SUMMARY
April 30, 2026

2026COA30

No. 23CA1161, *People v. Slusher* — Constitutional Law — Fourth Amendment — Searches and Seizures — Electronic Devices or Information — Peer-to-Peer File Sharing — Torrential Downpour

A division of the court of appeals holds that law enforcement's use of Torrential Downpour, proprietary government software, to download files from the defendant's computer over a peer-to-peer file-sharing network was not a search under the Fourth Amendment or the Colorado Constitution. The division also holds that the district court did not err by declining to order disclosure of the software to the defense team where the defendant presented no evidence that it would have been favorable to his defense.

COLORADO COURT OF APPEALS **2026COA30**

Court of Appeals No. 23CA1161
Arapahoe County District Court No. 22CR376
Honorable Eric White, Judge

The People of the State of Colorado,

Plaintiff-Appellee,

v.

Floyd David Slusher,

Defendant-Appellant.

JUDGMENT AFFIRMED

Division VI
Opinion by JUDGE SCHOCK
Grove and Yun, JJ., concur

Announced April 30, 2026

Philip J. Weiser, Attorney General, Josiah Beamish, Assistant Attorney General, Denver, Colorado, for Plaintiff-Appellee

Megan A. Ring, Colorado State Public Defender, Casey Mark Klekas, Deputy State Public Defender, Denver, Colorado, for Defendant-Appellant

¶ 1 Defendant, Floyd David Slusher, appeals his convictions on two counts of sexual exploitation of a child — one for possession with intent to distribute sexually exploitative material and one for possession of such material. He contends that the evidence was insufficient to support his convictions and that the district court erred by (1) denying his motion to suppress; (2) denying his motion for disclosure of a computer program used in the investigation; and (3) failing to remove four jurors for cause. We affirm the judgment.

I. Background

¶ 2 Using proprietary government software called Torrential Downpour, an investigator downloaded several files containing sexually exploitative material from a particular internet protocol (IP) address through a peer-to-peer file-sharing network called BitTorrent. Subsequent investigation connected that IP address to a group home where Slusher lived with several other men. The home had five bedrooms, and its residents changed often.

¶ 3 Law enforcement obtained a search warrant for the home and seized three computers that were later discovered to contain sexually exploitative material. The first was a laptop (identified as "scene item 6," or SI-6) found in a shed in the backyard where

Slusher and other residents kept their belongings. The other two were shared desktop computers in the living room (identified as SI-9 and SI-10). All three were connected to Slusher, as detailed below.

A. SI-6

¶ 4 The registered owner of SI-6 — meaning the person who initially registered and logged into the computer — was Ronald Campbell, another recent resident of the home. But Campbell testified that he gave the computer to Slusher and never used it.

¶ 5 There was a substantial amount of data on SI-6 indicating that Slusher had used the computer, and he appeared to have been the exclusive user in the month before the investigation. In particular, there were more than 13,000 "Windows event logs" associated with Slusher's email address, indicating actions taken — "a file that was created, a video that was viewed, [or] a website that was logged into" — under that email address. There were also several accounts on SI-6 under Slusher's name or email address.

¶ 6 A computer forensic analyst found ten videos containing sexually exploitative material in the "unallocated space" of SI-6. Unallocated space is where files go after they are lost or deleted. Although files in unallocated space are not accessible by the user,

they may sometimes be recovered with forensic tools. In addition to the files in unallocated space, other data on SI-6 indicated that files with titles indicative of child sex abuse material had recently been opened or accessed, though they were no longer on the computer.

¶ 7 The forensic analyst also identified two programs that were installed on SI-6: (1) "qBittorrent," an application that permits a user to send or receive files over a peer-to-peer file-sharing network like BitTorrent; and (2) "Eraser," an "anti-forensic tool" that can be used to inhibit the discovery and recovery of deleted items.

B. SI-9

¶ 8 Slusher was the registered owner of SI-9, and his email and username were associated with it. Although the computer was in the living room, the manager of the group home testified that Slusher was "probably the only one" who used it, and the forensic analyst found no indication that anyone else regularly used it.

¶ 9 More than 200 files of sexually exploitative material were found in the unallocated space of SI-9. Four of those files were screenshots from videos that the investigator had downloaded from the home's IP address using Torrential Downpour.

¶ 10 In addition, two such files — created one week before the investigator's downloads — were found in SI-9's recycle bin. The forensic analyst testified that a file goes to the recycle bin when the user moves it there or deletes it. The file remains accessible until it is deleted again, at which point it is in unallocated space.

¶ 11 There were also hundreds of "link files" with titles indicative of child sex abuse material on SI-9. According to the forensic analyst, link files are "essentially shortcut files" that are created when a file is accessed, opened, or viewed. Although the files themselves were no longer on SI-9, the existence of a link file on a computer means the associated file "was at one point in time on that device."

¶ 12 As with SI-6, qBittorrent was also installed on SI-9.

C. SI-10

¶ 13 Slusher was also the registered owner of SI-10. His Microsoft OneDrive account was set up on the computer, and his email account "showed up consistently" on it. SI-10 contained one file of sexually exploitative material in the form of a "thumb [cache]" — a "remnant" of "what used to be a thumbnail," or "a small jpeg that [a] computer creates to display to [the user] what is inside of a folder." Like SI-6, SI-10 had the Eraser program installed on it.

