STATE OF LOUISIANA
COURT OF APPEAL, THIRD CIRCUIT

15-40

STATE OF LOUISIANA

VERSUS

BENGY R. COOLEY

****

APPEAL FROM THE
THIRTIETH JUDICIAL DISTRICT COURT
PARISH OF VERNON, NO. 80641
HONORABLE JOHN C. FORD, DISTRICT JUDGE

****

SHANNON J. GREMILLION
JUDGE

****

Court composed of Ulysses Gene Thibodeaux, Chief Judge, Billy Howard Ezell, and Shannon J. Gremillion, Judges.

CONVICTION AND SENTENCE AFFIRMED; REMANDED.

Asa Allen Skinner
District Attorney, Thirtieth Judicial District Court
Terry W. Lambright
Assistant District Attorney
P. O. Box 1188
Leesville, LA 71496-1188
(337) 239-2008
COUNSEL FOR APPELLEE:
State of Louisiana

Jonathan W. Brown
Attorney at Law
1025 Mill Street
Lake Charles, LA 70601
(337) 564-6990
COUNSEL FOR DEFENDANT/APPELLANT:
Bengy R. Cooley

GREMILLION, Judge.

Pursuant to a search warrant executed on September 9, 2010, approximately fifty-three images of child pornography were found on a computer hard drive located at the home of Defendant, Bengy R. Cooley. In a statement to police, Defendant admitted to searching for child pornography, viewing child pornography, and deleting child pornography.

Defendant was charged by bill of information with one count of pornography involving juveniles, a violation of La.R.S. 14:81.1. Defendant initially entered a plea of not guilty to the charge but changed his plea to a plea of no contest. Defendant later filed a motion to withdraw his no contest plea, which was denied. Defendant then re-urged the motion to withdraw plea, and the trial court granted the motion.

Following a three-day bench trial, Defendant was found guilty as charged. Defendant filed a Motion for New Trial, which was denied. Defendant waived the delays for sentencing, and the trial court sentenced him to two years at hard labor, without benefit of probation, parole, or suspension of sentence.

Defendant now appeals alleging three assignments of error. Two assignments of error, which involve sufficiency of the evidence, merit serious consideration but ultimately lack merit. Additionally, Defendant's first assignment of error pertaining to sex-offender registration notification lacks merit. Thus, we affirm Defendant's conviction and sentence.

ERRORS PATENT

In accordance with La.Code Crim.P. art. 920, all appeals are reviewed for errors patent on the face of the record. After reviewing the record, we find there is one error patent.[1]

On February 1, 2013, Defendant's attorney filed a Motion to Elect Judge Trial which was granted. In *State v. Ray* 12-1217, p. 9 (La.App. 3 Cir. 5/1/13), 157 So.3d 13, 19, this court explained in pertinent part:

> Where the defendant's right to a jury trial was waived by his attorney, and there was no other indication that the defendant knowingly and intelligently waived that right, such as a confirmation in open court, the appellate courts have remanded the matter to the trial court for a determination of whether the defendant's waiver was knowing and intelligent. *State v. Zeringue*, 03–697 (La.App. 5 Cir. 11/25/03), 862 So.2d 186, *writ denied*, 03–3523 (La.4/23/04), 870 So.2d 298; *State v. Morris*, 607 So.2d 1000 (La.App. 3 Cir.1992), *rev'd on other grounds*, 615 So.2d 327 (La.1993). *See also State v. Pierre*, 02–2665 (La. 3/28/03), 842 So.2d 321.

In this case, the motion requesting waiver of jury trial was signed only by Defendant's attorney. Additionally, the record does not indicate Defendant knowingly and intelligently waived this right. The clerk of court of the district court attested in an affidavit that there were no minute entries or untranscribed hearings discussing Defendant's waiver of jury trial. The clerk of court also noted in the affidavit that "defendant was advised of his right to a judge or jury trial on February 1, 2011 and May 16, 2011." However, there are no minute entries or transcripts for February 1, 2011 or May 16, 2011 in the record or provided by the

[1]At sentencing, the trial court gave Defendant insufficient advice as to the time limitation for filing post-conviction relief as required by La.Code Crim.P. art. 930.8. The trial court stated, "You have 30 days within which to appeal and two years within which to file an application for post-conviction relief." However, when Defendant entered a guilty plea, which was later withdrawn, he signed a Waiver of Constitutional Rights which properly advised him of the prescriptive period of art. 930.8. Thus, we do not recognize the insufficient advisement at sentencing as an error patent.

clerk in the supplemental record. At a proceeding dated May 13, 2011, the transcript indicates that Defendant was advised of his right to be tried by a jury in the context of waiving his right at the guilty plea proceeding, which plea was later withdrawn. Thus, this matter must be remanded to the trial court for an evidentiary hearing.

In *State v. Clark*, 97-1064, p.8 (La.App. 3 Cir. 4/1/98), 711 So.2d 738, 742, *writ granted and remanded*, 98-1180 (La. 9/25/98), 726 So.2d 2, this court decreed:

> For the above reasons, we remand this case with instructions that the trial court (1) conduct an evidentiary hearing within thirty days of this date to determine whether defendant knowingly and intelligently waived his right to trial by jury and (2) re-lodge the appellate record, supplemented with a transcript of the hearing, within fifteen days of the hearing. The State and defendant will be given the opportunity to file supplemental briefs, should either party wish to raise any issues arising from the hearing.

See also State v. Fuslier, 06-1438 (La.App. 3 Cir. 4/4/07), 954 So.2d 866. Under the *Clark/Fuslier* procedure, this case will be marked final with the issuance of the opinion. The case will be remanded for the evidentiary hearing and the trial court ordered to prepare and lodge an appellate record containing the transcript of the evidentiary hearing. The new record will be issued a new docket number, and an opinion addressing the unresolved issues will then be issued under the new docket number.

SUFFICIENCY OF THE EVIDENCE

In assignments of error numbered two and three, Defendant challenges the sufficiency of the evidence. We address these assignments of error first, since a finding of merit would preclude the necessity of considering the remaining assignments of error. *State v. Hearold*, 603 So.2d 731 (La.1992).

Defendant asserts that the trial court was presented with only circumstantial evidence that he possessed child pornography–evidence that did not exclude every reasonable hypothesis of innocence. Additionally, Defendant asserts that the trial court incorrectly used the "dominion and control" standard in determining whether he possessed child pornography. Even using that standard, however, Defendant contends that the evidence was insufficient to find that he possessed the child pornography in question.

Standard of Review

This court has stated the following regarding the standard for reviewing a claim of insufficient evidence:

> The standard of review in a sufficiency of the evidence claim is "whether, viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found proof beyond a reasonable doubt of each of the essential elements of the crime charged." The *Jackson* standard of review is now legislatively embodied in La.Code Crim.P. art. 821. It does not allow the appellate court "to substitute its own appreciation of the evidence for that of the fact-finder." The appellate court's function is not to assess the credibility of witnesses or reweigh the evidence.
>
> The factfinder's role is to weigh the credibility of witnesses. Thus, other than ensuring the sufficiency evaluation standard of *Jackson*, "the appellate court should not second-guess the credibility determination of the trier of fact," but rather, it should defer to the rational credibility and evidentiary determinations of the jury. Our supreme court has stated:
>
> > However, an appellate court may impinge on the fact finder's discretion and its role in determining the credibility of witnesses "only to the extent necessary to guarantee the fundamental due process of law." In determining the sufficiency of the evidence supporting a conviction, an appellate court must preserve " 'the factfinder's role as weigher of the evidence' by reviewing 'all of the evidence . . . in the light most favorable to the prosecution.' " When so viewed by an appellate court, the relevant question is whether, on the evidence presented at trial, "*any* rational trier of fact could have found the essential elements of the crime

> beyond a reasonable doubt." Applied in cases relying on circumstantial evidence, . . . this fundamental principle of review means that when a jury "reasonably rejects the hypothesis of innocence presented by the defendant[ ], that hypothesis falls, and the defendant is guilty unless there is another hypothesis which raises a reasonable doubt."

