

Supreme Court of Kentucky

2012-SC-000591-DG

SAMUEL CRABTREE

APPELLANT

V.
ON REVIEW FROM COURT OF APPEALS
CASE NO. 2011-CA-000452-MR
MADISON CIRCUIT COURT NO. 09-CR-00258

COMMONWEALTH OF KENTUCKY

APPELLEE

OPINION OF THE COURT BY JUSTICE NOBLE
AFFIRMING IN PART AND REVERSING IN PART

The Appellant Samuel Crabtree was convicted of 67 counts of possession of matter portraying a sexual performance by a minor for partially downloaded child-pornography videos found on his personal computer and for still images found in an inaccessible cache on the computer. The Court of Appeals affirmed his convictions. On discretionary review, this Court concludes that the evidence related to the still images was insufficient to sustain those convictions, and thus those convictions are reversed. The proof as to the videos, however, was sufficient, and there was no other reversible error; thus those convictions are affirmed.

I. Background

In 2008, Samuel Crabtree was a student at Eastern Kentucky University. He had some cognitive impairment from multiple concussions, which slowed his decision-making, and for which the university made accommodations, including allowing him additional time on tests.

At some point, Crabtree used a peer-to-peer file-sharing program, Limewire,¹ to download images and videos from the internet. In October 2008, his computer began running slowly, and he took the computer to Resnet, a company contracted with the university to work on computers for students. A Resnet employee saw filenames that she deemed suspicious, so she contacted campus police. The responding officer did not inspect the files on the computer, but he confiscated it, obtained a search warrant, and sent it to the Kentucky State Police lab in Frankfort for examination..

When Crabtree went to retrieve his computer, he was told to contact the campus police. He immediately met with Detective Brandon Collins and agreed to talk about his laptop.

Crabtree admitted to downloading images and videos (e.g., videos showing violence) to “shock” himself, and that some of the files had been child pornography. He specifically admitted to having seen five to six still images and one video of child pornography, and stated that the video had depicted children having oral sex with an adult man. He told the detective that he felt sick upon viewing the material, knew it was wrong, and had attempted to delete the material from his computer.

He eventually wrote and signed a statement in which he admitted the following:

A while ago, out of boredom and curiosity I looked at some mature content using limewire [sic]. Limewire is a file sharing program. I

¹ Limewire is now defunct, having been enjoined from operation for copyright violations. The software coordinated connections between its users, who uploaded and downloaded files directly to and from each other. Limewire did not have central servers where files were located.

looked to find disturbing images or videos that would shock me. Some of these could be classified as child pornography. I tried to delete these things from my laptop. After a while my computer became slow and a friend told me to take it to Resnet and I did. I went to retrieve my laptop but it had been confiscated and I had a good idea of the reason why. I realize that looking at this type of stuff was wrong and I feel sick because I did look at things that I should not have looked at. However I did not realize that anyone would find out.

But Crabtree's attempt to delete the material from his laptop was not completely successful. Forensic examination revealed five videos and sixty-two still images, all pornographic, that were suspected to depict children, but did not find any trace of deleted files containing child pornography, as is often possible.² At trial, this was explained as possibly resulting from cleaning software having been run on the computer by Resnet before discovery of the suspicious files.

One of the videos was complete and was found in the Limewire "saved" folder. The remaining four videos were incomplete (their downloads had been interrupted) though they were still partially viewable. These videos were found in the Limewire "incomplete" folder.

The still images were not found in a readily accessible folder or file, but were found in the thumbcache of the computer operating system (Windows Vista). The thumbcache is a file used by the operating system to facilitate access to images and videos through the use of thumbnail images. The images in the thumbcache are separate from the original image or video files and are

² The Commonwealth's forensic expert explained that deleted files are not truly deleted but instead are "unallocated," meaning they do not appear on standard searches of the computer and do not go away until written over by another file. The unallocated files can only be retrieved by special software.

automatically generated by certain settings on the operating system when image files are on the computer.

The original still images that led to the images in the thumbnail cache were no longer on Crabtree's computer. It is impossible to know, merely from the thumbcache images, when those original images were on the computer, what the names of the files originally had been, or whether they had been seen by Crabtree. The names of the thumbnails in the thumbcache did not reflect the original file names, consisting instead of a series of characters assigned by the computer as part of the thumbnail process followed by a file extension indicating the type of file (either a .bmp or .jpg file). According to the forensic expert's testimony, the thumbcache images did not state when the original images had been saved to the hard drive, where they came from, or where on the drive (i.e., what folder) they had been saved.

Crabtree was indicted on 67 counts of possession of matter portraying a sexual performance by a minor (KRS 531.335), one count for each video and still image. The evidence at trial consisted primarily of testimony by the police officers involved and the Commonwealth's forensics expert. The jury was shown all of the still images and either still images or very short clips from the beginnings of the videos, presumably to prove that they depicted an actual sexual performance by a minor. The images and videos are not visible on the video record, having been shown to the jury just out of view of the camera on a television. In at least one instance, based on the interaction between the Commonwealth and the forensics expert, the portion of the video shown to the jury appears not to have shown a sexual act, though the expert testified,

without objection, that at the end of the video, the children in the video engaged in a sex act with an adult.

At trial, the jury instruction on each count identified the file it was based on by filename. Crabtree was acquitted of the count related to the single completely downloaded video; the jury specifically found that the person depicted in the video was not a minor.³ As to another of the videos, which showed a fully clothed girl but had a very provocative file name,⁴ the jury found him guilty of attempted possession, a misdemeanor. He was found guilty of the remaining 65 counts. He was sentenced to five years in prison for each felony count, all to run concurrently for a total of five years.

The Court of Appeals affirmed the convictions, concluding that there was sufficient evidence that Crabtree knowingly possessed the material, that Crabtree was not entitled to an innocent-possession instruction, that the jury was not improperly allowed to determine the legal meaning of various parts of KRS 531.355 (e.g., “knowingly”), that the trial court did not err in excluding positive evidence of Crabtree’s character, and that there was not cumulative error requiring reversal.

This Court granted discretionary review to address, among other things, the sufficiency of the proof and whether Crabtree was entitled to an innocent-possession jury instruction.

³ On the verdict form for each count of possession (but not those for attempt), the judge instructed the jury to determine whether Crabtree was guilty or not guilty and, separately, whether the videos showed minors. The portion of the video leading to the acquittal that was shown to the jury depicted only female genitals, without enough identifying details to discern the age of the person.

⁴ The jury instructions on this charge did not allow a finding of possession, only attempted possession.

II. Analysis

A. Sufficiency of the evidence

Crabtree's motion for a directed verdict as to all charges (except the one he was ultimately acquitted of) at the end of the proof was denied. Whether a directed verdict should have been granted, and thus whether the evidence was sufficient to support a conviction, is determined by applying the standard set out in *Commonwealth v. Benham*, 816 S.W.2d 186 (Ky. 1991). The Commonwealth's proof is assumed to be true, and the court must draw all fair and reasonable inferences from the evidence in favor of the Commonwealth. *Id.* at 187. On appeal, a reviewing court must determine "if under the evidence as a whole, it would be clearly unreasonable for a jury to find guilt." *Id.* If so, "then the defendant is entitled to a directed verdict of acquittal." *Id.* Or, as summed up in a single inquiry, "the relevant question is 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." *Jackson v. Virginia*, 443 U.S. 307, 319 (1979).

The controlling statute is KRS 531.335, which at the time⁵ read:

A person is guilty of possession of matter portraying a sexual performance by a minor when, having knowledge of its content, character, and that the sexual performance is by a minor, he or

⁵ The statute has since been amended to also criminalize intentionally viewing child pornography. See 2013 Ky. Acts ch. 41, § 5.

