

Guide to Child Pornography Cases – Larry E. Daniel, EnCE, DFCP, BCE, ACE

Copyright 2012 by Larry E. Daniel, All Rights Reserved. Any copying or distribution of this document in any form is prohibited without express permission by the author.

There are common issues with child pornography cases that can be dealt with to make the case go more smoothly for you and your client.

Contraband cases are unique in the sense that they are covered by the Adam Walsh Child Safety and Protection Act of 2006. Because of this federal law, barriers are in place to prevent actions that would result in the distribution of the materials to defense attorneys and defense experts.

It is important to know that cases involving child pornography are more complicated than whether or not a file simply exists on a hard drive. The case must be fully developed to show not only how the investigation leading to the search and arrest was performed, but also to show exactly what the accused knew or did not know about the file(s) that are charged.

Overview of Child Pornography Cases:

While the evidence in many of these cases may seem overwhelmingly affirmative for the prosecution, that is not always the case. The issue always comes down to the details of how the evidence was gathered and examined. In some cases, the prosecution will only provide you with a list of charged images and little or no other discovery materials.

One of the most critical pieces of information you and your expert needs is the computer forensics report from the prosecution's expert. The reason is this report is the basis for supporting any charged images against your client and is what the prosecution's expert will testify to in the event the case goes to court.

What the prosecution expert's report should contain:

1. The name of the examiner and a short statement of their qualifications.
2. The name, original location and time stamps for any charged files.
3. A short description of the steps the examiner took in the process of making the forensic copies, protecting the evidence and the processes used to recover any contraband material.
4. Information about each device that was examined by the forensic examiner.
5. Information about any user accounts on the computers.
6. Additional information about email, chat logs, internet history and other data, as appropriate to the case.

In a recent case the prosecution charged the client with several counts of possession of child pornography. However, the defense received only a list of file names of charged images without any information as to the original location and time stamps for the files. When the forensic report was requested by the defense, the prosecution could not supply the report. As it happened, the examination was performed by an FBI examiner in support of the local law enforcement agency. The FBI failed to provide the report to the local law enforcement agency or to the state prosecutor. When it was made clear to the prosecutor that without the report, they could not prove from what computer or location the images were collected, nor could they attach the images to any particular person in the household, the client was offered a plea bargain.

The result of this case was the prosecution offered a plea of two misdemeanor counts of contributing to the delinquency of a minor with a 12 month

suspended sentence and all the felony charges were dropped. No sex offender registration.

Another recent case involved charges against an elderly client for possession of child pornography. In this case, the client was legally blind and was also using a particular file sharing program that allowed for the bulk downloading of files from the file sharing network Gnutella.

Upon examination of his computer, he had over 9,000 adult pornography files. In contrasting this to the three contraband files found on his computer, it was apparent that he did not intend to download the files. In addition, the files downloaded did not have file names indicative of child pornography, and there was evidence that he had never viewed the files.

On the morning the case was going to be tried, the prosecutor reviewed the forensic report provided by the defense and dropped all charges against our client.

Included here is the forensic report in this case, with the names redacted:

Computer Forensics Report

Date: 6/16/2011

Prepared By: Larry E. Daniel, EnCE, DFCP, BCE

Prepared For: (Redacted)

Case Name: (Redacted)

I completed a forensic examination of the subject hard drives at the (redacted) police department during multiple visits in February and March of 2011 in the presence of (Redacted) Police department Forensic Examiner (redacted).

During my examination of the subject hard drives, I noted that the hard drives contained hundreds of adult pornography files.

I also noted that the file sharing program Shareaza was installed on the hard drive. The file sharing program Shareaza allows for the user to select all of the files returned by a keyword search at once and mass download them. This can cause a user to download files that they may not know the content of due to the ability to select all and download them at once.

Attached to this report is the installation screen shots and configuration pages of the Shareaza program showing that the program issues no warnings during installation that files will be shared from the user's computer. The screen shots also show that there is no

place that indicates that file sharing can be turned off. The only screen where file sharing can be modified does not indicate that it is for that purpose.

Based on my analysis of the contents of the subject hard drives I examined, there were over 9,000 adult pornography files present on the 300 GB SATA hard drive alone.

Additionally, the computer used to download files was not capable of playing an AVI format movie file. In order to play a file of this type, the file would have to first be converted to the .WMV format.

The two charged movie files were both in .AVI format, indicating that they could not be viewed without first converting them.

Only one of the two charged files was ever converted: Virgin Sex After School (Debut 12 yo) – Minori Aoi – Japan Sexy Doll Creampie (Sperm inside) (Bestpart 5m55S)_WMV V9.wmv.

However, the date and time stamps of the converted file indicate that the file was never viewed after conversion due to the fact that the last modified time was later than the last accessed time. When a file is converted, the last modified time for the file is the time that the conversion completed. If the file were opened after that time for viewing, the last accessed time would be later than the last modified time. The last accessed time for the file is five minutes and 28 seconds prior to the last modified time.

The file name contains the term “sex” which would include the file in any search results for that term. This indicates that the file would have appeared in searches for adult pornography and was most likely downloaded as the result of a “select all” and download operation of adult pornography files.

The other charged movie file, Pthc – Thee Classic Movies Two Lesbian Scenes (*yo Girl) Plus Indian Girls with Man.avi was never converted into a format that could be viewed on the computer.

Also, the file name contains the term lesbian, which was a common term in the adult pornography files downloaded on the computer indicating that the file appeared as the result of a search for adult pornography and was most likely downloaded during a “select all” download operation of adult pornography files.

The final three charged files all came from an area of the hard drive that was inaccessible to the user. The original file names are lost due to the fact that the files themselves were not present on the hard drive outside of in thumbnail form inside of two thumbnail database files. Thumbnail database files are files that contain small thumbnail images of files that were present on the hard drive at some point in the past, but are not an indication that the files were ever viewed by the computer user. They only indicate that the files may have appeared in thumbnail form at one time on the computer.

The created, modified and last accessed times for the files recovered from the thumbnail database files are not the dates and times for the images, but are the dates and times for the thumbnail databases. There is no way to determine the exact creation or last accessed dates for files recovered from inside a thumbnails database file.

Due to the fact that the hard drives contained thousands of adult pornography files, that the Shareaza program allows for selecting multiple files at once for download and that the number of images located that contain contraband are less than 1 percent of the downloaded file content, it is most likely that any such files were downloaded without the user's direct knowledge of their content while downloading legal adult pornography.

END OF REPORT

In a case in Alabama, the client was charged with possession and distribution of child pornography based on LimeWire activity on his computer. Upon examination of the computer, it was found that the files were all downloaded during a period of four days prior to the computer being turned over to the local Sheriff's department. Also, the files were under a user account that the client did not have a password to access. It was also determined that the computer was in the possession of the client's girlfriend's ex-husband at the time the downloading occurred. Finally, the time stamps on the files showed that they were all accessed on the day that the computer was given to the local Sheriff's department indicating that the files were viewed by either the ex-husband or by the law enforcement officers without any method for protecting the integrity of the evidence. The result of this case was a misdemeanor plea for criminal misuse of a computer by our client. All of the felony child pornography charges were dropped.

We receive questions in nearly every case along the lines of the following;

1. What would be the charge for doing such a forensic examination?

The amount of time it takes to perform a child pornography examination varies by the amount of evidence that must be examined, the number and type of charges and the type of evidence to be examined.