D. Charges and Convictions

¶ 14 Slusher was charged with two counts of sexual exploitation of a child — one for possession with the intent to distribute sexually exploitative material and the other for possession of sexually exploitative material — as well as two habitual sex offender against children sentence enhancers. A jury convicted Slusher as charged.

II. Sufficiency of the Evidence

¶ 15 Slusher argues that the evidence was insufficient to prove he knowingly possessed sexually exploitative material. He contends that (1) the files in the unallocated space cannot show knowing possession because he did not have access to them, and (2) the files on SI-9 and SI-10 cannot show *his* knowing possession because he did not have exclusive control over those computers. We disagree.

A. Standard of Review and Applicable Law

¶ 16 In reviewing the sufficiency of the evidence, we review the record de novo to determine whether the evidence was sufficient in both quantity and quality to sustain the conviction. *Johnson v. People*, 2023 CO 7, ¶ 13. We do not "serve as a thirteenth juror and consider whether [we] might have reached a different conclusion." *People v. Harrison*, 2020 CO 57, ¶ 33. Instead, we view the evidence

as a whole and in the light most favorable to the prosecution to determine if it is "substantial and sufficient to support a conclusion by a reasonable mind that the defendant is guilty of the charge beyond a reasonable doubt." *Johnson*, ¶ 13 (citation omitted).

¶ 17 As relevant in this case, a person commits sexual exploitation of a child if that person knowingly "[p]ossesses or controls any sexually exploitative material," § 18-6-403(3)(b.5), C.R.S. 2020,[1] or if they knowingly "[p]ossess[] with the intent to deal in, sell, or distribute, including but not limited to distributing through digital or electronic means, any sexually exploitative material," § 18-6-403(3)(c). Sexually exploitative material includes a photograph or video that "depicts a child engaged in, participating in, observing, or being used for explicit sexual conduct." § 18-6-403(2)(j).

¶ 18 In this context, "possession" means "the non-exclusive control or dominion over sexually exploitative material." *People v. Marsh*, 396 P.3d 1, 8 (Colo. App. 2011) (*Marsh I*), *aff'd*, 2017 CO 10M (*Marsh II*). A person acts "knowingly" with respect to conduct or a

[1] We cite the version of the statute in effect at the beginning of the charged date range of Slusher's offenses.

circumstance if "he is aware that his conduct is of such nature or that such circumstance exists." § 18-1-501(6), C.R.S. 2025.

B. Unallocated Space

¶ 19 Slusher does not dispute that the evidence would support a finding that he had exclusive control over SI-6. Nor does he dispute that sexually exploitative material was found in the unallocated space on that computer (and on SI-9). But he relies on *Marsh II* and *State v. Ballantyne*, 543 P.3d 1152, 1160 (Kan. Ct. App. 2024), to argue that the presence of such material in a computer's unallocated space cannot alone establish knowing possession.

¶ 20 In *Marsh II*, the supreme court held that internet cache files stored on a defendant's hard drive — images that are "automatically downloaded when an image is viewed online" — may constitute some evidence that the defendant knowingly possessed those images. *Marsh II*, ¶ 29. But such files were not alone sufficient to prove knowing possession where "numerous people had access to the computer" and there was evidence that "viruses, hacking, and other means" could cause a computer to display and download sexually exploitative images without the user's knowledge. *Id.* at ¶ 35; *see also Ballantyne*, 543 P.3d at 1160 ("[T]he mere presence of

child pornography in a computer's cache or unallocated space, without more, is not sufficient to establish knowing possession.").

¶ 21 There are a couple differences between *Marsh II* and this case. First, other than the evidence that Campbell initially set up SI-6, there was no evidence that "numerous people had access to the computer." *Marsh II*, ¶ 35. To the contrary, Campbell testified that he never used it, and the forensic analyst testified that Slusher had "the most information as a user" on the computer and had been the exclusive user before the investigation. Second, there was no evidence that the images in SI-6's unallocated space could have gotten there without the user's knowledge — whether through a virus, hacking, or other means. *See id.* at ¶¶ 30, 35; *see also Ballantyne*, 543 P.3d at 1158, 1171 (noting testimony that internet cache files could be downloaded onto computer "through some automatic function" without picture ever being visible on screen). Rather, the forensic analyst testified that the files in the unallocated space "were on the device at some point" and then deleted.

¶ 22 But even assuming that *Marsh II*'s holding concerning internet cache files applies to all files in unallocated space, this case involves more than the mere presence of such files. As addressed

below, another computer that Slusher regularly used (SI-9) had files containing sexually exploitative material in the recycle bin. *See Marsh II*, ¶ 36 (holding that the evidence was sufficient where other images in the defendant's deleted files were sexually exploitative). And both SI-6 and SI-9 had other data — "most recently opened" data and link files — indicating that files with titles consistent with sexually exploitative material had previously been located on, or accessed from, those computers. *Cf. id.* at ¶ 35 (noting other evidence of the defendant's access to child pornography, including that child pornography websites were saved to internet "Favorites").

