IN THE COURT OF APPEALS OF THE STATE OF NEW MEXICO

STATE OF NEW MEXICO,

Plaintiff-Appellee,

v. **No. A-1-CA-36490**

JEFFREY MORRILL,

Defendant-Appellant.

APPEAL FROM THE DISTRICT COURT OF BERNALILLO COUNTY
Briana H. Zamora, District Judge

Hector H. Balderas, Attorney General
Santa Fe, NM
Lauren J. Wolongevicz, Assistant Attorney General
Albuquerque, NM

for Appellee

Bennett J. Baur, Chief Public Defender
Kimberly Chavez Cook, Assistant Appellate Defender
Santa Fe, NM

for Appellant

MEMORANDUM OPINION

BOGARDUS, Judge.

{1} Defendant appeals his conviction, following a bench trial, of two counts of sexual exploitation of children (distribution), contrary to NMSA 1978, Section 30-6A-3(B) (2007, amended 2016).[1] This crime is commonly referred to as distribution of child pornography. Defendant advances four arguments: (1) there was insufficient evidence to support his convictions for distribution; (2) his convictions of multiple counts of

1Defendant was also convicted of one count of sexual exploitation of children (possession), contrary to Section 30-6A-3(A). Defendant does not challenge this conviction in this appeal.

distribution violate double jeopardy; (3) the district court abused its discretion in finding the Roundup Torrential Downpour (Roundup) software to be reliable; and (4) the district court erred in admitting the evidence produced by Roundup and Forensic Toolkit. Persuaded only by Defendant's double jeopardy argument, we remand to the district court to vacate one of the two counts of distribution and otherwise affirm.

BACKGROUND

{2} Defendant's charges stem from his use of BitTorrent, a peer-to-peer, file-sharing network, to access child pornography. The evidence at trial established the following. While there is nothing inherently illegal about peer-to-peer, file-sharing networks, they are the most common way to download or distribute child pornography. BitTorrent is one of the most popular peer-to-peer, file-sharing networks. People can connect to the BitTorrent network through a number of different software programs, including µTorrent, which is what Defendant used.

{3} Unlike users of other peer-to-peer, file-sharing networks, BitTorrent users do not search for files within µTorrent. Rather, BitTorrent users must search websites that act as a directory in order to obtain torrent files, which can contain a single file or a number of files. Once a BitTorrent user locates a torrent file they would like to download, the user downloads an info hash file. The info hash file tells µTorrent what the user is looking for and where it can be found. Once the info hash is downloaded, µTorrent connects to Internet Protocol (IP) addresses that have been identified as having the requested torrent file until it is able to download all or part of the file. The more people on the peer-to-peer, file-sharing network who have a torrent file, the faster that file can be downloaded.

{4} One of the State's witnesses testified that peer-to-peer, file-sharing networks, including BitTorrent, operate on the same protocol—"to download, you have to share." In furtherance of that protocol, µTorrent is configured to automatically share anything that a user downloads as long as it remains in the shared folder or in any other folder the user designates to be shared. There is no way to turn off the sharing feature in µTorrent. If a µTorrent user is not sharing, the network notices and can put the user's software in a temporary state that does not allow the user to download from others.

{5} Special Agent Owen Peña with the New Mexico Internet Crimes Against Children Task Force was qualified as an expert in peer-to-peer and peer-to-peer investigations and testified to the following. Agent Peña conducts investigations on the BitTorrent network using Roundup. Agent Peña's computer runs Roundup twenty-four hours a day, seven days a week. Roundup looks for particular torrent files that are identified based on their unique info hash.

{6} If an IP address believed to be in New Mexico is sharing one of those particular torrent files, the Roundup software used by Agent Peña attempts to make a connection to that IP address. In order to make a connection, three things must be true: (1) the sharing computer is on; (2) the file-sharing software is running on the sharing computer;

and (3) the user has to be sharing at least a part of the identified torrent file. If Roundup is able to make a connection to the identified IP address, it attempts to download the identified torrent file. Unlike µTorrent and other peer-to-peer, file-sharing software, Roundup only downloads from a single source—the specific IP address it has identified. Roundup logs every action it takes.