The primary driver for high costs in child pornography cases is the Adam Walsh Child Safety and Protection Act of 2006. This act requires that the evidence be kept in the custody of law enforcement at all times.

This means that you will not receive a copy of the evidence for review at your office or at your expert's office. Because the expert must work at the law enforcement location, he cannot work on anything else during the examination. This means that all hours spent by the forensics software in processing the evidence for examination, in most cases, will have to be billed as examiner hours.

While some states and local jurisdictions have allowed this to occur via protective orders, the risk of holding contraband materials, even with a protective order is probably greater than the benefit. In any case, if your expert is not located in that particular area that allows for the protective order, then the protective order is not going to allow you to transport or send contraband materials to the expert's location. And, even if you can get such a protective order, most qualified experts would still refuse to be in possession of the contraband due to the risk to them.

The only way to get a reasonable idea of what it will cost to perform the forensic examination in a child pornography case is to provide to the expert as much up front information as possible prior to getting them to give you an estimate. The source of some of this information is covered in the discovery information in this document, in the "First Round of Discovery" section of this guide.

At a minimum, the expert needs to know the number and size of any computer hard drives that were examined as this will determine the amount of processing time for the case. This information should be available in the law enforcement computer forensics report, or in the warrant return inventories of what was seized.

The expert will also need to know some details about the case itself, such as how the case developed; is it from a file sharing investigation, was the person reported to the police by a concerned citizen, is it extant to another charge where the computers or cell phones, cameras, etc., were seized as part of another investigation?

In some cases, all you and the expert receive are a list of chargeable images, with no information as to their origination. This can make the examination considerably more expensive if your expert has to go and find those images or movies among hundreds and thousands of images that may be contained on the evidence media.

This is why it is so important to get a copy of the forensic examination report from law enforcement prior to getting an estimate from the expert, and it is especially important to have prior to the expert performing the examination. The reason is that law enforcement may have seized multiple computers and hard drives. However, the contraband may have only been recovered from part of the seized evidence. While you want your expert to have the option to review all of that evidence if he or she deems it necessary, in many cases, the expert does not need to fully examine hard drives that do not contain contraband according to the law enforcement forensic examination report. This can save a considerable amount of time and money if the expert knows which items of evidence that law enforcement examined that do not contain contraband and therefore can avoid having to spend time processing and examining that evidence.

2. How do you work the logistics of doing the examination as far as getting access to the computer?

Your expert will not need access to the actual computer to do his forensic examination. When any expert needs to examine evidence, the first step is to make a forensically sound copy of the original evidence. No one should ever examine original evidence without first making a forensic copy. The exception is to perform

a forensics “preview” which can be done without modifying the original evidence. It is up to the law enforcement agency examiner to create forensically sound copies of the original evidence and these can be made available via the discovery process.

Once the agency examiner makes the forensic copies of the evidence that he or she will be working on during their examination, copies of those copies should be made available for use by your expert during the examination.

While different agencies use different tools to perform their forensic copying and examinations, the standard “format” for the forensic copies is called EnCase, .E01 or Expert Witness format. All of those refer to the same type of forensic file copy format. A copy of the original evidence in this type of forensic format is an exact copy of the original evidence and is all that your expert will need to perform their examination.

If cell phones are involved, and if the originating agency was able to perform a forensic examination of the phone using one of the cell phone forensic tools for that purpose, then copies of the phone extraction files should be made available to your expert for examination using their phone forensic tools. If the agency does not use the same tools as your expert, then you can ask that the phone be made available for examination by your expert using his phone forensic tools. This is more difficult to have happen since they are now putting original evidence in the hands of your expert, but in the event that a phone is part of the evidence, the defense has a right to perform an examination of the phone, the same way the defense would have a right to test DNA samples and so on.

If you can get the prosecution and or law enforcement agency to assist with transferring the evidence copies to be reviewed to a host law enforcement agency close to the examiner, you can save time and money both for travel costs and on-site costs. Plus, it gives the examiner the option to go back and review the evidence again at a later time if needed. For instance, if the case is a federal case, it could be

possible to have the evidence copies transferred to a FBI office that may be local to your expert. If a local FBI office is not available, don't overlook using offices for other federal agencies to host the examination such as the Secret Service, Postal Inspectors and Homeland Security offices.

Even if your case is under local or state jurisdiction there is a possibility that the forensic examination was performed by the FBI, ICE (Homeland Security) or the Secret Service as part of their assistance to local law enforcement. That can open the door to having the evidence copies transferred to one of those agency offices to host your expert's examination. Your expert may have contacts at the local, state and federal agencies and may be able to assist you with finding a host law enforcement agency that will allow the evidence copies to be sent to their location for examination by your expert.

If you cannot get the evidence transferred to a location local to your expert, then you will incur travel expenses to the location where the examination will take place.

3. How long would the examination take to be completed?

This is always the most difficult question to answer up front. The more information your expert has up front, the more accurate the estimate can be. Some exams only take a few hours and some can take days. For instance, a single charge of possession on a hard drive may only take a few hours to do the examination, if information is available up front from the prosecution as to the location of the image.

However in a case where there are multiple hard drives that are terabytes in size, examinations take a lot of time. To simply process a terabyte of data can take up to two days before the examiner can start the analysis. This is time that your expert will have to spend sitting around while the machine processes the evidence.

Anything that can be done to limit the amount of evidence to be processed can be a real time and money saver.

The size and amount of evidence to be processed is only one factor that determines how long an examination may take. The complexity of the case is another factor; cases involving other sources of evidence that may be a factor in the case such as chat messages, email, message boards, instant messaging, peer to peer file sharing and so on, can impact the amount of time that it takes to examine the evidence and also the amount of time it takes to analyze the evidence once it is processed.

When an expert performs an examination in a contraband case, he or she is limited in both time and in the ability to conserve derivative evidence for the analysis stage. In other words, your expert will be looking for evidence not only about the charged files but also about the case in general. In many cases this can involve collecting file listings with date and times, machine configuration information, peer to peer file sharing configuration, user information, chat logs, emails, internet history, and manually making notes about images the examiner views during the examination. All of this information becomes the basis for the analysis performed by your expert.

Analysis

Analysis is normally done after the examination of the evidence on site. The results of the analysis will then be put into a case assessment for you and your client to review that is not a forensic report or an opinion by your expert. It is a document that simply recaps the evidence examined by the expert and the information they gathered along with an assessment of how that evidence aligns with the case and should contain the following header language:

Case Assessment – CONFIDENTIAL ATTORNEY WORK PRODUCT

Overview:

This is a case assessment and not a forensic report. This is for the use of the attorney only in discussing the evidence related to this case with this expert and persons the attorney selects for inclusion in discussing this report. This is neither an opinion nor a fact statement by this expert and is not intended for any use other than to present information to the attorney and his client.

Overall the process of performing the examination and doing the post analysis for the case assessment can take several weeks based on scheduling time at the law enforcement agency to perform the exam, the availability of your expert and the time it takes to write the assessment post examination. It is always best to get an expert involved early in your case to avoid potential issues with hearing and trial dates. Since the expert will have to schedule their exam at the convenience of the hosting law enforcement agency, this can impact the schedule of when the examiner can perform the work.

