaded through the uTorrent software were accessible to others within the uTorrent network and that he could therefore 'distribute' those files to others once they were downloaded." *Id*. at 818. Based on this holding, the court determined that the government did not have to prove that the defendant knew what the images were before he distributed them to investigators, he only had to know how the uTorrent software worked.

The *Dillingham* Court found that the government presented sufficient evidence to prove the distribution charge because it proved beyond a reasonable doubt that the *Dillingham* defendant understood how uTorrent allowed other users to download content stored on the defendant's device. This Court should similarly find that the State presented sufficient evidence that the defendant distributed CSAI six times because he understood how BitTorrent worked, and because an investigator successfully downloaded the six items from the defendant's device using Torrential Downpour. The State did not have to prove in this case that the defendant possessed the distributed CSAI prior to his distribution of it, nor did the State charge the defendant with possessing the distributed CSAI. *See* DAI 4 ("[RSA 649-A] not only criminalizes the distribution of [CSAI] in the actual possession of the actor but also the intentional or knowing brokering of such images in the possession of another to a third party.").

The defendant also argues that the distribution convictions must be vacated because the State failed to exclude all reasonable conclusions consistent with innocence. DB 44-46. Specifically, he argues that because the defendant told police that he did not know there was CSAI "on or downloaded from his computer as charged in the indictment," the State did not exclude the reasonable conclusion that the defendant did not commit the charged crimes. DB 46. This argument fails because this is not a reasonable conclusion based on all of the evidence presented at trial.

"An evaluation of the reasonableness of other hypotheses of innocence provides a helpful methodology for determining the existence of reasonable doubt." *State v. Germain*, 165 N.H. 350, 361 (2013) (citation and quotations omitted). "Rather, the reviewing court evaluates the

evidence in the light most favorable to the prosecution and determines whether the alternative hypothesis is sufficiently reasonable that a rational juror could not have found proof of guilt beyond a reasonable doubt." *Id*. at 361-62 (citation and quotations omitted). This Court does "not review each circumstance proved in isolation, or break the evidence into discrete pieces in an effort to establish that, when viewed in isolation, these evidentiary fragments support a reasonable hypothesis other than guilt." *Id*. at 362 citation and quotation omitted). This Court instead considers "whether the circumstances presented are consistent with guilt and inconsistent, *on the whole*, with any reasonable hypothesis of innocence." *Id*. (citation and quotation omitted).

Here, the evidence presented at trial is inconsistent with any reasonable hypothesis of innocence. While the defendant claimed that he did not know that his computer contained CSAI, the trial court, as the fact-finder, was free to reject that statement as untrue. *See State v. Carr*, 167 N.H. 264, 275 (2015) ("The [fact-finder] is free to accept or reject any portion of a witness's testimony and to resolve any conflicts in testimony. Credibility determinations are within the sole province of the [fact-finder] and will be upheld on appeal unless no rational trier of fact could have reached the same conclusion." (citations and quotations omitted)). Indeed, the trial court found parts of the defendant's police interview not credible based on the other evidence presented by the State. *See* V 10 ("He also made various denials, which given the totality of the evidence, I do not find to be credible, regarding his knowledge of what he was looking at and when he was looking at, particularly in light of the testimony from

Detective James . . . as well as the number of images recovered by Detective LaRoche . . .").

While the defendant claimed at different points in his interview that he not know that other BitTorrent users could download his downloaded files, he also explained in his interview that he knew BitTorrent could take a part of a file from his computer and other users' devices to "reassemble," or download content to another user's device. SA 144-45. The defendant also admitted to having viewed CSAI using BitTorrent before, so it was rational for the trial court, acting as the fact-finder, to conclude that the defendant knew he was downloading CSAI that he could then distribute to other BitTorrent users should they want to download the same files he saved onto his device.

Accordingly, the trial court correctly found that the State presented sufficient evidence to convict the defendant of the six distribution of CSAI charges at trial.