Crabtree's argument on appeal discussed this amendment and suggests that to the extent his conviction was based on his having viewed the videos and images, the amendment shows that his conduct was not criminal at the time. While the evidence that he viewed at least some images and a video has bearing on whether the proof overall was sufficient, whether he viewed the material, as will be seen below, is not determinative of this Court's ruling. Thus, changes to the statute are discussed only when necessary, and Crabtree's argument does not have to be addressed.

she knowingly has in his or her possession or control any matter which visually depicts an actual sexual performance by a minor person.

KRS 531.335(1). Thus, the essential elements are (1) knowingly having possession or control (2) of a visual depiction (3) of an actual sexual performance by a minor, and (4) having knowledge of its contents. The statute contains two separate mental states: the defendant must know the content of the images and videos (i.e., that they depict a sexual performance by a minor) and the defendant must knowingly possess the images or videos. Crabtree's argument goes primarily to whether he knowingly possessed or controlled the images and videos.

The evidence related to the videos and the still images differed and thus they are addressed separately.

1. Crabtree was not entitled to a directed verdict on the charges related to the videos.

As noted above, Crabtree was acquitted of one count related to the videos, convicted of three other counts, and convicted of criminal attempt as to yet another count. The videos for which he was convicted were incomplete but were still playable to some extent.

There is no question that the videos leading to the possession convictions met the elements of a visual depiction of an actual sexual performance by a minor. Those videos were child pornography.

The question at issue is whether the proof actually showed, directly or by implication, that Crabtree knew the videos were child pornography and.

whether he knowingly possessed them. The burden is on the Commonwealth to prove both mental states.

First, whether Crabtree had knowledge of the content of the videos is a close question. The Commonwealth's proof focused on the filenames of the videos, which, according to a forensic expert, included various known buzzwords or code words (such as "r@gold," "brazilkids," and "pthc") used to indicate to those in the know that the files contain child pornography. The filenames also contained language, such as "illegal underage Lolita preteen pedo" and "baby rape," that was indicative of their content even to those unfamiliar with buzzwords.

The Commonwealth's forensics expert testified that files are found on Limewire through the use of search terms,⁶ and while she did not know which ones were used here, files are returned in a search only when the search term used shows up in the file name or its metadata (there was no testimony about whether metadata was found in the files in this case). Thus, a search using one of the buzzwords or terms clearly related to child pornography will only turn up files with those terms in the file name or metadata (though the files would not necessarily contain child pornography). And even Crabtree's witness admitted that a Limewire user would see the provocative filenames before downloading the files.

The Commonwealth's expert further testified that to search for child pornography, people usually use the buzz words as search terms, though she

⁶ Though Limewire is now defunct, we discuss how it operates in the present tense to improve clarity.

had seen the term “child pornography” used directly as a search term. To download a file from the list of Limewire search results, the user would click on a file name; the software would then ask whether the user wanted to download the file and, to do so, he would have to click “yes.”

Both the Commonwealth’s forensic expert and Crabtree’s “expert”⁷ testified, however, that an innocent search could also turn up child pornography, such as a search for “Michael Jackson’s Thriller.” However, given the actual names of the files on Crabtree’s computer, both testified that he would have seen those file names before downloading the files. The forensic expert also testified that another Limewire user could not simply send another user a file, as with email, which simply arrives on one’s computer.

Instead, she reiterated, the user would have to search for a term appearing in the filename or description, and then initiate the download and confirm it (clicking “yes”), which is a two-step process. She testified that the version of Limewire Crabtree had used *required* the two-step process (whereas some versions may not have). In short, files could not be downloaded without the user taking the affirmative steps to initiate and confirm the start of the download. Another Limewire user could not have pushed files into Crabtree’s computer without his participation. The Commonwealth’s forensic expert also testified that her review of the literature had not shown instances where viruses and other malware put child pornography on a person’s computer.

⁷ Crabtree’s “expert” was an acquaintance of his who had been a regular user of Limewire. He testified how the software worked based on his experience using it.

The Commonwealth offered no proof of the actual searches conducted by Crabtree. Either the version of Limewire on his computer did not keep such a history, or that history had been deleted somehow.⁸

Given the filenames in question, there is little doubt that a person downloading such files *expects* them to contain child pornography. Each video filename contained language that would leave little doubt as to its expected content (and, as it turned out with respect to three of the videos, their actual content).

This proof established at least constructive knowledge of the content of the videos as Crabtree had to have seen their filenames. *See Newman v. Conover*, 313 F.Supp. 623, 630 (N.D.Tex. 1970) (defining “constructive knowledge” as “knowledge of facts which would put a reasonable and prudent man on notice as to the suspected nature of the material”). But more is required to establish the *mens rea* of “knowingly.” As Professors Lawson and Fortune have stated “[i]t is widely accepted that this culpable mental state does not exist when an individual has no belief in the existence of a fact or circumstance but has information that would have caused a reasonable person to believe in the existence of that fact or circumstance.” Robert G. Lawson & William H. Fortune, *Kentucky Criminal Law* § 2-2(c)(1), at 45 (1998). In other words, merely negligently possessing child pornography is not a crime under

⁸ There was no suggestion that Crabtree himself deleted his searches, if they were ever saved. He at most stated that he tried to delete the child pornography files he had seen. The Commonwealth’s forensics expert, however, testified that Resnet had run a cleaning software on the computer when it was first brought in (and before the suspicious filenames were seen), and that the cleaning software may have affected data on the computer, such as deleted or “unallocated” files (making them unrecoverable) and lists of recently used files. It stands to reason that this software could also have affected a search history.

the statute. *Id.* Rather, “the culpability involved in this mental state is described in a single word—*awareness.*” *Id.*

The question then is whether there was evidence to support a finding that Crabtree was aware of the nature of the material in the files on his computer. The Commonwealth presented no proof that Crabtree watched the videos that served as the bases of the charges for which he was convicted, which would have established such awareness. And while Crabtree admitted to the police that he had watched one video, the proof did not show that that video was one of the videos he was ultimately charged with possessing.⁹ Also, while independent proof showed that one of the videos had been watched, Crabtree was acquitted of the charge related to that video.

However, knowledge can also be “based on factors other than personal observation, such as information provided by credible observers.” Robert G. Lawson, *Kentucky Penal Code: The Culpable Mental States and Related Matters*, 61 Ky. L.J. 657, 664 (1972–73). Thus, if someone else had watched the videos on the computer and told Crabtree of their content, he would have knowledge of their content. There was no direct proof that anyone else watched the videos

⁹ Crabtree’s brief suggests that the charge of which he was acquitted was the video he admitted to having watched. This may be possible, but the description of that video as shown to the jury (depicting only genitals from which age could not be determined) differed from the description Crabtree gave of the video he watched. Although evidence showed that the video of genitals was viewed, it could have been a different video from the one Crabtree admitted to having viewed. Indeed, defense counsel argued in closing that the video Crabtree admitted having seen was not one of the videos presented to the jury. On the other hand, since it appears that the Commonwealth showed only a portion of the video to the jury, it is possible that the sequence Crabtree described to the police appeared later in the video. If that was the case, then it could have been the same video.

on Crabtree's computer, much less that they told Crabtree about the videos' content.

But the file names are evidence that someone at some point viewed the files, saw that they were child pornography, and labeled them as such. The titles were then communicated to Crabtree when he searched for whatever he searched for and saw the filenames. This clearly informed him of what the files contained.

