

STATE OF INDIANA            )  
  )  
ST. JOSEPH COUNTY        )            IN THE ST. JOSEPH SUPERIOR COURT  
  )  
  )            GENERAL BOOK ENTRY

IN RE: A PENDING CRIMINAL INVESTIGATION        )  
of Child Exploitation that occurred in St. Joseph County,        )  
Indiana on or about March 24, 2017                                        )  
SJCPD Cyber 17114    )

**PROSECUTOR'S SUBPOENA DUCES TECUM AND ATTACHED COURT ORDER**

TO: Comcast Legal Response Center  
Fax: 866-947-5587

Upon receipt of this Subpoena, you are hereby commanded to present to Eric Tamashasky of the St. Joseph County Police Department via email to [etamashasky@co.st-joseph.in.us](mailto:etamashasky@co.st-joseph.in.us) or fax to 574-696-0303, the following tangible items and documents:

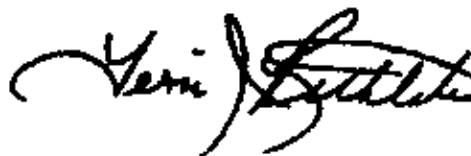
Internet Records for subscribers assigned 98.228.124.179 from Midnight EST March 24 2017 to 08:10AM EST May 25 2017

- Customer Account Records
  - Account owner, contact information, service type, service location, email addresses.
- IP Address Assignment Records
  - Records associated with the IP address 98.222.124.179

**\*\*\* JUDGE HAS ORDERED NON-DISCLOSURE (SEE JUDGE PAGE) \*\*\***

ANY QUESTIONS SHOULD BE DIRECTED TO ERIC TAMASHASKY AT THE ST. JOSEPH COUNTY POLICE DEPARTMENT (574) 876-9047

Attorney for State of Indiana  
Jennifer McKinney  
Deputy Prosecuting Attorney  
South Bend, IN 46601  
(574) 235-9544



Clerk of St. Joseph Superior Court

DATED: May 25, 2017

STATE OF INDIANA            )  
  )  
ST. JOSEPH COUNTY        )            IN THE ST. JOSEPH SUPERIOR COURT  
  )  
  )            GENERAL BOOK ENTRY

IN RE: A PENDING CRIMINAL INVESTIGATION        )  
of Child Exploitation that occurred in St. Joseph County,        )  
Indiana on or about March 24, 2017                                )  
SJCPD Cyber 17114    )

### AFFIDAVIT OF PROSECUTOR

Jennifer McKinney, upon information and belief, affirms under the penalties of perjury that:

I am a Deputy Prosecutor for the 60<sup>th</sup> Judicial Circuit, County of St. Joseph, State of Indiana. I have read a verified affidavit by Eric Tamashasky of the St. Joseph County Police Department concerning an investigation into the Possession and Distribution of Child Pornography.

The facts which render the foregoing subpoena *duces tecum* reasonable are set forth in the narrative supplemental report of Eric Tamashasky, a copy of which is attached hereto and incorporated herein as "Affidavit of Investigator." I believe that this request is reasonably relevant to a valid criminal investigation. I further believe that the request is sufficiently limited in scope and specific in directive so that compliance will not be unreasonably burdensome to the recipient.

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

  
\_\_\_\_\_  
Deputy Prosecuting Attorney

STATE OF INDIANA            )  
                                      )  
ST. JOSEPH COUNTY         )           IN THE ST. JOSEPH SUPERIOR COURT  
                                      )  
                                      )           GENERAL BOOK ENTRY

IN RE: A PENDING CRIMINAL INVESTIGATION         )  
of Child Exploitation that occurred in St. Joseph County,         )  
Indiana on or about March 24, 2017                         )  
SJCPD Cyber 17114   )

### **AFFIDAVIT OF INVESTIGATOR**

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), BitTorrent peer-to-peer file sharing (December 2014) and the eMule/eDonkey network (May 2016). I have been conducting P2P investigations since September 2013.