State v. Francis, 12-1221, pp. 6-7 (La.App. 3 Cir. 4/3/13), 111 So.3d 529, 533, *writ denied*, 13-1253 (La. 11/8/13), 125 So.3d 449 (citations omitted).

State's Evidence

The first witness to testify at trial was Detective Carla Smith, a computer forensic examiner with the Beauregard Parish Sheriff's Office from 1996 to 2011. Detective Smith used a program called the Wyoming Tool Kit to search for activity involving child pornography in her geographic area. Files that contain child pornography are identified by a "SHA Value" or "Hash Value"–a string of alphanumeric characters provided to law enforcement by the Missing and Exploited Children's Group from Virginia. Law enforcement agencies know that certain SHA values represent child pornography. The Wyoming Took Kit program creates a list of files with SHA values that are known to be child pornography. With the file list, Internet Protocol (I.P.) addresses are also assigned to each file. Each modem has an I.P. address.

In May 2010, Detective Smith conducted an internet investigation to determine if anyone in her area was downloading child pornography. Detective Smith's attention focused on I.P. address 74194243212 because "there were [sic] a huge amount of child pornography, known child pornography, images with that I.P. address." Detective Smith obtained a search warrant for Suddenlink Communications to obtain the subscriber information for I.P. address 74194243212. Detective Smith identified State's Exhibit Number One as the list

she obtained from the Wyoming Tool Kit regarding files accessed by this I.P. address. In addition to the I.P. address, Exhibit One also contained a date stamp of when the files were downloaded onto that computer. The date stamps ranged from October 15, 2009, to June 7, 2010.

Detective Smith testified that a "GUID," a "globally unique identifier," "identifies the computer to the file itself to that I.P. address." Detective Smith further testified that when LimeWire is installed on a computer, the installation will be assigned a "GUID" number and is unique to that installation of LimeWire.[2] According to Detective Smith, all of the files on the list in S-1 were pulled up as a result of searching for child pornography.

Detective Smith identified State's Exhibit Number Two as the subpoena she sent to Suddenlink Communications to find out the subscriber information for the I.P. address at issue. According to representatives from Suddenlink Communications, the subscriber to the I.P. address was Defendant who lived at 296 Ambler Road, Leesville, Louisiana. When Detective Smith realized that the address was outside of her jurisdiction, she contacted the Louisiana State Police.

Trooper Amanda Fournier of the Louisiana State Police testified that after she received information from Detective Smith, she obtained a search warrant for Defendant's residence. The search warrant was executed on September 9, 2010, at which time Trooper Fournier and other troopers knocked on the door of Defendant's residence. When no one answered the door, the troopers entered through an unlocked door to the kitchen. The troopers located a document indicating that Defendant worked for Probation and Parole and then contacted

[2]Limewire is a program that allows users to share files over the internet.

Defendant at work. While waiting for Defendant to arrive, the troopers located a laptop at the residence.

Shortly after Defendant arrived at his residence, he was advised of his rights. When Defendant was asked if he downloaded pornography at his residence he originally answered, "No." At some point, however, Defendant changed his answer. When Trooper Fournier was asked what Defendant told the troopers when he changed his answer, the following colloquy ensued:

> A: That he downloaded pornography via the Internet and that he may have seen some pornography involving juveniles.
>
> Q: All right and at that time was he asked about the downloading of the pornography and utilizing LimeWire?
>
> A: Yes.
>
> Q: All right and did he admit to you to using LimeWire to download pornography?
>
> A: Yes.
>
> Q: So, your testimony is that he admitted to downloading pornography, he may have downloaded some involving children? Did he say may?
>
> A: Yes.
>
> Q: That he may have downloaded some involving children?
>
> A: Correct.

Since the GUID listed on the file list Trooper Fournier received from Detective Smith matched the GUID number on the computer found in Defendant's residence, Trooper Fournier concluded that the computer seized from Defendant's residence was the computer being used to download child pornography.

Defendant was transported to the Vernon Parish Sheriff's Office to be interviewed further. When Trooper Fournier was asked what Defendant said when asked if he downloaded videos from LimeWire, the following colloquy ensued:

> A: He indicated that he used search terms such as P.T.C.H. which the actual term is P.T.H.C. which stands for pre-teen hard core and I believe one of the other search terms he indicated was Little Teens or Little Girls. He also indicated that some of the videos that he had seen and he was able to describe two of those videos for us.
>
> Q: Let me ask you about the search terms. We can just take it as is, but you actually would have to place those terms into the computer in order for it to search for that type of material, is that correct?
>
> A: Yes.
>
> Q: Would have taken some effort on his part?
>
> A: Yes.
>
> Q: And, I mean, the fact that he used those terms, are those terms that in your experience and training and knowledge are terms that are known child pornographic type search terms.
>
> A: Yes.
>
> Q: In fact, those are the terms that you - - the State Police uses in order to do their investigation, is that right?
>
> A: Yes.
>
> Q: Was he ever asked why he used those particular search terms?
>
> A: I don't recall if I asked him that specific question.
>
> Q: All right. Was he ever asked - - did he ever indicate to you that he was curious about anything?
>
> A: Yes.
>
> Q: What, if anything, did he state?
>
> A: He stated that he had heard of several people that had gotten arrested for child pornography and he was interested and curious as to what child pornography was about.

Q: All right. Did he admit to you that he had indeed searched for child pornography?

A: Yes.

Q: Now, did - - in interviewing him did he ever admit to you that he viewed certain videos containing child pornography?

A: Yes.

Q: Okay. Did he provide a description?

A: Yes.

Q: Okay, explain.

A: One of the files that he described, if I remember correctly, involved a Brazilian female child approximately ten years old that was performing oral sex on a male's penis. And I believe he described another video in where a female child was involved in sexual intercourse with an adult.

Q: All right and did he specifically use that - - tell you that he viewed a video of a female under the age of ten who had no pubic hair and small breasts?

A: Yes.

Q: And he specifically said under ten?

A: I believe so.

. . . .

Q: Did he describe a second video? Well, you mentioned two videos, particularly, did he describe a video containing a 13 or a 14 year old performing oral sex on a male's penis?

A: Yes.

Q: And he provided a description of that for you?

A: Yes.

Q: Was Mr. Cooley asked how long the videos were?

A: Yes, sir, he said that they averaged approximately 30 seconds to a minute and a half.

> Q: Okay and was he asked about whether he downloaded the videos and viewed them?
>
> A: Yes.
>
> Q: Okay and other than the two videos that you've spoken about, did he tell you whether or not he viewed any other videos? Just trying to get what he told you at that particular moment.
>
> A: I believe he said that he would download the videos, view the videos, and then delete then [sic].

An audio recording of Defendant's statement was introduced into evidence as State's Exhibit Number Eight and played for the jury. It is clear from listening to the recording that a portion of Defendant's interview was accidentally unrecorded. In the portion that was recorded, Defendant was asked if the file he looked at was a girl younger than ten engaged in oral sex with a man. After listening to the audio recording, it sounded like Defendant responded, "Yes." Defendant was then asked if he saw a file from Brazil in which several girls were giving oral sex to a man wearing a hood. Defendant responded, "Right." When asked if he had looked at "fifty something" files, Defendant said "No sir, not with underage girls." Defendant insinuated that some of the files were of "animals and such" that he should have never looked at. Defendant allowed the detective to look at the photos on his phone. When asked by the detective what he did with the "child pornography" files after he looked at them, Defendant responded, "I just deleted them." When asked how soon he deleted the files after he looked at them, Defendant explained that he tried to set up his computer to erase everything. Defendant told the detective that he never went in and did it himself but selected the option for it to be done. Defendant said he never used anything to erase his hard drive. Finally, Defendant stated that he "was completely innocent as far as looking at that for any kind of stupid reason."

