APPENDIX

TABLE OF CONTENTS

APPENDIX A

Cite as 2023 Ark. App. 295

ARKANSAS COURT OF APPEALS

DIVISION III
No. CR-22-572

JONATHAN WALKER APPELLANT V. STATE OF ARKANSAS APPELLEE	Opinion Delivered May 17, 2023 APPEAL FROM THE CLARK COUNTY CIRCUIT COURT [NO. 10CR-20-107] HONORABLE BLAKE BATSON, JUDGE AFFIRMED AS MODIFIED

KENNETH S. HIXSON, Judge

Appellant Jonathan Walker was convicted in a jury trial of thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child and Walker was sentenced as a habitual offender to thirty consecutive fifteen-year prison terms. Pursuant to Ark. Code Ann. § 5-27-602(a)(2) (Repl. 2013), a person commits this offense "if the person knowingly possesses or views through any means, including on the Internet, any photograph, film, videotape, computer program or file . . . or any other reproduction that depicts a child or incorporates the image of a child engaging in sexually explicit conduct."[1] Walker's convictions arose from a cyber tip from an internet-service provider that resulted in a police search of Walker's computer

[1] A "'Child' means any person under seventeen years of age." Ark. Code Ann. § 5-27-601(1) (Repl. 2013).

equipment on which they found images of juvenile males in sexually explicit poses and juvenile males engaged in sexually explicit conduct with adult males. On appeal, Walker does not challenge the sufficiency of the evidence supporting the convictions; rather, Walker raises these seven arguments: (1) the trial court erred in not recusing; (2) the trial court erred in admitting the items seized from his home because the search was illegal; (3) the trial court erred in admitting his prior convictions from Oregon during the guilt phase of the trial; (4) the trial court erred in admitting images from his computer for which he was not charged; (5) the trial court erred in allowing the State to play a portion of Walker's statement to the police wherein his sex-offender status was discussed; (6) the trial court erred in admitting Walker's Oregon "pen pack" during the guilt phase of the trial; and (7) the trial court erred in refusing Walker's affirmative-defense jury instruction that he reasonably believed five of the persons depicted in the images were seventeen years of age or older. We affirm Walker's convictions, and we modify the sentencing order as explained below.

I. *Facts*

On April 28, 2020, an image or file from Walker's computer was uploaded to a Microsoft OneDrive account. Microsoft's internal algorithm program[2] determined, based on the "hash value" of the file, that the image was a known catalogued image of child

[2] Neither the mechanics nor the accuracy of the Microsoft internal algorithm program was challenged at trial and neither is an issue in this appeal.

pornography.[3] Without viewing the image and based solely on the hash value, Microsoft reported the image, the Internet Protocol (IP) address, and the date uploaded to the National Center for Missing and Exploited Children (NCMEC).[4] The IP address was associated with Suddenlink Communications. NCMEC then forwarded this information, along with the image, to the Arkansas State Police.

The Arkansas State Police has an internal task force referred to as the Internet Crimes Against Children Task Force (ICAC). Special Agents Adam Pinner and Corwin Battle are assigned to the task force and investigated the cyber tip from NCMEC. Agent Pinner reviewed the image and determined it constituted child pornography. Through its investigation, the ICAC determined that the account

---

[3] In technical terms, a hash value is an "algorithmic calculation that yields an alphanumeric value for a file." *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents. In the words of one commentator, "[t]he concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the hash value) unique to that data." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).

[4] NCMEC is a nonprofit private entity. NCMEC's Cyber Tipline is the nation's centralized reporting system for the online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child-sexual-abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the Internet.

name associated with the IP address was Jonathan Walker with a service and billing address at an apartment in Arkadelphia. Agent Pinner swore out an affidavit for a search warrant for Walker's apartment and computer equipment. The affidavit set forth the facts constituting probable cause, which included information that the uploaded image was of a prepubescent male depicting nudity in a sexually suggestive pose. Based on the information in the affidavit, a search warrant was issued.[5]

During the search of Walker's apartment, the police seized several laptop computers, including a Dell computer with a Toshiba hard drive. While Walker's apartment was being searched, Walker was Mirandized and gave a statement. In his statement, Walker admitted that he lived alone at the apartment, that his wireless Internet was password protected, and that the computers belonged to him. Walker denied possessing any child pornography.

Agent Battle subsequently conducted a forensic examination of the Toshiba hard drive in the Dell computer seized from Walker's apartment. According to Agent Battle's trial testimony, the Windows operating system had the username "Jonathan." Agent Battle testified that the hard drive was divided into seven partitions and that the seventh partition of the hard drive contained hundreds of images and videos of child-sexual-abuse material, which he stated is synonymous with child pornography. The seventh partition also contained images of Walker,

---

[5] As will be discussed, *infra*, Walker filed a motion to suppress on the grounds that the affidavit for search warrant lacked probable cause, and after a suppression hearing, Walker's motion was denied.

his car, and his marriage license. Agent Battle testified that State's exhibits 1–30 contained images of child-sexual-abuse material retrieved from Walker's computers, and these exhibits were admitted into evidence at the jury trial.[6]

From this evidence, the jury found Walker guilty of thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child, and the jury sentenced Walker to a total of 450 years in prison. Walker now appeals.

II. *Points on Appeal*

A. The Trial Judge's Refusal to Recuse Himself

Walker's first argument on appeal is that the trial judge abused his discretion in refusing to recuse himself. During a pretrial hearing, Walker's attorney raised the issue of Circuit Judge Blake Batson's former law partnership with the prosecutor, Dan Turner. At the pretrial hearing, Walker's counsel argued:

> My client feels that he's being prejudiced about the fact that you and the prosecutor used to be in business together. And he believes that . . . representation of Arnold, Batson, Turner, and Turner is still showing up on the Internet, even if it's not on the sign.

Prosecutor Turner responded:

> I think this court has dealt with this very issue numerous times over the last twenty

---

[6] Several of the charged counts were video files, and in support of these counts, the State offered screen shots from the videos rather than the videos themselves.

> months. I don't think that's a basis for a requirement that the court recuse.

Judge Batson declined to recuse himself and stated:

> Mr. Walker, there are specific rules this court complies with. And the fact that there may be something on the Internet that indicates our past business relationship, it's not sufficient for disqualification.

Walker now assigns error to the trial judge's refusal to recuse himself due to the trial judge's former partnership with Turner and the alleged appearance of impropriety.

Canon 2.11(A)(1) of the Arkansas Code of Judicial Conduct states that "[a] judge shall disqualify himself or herself in any proceeding in which the judge's impartiality might be reasonably questioned, including . . ." when "[t]he judge has a personal bias or prejudice concerning a party or a party's lawyer[.]" Walker argues that because there was still information online that the trial judge and the prosecutor were practicing law together twenty months after the judge took the bench, the trial judge's impartiality was reasonably questioned, and there was at least an appearance of impropriety. Walker cites *Burrows v. Forrest City*, 260 Ark. 712, 543 S.W.2d 488 (1976), for the proposition that a trial judge should not remain on a case where there exists even an appearance of impropriety.[7] Walker further

[7] *Burrows* was a revocation case, and the supreme court reversed and remanded for a new trial with a new judge because, prior to the revocation hearing, the sitting judge had requested that appellant bring his toothbrush and also made numerous other comments during the proceedings that created the appearance of partiality.

asserts that the trial judge's adverse rulings indicated bias or an appearance of bias. For these reasons, Walker contends that the trial judge's refusal to recuse himself constituted reversible error. We disagree.

In *Owens v. State*, 354 Ark. 644, 654–55, 128 S.W.3d 445, 451–52 (2003), the supreme court set forth these standards:

> A trial judge has a duty not to recuse from a case where no prejudice exists. Thus, if there is no valid reason for the judge to disqualify himself or herself, he or she has a duty to remain on a case. There is a presumption that judges are impartial. The person seeking disqualification bears the burden of proving otherwise. The trial judge's decision not to recuse from a case is a discretionary one and will not be reversed on appeal absent an abuse of that discretion. An abuse of discretion can be shown by proving bias or prejudice on the part of the trial judge. To decide whether there has been an abuse of discretion, this court reviews the record to determine if prejudice or bias was exhibited. It is the appellant's burden to demonstrate such bias or prejudice.

(Citations omitted.)

We conclude that Walker failed to prove that the trial judge exhibited prejudice, and we hold that the trial judge's decision not to recuse himself was not an abuse of discretion. In *Carmical v. McAfee*, we stated that a trial judge is not required to recuse himself or herself if his or her former law partner is counsel in the proceeding at hand. 68 Ark. App. 313, 7 S.W.3d

350 (1999) (citing *Dolphin v. Wilson*, 328 Ark. 1, 942 S.W.2d 815 (1997)). Moreover, absent some objective demonstration by the appellant of the trial judge's prejudice, it is the communication of bias by the trial judge that will cause us to reverse his or her refusal to recuse. *Carmical*, *supra*. The mere fact that there were adverse rulings is not enough to demonstrate bias. *Id.* The fact that the trial judge and the prosecutor were former law partners did not require the trial judge's recusal, nor was there any demonstration of bias by the trial judge. Therefore, we reject Walker's argument that the trial judge was required to recuse from the case or that he abused his discretion in not recusing.

B. Suppression of Evidence

Walker next argues that the trial court erred in denying his motion to suppress the incriminating evidence based on his claim that the search of his apartment and computer equipment therein constituted a violation of his constitutional right against unreasonable searches and seizures. Walker's narrow argument is that, although Microsoft and NCMEC (both private entities) had observed a hash value of a file that was catalogued as child pornography, neither of those private entities actually opened the file to view and confirm that the file image contained child pornography prior to providing the cyber tip to the Arkansas State Police. Walker argues that when Agent Pinner opened the file and viewed the image, he exceeded the scope of the private search and that the search warrant was invalid because it was based almost entirely on this illegally obtained information.

In reviewing the denial of a motion to suppress evidence, this court conducts a de novo review based on the totality of the circumstances, reviewing findings of historical facts for clear error and determining whether those facts give rise to reasonable suspicion or probable cause, giving due weight to inferences drawn by the trial court. *Lewis v. State*, 2023 Ark. 12. A finding is clearly erroneous, even if there is evidence to support it, when the appellate court, after review of the entire evidence, is left with the definite and firm conviction that a mistake has been made. *Id.* We defer to the superiority of the trial court to evaluate the credibility of witnesses who testify at a suppression hearing. *Id.*

In the affidavit for search warrant, Agent Pinner stated:

> Microsoft OneDrive made the report to NCMEC on April 28, 2020. The cyber tip reported that one (1) image of apparent child pornography (unconfirmed) was uploaded to a Microsoft OneDrive Account. Microsoft OneDrive provided the image to NCMEC and I was eventually provided the image that was uploaded. The image is of a prepubescent minor male depicting nudity in a sexually suggestive pose.

Agent Pinner's affidavit went on to state that, with the IP address that had been provided in the cyber tip, it was later determined that the account associated with the IP address belonged to Walker. Based on Agent Pinner's affidavit, a search warrant was issued, and the illicit images were found on Walker's computer during the search.

A hearing was held on Walker's motion to suppress. At the suppression hearing, both Agents Pinner and Battle testified about the investigation and the process by which hash values are instrumental in detecting and investigating child pornography.

Agent Pinner testified that he was assigned to investigate the cyber tip received from NCMEC. Pinner stated that he commonly works with such cyber tips in his investigative duties with the ICAC. Agent Pinner explained that the cyber tip was the result of hash-value identification from a known catalogue of images that had been previously determined to be child-sexual-abuse material. He compared a hash value to the DNA of a person. Agent Pinner stated that, although Microsoft and NCMEC had identified the file as containing known child pornography by the hash value and were in possession of the file before forwarding it to the Arkansas State Police, neither Microsoft employees nor NCMEC employees had actually viewed the image. Agent Pinner opened the file and confirmed its content as child pornography.

Agent Battle similarly testified that he is familiar with the cyber tipline used by NCMEC. Agent Battle stated that it is customary for him to receive cyber tips from NCMEC and, through those cyber tips, initiate an investigation and swear out an affidavit for a search warrant. Agent Battle stated that hash-value identification is instrumental in the cyber tips generated by NCMEC. Agent Battle explained that a hash value is a "digital fingerprint" of a file, which is unique to the file and the image it contains. Agent Battle stated that NCMEC maintains a database of hash values that are known to contain child-sexual-

abuse material. Thus, NCMEC is able to compare a known hash value to a file and, if the hash values match, determine that the file contains child pornography.