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 98.228.124.179 as a potential download candidate (source) for a file of investigative interest. That IP address geolocates to Mishawaka, Indiana and appears to be owned by Comcast Internet Services. I have obtained a download of a file from a computer at 98.228.124.179. 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 24, 2017, my RoundUp Ares program identified 98.228.124.179 as an IP address that had a file of interest available. I was able to download a part of a video file from that IP address around 5:00PM EST. I confirmed this connection and download via log files maintained during the download. The file's name was "\$rr9s90a(3).mpg." The segment of the video file I downloaded is approximately 6 seconds long (though the entire file appears to be 6:50 long. The video begins with three boys approximately 8-10 years old, naked, on their hands and knees on a bed. Their scrotums are visible as they bounce around and wrestle. The last portion acquired shows one of the boys sitting up on the bed, completely naked, with his left hand on his exposed penis.

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. Further, I know that the Ares program contains database files that contain

listings of all files downloaded and shared in that a forensic examination of the user's computer can show a history of activity by that machine using Ares. The Ares client records the digital fingerprint of all files successfully downloaded. According my RoundUp Ares tool, the user at 98.228.124.179 has been seen with 17 different files of investigative interest since February 2017. As recently as yesterday, May 24, 2017, the user reported having five different files of investigative interest on that day alone. As I type this affidavit, the user at 98.228.124.179 is currently online on Ares (as of 8:10AM on May 25, 2017).

On May 25, 2017, a query on the IP address 98.228.124.179 was conducted through the American Registry for Internet Numbers (ARIN) via whatismyipaddress.com. I received information that the IP address is registered to Comcast Internet Services. I believe that a subpoena to Comcast to identify the subscriber(s) who was/were using 98.228.124.179 on March 24, 2017 through today, May 25, 2017 is relevant to my ongoing investigation into the possession and distribution of child pornography. Further, I believe that the facts and information contained within this affidavit represent specific, articulable facts that show there are reasonable grounds to believe the records sought are relevant and material to an ongoing criminal investigation as is the standard under federal law pursuant to 18 U.S.C. § 2703(d).

Finally, I believe that notice of this investigation will necessarily alert the target user that law enforcement has begun to take steps to identify them. The possession of child pornography is a state and federal felony; if convicted, the person faces both incarceration and placement on the sex offender registry. I believe that any notice of our interest will result in reasonable individuals taking steps to thwart our investigation including destroying evidence, taking steps to securely destroy evidence (means of which are available via a simple google search), applying encryption to evidence drives, and otherwise adversely affecting our ability to effectively determine the identity of the user whose machine provided us with child abuse imagery.

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

  
Eric Tamashaky

St. Joseph County Police Department

STATE OF INDIANA            )  
  )  
ST. JOSEPH COUNTY         )           IN THE ST. JOSEPH SUPERIOR COURT  
  )  
  )           GENERAL BOOK ENTRY

IN RE: A PENDING CRIMINAL INVESTIGATION         )  
of Child Exploitation that occurred in St. Joseph County,         )  
Indiana on or about March 24, 2017                         )  
SJCPD Cyber 17114   )

**SUBPOENA DUCES TECUM/COURT ORDER**

The Court, having reviewed the application for a *subpoena duces tecum/court order* and accompanying Affidavit of Prosecutor in the following manner [H.I.], orders:

I find that the foregoing subpoena duces tecum is reasonable in that it is: relevant in purpose to a valid criminal investigation; sufficiently limited in scope; and specific in directive so that compliance will not be unreasonably burdensome. I also find that the affidavit in support provides specific and articulable facts showing there are reasonable grounds to believe the information sought is relevant and material to a pending criminal investigation and that this court order is proper. Its issuance is therefore **APPROVED**. Further, pursuant to 18 USC 2705, having considered the facts and circumstances contained within this application, I find that there exists a reason to believe that prior notification may have one or more of the following adverse results:

- ☒ (1) endangering the life or physical safety of an individual;
- ☒ (2) flight from prosecution;
- ☒ (3) destruction of or tampering with evidence;
- ☒ (4) intimidation of potential witnesses; or
- ☒ (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

**THEREFORE, the recipient of the foregoing subpoena duces tecum/Court Order is hereby ORDERED to comply with the subpoena duces tecum/Court Order and to not disclose the existence of this subpoena/court order for a period of ninety (90) days from the date of issuance, unless otherwise ORDERED by this Court.**

SO ORDERED this 25 day of May, 2017.

\_\_\_\_\_  
Judge/Magistrate, St. Joseph Superior Court