Discovery and Getting Access to the Evidence

Having worked as defense experts on many contraband cases, we have found that the discovery process should happen in two steps in order for the defense expert to have as much information as possible to help you and your client. Here are the items that you and the expert need to begin the process of analyzing the case, and should be included in any initial discovery request from the prosecution, with special care to ask for the forensic reports in a redacted form. This allows the expert to get a good idea of the merits of the case prior to performing an examination of the evidence. It will also help the expert to prepare for the on-site examination so that the expense and time can be kept to a reasonable amount.

The First Round of Discovery

1. A copy of all police reports, witness statements, defendant statements, and any audio or video recordings made by police or other parties.

2. A copy of any computer forensic report completed by law enforcement experts with any contraband images redacted in accordance with the Adam Walsh Child Protection and Safety Act of 2006.
3. A copy of all search warrant affidavits, search warrant returns, item inventories, chain of custody reports, case reports and field notes made by police.
4. A copy of any records obtained in the course of the investigation including but not limited to criminal histories, phone records, internet service provider records, or other third party records.
5. A copy of the resume or curriculum vitae of any prosecution or police expert, who acquired, collected, copied or examined any form of evidence.
6. A copy of any screen shots, photographs or other images created by police during the course of the investigation. If such screen shots or other images contain contraband, the contraband images are to be redacted in accordance with the Adam Walsh Child Protection and Safety Act of 2006.
7. A copy of any subpoenas issued by police to third parties.

The Second Round of Discovery

The second step in a contraband case involves getting access to the evidence for examination by the defense expert. For this purpose we have provided the following language for use in cases in as a method for setting up the ground rules for the expert to perform an examination of the evidence containing contraband.

We will provide this language in electronic format for inclusion by the attorney in their motion or order.

Example Language for Motions and Orders

ACCESS TO FORENSIC EVIDENCE

The Defendant moved the Court to compel the _____ to provide to the Defendant access to the physical evidence seized by the prosecution in the course of its investigation. The Court considered this motion and arguments of counsel and for good cause shown allows the Defendant's motion under the following conditions:

1. The defense expert will supply in advance, an external hard drive, factory new, if required, by the law enforcement agency, for the purpose of providing forensic copies of the evidence to be examined during the defense expert's forensic examination at the law enforcement agency.
2. The law enforcement agency shall copy to the provided hard drive any FTK, Encase or other type of forensic image files that are an exact copy of the hard drive(s), CD-ROM or DVD-ROM media, flash cards, floppy disks, smart media cards or any other digital evidence seized and copied by law enforcement.
3. The law enforcement agency shall provide to the defense expert an un-redacted copy of any computer forensic reports for the use of the defense expert while performing the forensic examination. Such un-redacted reports shall be returned to the law enforcement agent at the end of each day's examination period.
4. The law enforcement agency shall have available for inspection by the defense expert copies of any derivative evidence created and supplied to the prosecution, including but not limited to media created for the purpose of prosecution review, submission to the National Center for Missing and Exploited Children, or for the use by other law enforcement parties to the investigation of the charges, pending or otherwise.
5. The expert will perform all of his work on the provided hard drive, using at his option; either his own forensic analysis equipment and software or forensic analysis equipment provided by the law enforcement agency, provided that the software and hardware provided by the law enforcement agency is equivalent to a full copy of EnCase 6.XX forensic software and that the expert may install other forensic analysis software on the provided computer for the purpose of performing his examination.

6. At the end of the forensic examination session, the examination hard drive will be sealed in the presence of the defense expert and given to the law enforcement agent and kept in the custody of law enforcement in case further review is needed at a future time.
7. When the expert sets up his case in his forensic analysis software, he will ensure that all temporary files, exports, and any other files that would normally be written out during the analysis will be written to the provided examination hard drive. The expert if required to do so, will show the law enforcement agent the setup of his analysis software for this case to support the above.
8. The law enforcement agency shall make such supervisory arrangements as deemed appropriate in accordance with the law enforcement agencies' policies and procedures for the forensic examination of contraband material by a defense expert.
9. The expert will show to the law enforcement agent any items he wishes to copy or print, to provide to defense counsel as part of his analysis reporting, to ensure that no contraband images are copied or transferred.
10. The expert will be given a minimum window of 6 hours per day, scheduled in advance, to perform the analysis. With further analysis time to be provided if needed at a future date.
11. All items and information discovered by the expert are to be treated as attorney work product, and protected as such even though the law enforcement agent will review said documents and information for the presence of contraband.

In many cases, this has not been required to be put into a motion, but simply shared with the prosecution as a way to clearly communicate who will do what to facilitate the examination of the evidence by the defense expert.

Additional Information about Child Pornography Cases

Child Pornography Forensics Report Example:

The typical law enforcement child pornography forensics report may contain all or part the following;

1. A synopsis of the examination, example:

- a. "The following items submitted for forensic examination in relation to child pornography...The items were received at (location). Photographs of the evidence items are included with this report.

2. Evidence Photos of the seized items.

3. A List of all the items examined in the course of the examination by the forensic examiner.

- a. Details concerning the devices, such as serial number, make and model of the device, and size of the media.

4. Acquisition Process

- a. Showing the verification and acquisition MD5 hash values; will also sometimes list the hardware and software used to perform the forensic acquisition of the evidence items.

5. Information about the Evidence Items of Interest:

a. General Information

- i. The operating system of the computer
- ii. The user accounts on the computer
- iii. The installed software on the computer

b. Case Specific Information

- i. Information about the particular case, such as software of interest that was located. Example: "The Limewire.props file was located at Users\JohnDoe\Preferences\LimeWire.props"
- ii. An examination of the internet history on the computer, which would typically look like a spreadsheet listing of webpages visited, the time they were visited, and searches performed on the internet.
- iii. A List of files that were recovered from unallocated, or "deleted" space on the computer that are of interest. Example: "Four (4) pictures which may be considered child erotica were observed in

- unallocated space on the computer...one (1) movie which may be considered child pornography was observed on the computer...”
- iv. The names, file paths, and dates and times of images or videos which might be considered child pornography should also be listed.
 - v. A list of files that are charged or chargeable , including the original locations of the files, the date and time that the files were created modified and last accessed.
 - vi. Any information that could connect the files downloaded during the online investigation to the actual computer evidence located on the hard drive(s) of the examined computers.

Explanation of Peer to Peer Networking

Peer to Peer File Sharing

The peer to peer file sharing protocol, Gnutella, allows individual computers to form ad hoc networks for the purpose of sharing files. This is done by a computer user installing and then running a Gnutella client application such as LimeWire or FrostWire. The peer to peer client application will then connect to other computers running the same protocol.

Once connected to other computers via the peer to peer network protocol, the computer user can then perform searches for files by keyword. This will return a listing of files for the user to select and download.

Using the peer to peer file sharing networks to search for and download adult pornography poses a great risk to any computer user who is not looking for child pornography. This is because all files on the peer to peer networks have file names that can be created by the person who shares the file. It is very common for a file containing child porn to have a file name that also contains common adult pornography keywords. When a user performs a keyword search in one of the peer to peer file sharing programs, the software will return a list of files containing that keyword. For instance if the keyword is “porn”, this will any file containing that word in the file name.

There is no way for the user to know the contents of a file prior to selecting it for downloading.