And direct proof of knowledge is not necessary. "[P]roof of actual knowledge can be by circumstantial evidence." *Love v. Commonwealth*, 55 S.W.3d 816, 825 (Ky. 2001). Thus, "proof of circumstances that would cause a reasonable person to believe or know of the existence of a fact is evidence upon which a jury might base a finding of full knowledge of the existence of that fact." *Id.* (quoting *Lawson & Fortune, supra*, § 2-2(c)(1), at 45).¹⁰ The circumstantial evidence of Crabtree's knowledge of the content of the files

¹⁰ This differs from constructive knowledge in that the nature of the files is communicated to the defendant, which would justify a jury inference that the defendant had knowledge, rather than the defendant merely being on notice of the nature of the files from the circumstances. A much broader definition of knowledge was originally proposed to the General Assembly; under it, "awareness of highly suspicious circumstances would have been sufficient for conviction in the absence of an actual belief by an offender contrary to the suspicion." *Lawson, supra*, at 665 n.3. But this definition was rejected. *Id.* Under the version of the statute actually adopted, the current version, "this type of mental awareness would serve only to support an inference by [the jury] that the offender had the requisite knowledge for conviction." *Id.* Thus,

it has always been held that the proof of receiving goods under circumstances that would cause a reasonable man of ordinary observation to believe or to morally know that they were stolen constitutes evidence from which a jury is authorized to infer and to find that the recipient of stolen goods had full knowledge of their character, and hence a conviction of guilty knowledge may be sustained by circumstantial evidence.

Id. (quoting *Ellison v. Commonwealth*, 190 Ky. 305, 227 S.W. 458, 461 (1921)).

included his own statement that he had watched a child-pornography video from among his downloads. This buttressed the fact that the file names were reliable indicators of the content of the other videos that he downloaded in part.

The direct evidence of the filenames of the videos, along with the circumstantial proof that he admitted viewing one child pornography video, even if it was not one of the charged videos, taken together, were evidence from which a jury could infer that Crabtree knowingly partially downloaded files that contained child pornography.¹¹ As to this point, there was sufficient evidence to submit the case to the jury.

But we must also determine whether the Commonwealth proved the other knowledge element, i.e., that Crabtree *knowingly possessed* the videos. This question relates more to the proof about *how* he obtained the videos.

Unlike the completely downloaded video in the Limewire saved folder, for which

¹¹ The filenames are also the key to understanding why the trial court ultimately instructed on one count of criminal attempt without a higher possession charge. Though the video giving rise to that charge ultimately turned out not to contain child pornography (since the child in it was fully clothed), it would be reasonable to infer that a person downloading a video with that filename had taken a substantial step toward possessing child pornography and had intended to possess child pornography, and thus had committed criminal attempt. Thus, for example, a person who sells a bag of powder containing baby powder believing it is cocaine has attempted to traffic in a controlled substance. *See People v. Culligan*, 434 N.Y.S.2d 546, 546 (N.Y. App. Div. 1980). A mistake as to the ultimate content of the video does not bar conviction for criminal attempt where the name of the video unmistakably suggests its expected content. That proof, along with proof that the defendant voluntarily downloaded the video, shows that the defendant “[i]ntentionally engage[d] in conduct which would constitute the crime if the attendant circumstances were as he believe[d] them to be,” KRS 506.010(1)(a), which is sufficient to establish criminal attempt. It also shows that he “[i]ntentionally d[id] ... anything which, under the circumstances as he believe[d] them to be, [wa]s a substantial step in a course of conduct planned to culminate in his commission of the crime,” KRS 506.010(1)(b), which is another way to commit criminal attempt. Thus, the proof with respect to that charge, though not directly attacked in the brief, was sufficient.

he was not convicted, the videos for which Crabtree was convicted were not completely downloaded and were in a different folder (the “incomplete” folder). The Commonwealth’s forensics expert testified that while a file was being downloaded, the data was temporarily stored in the incomplete folder, and that when the download was complete, Limewire would automatically move the file to the saved folder. The files in this case were still in the incomplete folder because their downloads had been interrupted, which could have happened for any of several reasons, including that the person uploading the file (i.e., the Limewire user from whom Crabtree was downloading the file) had stopped it, that the internet connection had dropped, or that Crabtree had stopped the download himself. The expert could not state which of these had happened.

At the very least, this proof, combined with the proof of how a person finds files to download on Limewire, what the person sees before beginning a download (i.e., file names), and the steps required to begin downloading them, shows that Crabtree attempted to download and possess child pornography. He had taken a substantial step toward securing those files and had acted with the kind of culpability required for commission of the crime (i.e., knowledge of the contents of the files and, upon successful download, knowing possession). That suffices to prove criminal attempt under KRS 506.010(1)(b). In fact, the jury was instructed on criminal attempt as a possible lesser-included offense as to the three child-pornography videos in the temporary folder (and instructed only on attempt as to the video of the clothed child).

But this proof can also show that Crabtree knowingly possessed the incomplete videos found on his computer. Crabtree suggests that the

Commonwealth was required to show that he viewed the videos before it could prove he knowingly possessed them. But this is not necessary to secure a conviction.

The proof that Crabtree chose files with names clearly indicative of child pornography and clicked on these files to start their downloads demonstrated knowing possession. It would be reasonable for the jury to infer that Crabtree knowingly possessed a partial file from the instant he began the download. The jury could have believed that he knew he was receiving and thus possessing each new bit of the child pornography file as it was downloaded.

To illustrate, when a person orders an old-fashioned reel of celluloid film of clearly labeled child pornography that ends up being shipped frame by frame (perhaps in an effort to avoid detection by the police) to be reassembled by the recipient, the offense is completed upon receipt of the first frame; possession of the entire reel of film is unnecessary. If the images of pornography in the partial downloads were knowingly received by Crabtree, which the evidence supports, they were possessed.

One of the purposes of file-sharing software like Limewire is to download and then possess files. Though not the issue here, the Eighth Circuit has said with respect to the other purpose of such software, the distribution of files:

One can hypothesize, as defense counsel has vigorously argued, that even a defendant who pleaded guilty to knowing receipt and possession might have no knowledge that his computer was equipped to distribute. But the purpose of a file sharing program is to share, in other words, to distribute. Absent concrete *evidence* of ignorance—evidence that is needed because ignorance is entirely counterintuitive—a fact-finder may reasonably infer that the defendant knowingly employed a file sharing program for its intended purpose.

United States v. Dodd, 598 F.3d 449, 451-53 (8th Cir. 2010). The same inference is available here with respect to downloading and possessing files.

Crabtree cites cases holding that images stored on a computer through various automatic caching functions are not necessarily knowingly possessed. For example, he cites *United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011), in which the court held that image files stored in an automatically generated temporary cache for a web browser upon viewing an original image were not knowingly received unless the defendant knew of the automatic-caching function. (The defendant was charged with knowingly receiving child pornography instead of knowing possession.) The Court specifically noted that the evidence showed the defendant received the files, because they were on his computer, but “for this evidence to be probative of the question of *knowing* receipt, the government needed to present proof that [the defendant] at least knew of the automatic-caching process.” *Id.* at 1205. The court went on to distinguish other cases in which the proof showed, albeit circumstantially, that the defendant had knowledge of the automatic processes.

But this case is clearly distinguishable. Here it suffices to show that Crabtree knew that the software was used to download files, and that he started downloading files that he knew contained child pornography. The download of video files via a file-sharing program like Limewire is not instantaneous. The time of the download depends on the size of the file and the overall download speed. The bits have to go somewhere—and that can only be on the computer being used to download the file. Also, these videos ended up on Crabtree’s computer through a different process than the files in *Dobbs*.

At least as to the videos, this case is more like *United States v. Figueroa-Lugo*, 915 F. Supp. 2d 237 (D.P.R. 2013), which involved the use of Limewire and, in part, incompletely downloaded videos. The district court in that case held: “In contrast [to *Dobbs*], the ... videos in this case were not found via a caching function that was unknown to [the] defendant Rather, the files were found stored in the hard drive of [the] defendant[’s] ... personal computer in folders related to software that requires a user specifically to request for items to be downloaded.” *Id.* at 243–44. The court concluded that the proof was sufficient to prove that the defendant knowingly possessed the child pornography on his computer, including the partially downloaded files. *Id.* at 244.

