

STATE OF INDIANA
ST. JOSEPH COUNTY

)
) SS:
)

IN THE ST. JOSEPH SUPERIOR COURT

AFFIDAVIT IN SUPPORT OF A SEARCH WARRANT

Eric Tamashasky, SJCPD, swears or affirms that:

Affiant believes and has good cause to believe that there is located on the following described person or place:

The Property located at 23711 State Road 23, South Bend, Indiana, 46614 shown below:



Certain evidence, to wit:

1. Internet-enabled computer equipment for seizure and subsequent forensic search for digital files containing child pornography, torrent files containing information relating to files containing sexual images of minors, software for searching for, downloading, and viewing digital files online, including bittorrent clients and P2P file sharing devices, evidence of external devices connected to the machine (e.g. flash drives or external storage devices), evidence of owner and/or user of the machine, evidence pertaining to internet networks (both wired and wireless) connected to, internet history or documentary guidance on how to locate, acquire, and use torrents to obtain shared internet files, internet history related to the search for or acquisition of prohibited images, evidence of passwords or encryption methods that could be used to store digital images or videos
2. Cellular telephones, digital storage devices, commercial software and hardware, computer disks, flash drives, micro-SD cards, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, computer software, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners and the data stored within these materials, which has been used or may be used: 1) to visually depict minors engaged in sexually explicit conduct and/or child erotica; 2) to advertise, transport, distribute, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct and/or child erotica; and 3) to show or evidence a sexual interest in minors or desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct. Any items not responsive to this section shall be promptly returned to the owner.
3. The Modem and/or Router used to connect to ATT internet service, to include an examination of logs contained therein about connected devices, times, and any other information to the use or access of the Internet connect in that residence
4. Records, documents, writings, and correspondence with others pertaining to the production, possession, receipt, distribution, transportation or advertisement of visual depictions of minors engaged in sexually explicit conduct.
5. Any and all photographs, compact disks, DVDs, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct.
6. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter to show or evidence a sexual interest in minors or desire or motive to produce, advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.

7. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential premises and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on memory storage devices such as optical disks, or storage media.
8. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.
9. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access relating to ATT or any other Internet service provider, all handwritten notes and handwritten notes in computer manuals.
10. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of the production, collection, advertising, transport, distribution, receipt, or possession of child pornography.
11. No more than three (3) records or other items of evidence of occupancy of 23711 State Road 23, South Bend, Indiana

That is related to an investigation of the offense(s) of:

Possession of Child Pornography, I.C. 35-42-4-4

The reasons and grounds for affiant's belief that there exists probable cause for conducting a search and seizure as detailed above are as follows:

I, Eric Tamashasky, am deputized as a Special Deputy with full law enforcement powers with the St. Joseph County Police Department. I have been a special deputy since 2011 and am responsible for the St. Joseph County Cybercrimes Against Children Unit. Prior to my role as a Special Deputy with the St. Joseph County Police Department, I was a deputy prosecuting attorney for the St. Joseph County Prosecutor's Office since 2004. In that capacity, I prosecuted major crimes—including cybercrimes cases. I was the lead prosecutor for the St. Joseph County

Prosecutor's Office High Tech Crimes Unit from 2007 until its closure in 2009. I have training on cybercrime investigations from the United States Secret Service, the National Center for Missing and Exploited Children, the National White Collar Crime Center, and the Internet Crimes Against Children (ICAC) Taskforce.

I received training specifically related to the online sharing and distribution of child pornography from the ICAC Task Force that was specifically related to online file sharing via peer-to-peer clients. Peer-to-Peer (P2P) file sharing is the method by which users on the same network share digital files with one another. I am trained to search for child pornography on both the Ares Peer to Peer Network (September 2013) and BitTorrent peer-to-peer file sharing (December 2014).

P2P investigations typically center upon contact with particular IP addresses. An "IP address" is a numeric address for a particular computer accessing the internet on a particular date and time. Once online, the IP address is unique to a particular access point. It is possible for multiple computers to use one public IP address through the use of internal networking. Should a particular IP address become an address of interest in an investigation, it is reasonable to believe multiple computers may be using the same IP address.

INVESTIGATORY METHODS

During my training in Ares investigations, I was given a program that allowed me to search the Ares P2P network for files possibly containing child pornography. We tested and validated the program during the training class itself to ensure it located appropriate files and only downloaded from a single source at a time. The program works by comparing the Ares network's own listing of user's files versus a list of files known to law enforcement to be associated with child pornography. Not every file contained within the law enforcement Ares database is child pornography in that some of the files depict the child victims of child abuse in licit states. The existence of a photograph of a known victim of child abuse is relevant because child pornography collectors may acquire "series" images of victims. A "series" may be a couple of licit pictures followed by that same child being abused and raped. Files are generally catalogued on file sharing sites by the hash value of a particular file, not by the file name attached to the file. "Hash values" are numeric values calculated by the application of a

particular algorithm or formula to a digital data. The formulas that calculate hash values are so sensitive that a change of one pixel in a picture will completely change the hash value. They are akin to digital fingerprints. File names are easily changed and altered to disguise the contents of a file. To change a hash value requires additional knowledge and skill not generally displayed by P2P traders.