C. The State Presented Sufficient Evidence That The Defendant Possessed CSAI.

To find the defendant guilty of the sixteen possession of CSAI charges, the State had to prove beyond a reasonable doubt that the defendant knowingly "possessed or controlled a visual representation of a child engaging in sexually explicit conduct." DAII 8-23; RSA 649-A:3, I(a). The State also had to prove that the defendant possessed or controlled the sixteen images of CSAI described in each indictment. *Id*. At trial, the parties stipulated that the images described in the possession charges were CSAI as defined by RSA 649-A:2. DAII 24; T 4-5. Thus, the State only

needed to prove that the defendant knowingly possessed or controlled the CSAI described in each indictment.

As the trial court noted, RSA 649-A does not define possession. However, this Court has held that, when a defendant is charged at trial with possession of CSAI, "[t]he relevant inquiry thus becomes whether the defendant knowingly possessed the images, in that he exerted some control over them, or whether the presence of the images on his computer was merely inadvertent. This inquiry is a question of fact." *Clark*, 158 N.H. at 20 (citations omitted). More generally, this Court has held that to prove possession, "the State [must] prove that the defendant 'had custody of the [CSAI] and exercised dominion and control over it.'" *State v. Crie*, 154 N.H. 403, 406 (2006) (citing *State v. Smalley*, 148 N.H. 66, 68 (2002)). "A person is not guilty of an offense unless his criminal liability is based on conduct that includes a voluntary act . . . ." RSA 626:1. "Possession is a voluntary act if the possessor knowingly procured or received the thing possessed or was aware of his control thereof for a sufficient period to have been able to terminate his possession." RSA 626:1I.

Here, the State presented sufficient evidence that the defendant knowingly possessed or controlled the sixteen charged CSAI. Detective Goodyear explained that a user had to take "affirmative action" to seek out and download content onto his device. T 44. These actions included searching certain keywords to find a file to download, downloading that file, and saving the content onto a device.

When investigators forensically analyzed two of the defendant's devices, they found a "significant amount" of CSAI, including files that were named "Pre-Teen Hard Core," "12-year-old," "15-year-old," and

some from a "series" of "Russian electronic magazine[s] that featured child erotica, anywhere from preteen girls to single digits, like, eight, nine-year-old females, and that ranged from anywhere from in bathing suits, to lingeries, to nude." T 181. Investigators also determined that "many of the files on the devices had been accessed" based on "the file times." T 197.

During his police interview, the defendant said that he was a risk-taker and was curious about viewing what was "out there." SA 127. He also said that he was attracted to viewing clothed teenage models in erotic positions and that he had been diagnosed with "paraphilia," which he said meant he was attracted to the "beauty the loveliness the purity" of images of teenage models. SA 137-38, 164. He also admitted to seeing a video he had downloaded of a Russian man sexually assaulting a young girl. SA 152. He apologized if he had done anything wrong, and said that he "certainly did not want to keep anything that was incriminating." SA 189.

Based on this evidence, the trial court concluded that "the presence of [the charged CSAI] on the defendant's computer was neither inadvertent nor accidental," and concluded that "the defendant intentionally made use of the software he installed on his computer to knowingly reach out on the internet and acquire the [charged images]." DAI 4.

As this Court held in *Clark*, the State in this case did not need to prove that the defendant actually viewed the charged CSAI to prove that he possessed the charged images. In *Clark*, this Court held that the State provided sufficient evidence that the defendant possessed multiple images of CSAI when it proved at trial: (1) that the defendant communicated with a fictitious child about sending CSAI, but did not, for fear of being detected; (2) that the defendant said he would bring CSAI with him when he met the

fictitious child; and (3) that the defendant possessed additional CSAI that was saved on the defendant's hard drive and computer. *Clark*, 158 N.H. at 20-21.