According to Trooper Fournier, State Trooper J.D. Parker, a computer forensic examiner with the Louisiana State Police, located fifty-three images of child pornography on the computer seized from Defendant's residence. Trooper Fournier testified that Defendant never indicated that anyone other than himself downloaded the images.

During cross-examination, Trooper Fournier stated that when she searched Defendant's residence, she did not find any materials to clean a hard drive. Trooper Fournier described Defendant as cooperative and friendly. Trooper Fournier agreed with Trooper Parker that neither saw pornography when previewing Defendant's computer at Defendant's residence.

Trooper Fournier agreed that LimeWire is used to download other things besides pornography. In fact, Trooper Fournier testified, music is a popular item to download with LimeWire. Legal pornography is also available for downloading with LimeWire. When asked if Defendant said he used LimeWire to download music, Trooper Fournier believed Defendant stated that he used it to download music and videos. Although Defendant originally denied using LimeWire to watch legal pornography, Defendant eventually told Trooper Fournier that he did use it to watch legal pornography. Defense counsel then asked Trooper Fournier the following:

> Q: And, I mean, we heard him just now on the tape when y'all were asking him about - - y'all were describing the movies kind of that you said he talked about off the tape and telling him about the amount and he went on to tell you, well, actually, it's , you know, the animals and some other things that he had watched, correct?
>
> A: Yes.
>
> Q: He was kind of embarrassed about that he kind of watched those things, correct?

A: Yes.

Defendant willingly gave the trooper his cell phone, which contained nothing prohibited.

On re-direct examination, Trooper Fournier opined that because the computer was in her care from the time it was seized until a forensic examination was performed on it, the pornographic images were on Defendant's computer at the time it was seized. Regarding Defendant's admission that he searched for adult porn, the following colloquy ensued between the State and Trooper Fournier:

> Q: Now, she asked about the fact that this defendant admitted that he searched for adult porn, but isn't it also true that your previous testimony is that he specifically searched for pre-teen hard core porn?
>
> A: Yes.
>
> Q: That's - - that involves juveniles, is that correct?
>
> A: Yes, sir.
>
> Q: Also, you indicated he searched for under terms Little Teens, is that correct?
>
> A: Yes.
>
> Q: And he also admitted to you that he did that because he was curious?
>
> A: Yes.
>
> Q: And pornography involving juveniles, it includes still shots or images or reproductions, does it not?
>
> A: Yes.
>
> Q: And is it also true that this defendant admitted to you that he attempted to delete the videos, is that right?
>
> A: Yes.
>
> Q: So, the fact that you don't have any videos could be that he attempted to delete them, is that right?

A: Yes.

On re-cross examination, Trooper Fournier again testified that Defendant said he did not possess anything that would allow him to be able to clean a hard drive or delete images. Trooper Parker examined Defendant's computer on September 16, 2010. When Trooper Parker previewed Defendant's computer at Defendant's residence, he did not see any pictures on the computer. Trooper Parker had no doubt, however, that he found the computer they were looking for because the computer had the same GUID (Global Unique Identifier) number that they had been investigating. Trooper Parker further stated that it is not unusual to find no images on the computer during a cursory preview of the computer.

On September 16, 2010, Trooper Parker started a forensic examination of the computer. Trooper Parker explained the examination process, which begins with removing the hard drive from the computer and making an exact copy of the hard drive. Once the drive is copied, the copy is loaded into a Forensic Tool Kit (FTK). Trooper Parker further explained:

> A: Once I started examining the computer at some point I saw that I wasn't finding the images and pictures and videos that we had saw on the front end pursuant to our search warrant. So, I did what's called data carving and what that does is that just goes through the drive, starts from start to finish, and looks for - - every file has a header at the beginning of it and it tells the computer what type of file it is. So, if it, you know, starts out with these letters it's a picture file. If it starts out with these letters it's a [sic] AVI video file. So, it - - the data carving goes through the drive looking for those headers and then pulls out that bit of information so you can look at it and, you know, make sure it is what it says it is. And I was able to data carve approximately 53 - - well, I was able to data carve a lot of picture files, but I was - - I found 53 images of child notable - - of children that are being sexually abused.

The State asked Trooper Parker if the fact that he had to use this tool in order to draw the images out of the computer meant that the fifty-three files were not capable of being viewed without such equipment. Trooper Parker explained:

> A: No, you could use any off the shelf - - there's software off the shelf that you can recover files. One is called Recover, it's a free utility for getting pictures back that you've deleted on your camera, on your SD card or whatever media. It will pull those files right out for you.
>
> Q: And the fact that you did this does this mean that the files were not viewable at one time of this computer?
>
> A: No, absolutely not.
>
> Q: What is it? I mean . . .
>
> A: It indicates that the files were on the computer, they were viewable on the computer and that they'd only been deleted which when you delete a file it only deletes the portion of where the file is. If your remember back in the days of the library, if you have the card catalog in the library, you looked in the card catalog to find the book you wanted to look at. Well, this would be like taking the card out of the card catalog but the book is still sitting on the shelf. It's still available. It's just saying to the computer if you want to write something you can write it in this space now.
>
> Q: I got you and once you located these images on the computer what, if anything, did you do next?
>
> A: I went back and I also confirmed again the GUID number and that the GUID number was the GUID number that we had looked at prior to the execution of the search warrant and it's an exact match too.

Trooper Parker testified that he tracked the images located on the computer with the file list obtained from Detective Smith and found images on the computer that were identified with the file list. Trooper Parker made copies of the images, and those images were displayed for the trial court.

On cross-examination, Trooper Parker testified that Defendant's computer was password protected. Trooper Parker explained that Exhibit One was a report

generated on the front end of their investigation, which shows the dates on which files were available for file sharing, not necessarily downloading. Trooper Parker explained:

> A. What this report [(S-1)] shows is those are dates that they were available for sharing, not necessarily a download. The way - - the way file sharing software works is when you start downloading it, it puts it in your shared folder. It comes down in chunks, so, say, I get half of a file. Well, then somebody else wants to download that same file it's in my shared folder. Well, it was half a file so it starts grabbing from me also because when you're downloading the idea behind peer to peer software is is [sic] not just two users, it's a whole network of users. And, that when I download the file, if ten people have it I get a little chunk from this person, little chunk from that person, I get it a lot quicker. So, that's how peer to peer works.

The dates listed on Exhibit Number One are October 15, 2009, to June 7, 2010. Trooper Parker explained that on these dates, the information was available for sharing. Trooper Parker agreed that the date the computer was purchased would be important. Although Trooper Parker was not aware of any case wherein a computer was purchased already containing illegal information, the trooper acknowledged that it could happen. Trooper Parker explained that this did not happen in the present case:

> A: But in this case here, you know, what you're saying is not what happened because these - - the FrostWire or the LimeWire files were downloads to - - is in the user name of Ben. So, if it had been owned previously by - - it would have to be somebody named Ben. It's in his - - it's in Ben's user name.
>
> Q: Okay.
>
> A: And it's installed in that user name, so there's no way that somebody else owned it, you know, unless their name was Ben would it be in that file.
>
> Q: Okay. So, if there were downloads in 2009 and a computer was purchased some time, maybe, in the spring of 2010 you would still think that that was for Ben, so to speak, or whoever you saw the name being associated with?

A: Okay. If you're - - if you're indicating from the list, and I'm catching kind of where you're going, that list depicts the I.P. address which has nothing to do with the computer that's entered into evidence.

