COURT OF APPEALS OF VIRGINIA

UNPUBLISHED

Present: Judges Alston, Chafin and Malveaux
Argued at Salem, Virginia

ALBERT HENRY CHRISTY, JR.

v. Record No. 0169-17-3

COMMONWEALTH OF VIRGINIA

MEMORANDUM OPINION* BY
JUDGE MARY BENNETT MALVEAUX
APRIL 10, 2018

FROM THE CIRCUIT COURT OF AUGUSTA COUNTY
Victor V. Ludwig, Judge

Kieran Bartley, Assistant Public Defender, for appellant.

John Ira Jones, IV, Assistant Attorney General (Mark R. Herring, Attorney General, on brief), for appellee.

Albert Henry Christy, Jr. ("appellant"), appeals his convictions for three counts of possession of child pornography, in violation of Code § 18.2-374.1:1(A).[1] He argues the evidence was insufficient to prove that he had knowledge of, access to, or dominion and control over the pornographic images at issue on or about March 1, 2016. For the reasons that follow, we affirm appellant's convictions.

* Pursuant to Code § 17.1-413, this opinion is not designated for publication.

[1] Appellant was also indicted for additional counts of possession of child pornography, in violation of Code § 18.2-374.1:1(A), reproduction of child pornography, in violation of Code § 18.2-374.1:1(C)(i), and reproduction of child pornography, second or subsequent offense, in violation of Code § 18.2-374.1:1(C)(i). The Commonwealth entered a *nolle prosequi* to several possession and reproduction charges. A jury found appellant not guilty of reproduction of child pornography and guilty of five counts of possession of child pornography. Two of appellant's convictions are not before this Court in this appeal.

## I. BACKGROUND

"Under familiar principles of appellate review, we will state 'the evidence in the light most favorable to the Commonwealth, the prevailing party in the trial court, and will accord the Commonwealth the benefit of all reasonable inferences fairly deducible from that evidence.'" Sidney v. Commonwealth, 280 Va. 517, 520, 702 S.E.2d 124, 126 (2010) (quoting Murphy v. Commonwealth, 264 Va. 568, 570, 570 S.E.2d 836, 837 (2002)).

In 2015, Detective Mark Belew of the Albemarle County Police Department was a member of the Southern Virginia Internet Crimes Against Children Task Force. In that role, Belew investigated computer file-sharing of sexually explicit materials involving children. To identify those who were sharing such materials, Belew employed a variety of software, including a program called Shareaza LE.[2] He testified that Shareaza allows its users to share files by accessing peer-to-peer ("P2P") computer networks.[3] Shareaza users employ search terms to look for files on such networks, and the program provides them with a list of other users' files that match their terms. Users then select the files they want and download them directly to their computers from other computers. However, Shareaza does not allow its users to force others to accept files.

In December 2015, Belew used Shareaza to download several files that a specific computer user had made available for P2P sharing. The images contained within the files

[2] "Shareaza is a peer-to-peer sharing program that allows users to trade electronic files, including music, photographic, and video files." Rideout v. Commonwealth, 62 Va. App. 779, 783 n.2, 753 S.E.2d 595, 597 n.2 (2014). The law enforcement version, Shareaza LE, "differs from the regular Shareaza in that it does not permit law enforcement to share files with other users." Id.

[3] "[P]eer-to-peer networks are 'so called because users' computers communicate directly with each other, not through central servers.'" United States v. Vadnais, 667 F.3d 1206, 1208 (11th Cir. 2012) (quoting Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919-20 (2005)).

depicted sexual acts committed with minors. Belew identified the Shareaza user's internet protocol ("IP") address[4] and subpoenaed documents from the user's internet service provider. Those documents identified appellant as the internet service subscriber associated with that particular IP address. Belew also identified a global unique identifier ("GUID")[5] associated with the Shareaza user's computer. He testified that a GUID is a specific numerical code assigned to a device connected to a P2P network, which is "unique and specific. . . . [A] fingerprint[,] if you will," that allows the network to recognize that specific device.

On March 1, 2016, deputies from the Augusta County Sheriff's Department, accompanied by Belew, executed a search warrant at appellant's home and recovered several computers. Appellant told Belew that he had downloaded Shareaza some years earlier in order to download music.

Zachary Moyer was a computer forensic examiner for the Office of the Attorney General and qualified as a computer forensic expert at trial. He testified that he participated in the search of appellant's home and found, in a bedroom, appellant's laptop computer open and running Shareaza. Moyer identified a folder on the computer's desktop which appeared to contain "child exploitation materials."

