

COURT OF APPEALS OF VIRGINIA

Present: Chief Judge Decker, Judges AtLee and Malveaux
Argued at Richmond, Virginia

JERRY WAYNE REMINES

v. Record No. 0737-21-2

COMMONWEALTH OF VIRGINIA

MEMORANDUM OPINION* BY
JUDGE RICHARD Y. ATLEE, JR.
DECEMBER 20, 2022

FROM THE CIRCUIT COURT OF HALIFAX COUNTY
Kimberley S. White, Judge¹

David B. Hargett (Hargett Law, PLC, on brief), for appellant.

Timothy J. Huffstutter, Assistant Attorney General (Jason S.
Miyares, Attorney General, on brief), for appellee.

Following a bench trial, the circuit court convicted appellant Jerry Wayne Remines of one count of possession of child pornography and ten counts of possession of child pornography, second or subsequent offense, all occurring between August 24, 2019, through October 12, 2019.² On appeal, he argues “[t]he evidence was insufficient on each count as to knowingly possessing the illegal files and/or exercising dominion and control over said files.” For the following reasons, we affirm.

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

¹ The Honorable Kimberley S. White presided over the proceedings below. Now a member of this Court, Judge White took no part in this decision.

² Remines also pled guilty to making an unauthorized copy of computer software (computer trespass). This conviction is not challenged on appeal.

I. BACKGROUND

“On appeal of criminal convictions, we view the facts in the light most favorable to the Commonwealth, and [we] draw all reasonable inferences from those facts.” *Johnson v. Commonwealth*, 73 Va. App. 393, 396 (2021) (alteration in original) (quoting *Payne v. Commonwealth*, 65 Va. App. 194, 198 (2015)). So viewed, the facts reflect the following.

Remines operated an electronics repair business, Airborne Electronics Repair, out of his home. In the fall of 2019, South Boston Police Department Corporal Adam Whitmore brought his phone to Remines to fix a broken screen. Remines said the screen was not repairable, and Whitmore purchased a new phone. When Whitmore downloaded his cloud data to his new phone, he saw several text messages sent from his phone number to a number associated with Airborne Electronics Repair. These messages were sent after Whitmore had dropped his phone off for repair with Remines, without Whitmore’s permission or knowledge, and included photographs of Whitmore’s wife in “states of undress” and an intimate video of Whitmore and his wife. Whitmore brought this information to the Department’s attention, and South Boston Police Department Detective Tiffany Bratton obtained a search warrant for Remines’s cell phone and “any computer hardware or software that is capable of data storage and handling.”

When the police executed the search warrant at Remines’s home, Remines came to the door holding his cell phone, an iPhone 8 Plus. Bratton took the phone and gave it to Special Agent Travis Barr of the Virginia State Police, who secured the device. Bratton proceeded to interview Remines, who denied taking images from Whitmore’s phone but said he may have backed up the phone’s contents. He stated he used his own cell phone for both personal and business purposes. He refused to provide his passcode to unlock the phone, claiming there was “confidential information inside the phone.”

Barr testified at trial as an expert in digital examination and analysis. Upon receiving Remines's phone, Barr put it in "airplane mode" and changed the settings so it would not go to sleep. He immediately noticed a TOR browser, which permits a user to browse the "dark web." He transported the phone, along with other recovered devices, to a secure location for analysis. Barr connected the phone to "GreyKey," which permits law enforcement to collect data from a locked device. The resulting zip file, containing the phone's contents, can then be indexed and analyzed by other programs. While searching for Whitmore's photos, Barr came across child pornography. He also noted a browser bookmark for "young lolita lesbians."

Barr provided the devices and extracted material to Special Agent James Trogon of the Virginia State Police's computer evidence recovery section, who also testified at trial as an expert in digital forensic examination and analysis.³ Trogon noted several things that connected Remines to the device: the phone's device display name was registered as "Airborne Electronics Repair," and there were multiple emails using "masstech" and "phonerepair22@gmail.com," with the email contact name being "Jerry R."

Trogon's analysis found that "the bulk of" the child pornography was from three different applications ("apps"): MEWE (a social networking app), VK (a Russian social networking app), and Mega (a cloud storage provider). The MEWE app indicated that Remines accessed it with the username "tlbytes" or "littletlbytes." Cached photos associated with the MEWE app included images of Remines and his wife, Remines in military uniform, a race car with a "Airborne Electronics Repair" decal on the bumper, and Remines's family tree.

³ Remines called his own expert witness in digital forensic analysis, Patrick Eller. To the limited extent this testimony is meaningfully inconsistent with that of the Commonwealth's expert, we "discard the evidence of the accused in conflict with that of the Commonwealth[] and regard as true all the credible evidence favorable to the Commonwealth and all fair inferences to be drawn' from that evidence." *Johnson*, 73 Va. App. at 398 (alteration in original) (quoting *Haba v. Commonwealth*, 73 Va. App. 277, 283 (2021)).