Both the United States and Arkansas Constitutions prohibit unreasonable searches and seizures not supported by probable cause or reasonable suspicion. U.S. Const. amend. IV; Ark. Const. art. II, § 15. Such limitations do not apply to searches conducted by private parties because, under the private-search doctrine, the prohibition against unreasonable searches and seizures does not apply to searches conducted by private citizens. *Whisenant v. State*, 85 Ark. App. 111, 146 S.W.3d 359 (2004). However, the government agency may not then exceed the scope of the private search unless it has the right to make an independent search. *Id.*

Walker argues that when law enforcement received a cyber tip from NCMEC regarding an unopened file that was alleged—but not visually confirmed—to contain child pornography, law enforcement exceeded the scope of the private search by opening the file. Walker argues that law enforcement lacked probable cause from the hash value itself, and that only by viewing the contents of the file did they have probable cause of criminal activity. When a search warrant is based on illegally obtained information, the appellate court examines the search warrant by excising the offending information from the search warrant and determines whether the affidavit nevertheless supports the issuance of a search warrant. *Lauderdale v. State*, 82 Ark. App. 474, 120 S.W.3d 106 (2003). Walker argues that, when excising from Agent Pinner's affidavit his statement that the file image was of a prepubescent

minor male depicting nudity in a sexually suggestive pose, there was no probable cause to issue the search warrant. Walker thus argues that the trial court's denial of his motion to suppress was clearly erroneous. For the following reasons, we disagree.

In discussing the private-search doctrine in *Whisenant*, *supra*, we stated that there is no additional intrusion by the government agency during its inspection of the materials where the agent learned nothing that had not previously been learned during the private search. The critical inquiry is whether the authorities obtained information with respect to which the defendant's expectation of privacy had not already been frustrated. *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018). When the government's conduct merely confirms information gleaned in a private search and does not enable the government to discover information that had not previously been learned during the private search, it does not constitute a subsequent search. *United States v. Jacobsen*, 466 U.S. 109 (1984). In *Jacobsen*, the Supreme Court observed that protecting the risk of misdescription by the private party hardly enhances any legitimate privacy interest and is not protected by the Fourth Amendment.

Both Microsoft and NCMEC determined from the hash value of one of Walker's files that the file contained child pornography. Agents Pinner and Battle testified at the suppression hearing about hash-value technology and its accuracy and effectiveness in investigating internet crimes against children. Agent Pinner compared hash-value identification to a DNA match, and Agent Battle compared it to a fingerprint match. After both private

entities observed the hash value and determined from the hash value that the file contained child pornography, the information was forwarded to the Arkansas State Police. By opening the file and viewing its contents, Agent Pinner merely confirmed what had already been learned in the private search; therefore, no constitutional violation occurred.

In reaching our decision on the suppression issue, we are strongly persuaded by the Fifth Circuit Court of Appeals' decision in *Reddick*, *supra*. In *Reddick*, the defendant uploaded digital-image files to Microsoft SkyDrive. SkyDrive uses a program to automatically scan the hash values of user-uploaded files and compare them to the hash values of known images of child pornography. When a match is detected between the hash value of a user-uploaded file and a known child-pornography hash value, it creates a cyber tip and sends the file—along with the uploader's IP address information—to NCMEC. Microsoft sent cyber tips to NCMEC based on the hash values of files that the defendant had uploaded to SkyDrive. NCMEC then forwarded the cyber tip to the Corpus Christi Police Department. Upon receiving the cyber tip, a police officer opened the suspect files and confirmed that each contained child pornography. The police officer then applied for and received a warrant to search the defendant's home and seize his computer. The defendant argued that the police officer's warrantless opening of the files associated with the cyber tip—which were not first opened and viewed by Microsoft or NCMEC—was an unlawful search. The Fifth Circuit Court of Appeals disagreed.

Before addressing the merits of the suppression issue in *Reddick*, the federal appeals court set forth

the following observations regarding hash-value technology and its usefulness in combating child pornography:

> Private businesses and police investigators rely regularly on "hash values" to fight the online distribution of child pornography. Hash values are short, distinctive identifiers that enable computer users to quickly compare the contents of one file to another. They allow investigators to identify suspect material from enormous masses of online data, through the use of specialized software programs—and to do so rapidly and automatically, without the need for human searchers. Hash values have thus become a powerful tool for combating the online distribution of unlawful aberrant content.
>
> ….
>
> In technical terms, a hash value is an "algorithmic calculation that yields an alphanumeric value for a file." *United States v. Stevenson*, 727 F.3d 826, 828 (8th Cir. 2013). More simply, a hash value is a string of characters obtained by processing the contents of a given computer file and assigning a sequence of numbers and letters that correspond to the file's contents. In the words of one commentator, "[t]he concept behind hashing is quite elegant: take a large amount of data, such as a file or all the bits on a hard drive, and use a complex mathematical algorithm to generate a relatively compact numerical identifier (the

> hash value) unique to that data." Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38, 38 (2005).
>
> Hash values are regularly used to compare the contents of two files against each other. "If two nonidentical files are inputted into the hash program, the computer will output different results. If the two identical files are inputted, however, the hash function will generate identical output." Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 541 (2005). Hash values have been used to fight child pornography distribution by comparing the hash values of suspect files against a list of the hash values of known child pornography images currently in circulation. This process allows potential child pornography images to be identified rapidly, without the need to involve human investigators at every stage.

Reddick, 900 F. 3d at 636-37.

The *Reddick* court concluded that the police officer did not conduct an illegal search when he viewed images that had not been actually viewed by Microsoft or NCMEC but had been identified by the private entities as child pornography by their hash values. The appeals court began by stating that, under the private-search doctrine, "the critical inquiry under the Fourth Amendment is whether the authorities obtained information with respect to which the defendant's expectation of privacy had not already been frustrated." *Reddick*, 900 F.3d at 638 (citing *United States v. Runyan*, 275 F.3d 449 (5th

Cir. 2001)). The *Reddick* court stated that when the police officer first received the defendant's files, he already knew their hash values matched the hash values of child-pornography images known to NCMEC. *Reddick*, 900 F.3d at 639. The court went on to state that hash-value comparison allows law enforcement to identify child pornography with almost absolute certainty because hash values are specific to the makeup of a particular image's data, which can be described as a unique digital fingerprint. *Id.* The court held that when the police officer opened the files, there was no significant expansion of the search that had been conducted previously by a private party and that his visual review of the images merely dispelled any residual doubt about the contents of the files. *Id.* The federal appeals court in *Reddick* stated that the government effectively learned nothing from the police officer's viewing of the files that it had not already learned from the private search, and that under the private-search doctrine, the government did not violate the defendant's Fourth Amendment rights. *Id.* at 640.

We also find the Sixth Circuit Court of Appeals' decision in *United States v. Miller*, 982 F.3d 412 (2020), to be instructive. In *Miller*, the appeals court also dealt with the issue of whether a police officer could view images that had been identified by private entities as child pornography only by hash identification and not by visual inspection. The *Miller* court focused on the level of certainty of the hash identification. The court wrote:

> The magistrate judge, whose findings the district court adopted, found that the technology was "highly reliable—akin to the reliability of DNA." *United States v. Miller*,

> 2017 WL 9325815, at *10 (E.D. Ky. May 19, 2017). The evidence in one cited case suggested that "[t]he chance of two files coincidentally sharing the same hash value is 1 in 9,223,372,036,854,775,808." *United States v. Dunning*, 2015 WL 13736169, at *2 (E.D. Ky. Oct. 1, 2015) (citation omitted). (That is 1 in 9.2 *quintillion* in case you were wondering.) Another cited source suggested that the common algorithms "will generate numerical identifiers so distinctive that the chance that any two data sets will have the same one, no matter how similar they appear, is less than one in one billion." Barbara J. Rothstein et al., *Managing Discovery of Electronic Information: A Pocket Guide for Judges* 38 (2d ed. Federal Judicial Center 2012).

Miller, 982 F.3d at 430. The *Miller* court concluded that, through the information available, "a computer's 'virtual' search of a single file creates more certainty about the file's contents than a person's 'manual' search of the file." *Id.* The *Miller* court applied the private-search doctrine and rejected the defendant's Fourth Amendment challenge. *Id.* at 431.[8]

---

[8] We observe that Walker relies on the Ninth Circuit Court of Appeals decision in *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021), asserting that the appeals court in that case reached a different result than in *Reddick* or in *Miller* on similar facts. However, as stated, we are persuaded by the analysis in *Reddick* and *Miller*, and we apply those holdings to the facts herein.

The testimony by Agents Pinner and Battle at the suppression hearing showed that the hash-value match that resulted in the cyber tip from private entities was akin to a DNA match or fingerprint match. The reliability of hash-value matching to identify known child pornography was explained at length in both *Reddick* and *Miller*, discussed above. By visually inspecting the image provided by the private entities, Agent Pinner learned no more than had already been learned from the hash-value analysis of the private search, and his review of the image merely confirmed what was already known and dispelled any residual doubt about the contents of the file. *See Reddick*, *supra*. Therefore, we conclude that under the private-search doctrine, Agent Pinner's opening of the file did not violate Walker's constitutional right against unreasonable searches and seizures, and we hold that the trial court's denial of Walker's motion to suppress was not clearly erroneous.

C. Admission of Prior Crimes

Walker's next argument is that the trial court erred by admitting Walker's prior convictions during the guilt phase of the trial. Prior to trial, the State filed a notice of intent to introduce evidence pursuant to Rule 404(b) of the Arkansas Rules of Evidence. This evidence consisted of Walker's three 2009 Oregon convictions for encouraging child sexual abuse in the first degree. Walker subsequently filed a motion in limine to exclude the convictions, arguing that they were inadmissible under Rule 404(b) and also that the evidence was more prejudicial than probative under Rule 403. After a hearing on Walker's motion in limine, the trial court denied the

motion and allowed the State to introduce the convictions at trial.

Rule 404(b) provides:

> **Other Crimes, Wrongs, or Acts.** Evidence of other crimes, wrongs, or acts is not admissible to prove the character of a person in order to show that he acted in conformity therewith. It may, however, be admissible for other purposes, such as proof of motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.

The State is not entitled to introduce evidence of other offenses to persuade the jury that the accused is a criminal and likely to commit the crimes he has been charged with. *Green v. State*, 365 Ark. 478, 231 S.W.3d 638 (2006). However, if the evidence of another crime, wrong, or act is relevant to show that the offense of which appellant is accused actually occurred and is not introduced merely to prove bad character, it will not be excluded. *Lindsey v. State*, 319 Ark. 132, 890 S.W.2d 584 (1994). In dealing with issues relating to the admission of evidence pursuant to Rule 404(b), a trial court's ruling is entitled to great weight, and this court will not reverse absent an abuse of discretion. *Green*, *supra*.

Walker argues that the trial court abused its discretion in admitting the prior convictions under Rule 404(b) because this evidence was not independently relevant to prove some material point at issue but was rather introduced merely to prove he is a criminal. We disagree.

The statutory elements of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child—with which Walker was charged in this case—are very similar to the elements of encouraging child sexual abuse in the first degree under the 2009 version of the Oregon statute upon which Walker was convicted.[9] Moreover, the record reveals factual similarities between Walker's Oregon convictions and the charges herein. Here, the proof showed that Walker possessed multiple images on his computer of juvenile males in sexually explicit poses and juvenile males engaged in sexually explicit conduct with adult males. In the Oregon case, the investigation began when a public library reported that a printed copy of an adult male sodomizing a juvenile was discovered in a restroom. The police confirmed that Walker's fingerprints were on the photograph, and a subsequent search of a flash drive in Walker's possession uncovered 120 images of nude juveniles, juveniles in sexually explicit poses, and a juvenile engaging in sexual acts. Walker admitted to the Oregon authorities that he had downloaded these images from a computer.

We conclude that the Oregon convictions were probative of Walker's knowledge and intent under Rule 404(b). Walker's defense at trial was that he simply did not possess any of the illegal images attributed to him, as he stated in his opening argument and argued in his directed-verdict motion and closing argument. In Walker's custodial

---

[9] At the time of Walker's 2009 Oregon convictions, the elements of Or. Rev. Stat. § 163.684 prohibited possessing photographs or other visual recordings of sexually explicit conduct involving a child.

interview with the police, Walker denied possessing child pornography on his computer equipment. Therefore, the prior convictions for similar conduct were relevant to establish Walker's knowledge and intent to commit these crimes. The supreme court has held that Rule 404(b) evidence is admissible to prove knowledge and intent of the criminal defendant due to similar conduct. *See, e.g.*, *Davis v. State*, 362 Ark. 34, 207 S.W.3d 474 (2005) (similar incident of sexual assault admitted to show intent); *Fells v. State*, 362 Ark. 77, 207 S.W.3d 498 (2005) (victim of similar, but earlier, rape by defendant allowed to prove intent, motive, or plan); *see also Nelson v. State*, 365 Ark. 314, 229 S.W.3d (2006) (affirming the admission of multiple prior drug convictions to show intent when Nelson claimed he was simply in the car and the drugs found there belonged to another passenger.) For these reasons, we hold that the trial court's decision to admit the prior convictions under Rule 404(b) was not an abuse of discretion.