¶ 23 Moreover, both SI-6 and SI-9 had a file-sharing program installed that allowed those computers to share files through BitTorrent, and four of the files in SI-9's unallocated space were screenshots of videos that the investigator had downloaded from the home's IP address through that program. To be shareable, those videos must have been in a shared folder — not unallocated space — at the time. From this evidence, a jury could have reasonably inferred that Slusher knowingly possessed the files in the unallocated space *before* deleting them. *See Lee v. State*, 507 P.3d 483, 489 (Alaska Ct. App. 2022) (holding that presence of

BitTorrent on defendant's computer was evidence that he possessed files in shared folder before he deleted them); *People v. Cook*, 197 P.3d 269, 279 (Colo. App. 2008) (holding that evidence was sufficient where, among other things, "there was a file sharing program on one computer that contained defendant's profile").

¶ 24 Slusher asserts that the specific files the investigator downloaded through Torrential Downpour were not found on any of the computers (though screenshots from those videos were). But such direct evidence is not required. *See People v. Martinez*, 165 P.3d 907, 915 (Colo. App. 2007) (holding that circumstantial evidence was sufficient to prove knowing possession of child pornography). The evidence that the files were downloaded from a computer at the IP address — along with the evidence that both SI-6 and SI-9 had a file-sharing program that allowed them to share such files — was sufficient to support a conclusion that those files were on one of those computers at some point. And although Slusher cites Campbell's testimony that he gave SI-6 to Slusher after the summer of 2021, there was also testimony that Slusher exclusively was using the computer before then. It was for the jury to resolve any inconsistencies in the evidence. *See Harrison*, ¶ 33.

¶ 25 In light of this evidence, Slusher's contention that he did not access the files or know they existed *while they were in unallocated space* misses the point. Viewed in the light most favorable to the prosecution, the evidence is sufficient to support a jury finding beyond a reasonable doubt that Slusher knowingly possessed the sexually exploitative material *before* it was deleted and moved to unallocated space. *See Marsh II*, ¶¶ 34-36; *Lee*, 507 P.3d at 489.

C. Nonexclusive Possession of SI-9 and SI-10

¶ 26 We also reject Slusher's contention that the evidence was insufficient to prove that he knowingly possessed the sexually exploitative material on SI-9 and SI-10 because those computers were in shared space and accessible by other residents of the home.

¶ 27 Possession under section 18-6-403 "need not be exclusive." *Marsh I*, 396 P.3d at 8; *see also Martinez*, 165 P.3d at 915 (holding that jury was "correctly instructed that proof of exclusive possession was not required"). All that is required is that the defendant knowingly had control or dominion over the sexually exploitative material. *Marsh I*, 396 P.3d at 8.

¶ 28 There was ample evidence to support a finding that Slusher exercised at least nonexclusive control over SI-9 and SI-10 and, in

so doing, knowingly possessed the sexually exploitative material on those computers. He was the registered owner of both computers, his email account was used consistently on both, the username on SI-9 consisted in part of his initials, and his OneDrive account was set up on SI-10. *See Martinez*, 165 P.3d at 915 (holding that the evidence was sufficient where the defendant "used [the] computer and account profile" that the sexually exploitative material was on). The home's property manager testified that although there was a "community computer in the living room," Slusher was "probably the only one that did use it." And there was no evidence that anyone other than Slusher regularly accessed or used SI-9.

¶ 29 Beyond the evidence of Slusher's extensive use of the computers, Slusher told an investigator he knew what "torrents" were — the type of file-sharing program that was installed on SI-9 and that had been used to share the sexually exploitative files that were downloaded by the investigator. He also volunteered that his cell phone had once "browsed the internet for how to install BitTorrent" (though he claimed it had been accidental).

¶ 30 Even without direct evidence that Slusher accessed or viewed the sexually exploitative material on SI-9 and SI-10, this evidence

was sufficient to prove that he knowingly possessed that material. *See id.* The fact that others also had access to the computers and may also have knowingly possessed the files does not render the evidence insufficient to support Slusher's conviction. *Id.*

D. Ex Post Facto Law

¶ 31 Slusher also embeds within his challenge to the sufficiency of the evidence an argument that his conviction for possession violates the Ex Post Facto Clauses of the United States and Colorado Constitutions because he was charged under a version of section 18-6-403(3)(b.5) that did not become effective until two months after the beginning of the charged date range of his offense.

¶ 32 Specifically, the charged date range for Slusher's possession offense was July 1, 2021, to November 30, 2021. In July 2021, section 18-6-403(3)(b.5) prohibited knowingly "[p]ossess[ing] or control[ling] any sexually exploitative material." But effective September 7, 2021, the statute was amended to add "[a]ccesses with intent to view" and "views." Ch. 446, sec. 2, § 18-6-403(3)(b.5), 2021 Colo. Sess. Laws 2941. Both the complaint and the jury instructions included the language added by the amendment.

¶ 33 Because the evidence was sufficient to support a conviction under the pre-amendment version of the statute, the amendment has no bearing on the sufficiency of the evidence analysis.

¶ 34 To the extent Slusher asserts his ex post facto argument as a stand-alone basis for vacating his possession conviction, it would appear at first blush to have some merit. *See People v. Luman*, 994 P.2d 432, 436-37 (Colo. App. 1999) (holding that application of statute to date range beginning before its enactment violated prohibition on ex post facto laws). But *Marsh II* held that the prior version of the statute — the one in effect at the beginning of the charged date range — already prohibited accessing and viewing sexually exploitative material. *Marsh II*, ¶ 28 ("[K]nowingly seeking out and viewing child pornography on the internet constitutes knowingly possessing or controlling it under the statute.").