Some file sharing programs like FrostWire allow the user to select multiple files for downloading at once. This is called multi-select. The user can click on one file, scroll to the bottom of the listing, hold the shift key down and select the last file and then tell the program to start downloading. When doing this, the user is not required to acknowledge each of the files to be downloaded or to read the individual file names.

Quality	#	License	?	Name	Type
☆☆☆☆				Johnny Cash - Ring of Fire	mp3
☆☆☆☆				Johnny Cash - Folsom Prison Blues	mp3
☆☆☆☆				johnny cash - I Won't Back Down	mp3
☆☆☆☆				Jonny cash - Johnny cash - Fols...	mp3
☆☆☆☆				Laurent Wolf Feat Johnny Cash (...)	mp3
☆☆☆☆				Johnny Cash - Big Bad John	mp3
☆☆☆☆				Johnny Cash & June Carter - It Ai...	mp3
☆☆☆☆				Johnny Cash - Hurt	mp3
☆☆☆☆				Johnny Cash - Ring of Fire	mp3
☆☆☆☆				Johnny Cash & June Carter - Tim...	mp3
☆☆☆☆				Johnny Cash - Ring of Fire	mp3
☆☆☆☆				George Jones & Johnny Cash & ...	mp3
☆☆☆☆				Johnny Cash - I Hurt Myself Toda...	mp3
☆☆☆☆				Johnny Cash - a boy named sue	mp3
☆☆☆☆				Johnny Cash - Ghost Riders In th...	mp3
☆☆☆☆				Johnny Cash - I Walk The Line	mp3
☆☆☆☆				Johnny Cash - Get Rythem	mp3
☆☆☆☆				Johnny Cash - Get Rhythm	mp3
☆☆☆☆				Johnny Cash - The Night They Dr...	mp3





 Download Here
 **Download**
 **Browse Host**
 **Stop Search**

Figure 1 An example of multi selecting files.

Connecting to a Suspect Computer

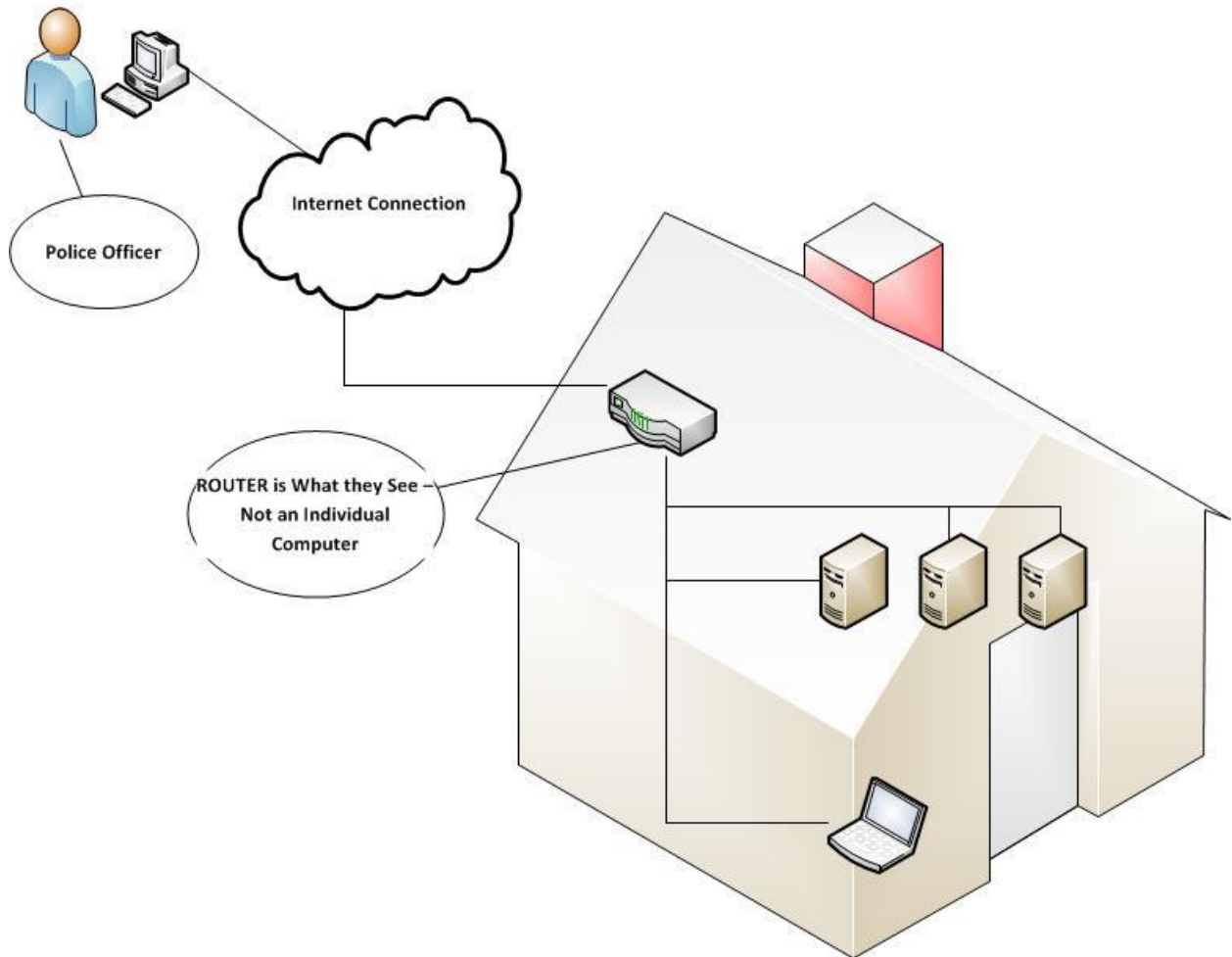


Figure 2 How the police connect to a location using file sharing software.

Downloading Files

One of the characteristics of peer to peer file sharing is that the network of computers providing files for sharing is inherently unreliable. This is because the network is made up of computers that belong to individuals who may shut down their computer at any time, may be having connection problems or may not actually have the file being advertised as available at the time the download is requested.

For these reasons, the peer to peer software will make an attempt to download a file from multiple source computers at once with some or all of the sources failing to provide any part of the file to be downloaded.

This inherent unreliability can frustrate users and encourage them to download lots of files en-mass in order to successfully download files. In many cases, a user will queue up dozens

and even hundreds of files that may take as long as several days to weeks to completely download.

File Searches

Searching for terms using file sharing software such as LimeWire or FrostWire will return file names that contain those keywords in the name of the file. Filenames on the peer to peer network are created by the user who is sharing the file and it is common for files to contain up to a dozen keywords in the file name.

File Names

It is well known in the forensic community that file names ***do not accurately represent*** the content of files available for downloading from the peer to peer file sharing network. It is also well known in the forensic community that files that contain adult pornography may contain keywords in the file name that are suggestive of child pornography. By the same token, files that contain child pornography will in many cases contain keywords that are either generic, such as girl, or sex, or will contain keywords that are suggestive of adult pornography such as anal, hardcore, bondage, bj, handjob, oral and so forth.

Hash Values

While law enforcement investigative tools such as GnuWatch use the hash values of known child pornography files to attempt to locate contraband files on the peer to peer file sharing network, these hash values are not something that a user would have the ability to use to determine if a file that is listed as a result of a search for adult pornography is instead, child pornography.

Law enforcement uses two types of tools designed for the purpose of scanning the gnutella network for child pornography files. One that uses known hash values and one that scans for keywords.