When Moyer conducted a forensic examination of appellant's laptop, he determined that it contained a single user-generated account named "bubba." That account was secured by a password, "bubba23," which a user would need to log on to the laptop and access any files contained within the "bubba" account. Moyer testified that the GUID associated with appellant's

[4] "An IP address is a string of . . . integer numbers . . . that identifies the location of a specific computer connected to the Internet." Am. Online, Inc. v. Nam Tai Elecs., Inc., 264 Va. 583, 587 n.3, 571 S.E.2d 128, 130 n.3 (2002).

[5] "A GUID number is produced whenever a peer-to-peer . . . file-sharing application . . . is installed or updated on a computer, and remains associated with the computer whenever the file-sharing program is in use." United States v. Pirosko, 787 F.3d 358, 363 n.1 (6th Cir. 2015).

laptop matched the GUID identified by Belew. He also testified that Shareaza was not set to run automatically when the laptop was turned on, but would have to be manually started by a user after they accessed the password-protected "bubba" account. Moyer's examination revealed that between February 10 and March 1, 2016, the laptop's user started Shareaza twenty times. On March 1, the day the laptop was seized by law enforcement at approximately 11:00 a.m., the laptop was turned on at 10:24 a.m., a user accessed the "bubba" account at 10:29 a.m., and at 10:32 a.m. the user started Shareaza. Moyer further testified that the program had been configured to download files into a sub-folder on the computer's desktop and that the user had to manually change Shareaza's default download destination to establish that configuration. He also noted that it is not possible for a person to use Shareaza to place files on someone else's computer. Instead, an individual must use the program to execute a search before double-clicking on specific search results to download files. Moyer used forensic software to recover some of the search terms used in the Shareaza program on appellant's laptop. Those terms included "Toddler," "Pre-teen," "Jailbait," "PTHC," "3 YO," "5 YO," "6 YO," and "7 YO." Moyer testified that "PTHC" is an acronym for "Preteen Hardcore" and that, based on his experience with other child pornography cases, "YO" stands for "years old."

Moyer located 31 relevant images and videos on the laptop's hard drive, stored in three distinct areas: allocated space, the thumb cache, and unallocated space. He testified that the videos and images stored in allocated space, including those in the desktop file, would have been readily accessible to the laptop's user, because the computer's operating system was aware of their existence and where to find them on the hard drive.

Moyer stated that the thumb cache images were smaller versions of images that had been deleted from other locations on the hard drive and that thumb cache images remain on the hard drive unless the computer user specifically acts to delete them. The thumb cache image files

contained no information indicating when they were stored on the hard drive, or later accessed or modified. Moyer used a forensic software program to find and recover the images from the thumb cache.

Lastly, some images were "orphan" images stored in the laptop's unallocated space. Moyer explained that there are two components for every file stored on a computer's hard drive. First, there is the actual file itself, which is stored in one location. Separately, in another location, the computer creates a directory entry containing information about the file, including its name and where it is stored on the hard drive. Moyer stated that "when you delete a file, it is not like the actual picture [or] video disappears. All [that] is happening is the [directory] entry referencing the file is marked in a way that the computer knows that [the] file is deleted." Thus, until the "deleted" images or videos are overwritten with new files, they will remain on the hard drive. Moyer testified that "these [orphan] files, their [directory] entries had been deleted, but the actual images or videos themselves . . . remained behind." Moyer stated that because the orphan images' directory entries had been deleted, the computer's operating system no longer knew where the image files were stored. Thus, the computer's user would not have been able to access or recover those images from unallocated space without using special software. However, unlike the images in the thumb cache, the orphan images did retain associated dates and times indicating when they were first stored on the computer.

The Commonwealth introduced three orphan images into evidence. The first was stored on appellant's laptop at 9:34 a.m. on February 21, 2016. Its file name included the terms "preteen," "PTHC," and "10yo." The second image was also stored on appellant's laptop at 9:34 a.m. on February 21, 2016. Its file name included the terms "Preteen," "Pthc," and "10Yo." The third image was stored on appellant's laptop on February 25, 2016 at 12:14 p.m. Its file name included "((PTHC))."