The MEWE app data also included group memberships and chat history regarding the searching for and dissemination of child pornography. Remines was the moderator/administrator—meaning he could approve or deny new members or ban existing members—of one of these groups. It had a series of “yes or no” questions a user must answer in order to join, each of which the “tlbytes” user responded to in the affirmative. These questions included:

- Do you agree to post content whether forbidden or just plain sexy taboo content so that everyone in the group can enjoy it[?]
- [T]o ensure that the group . . . hangs around for a while, do you agree to put any underage or extreme porn content on timers[?]
- [B]y joining the group, do you agree not to report any content [of] this group no matter what . . . pics, gif[s], videos, links or comments [are] posted . . . [?]
- [I]f you choose to join this group, you are admitting that you are a sick, perverted fuck that enjoys filling the void of his/her life with the most devious porn known to the internet. Agree[?]

The chat history for the MEWE app “tlbytes” account included messages sent to another user about finding and joining groups. These messages included: “What the fuck wrong with these morons they can insert a fucking three inch diameter wine bottle up a pussy and ass but go crazy about the word incest”; “Are there any incest groups on here?”; and “Feel free to add me to any of your taboo or young groups.”

The VK app cache data contained five images depicting child pornography. These images were downloaded on November 29, 2018, September 7, 2019, and November 18, 2019. The VK app had been downloaded by the user of the phonerepair22@gmail.com email address.

The Mega app cache contained the “majority of” the child pornography. The Mega app provides cloud storage, allowing a user to store their files for future access and to create links to share with others. Trogon identified 919 media files, and at least 96 images, depicting child pornography in the Mega app data. The images were in a “thumbnailsV3” folder, which Trogon explained would only occur if a user clicked on the image. All but one file indicated a

“created date,” which Trogdon described as the “date in which that artifact was created on the device,” between August 24, 2019, and October 12, 2019.⁴ The app data also contained a video depicting child pornography with a created date of October 8, 2019. Trogdon testified that “[i]n order for the video file to arrive in the temporary location, it would have had to have been clicked and played through the Mega application.”

The phone data also indicated that Remines used a virtual private network, or VPN, when accessing these apps and images. This would disguise Remines’s actual IP address and location in South Boston, and display IP addresses in other locations (such as Guadalajara, Mexico), providing additional anonymity and privacy protection.

Remines moved to strike at the close of the evidence, arguing that the evidence was insufficient to prove that he knowingly possessed or exercised dominion or control over the files. In denying Remines’s motion, and prior to convicting Remines, the circuit court determined that “clicking and viewing an image of child pornography is exercising dominion and control over that image. When you click it, you can save it, you can send it, you can print it, you can delete it, you can do any number of things with that—with that image.” It noted that the Commonwealth had established that Remines intentionally “repeated[ly] access[ed] exceedingly graphic and violent child pornography.”

The circuit court ultimately found Remines guilty. It found Trogdon’s expert testimony credible and determined that, because “images do not land in that cache unless they’ve been clicked and opened,” Remines intended to view these images. It noted that Remines had repeatedly denied ever viewing child pornography, even accidentally. The circuit court also emphasized that Remines “answered the MEWE app questions that clearly are meant to weed out those people who would be disturbed or apt to report” the child pornography distributed in that group. Furthermore, it noted

⁴ One “outlier” file had a “created date” of July 31, 2015.

Remines’s chat evidence and his bookmark to a “young lolita site.” Accordingly, the circuit court convicted Remines of one count of possession of child pornography, and ten counts of possession of child pornography, second or subsequent offense. He received a sentence of 55 years and 12 months, with 35 years and 12 months suspended. This appeal follows.

II. ANALYSIS

Remines presents two primary arguments. First, he claims that under this Court’s precedent, the lack of forensic tools providing Remines with access to the cached images at the time of the device’s seizure meant the evidence was insufficient to prove that he knowingly possessed the images. Second, he argues that Code § 18.2-374.1:1,⁵ which criminalizes “knowingly possess[ing] child pornography,” does not include the “mere viewing” of images in the scope of “possession.” Both arguments fail under existing precedent.

A. *Standard of Review*

“We apply a deferential standard of review to challenges based on the sufficiency of the evidence, and the decision of ‘[t]he lower court will be reversed only if that court’s judgment is plainly wrong or without evidence to support it.’” *Otey v. Commonwealth*, 71 Va. App. 792, 797 (2020) (alteration in original) (quoting *Cartagena v. Commonwealth*, 68 Va. App. 202, 207 (2017)). “[T]he relevant question is, upon review of the evidence in the light most favorable to the prosecution, whether *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.” *Id.* (quoting *Smith v. Commonwealth*, 296 Va. 450, 460 (2018)).