Child Pornography Keywords

While forensic examiners who work child pornography cases are familiar with search terms related specifically to child pornography files such as PTHC, Hussyfan, R@ygold, Lolita, PTSC and so on, these terms would not by default be something a computer user would know about. Seeing such terms in a file name would not necessarily trigger a warning or confirmation for a computer user who is not familiar with such terminology, that such a file may contain child pornography.

Nor are the presence of these keywords a guarantee that the file contains child pornography.

Peer to Peer File Sharing Keyword Searches

The search methodology employed by LimeWire to locate files based on a keyword search is based on a “contains” type of search. In other words, if the file name contains “porn” it

would return files with the words porn, childporn, kidporn, animalporn, porno, pornography and so on.

Peer to Peer File Sharing Applications

The purpose of peer to peer file sharing applications is to share files. Because of this, the default installation of these programs will set the computer to automatically share files. The majority of computer users will accept the default settings for the program installation, allowing the program to share their files.

These applications will automatically share files from the user's computer and are set by default to automatically share files that are in the process of being downloaded that reside in the USER\Incomplete folder. These programs will also default to sharing any files in the USER\Shared folder and in the USER\Saved folder.

In some cases, it is impossible to turn off file sharing, depending on the file sharing application installed on the computer.

Date and Time Stamps for Files Downloaded with Peer to Peer File Sharing Programs

The date and time stamps for files placed on a hard drive from peer to peer file sharing application reflect important information about the downloading process of files, movement of files to new locations, or editing of files on a computer.

However, these date and times are also governed by the operating system of the computer. Windows Vista, 7 and 8 handle date and time stamps differently from Windows XP.

The MAC OS and Linux also treat file dates and times differently.

File Names Created by Peer to Peer File Sharing Programs

When a file is in the process of being downloaded and is still located in the "Incomplete" folder, the file name may be preceded by a "T-". When the file download completes, the file is automatically moved to the user/Shared folder and the "T-" is removed from the file name.

However, this is depending on the file sharing application, as different versions of the same application or different applications may or may not use this type of file naming convention for files in the process of downloading.

If at any time during the downloading process the file is previewed by the user, a copy of the file may be created in the "Incomplete" folder and it preceded by a "P-" or "Preview", to indicate it is a preview file.

Again, this is depending on the version of the application and the application itself.

File Trading Software

Another application used to share child pornography is GigaTribe. GigaTribe is different from peer to peer file sharing programs as it is based on sharing with friends.

The only people who can see and access shared files on GigaTribe are the people in the person's friend list. These people have to be added by the user, which is an affirmative, manual step.

The FBI will assume the identity of persons they arrest sharing child pornography via GigaTribe and then use that person's friends list to develop new cases.

Bear in mind that when a user is accessing the files of one of their friends using GigaTribe, the user can view the files in "thumbnail" view before downloading them. These thumbnails will show the content of the file to the user and they can decide to download them or not.

While this may seem to make the case a "slam dunk" for the prosecution, it is still best to have a forensic expert examine the case and evidence on your client's behalf.

Also be aware that GigaTribe contains a chat application and these logs can be recovered in some cases, showing any conversation between the agent and the user.

Common Sources of Child Pornography Files Recovered From Computers

Unallocated Space:

You can think of the files in unallocated space just like files that have been removed from the office trash bin and run through though the office shredder.



Figure 3 File carving is like electronically taping pieces of a document back together from the office shredder.

What file carving does is to find the pieces of deleted files in unallocated space and electronically tape them back together, much the in same way you would find all the pieces of a paper document in a shredder bin and tape them back together.

Figure 4 shows what a file carved from unallocated space looks like in forensic software. The important takeaway from this is that you will notice that all of the date and time information is missing. This is because files carved from unallocated space are not known in any way by the file system and no longer contain the file system metadata.

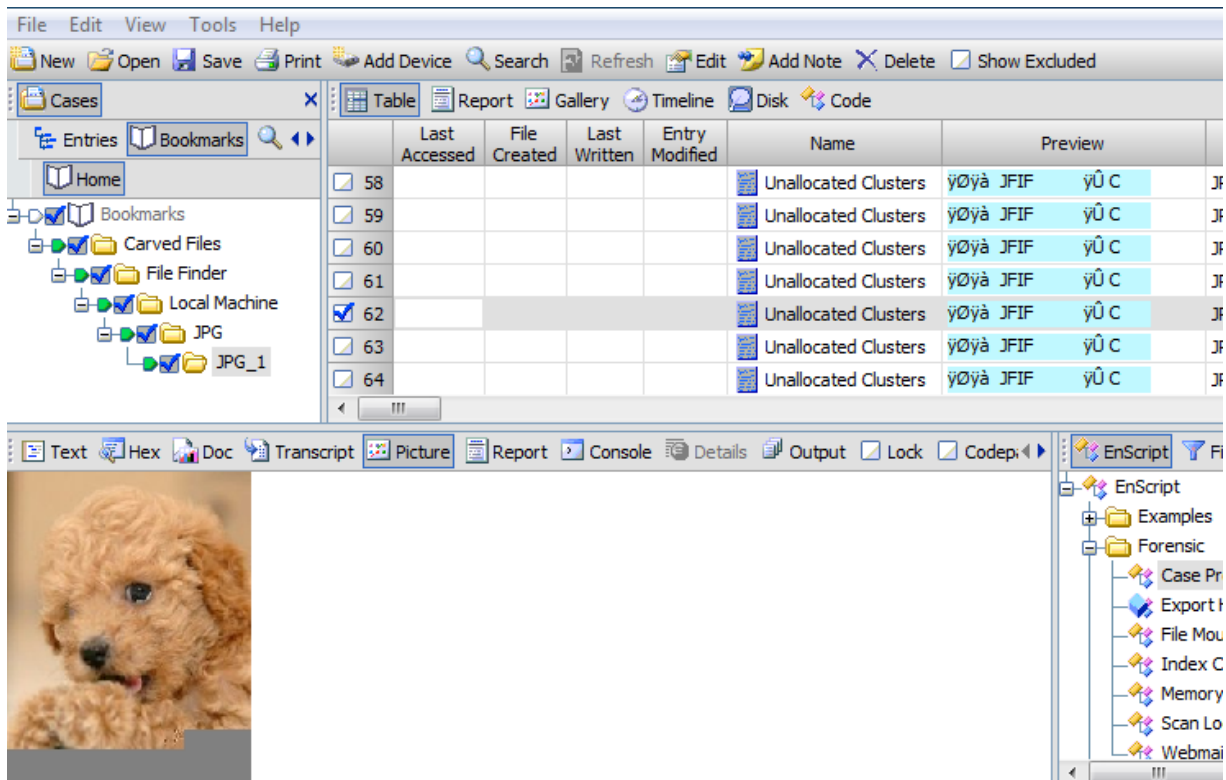


Figure 4 File carving is like electronically taping pieces of a document back together from the office shredder.

You can see that while we got about ninety percent of the picture back from the unallocated space, we did not get all of it. This is very common when doing file carving.

In the case of child pornography, this type of evidence should not be allowed as evidence as the user has no knowledge of or any way to access data in the unallocated space on a computer without the use of forensic software.

Relevant case law for images in unallocated space is included here for easy review.

Highlights to show the parts that concern unallocated space and other relevant case law are mine.