Appellant denied knowing that any of the pornographic images were on his computer. He testified that he used Shareaza to search for and download music, but accessed his laptop "just rarely" to play a computer game. He denied changing the default download settings for Shareaza and stated that the program would sometimes "pop open" on its own. Appellant also testified that his nickname is Bubba and that his laptop was protected by the password "bubba23." He stated that he and Jody Pritts were the only residents of his home, that Pritts could not get to his laptop in his bedroom, and that he sometimes locked that room. Pritts' testimony confirmed these facts. Pritts, who was not at the house when police executed the search warrant, testified that she was not permitted to enter appellant's room and that appellant locked the room "[p]retty much" every time he left. Appellant would keep the key with him. Pritts, who uses a wheelchair, was also unable to enter the room because it was too physically confining.

At the close of the Commonwealth's case, appellant moved to strike with respect to the thumb cache images. He argued that the evidence failed to demonstrate he knowingly possessed the images on the dates charged in the indictments, because there were no dates associated with the images, the images were not "easily accessible," and there was no way for him to know they were present on his computer. The trial court denied the motion, but later revisited its ruling and granted the motion to strike.

Appellant also moved to strike with respect to the orphan images stored in unallocated space, arguing that a "general user" would have believed the images were "gone" after deleting them, and would not have been able to access them without "special technology" and the "special knowledge" that they could still be found. Further, it was impossible to know when and how the images had been deleted and they could have been deleted "long before" March 1. The trial court denied the motion.

A jury convicted appellant of five counts of possession of child pornography—two counts for possession of images which were stored on the computer's desktop in allocated space, and three counts for possession of orphan images that were stored in unallocated space. Appellant moved to vacate the verdicts with respect to the orphan images, and his motion was denied. This appeal followed.

## II. ANALYSIS

Appellant argues that the Commonwealth's evidence was insufficient to prove that he had knowledge of, or access to, or dominion and control of the orphaned images on or about March 1, 2016, the dates alleged in his indictments.

When considering a challenge to the sufficiency of evidence on appeal, "we review the evidence in the light most favorable to the Commonwealth," the prevailing party at trial, "granting to it all reasonable inferences fairly deducible therefrom." Sierra v. Commonwealth, 59 Va. App. 770, 774, 722 S.E.2d 656, 657 (2012) (quoting Archer v. Commonwealth, 26 Va. App. 1, 11, 492 S.E.2d 826, 831 (1997)). The Court "discard[s] the evidence of the accused in conflict with that of the Commonwealth." Johnson v. Commonwealth, 53 Va. App. 79, 99, 669 S.E.2d 368, 378 (2008) (quoting Parks v. Commonwealth, 221 Va. 492, 498, 270 S.E.2d 755, 759 (1980)). Further, "circumstantial evidence may be more compelling and persuasive than direct evidence, and when convincing, it is entitled to as much weight as direct evidence." Booker v. Commonwealth, 61 Va. App. 323, 335-36, 734 S.E.2d 729, 735 (2012) (quoting Bridgeman v. Commonwealth, 3 Va. App. 523, 526, 351 S.E.2d 598, 600 (1986)).

In conducting our inquiry, "the relevant question is, after reviewing the evidence in the light most favorable to the [Commonwealth], whether any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." Sullivan v. Commonwealth, 280 Va. 672, 676, 701 S.E.2d 61, 63 (2010). "This familiar standard gives full play to the

responsibility of the trier of fact fairly to resolve conflicts in the testimony, to weigh the evidence, and to draw reasonable inferences from basic facts to ultimate facts." Kelly v. Commonwealth, 41 Va. App. 250, 257-58, 584 S.E.2d 444, 447 (2003) (*en banc*) (quoting Jackson v. Virginia, 443 U.S. 307, 319 (1979)). We "presume the judgment of the trial court to be correct," White v. Commonwealth, 68 Va. App. 111, 118, 804 S.E.2d 317, 320 (2017) (quoting Kelly, 41 Va. App. at 257, 584 S.E.2d at 447), and do not "substitute our judgment for that of the trier of fact," Wactor v. Commonwealth, 38 Va. App. 375, 380, 564 S.E.2d 160, 162 (2002). Thus, we "will reverse only where the trial court's decision is 'plainly wrong or without evidence to support it.'" Calloway v. Commonwealth, 62 Va. App. 253, 261, 746 S.E.2d 72, 76 (2013) (quoting Seaton v. Commonwealth, 42 Va. App. 739, 746, 595 S.E.2d 9, 12 (2004)).