And Crabtree admitted that he had actually downloaded files from Limewire, thus establishing that he had knowledge of the process necessary to obtain such files. This is sufficient to answer the question “whether a reasonable jury, on this record, could have rationally concluded that [the] defendant ... knew ‘that his own computer contained such files.’” *Id.* (quoting *United States v. Salva-Morales*, 660 F.3d 72, 75 (1st Cir. 2011)). Certainly, it could.

The simple fact is “that a person does knowingly receive and possess child pornography [videos] when he seeks them out over the internet and then downloads them to his computer.” *United States v. Kuchinski*, 469 F.3d 853, 861 (9th Cir. 2006). There is no proof that Crabtree began downloading the files innocently, for example, by searching for music or legal adult pornography; there was only proof that he *could* have obtained child

pornography in that way. But the evidence showed that he did not obtain the files in that way.

The filenames, which Crabtree would had to have clicked to start the downloads, were obviously indicative of child pornography. Even if the files had been returned in an innocent search, their filenames were a clear giveaway of their contents. Nevertheless, Crabtree began those downloads anyway. As soon as any of the data arrived on his computer, Crabtree could be found to have completed the offense of possessing matter portraying a sexual performance by a minor, even though the rest of the data had yet to be received.

Nor is it a defense that Crabtree was looking for shocking videos when he stumbled on the child pornography videos. That does not excuse his subsequent actions of beginning to download the videos, nor does it change his mental state. No person with an understanding of English would have seen these video titles and believed they contained anything other than child pornography. (And there is no suggestion that Crabtree did not understand English.)

Likewise, that he may not have downloaded the videos for sexual gratification does not matter as that fact does not undermine the mental state that established the crime. Although the General Assembly has limited other crimes by including the requirement that certain acts be for the purpose of sexual gratification, *see, e.g.*, KRS 510.110-.130 (criminalizing various degrees of non-consensual sexual touching “done *for the purpose of gratifying the sexual desire* of either party,” 510.010(7) (emphasis added)), this offense is not one of them. The crime requires only the knowing possessing of child

pornography, regardless of the purpose. The *mens rea* requirements of KRS 531.355 are satisfied by showing that the defendant knew the videos were child pornography and that he knowingly possessed them.

The Commonwealth met that burden as to the videos here, and Crabtree was not entitled to a directed verdict. His convictions for possession of the videos are affirmed.

2. The evidence was insufficient to show knowing possession of the still images.

The evidence surrounding the still images found on Crabtree's computer differs substantially from that of the videos. Crabtree's argument on appeal focuses primarily on these files.

As noted above, the still images were not found in an ordinary, user-accessible folder on the computer; they were instead found in the operating system's thumbcache. The Commonwealth's forensics expert testified at trial that the thumbcache allows for the quicker display of images without having to load them from the hard drive each time, and works as an index of images and videos. Using thumbnails is an option that the user can choose; if the thumbnail option is turned on for a folder of images or videos, a small image (a "thumbnail"), rather than just a file name, will appear for each file in the folder. The thumbnail is a smaller version of the image or the first frame of a video, and serves as a preview of the original file. Separate thumbnail images are automatically generated in the thumbcache, which is a separate file.

The forensics expert testified that the image appears in the thumbcache only when the original image "is viewed as a thumbnail," and that the image in

the thumbcache is separate from the original image file. Thumbcache images are not deleted when the original file is deleted, and the images contained in the cache are not readily accessible to the average user but instead require special software to view. The expert testified, however, that if an image is in the thumbcache, it has been “viewed as a thumbnail.” When later recalled by the defense, she clarified that the thumbcache image is generated whenever a file in a folder is put in the thumbnail view but that she could not tell from that fact that a given image had been seen by a user of the computer.

Specifically, she could not say who viewed the pictures on Crabtree’s computer or when they were viewed. She did not know what search terms were used to find them because the original file names were not available. She could not even say that the images were downloaded with Limewire, though there were no traces that other programs, such as a web browser, had been used to get the images, and Crabtree’s statements to police indicated that he had used Limewire to obtain the files on his computer. The expert did testify, however, that the images were viewed on Crabtree’s user account on the computer.¹²

The original images that led to the thumbcache images were not found on Crabtree’s computer, though they had to have been there at one time. In fact, no trace of the original images, aside from the thumbcache, could be found, even with the use of specialized forensic software that can show files that users believe they have deleted (but which are still on the computer in

¹² According to the expert, the operating system on the computer allowed individual user accounts, which can be protected by a password, allowing multiple people to use the same computer at different times without encountering each other’s data. She also testified that each account has its own thumbcache.

unallocated space until overwritten). The expert testified that a cleaner program had been run on the computer as part of the work by Resnet and the effect of that program would have been to erase forensic traces (such as seemingly deleted files in unallocated space).

The question is whether proof of the existence of the 65 still images in the thumbcache was sufficient to prove that Crabtree knowingly possessed still images of child pornography and knew of their content.

To the extent that the charges were based on Crabtree's possessing the thumbcache images themselves, the proof necessarily fails. There was no evidence that Crabtree knew of the existence of the thumbcache or could access the thumbcache. The images in the thumbcache were there because of an automatic function of the computer itself. Crabtree did not place the images in the thumbcache.

Like the automatically generated cache images in *United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011), the thumbcache images are evidence of possession of child pornography, but they are not evidence of *knowing* possession without additional proof that Crabtree "at least knew of the automatic-caching process." *Id.* at 1204. This differs significantly from the video files, which required affirmative steps including reading the incriminating filenames to download the video, and for which proof of the incriminating filenames was available.

The Ninth Circuit has addressed this scenario concerning the pictures and concluded that a person with no knowledge of the caching process does not even *possess* the files in question:

Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images. To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control.

United States v. Kuchinski, 469 F.3d 853, 863 (9th Cir. 2006).

In fact, in several instances where the federal courts¹³ have affirmed child pornography convictions, they have focused at least in part on the defendant's knowledge of the computer's processes to establish knowing possession or receipt. For example, in *United States v. Romm*, 455 F.3d 990, 995 (9th Cir. 2006), the evidence demonstrated that the defendant knew about the cache files and had actually taken steps to access and delete them, and on appeal, he conceded knowledge, contesting instead dominion and control. *Id.* at 995–98. In affirming the conviction, the court pointed out that “to possess the images in the cache, the defendant must, at a minimum, know that the unlawful images are stored on a disk or other tangible material in his possession.” *Id.* at 1000.

¹³ We rely on federal cases not because they have applied and interpreted our statutes but because the elements in the federal child pornography statutes are similar to the Kentucky statutes in that they require knowing possession or receipt of the images. Moreover, so many child-pornography prosecutions are in federal court, rather than state court, that the federal decisions are the primary source of precedent on the subject. One important difference, however, is that the federal prosecutions group all the images and videos together into a single count. *See, e.g., United States v. Kain*, 589 F.3d 945, 947 (8th Cir. 2009) (defendant prosecuted for only one count of possession of child pornography despite having more than 20 images). The number of images possessed appears to be relevant in determining the defendant's sentence under the Federal Sentencing Guidelines. *See id.* at 952 (discussing application of the sentencing guidelines to possession of 27 images). Apparently, however, defendant may be separately charged with and convicted of both knowingly receiving and knowingly possessing child pornography. *See, e.g., United States v. Romm*, 455 F.3d 990, 993 (9th Cir. 2006).