Thumbnail Files

When you view images on a computer where you see the images as thumbnail images, a copy of the image is created and stored in a database on the computer. These thumbnail images are not the originals.

If an image is deleted, the thumbnail will remain behind in the database on the computer hard drive. However, the thumbnail images can only be view using forensic software. Once a file is deleted and the only artifact left is the thumbnail image, there is no way for the user to see the thumbnails any longer or to be aware of their existence.

FOR PUBLICATION
UNITED STATES COURT OF APPEALS
THE NINTH CIRCUIT

UNITED STATES OF AMERICA, ü No. 08-10580

Plaintiff-Appellee, D.C. No.

v. ý 4:05-CR-01049-

ANDREW EDWARD FLYER, FRZ-GEE

Defendant-Appellant. þ OPINION

Appeal from the United States District Court
for the District of Arizona

Frank R. Zapata, District Judge, Presiding
Argued and Submitted

April 15, 2010—San Francisco, California

Filed February 8, 2011

Before: Andrew J. Kleinfeld, A. Wallace Tashima, and
Sidney R. Thomas, Circuit Judges.

Opinion by Judge Thomas

2415

COUNSEL

Nina Wilder; Weinberg & Wilder; San Francisco, California,
for the appellant.

Dennis K. Burke, United States Attorney, District of Arizona;
Christina M. Cabanillas, Appellate Chief for United States
Attorney; and Celeste Benita Corlett, Assistant United States
Attorney, Tucson, Arizona, for the appellee.

OPINION

THOMAS, Circuit Judge:

Andrew Flyer appeals his conviction in federal district court under 18 U.S.C. § 2252 (2004) for two counts of attempted transportation and shipping of child pornography (Counts One and Two); one count of possession of child pornography on the unallocated space of a Gateway computer hard drive (Count Three); and one count of possession of child pornography on CDs (Count Four). Flyer contends that the evidence was insufficient to establish the jurisdictional and intent elements of his convictions on Counts One and Two and the possession element of his conviction on Count Three.¹ We agree and reverse in part.

¹Because we reverse Flyer’s Count Three conviction, we decline to reach Flyer’s challenge to the district court’s denial of his motion to dismiss either Count Three or Count Four on the basis of multiplicity. We also decline to reach Flyer’s insufficient-evidence challenge to the jurisdictional element of Count Four, as Flyer conceded the issue at oral argument.

I

A. Preliminary Investigation and Execution of Search Warrant

B.

On March 9, 2004, FBI Special Agent Robin Andrews, acting undercover from Tucson, Arizona, allegedly initiated a session on LimeWire, a peer-to-peer file sharing program. LimeWire and similar programs connect network participants directly and allow them to download files from one another. *See Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919-20 (2005). To download a file, a LimeWire user opens the application and inputs a search term. LimeWire then displays a list of files that match the search terms and that are available for download from other LimeWire users. When a user downloads a file using the LimeWire network, he or she causes a digital copy of a file on another user's computer to be transferred to his or her own computer. *See Arista Records LLC v. Lime Group LLC*, 715 F. Supp. 2d 481, 494 (S.D.N.Y. 2010).

Andrews launched LimeWire and typed in the search term "PTHC," an apparent acronym for "pre-teen hardcore," a term associated with child pornography. She identified a file titled "O-KIDDY-PTHC BW025.jpeg" and selected a host computer that appeared to have the file available for download.

Andrews then clicked "browse host," a LimeWire feature that allows users to view all the files available for download from a host computer's "share" folder. The host computer Andrews had selected listed 261 files available for download, including around twenty files with titles associated with child pornography.

Andrews downloaded "O-KIDDY-PTHC BW025.jpeg" from the host computer. She tried to download a second file from the same host, but was unsuccessful.

On March 10, 2004, Andrews allegedly again used LimeWire to search the term "PTHC" and determined that the same host computer had sixty files available for download with titles associated with child pornography. Andrews downloaded one file containing such a title, and tried, but was again unable, to download a second file from the host computer.

Andrews identified the Tucson, Arizona, residential address associated with the host computer by contacting an internet access provider in Arizona. Flyer lived at the Tucson address, along with his father, mother, and sister.

After securing a warrant, agents executed a search of the property on April 13, 2004. They seized from Flyer's bedroom a Gateway computer, loose media (CDs, floppy disks, and DVDs), and an Apple laptop. They also seized a thumb drive and a family computer that did not contain any child pornography.

Agents interviewed Flyer, who admitted, according to Andrews's testimony, that he used the Gateway computer and Apple laptop in his bedroom, that he had downloaded, saved, and shared child pornography through LimeWire, and that he knew it was illegal to possess child pornography. Flyer also admitted to having saved a minimal amount of child pornography onto his shared folder on LimeWire and around one hundred child pornography files on a computer.

B. Forensic Examination of Electronic Devices

1. The Apple Laptop

FBI Special Agent Steven Gumtow examined Flyer's Apple laptop. He determined that LimeWire had been installed on the laptop and that the setup required the laptop user to manually activate LimeWire each time the laptop was turned on. When a user runs LimeWire, all files on the user's computer located in folders designated as "shared" folders are made available for upload to other LimeWire users. Gumtow testified that the settings on Flyer's laptop were customized to cap the maximum number of uploads at one file at a time by up to twenty individuals. Defense computer forensics expert Tami Loehrs, on the other hand, testified that the upload bandwidth setting on the laptop was set to zero, which allows only a small amount of data to be leaked out. The directories set up for sharing on the laptop through LimeWire included the directory "Z" and its folder "R@Y," two directories where Flyer had admitted to saving child pornography.

In a subfolder of "R@Y," Gumtow discovered files identical to those that Andrews claimed to have downloaded. Before Gumtow performed his analysis, the Apple laptop had been in the custody of FBI Special Agent Robert J. Meshinsky. While attempting to image the laptop's hard drive, Meshinsky mistakenly allowed his own computer's operating system to mount on the laptop and access the files stored there. He later testified that he noticed the problem approximately one hour after he had booted up the laptop. He stopped the process, researched another method to use, and successfully copied the hard drive. In his report, Meshinsky made no mention of the improper mounting of the target hard drive. He stated that "[a]pproved procedures and protocols were used as tested and verified by the FBI," a statement which he later admitted to be false.

Defense expert Loehrs independently examined the Apple laptop and discovered that 6,100 files listed last access dates of November 3, 2005, when Meshinsky examined the machine, and that an additional 63,000 files—including the two files allegedly downloaded by Andrews on March 9 and 10, 2004—listed last access dates of March 18, 2005, between 2:05 p.m. and 3:53 p.m. Both dates post-dated seizure of the laptop from Flyer's residence. No information could be recovered regarding any previous access dates for the two files.

Meshinsky reviewed Loehrs's findings and agreed with them.

2. The Gateway Computer

FBI Special Agent Christopher Pahl examined the hard drive from the Gateway computer. After duplicating the hard drive to preserve the evidence, Pahl searched the duplicate drive using the term "r@ygold," which is associated with child pornography. The search produced numerous positive hits all over the drive, but the only images believed to be child pornography and later listed in the indictment were found in "unallocated space."

3. The Loose Storage Media.

FBI Analyst Tammy Lepisto examined the CDs, DVDs, and floppy disks seized from Flyer's bedroom. Lepisto determined that twenty-six CDs contained images believed to be child pornography. One file Lepisto located on Flyer's CDs was titled "r@ygold style ST 06122.jpeg." That file, among others, was later listed under Count Four of the indictment.