Code § 18.2-374.1:1(A) provides that "[a]ny person who knowingly possesses child pornography is guilty of a Class 6 felony."[6] This Court "[has] previously held that possession of child pornography found in computers may be analyzed under familiar principles of constructive possession." Kobman v. Commonwealth, 65 Va. App. 304, 307, 567 S.E.2d 565, 567 (2015). See also Kromer v. Commonwealth, 45 Va. App. 812, 817-18, 613 S.E.2d 871, 873-74 (2005). To convict a defendant for constructive possession, "the Commonwealth must point to evidence of acts, statements, or conduct of the accused or other facts or circumstances which tend to show that the defendant was aware of both the presence and character of the [contraband] and that it was subject to his dominion and control." Terlecki v. Commonwealth, 65 Va. App. 13, 24, 772 S.E.2d 777, 782 (2015) (quoting Drew v. Commonwealth, 230 Va. 471, 473, 338 S.E.2d 844, 845 (1986)). Further, "[o]wnership or occupancy of the premises on which the contraband was

[6] Appellant does not challenge that the images at issue constituted child pornography, as defined by Code § 18.2-374.1(A).

found is a circumstance probative of possession." Id. (quoting Kromer, 45 Va. App. at 819, 613 S.E.2d at 874).

Appellant contends that the instant case is analogous to Kobman. In Kobman, this Court considered whether the evidence was sufficient to sustain the defendant's convictions for possession of child pornography based upon photographs stored in the unallocated space of two computers. Kobman, 65 Va. App. at 307-08, 777 S.E.2d at 567. Both computers were seized from the defendant's home. Id. at 306, 777 S.E.2d at 566. The photographs were recovered by an investigator using specialized forensic software, and the investigator testified that "files and data in the unallocated space of a computer are 'invisible' to the computer's operating system and inaccessible to the user unless . . . specialized software is downloaded on the computer." Id. at 306, 777 S.E.2d at 567. Applying principles of constructive possession, this Court reversed the convictions after concluding that "[n]o evidence established [the defendant] had access to or used the required forensic software necessary to retrieve the deleted photographs. Further, no evidence showed other indicia of knowledge, dominion, or control of the . . . photographs found in the unallocated space on the specific date [*sic*] of the indictments." Id. at 308, 777 S.E.2d at 567. The Court also noted that "[w]hile the evidence may suggest [the defendant] at one time possessed the photographs in the unallocated space, there was no evidence that he had dominion or control of them on or about May 19, 2013, as the indictments charged." Id.

Appellant argues that the evidence in the instant case is "equivalent" to the evidence in Kobman, and thus insufficient for the same reasons. He acknowledges that in the instant case, the computer containing the images was seized from his residence—a circumstance Kobman notes is probative of possession. See id. However, appellant contends that, as in Kobman, there was no evidence he possessed the special software necessary to access the images, and no other

evidence that he "had dominion and control of the images at the date alleged in the indictments, or knew of their continued existence."

We find appellant's argument unpersuasive. Here, viewing the evidence in the light most favorable to the Commonwealth, a rational trier of fact could have found that although appellant lacked special software to access the orphan images, unlike in Kobman, there were sufficient "other indicia" that he had knowledge of and dominion and control over the images on or about March 1, 2016.

The images at issue were found on a laptop containing a single user account, named "bubba," which was secured by the password "bubba23." Appellant testified that Bubba is his nickname and that he protected his computer with the stated password. Only two people—appellant and Pritts—lived in appellant's home. Appellant maintained a separate bedroom, where he kept several computers, and Pritts was not permitted to enter that room. Further, Pritts was physically unable to enter the room because appellant frequently kept it locked and because the room was too confining for her wheelchair. When law enforcement officers searched appellant's home, Shareaza was running on the laptop in that room and appellant was the only person in the home. Appellant admitted to Detective Belew that he had installed Shareaza on the laptop and testified that he used the program to download music files from the internet. Zachary Moyer testified that the Shareaza program on appellant's laptop had been manually reconfigured and had to be manually started by the computer's user and that between February 10 and March 1, 2016, Shareaza had been started twenty times. A reasonable inference may be drawn from this evidence that appellant was the sole person who had access to and used the laptop computer and the "bubba" account. This evidence further supports the reasonable inference that appellant was familiar with how to use Shareaza and frequently used it in the days and weeks prior to March 1, 2016.

Both Belew and Moyer testified that a Shareaza user acquires files from a P2P network by entering search terms and selecting and downloading files of interest from the search results. They also testified that it is not possible for someone else to use Shareaza to place files on a person's computer. Moyer testified that the laptop's user employed search terms associated with child pornography, including "Pre-teen," "PTHC," and "YO" and that these terms were found in the file names of images on appellant's laptop, including the orphan images. Also, Belew was able to use Shareaza to download images of child pornography from a computer with the same IP address and GUID as appellant's laptop. This evidence supports the inference that appellant used Shareaza to access P2P networks, search for images of child pornography, and download those images to his laptop.