Here, the State established similar evidence at trial: (1) the defendant had a substantial amount of uncharged CSAI on two of his devices; (2) he had accessed some of these files; (3) files on his device had names indicating they contained CSAI, such as "pre-teen hard core," and "twelve-year-old;" and (4) he admitted that if he downloaded and saw something that was "really bad," he would delete it, because he "did not want to keep anything that was incriminating." He also expressed an interest in child erotica, specifically clothed teenaged models in erotic positions, and he expressed a "curiosity" in the "fascination" that others had with CSAI. SA 129. He also said that he was sexually "stuck" in a teenage mindset, which is why he used BitTorrent to find images of clothed teenage models in erotic positions. SA 160. He also described viewing CSAI in the past, and claimed that once he viewed it, he deleted it. He also admitted that for him, the "perfect rose" is a "twelve-year-old." SA 164. Indeed, the girls described in the possession charges were mostly prepubescent, some of whom were estimated to be as young as five and as old as fourteen. DA II 8-23. Thus, the State admitted sufficient, circumstantial evidence that the defendant knew of the nature and presence of the images that were downloaded onto his devices, contrary to the defendant's arguments on appeal. DB 28-32.

To the extent the defendant argues on appeal that the State presented insufficient evidence that the defendant possessed the sixteen charged images on the date listed in the indictment, DB 33-34, this argument fails

because this Court has held that "under RSA 649-A:3, time is not an element of the crime." *Clark*, 158 N.H. at 21. Here, investigators found all sixteen charged images on the defendant's devices when they forensically examined them. The devices were seized on March 26, 2018, which is the date listed in the possession indictments. This, combined with the other evidence at trial as detailed above, supports the conclusion that the defendant knowingly possessed these sixteen images of CSAI within the statute of limitations and on or before the indictment date. *Id*.

The defendant also argues that the State failed to exclude any rational inference consistent with innocence relative to the possession convictions. DB 44-46. As argued above regarding the distribution charges, the evidence presented at trial regarding the defendant's possession charges is inconsistent with any reasonable hypothesis of innocence. The trial court did not credit the defendant's denials of possessing or viewing CSAI as true, given the other evidence presented at trial. V 10. The trial court also found that the defendant specifically caused the charged images to be downloaded onto his computer and knew that he possessed the charged images based, in part, on the "defendant's wide ranging and often incriminating statement to the investigating officers and that the images were readily assessable [sic] to him via a software system he had installed for that purpose on his computer." DAI 4. Because the evidence at trial supports the trial court's credibility determination, the State did exclude all other reasonable inferences consistent with innocence at trial.

Accordingly, the trial court correctly found that the State presented sufficient evidence that the defendant possessed the sixteen charged images of CSAI.

CONCLUSION

For the foregoing reasons, the State respectfully requests that this Honorable Court affirm the defendant's convictions below.

The State requests a 15-minute oral argument, delivered by Audriana Mekula, Esq.

Respectfully Submitted,

THE STATE OF NEW HAMPSHIRE

By Its Attorneys,

JOHN M. FORMELLA
ATTORNEY GENERAL

ANTHONY J. GALDIERI
SOLICITOR GENERAL

December 20, 2023

/s/ Audriana Mekula
Audriana Mekula, Bar No. 270164
Assistant Attorney General
Office of the Solicitor General
New Hampshire Department of Justice
1 Granite Place South
Concord, NH 03301

CERTIFICATE OF COMPLIANCE

I, Audriana Mekula, hereby certify that pursuant to Rule 16(11) of the New Hampshire Supreme Court Rules, this brief contains approximately 9,433 words, which is fewer than the words permitted by this Court's rules. Counsel relied upon the word count of the computer program used to prepare this brief.

December 20, 2023 *<u>/s/ Audriana Mekula</u>*
Audriana Mekula

CERTIFICATE OF SERVICE

I, Audriana Mekula, hereby certify that a copy of the State's brief shall be served on Cabot Teachout, Esq., counsel for the defendant, through the New Hampshire Supreme Court's electronic filing system.

December 20, 2023 */s/ Audriana Mekula*
Audriana Mekula