Also, in *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002), the Tenth Circuit declared that the defendant was properly found guilty where he knew that child pornography images would be sent to his “browser cache file and thus saved on his hard drive.” *Id.* at 1204. The court noted that the defendant “intentionally sought out and viewed child pornography knowing that the images would be saved on his computer,” and that he “may have wished that his Web browser did not automatically cache viewed images on his computer's hard drive, but he concedes he knew the web browser was doing so.” *Id.* at 1205.

There was no proof that Crabtree knew the thumbcache images existed. His convictions, therefore, cannot be for knowingly possessing those images.

As the Commonwealth noted at trial, however, the images in the thumbcache were circumstantial evidence of Crabtree’s prior possession of the original image files. *See United States v. Kain*, 589 F.3d 945, 950 (8th Cir. 2009) (“The presence of child pornography in temporary internet and orphan files on a computer's hard drive is evidence of prior possession of that pornography, though of course it is not conclusive evidence of knowing possession and control of the images, just as mere presence in a car from which the police recover contraband does not, without more, establish actual or constructive possession of the contraband by a passenger.”).

At the time the original images are downloaded (and the thumbcache image is created), the defendant possesses the image. That the original download occurred, even though the images are later deleted, is shown indirectly by the persistence of the thumbcache images. Those images show

that at some point in the past, the defendant possessed the original images. The thumbcache is evidence of a previous possession just as a fingerprint can be evidence of a defendant's earlier presence at a crime scene.

The Commonwealth's burden, however, is not merely to show that Crabtree literally had the original images on his computer but to show he *knowingly* possessed them. In other words, although the thumbcache is evidence of prior possession (at least in some sense), is it evidence of knowing prior possession of the original images?

By itself, it is not. There are numerous reasons why those images could have been on Crabtree's computer. For example, they could have been the product of an innocent search on Limewire that happened to return results containing child pornography. The expert for the Commonwealth testified that, for example, a search for picture files using the term "beagle puppy" could return a file that nonetheless contained child pornography. While an innocent search will not turn up the buzz words for child pornography, sometimes an innocent search term such as "puppy" could be included on child pornography files or in its metadata. There was also testimony that files on Limewire and similar services are frequently misnamed and that the content of the files did not always match the descriptions. Thus, child pornography files could appear in the results of searches using innocent terms, and child pornography files could have innocent names. A person downloading such a file would have no idea that it contains child pornography until opening and viewing it.

Given the evidence in this case that files on Limewire were frequently mislabeled, it is possible that Crabtree downloaded a file that appeared, based

on its filename, to contain legal images but turned out to contain child-pornography images.

The problem is that the Commonwealth had no evidence related to the source of the original files, what their names were, or anything. In fact, that the original images are no longer on the computer is equally consistent with Crabtree's innocence, i.e., that he unknowingly downloaded the images and deleted them as soon as he knew what they were.

In the federal cases affirming possession convictions, there is more proof about how the defendant acquired and handled the original images. For example, in *Romm*, the defendant claimed that he had not downloaded the images, in the sense of manually saving them to his computer, and instead had only viewed them online through his web browser. 455 F.3d at 993. The court held that “[i]n the electronic context, a person can receive and possess child pornography without downloading it, if he or she seeks it out and exercises dominion and control over it.” *Id.* at 998.

And, in affirming a conviction for possession based on images in a temporary web-browser cache, the court noted that the defendant knew the images had been saved in his cache; that the defendant had “repeatedly sought out child pornography over the internet,” *id.* at 1000; that he had admitted to saving and downloading the images, despite claiming on appeal to having only viewed them; and that he had admitted to viewing (and, in some cases, enlarging) the images for up to five minutes before deleting them, *id.* The court also noted that the defendant’s “ability to control the images while they were displayed on screen, and the forensic and other evidence that he actually

exercised this control over them, ... [c]oupled with [his] conceded knowledge that the images were saved to his disk,” *id.* at 1005, were sufficient evidence to support the conviction.

Similarly, in the main case relied on by the Commonwealth on appeal, *United States v. Kain*, 589 F.3d 945 (8th Cir. 2009), some of the images found on the defendant’s computer were in temporary internet files or had been deleted (and thus were “orphan” files), but more than 20 other readily viewable images were found saved in a desktop folder labeled only “Y.” *Id.* at 949. The government produced evidence that the defendant admitted he had saved child pornography to the “Y” file, that he had accessed child-pornography websites, and that his saved images were associated with those websites. *Id.* at 950. The defendant also admitted that he “had used [the computer] to download 40–50 images of child pornography to the ‘Y’ file.” *Id.* at 949. When told that 405 images had been found on the computer, the defendant “responded, ‘[i]f they found 405 images, then there were 405 images on the computer.’” *Id.* (alteration in original).

Here, there was no direct evidence of how Crabtree obtained the still images. His own statement suggests that he got *some* child pornographic images from Limewire, but there is no proof that these were the same images. There is no proof that he sought out *these* still images—e.g., by finding their filenames with child-pornography terms and then downloading them. That proof simply was not available to the Commonwealth.

Crabtree’s own statement was that he was seeking out shocking images, not child pornography, and that in the course of seeking shocking images, he

had seen images that could be considered child pornography. But that statement could easily be accounted for by his having downloaded a file with a name indicative of shocking content (e.g., one of the videos of journalists murdered in the Middle East recently put on the internet) that turned out to contain child pornography instead.

And there was insufficient proof that Crabtree had viewed and exercised control over the images in the way the defendant in *Romm* had, for example, by viewing them for several minutes or enlarging them. The Commonwealth's expert testified only that the thumbcache images had been generated by the thumbcache process. While she stated at times that this meant that the images had been "viewed as thumbnails," she also noted that this was an automatic process and did not necessarily mean the images had been seen. This is consistent with Crabtree's own statement that he had seen five or six still images before becoming disgusted and deleting the content. Indeed, for anyone familiar with computers, it is easy to see how a series of more than sixty images could be in a single folder, all with thumbnails ready for viewing (and with consequent images in the thumbcache), yet most of those images are never seen because the user does not scroll down through all of the folder. Although the images are in the folder, and thus are "viewed as a thumbnail," possibly only a few are displayed on the screen. Crabtree cannot be said to have viewed—and thus exercised control—over those images. To so conclude would be mere speculation.

The remaining analysis, then, is whether the evidence related to the videos discussed above was sufficient circumstantial proof from which knowing

possession of the separate still images could be inferred. The jury heard that Crabtree had to have seen the child-pornography terms in the file names of the videos he partially downloaded, and that he had used Limewire to obtain videos and other files. The jury also heard proof that Crabtree used Limewire to obtain still images.¹⁴ But does that proof create a sufficient link to establish that these pictures were obtained in this manner?

Again, the federal courts give us examples for comparison. In *Dobbs*, the defendant was charged with knowing possession of two images that were found in his Web browser temporary cache and which “were banner images, comprised of multiple, smaller images, measuring 3.25 inches by .5 inch.” 629 F.3d at 1201–02. The government offered proof that the defendant had repeatedly searched for terms consistent with child pornography and had visited child-pornography websites. *Id.* at 1201. Nevertheless, the court concluded that the evidence was insufficient to show knowing receipt of the two images. *Id.* at 1204.

The government posited that the defendant’s search activity and visits to child-pornography websites were circumstantial proof of knowing receipt of the charged images, but the court rejected that reasoning because the proof showed no search that had been done contemporaneously with the saving of the charged images, and thus ““the pattern of child-pornography-related searches immediately preceding the creation of illegal images in the cache ...