C. Indictment

A superceding indictment filed in January 2006 charged Flyer with two counts of attempted transportation and shipping of child pornography— specifically, the images allegedly downloaded by Andrews on March 9 and 10, 2004—in violation of 18 U.S.C. §§ 2252(a)(1) and (b)(1) (Counts One and Two); possession of child pornography on the Gateway computer on or about April 13, 2004, in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (Count Three); and possession of child pornography on CDs, in violation of § 2252(a)(4)(B) and (b)(2) (Count Four).² The jury returned guilty verdicts on all four counts, and the district court sentenced Flyer to concurrent terms of 60 months imprisonment.

²A fifth count for possession of child pornography on the Apple laptop was later voluntarily dismissed by the government.

II

[1] Flyer contends that the district court erred when it denied his motion to dismiss Counts One and Two on due process grounds and to suppress evidence pursuant to *United States v. Loud Hawk*, 628 F.2d 1139, 1152 (9th Cir. 1979) (en banc) (Kennedy, J., concurring), *overruled on other grounds by United States v. W.R. Grace*, 526 F.3d 499, 505-06 (9th Cir. 2008) (en banc), based on the FBI's mishandling of his Apple laptop.

We review de novo a due process claim involving the government's failure to preserve potentially exculpatory evidence. *United States v. Cooper*, 983 F.2d 928, 931 (9th Cir. 1993). We review factual findings, such as the absence of bad faith, for clear error. *United States v. Hernandez*, 109 F.3d 1450, 1454 (9th Cir. 1997); *United States v. Booker*, 952 F.2d 247, 249 (9th Cir. 1991).

[2] The government's failure to preserve potentially exculpatory evidence rises to the level of a due process violation if a defendant can show that the government acted in bad faith. *Arizona v. Youngblood*, 488 U.S. 51, 58 (1988). Bad faith requires more than mere negligence or recklessness. *Id.* If the government destroys evidence under circumstances that do not violate a defendant's constitutional rights, the court may still impose sanctions including suppression of secondary evidence. *Loud Hawk*, 628 F.2d at 1152 (Kennedy, J., concurring).

In so doing, the court must balance "the quality of the Government's conduct and the degree of prejudice to the accused." *Id.* "The Government bears the burden of justifying its conduct and the defendant bears the burden of demonstrating prejudice." *Id.*

[3] Here, the district court did not clearly err in finding no evidence of bad faith. The government presented evidence that Meshinsky did not intentionally corrupt data on the Apple laptop hard drive, but rather mishandled it. The government also voluntarily dismissed the count in the indictment relating to possession of child pornography on the Apple laptop. We thus affirm the district court's denial of Flyer's motion to dismiss Counts One and Two on the basis of a due process violation.

[4] The district court properly denied Flyer's request for suppression of the evidence. First, as we explained above, there is no clear error in the district court's determination that the government's conduct evidenced negligence, rather than bad faith. On the other side of the scale, Flyer did not show that mishandling of the evidence prejudiced his defense. That the government could no longer prove the success of the downloads does not prove that Andrews never downloaded the files or that properly preserved data on the Apple laptop would have exculpated Flyer. Indeed, Andrews's testimony indicates that Flyer admitted to using LimeWire to download child pornography on his laptop. We thus affirm the district court's denial of the suppression motion.

III

[5] Flyer next argues that the district court erred in denying his motion for a *Franks* hearing³ and for suppression of the evidence derived from the April 13, 2004, search based on false and intentionally misleading statements in the affidavit supporting the search warrant. We review Flyer's challenge de novo, see *United States v. Gonzalez, Inc.*, 412 F.3d 1102, 1110 (9th Cir. 2005), and affirm.

When requesting a *Franks* hearing based on allegations of material false statements or omissions in an affidavit supporting a search warrant, a defendant must make a "substantial preliminary showing" that false or misleading statements were (1) deliberately or recklessly included in an affidavit submitted in support of a search warrant; and (2) "necessary³ See *Franks v. Delaware*, 438 U.S. 154 (1978). to the finding of probable cause." *United States v. Craighead*, 539 F.3d 1073, 1080 (9th Cir. 2008) (quoting *Franks*, 438 U.S. at 155-56).

[6] Flyer did not make a substantial preliminary showing that Andrews lied when she claimed in the affidavit to have downloaded two images of child pornography from Flyer's computer. As the district court determined, evidence of corruption of data on the Apple laptop does not indicate that Andrews lied before the computer was seized.

[7] Andrews's statements concerning her inability to download additional files due to traffic on Flyer's laptop similarly fail to justify a *Franks* hearing. We agree with the district court that these statements were not necessary to the finding of probable cause. The district court properly denied Flyer's motion for a *Franks* hearing.

[8] As Flyer did not demonstrate the invalidity of the search warrant, his motion to suppress evidence derived from the April 13, 2004, search also fails. IV

Flyer challenges the sufficiency of the evidence to support his conviction. When a sufficiency-of-the-evidence claim is properly preserved, “review of the constitutional sufficiency of evidence to support a criminal conviction is governed by *Jackson v. Virginia* . . .” *United States v. Nevils*, 598 F.3d 1158, 1163 (9th Cir. 2010) (citing *Jackson v. Virginia*, 443 U.S. 307, 319 (1979)). *Jackson* establishes a “two-step inquiry.” *Id.* at 1164. “First, a reviewing court must consider the evidence presented at trial in the light most favorable to the prosecution.” *Id.* “Second, . . . the reviewing court must determine whether this evidence, so viewed, is adequate to allow any rational trier of fact [to find] the essential elements of the crime beyond a reasonable doubt.” *Id.* When a sufficiency-of-the-evidence claim is not properly preserved, we apply plain-error review. *See United States v. Cruz*, 554 F.3d 840, 844 (9th Cir. 2009). “Under plain-error review, reversal is permitted only when there is (1) error that is (2) plain, (3) affects substantial rights, and (4) seriously affects the fairness, integrity, or public reputation of judicial proceedings.” *Id.* at 845 (quotation omitted).

However, plain-error review of a sufficiency-of-the-evidence claim is only “theoretically more stringent” than the standard for a preserved claim. *Id.* at 844; *see also United States v. Garcia-Guizar*, 160 F.3d 511, 517 (9th Cir. 1998) (noting that even under plain-error review, a court should not “affirm a conviction . . . if the record clearly showed that the evidence was insufficient”). “When a conviction is predicated on insufficient evidence, the last two prongs of the [plainerror] test will necessarily be satisfied.” *Cruz*, 554 F.3d at 845 (citations omitted).

[9] Here, Flyer did not renew his motion for judgment of acquittal at the close of the evidence and thus did not preserve his claim. Accordingly, we apply plain-error review as described in *Cruz*.