¶ 35 Thus, the September 2021 amendment did not "impose[] punishment for an act which was not a crime when it was committed" or otherwise "change the legal consequences of [Slusher's] acts completed before its effective date." *People v. Gholston*, 26 P.3d 1, 12 (Colo. App. 2000). It is therefore not an ex post facto law as applied to Slusher. *See id.* at 12-13.

III. Motion to Suppress

¶ 36 Slusher next contends that the district court erred by denying his motion to suppress the evidence resulting from the investigator's use of Torrential Downpour. We again disagree.

A. Additional Background

¶ 37 Slusher moved to suppress evidence of the files the investigator downloaded through Torrential Downpour and all other evidence resulting from the ensuing search warrant. He argued that the use of Torrential Downpour was an unconstitutional warrantless search and trespass because it "exploit[ed] an opening in the user's network" created by the BitTorrent software to "hack[] into SI-6" and download entire files from that computer.

¶ 38 At the evidentiary hearing on the motion to suppress, the investigator testified as follows about BitTorrent and Torrential Downpour. BitTorrent is a peer-to-peer file-sharing program that can be installed on a phone or computer. It allows users on the BitTorrent network to send and receive files to and from other users. The files are broken up into multiple pieces so that when a user downloads a file, they are not necessarily receiving all pieces of that file from the same other user. Instead, BitTorrent connects to

multiple users at the same time and receives pieces of the file from each user, which increases the speed of the download.

¶ 39 When a user installs BitTorrent, the program creates a "shared folder" on the computer. Files downloaded through BitTorrent go into this folder, and anything in the folder is accessible to other BitTorrent users. A BitTorrent user can only access files in other users' shared folders, not other files on their computers.

¶ 40 The process of one BitTorrent user connecting to another is called a "handshake." When this handshake occurs, each user may download files from the other and send files (or pieces of files) that the other user is looking for. Generally, the BitTorrent network "tries to enforce sharing," meaning that if a user only downloads files without sharing files in return, the user may get "choked out."

¶ 41 Torrential Downpour is a proprietary government software program that connects with BitTorrent users seeking to share and download child sex abuse material. It identifies files known to contain such material and IP addresses known to have sought out such files.[2] It then reaches out to an identified IP address to see if

[2] More precisely, the identification of IP addresses is completed by a related program called Torrential Downpour Receptor.

it is sharing any of the identified files. If it is, Torrential Downpour downloads the files from the other user's shared folder. Like BitTorrent, Torrential Downpour cannot download files from another user unless those files are in the other user's shared folder.

¶ 42 Torrential Downpour operates differently than a typical BitTorrent user in two primary ways. First, Torrential Downpour does not share any files. It "offer[s] to share," but because it never has anything the other user needs, it makes it "seem like [it's] sharing but [it's] not." Second, Torrential Downpour connects to only one computer at a time, which allows it to download an entire file from a single source. Torrential Downpour also differs from a typical BitTorrent user in that it targets specific IP addresses.

¶ 43 After the hearing, the district court denied Slusher's motion to suppress. It concluded that although Slusher had a reasonable expectation of privacy in his computer, he did not have any privacy interest in the files he sent and received over the peer-to-peer file-sharing program or in the IP address he used to share those files.

B. Standard of Review and Applicable Law

¶ 44 A ruling on a motion to suppress presents a mixed question of fact and law. *People v. Seymour*, 2023 CO 53, ¶ 19. We defer to the

district court's factual findings if they are supported by competent evidence and review the legal effect of those findings de novo. *Id.*

¶ 45 Both the United States and Colorado Constitutions prohibit "unreasonable searches and seizures." U.S. Const. amend. IV; Colo. Const. art. II, § 7. A search occurs when the government infringes on an individual's "reasonable expectation of privacy." *Seymour*, ¶ 20. To determine if a claimed privacy interest warrants constitutional protection, courts consider (1) whether the individual "exhibited an actual (subjective) expectation of privacy"; and (2) whether, objectively, "the expectation [is] one that society is prepared to recognize as 'reasonable.'" *Id.* at ¶ 22 (citation omitted).

¶ 46 A search also occurs when the government physically intrudes in a constitutionally protected area in order to obtain information. *United States v. Jones*, 565 U.S. 400, 404-05, 407 (2012).

C. Reasonable Expectation of Privacy

¶ 47 As Slusher appears to acknowledge, he had no reasonable expectation of privacy in the files that he shared on the BitTorrent network. Although a person has a reasonable expectation of privacy in their personal computer, that expectation does not encompass files that the person makes available through a file-

sharing software. *People v. Phipps*, 2016 COA 190M, ¶¶ 26, 30. Thus, when Slusher made the files available to everyone on the BitTorrent network, he lost any reasonable expectation of privacy he had in those files. *See United States v. Ewing*, 140 F.4th 1339, 1348 (11th Cir. 2025) (holding that the defendant had no reasonable expectation of privacy in files he shared on BitTorrent because everyone on the BitTorrent network had access to the files).

¶ 48 Relying on *United States v. Horton*, 863 F.3d 1041, 1047 (8th Cir. 2017), and *Kyllo v. United States*, 533 U.S. 27, 40 (2001), Slusher asserts that the government's use of technology to discover those files was still a search. In *Horton*, law enforcement sent computer code to the defendants' computers that "searched those computers for specific information and sent that information back to law enforcement." 863 F.3d at 1047. In *Kyllo*, the government used technology to "explore details of the home that would [otherwise] have been unknowable." 533 U.S. at 40. In other words, both cases involved government infiltration of areas in which the defendant otherwise had a reasonable expectation of privacy.

