

IN THE CIRCUIT COURT
THIRD JUDICIAL CIRCUIT
MADISON COUNTY, ILLINOIS

18 MR 500118
FILED

JAN 25 2018

CLERK OF CIRCUIT COURT #31
THIRD JUDICIAL CIRCUIT
MADISON COUNTY, ILLINOIS

COMPLAINT FOR SEARCH WARRANT

Detective Sergeant Brian Koberna DSN 321, COMPLAINANT, now appears before the undersigned Judge of the Circuit Court of the Third Judicial Circuit of Illinois, and requests the issuance of a Search Warrant to search the following described premise(s) or item(s):

The Madison County Administration building located at 157 N. Main St., Edwardsville, Illinois and the Madison County Sheriff's Office located at 405 Randle St., Edwardsville, Illinois to specifically include the backup disk image files and backup user files located on a network server, Network\tech1\images\Information Technology, with a folder called "hp-dorman arc_18071719502154" and Network\tech1\images\County Board, with a folder called "dehulme"

and to there seize, secure, analyze, tabulate and make return thereof according to law, the following property or things:

respect to the above seized backup disk image files and backup user files to analyze any or all search history, images, communications, videos, calendar, audio, email, deleted data, encryption, operating system files, emails, documents, and programs

or things which have been used in the commission of or which may constitute evidence of the offense(s) in connection with which this warrant is issued, being **720 ILCS 5/17-51 Computer Tampering, 720 ILCS 5/33-1 Bribery, 720 ILCS 5/14 Violation of Article 14:Eavesdropping Statue and 720 ILCS 5/33-3 Official Misconduct.**

The following facts having been sworn to by Complainant in support of the issuance of this Warrant. (See attached Affidavit, which is, in its entirety, made a part of this Complaint for search warrant by incorporation, and express reference.)

WHEREFORE, your Complainant requests that the Court issue a Search Warrant directing a search for and seizure of the property described above at the premises described above.

DET. SGT. D. K. 321
Complainant

Subscribed and sworn to before me on this 9 day of JAN, 2018

W. J. Schurde
Judge

18MR 500118

STATE OF ILLINOIS)
) SS
COUNTY OF MADISON)

FILED

JAN 25 2018

CLERK OF CIRCUIT COURT #31
THIRD JUDICIAL CIRCUIT
MADISON COUNTY, ILLINOIS

AFFIDAVIT

I, **Detective Sergeant Brian Koberna**, do hereby state and affirm as follows:

1. I have been a sworn peace officer in this State since 2003. I am employed as a Detective with the Madison County Sheriff's Office and I am assigned to the Forensic Computer Crime Unit. I am also assigned to the Federal Bureau of Investigations, Metro East Cyber Crime Task Force as a Special Federal Officer (SFO). I have received training related to computer crimes consisting of on-line investigations, computer forensic and cellular phone forensics.
2. The statements contained in this affidavit are based upon my investigation, information provided by other investigators, other personnel specially trained in the seizure and analysis of computers and electronic media, and/or on my experience and training as a deputy with the Madison County Sheriff's Office and an SFO with the FBI. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence of a **720 ILCS 5/17-51 Computer Tampering, 720 ILCS 5/33-1 Bribery, 720 ILCS 5/14 Violation of Article 14:Eavesdropping Statue and 720 ILCS 5/33-3 Official Misconduct** exists on the aforementioned item in the search warrant of targeted

search.

3. On January 4th, 2018, notification was made from the State's Attorney's Office regarding possible illegal activity including violations of **720 ILCS 5/17-51 Computer Tampering, 720 ILCS 5/33-1 Bribery, 720 ILCS 5/14 Violation of Article 14:Eavesdropping Statue and 720 ILCS 5/33-3 Official Misconduct.** Specifically, I was informed that two individuals identified as Lisa Ciampoli and Chris Slusser provided Grand Jury testimony relating to the aforementioned charges. Both individuals are elected officials and associated to the Republican Party.
4. Lisa Ciampoli provided information surrounding improper activity when she filed petitions for precinct committee person while at the front desk of the Madison County Clerk's Office. She indicated that within approximately twenty seconds after she arrived at the counter, an individual by the name of Robert Dorman confronted her and interfered with her filing of the petition. She provided details that Dorman's father was also running for the same position against her that she was filing paperwork for. Robert Dorman is employed as the Madison County Information Technology (IT) director and was appointed by the Chairman of the County Board, Kurt Prenzler sometime around December 2016. During her encounter with Dorman, Dorman tried to swipe the paperwork out of the clerk's hands. This information was corroborated by video surveillance footage from Madison County cameras. In addition, she was suspicious about how Dorman knew she was filing the paperwork at the time and believed he was monitoring her whereabouts on Madison County cameras during working hours within the administration building.

A subsequent FOIA (Freedom of Information Act) request was filed by Dorman's father for this video footage. Lisa Ciampoli is an elected official serves as a Madison County Board member.

5. Chris Slusser, the elected Madison County Treasurer, testified that in February of 2017 a Madison County employee by the name Doug Hulme bragged about having evidence of circuit judge using county resources for political fundraising. Doug Hulme is employed as the Madison County Administrator and was appointed by Kurt Prenzler. When Slusser confronted Hulme on how he obtained this evidence, he alluded that they have access to everyone's emails, of which they performed keyword searches and found them. He touted about saying how they had enough evidence to force this judge to resign. Slusser indicated that this activity made him feel uncomfortable. He subsequently reported this to the Federal Bureau of Investigation. Hulme also said sometime around April 2017 that they were going to install new printers and copiers throughout the departments and Rob Dorman will be able to monitor the internal hard drives to see what everyone is printing. Hulme made a comment about having GPS devices on all county vehicles so Dorman can monitor them. Slusser was told about an incident involving Deb Detmers who was the deputy chief of staff for Congressman John Shimkus when she wanted to schedule a meeting with Kurt Prenzler for a position in his administration. She was supposed to have lunch with Prenzler; however, upon arrival was met by Hulme and Steve Adler. Steve Adler has served in many different positions in Madison County government since Prenzler has been elected to office and is no longer employed in

Madison Government. Hulme and Adler offered her the job on the condition that Congressman Shimkus submit Don Weber's name for the United State's Attorney.