{7} On September 11-12 and October 2, 2015, the Roundup software used by Agent Peña connected to an IP address and downloaded a total of eight distinct torrent files, which contained a total of 10,867 individual files. Once the torrent files were finished downloading, Agent Peña reviewed them and went through all of their file structures. Upon finding child pornography, Agent Peña initiated further investigation.

{8} Qualified as an expert in peer-to-peer investigations and peer-to-peer systems, Detective Kyle Hartsock with the Bernalillo County Sheriff's Department testified to the following. Detective Hartsock received a case packet from Agent Peña that included a paper report and a CD/DVD that contained the actual files downloaded and the log reports that showed the dates, times, and how the software was operating. Based on the information contained in the case packet, Detective Hartsock obtained and executed a search warrant for an apartment located in Albuquerque, New Mexico. Following the search of the apartment, a number of electronic items, including Defendant's computer and external hard drives, were seized. Detective Hartsock took the seized items to the Regional Computer Forensics Laboratory where they underwent forensic examination using Forensic Toolkit.

{9} Defendant was present when the search warrant was executed on the apartment.[2] Several minutes after the search began, Detective Hartsock interviewed Defendant. The interview lasted approximately fifty minutes and was recorded on camera. The video of the interview was played at trial.

{10} During the interview, Defendant made a number of admissions and denials. When Detective Hartsock told him why they were conducting the search, Defendant admitted to having the images they were looking for on one or more of his external hard drives. Defendant followed this statement by saying that it was his understanding that the images were not child pornography.

{11} Defendant reported that the text associated with the images indicated that they were of an artistic nature and were not meant for pornographic purposes. Defendant also stated that he looked up the relevant laws and the images did not seem to meet the statutes. Defendant admitted to downloading µTorrent to his computer, using µTorrent to download the files, and setting up µTorrent to save the downloaded files directly to his external hard drives. However, Defendant denied being aware that the images were available to upload.

2Defendant's roommate was also present during the search. When he was interviewed, Defendant reported that, to his knowledge, his roommate was not involved, which was corroborated by the investigation.

{12} Defendant admitted to searching for "LS," but reported that it was his understanding that the LS series[3] was not child pornography. Defendant admitted to viewing pictures from the LS series for over twenty years. On his external hard drive in a "/Torrents folder," Defendant created a folder titled "L" where he put the images. Defendant stated child pornography charges were brought in different countries against those involved with the LS series, but stated that all charges were dropped and did not result in trials or convictions. Based on this information and the text associated with the images, Defendant reported that he did not believe that the images were illegal.

{13} At Defendant's bench trial, Detective Hartsock demonstrated how to install the same version of µTorrent that Defendant used onto a computer. The demonstration showed that an end user license agreement (EULA) must be agreed to in order to install µTorrent. While a user does not have to scroll through the EULA before agreeing, the agreement did contain a section titled "automatic uploading" that explained that using µTorrent to download files would allow other users to access those downloaded files. When the installation was complete, µTorrent opened and then the window closed; however, the program remained running in the task bar. Detective Hartsock explained that µTorrent was designed to be running all the time.

{14} Detective Hartsock then demonstrated how to obtain a torrent file by going to one of the online directories and finding an e-book. When he clicked on the download link for the e-book, µTorrent opened to confirm what was to be done with the file, including where to download the file. As the e-book downloaded, it was shown in a downloading folder in µTorrent that indicated information like the file name, file size, download speed, upload speed, and estimated time the download would finish. Once the e-book was completely downloaded, the file was no longer shown in the downloading folder and instead showed in µTorrent's seeding file, indicating it was available to be shared.

{15} Defendant moved for a directed verdict at the close of the State's evidence. The district court granted the motion in part, but allowed two counts of distribution of child pornography and one count of possession of child pornography to go forward. Defendant did not put on any evidence, but renewed his directed verdict motion after the defense rested. The district court denied the motion and ultimately convicted Defendant of all remaining counts.

{16} Because this is a memorandum opinion and the parties are familiar with the facts and procedural history of this case, we reserve discussion of additional pertinent facts for our analysis.