¶ 49 The investigator's use of Torrential Downpour was different. Although the program itself is "not in general public use," *id.*, it did

not "go" anywhere Slusher had not already invited the public. It simply allowed the investigator to download files that Slusher had already made publicly available — files that any BitTorrent user could have downloaded. *See Ewing*, 140 F.4th at 1349-50 (holding that the government's use of Torrential Downpour was not a search and citing cases concluding that the government does not conduct a search "when it downloads files that a person shares over a public network"); *United States v. Hoeffener*, 950 F.3d 1037, 1044 (8th Cir. 2020) (reaching the same conclusion regarding Torrential Downpour and rejecting the defendant's "attempt to distinguish BitTorrent software from other peer-to-peer programs").

¶ 50 Slusher nevertheless asserts that he had a reasonable expectation of privacy in his "identity and address" because that information was not shared with other BitTorrent users. By that, we understand him to mean his IP address — the unique string of numbers assigned to an individual computer or network that helps identify a specific user or user's location. *Seymour*, ¶ 8 n.2; *see also id.* at ¶¶ 28-32 (holding that individuals have a reasonable expectation of privacy in their internet search histories "when viewed . . . in connection with an anonymized IP address").

¶ 51 As an initial matter, we question whether the record supports Slusher's premise — that his IP address was not shared with other BitTorrent users. It is true that the investigator testified that regular BitTorrent users cannot seek out files from a particular IP address the way that Torrential Downpour does. But he also testified that when two computers exchange information through a "handshake," they "would know [each other's] IP address." He explained that, in a handshake, the two computers "tell each other what [their] IP addresses are, what port [they're] using, and then they report what pieces [of the requested file] they have."

¶ 52 We also note that this argument appears to confuse the sequence by which law enforcement connected the shared files to Slusher's group home. The investigator did not download the files and then identify the IP address of the computer that had sent them. Rather, he targeted a particular IP address (that had previously been identified as seeking child sex abuse material[3]) and

[3] We recognize that these IP addresses are identified by Torrential Downpour Receptor, another government program. But Slusher did not challenge this first step in the process, which consists merely of logging the IP addresses of computers that request particular files from a government computer on the BitTorrent network.

downloaded files that IP address had publicly shared. Another investigator then identified the physical address of that subscriber through a different court order (which Slusher does not challenge).

¶ 53 In any event, we conclude that Slusher did not have a reasonable expectation of privacy in the IP address, distinct from the shared files. In *Seymour*, the supreme court first concluded that the defendant had a reasonable expectation of privacy in his Google search history. *Seymour*, ¶¶ 26, 32. It then concluded that the government had infringed on that privacy interest, even though the search history it received was tied to an IP address and not the defendant himself. *Id.* at ¶ 31. In contrast, Slusher had no reasonable expectation of privacy in the files the investigator downloaded. Slusher cites no authority to support the proposition that someone can publicly share illegal files while maintaining a reasonable expectation of privacy in the location (physical or digital) from which those files were shared. We decline to so hold.

D. Trespass

¶ 54 For similar reasons, we also reject Slusher's contention that the investigator's use of Torrential Downpour physically intruded,

or trespassed, onto Slusher's computer. *See Jones*, 565 U.S. at 404-05; *Florida v. Jardines*, 569 U.S. 1, 5 (2013).

¶ 55 Unlike in *Jardines*, the investigator did not go anywhere or do anything that Slusher had not authorized the public to go and do. *See* 569 U.S. at 8-9 (holding that officer exceeded scope of implicit invitation to knock on front door by using drug-sniffing dog to explore area around home). By using BitTorrent and holding files in a shared folder, Slusher consented to other users downloading content from that folder. *See Ewing*, 140 F.4th at 1347. That is all the investigator did. There was no evidence that he "hacked" into the computer or accessed any information beyond files in the shared folder. *See id.* The only difference is that he reached out to Slusher's computer instead of ending up there by chance. But once there, the investigator did "no more than any private [BitTorrent user] might do." *Jardines*, 569 U.S. at 8 (citation omitted).

E. Seizure

¶ 56 Finally, Slusher asserts that the investigator conducted an unconstitutional seizure by downloading the files. *See Seymour*, ¶ 34 (holding that copying a user's digital data is a seizure).

¶ 57 But law enforcement can lawfully seize evidence of a crime in plain view if (1) the initial intrusion was legitimate; (2) law enforcement had a reasonable belief that the evidence seized was incriminating; and (3) law enforcement had a lawful right of access to the object seized. *People v. Glick*, 250 P.3d 578, 585 (Colo. 2011). In short, "as long as the incriminating character of an item is immediately apparent and the officer seizing it is lawfully located in a place from which he can both plainly see and lawfully access it, a warrantless seizure does not offend the Fourth Amendment." *Id.*

¶ 58 Even assuming that downloading files Slusher had made available for download was a seizure, the plain view doctrine is satisfied. The investigator's use of Torrential Downpour to access Slusher's shared folder was legitimate, and the investigator had a lawful right to access the files in that folder. And Slusher does not dispute that the incriminating nature of those files was readily apparent. *See People v. Alameno*, 193 P.3d 830, 836 (Colo. 2008) ("[T]he content of pornography is generally apparent on its face.").