Q: Okay.

A: The I.P. address is assigned to the modem at the house of Mr. Cooley. So, if he buys this computer - - if you're saying he's buying this computer after a date that's on the list then another computer at his house at that time was downloading child pornography.

Q: Okay and, so, the GUID number also stays with him is what you're saying?

A: No, the GUID number is assigned to the installation of the software.

At Defendant's residence, Trooper Parker verified that the GUID number provided by Trooper Fournier was on the computer. Trooper Parker testified that he did not remember seizing any data-carving software from Defendant's residence. When Trooper Parker initially examined the hard drive of the computer, he did not find anything. Trooper Parker discovered the files only after using the data-carving software that allowed him to view files that had been deleted. Pursuant to defense counsel's questions regarding the capability to view these files, the following colloquy took place:

Q: It's my understanding, sir, and correct me if I'm wrong, that these are files that are in unallocated space, is that correct?

A: That's correct.

Q: Okay. So, that means that they've basically lost their connection to the computer's operating system?

A: They have just - - just the - - what's in the operating system saying that - - pointing to that file is what's lost.

Q: Okay. Does it mean that there are no identifiable artifacts that remain when something is in an unallocated space?

A: There are no file properties associated with the files.

Q: Okay and unless I have software that can do the carving that you can do I can't view these, correct?

A: No, you can view them.

Q: Without carving software?

A: You can - - you can get Recover which is - - it's a carving software. But you're making a point that I have to do it, but anybody can do it. You can do it . . .

Q: I can if I possess the software, but absent the software I can not?

A: That's correct.

As for being able to tell when images in unallocated space were placed on the computer, Trooper Parker agreed that he could not tell when the images were loaded to the computer. On re-cross examination, Trooper Parker stated that when he examined the computer, he verified the GUID number and recovered child pornography from an unallocated space. In summation, Trooper Parker testified that the child pornography was on the computer "at one time or another."

Defense Evidence

The first witness to testify for the Defense was Cody Cole, a shift manager for Wal-Mart. Cole identified Defendant's Exhibit Number One as a Wal-Mart receipt from the Deridder Wal-Mart store. The receipt was for the purchase of a laptop computer on March 17, 2010. On cross-examination, Cole testified that his store's computers are sealed and are not sold with any preinstalled software.

Maria Manuel, Defendant's fiancé, testified that she visited Defendant at his home every Wednesday and Thursday. When Manuel first met Defendant in June 2010, Defendant did not keep his house locked. Manuel testified that Defendant had a laptop, which he kept in the living room. Manuel admitted to using the

laptop and stated that the laptop was not password protected. On cross-examination, Manuel denied ever downloading pornography to the computer. Manuel also stated that she had no knowledge of Defendant downloading pornography. Manuel did remember using LimeWire on Defendant's computer to download a song. When asked if she knew when Defendant purchased the computer, Manuel said she saw the receipt dated March 2010. Although no one else lives in Defendant's home, Manuel testified that his kids visit on weekends. On re-direct, Manuel testified that Defendant kept the computer in the living room when family and friends visited.

Robert Davis, a former neighbor of Defendant, described Defendant as a carefree guy who did not lock his home. According to Davis, Defendant gave him an open invitation to go into his home even if Defendant was not home.

Victor Warwick, a pastor, testified that he is Defendant's brother-in-law. Warwick stated that he had known Defendant for twenty-six years and knew Defendant to leave his doors unlocked. Warwick described Defendant as a man of integrity.

The final witness offered by the defense was Derek Hinch, a software developer employed by Lamar Advertising as the head of software development. Hinch testified that he formerly worked in the United States Air Force Electronic Warfare Research and Development and consults with the Federal Bureau of Investigation "on technical feasibility questions." Hinch explained technical feasibility questions as follows:

> A: Okay. Generally, it's technical feasibility questions. If they have a search warrant that says that sets certain parameters down on their investigative methods to determine who a person is. Let's say, a person anonymizes themselves using some sort of file sharing software and they receive some content. The FBI might may not

> know who that person is because they may have used some method to obscure themselves, technology such as Tor. I would consult with them to help unmask, if you will, the person on the other side of the coin while staying within those bounds of what they're restricted to be able to do.

Hinch also worked with an agency called "ICE" regarding pornography cases, evaluated reports of forensic examiners, and performed his own forensic examination of computers.[3] When the State objected to Hinch testifying as an expert, the trial court stated that it would allow Hinch to testify in the same capacity as Trooper Parker because Hinch seemed to be as knowledgeable about computers as Trooper Parker.

Hinch explained that he was given a summary analysis of a disc forensic examination done by Trooper Parker. Hinch also gave the following "layman's definition" of LimeWire:

> A: Sure. People send and receive files, those files are then indexed. When somebody searches for the files it returns the result list of who has those files. You can browse an individual's share of items that they share as well as browse other people's that may have something you're interested in. It's commonly known as a pretty nefarious place because the files are - - they're just - - it's more used for criminal activity and the distribution of . . .
>
> Q: But, you said it's known as a nefarious place and used for criminal activity. How do you know that?
>
> A: Okay. There have been several publications on it. Hackers Magazine actually did an example of people who would use LimeWire for muling. In a lot of cases . . .
>
> Q: When you say LimeWire for muling, you know, I'm a former prosecutor so . . .
>
> A: Okay.
>
> Q: . . . when I think of muling, I think of drug trade, so I want you to . . .

[3]When asked what ICE was, Hinch simply stated, that it "was more cases involving pornography."

A: Kind of similar.

Q: . . . explain to this Court what you mean when you say LimeWire is used for muling.

A: Okay. Let's say that there was a file on a web site that if I were to access that file somebody would discover who I was. So, what I do is I find basically what's trending on the Internet. Let's say a Miley Cyrus video and I turn that video malicious in such that it performs an action that goes out and gets the file that I originally wanted from the location of the place I can't go. So, I give you a Miley Cyrus video but what you don't know is that the user, sure you're watching a Miley Cyrus video, but in the background it's actually installed some software that I can now make requests through your LimeWire to go get other types of content.

. . . .

Q: [L]et's say that I'm doing a search and I want to search for adult porn, and, so, I might put in some key words that would get me adult porn. Is there a way that if I'm downloading that through what's legal, through LimeWire, that illegal porn might come to me without me asking for it?

A: Most definitely, yeah.

Later, Hinch explained that when a file is deleted, an "artifact" is left over:

A: Windows gets rid of the file name, leaves the bytes on the disc, but it also records the action of the file deletion. That's called an artifact, it's not a log, you don't delete that.

According to Hinch, these artifacts would show the creation date and modification date of the file. When defense counsel began questioning Hinch as to Trooper Parker's preview of Defendant's computer at his residence, the following colloquy ensued:

Q: Okay. So, let's say if I had downloaded some child pornography and kept it for a while and deleted it. Is - - is it possible with a preview to see that on my computer?

A: Yes. It really depends - - that's kind of hit or miss, it depends on what you deleted it with. If you use some form of special delete tool you may not find it in the preview. However, you will find other

artifacts on the disc about the file, but a preview is - - basically what the operating system is willing to tell you about or what the disc . . .

. . . .

Q: Do you think it's probable that you should see it in a preview?

A: Yeah, yeah. I mean, typical computer usage you would see the fact that the file once existed.

Q: Okay and, so, what you're saying is you'd see some artifacts?

A: Definitely and here's how sensitive artifacts are, let's say you got all this content, okay, from LimeWire sat down at your computer, don't have a preview pane open, don't click on any image. It's simply a - - the file folders open with the list of files that it downloaded. Okay? Let's say you highlight them all and click delete. Not only is every file name still kept, not only are the file creation times, all those artifacts, but I also know that you only had the browser window open, that you didn't click on anymore of them. I can also tell what you didn't do. I can tell that you didn't go and open them or didn't preview them. The fact that no artifacts exist whatsoever on this system is probably the most disturbing fact in the prosecution's assessment of a user participating in a action with child pornography. Those artifacts will be left.