However, as Walker points out in his brief, even if evidence is relevant under Rule 404(b), Arkansas Rule of Evidence 403 provides that evidence may be excluded if its probative value is substantially outweighed by the danger of unfair prejudice. The standard of review for the admission of Rule 403 evidence is whether the trial court abused its discretion. *Harmon v. State*, 286 Ark. 184, 690 S.W.2d 125 (1985). Walker argues that, even if the evidence of his prior convictions had some probative value, the evidence was unfairly prejudicial under Rule 403. We, however, disagree with this argument as well. In *Rounsaville v. State*, 374 Ark. 356, 288 S.W.3d 213 (2008), the supreme court stated that evidence offered by the State in a criminal trial is

likely to be prejudicial to the defendant to some degree, otherwise it would not be offered. On this record, we find no abuse of discretion in the trial court's determination that the probative value of Walker's prior convictions was not substantially outweighed by the danger of unfair prejudice. Therefore, we find no error in the admission of the prior crimes.

D. Admission of Uncharged Images

In Walker's pretrial motion in limine, he also argued that the State should be prohibited from introducing other images seized from his computer for which he was not charged. After the hearing on Walker's motion, the trial court denied that portion of Walker's motion and ruled that these other images were admissible, and Walker now asserts that this was erroneous.

During Agent Battle's trial testimony, he explained that child-sexual-abuse material is the same thing as child pornography. Agent Battle testified that State's exhibits 1–30 contained images of child-sexual-abuse material, and these exhibits were admitted as evidence of Walker's guilt on the charged offenses. Agent Battle explained further that child-exploitative material is material depicting a child that may be in a provocative or sexual pose, but the child is clothed. Over Walker's objection, the State was permitted to admit exhibits 31–45, for which Walker was not charged and that consisted of fifteen images from Walker's computer containing child-exploitative material.

Walker argues that the introduction of these uncharged images violated Rule 404(b) because they served no legitimate purpose and were introduced

only to show his propensity for viewing child-exploitative material. Walker also argues that this evidence was inadmissible because it was extremely prejudicial.

The mere fact that a photograph is inflammatory or is cumulative is not, standing alone, sufficient reason to exclude it. *Lewis v. State*, 2023 Ark. 12. However, if a photograph serves no valid purpose and could be used only to inflame the jurors' passions, it should be excluded. *Id.*

The State argues that the images of child-exploitative material were relevant to show Walker's predilection for sexualized images of prepubescent boys and to show knowledge, intent, absence of mistake, or accident under Rule 404(b), and we agree. In *Lewis*, *supra*, the supreme court affirmed the admission of additional uncharged pornographic images, stating that "[g]iven Lewis's defense that he lacked knowledge, the admission of the additional images was relevant to show knowledge, intent, and absence of mistake or accident." *Lewis*, 2023 Ark. 12, at 19–20; *see also Steele v. State*, 2014 Ark. App. 257 (holding that evidence of computer images of child pornography, for which Steele was not charged with possessing, was relevant to show knowledge, intent, and absence of mistake and was thus properly admitted in prosecution for distributing, possessing, or viewing child pornography on his computer). Moreover, the fifteen additional images introduced in this case that contained child-exploitative material were not unfairly prejudicial because they were less inflammatory than the thirty images depicting child-sexual-abuse material that had already been introduced and for which Walker was being charged. For these reasons, we hold that the trial court did not

abuse its discretion in admitting the uncharged images at trial.

E. Admission of Walker's Statement to the Police Pertaining to Sex-Offender Registration

Walker next argues that the trial court erred in allowing the State to play the portion of his custodial statement to the police where the officer incorrectly alleged that Walker was delinquent in his sex-offender registration. Walker again cites Rule 404(b) and argues a violation of that evidentiary rule and further argues that any probative value of this evidence was substantially outweighed by the danger of unfair prejudice.

During the search of Walker's apartment, Walker gave a Mirandized statement to Agent Pinner. Prior to the introduction of the recording of the statement at trial, Walker objected to the portions in which his sex-offender status was discussed, and the trial court overruled the objection. In the custodial interview that was played to the jury, Agent Pinner asked whether Walker had ever been arrested for child pornography, and Walker replied no. Agent Pinner then asked whether Walker was a registered sex offender and whether he had failed to register in Arkansas, and Walker replied no to both questions. Later in the interview, Agent Pinner again questioned whether Walker was a sex offender in Oregon and whether he was delinquent there, and Walker denied that accusation, indicating that he was current on his Oregon sex-offender registration. Agent Pinner then suggested that "your problem right now" is that "you have not registered in the state of Arkansas." Walker replied, "Okay."

We conclude that any error in admitting the discussion pertaining to Walker's sex-offender status was harmless. We may declare an evidentiary error harmless if the evidence of guilt is overwhelming and the error is slight. *Johnston v. State*, 2014 Ark. 110, 431 S.W.3d 895. As we have already explained, the trial court committed no error in admitting Walker's three prior Oregon convictions for encouraging child sexual abuse in the first degree, so the jury knew about Walker's sex-offender status from competent evidence independent of the police interview. Moreover, any possible error with respect to whether Walker had registered as a sex offender in this state was slight when compared to the overwhelming evidence of his guilt for the crimes charged. Therefore, no reversible error occurred under this point.

F. Admission of Walker's Oregon Pen Pack

Walker next argues that the trial court erred in admitting his Oregon "pen pack" during the guilt phase of the trial. Walker argues that any marginal probative value of the contents of the pen pack was grossly outweighed by the danger of unfair prejudice and confusing the issues. In particular, Walker points out that his pen pack contained a reference to a drug-possession case, information that he was indigent, and information about his mandatory mental-health treatment for sexually deviant behavior.

We conclude that this argument is not preserved for review. When the State introduced evidence of Walker's convictions at trial (which had already been ruled admissible prior to trial) it stated, "[I]t is in the form of a pen pack." Walker objected, arguing:

> With regard to this, the court did make a decision that it could be admissible. Our objection would be to the way it's being admitted at this point in time . . . . Whether or not the document could come in is not an issue, but how it comes in . . . . I believe the keeper of the records would have to be here for this to be introduced.

At trial, Walker's only objection to the pen pack was, in effect, for lack of foundation and that it should not be admitted without the record keeper to introduce it. Walker does not make that argument on appeal; rather, his argument on appeal is that the specific information in the pen pack was unduly prejudicial. Our law is well established that in order to preserve a challenge for our review, the movant must apprise the trial court of the specific basis on which the motion is made. *Stewart v. State*, 320 Ark. 75, 894 S.W.2d 930 (1995). Parties may not change their arguments on appeal and are limited to the scope and nature of their arguments made below. *Id.* Because Walker has changed his argument on appeal, we will not address it.

G. Affirmative-Defense Jury Instruction

Walker next argues that the trial court erred in denying his request for an affirmative-defense jury instruction based on Ark. Code Ann. § 5-27-602(c), which provides, "It is an affirmative defense to a prosecution under this section that the defendant in good faith reasonably believed that the person depicted in the matter was seventeen (17) years of age or older." Walker requested this jury instruction with respect to only five of the thirty images for which he was charged. Walker argues that the jury

instruction should have been given with respect to those five charges because, at the very least, those images contained the slightest evidence that they could involve persons seventeen years of age or older.

A party is entitled to a jury instruction when it is a correct statement of the law and when there is some basis in the evidence to support giving the instruction. *Vidos v. State*, 367 Ark. 296, 239 S.W.3d 467 (2006). We will not reverse a trial court's decision to give an instruction unless the court abused its discretion. *Id.*

We hold that the trial court did not abuse its discretion in denying the affirmative-defense jury instruction. Walker's defense at trial was that he did not possess any of the illegal images attributed to him, as he stated in his opening argument and argued in his directed-verdict motion and closing argument. In Walker's custodial interview with the police, Walker denied possessing child pornography on his computer equipment. From the evidence presented, there was no basis in the evidence to conclude that Walker reasonably believed that some of the images found on his computer depicted persons seventeen years of age or older. Therefore, this argument is without merit.

H. Illegal Sentence – Sexually Dangerous Person

Finally, in his reply brief, Walker raises an issue that a portion of his sentence was illegal. Normally, an appellant may not raise an issue for the first time in his reply brief. *See Adams v. State*, 2020 Ark. App. 501, 612 S.W.3d 191. However, we may address an illegal sentence sua sponte, *Muhammad v. State*, 2021 Ark. 129, 624 S.W.3d 300, and when an error has nothing to do with the issue of guilt or innocence

and relates only to punishment, it may be corrected in lieu of reversing and remanding. *Bangs v. State*, 310 Ark. 235, 835 S.W.2d 294 (1992). For the following reasons, we conclude that a portion of Walker's sentence was illegal.

In the sentencing order, the trial court checked the yes box for: "Defendant is alleged to be a sexually dangerous person and is ordered to undergo an evaluation at a facility designated by A.D.C. pursuant to A.C.A. § 12-12-918." However, this designation in the sentencing order was erroneous. Arkansas Code Annotated section 12-12-918 (Supp. 2021 2021) provides, in relevant part:

> (a)(1) In order to classify a person as a sexually dangerous person, a prosecutor may allege *on the face of an information* that the prosecutor is seeking a determination that the defendant is a sexually dangerous person.
>
> (2)(A) If the defendant is adjudicated guilty, the court shall enter an order directing an examiner qualified by the Sex Offender Assessment Committee to issue a report to the sentencing court that recommends whether or not the defendant should be classified as a sexually dangerous person.

(Emphasis added.) Here, the State did not allege on the face of the original information or on the face of the amended information that it was seeking a determination that Walker is a sexually dangerous person. Therefore, we modify and correct the sentencing order to delete this designation.

III. *Conclusion*

In conclusion, we find merit in none of Walker's arguments on appeal, and we affirm his convictions for thirty counts of distributing, possessing, or viewing matter depicting sexually explicit conduct involving a child. However, we modify the sentencing order as explained above.

Affirmed as modified.

MURPHY AND BROWN, JJ., agree.

Lassiter Cassinelli, by: *Michael Kiel Kaiser*, for appellant.

Leslie Rutledge, Att'y Gen., by: *Joseph Karl Luebke*, Ass't Att'y Gen., and *Karen Virginia Wallace*, Ass't Att'y Gen., for appellee.

APPENDIX B

IN THE CIRCUIT COURT OF
CLARK COUNTY, ARKANSAS
CRIMINAL DIVISION

STATE OF ARKANSAS PLAINTIFF

VS. 10CR-20-107

JONATHAN WALKER DEFENDANT

ORDER

COMES NOW, the State, represented by Dan Turner, Prosecuting Attorney, Ninth-East Judicial District, and the Defendant, represented by his attorney, Clint Mathis and the Court having considered the pleadings, arguments of counsel and matters presented hereby finds and orders:

1. The Defendant's Motion to Suppress Evidence Seized Based on Search Warrant is hereby DENIED.

IT IS SO ORDERED.

/s/
Circuit Judge

October 18, 2021
Date

COPIES:
Prosecuting Attorney
Defendant's Attorney

ELECTRONICALLY FILED
Clark County Circuit Court
Brian Daniel, Circuit Clerk
2021-Oct-18 13:13:15
10CR-20-107
C09ED01: 1 Page

APPENDIX C

OFFICE OF THE CLERK
ARKANSAS SUPREME COURT
625 Marshall Street
Little Rock, AR 72201

September 21, 2023

RE: SUPREME COURT CASE NO. CR-22-572
Jonathan Walker v. State of Arkansas

The Arkansas Supreme Court issued the following order today in the above styled case:

"APPELLANT'S PETITION FOR REVIEW IS DENIED."

Sincerely,

/s/ Kyle Burton
KYLE E. BURTON, CLERK

cc: Michael Kiel Kaiser
Joseph Karl Luebke and Karen Virginia Wallace,
Assistant Attorneys General
Clark County Circuit Court
(Case No. 10CR-20-107)

APPENDIX D

[RT-001]
IN THE CIRCUIT COURT OF
CLARK COUNTY, ARKANSAS
CRIMINAL DIVISION

STATE OF ARKANSAS PLAINTIFF

VS. 10CR-20-107

JONATHAN WALKER DEFENDANT

RECORD—TRANSCRIPT (HYBRID)
VOLUME I OF II
PAGES 01-842

* * *

[RT-052]

****

HEARING ON MOTION TO SUPPRESS:
OCTOBER 11, 2021

****

P R O C E E D I N G S

{Whereupon, at 1:39 p.m., the following proceedings were had, to-wit:}

THE COURT: This is 10CR-20-107, *State of Arkansas versus Jonathan Walker*. Mr. Walker is present with his attorney Mr. Mathis. And Mr. Turner is here on behalf of the State.