B. *Lack of Forensic Tools and Knowing Possession*

Remines points to *Kobman v. Commonwealth*, 65 Va. App. 304 (2015), for the principle that the lack of specialized knowledge or forensic tools meant that he could not access the

⁵ Remines cites “Code § 8.01-374.1:1” on brief, but it is clear from the context that he means Code § 18.2-374.1:1.

images obtained from the cache, and thus could not have possessed the images. He ignores one key distinction, however, which the circuit court noted in pronouncing him guilty: the defendant in *Kobman* (and subsequently in *Kovach v. Commonwealth*, No. 2013-15-2 (Va. Ct. App. Dec. 6, 2016), which Remines also relies upon) was indicted for possession of the images *on the date the search warrant was executed*. Therefore, in *Kobman*, the lack of evidence that the defendant could access the cached images, *i.e.*, the absence of specialized knowledge or forensic software, on the date provided in the indictment was critical in finding the evidence insufficient. Here, the indictments were for possession of child pornography between August 24, 2019, and October 12, 2019,⁶ which encompasses the “created date” of each of the images for which Remines was convicted. Expert testimony established that the “created date” reflected the time which the image was clicked, viewed, or accessed on Remines’s cell phone. Accordingly, because the cached pornographic files in question were all accessed between August 24, 2019, and October 12, 2019, the evidence is sufficient to show that Remines possessed the images on those dates set forth in the indictments. Additional proof that he used or had specialized knowledge or forensic tools to access cached files at a later point is unnecessary.

C. *Viewing or Clicking on Images as Possession*

In *Kromer v. Commonwealth*, 45 Va. App. 812 (2005), this Court adopted the stance that “each time [an individual] intentionally sought out and viewed child pornography with his Web browser[,] he knowingly acquired and possessed the images.” 45 Va. App. at 817 (quoting *United States v. Tucker*, 305 F.3d 1193, 1205 (10th Cir. 2002)). This Court specifically noted: “While the facts in *Tucker* differ from the facts here, *we adopt the court’s definition of*

⁶ The original indictments referenced the dates “September 1, 2019 through November 20, 2019,” but were subsequently amended.

possession of computer images.” Id. (emphasis added). This previous holding is dispositive here.⁷

There is overwhelming evidence that Remines “intentionally sought out” child pornography, as well as viewed it, not only from the recovered cached files, but also from his browser bookmarks, app chat history, and group memberships. Remines does not contest that he possessed and had control over his phone, nor does he offer any theory that some other user might have been responsible for any activity on the phone. Moreover, the presence of Remines’s name, email address, and personal images in these app user profiles and app data further link Remines to the recovered files and phone activity.

Remines’s phone contained data from apps that contained hundreds of images depicting graphic child pornography. Five of those images were in the app data for the VK app, indicating the images were accessed on November 29, 2018, September 7, 2019, and November 18, 2019. Hundreds of additional images were in the app data for the Mega app, indicating they had been created, or actively interacted with by clicking on or enlarging them, by Remines, between August 24, 2019, and October 12, 2019. A video depicting child pornography on the Mega app was viewed on October 8, 2019.

Crucially, the evidence was not limited to the recovered cached media files. Remines’s phone contained records indicating he actively sought out underage content, including belonging to groups dedicated to sharing it. He even facilitated its distribution through his role as a group moderator, to which membership required sharing “forbidden or just plain sexy taboo content” and “underage or extreme porn.” It was also forbidden to report images or activity within the

⁷ Remines cites precedent from other jurisdictions, and he notes that the federal system amended the child pornography statute to provide that it is illegal for any person who either “knowingly possesses” or “knowingly accesses with intent to view” any “material that contains an image of child pornography.” 18 U.S.C. § 2252A. While Code § 18.2-374.1:1 does not contain such an amendment, it is not necessary in light of *Kromer*.

group, and joining required agreeing that the user is a “sick, perverted fuck that enjoys filling the void of his/her life with the most devious porn known to the internet.” Remines’s chat history also showed that he sought to be added to more groups that shared “taboo or young” content and expressed interest in “incest” content. He even expressed dismay that others who were fine with images depicting “insert[ing] a fucking three inch diameter wine bottle up a pussy and ass” would “go crazy about the word incest.” Remines never claimed to have accidentally accessed or clicked on these illegal images, despite having the opportunity to do so. He also concealed his activities by accessing these apps via a VPN.

Our case law is clear that any time someone intentionally seeks out and views child pornography on the internet, that person knowingly acquires and possesses the images. *Kromer*, 45 Va. App. at 817. The evidence here is overwhelming that Remines sought out and viewed child pornography and that the images recovered from his phone’s cached data were there due to his interaction with that content. Accordingly, the circuit court did not err in finding him guilty of possession of child pornography.

III. CONCLUSION

The evidence was sufficient to show that Remines knowingly possessed child pornography when he intentionally sought it out and accessed it. We find no error in the circuit court’s decision and, therefore, affirm.

Affirmed.