DISCUSSION

I. Sufficiency of the Evidence

3Both Agent Peña and Detective Hartsock were familiar with the LS series through their experience in child pornography investigations. Detective Hartsock stated that a series can be dozens or hundreds of depictions with either the same victim or the same location.

{17} Relying on the analysis found in *State v. Granillo*, 2016-NMCA-094, 384 P.3d 1121, Defendant asks that we determine that general criminal intent is insufficient to convict for distribution of child pornography under Section 30-6A-3(B). Defendant argues, in the alternative, that the intent evidence was insufficient even if we conclude that the mens rea is general intent.

{18} We recently rejected a nearly identical argument for a heightened mens rea under Section 30-6A-3(B) in *State v. Franco*, 2019-NMCA-____, ¶ 13, ____ P.3d ____ (No. A-1-CA-35470, June 13, 2019). Like Defendant, the *Franco* defendant also relied on *Granillo* in urging this Court to determine that general criminal intent was insufficient under Section 30-6A-3(B). *Franco*, 2019-NMCA-____, ¶ 13. We reasoned that Section 30-6A-3(B) could not be said to "lean[] away from the common law approach" like the statute involved in *Granillo*, NMSA 1978, § 30-6-1(D)(1) (2009) (criminalizing intentional child abuse by endangerment), because they did not have the same tiered structure. *Franco*, 2019-NMCA-____, ¶ 16. Therefore, under the common law, we concluded Section 30-6A-3(B) only requires general criminal intent because it "only describes a particular act and does not include an intent to do a further act or achieve a further consequence." *Franco*, 2019-NMCA-____, ¶ 16.

{19} For that reason, we analyze whether there was sufficient evidence presented at trial that Defendant acted with general criminal intent. "The test for sufficiency of the evidence is whether substantial evidence of either a direct or circumstantial nature exists to support a verdict of guilty beyond a reasonable doubt with respect to every element essential to a conviction." *State v. Montoya*, 2015-NMSC-010, ¶ 52, 345 P.3d 1056 (internal quotation marks and citation omitted). "[S]ubstantial evidence means such relevant evidence as a reasonable mind might accept as adequate to support a conclusion[.]" *State v. Salgado*, 1999-NMSC-008, ¶ 25, 126 N.M. 691, 974 P.2d 661 (internal quotation marks and citation omitted). "In reviewing the sufficiency of the evidence, we must view the evidence in the light most favorable to the guilty verdict, indulging all reasonable inferences and resolving all conflicts in the evidence in favor of the verdict." *State v. Cunningham*, 2000-NMSC-009, ¶ 26, 128 N.M. 711, 998 P.2d 176.

{20} "The element of general criminal intent is satisfied if the [s]tate can demonstrate beyond a reasonable doubt that the accused purposely performed the act in question." *State v. Gonzalez*, 2005-NMCA-031, ¶ 23, 137 N.M. 107, 107 P.3d 547 (alterations, internal quotation marks, and citation omitted); *see* UJI 14-141 NMRA. Here, the evidence established the following. Defendant admitted to downloading µTorrent, which he used to access BitTorrent, a peer-to-peer, file-sharing network. The BitTorrent network and µTorrent required Defendant to share to be able to continue to download files from others. Defendant chose to use µTorrent, which does not allow users to turn off the sharing feature. Defendant used µTorrent to download images from the LS series, a known child pornography series. Defendant kept the child pornography he downloaded in a shared folder that allowed others on the BitTorrent network to access it. The µTorrent software moved files that were fully downloaded into a folder titled "seeding," which indicated that the files were being shared. Based on this evidence, we conclude there was substantial evidence that Defendant acted with the requisite intent.