Based on the foregoing evidence and inferences, a rational trier of fact could have concluded that appellant purposely searched for and downloaded the images at issue, and thus knew of their character and presence on his computer at that time. A rational trier of fact could also have concluded that the images were subject to appellant's dominion and control from their download dates until he acted to delete them, thus making them "orphan" images, at some point during the five to nine days between their download dates and the laptop's seizure. Thus, the evidence was sufficient to prove that appellant knowingly possessed the three orphan images.[7]

[7] Appellant also argues that the trial court's rationale in granting his motion to strike the evidence of the thumb cache images applies equally to the evidence of the orphan images—that, as in Kobman, there was neither evidence that he possessed the special software necessary to access the images, nor "other indicia" of his knowledge of or dominion and control over them. This argument is without merit. The orphan images in the unallocated space on appellant's hard drive are distinguishable from the thumb cache images, because they retain indicia of the specific dates on which they were downloaded and stored on the hard drive. For the reasons discussed above, those dates support that appellant knowingly possessed the images, because the other evidence shows that appellant used Shareaza to search for and download child pornography and only appellant could have accessed and used his laptop to download the images on those dates.

Finally, we address appellant's contention that the evidence failed to prove he knowingly possessed the images at issue "on the dates alleged," that is, "on or about March 1, 2016." In support of his argument, appellant again analogizes to Kobman, noting in particular this Court's statement that "[w]hile the evidence may suggest [the defendant] at one time possessed the photographs in the unallocated space, there was no evidence that he had dominion or control of them on or about May 19, 2013, as the indictments charged." Kobman, 65 Va. App. at 308, 777 S.E.2d at 567.

We first note that the Commonwealth was not required to prove the exact date appellant was in possession of each image in order to convict him of possession of child pornography. Code § 19.2-226 provides that "[n]o indictment . . . shall be quashed or deemed invalid . . . [f]or omitting to state, or stating imperfectly, the time at which the offense was committed when time is not the essence of the offense." "When time is not an element of the crime charged, the jury verdict will stand" so long as the evidence proves that "a crime occurred and that the defendant committed the crime, even though the evidence is such that there may be a reasonable doubt as to the day on which the offense occurred." Marlowe v. Commonwealth, 2 Va. App. 619, 623-24, 347 S.E.2d 167, 170 (1986). Further, "[t]ime is not a material element of a criminal offense unless made so by the statute creating the offense." Farhoumand v. Commonwealth, 288 Va. 338, 351, 764 S.E.2d 95, 102 (2014) (alteration in original) (quoting United States v. Stuckey, 220 F.3d 976, 982 (8th Cir. 2000)). Thus, where there is no such statutory provision, "[i]n a felony case the Commonwealth may prove the commission of a crime charged on a date different from that alleged in the indictment." Id. (alteration in original) (quoting Harris v. Commonwealth, 185 Va. 26, 34, 37 S.E.2d 868, 871 (1946)).

Code § 18.2-374.1:1 does not establish time as a material element of the crime of possession of child pornography, and thus time is not of the essence of that offense.

Consequently, even if there is reasonable doubt as to the exact date or range of dates on which appellant possessed the images at issue, the jury verdict convicting appellant will stand so long as the evidence is sufficient to prove he possessed child pornography as charged in the indictments. As discussed above, the evidence is sufficient to so prove.

Further, we reject appellant's argument that Kobman compels a different result, as Kobman is factually distinguishable. In Kobman, the only evidence supporting the defendant's convictions for possession of images stored in his computers' unallocated space was the presence of those images themselves—undated images which he may have knowingly possessed, if at all, at some indefinite point long before the time frame referenced in his indictments. Here, by contrast, the evidence showed that appellant possessed the images at issue and that he did so not more than five to nine days prior to the date specified in the indictments—March 1, 2016. Thus, because time is not an element of the crime of possession of child pornography and Kobman is distinguishable on the facts surrounding the images, contrary to appellant's contention, the evidence was sufficient to prove that he was in possession of those images "on the dates alleged," *i.e.*, "on or about March 1, 2016."

## III. CONCLUSION

For the foregoing reasons, we hold that the evidence was sufficient to convict appellant for possession of child pornography, in violation of Code § 18.2-374.1:1(A), and affirm appellant's convictions.

Affirmed.