¹⁴ Crabtree’s counsel cross-examined the police with the search warrant affidavit and ultimately introduced that document into evidence. The affidavit noted that Crabtree admitted that he had used Limewire to download the six still images that he admitted viewing.

d[id] not apply to the two images submitted to the jury.” *Id.* The court also noted that there was no “indication that [the defendant] visited suspect websites prior to [the images]’ arrival in his cache.” *Id.*

Similarly, in *United States v. Keefer*, 405 F. App’x 955, 958 (6th Cir. 2010), the court refused to allow proof of the defendant’s knowing possession of seven images to show that he also knowingly possessed more than 1,200 other images in “unallocated” space on the computer. The defendant was charged because he had sent seven child pornography images to a law enforcement officer over the internet. When his computer was searched, 1,215 child pornography images, including the seven transmitted files, were found in the unallocated space on the computer. The proof showed that files in unallocated space had been deleted, but that they could have been deleted by the user or by the computer.

The numerous files were not used to convict the defendant but were instead used to enhance his offense level for sentencing purposes. The court noted that sentencing enhancements needed only to “be proven by a preponderance of evidence,” *id.* at 957, but nevertheless reversed the sentence, stating that “the fact that at one point [the defendant] knowingly possessed seven of the 1,215 images (the ones he sent to the detective in Florida) is not adequate to support a finding that he ever knowingly possessed or knowingly accessed with intent to view the other 1,208 images,” *id.* at 958. The court noted that the proof established only that the images “were *present* on [the] computer at some point,” *id.*, and that their “[p]resence ... d[id] not inherently require knowing possession or access, as anyone who has received spam email

or visited one website only to have another, inadvertently accessed, website pop-up knows all too well,” *id.*

From these cases, it is clear that there must be an evidentiary nexus between the evidence that could show knowledge and the illegal images found on the computer. Here, the evidence that could show Crabtree’s knowledge—his possession of the videos, the circumstances of their acquisition, and his statement that he used Limewire to download files—does not have a sufficient evidentiary nexus with the images actually found in the thumbcache (or the original images that must have led to the creation of the thumbcache images).

As we have stated: “Circumstantial evidence has its limits.”

Commonwealth v. Goss, 428 S.W.3d 619, 626 (Ky. 2014). The “proof ‘must do more than point the finger of suspicion.’” *Id.* (quoting *Rogers v. Commonwealth*, 315 S.W.3d 303, 311 (Ky. 2010)). Moreover, “[a] conviction obtained by circumstantial evidence cannot be sustained ‘if [the evidence] is as consistent with innocence as with guilt.’” *Id.* (quoting *Collinsworth v. Commonwealth*, 476 S.W.2d 201, 202 (Ky. 1972)).

The Commonwealth here had no direct proof as to when the original still images were acquired, whether they had provocative filenames, or whether they were viewed by Crabtree. That at some point Crabtree began but failed to complete downloads of video files with names clearly indicative of child pornography, while sufficient to show knowing possession of those files, does not mean he also knowingly downloaded and possessed the still images. That is an inference too far. The proof is equally consistent with Crabtree having accidentally received the still images while searching for shocking, but legal,

content, as it is with his guilt. (As discussed below, accidental possession is not a crime unless the person decides to keep the material.) While the Commonwealth is not required to dispel all possibilities to make its case, it must do more than leave the evidence in equipoise.

The failure of proof in this case was not the Commonwealth's fault. It is likely that the lack of proof was the unintended result of the very circumstances that led to the discovery of the material on the computer in the first place: the work on the computer by Resnet. As the Commonwealth's expert testified, a cleaner program had been run on the computer as part of that work and the effect of that program could have been to erase forensic traces (such as seemingly deleted files in unallocated space or evidence that images had recently been viewed or videos had been watched) that might have shown knowledge on Crabtree's part.

That missing proof, however, could very well support Crabtree's own theory that he was looking only for shocking videos, had inadvertently downloaded the still child-pornography images in the process, and immediately deleted the images upon discovering their true nature. In essence, Resnet's inadvertent deletion of data from the computer in the course of trying to fix it may have turned the circumstances surrounding the still images into a black box or blind spot, where the outcomes are known (images in the thumbcache) but the processes leading to them cannot be known and may only be speculated at.

Nevertheless, we cannot affirm a conviction based purely on speculation. That there *may* at one time have been sufficient proof that Crabtree knew the

still images were on the computer is insufficient, by itself, to uphold his convictions for the still images. The Commonwealth has the burden to prove that the defendant, in fact, committed the crime, not that he may have committed the crime. The evidence here and reasonable inference from it show only that Crabtree *may* have known that he had still images of child pornography on his computer.

For that reason, his convictions for possessing the still images must be reversed.

B. Crabtree was not entitled to an innocent-possession instruction.

Crabtree also argues that he was entitled to an innocent-possession instruction under *Commonwealth v. Adkins*, 331 S.W.3d 260 (Ky. 2011), which required an innocent-possession instruction in a drug-trafficking case. He claims that because there was evidence that he temporarily possessed the child-pornography files and attempted to dispose of them as soon as he discovered their content, he should have been given the instruction. Because we have reversed his convictions relating to the still pictures, analysis of this claim applies only to his convictions for possession of the videos. This Court concludes that he was not entitled to an innocent-possession instruction on the videos.

In *Adkins*, the defendant was discovered with a sock in his pocket containing two plastic baggies with almost 17 grams of methamphetamine, two straws for snorting or smoking the drug, and several other unused plastic baggies. *Id.* at 261. He was charged with first-degree trafficking in methamphetamine, which required proof that he “knowingly and unlawfully

traffic[ked] in ... [t]wo ... grams or more of ... methamphetamine.” KRS 218A.1412(1)(b). The defendant conceded that he possessed the drugs and other items but claimed that he had no intent to traffic. 331 S.W.3d at 262. He claimed “that a short time before his arrest, he found the sock lying in the driveway that serves both his and his brother's residences and placed it into his pocket to keep it away from his young son.” *Id.* He also claimed that “he believed [the sock] had been dropped by one of his brother's acquaintances, a reputed drug dealer,” and that he had “attempted to report it to the sheriff by phone.” *Id.* He presented testimony from himself and some friends that the brother's acquaintance had been at his brother's home earlier that day and that they had seen a small object fall from the acquaintance's truck as he left the driveway. *Id.* The defendant also “testified that when he was unable to contact the sheriff by phone he intended to turn the drugs in at the sheriff's office and to report his suspicions about his brother's acquaintance.” *Id.*

This Court concluded that the trafficking statute under which the defendant was charged “implicitly recognize[d] an innocent possession or innocent trafficking defense,” *id.* at 264, because it, like all the other possession and trafficking statutes, required that possession of the drug be both “knowing and *unlawful*,” *id.* That the crime occurs only when the possession is unlawful necessarily implies that under some circumstances, possession of controlled substances could be lawful.

Thus, we concluded that the drug-trafficking and drug-possession statutes “recognize[] the possibility of innocent, incidental possession or transfer, and thus allow[] for a defense of innocent possession where there is

evidence that the possession came about incidentally and continued no longer than reasonably necessary to allow for lawful and appropriate disposal.” *Id.* at 267. We also recognized that “the instructions should expressly reflect a statutory defense if there is evidence reasonably supporting it,” *id.* at 265, and that in Adkins’s case, the proof did support such an instruction.

This Court also noted that this implicit defense was confirmed by KRS 218A.220, which expressly “exempts from the controlled substance prohibitions persons engaged in the lawful storing or transporting of such substances, public officials and their employees and agents whose duties require possession of them, and ... persons whose ‘temporary incidental possession ... is for the purpose of aiding public officers in performing their official duties.’” *Id.* (quoting KRS 218A.220). We concluded that this statute protects “citizens who take temporary possession of controlled substances in order to turn them over to police officers [and thus] aid the officers in the performance of their drug interdiction duties.” *Id.* at 266.

The versions of the child-pornography statute in effect both now and at the time of Crabtree’s offenses do not qualify the crime with the term “unlawful.” Rather, the crime occurs upon knowing possession of matter that one knows depicts child pornography. In this respect, the statute differs from the drug-possession and drug-trafficking statutes. Moreover, the exemption statute in KRS Chapter 531, the chapter governing pornography, is far narrower than that in KRS Chapter 218A.