Q: So, and you say that's probably the most disturbing, why? Why do you think that?

A: If somebody were to come to me and - - as they have before, investigators, and say, listen, we recovered this disc, we found this unallocated space, there were these chunks of bytes that when formed up are pictures of child porn. However, we have no record of the user having ever deleted them. We don't have a record of the user having touched them, viewed them, previewed them, opened them. We have no knowledge of the time that they were created, modified, edited, anything. We don't know anything about these files that we can tie back to a user or the operating system. The common person would have no way to recover these files unless they had the same type software that the forensic investigator did.

Q: Okay.

A: I would have advised - - I would have said, well, you're going to have trouble prosecuting because this person never even opened a window that the file was seen in. That's what it's telling me is that the user had never had knowledge of it.

> Q: So, are you telling me that when you go back in, you should be able to see even if I've deleted it, when I opened it, when I viewed it?
>
> A: Yeah, when it was created. All of these things are kept.

When asked if Trooper Parker, during his initial preview of Defendant's computer, should have been able detect an image that was deleted without any special tools for deleting, Hinch replied, "You can, yes." Hinch further stated that "[t]here would have been some record of him interacting with any one of those 53 files which, per the State's own admission, do not exist." Because no artifacts of the fifty-three files were recovered, Hinch concluded:

> A: These files were never actively used on this computer and all that means is that we have no record of that person ever accessing these bytes. We can not prove that the defendant in this case with forensics touched, opened, deleted these files. Now, they're going to say deleted because there's empty bytes left from the end of the disc and there's no record of those files on the operating system. But there's no artifacts showing that they were deleted either, so that's sort of an intelligently dishonest statement in saying that they were deleted files recovered because there's no action of deletion that's found in the artifact logs.

Hinch went on to say that with a "hundred percent surety that the individual who used that computer never accessed any one of those 53 files with certainty."

When asked if there was any way to tell how the images found with Trooper Parker's data-carving equipment were put on the hard drive, Hinch replied, "No, because they're not actual files, they're contiguous branches of bytes." Hinch also opined that it was important to know when Defendant came into possession of the computer, noting that Trooper Parker's report showed some of the downloads occurred prior to the computer purchase date. When asked if Defendant could have been using another computer, Mr. Hinch responded:

> A: Well, I mean, that's always feasible, the I.P. address-wise you could have any computer behind the I.P. address, but all the I.P.

address nowadays tells me that somebody used his Wi-Fi, doesn't even tell me what computer they used.

Q: Okay. So, what you're saying is what an I.P. address tells is that somebody was using my Wi-Fi . . .

. . . .

A: Could be you, could be your neighbor, could be - - I mean, even the most modern encryption standards can be broken with free tools off the Internet.

Hinch further testified that there have been several cases in which computers have been bought that already contained pornography.

On cross-examination, Hinch stated that he would need to examine Defendant's computer to determine if Defendant was used as a "mule." When asked if he had no personal knowledge as to whether or not Defendant's computer was hacked, Hinch responded, "Neither does the State."

On re-direct examination, when defense counsel asked Hinch why he thought something was wrong with the State's case against Defendant, Hinch responded:

A: The number one thing that bothered me is that the evidence that was presented to me showed files did exist in unallocated space, the data did, but the user of the operating system had no knowledge of their existence and that was further proven by no artifacts existing in the forensic examination of those files when they were created, modified, deleted. There was information that a person who would normally be involved in downloading, viewing, deleting or otherwise those particular files - - that information would have been there. And, so, by whenever I see that if it was a law enforcement agent that came to me with that report I'd advise them no prosecution. It would be intelligently and morally dishonest to prosecute when the evidence clearly dictates forensically that the user is not the one who viewed or deleted the files that they found at the end of the disc. That's my personal conviction on it.

Hinch further testified on re-cross examination:

A: I can testify that the user on the computer did not interact with those 53 files and that's based off the statement from your own

forensic examiner during his preview which would have detected the interaction.

The State called Trooper Parker to testify on rebuttal. The State asked Trooper Parker about the fact that there were downloads to Defendant's I.P. address before the purchase date of his computer on March 17, 2010. Trooper Parker responded:

> A: Funny you would ask that question because if you look at the - - you know, I'm looking at this receipt here, it's bought - - this computer was bought on 3/17/2010. Windows on that day, 3/17/2010, was registered to Ben. Also, on that day, 3/17/2010, LimeWire was installed with the GUID number that I previously testified about that we found on that computer. If you look at the file list there's numerous GUIDs on that file list.

When asked whether LimeWire could have been installed on another computer that was owned by Defendant prior to March 17, 2010, Trooper Parker responded:

> A: Yes, sir, by the - - by the evidence here with it being purchased on 3/17 there would have been another computer prior to. But if you look at this file list, this associated - - this GUID had 163 files shared that we saw and I was able to physically verify 14 of those files shared with that GUID number were files that we introduced into evidence that we showed the Court. So, 14 of those files were on this file list shared with this GUID number between 3/17/2010 and 6/17/2010.
>
> Q: All right. So, in layman's terms what you're telling us is that this computer with - - even after it was purchased there was 163 images of child pornography downloaded to this computer?
>
> A: They were shared from that computer.

On cross-examination, Trooper Parker testified that he tested Defendant's computer for rogue software that would cause unintentional downloads. Finally, when asked how he could tell that fourteen of the images from the file list were on Defendant's computer between March 17, 2010, and the date the computer was seized, Trooper Parker testified that he "took a totality of all the evidence[.]"

Trial Court's Decision

After hearing the above testimony and closing arguments, the trial court found Defendant guilty as charged:

BY THE COURT:

> All right, the Court has heard the case, closing arguments of counsel, considered the evidence, the offerings and the testimony. There's no question that this defendant did access these - - this site of - - pornographic site that contained these horrible and filthy pictures. There's no question about that. Looking at pictures is not proscribed under the law, it's possession of child pornography. No question that he searched for it, no question that he viewed it. His admissions were to that effect. It was not established when he did this by his statements. The list of Internet providers or I.P. address list indicated that there were four computers that were used at different times. The pictures that were introduced into evidence were not identified with any of the - - of these I.P. searches that were introduced into evidence. These pictures were, according to the State's expert, Mr. Parker, were contained in an area of inaccessible memory that you couldn't get to it without a special computer program that you would have to get off of the Internet somewhere. No evidence that this defendant was a sophisticated computer user, no evidence that he knew how to get this program or was disposed to do it anyway. There's no evidence that he tried to access these hidden files, for lack of a better description. They were inaccessible. There's no evidence that he knew they were even there and they don't know when they were put there. They got there, they just don't know when or what vehicle was used to place them there. Possession is defined as the - - as being the act of exercising dominion and control over a thing. Certainly, the defendant exercised dominion over these things because he had the computer. They were in the computer and he exercised - - he had the computer. That's dominion. Control is the ability to put your hands on it, so to speak - - get it. That's where I think the problem lies is that this defendant did not have control over the images contained in the computer that were introduced into evidence. However, the I.P. address list shows that defendant accessed child porn from the time he purchased this computer, March 19th, extensively, or this pornographic site. I think that site had both adult pictures and juvenile pictures on it and the - - it shows that accessed it extensively. He admitted looking at the pictures and he admitted deleting the pictures. The act of deleting an image is the exercise of control. That's where we had dominion and control during when these - - I don't know what images they were. I don't know if - they weren't the ones that got in this - - they found in the computer, but I find that it's - - it is - - the Court can conclude that this defendant possessed

> those items when he deleted them at the time shown on the I.P. list after March 17th, 2010. So, I find the defendant guilty as charged.