The tool also captures the IP addresses of those individuals offering files of interest for distribution. The program determines the approximate geographic location of a particular user's device by searching publically available tools with the captured IP address information. Because of this feature, investigators may focus on users offering files for distribution that are located in particular geographic areas. Our program has been tested and validated to do only single source downloads; this means that when we attempt to download a file from a user it is only that particular user who provides the file to us. While the general architectural design of P2P file sharing is to gather file pieces from multiple users, our search methodology only allows us to retrieve file pieces from a single user. This ensures we have relevant information about the file(s) possessed by that singular user.

Once a file of interest has been located on an appropriate geographically located machine, the Ares tool attempts to download the files. The acquisition of partial files—so long as those fragments themselves contain verifiable contraband—is not a weakness of this tool. Internet connections may time out or the user sharing the file could leave the network or move the file. The reason a partial file I obtain is significant is that it is proof the user possessed the entire file at one time. Since Ares clients only report hash values to the network once the user possesses the complete file, the only files our tool can seek to obtain are those files the user's machine reported as possessing completely. The partial obtained by the Ares tool represents a sample of the entire item possessed by the user.

Note that newly manufactured child pornography will not show up in via our Ares investigatory tool. The only files we attempt to download are those files already known to law enforcement for their relevance to online child exploitation because they've been obtained previously. New files have as-of-yet unknown hash values that cannot have been entered into our database of previously found files of interest.

INVESTIGATORY DETAILS

During my the course of my investigations of Ares, my investigative program identified a computer with the IP address **23.119.118.36** as a potential download candidate (source) for over 100 file(s) of investigative interest. That IP address geolocates to South Bend, Indiana and appears to be owned by AT&T Internet Services. I have obtained a complete download of a file from a computer at **23.119.118.36**. I viewed the movie file and I believe that it represents child pornography as defined by both state of Indiana and federal law. A description of the video follows:

- On March 4, 2016, my computer began a download from a user at **23.119.118.36**. Specifically, I was connected to **23.119.118.36** from 2016/Mar/04 20:46:08 UTC 05:00 to 2016/Mar/04 21:04:09 UTC 05:00. I obtained a file named “sexo infantil pai filha pai mete na menina sado anal-partel.mpg” from a device at that IP address. I viewed the file and it is 1:15 long. The video shows a child that appears to be younger than 10 years old, gagged, bent over a table while an adult male inserts his penis into the child. Ultimately, the adult male ejaculates onto the child’s back. I am not able to determine the gender of the child due to the camera angle.

The record I have of contacts with **23.119.118.36** dates back to 2013. Over that time, my machine reported over 181 files of investigatory interest from that IP address. This is the first time I have successfully initiated a download from that device.

Through my training and experience, I believe that people who search for and view child pornography generally keep the items they collect. And even if a person deletes the item after some period of time, a forensic computer examination often can find part (or all) of the deleted files on the person’s hard drive; it is very difficult to successfully remove all traces of a deleted file from a hard drive.

On March 7, 2016 a query on the IP address **23.119.118.36** was conducted through the American Registry for Internet Numbers (ARIN) via whatismyipaddress.com. I received information that the IP address is registered to AT&T Internet Services. I obtained a subpoena to AT&T for the subscriber information and service location of that IP address. As a result of that subpoena, ATT replied that “Gerald Wendt” is responsible for the billing for the IP address. Mr. Wendt’s billing and service address are the same: 23711 State Road 23, South Bend, Indiana, 46614.

As of May 13, 2016, my investigative program still showed the presence of a computer at the 23.199.118.36 IP address on the ARES network within the last several days. Detective Phil Williams, SJCPD, drove by the address and took photographs of the property listed in the ATT subpoena results. A photograph taken by Detective Williams of 23711 State Road 23, South Bend, Indiana 46614 is below:

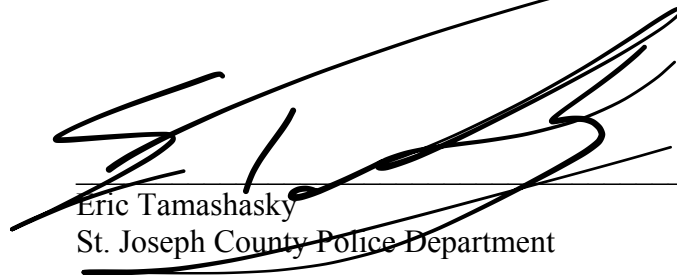


I believe that a search warrant for the items detailed above is relevant to provide evidence of who is utilizing the internet connection at 23711 S.R. 23, South Bend, Indiana to search for and download digital files containing child pornography. I have learned through my training and experience that individuals who seek out child pornography on the internet often save those items once found to remote storage devices, including flash drives, external hard drives, or even memory cards. Further, even if a user deletes materials after a period of time, I believe that a

forensic examination of the computer equipment can often reveal the presence of deleted files, even after years of user deletion.