II. Defendant's Multiple Convictions for Distribution Violate Double Jeopardy

{21} The district court convicted Defendant of two counts of distribution of child pornography contrary to Section 30-6A-3(B). Defendant argues, and the State concedes, that *State v. Sena*, 2016-NMCA-062, 376 P.3d 887, requires us to vacate all but one count. While we are not bound by the State's concession, *State v. Tapia*, 2015-NMCA-048, ¶ 31, 347 P.3d 738, we accept that concession because it is based on binding precedent. *See Sena*, 2016-NMCA-062, ¶¶ 13-19 (concluding a defendant who was convicted under similar circumstances could only be convicted of one count of distribution of child pornography under Section 30-6A-3(B)). Accordingly, under the facts and circumstances of this case, we hold that Defendant's two convictions for distribution of child pornography violate double jeopardy and must be reduced to a single conviction. *See Sena*, 2016-NMCA-062, ¶ 19.

III. The District Court Did Not Abuse Its Discretion in Finding Roundup Reliable

{22} Defendant argues that the district court abused its discretion in finding the technical conclusions reached by Roundup to be reliable. Defendant makes four contentions: (1) the development and testing process of Roundup did not meet industry standards; (2) any peer review Roundup was subject to was inadequate; (3) Roundup's error rate is unknown; and (4) Roundup does not incorporate any accuracy-ensuring measures.

{23} "We review evidentiary decisions by the district court for an abuse of discretion." *State v. Nichols*, 2006-NMCA-017, ¶ 20, 139 N.M. 72, 128 P.3d 500. "An abuse of discretion occurs when the ruling is clearly against the logic and effect of the facts and circumstances of the case." *State v. Flores*, 2010-NMSC-002, ¶ 25, 147 N.M. 542, 226 P.3d 641 (internal quotation marks and citation omitted). "We cannot say the [district] court abused its discretion by its ruling unless we can characterize it as clearly untenable or not justified by reason." *Id.* (internal quotation marks and citation omitted).

{24} Three requirements must be met before evidence is admissible under Rule 11-702 NMRA, which governs the admissibility of expert testimony: "(1) [the] experts must be qualified; (2) their testimony must assist the trier of fact; and (3) their testimony must be limited to the area of scientific, technical, or other specialized knowledge in which they are qualified." *State v. Torres*, 1999-NMSC-010, ¶ 23, 127 N.M. 20, 976 P.2d 20. Here, Defendant's challenge is to the third requirement, which involves a determination of the reliability of scientific evidence. *See State v. Alberico*, 1993-NMSC-047, ¶ 47, 116 N.M. 156, 861 P.2d 192 ("When scientific evidence is employed as a means of obtaining or analyzing data, the [district] court must determine whether the scientific technique is based upon well-recognized scientific principle and whether it is capable of supporting opinions based upon reasonable probability rather than conjecture.").

{25} Because "evidentiary reliability is the hallmark for the admissibility of scientific knowledge[,]" *Torres*, 1999-NMSC-010, ¶ 26, "the party offering expert testimony based

on scientific knowledge must establish that such knowledge is not only relevant, but reliable." *State v. Yepez*, 2018-NMCA-062, ¶ 21, 428 P.3d 301, *cert. granted*, 2018-NMCERT-___ (No. S-1-SC-37217, Sept. 28, 2018). To determine reliability, the following factors should be considered:

> (1) whether a theory or technique can be (and has been) tested; (2) whether the theory or technique has been subjected to peer review and publication; (3) the known [or] potential rate of error in using a particular scientific technique and the existence and maintenance of standards controlling the technique's operation; and (4) whether the theory or technique has been generally accepted in the particular scientific field.

Id. ¶ 22 (internal quotation marks and citation omitted). "In addition to these four *Daubert* factors, New Mexico courts rely upon a fifth factor: whether the scientific technique is capable of supporting opinions based upon probability rather than conjecture." *Id.* (omission, internal quotation marks, and citation omitted); *see Daubert v. Merrell Dow Pharms., Inc.*, 509 U.S. 579 (1993); *Alberico*, 1993-NMSC-047, ¶ 47.

{26} The district court held a *Daubert-Alberico* hearing over the course of two days. Three witnesses testified in regard to the reliability of Roundup—Detective Robert Erdely and Agent Peña for the State and Thomas Blog for Defendant. At the conclusion of the hearing, the district court found that the State had met its burden on reliability and that Defendant's arguments went to the weight of the evidence. After careful review of the testimony of the witnesses, we conclude that the district court did not abuse its discretion when it determined that the evidence generated by Roundup was sufficiently reliable to be admitted at trial. We summarize the witnesses' testimony as follows.