And we're here on the Defendant's motion to suppress; is that correct?

MR. TURNER: That's correct, Your Honor.

MR. MATHIS: Yes, Your Honor.

MR. TURNER: As a preliminary matter, Your Honor, I believe we are prepared to stipulate to some exhibits.

THE COURT: Okay.

MR. TURNER: If I could identify those for the record: Exhibit A will be the Application and Affidavit for Search and Seizure Warrant. And it is a six-page document.

{The Application and Affidavit for Search and Seizure Warrant was received and marked for [RT-053] identification as Joint Exhibit A and is attached hereto.}

MR. TURNER: Exhibit B will be a Cyber Tipline Report, 71173604, from the National Center for Missing and Exploited Children. That is a ten-page document, Your Honor.

{The NCMEC Cyber Tipline Report was received and marked for identification as Joint Exhibit B and is attached hereto.}

MR. TURNER: And some of these are out of order, but we'll — hopefully, it won't be too confusing.

Exhibit C is the actual Search and Seizure Warrant itself, Your Honor. And it is a five-page document.

{The Search and Seizure Warrant was received and marked for identification as Joint Exhibit C and is attached hereto.}

MR. TURNER: And then Exhibit D is the Search Warrant Return that was executed and filed of record. And it's a single page.

{The Search Warrant Return was received and marked for identification as Joint Exhibit D and is attached hereto.}

MR. TURNER: And, so, I believe the [RT-054] Defense and the State are prepared to move for introduction of a A, B, C and D for purposes of this hearing only by stipulation.

MR. MATHIS: Defense so moves.

THE COURT: Okay. Be admitted without objection.

TESTIMONY AND EVIDENCE
ON BEHALF OF STATE

MR. TURNER: State will call Adam Pinner.

THE COURT: All right. Agent Pinner, can you hear me?

Agent Pinner, can you hear me?

MR. MATHIS: You're muted, Judge.

THE COURT: Agent Pinner, can you hear me?

Can you hear me?

{Reporter's Note: Brief pause for equipment adjustment.}

THE COURT: Can you hear me?

Can you hear me?

THE WITNESS: Hey, Judge, can you hear me? This is Adam.

THE COURT: I can hear you. Can you hear me?

THE WITNESS: Yes, Sir.

THE COURT: Raise your right hand.

[RT-055]

ADAM PINNER,

Having been called by and on behalf of the State, and having been duly sworn, was examined and testified as follows, to-wit:

THE COURT: You may proceed, Mr. Turner.

DIRECT EXAMINATION

BY MR. TURNER:

Q. Special Agent Pinner, Dan Turner. For the record, state your full name and occupation.

A. Special Agent Adam Pinner; Arkansas State Police.

Q. And do you work in any special capacity with the Arkansas State Police?

A. I'm a special agent within the Criminal Investigation Division, also assigned to the Internet Crimes Against Children's task force.

Q. And you receive training in that regard?

A. Yes, Sir.

Q. Were you involved in the application for a search warrant for Jonathan Walker, also known as, I believe, Robert Jennings, back in July of 2020?

A. Yes, sir.

Q. And did you, in fact, cause an application and affidavit for that search warrant to be presented to Judge Randy Hill?

A. Yes, Sir.

[RT-056]

Q. Now, we do have some limitations here, Special Agent Pinner, because we're doing this via Zoom, and, so, I don't know – I don't know how I can show you this exhibit. But you – you would agree with me that there was a – an affidavit that you prepared that would have been dated July the 29th of 2020 that was attested to by Judge Hill?

A. Yes, Sir.

THE WITNESS: And, by the way, did we lose the judge? He's not on my screen anymore – or are we still good?

MR. TURNER: He can hear you.

THE WITNESS: Okay. Good.

BY MR. TURNER:

Q. If you would, Special Agent Pinner, I'd like you to tell the Court how you came to investigate this case. What information came to your attention that led you to seek this search warrant?

A. Yes, Sir. So on July 13, 2020, I was assigned this CyberTip. CyberTip comes from the National Center for Missing and Exploited Children. I get assigned the CyberTip through my lieutenant, Dennis Morris.

And, at the time I was assigned this case, we were also obtaining a subpoena from the prosecutor's office there in Clark County. And when we received that [RT-057] subpoena – the subpoena was in

regards to the IP address – suspect IP address – listed on the CyberTip. Once we got the subpoena production back from, I believe, Suddenlink Communications, that provided us subscriber information in regards to that IP address, which led us to 1820 Mill Creek Drive there in Arkadelphia.

Q. And for – just for the Judge's benefit, Special Agent Pinner, so you commonly work with these CyberTips; is that accurate?

A. Yes, Sir.

Q. So if you'll just explain that process, generally, to the Court. How does that work? How do you get a CyberTip? Where did you get it from? What does it consist of?

A. When I get them, they come from – I get advised by my lieutenant, my supervisor, that I've been assigned a CyberTip. He gets them from our Arkansas Internet Crimes Against Children's task force coordinator, which is in our headquarters in Little Rock. She gets the CyberTips from the National Center for Missing and Exploited Children.

She looks through the CyberTips. And once she has them, she sees what part of the state they're in and sends them out accordingly where they need to go. And [RT-058] then just – and she has received from NCMEC, who NCMEC receives from different electronic service providers.

Q. And, so, it – just for clarity of the record, when we say "NCMEC," we're talking about the National Center for Missing and Exploited Children?

A. Yes, Sir.

Q. So an Internet service provider or Internet provider provides this information to NCMEC, and then it's farmed out to local law enforcement from there; is that accurate?

A. Yes. The IP address is provided by the service provider. And then use Open-source to see where the IP address could be located. And, for instance, this IP address was Arkansas, so it got sent to the Arkansas task force – or the Internet Crimes Against Children's division – I'm sorry – Internet Crimes Against Children's task force, in which our analysts – or, I'm sorry – our coordinator in Little Rock checks the IP address, again, through Open-source and sees it was Suddenlink and gives a GPS location in Arkadelphia.

Q. Backing up just a little bit, we talked about the search warrant application. You were, in fact, granted a search warrant by Judge Hill; is that true?

A. Correct.

Q. And, then, following execution of that search [RT-059] warrant, did you – you or Special Agent Battle cause a Search Warrant Return to be filed, showing what evidence or items, if any, were obtained pursuant to that execution?

A. Correct.

Q. Now, I want to ask you about this Tipline. Do you have documentation that might be contained in your case file related to CyberTips that originate from NCMEC?

A. Yes. It will be the actual CyberTip I received.

Q. All right. Let's talk about this case in particular. So you received – do you have access to that CyberTip documentation?

A. Yes, I do.

Q. Okay. So you received this information. And did you – did you obtain or were you provided any kind of images or anything of that nature related to this?

A. Yes. Excuse me. When we are provided – when we are assigned these CyberTips, a CyberTip is actually uploaded to the computer software, I would say, that the Criminal Investigation Division utilizes for all our reports. The CyberTip itself is uploaded to it and that's where I receive it.

It's also uploaded to another software we utilize that the images – that the child pornography images or actually on that is protected. And I can also obtain [RT-060] the CyberTip from there along with that image.

Q. And in this particular case, did you or Special Agent Battle actually view the image that was the – provided as —

A. I did. I received the image and the CyberTip.

Q. All right. Now, let's talk a little bit about – can you tell the Court what a "hash value" is?

A. A hash value is when a computer software takes that image and hashes it out. And that's where it get it — kind of like a DNA. Just like everybody has a DNA within their person, a photograph does.

When we get these images, the images actually shows the file name – which I don't know if you have the CyberTip – is listed throughout the CyberTip file name. And the actual image, whenever I downloaded

it, has all these letters, numbers, dashes. It's a dot, jpg file. The image I was provided, the file name for the image is what matched the file name on the CyberTip.

MR. TURNER: Your Honor, may I approach? Honor?

THE COURT: Yes.

MR. TURNER: And I apologize to the Court. Here are A, B, C and D. We're going to – I'd like to ask him questions about B in particular and wanted the Court to have that.

[RT-061]

THE COURT: Okay.

MR. TURNER: I think Mr. Mathis has a copy.

MR. MATHIS: I do.

BY MR. TURNER:

Q. Okay. Special Agent Pinner, if you'll look at the Cyber Tipline Report that you just described. And there's a section that references "uploaded file information." Do you find that —

A. Yes, Sir.

MR. TURNER: Your Honor, it should be on Bates stamp 010.

THE COURT: Okay.

BY MR. TURNER:

Q. Underneath "uploaded file information," there is a category that says "original binary hash of file." Is that the hash value?

A. I go by the file name up there. That file name —

Q. I see it.

A. – D02 —

Q. Right.

A. – Denny, dot, jpeg. And then MD5 is the hash value. The original binary hash value photo DNA – yeah, that would be it also. That is something that Special Agent Battle would do, is hashing a photo out. [RT-062] What I do is look at the file – the actual file names.

Q. Understand.

And when you receive a tip, a CyberTip, from the National Center for Missing and Exploited Children, do they have a library or a catalog of images that they have previously determined to be child sexual abuse material?

A. Yes.

Q. And, so, they can tell that my looking at that hash value?

A. Yes, that's what I've been advised.

Q. And, so, based from this tip, you obtained the search warrant that we've already talked about, then you did, in fact, recover evidence from that location that you described previously; is that true?

A. Correct.

Q. And the Search Warrant Return that we've introduced as State's – or as Joint Exhibit D will identify all of the items of property or items of evidence that were recovered; is that true?

A. Yes, Sir.

MR. TURNER: That's all I have for Agent Pinner. I'll have some questions for Special Agent Battle.

THE COURT: Mr. Mathis?

[RT-063]

MR. MATHIS: Yes, Sir.

CROSS-EXAMINATION

BY MR. MATHIS:

Q. Now, this report, as you stated, originated by NCMEC reporting a CyberTip given to it by Microsoft and turning that information over to the Arkansas State Police; is that correct?

A. Correct.

Q. And, in this case, photo DNA was used identify what is known as the hashtag [sic] value of the picture, correct?

A. Say that again, please.

Q. Photo DNA, the program – you're familiar with it?

A. Yes, Sir.

Q. Was used in this matter to automatedly [sic] scan the files and match hashtags, correct?

A. Yeah. I don't know how the electronic service provider come about it, whether it was not [sic] that the hash value or they actual – saw the image and sent it to NCMEC.

Q. Okay. Well, let's talk about that for a moment.

A. Oh, hold on just a minute.

Q. Do you see what's on your page there?

A. Oh, okay. All right. My screen —

Q. You see that?

[RT-064]

A. Yeah, I see it now.

Q. Okay. So I'm going to take you down to the NCMEC report here. Okay. Now, do you see the "incident type" right there under the "executive summary"?

A. Yes, Sir. I'm trying to look at my CyberTip because I got other boxes over here.

Q. Okay. Do you have the executive —

A. Yes, Sir.

Q. You see that, right.

A. Yes. Incident type – yes, Sir, I see.

Q. And you see where it says (as read), "Apparent child pornography, unconfirmed"?

A. Yes, Sir.

Q. And you also see where the files were not reviewed by NCMEC, correct?

A. Correct.

Q. Okay. Now, I'm taking you to the same section that Dan talked to you about – additional information – "uploaded file information." Do you see that?

A. Yes, Sir.

Q. Okay. And do you see on the third line down (as read): "Did reporting ESP view entire contents of uploaded file?" And it says, "No," doesn't it?

A. Yes, Sir.

Q. All right. (As read): "Were entire contents of [RT-065] file – uploaded file publicly available?"

And they didn't even provide that information, did they?

A. Okay. Say that one more time.

Q. You see where it says, (as read), "Were entire contents of uploaded file publicly available?" Do you see that line? It's the fourth one —

A. Yes, Sir.

Q. Okay. At that information wasn't provided at all, was it?

A. (As read): "Information not provided by company."

Q. Right. Okay. And I think we've already established this, but this was an unfounded report, wasn't it?

A. No, Sir.

Q. Oh, okay. All right. Well, then, I would like to take you up to the application for search warrant. And you did that, didn't you?

A. Yes, Sir. As in "unfounded" as in —

Q. Unfounded.

A. – what's unfounded?

Q. Yeah. It's unfounded, isn't it?

A. What is unfounded?

Q. The report —

A. We did locate images —

[RT-066]

Q. – that you received from NCMEC was marked "unfounded," wasn't it?

A. I don't know where it says "unfounded." It said (as read), "Information not provided."

Q. Okay. Well —

A. It says (as read), "NCMEC's incident type is based on NCMEC's review or the report of a hash match."

Q. Right. Not a review of the picture?

MR. MATHIS: I'm sorry about this. This is kind of new to me too.