All of the above events occurred within St. Joseph County, Indiana.

I affirm, under the penalties for perjury that, to the best of my knowledge and belief, the foregoing is true.



Eric Tamashasky
St. Joseph County Police Department

SEARCH WARRANT

STATE OF INDIANA

)

) SS: In The St. Joseph Superior Court

ST. JOSEPH COUNTY

)

TO: ANY CONSTABLE, POLICE OFFICER, SHERIFF, or CONSERVATOR of the PEACE.

GREETINGS:

WHEREAS, there as been filed with me an AFFIDAVIT, a copy of which is attached hereto and incorporated herein by reference; and,

WHEREAS, I find there exists probable cause to believe that:

1. Internet-enabled computer equipment for seizure and subsequent forensic search for digital files containing child pornography, torrent files containing information relating to files containing sexual images of minors, software for searching for, downloading, and viewing digital files online, including bittorrent clients and P2P file sharing devices, evidence of external devices connected to the machine (e.g. flash drives or external storage devices), evidence of owner and/or user of the machine, evidence pertaining to internet networks (both wired and wireless) connected to, internet history or documentary guidance on how to locate, acquire, and use torrents to obtain shared internet files, internet history related to the search for or acquisition of prohibited images, evidence of passwords or encryption methods that could be used to store digital images or videos
2. Cellular telephones, digital storage devices, commercial software and hardware, computer disks, flash drives, micro-SD cards, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, computer software, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners and the data stored within these materials, which has been used or may be used: 1) to visually depict minors engaged in sexually explicit conduct and/or child erotica; 2) to advertise, transport, distribute, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct and/or child erotica; and 3) to show or evidence a sexual interest in minors or desire or motive to collect or distribute visual depictions of minors engaged in sexually explicit conduct. Any items not responsive to this section shall be promptly returned to the owner.
3. The Modem and/or Router used to connect to ATT internet service, to include an examination of logs contained therein about connected devices, times, and any other information to the use or access of the Internet connect in that residence

4. Records, documents, writings, and correspondence with others pertaining to the production, possession, receipt, distribution, transportation or advertisement of visual depictions of minors engaged in sexually explicit conduct.
5. Any and all photographs, compact disks, DVDs, cameras, documents, books, records, ledgers, correspondence, receipts, magazines and other materials reflecting the purchase, sale, trade, transmission, advertising, transport, distribution, receipt and possession of any visual depiction of minors engaged in sexually explicit conduct or to show or evidence a sexual interest in minors or desire or motive to collect, distribute, and receive visual depictions of minors engaged in sexually explicit conduct.
6. Any and all magazines, books, photographs, letters, written narratives and computer text files or any other printed or electronic matter to show or evidence a sexual interest in minors or desire or motive to produce, advertise, distribute, transport, receive, collect or possess visual depictions of minors engaged in sexually explicit conduct.
7. Any and all records showing or bearing indicia of the use, ownership, possession, or control of the residential premises and items contained therein, including visual depictions of minors engaged in sexually explicit conduct, computer equipment, accessories, telephone(s), modem(s), or such records, whether stored on paper, in files, invoices, bills, leases, deeds, permits, licenses, telephone bills, tax receipts, or other documentation, or on memory storage devices such as optical disks, or storage media.
8. Envelopes, letters, and other correspondence, including, but not limited to, electronic mail, chat logs, IRC logs, ICQ logs, all usage records for distributed file sharing technologies, and electronic messages, offering to distribute and receive visual depictions of minors engaged in sexually explicit conduct, or to show or evidence a sexual interest in minors or desire or motive to advertise, distribute, transport, receive, collect and possess visual depictions of minors engaged in sexually explicit conduct.
9. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, correspondence, sales receipts, and bills for Internet access relating to ATT or any other Internet service provider, all handwritten notes and handwritten notes in computer manuals.
10. Keys, storage combinations, passwords, and paperwork which indicate any other storage containers or facilities that could contain evidence of the production, collection, advertising, transport, distribution, receipt, or possession of child pornography.
11. No more than three (3) records or other items of evidence of occupancy of 23711 State Road 23, South Bend, Indiana

is/are located at/in/upon:

The Property located at 23711 State Road 23, South Bend, Indiana, 46614 shown below:



YOU ARE THEREFORE ORDERED AND COMMANDED, in the name of the State of Indiana, with the necessary and proper assistance, in the daytime or in the nighttime to enter into or upon the location described herein and diligently search for all said items described herein. You are ordered to seize such property, or any part thereof, found on such search and after seizure, perform any necessary examinations to locate the presence of the evidentiary materials listed above.

Dated this 18th day of May, 20 16, at the hour of 10:49AM.

A handwritten signature in black ink, appearing to be "David J. H. H.", written over a horizontal line.

Judge, St. Joseph County Superior Court