{27} Mr. Blog testified regarding his concerns with Roundup's reliability in general, including that the software had not been appropriately tested, had not been subjected to formal peer review, and that its error rate had not been specifically established. However, Detective Erderly testified that the software had been independently tested one time to ensure that the program does single source downloads, it was not sharing, and it was keeping accurate logs. The independent test was done by an unidentified person hired by the FBI and involved a review of Roundup's source code, black-box testing, and a determination of the rate of failure. The independent test used Wireshark, a widely accepted form of monitoring the flow of information over an internet cable, to evaluate Roundup's results. Detective Erdely reported that the independent tester concluded that Roundup performed as described. Detective Erdely also testified that Roundup's results are validated at the end of every training that he teaches on the program and through every investigation that is undertaken with it. Mr. Blog acknowledged that real-world testing is a form of black-box testing.

{28} Detective Erdely conceded that Roundup had not been subjected to academic peer review outside of the University of Massachusetts Amherst, where the program was developed. He noted, however, that every investigator that uses Roundup does black-box testing and validation, which is a form of peer review. Mr. Blog testified that

Roundup's change logs were not public, which would have shown what bugs have been fixed, what bugs remain, and what operating systems and environments Roundup had been tested on. Detective Erdely explained that the release of software source code is not done for law enforcement tools, which also explains why change logs are not made available.

{29} Addressing concerns regarding Roundup's error rate, Detective Erdely stated that false positives are prevented because the program uses SHA-1 hashing, which compares two groups of information to see if they are exactly the same. Detective Erdely has never seen Roundup return a false positive during any of his in-class validations, nor has he received any reports of false positives from the 1,000 plus law enforcement personnel who use the program worldwide. Agent Peña testified that he had been using Roundup for over two years and that it had a zero percent error rate in his experience. Agent Peña also testified that he completed an in-class validation at the end of his training on Roundup, which demonstrated a zero percent rate of error.

{30} Detective Erdely testified that the log created by Roundup, which documents the time actions are taken, what torrent is being investigated, the suspect computer's IP address, the suspect's computer's port, the version of the software used by the suspect computer, and the investigator's IP address, is equivalent to Wireshark monitoring. Detective Erdely opined that Roundup's logs are even better than Wireshark in some aspects because the suspect computer is the computer identifying both the investigator's IP address and its own IP address.

{31} Based on the foregoing, we cannot conclude that the district court's determination that Roundup was reliable to be clearly untenable or not justified by reason. *See Flores*, 2010-NMSC-002, ¶ 25. While it does not appear that Roundup has not been subjected to peer review, and Defendant presented expert testimony that pointed out potential problems with the reliability of Roundup, the State provided sufficient evidence from which the district court could reasonably conclude that Roundup was sufficiently reliable based on an analysis of all of the *Daubert-Alberico* factors. We agree with the district court that Defendant's arguments go to the weight of the evidence. *See Acosta v. Shell W. Expl. & Prod., Inc.*, 2016-NMSC-012, ¶ 28, 370 P.3d 761 ("Vigorous cross-examination, presentation of contrary evidence, and careful instruction on the burden of proof are the traditional and appropriate means of attacking shaky but admissible evidence." (internal quotation marks and citation omitted)). For these reasons, we cannot say the district court abused its discretion.

IV. The District Court Did Not Err in Admitting Evidence Produced by Roundup and Forensic Toolkit

{32} Over Defendant's objection, the district court admitted the evidence produced by Roundup after concluding the evidence was not hearsay because it was computer generated. Similarly, the district court admitted the evidence produced by Forensic Toolkit after concluding that it was admissible under several theories: that it was not hearsay either because it was computer generated or not offered for the truth of the

matter asserted or, alternatively, if it was hearsay, there was adequate foundation for admission under the business record exception. The district court did note that the bookmarks and comments from the officers contained on the evidence produced by Forensic Toolkit were hearsay and would not be considered. "[T]he threshold question of whether the [district] court applied the correct evidentiary rule or standard is subject to de novo review on appeal." *Torres*, 1999-NMSC-010, ¶ 28.