¶ 59 Thus, because the investigator's use of Torrential Downpour was not a warrantless search and any seizure was lawful, the district court did not err by denying Slusher's motion to suppress.

IV. Motion for Disclosure of Torrential Downpour

¶ 60 Slusher also contends that the district court violated his constitutional rights by denying his motion for disclosure of the Torrential Downpour software to the defense. We disagree.

A. Additional Background

¶ 61 The same day that Slusher filed his motion to suppress, he also filed a motion for production of the Torrential Downpour software and source code. He argued that disclosure of the program was necessary to allow his counsel and expert to verify that it worked as described, noting, among other things, that the files allegedly downloaded through Torrential Downpour were not found on Slusher's computers. He proposed the entry of a protective order limiting disclosure to his defense team and expert.

¶ 62 Although the prosecution produced raw data and reports generated through Torrential Downpour, it opposed disclosure of the program itself. It argued that Torrential Downpour is a proprietary program and that the "compelling government interest" in keeping the program confidential outweighed any probative value to the defense. As to the source code, the prosecution argued that it likely would not even have had the ability to disclose it.

¶ 63 As described above, the prosecution's forensic analyst testified extensively at the evidentiary hearing and was subject to extensive cross-examination about how Torrential Downpour works.[4] Among other things, he testified that the program (1) only receives files and does not send them; (2) only accesses files in a user's shared folder; and (3) generates "extensive logging" to confirm that the files were downloaded from a single source. The analyst explained that it is "fairly common" for files downloaded through Torrential Downpour not to be found on the target device because the user can delete them before law enforcement is able to execute a search warrant.

¶ 64 After the evidentiary hearing, the district court denied the motion for disclosure. It applied a "balancing test," weighing law enforcement's interest in not compromising its investigations against Slusher's interest in "being able to . . . vet" how the program works, concluding that the latter did not outweigh the former. It explained that any questions about how the program works, and any discrepancies in the evidence, would be for the "jury to decide."

---

[4] The district court held a combined evidentiary hearing on the motion to suppress and the motion for production.

B. Applicable Law and Standard of Review

¶ 65 There is no general constitutional right to discovery in a criminal case. *People in Interest of E.G.*, 2016 CO 19, ¶ 23. Rather, a defendant is entitled to discovery only as specifically "authorized by the Constitution, the rules, or by statute." *Id.* at ¶ 13.

¶ 66 The Due Process Clause entitles a defendant to discovery of evidence that is "both constitutionally material and favorable to the accused." *Id.* at ¶ 24 (citation omitted). The constitutional right to present a defense entitles the defendant to "all reasonable opportunities to present evidence that might tend to create doubt as to the defendant's guilt." *People v. Elmarr*, 2015 CO 53, ¶ 26. Crim. P. 16(I)(d)(1) grants a district court discretion to "require disclosure to the defense of relevant material and information . . . upon a showing by the defense that the request is reasonable."

¶ 67 We review a district court's discovery order in a criminal case for an abuse of discretion. *E.G.*, ¶ 6. We review alleged due process violations de novo. *People v. Burlingame*, 2019 COA 17, ¶ 11.

C. Analysis

¶ 68 Slusher grounds his argument exclusively in his constitutional rights to due process and to present a defense. But he failed to

establish either that the Torrential Downpour software would have been favorable to his defense — at most offering speculation as to why it might have been — or that he was denied a reasonable opportunity to present evidence casting doubt on his guilt. *See E.G.*, ¶ 24; *Elmarr*, ¶ 26. To the contrary, defense counsel was permitted to extensively cross-examine prosecution witnesses about how Torrential Downpour functions. *Cf. People v. Eason*, 2022 COA 54, ¶¶ 48-49 (holding that destruction of body camera recording did not violate due process where defendant's assertion that it had exculpatory value was "conclusory and speculative" and defendant was otherwise able "to effectively cross-examine key witnesses"); *People v. McLean*, 661 P.2d 1157, 1159 (Colo. 1983) (holding that, to obtain disclosure of a confidential informant, an accused must make "a minimal showing," beyond "[c]onjecture and speculation," that disclosure "may be needed to present an adequate defense").

¶ 69 In arguing that he should have been permitted to examine the software to test the prosecution witnesses' assertions, Slusher relies on *United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012) — a case that ordered disclosure of a similar government program under a federal rule, not the Constitution. In *Budziak*, the

court recognized that the defendant was required to make a "threshold showing of materiality" under the federal rule. *Id.* at 1111 (citation omitted). But it concluded that the defendant had met that burden by presenting (1) evidence suggesting that the FBI may have only downloaded fragments of files; (2) evidence suggesting that the FBI could have used its software to override the defendant's sharing settings; and (3) a declaration from a computer forensics expert stating that discovery of the software could reveal information helpful to the defense. *Id.* at 1112-13, 1112 n.1.[5]

¶ 70 Slusher made no such showing. Although his counsel hypothesized about ways in which Torrential Downpour's operation might be problematic — such as if it downloaded files from multiple sources or accessed parts of the computer that were not publicly shared — the forensic analyst refuted each of those theories. And Slusher presented no evidence to the contrary. The most that

---

[5] Slusher also cites *State v. Pickett*, 246 A.3d 279, 284 (N.J. Super. Ct. App. Div. 2021), in which the court ordered production of a "novel probabilistic genotyping software" used by the prosecution's DNA expert to opine that the defendant's DNA was present. The court allowed the defendant access to the software for the purpose of challenging the reliability of the expert's testimony. *Id.* We deem those circumstances sufficiently distinguishable from the circumstances of this case that we do not address *Pickett* further.

defense counsel did was point out that the downloaded files were not on Slusher's devices four months later when the search warrant was executed — a point the forensic analyst reasonably explained by saying the files could have been deleted during that time.