{Reporter's Note: Brief pause.}

BY MR. MATHIS:

Q. "NCMEC classification," do you see that on that page?

A. Yes, Sir.

Q. And do you see where it says – and I said "unfounded" – I mean, it's "unconfirmed," correct?

A. Correct; that's what it states.

Q. (As read): "Apparent child – child pornography is unconfirmed."

Now, Microsoft is a private company, isn't it?

A. I believe so.

Q. Yeah. Well, NCMEC isn't a government agency, is it? It's a private, non-for-profit [sic] agency, correct?

[RT-067]

A. Yes, Sir.

Q. Okay. You weren't sent a picture with the Tip, were you?

A. I was provided the image through another database.

Q. Oh, okay. All right. So what other database did you use?

A. The – it's the ICAC.

Q. Okay. And, so, you've got this picture that you used to justify this search warrant from – from who, again?

A. NCMEC – from the National Center for Missing and Exploited Children, who was provided of this image by Microsoft.

Q. Okay. So you had to request the image, correct?

A. No. Like I said, our – the ICAC commander is the one who provides it to me. And —

Q. Oh, so you don't know how it was requested, do you?

A. {No response.}

Q. Your commander —

A. No.

Q – just gave it to you, right?

A. Yes. The commander's the – who provides it to us.

Q. Okay. You don't know how he got it?

A. No.

Q. Thank you. Thank you.

[RT-068]

Now, this hashtag was generated based upon a database, I believe you testified earlier; is that correct?

A. Yes. From what I've been advised, these photos go through a software that gives it a hash value.

Q. Okay.

A. And, like I said, I'll look at the file name – the file name. If you scroll back up to "upload file information," there's a file name there.

Q. Well, anybody can change a file name, can't they?

A. I look at the picture that they send me, and that file name is then matched to the file name on the CyberTip.

Q. Well, now that picture wasn't sent to you by anyone, it was given to you by your superior officer, correct?

A. Right —

Q. Okay.

A – who –

Q. Now, the State – we said in, I believe – let's go back up to – let's see here – let's go back up to Exhibit A.

And, in paragraph one, facts constituting reasonable cause – do you see it right there?

A. Yes, Sir. I'm just turning to mine, because of the [RT-069] boxes here, I can't see all of it.

Q. All right.

A. Yes, sir. Yes, sir.

Q. Now, you don't – again, you don't know how this process worked, whether the picture was requested or by whom it was requested, do you?

A. {No response.}

MR. MATHIS: Hello?

THE WITNESS: Hey, Mr. Mathis, can you repeat that one more time? It went digital on me.

BY MR. MATHIS:

Q. You —

THE WITNESS: Yes, sir.

BY MR. MATHIS:

Q. You don't know —

THE WITNESS: Can you repeat that one more time? It went digital.

BY MR. MATHIS:

Q. You don't know who requested the picture or how it got there, do you?

THE WITNESS: It – oh, man – say it – are you asking: Do I know how the picture got here?

MR. MATHIS: No.

[RT-070]

BY MR. MATHIS:

Q. I'm asking you: You don't know how the picture was requested or how it was set up to be delivered to the State Police?

A. {No response.}

Q. You weren't involved in that process, according to your testimony, correct?

A. Yeah. I don't know how my agency – it's going digital – but, no, I do not know how my agency receives the actual image. It's provided from NCMEC to our agency through – how, I don't know – and then I'm provided it through them.

Q. And you see in the Cyber Tipline where neither Microsoft nor NCMEC ever viewed the picture, don't you?

A. Correct.

Q. The State used the picture to get the warrant, didn't they?

A. That and the IP address that was provided that uploaded the – that was advised uploaded images of child pornography.

Q. You're not aware of any warrant or subpoena that obtained the picture in the – never mind. I'll withdraw that question.

The purpose of obtaining the picture was to determine if there was a crime that had been committed; [RT-071] isn't that correct?

A. Yes, Sir. I was provided the Tip – that image.

Q. And it – that was for the purpose of determining if you had a case; isn't that right?

A. Yes, sir.

MR. MATHIS: Thank you. I'll pass the witness.

THE COURT: Mr. Turner?

MR. TURNER: Can I see stipulated Exhibit B, Your Honor?

{Reporter's Note: Brief pause.}

MR. TURNER: Special Agent Pinner, can you hear me fine?

THE WITNESS: Yes, Sir. I still can see the search warrant on the main screen.

MR. MATHIS: Oh, I'm sorry.

MR. TURNER: Mr. Mathis is ahead of me, he has everything digital. But you have access to that —

THE WITNESS: There we go.

MR. TURNER: — you have access to the NCMEC CyberTip Report?

THE WITNESS: {No audible response.}

MR. TURNER: You have that where you can review it?

[RT-072]

MR. MATHIS: I think he's gone digital again. I'm working on mine.

MR. TURNER: What does that mean, "gone

digital"?

MR. MATHIS: He's frozen.

{Reporter's Note: Zoom interruption. Brief pause for equipment adjustment.}

MR. TURNER: We're getting you now. Can you hear me?

THE WITNESS: Yes, Sir, uh-huh.

MR. TURNER: Okay.

REDIRECT EXAMINATION

BY MR. TURNER:

Q. And you have this Cyber Tipline Report that we've been talking about handy that you can review, right?

A. Correct.

Q. Okay. I want to ask you some follow-up questions because I believe that things got confused with Mr. Mathis. The actual image, wasn't that image transmitted from NCMEC to ICAC and then ultimately to you?

A. Correct.

Q. You just don't know how it got there?

A. Yeah, I don't know how it gets from NCMEC to our commander. I don't know how it gets there.

Q. But the Tipline itself references the files being [RT-073] submitted; true?

A. Correct.

Q. You don't understand the mechanics of how that happens?

A. The what?

Q. You don't understand the mechanics?

A. No. The – how it gets from – no. How it gets from NCMEC to – to our ICAC commander, who assigns us the case —

{Reporter's Note: Zoom interruption.}

MR. TURNER: Special Agent Pinner?

THE WITNESS: Froze up.

MR. TURNER: Okay. Can you hear me now?

THE WITNESS: Yes, Sir.

MR. TURNER: Okay. Unfortunately, your entire response was — we couldn't comprehend.

So if you'll restate what you said?

THE WITNESS: Yes.

A. Yes. How the – how the image gets from NCMEC to our agency, to our ICAC commander, I don't know how it gets from there to there.

Q. Okay.

A. I know, eventually, it – I mean, it gets there. Eventually, it gets to me.

Q. All right.

[RT-074]

A. I get provided the image through the ICAC data software. And then the hash value, how the computer software gives it the hash value, the MD5 value, I don't know how that works.

I look at the file name when I'm provided a CyberTip – a file name, uploaded file information that's on the uploaded file information and under —

{Reporter's Note: Zoom interruption.}

BY MR. TURNER:

Q. Okay. I'm – just to try —

A. – that I've been provided.

Q. Just to try to streamline this, Special Agent Pinner, if you'll turn to, I believe it's Page 6 of the

Cyber Tipline Report. And, again, at the bottom of that page you'll see a heading: "Uploaded file information."

A. Yes.

Q. And it says (as read): "Files not viewed by NCMEC," which Mr. Mathis has asked that question. But it also says that (as read), "NCMEC has not viewed the following uploaded files submitted with this report."

So the files were submitted with this report; true?

A. Correct.

MR. TURNER: I have no further questions.

THE COURT: Mr. Mathis?

CROSS-EXAMINATION

[RT-075]

BY MR. MATHIS:

Q. You testified earlier you don't know how the process worked. And indeed you just testified to the Prosecutor that you weren't sure how the pictures got from NCMEC to the – the State Police, correct?

A. Correct. I don't know how they get from – from NCMEC to the – our commander. I get them from – our commander assigns us the case through the ICAC data system.

Q. So – but you're – you – you – you know that neither Microsoft nor NCMEC ever viewed the picture, correct?

A. Yes. I see where it says —

Q. Okay.

A. – there on Page 5 – well, Page 6 – (as read), "Files not viewed by NCMEC." They list the file name, in which I look at, and then the computer does the — software to get the hash value, that MD5.

Q. Okay. Refer me to the entry in this Tip sheet that shows they transferred a file, a picture, of some sort. Take your time, Sir.

A. Where they – where they went from file to files?

Q. Where they submitted a picture. Can you show me? Can you tell me what page it's on where they submitted a picture with this report?

[RT 076]

A. No. Evident – I mean, yeah, I don't see where they said we sent the – the picture. I was ultimately provided that picture, so it went from Microsoft to NCMEC to me – or the file name did, because I ultimately received that picture with that file name.

Q. Right. But, again, you don't know whether it came with the Tip sheet or not. In fact, every indication is that it didn't come with the Tip sheet?

A. Well, it would not come with that Tip sheet —

Q. Thank you.

A – that's associated to the ICAC data system in which I received the CyberTip and the – the image —

MR. MATHIS: Pass the witness.

A. – file name.

THE COURT: Mr. Turner?

MR. TURNER: I have no further questions. I'd ask that he be held —

THE COURT: Okay.

MR. TURNER: – however the Court holds somebody on Zoom.

THE COURT: Agent Pinner, I'm going to place you back in the waiting room until – you may be recalled. Don't discuss your testimony with anyone other than the attorneys in this case. Do you understand?

[RT-077]

THE WITNESS: Yes, Sir.

THE COURT: Okay. All right. Call your next.

MR. TURNER: Call Corwin Battle.

THE COURT: Okay.

CORWIN BATTLE,

Having been called by and on behalf of the State, and having been duly sworn, was examined and testified as follows, to-wit:

{Reporter's Note: Brief pause for equipment adjustment.}

THE COURT: Mr. Turner?

MR. TURNER: Thank you, Agent Battle.

DIRECT EXAMINATION

BY MR. TURNER:

Q. State your full name for the record, please.

A. Yes, my name is Corwin Battle.

Q. And how are you employed?

A. I'm employed with the Arkansas State Police.

Q. And do you also work in conjunction with the Internet Crimes Against Children Unit?

A. Yes, that is correct.

Q. And you're familiar with the Cyber Tipline that's used by National Center for Missing and Exploited Children?

[RT-078]

A. Yes, I am.

Q. Is it customary for you to receive tips from that organization, and, based on those tips, either initiate an investigation and sometimes author an application for a search warrant based on that information?

A. That is correct.

Q. Were you involved or did you assist with an investigation involving Jonathan Walker?

A. Yes, I did, during the search warrant phase.

Q. All right. And so you're familiar with what information was provided – ultimately, Agent Pinner was the affiant; is that true?

A. Yes, that's correct.

Q. But you were familiar with the information that was provided and – and what went into the preparation for that application for search warrant?

A. Yes. He told me whenever we were fixing to execute the search warrant {indiscernible} – I wasn't on the investigative side —

MR. MATHIS: I can't understand him.

THE COURT: Okay. Agent – Agent Battle, your – got a lot of wind noise there. Is there any way that you can shield it from the wind – your microphone from the wind?

THE WITNESS: Yes, I will try to. I was [RT-079] trying to stay outside because it's kind of noisy on the inside. So....

Let me see if I can move locations real quick to see if it'll kind of block some of the wind.

THE COURT: Okay.

{Reporter's Note: Brief pause for equipment adjustment.}

THE WITNESS: Okay. Can you hear any better right here?

THE COURT: Yes.

THE WITNESS: Okay.

THE COURT: Okay.

BY MR. TURNER:

Q. Were you familiar with the Tip that was reported in this case, Agent Battle?

A. I did not – I was not involved on the investigative side of that except for whenever the actual search warrant was out, so I wasn't – I wasn't involved in the investigative phase of this particular investigation.

Q. Okay. But you have received CyberTips from NCMEC before?

A. Yes, that's correct.

Q. How are those tips presented, in what form? I [RT-080] mean, how – how do – what is – what does the Tip contain –

MR. MATHIS: Your Honor, I would just say that the information about how Tips are presented are important, but only in this case.

The Fourth Amendment violation is personal. It doesn't apply to anybody else but the person whose rights were violated.

And this is asking for information that's not even related to this case. If it's about the NCMEC report that we submitted in this matter, I – I have no – I have no objection. But my research shows that they have done differently in different times.

THE COURT: Mr. Turner?

MR. TURNER: I agree with Mr. Mathis that the Court will analysis this case based on the situation here. I believe that – and I hate to start making arguments now, Your Honor, but I believe that the Cyber Tipline Report that's been introduced as Stipulated Exhibit B references files that were submitted. I guess the Court can make that determination.