Defendant's Argument

Defendant asserts that the State relied solely on circumstantial evidence to prove that he possessed child pornography, since no witness saw him viewing such pornography and the police found no illegal material when his computer was first examined. Defendant argues that the State failed to exclude every reasonable hypothesis of innocence, since Defendant's expert explained various ways the images could have made their way to the inaccessible memory of Defendant's computer, even without his knowledge.

Defendant also argues that the trial court erred in using the "dominion and control" standard to determine whether he possessed the child pornography in the present case. Defendant argues that the appropriate standard is whether Defendant intentionally possessed the child pornography.

Finally, even under the "dominion and control" standard, Defendant argues that the evidence was not sufficient to prove that he exercised dominion and control over the child pornography. Defendant contends that he had no knowledge that "the pornography remained on his computer after it flashed across his screen and was immediately deleted." Additionally, Defendant argues that his rejection of the images by deleting them as soon as he saw them indicates a lack of intent to possess the child pornography. Finally, Defendant asserts that he could not possess images he could not access.

Analysis

Although Defendant asserts that the trial court used the wrong standard when it considered whether he exercised dominion and control over the images in

question, Defendant merely cites the absence of jurisprudence using such a standard for child pornography cases.[4] There is no need to address whether use of the "dominion and control" standard was correct, since the evidence was sufficient even under the standard asserted by Defendant as being correct.

Defendant was charged with the commission of pornography involving juveniles between the dates of June 23, 2010, and September 9, 2010. Although this issue was not discussed in the trial court, during that time frame, the legislature redefined pornography involving juveniles. The pre-amendment definition was in effect between June 23, 2010 (the beginning date charged in the bill of information), and August 14, 2010 (the day before the post-amendment definition became effective). At that time, the offense of pornography involving juveniles provided, in pertinent part:

> A. Pornography involving juveniles is any of the following:
>
> (1) The photographing, videotaping, filming, or otherwise reproducing visually of any sexual performance involving a child under the age of seventeen.
>
> (2) The solicitation, promotion, or coercion of any child under the age of seventeen for the purpose of photographing, videotaping, filming, or otherwise reproducing visually any sexual performance involving a child under the age of seventeen.
>
> (3) The intentional possession, sale, distribution, or possession with intent to sell or distribute of any photographs, films, videotapes, or other visual reproductions of any sexual performance involving a child under the age of seventeen.
>
> La.R.S. 14:81.1.

[4]The "dominion and control" standard has been used by some federal courts. *See United States v. Romm*, 455 F.3d 990, 998 (9th Cir. 2006), *cert. denied*, 123 S.Ct. 1335 (2003), and *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002), *Cert. Denied,* __ U.S. __, 1275 S.Ct. 1024 (2007)..

In *State v. Roberts*, 01-154, p. 6 (La.App. 3 Cir. 10/3/01), 796 So.2d 779, 784, *writ denied*, 01-2974 (La. 9/20/02), 825 So.2d 1163, this court interpreted the "visual reproduction" requirement of La.R.S. 14:81.1(A)(1) to be satisfied by the defendant's "intentional searching for nude images of juveniles by using certain key words to access web pages which contain such images and the pulling up and viewing of these offensive images on the computer screen . . . ." The court in *Roberts* found that such conduct constituted "visual reproduction" of child pornography and, thus, constituted pornography involving juveniles. In the present case, Defendant admitted to using terms to search for child pornography, to viewing the child pornography, and to deleting the child pornography. Thus, the "visual reproduction" requirement of the pre-amendment version of La.R.S. 14:81.1(A)(1) was satisfied.

There is an issue, however, with the date of the offense alleged in the bill of information. The bill of information charged Defendant with committing the offense between June 23, 2010, and September 9, 2010. According to Detective Smith and State's Exhibit Number One, the latest recorded date on which Defendant accessed pornography on his I.P. address was June 7, 2010. Thus, although there is evidence that Defendant's computer hard drive contained child pornography within the dates alleged in the bill of information, there is no evidence that the Defendant accessed those images between June 23, 2010, and September 9, 2010, the dates alleged in the bill of information.

Since the date was not essential to the offense, however, the State's proof is not limited to the dates alleged in the bill of information. Louisiana Code of Criminal Procedure Article 468 provides:

> The date or time of the commission of the offense need not be alleged in the indictment, unless the date or time is essential to the offense.
>
> If the date or time is not essential to the offense, an indictment shall not be held insufficient if it does not state the proper date or time, or if it states the offense to have been committed on a day subsequent to the finding of the indictment, or on an impossible day.
>
> All allegations of the indictment and bill of particulars shall be considered as referring to the same date or time, unless otherwise stated.

In *State v. Franklin*, 263 La. 344, 268 So.2d 249 (1972), *overruled on other grounds by State v. Tharp*, 284 So.2d 536, 543 (La.1973) *and State v. Douglas*, 278 So.2d 485 (La.1973), the supreme court found the trial did not err in denying a motion for directed verdict of acquittal based on the fact that the indictment charged the defendant with committing murder on January 14, 1970, and the coroner's report showed the victim died on January 15, 1970. The supreme court found that this variance did not vitiate the indictment or bar proof of the correct date. In a footnote, the supreme court stated:

> When the date is not essential to the offense, the indictment is not insufficient when it states the incorrect date, although amendment to conform to the proof may be permitted if objection is made.

Id. at 252 n.3 (citations omitted).

In the present case, the date of the offense is not an essential element because time is not an essential element of pornography involving juvenilles. No objection was made to the introduction of evidence regarding access to child pornography on Defendant's I.P. address prior to the date alleged in the bill of information, and no prejudice has been alleged. Furthermore, the State answered Defendant's bill of particulars with a file listing showing Defendant accessed child pornography prior to and on May 30, 2010, dates that are clearly outside the dates

alleged in the bill of information. Thus, the proof that Defendant accessed child pornography prior to the date alleged in the bill of information may be considered in evaluating the sufficiency of the evidence. After the State rested its case, defense counsel moved for a judgment of acquittal, arguing that the State failed to present any evidence that Defendant intentionally possessed child pornography between the dates set forth in the bill of information. Because the only evidence of peer sharing was between the dates of October 2009, and June 7, 2010, defense counsel argued that the State offered no proof that anything was placed on the Defendant's computer between June 23, 2010 and September 9, 2010, the dates listed in the bill of information. The trial court, however, denied the motion for acquittal, finding that the State was not bound to the exact dates alleged in the bill of information.

Considering the jurisprudence, the lack of any allegation of prejudice, and the lack of any argument on appeal regarding this issue, we find the trial court did not err in denying the motion for acquittal. Accordingly, the trial court properly considered evidence that showed Defendant accessed child pornography before the dates alleged in the bill of information. Considering the file list showing the pornographic files accessed by Defendant and Defendant's own admission that he searched for and viewed child pornography, we find the evidence was sufficient to prove Defendant "visually reproduced" images of child pornography in violation of La.R.S. 14:81.1(A)(1), the definition in effect until August 14, 2010.