¶ 71 That makes this case more like *Hoeffener* and *United States v. Pirosko*, 787 F.3d 358, 365-66 (6th Cir. 2015), than *Budziak*. In *Hoeffener*, the court held that the defendant was not entitled to disclosure of Torrential Downpour and its source code where he had offered "mere speculation that the software program could possibly access non-public areas of his computer or that there was a possibility that it malfunctioned during the officers' investigation." 950 F.3d at 1044. In *Pirosko*, the court distinguished *Budziak* because the defendant did not produce any evidence of government wrongdoing, "simply alleging that he might have found such evidence had he been given access to the government's programs." 787 F.3d at 365. Slusher presented no more evidence to support his motion than did the defendants in *Hoeffener* and *Pirosko*.

¶ 72 Without such a showing, the district court did not violate Slusher's constitutional rights or otherwise abuse its discretion by failing to require the prosecution to disclose Torrential Downpour.

V. Denial of Juror Challenges for Cause

¶ 73 Slusher's final argument is that the district court abused its discretion by not excusing four jurors for cause based on their responses during voir dire. We perceive no abuse of discretion.

A. Additional Background

¶ 74 During voir dire, defense counsel told the venire that the case was a child pornography case and that it was going to be presented with videos and photographs that were "quite severe in nature," including "images and videos of adult men . . . penetrating very young children maybe as young as perhaps two." She then asked:

> Is there anyone here who is feeling like based on kind of the description that I gave, the idea of having to sit on the jury and swear that you're going to pay attention, keep an open mind and all those things is an overwhelming expectation and something that you're not really sure you can do?

Several prospective jurors raised their hands, including jurors K.G., P.D., J.B., and P.C.

¶ 75 Defense counsel then asked several questions to individual jurors about whether they would be willing to find a defendant not guilty if the prosecution proved only six of seven elements of the crime beyond a reasonable doubt. Two jurors indicated that if the

prosecution failed to prove only one element of the crime — such as where the offense happened — they would still find the defendant guilty because to do otherwise would be a "technicality." Defense counsel asked who agreed with them. Although several prospective jurors raised their hands, none of the four jurors at issue did.

¶ 76 One prospective juror then explained: "[W]hat if these six elements that are proven are the kind that make me want to cry and throw up and the other one is . . . whatever, it would be really hard for me to not convict. I would venture to say impossible, especially if I was . . . that disturbed by the events themselves." Again, defense counsel asked who agreed and felt the same way, and twenty jurors raised their hands, including J.B. and P.D.

¶ 77 After defense counsel's voir dire, the district court told the venire that it had observed a "collective[] . . . visceral reaction" to defense counsel's description of the potential evidence in the case. The court then explained several principles, including that (1) the prosecution bears the burden of proof beyond a reasonable doubt; (2) the jury would have a "checklist of each element" that had to be proved beyond a reasonable doubt; and (3) if the prosecution did not prove each element, the jury must find the defendant not guilty.

¶ 78 The court continued:

> The other part of this has to do with where I started this conversation and that's this reaction that everybody has . . . . The question is not whether or not that may be disturbing, whether it's something you don't want to see, because I think pretty much every human in this room goes, I don't want to see that. . . . The question is whether or not if you see it you'll say, ah, the People don't have to prove any of the rest of their case, I saw this. They don't have to prove the elements. . . . I'm going to give the prosecution a freebie because I saw that picture. That's the question, okay? And I want to make sure that you folks are clear, that's what you're being asked, will you be fair. Will you be able to judge this based upon the evidence and the law and hold the prosecution to its burden. Don't give them a pass. Make them prove their case beyond a reasonable doubt. That's the question, okay?

¶ 79 The court then asked if there was "anybody who still feels . . . if the prosecution blows it, doesn't prove an element, I'm convicting him anyway." Several jurors raised their hands but not the four at issue. The court then asked: "[I]s just looking at [the] pictures . . . going to make you say, well, I don't care what else the prosecution proves, I saw the picture and he's guilty." Again, several jurors raised their hands but not the four at issue. The district court removed every juror who raised their hand to either question.

¶ 80 Defense counsel then challenged for cause all jurors who had raised their hands in agreement with the prospective juror's comment about having difficulty not convicting if the prosecution proved six of seven elements (including P.D.). The district court denied the challenges (with one exception). It explained that the jurors appeared "confused" and that the court had subsequently "clarified and reminded the jurors of the burden of proof." It said it was "satisfied that upon its further discussion with the jurors that had they persisted in the views they expressed, mostly without comment . . . they would have made the [c]ourt aware of it."

¶ 81 Defense counsel then challenged for cause three additional jurors (including J.B.) who had raised their hands in response to the question about their ability to pay attention and keep an open mind given the subject matter. Again, the district court denied the challenges. Defense counsel did not challenge K.G. or P.C., though they had also raised their hands in response to that question.