I think it's relevant if Agent Battle talks about what is custom with his practice [RT-081] because these are the same type of Tips that are going to come from the same organization for the same type of purpose.

THE COURT: I'll allow it.

BY MR. TURNER:

Q. Agent Battle, how do those Tips normally come to you? What – what's the –

A. They –

Q. Go ahead.

A. NCMEC usually sends the reports to the State Police. Which there's an analyst at State Police

headquarters that will receive those, and then they issue them out to the lieutenants or to our affiliate ICAC agencies in the state of Arkansas.

Usually, they provide us with a pdf form from an electronic service provider. And they will also provide whatever data that they have. Sometimes that may be in the form of a chat, or if there was a video or a picture that the electronic service provider provided, they will – they'll provide that also —

Q. So —

A. – with the CyberTip.

Q. So the image or the file is provided with the CyberTip?

A. Yes.

[RT-082]

Q. Now, what – what is a "hash value"?

A. A "hash value" is basically a digital fingerprint of a file. So that digital fingerprint, basically, if something changes with the file, that file signature or file hash will change.

So, for instance, if somebody takes a picture of me right now and sends that out, whenever it – it gets sent to another person, that hash value should be the exact same as whenever it was sent or received.

Q. So if I cropped you or edited you in any way, it would change that hash value?

A. Yes, it would change it completely.

Q. And that's why you refer to it as a digital fingerprint, because it's unique to that image?

A. Yes, to that particular file.

Q. How are hash tags important for the National Center for Missing and Exploited Children?

A. Well, they maintain a database of the – those hash values that they know that make – contain contraband images, so they run those hash values across their database to see if they files have been viewed before. That helps with not having to, you know, keep on getting exposed to child pornography images. So if they have those in the database, they already know that they're there and they can go ahead and send those out.

[RT-083]

Q. So if they can compare a known hashtag value to something that's in their database or library or catalog, they can determine if it contains child sexual abuse material?

A. Yes, that's correct.

Q. Can – can someone not go in and manipulate or change that hash value? Is that like a file name that I can delete and rename?

A. So the file name has nothing to do with the hash value. It's basically the content of the particular file. So if you take that same picture that I was talking about of me and send it and you rename that file and send it back to me, I should be able to hash that file, and it's still going to be the same thing. It's based on the content of the file.

Q. I can't go in to change that hash value?

A. No. No, you can't change it unless you go in and actually manipulate that actual photo, video file, whatever it is.

Q. So if you receive a Tip from NCMEC that says that there's an image of apparent child pornography, what does that tell you?

A. That usually tells me that the electronic service – electronic service provider, in some shape or form, knows that this file has been seen before. And they [RT-084] actually have a template that they – that they make that goes into the CyberTip.

So a lot of times the – especially on the CyberTips, they'll have, like, a little table that has that – it's as apparent child pornography, or whatever categorization it thinks, if it's child exploitative material, they'll have it broke down in that form or factor.

Q. All right. I'm going to put you in a difficult spot, Agent Battle, because you – I don't – I don't suppose you have access to the Cyber Tipline Report in this case, do you?

A. Yes, I – I brought it along with me.

Q. Oh, okay. Great. Great.

A. Yeah. I brought it along with me with what – what was in the file.

Q. Okay. If you would, if you'll turn to page – I believe it's Page 4. And it's a page that the heading at the top says (as read), "Section B: Automated Information Added by NCMEC Systems."

A. Yes.

Q. If you'll look about a third of the way down there's a heading that says (as read), "Further Information on Uploaded Files." Do you see that?

A. And this is on Page 4? Yes, I see that.

[RT-085]

MR. TURNER: I don't guess we can use this for you, can we?

THE COURT: No.

BY MR. TURNER:

Q. Okay. Just below that it says (as read), "Number of uploaded files in each categorization – Category 1," and then there's some boxes that talk about content ranking – rank, term, definition. What are those?

A. Okay. So those are categorizations that was made by the electronic service providers. And for this one it says that there was one – one file that was an A1 category.

So that – if you look at the table on the CyberTip, I know that's a prepubescent minor. And, also, the ranking system is the – No. 1 is going to be a sex act, and it has the definition of that beside it.

Q. So that information came to NCMEC from the ESP?

A. Yes.

Q. And that's an actual description of the image that was ultimately the basis for this Tip; is that true?

A. That's correct.

MR. TURNER: All right. Thank you, Agent Battle. Mr. Mathis will have some questions for you.

THE WITNESS: Okay.

[RT-086]

CROSS-EXAMINATION

BY MR. MATHIS:

Q. Agent Battle, how are you today?

A. I'm doing good, Sir.

Q. Now, I'm talking about that information on Page 4 where it refers to the uploaded files and each directory. Do you see that spot again?

A. Yes.

Q. That's talking about the files that were uploaded onto the OneDrive at Microsoft, isn't it?

A. Yes, I believe so.

Q. Yeah.

A. I believe it's from the OneDrive.

Q. You don't have any idea if the picture was actually transmitted at the time that the Tip was made, do you?

A. You said at the time the Tip was made?

Q. Yeah. You had testified earlier that a picture was usually transferred with a file but it – you don't have a clue whether it was done in this case or not?

A. Well, if you go back and look on Page 2, it has the information directly from the electronic service provider —

Q. Yes, Sir.

A. – that has the original URL, where the file was located.

[RT-087]

Q. Yes, Sir.

A. Also, it has the MD5 hash for that file and the actual file name. And then also on that same page has the upload date and time. So that's the information that we have from Microsoft that says that this is the file that was sent. So that —

Q. But it's not a picture.

A. – MD – that MD5 – that MD5 hash value from Microsoft should match the – the one for the – that was provided with NCMEC along with the report.

Q, And that's – and – but that's not the picture, is it?

A. Excuse me, I don't understand what you're asking. What'd you say?

Q. Did they – did – that's not the actual JPEG, is it?

A. Yes, that should be the JPEG.

Q. Where do they say that?

A. Well, you have right here on the MD5 hash for that actual file, and they also provided the file. So that's what they – that's what they provided, so that's what they're saying that that – that was uploaded.

Q. Are you sure? Look down there at "Additional Information."

(As read): "Images match identically to hash [RT-088] values of images reviewed by Microsoft content moderators."

They're not even talking about this particular picture that was on my client's OneDrive, are they?

A. Okay. So if you go right before that, below the MD5 hash, it says (as read), "Did the reporting ESP view the entire contents of the uploaded file?"

It has "no" down there. The reason they had the additional information, like I said before, is that a lot of times they won't continue to review these files. That's why they provided the MD5 hash and a photo DNA hash set for that.

Q. Right. But you have no idea if the picture came with it, do you?

A. You – that's something that you'd have to ask Microsoft. But I'm – I mean, that MD5 hash —

Q. I got ya.

A. – matched what —

Q. I – I – I thank you. I'll check with Microsoft.

Actually, you know what photo DNA is, don't you?

A, Yes. I'm familiar with it, but it is a proprietary format, so I don't know the Open-source content for that.

Q, It's an —

A. There is no Open-source —

[RT-089]

Q. It's an algorithm that automatically checks Microsoft's OneDrive, isn't it, and matches hash values?

A. Yes. And they provide that information to other forensic tool companies that I've used photo DNA before. So....

Q. And they send that information as required by federal law to NCMEC, correct?

A. Yes. By federal law, they have to scan their system and send that to NCMEC.

MR. MATHIS: Thank you. Pass the witness.

REDIRECT EXAMINATION

BY MR. TURNER:

Q. I just want to make sure that I'm clear because you – you referenced the MD5 on Page 2.

A. Yes.

Q. So that – that is the image?

A. That – that MD5 is going to be the hash value for the – the file name that they provided through the portal through NCMEC.

Q. So —

A. So the JPEG image that's referenced in the file name before, that's the MD5 hash value for – for that file.

Q. So if you were looking at an image that contained [RT-090] this same MD5, it's the same image?

A. Yes, it's going to be the same image no matter where you get it from.

MR. TURNER: I have no further questions.

THE COURT: Mr. Mathis?

MR. MATHIS: Yes, Sir. Corwin, this may take me a moment.

THE WITNESS: Okay.

MR. MATHIS: Apparently, I just got signed out.

{Reporter's Note: Brief pause for equipment adjustment.}

CROSS-EXAMINATION

BY MR. MATHIS:

Q. All right. Do you see "Facts constituting reasonable cause?"

A. Yes.

Q. All right. Do you see the sentence where it begins a parenthetical, about the fifth line up from the bottom, it says "Unconfirmed"?

A. Let's see – yes.

Q. Okay. And when you continue to read that (as read): "The CyberTip reported that one image of apparent child pornography, unconfirmed, was uploaded to Microsoft OneDrive account. Microsoft OneDrive provided [RT-091] the image to NCMEC, and I was eventually provided the image that was uploaded."

Do you see that?

A. Yes, I do see that.

Q. So it's clear that he didn't get the picture at the same time he got the Tip, isn't that correct?

MR. TURNER: Objection. We don't know that that's clear. Something the Court can decide.

MR. MATHIS: I'll withdraw the question.

THE COURT: Okay.

MR. MATHIS: Pass the witness.

THE COURT: Can you take your —

MR. TURNER: I have no other questions.

THE COURT: Can you take your screen-share off, Mr. Mathis?

MR. MATHIS: Oh, sorry, Judge.

THE COURT: Any more questions for this witness?

MR. TURNER: I don't have any more questions for either Agents Battle or Pinner. Unless the Court desires to keep them available or has questions, they can be released, as far as I'm concerned.

THE COURT: May they be released, Mr. [RT-092] Mathis[?]

MR. MATHIS: Yes, Your Honor.

THE COURT: Okay. Thank you, Agent Battle. You're released.

THE WITNESS: All right. Thank you, Sir.

THE COURT: Thank you.

{Reporter's Note: Brief pause.}

THE COURT: Agent Pinner, you're released. Could you hear me? You're released.

Call your —

MR. TURNER: That's all the State's testimony with respect to the suppression issue, Your Honor.

STATE RESTS

THE COURT: Okay. Mr. Mathis?

MR. MATHIS: We have arguments.

DEFENDANT RESTS

THE COURT: Okay.

MR. TURNER: I guess since I carry the burden, I'd ask for a brief rebuttal.

CLOSING STATEMENTS ON BEHALF OF STATE

MR. TURNER: The State believes that the – the proprietary of the search in this case rises or falls on the four corners of the [RT-093] warrant that's been presented to the Court.

Judge Hill found reasonable cause existed to authorize the issuance of a search warrant, and he did in fact issue that warrant.

And, so, based on that, this Court should not put itself in a position to second guess whether or not there was appropriate reasonable cause or probable cause for the warrant.

THE COURT: Mr. Mathis?

MR. MATHIS: Yes, Your Honor.

CLOSING STATEMENTS ON BEHALF OF DEFENDANT

MR. MATHIS: Fourth Amendment rights against unreasonable search and seizure are personal in nature. Here we see the Tip sheet that neither Microsoft or NCMEC viewed the photo. Microsoft clearly states that they reviewed photos in the past but not this particular photo. And that was the testimony that was given by our first witness.

Because the Fourth Amendment is personal, it has to be a picture on his account, though, that is viewed, not a prior viewing as detailed by Microsoft in the Tip sheet. And by "prior viewing," I don't mean prior viewing [RT-094] of this particular picture. I mean prior viewing of a picture in their database, which does not involve his Fourth Amendment rights.

It is undisputed that based on the hashtag information concerning the unfounded photo – or unconfirmed photo, I should say – Officer Corwin obtained this photo without a warrant and without a private entity having viewed it in the initial private search detailed on the Tip sheet. The Tip sheet clearly indicates numerous times that NCMEC never viewed the video.

The hashtags in the information that are present do not indicate a file was ever transferred.

The individuals who testified have no knowledge. And it is the State's burden to show that they have not violated the private search doctrine. And the private search doctrine arrises a Fourth Amendment violation narrowly construed that arrises prior to the issuance of the warrant. The private search doctrine states, simply – quite simply – that the – where a private individual conducts a search and finds contraband, the [RT-095] State or the government may only search within those bounds. Only within those bounds.

If it exceeds the private search, which it did in this case by viewing a picture that they had never seen themselves. When they did that, they exceeded the private search and they violated his Fourth Amendment rights.

Additionally, Arkansas recognizes this concept in *Whisenhunt v State*. In *Whisenhunt v State* – let's see – at 124. Headnote 21 will take you right to it.

The police cannot, without getting a warrant – without a warrant, exceed the scope of the private search.

Now, more on point and right directly down this alley, we have the 2021 case of *U.S. v Wilson*, 2021, U.S. App. LEXIS 28569. And let the record reflect that I've given a copy of each of these cases to the Court and provided one to the Prosecution.