KRS 531.070, which applies to the child-pornography statute, KRS 531.335,¹⁵ states that “[t]he prohibitions and penalties imposed in this chapter shall not extend to persons having a bona fide scientific, educational, governmental, or other similar justification for conduct which would, except for such justification, be criminal under this chapter.” The statute is aimed at protecting “[d]istribution of material otherwise obscene to institutions or persons for scientific, educational or governmental purposes” and “is designed to permit legitimate study of pornography for scholarly or scientific purposes.” KRS 531.070 Ky. Crime Comm’n/LRC Cmt. (1974).

Unlike the exemption statute in Chapter 218A, this statute does not expressly protect law enforcement or those attempting to aid law enforcement, though it does include “governmental, or other similar justification.” KRS 531.070. The statute thus appears to be drafted broadly enough to protect, for example, possession of such material by police, prosecutors, and courts as part of a criminal prosecution.¹⁶ It is less clear, however, that this would extend to a private citizen.

¹⁵ The exemption statute was enacted in 1974 as part of the penal code, see 1974 Ky. Acts ch. 406, § 271, and was aimed at exempting from criminal liability possession of obscene materials, see KRS 531.070 Kentucky Crime Comm’n/LRC Cmt. (1974). But child pornography was not specifically criminalized in Kentucky until 1992. See 1992 Ky. Acts ch. 201, § 1. Nevertheless, the exemption statute refers to all statutes in Chapter 531, which includes KRS 531.335.

¹⁶ When the child-pornography statute was amended in 2013 to also criminalize intentional viewing of child pornography, the General Assembly specifically added a provision excluding the “accidental or inadvertent viewing of such matter,” KRS 531.335(2)(a), “viewing by a person in the course of a criminal or civil investigation,” KRS 532.335(2)(b), and “viewing ... by a minor or the minor's parents or guardians, or to school administrators investigating violations of [the intentional-viewing] subsection ... of this section,” KRS 531.335(2)(c).

Nevertheless, we agree with Crabtree that the statute at least implicitly recognizes that possession of child pornography, even when knowing, can be innocent under certain circumstances. For example, a person could discover child pornography on his or her spouse's computer or in a box hidden in a closet, and seize that material to take to the police. While such conduct would violate the child-pornography statute, if read literally, we doubt that the General Assembly intended to criminalize it.

A more germane example would be an instance of accidental possession. As the proof in this case showed, files on file-sharing services are sometimes mislabeled, and seemingly innocent files could turn out to contain child pornography. No doubt, this mislabeling occurs in other parts of the internet. If a person were to download an innocently labeled file, and then open it to discover child pornography, at that instant, the person knowingly possesses material that he or she knows is child pornography. Even if the person immediately deleted the material, he or she could be "deemed [an] illegal possessor[]" under strictly construed [child-pornography] possession statutes." *Adkins*, 331 S.W.3d at 264.

But surely the General Assembly did not intend to criminalize such conduct either. The surprised person acts without a guilty mind, despite technically having knowledge sufficient to create criminal liability. Though the child-pornography statute does not include intent as a requisite mental state, something akin to intent must be shown to establish criminal liability here. Thus, the person who accidentally stumbles upon child pornography and immediately deletes it cannot be criminally liable, whereas the person who

similarly encounters such material but then chooses to keep it with no intent to turn it over to law enforcement has violated the statute and committed the offense.

As with illegal drugs, under very limited circumstances, temporary, incidental possession of child pornography does not amount to a criminal offense under Kentucky law. Like the drug statutes, our child-pornography statute “allows for a defense of innocent possession where there is evidence that the possession came about incidentally and continued no longer than reasonably necessary to allow for lawful and appropriate disposal.” *Adkins*, 331 S.W.3d at 267. If the proof shows the very limited circumstances of innocent possession, then a defendant would be entitled to a jury instruction laying out the defense.

Crabtree, however, failed to offer proof that would require such an instruction. On appeal, he suggests that he admitted to searching for shocking material and “that he may have just cast his net too wide while looking for legal shock videos.” But the proof did not establish, for instance, that the child pornography videos on his computer were innocently named and that he had encountered them while searching for other material. And even if he had encountered the videos while searching for other content, their filenames, which he had to have clicked and confirmed to begin the download, were clearly indicative of their content. A person cannot claim innocent possession when he sees files with terms unquestionably indicating child pornography and then chooses to download those files, even if he had originally been looking for legal content.

That he deleted, or at least attempted to delete, the material upon viewing and confirming the content of one of the files does not bring him within the ambit of the defense where he intentionally sought the material by initiating the downloads. That the possession may have been motivated by curiosity (Does this file being offered really contain child pornography?) or a misguided attempt to investigate on behalf of the police does not change the criminal nature of the possession.¹⁷ The defense is for temporary, incidental possession, not curiosity-driven possession. Such curiosity is better left to law-enforcement personnel, who have a duty to seek out and collect contraband as evidence for criminal prosecutions. And while curiosity may be an inherent human trait, the exercise of curiosity can be and is confined by law.

It was suggested by defense counsel at trial that the material on Crabtree's computer may have been put there by a virus, Trojan, or other malware on his computer. There are some media accounts suggesting that Trojans have been used to place and store child pornography on innocent people's computers.¹⁸ And courts have noted that "[t]he presence of Trojan

¹⁷ The most public example of such conduct is that alleged against Who guitarist Pete Townshend, who allegedly accessed child pornography in 1999. See Jamie Wilson, *Pete Townshend put on sex offenders register*, The Guardian, May 8, 2003, available at <http://www.theguardian.com/uk/2003/may/08/arts.ukcrime>. He claimed that he had done so for research purposes. *Id.* While Townshend was not prosecuted and was instead "cautioned" and placed on the sex-offender registry, his alleged conduct would be criminal under the Kentucky statute, and he would not be entitled to the innocent-possession defense. (Journalists later discovered that Townshend and thousands of similarly accused people may not have actually encountered child pornography and that Townshend "appears to have confessed to something he didn't do." Duncan Campbell, *Sex, lies and the missing videotape*, PC Pro, June 2007, at 21, available at <http://ore-exposed.obu-investigators.com/PC%20Pro%20article%20June%202007%20.pdf>.)

¹⁸ For example, CBS News has reported that malware can be used by a third party "to force someone else's computer to surf child porn sites, collecting images

viruses and the location of child pornography in inaccessible internet and orphan files can raise serious issues of inadvertent or unknowing possession.” *United States v. Kain*, 589 F.3d 945, 949 (8th Cir. 2009). Similar concerns exist for the dreaded pop-up advertising that is so ubiquitous now. See Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 Berkeley Tech. L.J. 1227, 1268 (2004).

If there was proof that malware had caused the child pornography to be on Crabtree's computer, he would have been entitled to an innocent-possession instruction, or possibly even a directed verdict on the basis of unknowing possession. But the evidence did not show that the pornography on Crabtree's computer was placed there by malware. The evidence, including Crabtree's own admissions, demonstrated that the videos had been downloaded through Limewire, not by malware. The closest Crabtree came to alleging the files were the result of malware was his counsel's questions to the Commonwealth's forensics expert about it. She answered that she had not seen examples of that actually happening in the literature she had reviewed, and that although malware had been found on Crabtree's computer, it had not put the videos on his computer.

Thus, we conclude that innocent possession is a proper defense to a charge of possession of child pornography and that if the evidence supports it,

along the way,” or to turn “a computer ... into a warehouse for pictures and videos that can be viewed remotely when the PC is online.” See, e.g., CBS/AP, *Viruses Frame PC Owners for Child Porn*, CBSNews.com (November 9, 2009, 12:49 PM), <http://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/>.

an instruction on the defense should be given. But the proof in this case simply did not support giving such an instruction.