Although the evidence was sufficient to convict Defendant using the pre-amendment definition of child pornography, we will discuss the sufficiency of the evidence under the post-amendment definition which was also in effect during the dates charged in the bill of information. Effective August 15, 2010, the legislature

amended La.R.S. 14:81.1. 2010 La. Acts No. 516, § 1 and La.Const. art. 3, § 19. As of that date, La.R.S. 14:81.1 provided in pertinent part:

> A. (1) It shall be unlawful for a person to produce, distribute, possess, or possess with the intent to distribute pornography involving juveniles.[5]

Although the "visual reproduction" element was eliminated from the amended version, both the pre-amendment and post-amendment version list possession as an element of child pornography.[6] In *State v. Wright*, 45,980, p. 7 (La.App. 2 Cir. 1/26/11), 57 So.3d 465, 470, *writ denied*, 11-421 (La. 9/2/11), 68 So.3d 520, the second circuit stated the following regarding the standard for determining whether possession of child pornography has been proven:

> Pornography involving juveniles is a general intent crime. See *State v. Cinel*, 94-0942 (La. 11/30/94), 646 So.2d 309, *cert. denied*, 516 U.S. 881, 116 S.Ct. 215, 133 L.Ed.2d 146 (1995). General criminal intent is present when the circumstances indicate that the offender, in the ordinary course of human experience, must have adverted the prescribed criminal consequences as reasonably certain to result from his act or failure to act. La.R.S. 14:10(2). The words "intentional possession," taken in their usual sense, mean that the individual knowingly and voluntarily possessed the pornography, in contrast to circumstances in which a person downloads images from the internet without realizing that some images included in the download were child pornography. *State v. Horton*, 42,199 (La.App. 2d Cir. 06/20/07), 962 So.2d 459, 466, *writ denied*, 07-1819 (La. 01/25/08), 973 So.2d 755.

---

[5]The definition was again amended by 2012 La. Acts. No. 446, § 1.

[6] The pre-amendment version proscribes the "intentional possession" of child pornography while the post-amendment version proscribes possession without specifying "intentional." In *State v. Cinel*, 94-942, p.6 (La. 11/30/94), 646 So.2d 309, 314, *cert. denied*, 516 U.S. 881, 116 S.Ct. 215 (1995), the supreme court stated that it has "frequently interpreted statutes which on their face are silent as to any requirement of intent or scienter, to impose in fact a requirement of intent . . . ." Citing La.R.S. 14:11, the court further stated that absent qualifying terms, the terms "intent" and "intentional" refer to general criminal intent. *Id.* We note that La.R.S. 14:95.1, possession of a firearm by a convicted felon, similarly proscribes possession as an element without specifying that the possession be intentional. The supreme court has stated that La.R.S. 14:95.1 is a general intent crime. *State v. Godeaux*, 378 So.2d 941 (La.1979). Accordingly, even though the post-amendment version of La.R.S. 14:81.1 does not specify that the possession is intentional, the possession must be committed with general intent.

In *Wright*, the pornographic images were actually saved to two different floppy disks found in the defendant's office. Thus, the defendant's access to the child pornography images was clearer than the present Defendant's access to the pornographic images found on his hard drive. However, Defendant's own admission makes it clear that he purposefully sought out child pornography rather than retrieving it accidentally.

In *State v. Svehla*, 06-397, (La.App. 1 Cir. 12/28/06) (unpublished opinion), *writ denied*, 07-285 (La. 5/4/07), 956 So.2d 607,[7] the first circuit addressed whether there was sufficient evidence of pornography involving juveniles when the defendant argued that there was no proof that he knew child pornography was contained on discs found in his room. The defendant asserted that even though some of the discs were labeled "porn," it is not illegal to possess pornography involving adults. The first circuit found that the "critical evidence" of the defendant's "intent and/or knowledge of the existence of the pornography was defendant's own statement to police." *Id.* When confronted by police that he was being charged with a probation violation for possessing child pornography, the defendant responded that he was not aware that such material was illegal. He told the officers "that if he had known that the material was illegal, he would have discarded it." *Id.* The first circuit concluded, "While this statement by defendant claims lack of knowledge of the illegality of the child pornographic material, it clearly evinces defendant's knowledge that the material was in fact contained on the discs." *Id.*

In the present case, Defendant admitted to police that he searched for child pornography, downloaded child pornography, viewed the child pornography, and

[7]This case is cited at 2006 WL 3804628.

that he either deleted the images himself or had his computer set up to delete them. At the end of this statement, Defendant specifically stated that he was not guilty of looking at the images for any "stupid" reason. Thus, Defendant's statement clearly shows that he knew the images that he was searching for, downloading, viewing, and deleting were child pornography. His retrieval of such images was not accidental. Unlike *Svehla*, however, Defendant believed he had deleted the images.

In *State v. Longo*, 08-405 (La.App. 5 Cir. 1/27/09), 8 So.3d 666, the fifth circuit addressed the sufficiency of the evidence where twenty-five images of child pornography were found on the defendant's computer in a Yahoo Messenger account under the user name "Mounted 42." Longo told a detective that he "recognized" some of the images but denied purposely downloading or keeping the images. Finding the evidence was sufficient, the fifth circuit stated the following:

> Longo's recorded statement shows that he was aware of the images under investigation at that point and that he had not deleted them.
>
> In addition to the images themselves, there was evidence of Longo's participation in several lascivious internet chat rooms. The texts of the chats under Longo's user name, "Mounted 42," revealed several references to the swapping of pictures involving juveniles. This evidence, coupled with the discovery of twenty-five different child pornography images with different creation, modification, and access dates spanning over several months was sufficient for a rational trier of fact to conclude Longo did not accidentally download the child pornography but, rather, that he intentionally possessed the images.

Id. at 670-71.

Like the defendants in the above cases, it is clear that Defendant did not accidentally download the child pornography images. However, unlike the images in the above cases, the images in the present case were found on an area of

Defendant's computer hard drive that was not accessible without using special equipment or software.

Although we have found no Louisiana cases involving possession of pornography found solely on a hard drive, there are numerous federal cases addressing similar factual scenarios. In *United States v. Moreland*, 665 F.3d 137, 152-53 (5th Cir. 2011), the Fifth Circuit set forth the following summary of federal cases dealing with possession of child pornography when the images are found in the hard drive of the defendant's computer:

> The proof deficiency here is underscored by a comparison with other federal courts of appeals' decisions holding that, even when the defendant has exclusive possession of his computer, evidence of storage of child pornography images in the hard drive of a defendant's computer, without more, is insufficient to sustain a conviction or sentence for knowing possession or receipt of child pornography; and that in exclusive possession cases in which convictions have been upheld, the government has presented additional evidence of the defendant's knowledge, access and control of the child pornographic images.
>
> In *United States v. Dobbs*, 629 F.3d 1199 (10th Cir. 2011), the Tenth Circuit concluded that Dobbs' conviction for receipt and attempted receipt of internet child pornography must be reversed because the evidence was insufficient to support the jury's finding of guilt. *Id.* at 1209. The prosecution proved only that two child pornography images were found in the cache of Dobb's computer. *Id.* at 1202. The court found that this evidence was insufficient to support Dobbs' conviction because the prosecution failed to demonstrate that Dobbs knew about his computer's automatic caching function, had seen the images, or had any ability to exercise control over them. *Id.* at 1205, 1207. Therefore, the Tenth Circuit determined that while a jury could conclude from that evidence that Dobbs – or at least his computer – received the images, no reasonable jury could find that he knowingly received the images.
>
> In *Dobbs*, the court specifically rejected the prosecution's argument that proof of Mr. Dobb's pattern of seeking out and downloading internet child pornography was sufficient circumstantial evidence to support Dobb's conviction, because the prosecution could not show that Dobbs conducted a search for child pornography or visited child pornography websites "immediately prior to the creation of those two images in the cache." *Id.* at 1204. Therefore, proof of

> illegal searches was still insufficient where those searches could not be linked to the pornographic images for the which the defendant had been indicted.

Dobbs dealt with the offense of knowingly receiving and attempting to receive child pornography in violation of 18 U.S.C. § 2252(a)(2). Thus, unlike the present case, the conduct being punished in *Dobbs* was the intentional *receipt* rather than the intentional *possession* of the pornography.