Now, in this case, the ESP did an automated search with its program and submitted the information on the picture to NCMEC. Neither the ESP nor NCMEC had viewed the picture, as is the case in the instant – [RT-096] in this instance. And, as a result, when the police officer viewed the picture without obtaining a warrant, they exceeded the private search doctrine.

Indeed, if you'll look at footnote three, an entire police force's policy was changed to ensure that they got a search warrant prior to – oh, I'm looking at the wrong case. I'm so sorry.

In *Wilson*, footnote three, it indicates Agent Thompson testified that San Diego ICAC, which includes both local, county, regional and federal agency, now obtains a search warrant before opening a CyberTip when the provider has not viewed the images.

And that is right on point with this case. In this – in *Wilson*, they suppressed it because they did exceed the private search when they viewed a picture without a warrant and without another exception, as is pointed out – they could have it – like, exigent circumstances could've existed. But

the State didn't – didn't provide proof of any other exceptions.

Now, exceptions to the Fourth Amendment [RT-097] are narrowly tailored, jealously [sic] and carefully drawn. And, so, it – for instance, they have held that where – in a FedEx case – where the box broke open and they found a powdered substance in it. They found that it was not, in fact, exceeding the private search when they tested the material they could clearly see.

But that is not the case with these pictures. And the *Wilson* case makes that extremely clear, that this is a Fourth Amendment violation taken in conjunction with *Whisenant* – I said Whisenhunt, but it's Whisenant – it applies in the state of Arkansas, as well as at the federal level.

There's no good faith exception here because the Fourth Amendment violation happened prior to the issuance of the warrant. So nobody was relying on a warrant. Indeed, no warrant was issued for getting the picture, which took them over the line in the private search doctrine, which is set forth in *Wilson*.

The fact is that the evidence clearly shows that this doctrine was exceeded. I believe the case law that I presented to the [RT-098] Court supports our position. And the information in this case should be suppressed based upon the Fourth Amendment protections in both the federal and state constitutions and Arkansas Rule of Criminal Procedure 16.2 as it was illegally obtained evidence as defined in 16.2, subsection B.

THE COURT: Mr. Turner?

REBUTTAL CLOSING STATEMENTS
ON BEHALF OF STATE

MR. TURNER: Your Honor, the State agrees that the private search doctrine is recognized in Arkansas. I would argue that that's really the only value of the *Whisenant* case. It's not really applicable otherwise.

The question of – that the Court will have to make the determination of under the private search doctrine is whether or not the State's search exceeded the scope of that when conducted by the private person or entity.

First of all, I would argue that there was no additional search here. Simply opening that document does not constitute a search. And I'll get to *United States/Wilson* in just a minute.

Now, Mr. Mathis and I can disagree; the [RT-099] Court can certainly review it. And I would encourage the Court to – Exhibit B. I think Exhibit B references – I mean, it shows, for example, on Page 2, it says (as read), "Images – images – match identically to hash values of images reviewed by Microsoft content moderators."

We also brought out in testimony through Agent Battle that that information in the Cyber Tipline that referenced the category as A1 – and I apologize to the Court that you didn't have that available during the testimony, but I would ask you to look at it – indicates that not only was the image viewed but that it was described to the National Center for Missing and Exploited

Children and ultimately to law enforcement that used that to obtain a search warrant.

This is not a case – I mean, this is a case that is distinguishable from *Wilson*, but you need not distinguish it because the – an opinion rendered by the Ninth Circuit Court of Appeals two weeks ago in California is not binding on this court. It is only offered as persuasive authority at best.

[RT-100]

I would further argue that I don't think there's any dispute that these hash values are unique to the images.

So the image that is described or defined by a hash value that happens to be a hash value that the National Center for Missing and Exploited Children has previously identified as containing child sexual abuse material and matches up to that hash value is demonstrative that that is illegal contraband, Your Honor. And the State would argue that the mere action of clicking a mouse to open that image does not constitution – constitute an additional search.

Now, we won't refute and we will concede that Agent Pinner did in fact open that image. And he used that information as part of the affidavit for the search warrant. And it was the image that was obtained or that was provided through the Tip. And, so, the question is – I mean, essentially, that's the question, Judge. This – on Page 2, this MD5 that the officers – both officers – have testified is unique – it's a fingerprint – that that is the child sexual abuse material.

[RT-101]

And, so, basically, that's the question, is: Is that not enough? If the service provider, which I dispute, hadn't looked at the image – I believe the Tip shows that they had. But let's assume for the sake of argument that they didn't. If they didn't and NCMEC didn't and it gets to the State police and they open that image, that that somehow magically pulls this out of the private search doctrine and is violative of the Defendant's Fourth Amendment privilege. I mean, that's really the question, Your Honor. And that's just silly.

I mean, it's just silly. That's – it's not any different than if I had an article – a child sexual abuse material photograph in a Manila envelope sitting in my – passenger seat of my car, and on the front it says, "Eight-year-old performing oral sex on adult." But the picture is contained in that envelope.

And a private citizen – well, you're not – Kelli Loy takes it, pulls it out and then gives that to law enforcement. If they open that envelope and pull out and see an eight-year-old performing oral sex on an [RT-102] adult, there's not a court on the – on planet Earth that would say that that violated the private search doctrine. That's the same thing that happened here.

A file that – actually, this is actually more compelling because this is a file that has an identifying feature, the hash value, that can't be manipulated, that's not – that is distinguishable from every other image known to mankind, that

that is the image that NCMEC has previously seen as being child sexual abuse material.

That's the issue. And I appreciate – I mean, Mr. Mathis, I'm – I'm impressed that he has pulled out this Ninth Circuit opinion that happened – I mean, it was literally decided two weeks ago. It's not applicable. And this Court should not follow that precedent that is not binding on it, because these hash values are unique, they are fingerprints, and the State would argue that State – that composite – Stipulated Exhibit B, if the Court will review it, I think you will see that it actually – the image actually had been viewed by ESP, the service provider, [RT-103] beforehand.

THE COURT: All right. I will review the files – or the exhibits and review the cases and issues a ruling.

What else do we need to take up?

MR. TURNER: I – unfortunately, Your Honor, I do need to ask the Court to continue this matter. I don't know that I talked to Mr. Mathis about it, but if the Court could tell, one of our witnesses is actually out of state and will be out of state during the week of the 25th. The State also anticipates that an older case will go to trial this month that would take precedence over this one anyway.

If it pleases the Court, we'd ask for the November setting for this and understand that speedy trial wouldn't be tolled.

THE COURT: Mr. Mathis?

MR. MATHIS: No objection.

THE COURT: I'll continue it on the State's motion. We'll take a – November the 2nd for pretrial, and trial the week of November the 15th, both at 9 a.m.

Anything else we need to take up this afternoon, Mr. Mathis?

[RT-104]

MR. MATHIS: Not today, Your Honor.

THE COURT: Okay.

MR. MATHIS: The only other motion I have pending is dependent upon my expert, and he's so busy working on other cases, I haven't had time to get him in yet.

THE COURT: Okay. All right.

All right. Well, that will conclude this hearing.

{At 2:53 p.m., the proceedings in this matter were concluded and adjourned.}

APPENDIX E

[HEARING ON MOTION TO SUPPRESS: 10/11/2021]
[STATE EXHIBIT A: APPLICATION FOR SEARCH AND SEIZURE WARRANT]

IN THE DISTRICT COURT OF
CLARK COUNTY, ARKANSAS

STATE OF ARKANSAS
COUNTY OF CLARK

APPLICATION AND AFFIDAVIT FOR SEARCH AND SEIZURE WARRANT

COMES NOW before the **Honorable District Judge Randy Hill** is Special Agent Adam Pinner, the undersigned affiant, a duly qualified and acting law enforcement officer of the Arkansas State Police, first being duly sworn upon oath, deposes and says: that he has reason to believe and upon reasonable cause does believe, at the below listed location that the following items may contain certain evidence in support of an ongoing investigation involving the Distributing, possessing, or viewing matter depicting Sexually Explicit Conduct Involving a Child. (5-27-602):

- 1820 Millcreek Drive Building G9, which is an apartment with in an apartment complex. The apartment complex is a two-story building with the lower level as brick and the upper level as a greyish siding. Apartment G9 is located on the second story.

ITEMS TO BE SEIZED

Items to be searched and seized during the execution of the Search and Seizure Warrant will include the following:

- Computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
- Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, Peer to Peer (P2P) software.
- Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography In any format and medium, all originals, computer files, copies, and negatives of child

pornography, visual depictions of minors engaged in sexually explicit conduct.

- Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by operator of the computer or by other means for the purpose of distributing or receiving child pornography or visual depictions of minors engaged in sexually explicit conduct.
- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce
- By any means, including, but not limited to, by the United States Mail or by computer, any child pornography or any visual depictions of minors engaged in sexually explicit conduct.
- Any and all notes, documents, records, or correspondence, in any format or medium {including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache. information) concerning the receipt, transmission, or possession of child pornography or visual depictions of minors engaged in sexually explicit conduct.
- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes,

letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
- Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
- Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage,

and user logins and passwords for such online storage or remote computer storage.

- Any and all cameras, film, videotapes or other photographic equipment.
- Any and all visual depictions of minors.
- Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files}, pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission through interstate or foreign commerce by any means, including by the United States Mail or by computer any child pornography or any visual depiction of minors engaged in sexually explicit conduct.
- Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
- Any and all diaries, notebooks, notes, and any other records reflecting personal contact and

any other activities with minors visually depicted while engaged in sexually explicit conduct.

FACTS CONSTITUTING REASONABLE CAUSE

WHEREAS, appearing before the court, affiant sets forth the following facts:

1. On July 13, 2020, I initiated an investigation due to receiving Cyber Tip 71173604 from the National Center for Missing and Exploited Children (NCMEC). Microsoft – Online Operations Microsoft OneDrive made the report to NCMEC on April 28, 2020. The cyber tip reported that one (1) image of apparent child pornography (unconfirmed) was uploaded to a Microsoft OneDrive Account. Microsoft OneDrive provided the image to NCMEC and I was eventually provided the image that was uploaded. The image is of a prepubescent minor male depicting nudity in a sexually suggestive pose.
2. After reviewing the CyberTip and the accompanying photograph that was upload to the Microsoft OneDrive Account, it was determined, the uploading occurred on April 28, 2020 at 02:03:37 UTC, and was associated with Internet Protocol (IP) Address: 173.216.82.149. The IP Address was associated with Suddenlink Communications.
3. On June 17, 2020, prior to me being assigned this case by Lieutenant Dennis Morris, Lt. Morris requested a prosecutor's subpoena to be served to Suddenlink to obtain the subscriber information for IP address 173.216.82.149.

4. On July 21, 2020, Becky Ursery, Ninth East Prosecutors Office, provided me with a response from the Subpoena to Suddenlink Communications. Suddenlink Communications provided the account name associated with IP address 173.216.82.149 on April 28, 2020 at 02:03:37 UTC as belonging to Jonathan Walker with a service and billing address of 1820 Millcreek Dr. Bld G9 in Arkadelphia, Arkansas.

5. As of July 29, 2020, I completed a check of investigative Internet Crimes against Children databases to deconflict any other ongoing investigations involving this user account or IP address with other law enforcement agencies. No activity for the IP or username were located during this process.

6. Based upon my knowledge, training and experience, I know that searching for information stored in computers often requires law enforcement officers to seize most or all electronic storage devices to be searched later by a qualified analyst in a laboratory or controlled office environment. This is often necessary to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine those storage devices in a controlled setting, it is often necessary that some computer equipment, peripherals, instructions, and software be seized and examined in the controlled setting.

7. Computers can store the equivalent of millions of pages of information and are sometimes concealed or deleted. The parsing process can take weeks or months and it would be impractical and invasive to attempt an on-site search of data.

8. **In light of these concerns,** I **hereby request the Court's permission to seize the above requested devices and peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, law enforcement officers executing the search conclude that it would be impractical to search the computer hardware on-site for this evidence.**

WHEREFORE, affiant[ ] prays that a warrant to search such within described person(s), place(s) or thing(s), be issued, and if such evidence be found and/or concealed therein, to seize it, and/or any individual(s) possessing any items described herein.

OATH

I hereby swear and affirm that the allegations contained in the foregoing Affidavit are the truth, the whole truth and nothing but the truth, so help me God.

*/s/*_____

AFFIANT
Special Agent Adam Pinner
2501 N. Hazel Street
Hope, AR 71801
(870) 777-8944

Subscribed and sworn to before this 29th day of July 2020 at [ ] 12:22 p.m. at the location of Court House.