C. The trial court did not err in declining to give the jury additional instructions on the meaning of knowing possession.

Crabtree also claims that the circuit court erred by allowing the jury to decide a question of statutory interpretation, namely, whether knowing possession requires more than temporarily viewing and then immediately discarding the illegal material. The trial court instructed the jury on the mental state of “knowingly” as laid out in the statute. Crabtree argues that the parties were then left to argue their interpretation of this definition to the jury, and that the prosecution specifically argued that the definition included no language allowing temporary possession of child pornography.

As this Court has stated on many occasions, we follow the bare-bones principle in jury instructions. *See, e.g., Harp v. Commonwealth*, 266 S.W.3d 813, 819 (Ky. 2008). “[J]ury instructions should tell the jury what it must believe from the evidence in order to resolve each dispositive factual issue while still ‘providing enough information to a jury to make it aware of the respective legal duties of the parties.’” *Id.* (quoting *Olfice, Inc. v. Wilkey*, 173 S.W.3d 226, 229 (Ky. 2005)). “In criminal cases, instructions ‘should conform to the language of the statute,’ and ‘[i]t is left to the lawyers to “flesh out” the “bare bones” in closing argument.’” *Wright v. Commonwealth*, 391 S.W.3d 743, 746–47 (Ky. 2012) (quoting *Parks v. Commonwealth*, 192 S.W.3d 318, 326 (Ky. 2006)).

The trial court's instructions to the jury, including the definition of *knowingly*, conformed to the language of the statutes. Crabtree's claim in this respect is really another way of arguing that he was entitled to an innocent-possession defense. The jury would only need further instruction as to the meaning of "knowing" if there had been evidence of inadvertent or accidental possession of the child-pornography videos. But, as discussed above, there was no such evidence.

D. The trial court did not abuse its discretion in excluding evidence of Crabtree's character for truthfulness.

Crabtree also argues that the Commonwealth attacked his character for truthfulness throughout trial, and that the trial court erred by excluding evidence of his good character. Specifically, he claims that he tried to introduce evidence of his character for truthfulness after his statement to police was attacked as an attempt to minimize his criminal conduct. He notes that Detective Collins, who conducted the interview with him, stated that criminally accused persons often try to minimize their criminal conduct in their statements to police. Crabtree claims the error was exacerbated when the prosecutor, in closing argument, claimed that she believed he had enjoyed the pornography on his computer and that he felt sick from having been caught, not from having seen the material.

Crabtree sought to introduce testimony about his character for truthfulness (through testimony of family friend Burt May) to rebut these attacks on his statement to police. The trial court concluded that unless

Crabtree took the stand or his veracity was attacked, the evidence would not be admitted.

Unlike character evidence about witnesses, which is limited, “evidence of a pertinent trait of character or of general moral character offered by an accused” is generally admissible.¹⁹ KRE 404(a)(1). This evidence, however, is still limited by the requirement of relevancy. Ordinarily, evidence of a particular character trait will be relevant only if it “tends logically to prove that [the defendant] did not commit the specific crime charged.” Robert G. Lawson, *The Kentucky Evidence Law Handbook* § 2.20[2][b][i], at 104 (5th ed. 2013). Thus, for example, character for honesty is relevant to prove innocence of theft, fraud, and similar crimes. *Gaugh v. Commonwealth*, 261 Ky. 91, 87 S.W.2d 94, 98 (1935). But character for truthfulness, the evidence offered by Crabtree, does not go to whether he committed the crimes charged, as it would if he had been prosecuted for perjury. Lawson, *supra*, § 2.20[2][b][i], at 105.

Even so, Crabtree’s character for truthfulness would be relevant if some other aspect of the trial had made it relevant. If the Commonwealth had attacked his truthfulness to undermine a statement he had made, or if he had taken the stand, then his character for truthfulness would be at issue and thus relevant and pertinent.

¹⁹ Crabtree did not seek to offer evidence of his general moral character, which would be admissible on the question whether he committed the crime at all. Robert G. Lawson, *The Kentucky Evidence Law Handbook* § 2.20[2][b][ii], at 105–06 (5th ed. 2013) (“Kentucky’s pre-Rules case law allowed of the use of [general moral character] evidence and KRE 404 codifies this position, specifically authorizing the use of ‘general moral character’ to prove the doing or absence of the doing of criminal acts.” (footnotes omitted)).

The question that Crabtree proposes is whether the Commonwealth's elicitation of testimony from the officer that suspects tend to minimize their criminal conduct was an attack on his character for truthfulness. At first blush, it would not seem to matter whether it was such an attack because the Commonwealth used that incriminating statement against Crabtree.

But, as Crabtree argues, the Commonwealth argued to the jury that Crabtree's culpability was much greater than even his statement to the police would warrant. Thus the prosecutor argued that she believed Crabtree actually enjoyed child pornography, which is why he had so many files of it on his computer, even though she did not have to prove that fact and Crabtree had claimed he was sickened by the images. She also suggested that he was sickened by having been caught with the material on his computer, which is an indirect attack on his claim that he was sickened by the images he saw.

The Court of Appeals concluded that the officer's testimony was not an attack on Crabtree's character but on his conduct. But that is incorrect here. To the extent that Crabtree attempted to use his own statement to show that he was not guilty (e.g., by using his claims to have been disgusted and to have deleted the files to show a lack of knowing possession), the officer's testimony put his character for truthfulness at issue. That made his character for truthfulness relevant to the trial and therefore admissible.

Nevertheless, this Court does not disagree with the Court of Appeals' conclusion that there was no prejudice from the exclusion of this "brief and generalized testimony." As discussed above, Crabtree's crime lay not in his continued possession or even viewing of the material he downloaded. Rather,

his offense was completed as soon as he began downloading the video files with knowledge of the filenames attached to them. His own statement corroborated this conduct—indeed, his own statement was an essential piece of proof showing that *he* began downloading the videos, rather than someone else, and showing that he did not accidentally get the videos from some other source. If Crabtree had been able to put on evidence of his truthfulness, he would have buttressed his own incriminating statements to the police and thus further supported the jury’s conclusion that he was guilty. Thus, this Court cannot say that the exclusion of the character evidence swayed the jury or otherwise affected the verdict. *See Winstead v. Commonwealth*, 283 S.W.3d 678, 688–89 (Ky. 2009). It was therefore harmless.

E. There was no cumulative error.

Finally, Crabtree argues that there was cumulative error requiring reversal. “We have found cumulative error only where the individual errors were themselves substantial, bordering, at least, on the prejudicial.” *Brown v. Commonwealth*, 313 S.W.3d 577, 631 (Ky. 2010). Although we have reversed some of Crabtree’s convictions, the errors requiring that reversal were related only to those convictions and did not infect the entire trial. The only other error was not prejudicial. Just as “we have declined to hold that the absence of prejudice plus the absence of prejudice somehow adds up to prejudice,” *id.*, so too does the absence of prejudice not equal prejudice when claimed to be cumulative error.

III. Conclusion

The Court of Appeals is affirmed in part and reversed in part. Crabtree's convictions related to the child-pornography videos found on his computer are affirmed; the convictions related to the still images found in the thumbcache of his computer are reversed.

All sitting. All concur.

COUNSEL FOR APPELLANT:

Fred E. Peters
Rhey Denniston Mills
Fred Peters Law Office
226 East High Street
PO Box 2043
Lexington, Kentucky 40588

COUNSEL FOR APPELLEE:

Jack Conway
Attorney General

James Hays Lawson
David Bryan Abner
Assistant Attorney General
Office of Criminal Appeals
Office of the Attorney General
1024 Capital Center Drive
Frankfort, Kentucky 40601