The Fifth Circuit continued its summary as follows:

> The Ninth Circuit also has demanded more than the mere presence of child pornography images in a computer's hard drive to prove knowing possession, when those images are found in an area of the computer that non-expert users do not know about or cannot access. In *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006), the defendant appealed his sentence because the court had taken into account additional images recovered on his computer after he pleaded guilty to receiving and possessing different child pornography images. *Id.* at 857. The court vacated his sentence because the additional images were found in the cache and the prosecution had offered no evidence to show that Kuchinski was a "sophisticated" computer user, had ever tried to access the cache, or "even knew of [its] existence." *Id.* at 862. The court therefore found that "[w]here a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of domination and control over the images. To do so turns abysmal ignorance into knowledge and a less than valedunarian [sic] grasp into dominion and control." *Id.* at 863.
>
> Cases in which we and other circuits have upheld convictions for possession of digital images of child pornography are as telling as the cases in which the convictions were overturned. Affirmation of convictions have been based on substantially more evidence than a defendant's mere ownership and custody of the computer. In fact, the evidence introduced in those cases tended, independently of ownership or custody of the computer, to prove the defendant's knowledge and possession of the unlawful images or material concealed in the computer's hard drive. When the images are stored in inaccessible areas of a hard drive or could have been downloaded and retained by a computer's automatic processes without the computer owner's knowledge – such as temporary internet files or, as here, in the computer's disk slack space – courts have treated as determinative whether the defendant had sufficiently expert computer

knowledge to know about and access those files or whether there were independent facts that showed the defendant's knowledge and dominion of child pornography images on the computer.

For example, in *United States v. Winkler*, 639 F.3d 692 (5th Cir. 2011), this court upheld a defendant's conviction for receipt and possession of child pornography because the government had produced sufficient evidence that "Winkler himself sought out, downloaded, viewed and had the ability to manipulate the images at issue in this case." *Id.* at 699. The prosecution produced evidence that illicit videos on Winkler's computer were "hidden … behind password walls in his … user account" or in "unnatural locations in the computer's file hierarchy rather than the normal location for downloaded material." *Id.* It also provided evidence that Winkler paid for members-only access to a child pornography site and transmitted videos from this site to his computer. *Id.*

Similarly in *United States v. Tucker*, 305 F.3d 1193 (10th Cir. 2002), the Tenth Circuit upheld a defendant's conviction for possession of child pornography in part because the prosecution presented evidence that Tucker admitted to the police that he viewed several thousand images of child pornography and that he intentionally deleted his computer's cache after viewing the images. *Id.* at 1197, 1204. The government also showed that Tucker paid a user fee to access newsgroups that gave him access to images of child pornography, and that he possessed the technical ability to access and manipulate the images stored in the cache. *United States v. Tucker*, 150 F.Supp.2d 1263, 1265, 1269 (D.Utah 2001), *aff'd*, 305 F.3d 1193 (10th Cir. 2002).

In *United States v. Sanchez*, 59 M.J. 566, 570 (A.F.Ct.Crim.App.2003), *aff'd in part, rev'd in part on other grounds,* 60 M.J. 329 (C.A.A.F. 2004), the U.S. Air Force Court of Criminal Appeals upheld a conviction for child pornography possession based on files located in a computer cache and on other files that had been deleted from the hard drive but were recoverable. In that case, the prosecution had presented evidence that the defendant was a subscriber of "numerous e-groups described as nude teen sites," that the child pornography images came through emails to an account to which only he had access, and that the defendant was "relatively sophisticated" in computer matters, such that a jury could find that he knew that the images were being downloaded. *See id.* at 570.

These cases show that courts have refused to find that a defendant constructively possessed child pornography located on his computer without additional evidence of the defendant's knowledge and dominion or control of the images.

Id. at 153-54.

This is not a case where the only evidence submitted was the presence of child pornography images on Defendant's hard drive. The State submitted evidence of Defendant's purposeful search of the pornographic images. Defendant admitted to using LimeWire to download pornography. Defendant also admitted to using search terms specifically designed to retrieve child pornography and specifically described videos he watched involving child pornography. According to Trooper Fournier, the terms used by Defendant were known child pornographic search terms. State's Exhibit Number One included pages of pornographic files retrieved by Defendant's I.P. address. In Defendant's statement to police, he stated that he deleted child pornography files after he viewed them, and explained that he tried to set up his computer to erase everything. Trooper Parker explained that the files were on Defendant's computer at one time but had been deleted.

There was no evidence, however, that Defendant knew the images remained on his computer after he deleted them or that he knew how to access those images. Considering the ample evidence that Defendant's retrieval of numerous images of child pornography was no accident, the evidence that the images were viewed on the Defendant's computer at one time, and the evidence that Defendant either manually deleted the images or set up his computer to automatically delete the images, this court finds the evidence was sufficient to prove Defendant intentionally possessed the images. Regardless, however, of the sufficiency of the evidence as to intentional possession, the evidence was sufficient to prove that Defendant "visually reproduced" the child pornographic images as defined in the pre-amendment version of La.R.S. 14:81.1(A)(1).

For the foregoing reasons, these assignments ultimately lack merit.

SEX-OFFENDER REGISTRATION NOTIFICATION

In assignment of error number one, Defendant asserts that he was not informed of the sex-offender notification and registration requirements as required by La.R.S. 15:543. Thus, Defendant requests a remand so that appropriate written notice can be given to him.

The offense of pornography involving juveniles is a sex offense for which Defendant is required to register as a sex offender. La.R.S. 15:541(24) and La.R.S. 15:542. Pursuant to La.R.S. 15:543(A), "The court shall provide written notification to any person convicted of a sex offense and a criminal offense against a victim who is a minor of the registration requirements and the notification requirements[.]" The notice must be included "on any guilty plea forms and judgment and sentence forms provided to the defendant, and an entry shall be made in the court minutes stating that the written notification was provided to such offenders." La.R.S. 15:543(A).

Defendant was notified by written notification of the sex-offender registration requirements when he originally pled no contest. Defendant was not notified again, however, when he was sentenced after his conviction. Additionally, the sentencing minutes following his conviction do not indicate that Defendant was again notified of the registration requirements. Defendant requests a remand even though he "has already registered in an effort to avoid being arrested for a bench warrant that was issued charging Mr. Cooley with failure to register."

Although this court has addressed whether the failure to notify a defendant of the registration requirements vitiates the voluntariness of a guilty plea, we have found no cases in which this court recognized an error as to the trial court's failure to advise the defendant of the sex-offender notification requirements at sentencing.

Both the fifth and second circuits have recognized as error patent the trial court's failure to advise the defendant of his registration requirements and have remanded cases to the trial court for the appropriate notice to be given. *State v. Trice*, 14-636 (La.App. 5 Cir. 12/16/14), ___ So.3d ___[8]; and *State v. Morning*, 49,300 (La.App. 2 Cir. 10/1/14), 149 So.3d 925.

Since Defendant has already been informed of the sex-offender registration requirement, has already registered as a sex offender, and fails to cite any authority requiring remand, remand is not necessary in this case. We note that the time period of which Defendant was notified that he must register (twenty-five years) has not changed since Defendant's written notification.

For the foregoing reasons, this assignment of error lacks merit.

DECREE

Defendant's conviction and sentence are affirmed. The trial court shall conduct an evidentiary hearing within thirty days of the date of this opinion to determine whether Defendant knowingly and intelligently waived his right to trial by jury. The trial court is further ordered to prepare and lodge an appellate record with this court that contains the transcript of the above-referenced evidentiary hearing within ten days of the hearing. Once that record is lodged with this court, the State and Defendant will be given the opportunity to file briefs should either party wish to raise any issue arising from the hearing.

CONVICTION AND SENTENCE AFFIRMED; REMANDED.

[8]This case is cited at 2014 WL 7185265.