¶ 82 K.G., P.D., J.B., and P.C. all served on the jury.

B. Applicable Law and Standard of Review

¶ 83 To protect a defendant's constitutional right to a fair trial by an impartial jury, the district court must sustain a challenge for

cause to a prospective juror who is biased or otherwise "unwilling or unable to accept the basic principles of criminal law and to render a fair and impartial verdict." *Marko v. People*, 2018 CO 97, ¶ 20 (citation omitted); *see also* § 16-10-103(1)(j), C.R.S. 2025 ("The court shall sustain a challenge for cause" if a juror's state of mind "evinc[es] enmity or bias toward the defendant or the state."). But a court must not excuse a juror for cause "if the court is satisfied, from the examination of the juror or from other evidence, that [the juror] will render an impartial verdict according to the law and the evidence submitted to the jury at the trial." § 16-10-103(1)(j).

¶ 84 Thus, "[a] prospective juror's expression of concern or indication that he or she possesses a preconceived belief as to some aspect of the case does not . . . mandate exclusion of that juror for cause." *Marko*, ¶ 21. Rather, when a juror initially expresses such a belief, the district court should explain the correct legal principles and then determine whether the juror can fairly and impartially follow the law. *People v. Clemens*, 2017 CO 89, ¶¶ 16-17. In making this determination, the district court must evaluate the juror's state of mind based on their responses, demeanor, and body language throughout voir dire. *Marko*, ¶ 21. Absent rehabilitation,

a challenge for cause must be granted when the juror's statements "compel the inference that he or she cannot decide crucial issues fairly." *People v. Merrow*, 181 P.3d 319, 321 (Colo. App. 2007).

¶ 85 We review the district court's denial of a challenge for cause for an abuse of discretion. *Marko*, ¶ 22. In doing so, we grant the district court great deference because it is in "a superior position to evaluate the 'juror's credibility, demeanor, and sincerity.'" *Id.* (citation omitted). And we consider the district court's ruling in the context of the entire voir dire. *People v. Ambrose*, 2021 COA 62, ¶ 30. A district court abuses its discretion when its decision is manifestly arbitrary, unreasonable, or unfair. *Marko*, ¶ 22.

C. Preservation

¶ 86 Slusher groups K.G., P.D., J.B., and P.C. together and argues that all four should have been removed for cause. But he did not challenge K.G. or P.C. Although both raised their hands in response to the question about their ability to pay attention and keep an open mind, defense counsel did not identify either in the challenges for cause based on that question. Slusher thus waived

any challenge to those jurors.[6] *See Richardson v. People*, 2020 CO 46, ¶ 25 ("[D]efense counsel must 'challenge an allegedly biased juror to preserve the issue for appellate review.'" (citation omitted)).

D. Analysis

¶ 87 We conclude that the district court did not abuse its discretion by denying Slusher's challenges for cause to P.D. and J.B.[7]

¶ 88 Both jurors raised their hands in response to defense counsel's questions about (1) whether they were "not really sure" they could "pay attention" and "keep an open mind" and (2) whether it would be "really hard . . . to not convict" if six of seven elements were proved. But in context, those responses did not "compel the inference" that the jurors could not decide the issues fairly. *Merrow*, 181 P.3d at 321. As the district court noted, the first response indicated a "visceral reaction" to defense counsel's

---

[6] Slusher asserts that he challenged P.C. before voir dire based on her written response to the questionnaire. But the written response he cites — that the juror's "job as an advocate may make [them] biased on the side of the alleged victim" — was actually given by a different prospective juror, who did not serve as a juror at trial.

[7] To the extent Slusher's challenge for cause to all jurors who raised their hands in response to the two questions at issue could be construed to include K.G. and P.C. — even though defense counsel did not identify them — our analysis would apply equally to them.

description of the evidence and the "overwhelming expectation" that came with it. *See People v. Rabes*, 258 P.3d 937, 944 (Colo. App. 2010) (holding that juror's recognition of "danger that he would convict based on his reaction to explicit photos" did not require removal for cause). And the district court found that the second indicated confusion rather than an inability to follow the law.

¶ 89 Moreover, to the extent the jurors' responses initially indicated some preconceived inclination or confusion, the district court clarified the correct legal principles, including the prosecution's burden of proof as to each element. *See Clemens*, ¶ 17. After doing so, the court asked the jurors again whether they would be unable to apply the law. And while several jurors still indicated they could not, neither P.D. nor J.B. (nor K.G. nor P.C.) did. *See id.* at ¶ 22 (holding that jurors' silence in response to a similar question demonstrated a willingness to follow the law). Based on this lack of response and the jurors' conduct throughout voir dire, the court found that the jurors no longer persisted in their initial views. The district court was in the best position to make that determination based on the context of the entire voir dire. *See Marko*, ¶ 22.

¶ 90 Thus, because the record supports the district court's determination, we conclude that the court did not abuse its discretion by declining to remove the challenged jurors for cause.[8]

VI. Disposition

¶ 91 The judgment is affirmed.

JUDGE GROVE and JUDGE YUN concur.

---

[8] Slusher also asserts in a single sentence that the district court abused its discretion by failing to submit his proposed jury questionnaire to the venire and failing to grant him more time for voir dire. Because he does not develop these arguments, we do not address them. *See People v. Stone*, 2021 COA 104, ¶ 52.