{33} Hearsay is defined as "a statement that (1) the declarant does not make while testifying at the current trial or hearing, and (2) a party offers in evidence to prove the truth of the matter asserted in the statement." Rule 11-801(C) NMRA. A "[d]eclarant" is defined as "the *person* who made the statement." Rule 11-801(B) (emphasis added). A "[s]tatement" is defined as "a *person's* oral assertion, written assertion, or nonverbal conduct, if the *person* intended it as an assertion." Rule 11-801(A) (emphasis added). Whether the computer-generated evidence produced by Roundup and Forensic Toolkit is hearsay depends on whether the evidence constitutes statements under our Rules of Evidence.

{34} Defendant asks this Court to "find that the attestations made by a computer program constitute 'statements,' whether attributable to an artificial intelligence software or the software developer who implicitly offers the program's conclusions as their own." (Emphasis omitted.) Based on that contention, Defendant further argues that the automated conclusions from Roundup and Forensic Toolkit constitute inadmissible hearsay statements that are not admissible under the business record exception.[4] In so arguing, Defendant acknowledges that such a holding would diverge from the plain language of our hearsay rule's relevant definitions that reference statements of a "person." Defendant does not cite any authority that supports his argument and instead cites out-of-state authority that discussed and rejected a similar argument. "We are entitled to assume, when arguments are unsupported by cited authority, that supporting authorities do not exist." *State v. Ibarra*, 1993-NMCA-040, ¶ 13, 116 N.M. 486, 864 P.2d 302.

{35} Based on the following, we conclude the district court correctly determined that the computer generated evidence produced by Roundup and Forensic Toolkit was not hearsay. Agent Peña testified that his computer runs Roundup twenty-four hours a day, seven days a week and automatically attempts to make connections with and downloads from IP addresses that are suspected to be sharing child pornography. As it does so, Roundup logs every action it takes. Detective Hartsock testified that Forensic Toolkit organizes information stored on seized electronic devices into various categories including graphics, videos, word documents, and internet history. Because the software programs make the relevant assertions, without any intervention or modification by a

4Defendant also argues that we should adopt a scientific reliability test for "out-of-court statements" made by Forensic Toolkit if we determine they are not governed by our hearsay rules. Defendant does not develop this argument. Rather, in conclusory and circular fashion, Defendant contends that Forensic Toolkit is unreliable because the State did not qualify an expert to discuss it. We decline to address this undeveloped argument. *See State v. Guerra*, 2012-NMSC-014, ¶ 21, 278 P.3d 1031 (stating that appellate courts are under no obligation to review unclear or undeveloped arguments).

person using the software, we conclude that the assertions are not statements by a person governed by our hearsay rules.[5]

{36} Our conclusion is supported by the purpose behind our hearsay rule. "The hearsay rule excludes from admissible evidence statements that are inherently untrustworthy because of the risk of misperception, failed memory, insincerity, ambiguity, and the like." *State v. Mendez*, 2010-NMSC-044, ¶ 19, 148 N.M. 761, 242 P.3d 328. Statements produced by software are not subject to the same types of risks.[6] Because the evidence produced by Roundup or Forensic Toolkit does not constitute hearsay, we conclude that the district court did not err in admitting the same.

CONCLUSION

{37} We remand to the district court with instructions to vacate one of Defendant's two convictions for distribution of child pornography. We otherwise affirm Defendant's convictions.

{38} IT IS SO ORDERED.

KRISTINA BOGARDUS, Judge

WE CONCUR:

M. MONICA ZAMORA, Chief Judge

ZACHARY A. IVES, Judge

5The only exceptions are the bookmarks and comments in Forensic Toolkit, which the district court did not consider.

6Evidence produced by software presents other potential risks. One such risk is a malfunction that could result in misleading data, which can be addressed through our authentication rule. *See* Rule 11-901(A) NMRA ("To satisfy the requirement of authenticating or identifying an item of evidence, the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is."). Another potential risk is the production of unreliable data, which can be addressed under Rule 11-702.