[10] Applying plain-error review, we must vacate Flyer’s convictions on Counts One and Two of the superceding indictment pursuant to *United States v. Wright*, ___ F.3d ___, 2010 WL 4345670 (9th Cir. 2010). In *Wright*, we held that 18 U.S.C. § 2252A(a)(1)4 required actual transportation of child pornography across state lines, *id.* at ___ F.3d ___, *3-*6, and that “a defendant’s mere connection to the Internet does not satisfy the jurisdictional requirement where there is undisputed evidence that the files in question never crossed state lines,” *id.* at ___, *6. *Wright*’s holding controls. Here, the government concedes that it presented no evidence at trial directly showing that the two files downloaded by Andrews traveled across state lines. Furthermore, Flyer cites uncontroverted expert testimony that a file shared between two users through LimeWire would not leave Tucson if, as here, both the host computer and recipient were located within that city. Andrews’ *intrastate* download of files from Flyer’s computer cannot by itself, consistent with *Wright*, provide sufficient evidence to convict Flyer of attempting to cause those files’ *interstate* or foreign movement. Accordingly, we reverse Flyer’s convictions for attempted transportation and shipment of the files in interstate commerce. *See id.* at ___, *

12. We thus decline to reach Flyer’s additional contention that the requisite specific intent for the crime was not supported by sufficient evidence.

4The jurisdictional element in that statute is effectively identical to that under which Flyer was charged in Counts One and Two of the indictment. Compare 18 U.S.C. § 2252A(a)(1) (2003) (“knowingly mails, or transports or ships in interstate or foreign commerce by any means, including by computer, any child pornography”) with *id.* at § 2252(a)(1) (2004) (“knowingly transports or ships in interstate or foreign commerce by any means including by computer or mails, any visual depiction” of child pornography).

V

[11] Flyer next alleges that the evidence is insufficient to support his conviction on Count Three for possession “on or about April 13, 2004” of child pornography on the Gateway computer in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) (2004). Subsection (a)(4)(B) provides that any person who “knowingly possesses . . . with intent to view, 1 or more books, magazines, periodicals, films, videotapes, or other matter” containing visual depictions of a minor engaged in sexually explicit behavior shall be punished as provided in subsection (b)(2).

Flyer contends that the evidence is insufficient to establish that he “possesse[d]” the files. We agree.

[12] “ ‘Possession’ is ‘[t]he fact of having or holding property in one’s power; the exercise of dominion over property.’ ” *United States v. Romm*, 455 F.3d 990, 999 (9th Cir. 2006) (quoting BLACK’S LAW DICTIONARY 1183 (7th ed. 1999)). “[T]o establish possession, the government must prove a sufficient connection between the defendant and the contraband to support the inference that the defendant exercised dominion and control over [it].” *Id.* (internal quotation omitted) (alteration in the original).

[13] The images charged in Count Three were all located in “unallocated space” on the Gateway hard drive. Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system’s trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software. Such space is available to be written over to store new information. Even if retrieved, all that can be known about a file in unallocated space (in addition to its contents) is that it once existed on the computer’s hard drive. All other attributes—including when the file was created, accessed, or deleted by the user—cannot be recovered.

Files in unallocated space differ from cache files, which are a “set of files kept by a web browser to avoid having to download the same material repeatedly . . . so that the same images can be redisplayed quickly when you go back to them.” *Id.* at 993 n.1 (quotation omitted). Cache files are located in “an area to which the internet browser automatically stores data to speed up future visits to the same websites.” *Id.* at 994 n.3 (citation omitted). The user does not manually save the cache files, *id.*, but can

access them and “print, rename, [or] save [the files] elsewhere, the same thing [he or she could] do with any other file,” *id.* at 998 (internal quotation marks omitted).

Flyer argues there was insufficient evidence to establish that he exercised dominion and control over the images recovered from the unallocated space on the hard drive. Alternatively, he argues that even if he could be said to have “possessed” the images before their deletion, no evidence indicated that the possession occurred during the time period charged in the indictment.

Our precedent relating to cache files suggests that a user must have knowledge of and access to the files to exercise dominion and control over them. In *Romm*, we affirmed a defendant’s conviction under 18 U.S.C. § 2252A(1)(5)(B) for possession of child pornography images deleted from the internet cache of his computer. *Id.* at 1000. We reasoned that:

[The defendant] had access to, and control over, the images that were displayed on his screen and saved to his cache. He could copy the images, print them or email them to others, and did, in fact, enlarge several of the images. *Id.* at 1001. Moreover, a forensic analysis of the defendant’s hard drive indicated that all of the child pornography on his computer (and reflected in his internet history) had been erased after Canada Border Services Agency had seen several pornography websites in the computer’s internet history. *Id.* at 994-95.

In comparison, in *United States v. Kuchinski*, 469 F.3d 853 (9th Cir. 2006), we held that we could not consider images recovered from the cache for purposes of a sentencing calculation when no evidence indicated that the defendant had tried to access the cache files or knew of their existence. *Id.* at 862.

We reasoned:

Where 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 dominion and control over the images.

To do so turns abysmal ignorance into knowledge and a less than valetudinarian grasp into dominion and control.

Id. at 863.

The decision of the Court of Appeals for the Armed Forces in *United States v. Navrestad*, 66 M.J. 262 (C.A.A.F. 2008)

is in accord. There, the court held that a defendant lacked dominion and control over child pornography images that he viewed while using an internet café computer. *Id.* at 267-68.

Although the viewed images had been automatically stored in the computer’s temporary cache, the court held that the defendant did not “possess” them. *Id.* The court reasoned that the defendant could not access the hard drive where the cache files had been saved

nor download the images to a portable storage device. *Id.* Additionally, no evidence indicated that the defendant had e-mailed or printed copies of the images or that he was aware that he could have done so. *Id.*

[14] We conclude that Flyer's conviction must be reversed under the reasoning in *Romm*, *Kuchinski*, and *Navrestad*. The government concedes that it presented no evidence that Flyer knew of the presence of the files on the unallocated space of his Gateway computer's hard drive. The government also concedes it presented no evidence that Flyer had the forensic software required to see or access the files. Unlike *Romm*, there is no evidence here that Flyer had accessed, enlarged, or manipulated any of the charged images, and he made no admission that he had viewed the charged images on or near the time alleged in the indictment.

The government counters that evidence demonstrating that the files had at some point been deleted, resulting in their placement in unallocated space, is sufficient to establish possession. In support, the government cites *United States v. Shiver*, 305 F. App'x 640 (11th Cir. 2008) (unpublished), for the proposition that one method for a defendant to exercise dominion and control over an image is to destroy a copy of the image located on his computer. *See id.* at 643.5 5As we recognized in *Romm*, "removal of files from the recycle bin generally requires manual steps to be taken by the user." 455 F.3d at 993 n.2.

[15] But deletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date within the meaning of § 2252(a)(4)(B) (2004). No evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there. Accordingly, the district court committed plain error, and we reverse Flyer's conviction on Count Three.

VI

[16] We affirm the district court's denial of Flyer's motion for a *Franks* hearing and for suppression of the evidence derived from the April 13, 2004 search. We decline to reverse the convictions on Counts One and Two on the basis of government's failure to preserve potentially exculpatory evidence. We reverse Flyer's convictions on Counts One, Two, and Three. The judgment of the district court is affirmed in part and reversed in part. Because we reverse three of the four counts on which Flyer was convicted and sentenced, we vacate the sentence and remand for resentencing on the remaining count. *See United States v. Avila-Anguiano*, 609 F.3d 1046, 1049 (9th Cir.) (permitting resentencing when part of a multi-count sentence is vacated), *cert. denied*, 131 S. Ct. 586 (2010).

AFFIRMED IN PART; REVERSED IN PART; SENTENCE VACATED and REMANDED.