/s/
DISTRICT JUDGE

APPENDIX F

[RT-454] HEARING ON MOTION TO SUPPRESS: 10/11/2021

STATE EXHIBIT B

CYBER TIPLINE REPORT 71173604

(10 PAGES)

[RT-455]
[LOGO] National Center for
Missing & Exploited Children[10]

CyberTipline Report 71173604

Priority Level: E

---

[10] The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501 (c)(3) organization to serve as a national clearinghouse and resource center for families, victims , private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevent ion messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce on line child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 04-28-2020 14:01 :20 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief overview of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography (Unconfirmed)
Files Not Reviewed by NCMEC

NCMEC Incident Type is based on NCMEC's review of the report **OR** a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

Total Uploaded Files: 1

[RT-456]

Contents

[RT-457]

Section A: Reported Information

The following information was submitted to the CyberTipline by the Reporting Person or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft – Online Operations
Microsoft Microsoft OneDrive

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Company Information

U.S. Law Enforcement - Where to serve Legal Process in Criminal Matters

OneDrive, Skype, Xbox, Binglmage and other Microsoft Online Services:

Microsoft Corporation
Attn: Custodian of Records
One Microsoft Way
Redmond, WA 98052
Service of Process Only: uslereq@microsoft.com
Inquiries Only: msndcc@microsoft.com

Emergency Requests

Microsoft responds to emergency requests, 24 hours a day, if it relates to the imminent threat of death or serious

physical injury as permitted in 18 U.S.C. section 2702(b)(8) and (c)(4). If you have an emergency request, please call the Law Enforcement National Security (LENS) hotline at (425) 722-1299. You may also submit an emergency request via e-mail to lealert@microsoft.com.

Non-U.S. Law Enforcement

Microsoft has established local contacts within your country/region to handle your legal process. If you are not already familiar with your local contact, send an email to globalcc@microsoft.com and you will be directed to the contact handling requests from your country/region. Your local contact will educate you as to what local process must be followed to obtain customer account records. All legal process from non-U.S. law enforcement /prosecutors /courts must be directed to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 U.S.A. Do not direct your legal process to a local subsidiary of Microsoft.

Incident Information

Incident Type:	Child Pornography (possession, manufacture, and distribution)
Incident Time:	04-28-2020 02:03:37 UTC
Description of Incident Time:	Incident Time reflects when first image/video in the series was scanned

Peer to Peer

[RT-458]

Peer-to-Peer Client:	OneDrive
IP Address:	173.216.82.149 at 04-28-2020 02:03:37 UTC
Peer to Peer Filenames:	d02c8b8d-6clb-4f2e-a8al-027fd57efcdb.jpg

Suspect

ESP User ID: 64000f49fbd16

IP Address: 173.216.82.149 04-28-2020 02:03:37 UTC

Additional Information Submitted by the Reporting ESP

No reportee name is available

Uploaded File Information

Number of uploaded files: 1

Uploaded File Information

Filename:	d02c8b8d-6c1 b-4f2e-a8a 1-027fd57efcdb.jpg
MD5:	b3d65caab88df72992167b4f386334e6
Did Reporting ESP view entire contents of uploaded file?	No
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorizatio n by ESP: (See Section B for further explanation)	A1
Original Binary Hash	0,40,0,40, 10, 10,0,51, 149,2,65,39, 127,91,216,82,40, 135,91,32,34,0,28,0,

of File (PhotoDNA):	1,97,50, 15,55,5,81, 10,178, 10, 109,31,80, 119,68, 126,155,100, 135,65,62,2,2 08,2,5, 120,255,4,75, 116,220,83,70,39,53,53,80,62,46, 114,208,21, 150,55, 44,0,40, 14,0,53,26, 10,32,255, 134,43, 111,60,53,57, 115,93, 113,53,202,2,7 5,30, 12,0,0, 14,0, 10,2,7,3, 111,90,6,38, 182, 115,62,210,23,78,61,74, 1,26, 1 6, 11,0,0,8,0,9,5,2,0,56, 12, 13,52, 149, 130,33, 130,28, 156, 19,50,0, 16, 10, 13, 0,3,2
Original URL Where File was Located:	https://public.ch.files.1 drv.com/y4aA0b39bRp52FPSvS4h4Dwwj 1 nocqpkE 3pQulLGnVkevHGvOChHORsM 1 NzVTSGD8ao1 upUG0SR65DaFWQXpL uVq3uDjU- 0U h UAoxVjxB h mfRks9Vnzu9cl v9rN IZ6B F C715sth0jxE MSG hZXV qJ 2oKU 6HAP8zblVMty7 AUi_FDirlHs YE Cs You5KFGCye56_DD
Additional Information:	Image[s] match identically to hash values of images reviewed by Microsoft content moderators.

Source Information:

Type	Value	Event	Date/Time
IP Address	173.216.82.149		04-28-2020 02:03:37 UTC

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The [RT-459] reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and

undertaken at the initiative of the Reporting Person or Reporting ESP.

[RT-460]

Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "Suspect," NCMEC Systems will geographically resolve the IP address via a publicly-available online query. The results of this lookup are displayed.

Geolocation data is approximate and may not display a user's exact location. Please be aware that the geolocation information provided is not exact but is providing a reliable estimate of location based on IP address(es) voluntarily provided by the reporting ESP.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:
A1: 1
The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Suspect)

IP Address	Country	Region	City	Metro Area	Postal Code
173.216.82.149	US	AR	Arkadelphia	Little Rock-Pine Bluff	71923
Area Code	**Lat/Long**		**ISP/Org**		
	34. 1123/ 93. 0713		SuddenLink Communications/ SuddenLink Communications		

Geo-Lookup (Uploaded Files)

[RT-461]

IP Address	Country	Region	City	Metro Area	Postal Code
173.216.82.149	US	AR	Arkadelphia	Little Rock-Pine Bluff	71923
Area Code	**Lat/Long**		**ISP/Org**		
	34. 1123/ 93. 0713		SuddenLink Communications/ SuddenLink Communications		

This concludes Section B

[RT-462]

Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from queries on publicly-available, open-source websites. Any queries conducted by NCMEC staff will be documented and any query results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level:	E (Report submitted by a registered Electronic Service Provider)
NCMEC Classification*:	Apparent Child Pornography (Unconfirmed) Files Not Reviewed by NCMEC
International Country:	United States
NCMEC Date Processed:	05-11-2020 20:05:53 UTC
Made Available to Law Enforcement by NCMEC:	Yes

NCMEC Classification is based on NCMEC's review of the report **OR** a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

NCMEC Note # 1

ECO-ARP 05-11-2020 20:05:53 UTC

***Please be advised that NCMEC staff have not opened or viewed any uploaded files submitted with this report at this time and have no information concerning the content of the uploaded files other than information provided in the report by the ESP.

===

CT/TA for the reported identifier(s) yielded negative or irrelevant results.

===

VPN: AR ICAC based on the reported IP address that returns to Suddenlink Communications in Arkadelphia, AR.

Uploaded File Information

Files Not Viewed by NCMEC:

NCMEC staff have not viewed the following uploaded files submitted with this report and have no information concerning the content of the uploaded files other than information voluntarily provided in the report by the reporting ESP.

Files Not Viewed by NCMEC

Filename	MD5
d02c8b8d-6c1b-4f2e-a8a1-027fd57efcdb.jpg	b3d65caab88df72992167b4f386334e6

This concludes Section C

* * *

[RT-464]

The report was made available to the Law Enforcement Agency listed below.

Arkansas State Police

Investigator:

Assigned Officer:	Access VPN
Title:	Analyst Lenore Paladino
City/State:	Little Rock, AR
Country:	United States
Phone Number:	501-297-8607
Email Address:	lenore.paladino@asp.arkansas.gov, kevin.richmond@asp.arkansas.gov

Time/Date was made available: 05-11-2020 20:05:53 UTC

This concludes Section D

This concludes CyberTipline Report 71173604

APPENDIX G

[HEARING ON MOTION TO SUPPRESS: 10/11/2021]
[STATE EXHIBIT C: SEARCH AND SEIZURE WARRANT]

IN THE DISTRICT COURT OF
CLARK COUNTY, ARKANSAS

STATE OF ARKANSAS
COUNTY OF CLARK

SEARCH AND SEIZURE WARRANT

TO: Any Sheriff, Constable, or Policeman in the State of Arkansas:

Upon application supported by a sworn affidavit having been filed before the court, it is hereby found that the located at the described premises as follows, to wit;

- 1820 Millcreek Drive Building G9, which is an apartment with in an apartment complex. The apartment complex is a two-story building with the lower level as brick and the upper level as a greyish siding. Apartment G9 is located on the second story.

ITEMS TO BE SEIZED

Items to be searched and seized during the execution of the Search and Seizure Warrant will include the following items:

- Computer{s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display

monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

- Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, Peer to Peer (P2P) software.
- Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography In any format and medium, all originals, computer files, copies, and negatives of child pornography, visual depictions of minors engaged in sexually explicit conduct.
- Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by operator of the computer or by other means for the purpose of distributing or receiving child pornography or visual depictions of minors engaged in sexually explicit conduct.

- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography or any visual depictions of minors engaged in sexually explicit conduct.
- Any and all notes, documents, records., or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography or visual depictions of minors engaged in sexually explicit conduct.
- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.
- Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages., chat logs

and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

- Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
- Any and all records, documents, invoices and materials, in any format or medium {including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
- Any and all cameras, film, videotapes or other photographic equipment.
- Any and all visual depictions of minors.
- Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages,

chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depiction of minors engaged in sexually explicit conduct.

- Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, email messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
- Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

It is hereby found that probable cause exist[s] to believe that such property conceals and/or contains such property and/or contraband.

THEREFORE, YOU ARE HEREBY COMMANDED TO:

- Search the above described premises within a reasonable time not to exceed (60) days;

- Search during the day time hours;
- The person(s), place(s), or thing(s) as herein, described
- An[d] if any such items of property and/or contraband as herein, described, be found, contained and/ or concealed therein, seize any such property and/ or contraband and maintain it according to law;
- Leave a true and correct copy of this warrant with the occupant or a person who is apparent responsible control of such premises;
- Conduct an off-site search of the hardware described in the warrant and image or copy if impractical to copy on-site and review the images and/ or copies off-site.
- If the occupant(s) or no one else in apparent and responsible control is not present therein, leave a copy of this warrant suitable affixed thereto;
- Upon completion of the search, make and deliver a receipt, fairly describing the things seized with the occupant or person in apparent responsible control of such premises;
- Also a copy of such things and property seized will be made and returned to the issuing Judicial Officer;
- Within a reasonable time not to exceed five (5) days, return this warrant to the issuing Judicial Officer along with a verified report of the execution thereof;

- In the course of execution of this search and seizure warrant upon discovery of the persons or things so specified, affiant shall take possession or custody of them under authority of this warrant.

IT IS SO ORDERED.

Dated this 29th day of July 2020, at 12:23 o'clock PM at the location of Courthouse.

/s/
DISTRICT JUDGE

APPENDIX H

[HEARING ON MOTION TO SUPPRESS: 10/11/2021]
[STATE EXHIBIT D: SEARCH WARRANT RETURN]

CLARK COUNTY
DISTRICT COURT
FILED THE 10 DAY
OF AUG 2020

SEARCH WARRANT RETURN

I received the attached search warrant on the 29th day of July 2020, and executed it as follows:

On **the 6th day of August 2020 at 7:10 O'clock A.M.,** the search of the property described in this warrant begin and a copy of this warrant and inventory of the items seized was left attached to the device.

THE FOLLOWING IS AN INVENTORY OF ITEMS TAKEN PURSUANT TO THIS SEARCH WARRANT:

- Dell Laptop computer SN# 32G7LJ2
- Samsung Cellphone SN# R28K63H0QDE
- Black Lenovo Laptop Computer SN# PF-0O571 K I 6/01
- HP Pavilion Laptop Computer SN# CND9440RBR
- PNY solid State Hard Drive SN# PNY33I92273350108274
- Seagate Hard Drive SN# 3HS0G3QF
- Black Container with five (5) USB flash drives

- Western Digital Hard Drive SN#WD-WCASYA639140
- Flash drive
- Samsung Cellphone SM-J260A SN# RF8MA36VWXJ
- One photo of young white male in speedo
- Two Oregon Driver's License (appear to be fictitious)
- Black circle case containing two flash drives

Due to the protracted nature of processing digital evidence, the laboratory and/ or controlled office offsite copying and examination is ongoing. Any additional evidence discovered in that process will be made a permanent part of the original agency case record.

This inventory was made in the presence of *SIA* Corwin Battle and S/A David Forthman.

I swear that this inventory is a true and detailed account of all items taken pursuant to the execution of this search warrant.

*/s/*_____
EXECUTING OFFICER

Sworn before me and subscribed in my presence this 10th day of August [2020].

*/s/*_____
JUDGE