6. Acting on this aforementioned information, it was apparent that the information was gleaned from reading digital correspondence in the form of emails through Madison County Government servers. The investigation began to surround the infrastructure and history of the Madison County computer servers. It also created the appearance that unauthorized access to Madison County emails accounts were also done without proper authority or in excess of authority granted to him/her.
7. Another witness/complainant identified as Gregory Nihiser contacted authorities regarding some suspicious activity was interviewed on Thursday January 4th, 2017. Specifically, he is employed as a maintenance worker at Madison County. He overheard a subject known as Bruce Cooper (Human Resources Department) telling Linda Ogden about destroying some items before a FOIA request is made yesterday January 3rd, 2018, outside the administrative services door. Specifically, he took notes which said "we need to destroy files according to time or legality before FOIA requests. I don't want anything that could be damaging personally or otherwise". He said that Ogden acknowledged it in the affirmative. The context at this point is unknown. He couldn't provide much more information about it; however, it showed a possible propensity to destroy items.
8. It was determined the best course of action without compromising the integrity of the investigation would be to interview individuals who were familiar with the network and/or servers. Due caution was exercised not to alert current employees of

the IT staff; therefore, previous employees were initially interviewed who were familiar with the network due to the sensitive nature of the case.

9. Thomas Hall, who served as the System Administrator over the network until around June 2017, reported suspicious actions on behalf of Robert Dorman and orders that were given by Robert Dorman. Specifically, Hall indicated that when Dorman was appointed as the director of IT, he was told to give Steve Adler and Doug Hulme full access to all email accounts of any employee within the county. He said this was never a past practice and that previous employees who held those same administrative positions did not have administrative access to the MailStore. Hall was also told to coordinate and/or instruct Hulme and Adler on how to operate the MailStore server application and show them how to use it. He indicated that he was given hand written notes in the form of "index" cards from Dorman to pull email accounts from the dates of their inception until the date requested for Frank Miles, Timothy Renick, Jeff Kochan, Barry Harris, Dave Stricklin, Joe Parente, and Alan Dunstan (phonetic spelling and pronunciation). These individuals were all employed or previously employed in Madison County Government. Steve Adler left Madison County government sometime around May 2017. Typical protocol would be to deactivate the email account and access to the network according to Hall and past practice; however, Dorman told him to keep it active which he found highly unusual.
10. Kyle Kielty who also served as the system engineer over the network until around June of 2017, gave similar accounts to Thomas Hall's statement indicating that he had knowledge of Dorman giving index cards to Hall to pull email accounts. He also

indicated he installed the MailStore server application on Hulme's and Adler's computer and showed them how to use it. Kielty indicated that he installed the MailStore application on the desktop computer in Hulme's Administrative Office and the desktop computer in Adler's Administrative Service's Office. Kielty advised that he recalled Adler's computer was Barry Harris' old computer.

11. Jeff Kochan was also interviewed and served as the deputy director of IT until around June of 2017. He was also handed index cards by Robert Dorman and ordered to obtain full email accounts. One name was Matt Jones (phonetic spelling and pronunciation). Kochan said he was also asked to pull emails from other individuals at the direction of Robert Dorman within Madison County Government but couldn't recall their names. Kochan indicated that he observed a web history audit of Jennifer Zolzer's activity on Dorman's computer. Kochan advised that he later spoke to Zolzer and confirmed that no one in the Auditor's Office to include Madison County Auditor, Rick Faccin, ever requested a web history search of her activities. Kochan advised that the web history is viewed through a web based platform and then the user generates a Portable Document Format (PDF) of the web history report. Kochan corroborated Hall's statement about keeping Adler's network, email account, and administrative rights open and active, which violated standard procedure. These accounts were left open despite Adler no longer being a Madison County employee and Adler's accounts still having administrative privileges to the network.
12. The MailStore Server creates 1:1 copies of all emails (whether incoming or

outgoing) in a central email archive to ensure the security and availability of large amounts of data over a period of years. The service allows for a complete record of all emails associated to accounts on the exchange server(s), (which is an email server). Thomas Hall and Jeff Kochan advised that Madison County uses the MailStore Server to backup all email accounts in the county. Administrative MailStore users have full access to search, read and export any historical email in the MailStore archive for any current or past employee (dating back to around the early 2000s). The service allows for administrative users to search specific accounts and/or all accounts through key words, as it relates to specific times, as it relates to where the email is sent from or to, and additional specific search criteria.

13. During the course of their interviews Hall, Kochan, and Kielty indicated that the MailStore Server and Applications were primarily used for Freedom of Information Act compliance under the previous IT Administration Director Timothy Renick. Hall, Kochan and Kielty indicated the scope of the service was expanded under the IT Director Robert Dorman, where unusual requests for full archives of specific email accounts were created and Administrative access was granted to individuals outside of the IT staff. Hall, Kochan and Kielty advised that they thought it was very unusual and enormous administrative power to grant Hulme and Adler MailStore administrative rights.
14. Additional interviews were conducted, to include a current employee of the Madison County IT staff, who told investigators that he currently has full administrative domain rights and is familiar with the network. The employee advised that he can

remotely access the network and provide account related information.

15. Emails previously accessed as indicated by witnesses commonly contain juvenile information, privileged information, legal, and/or law enforcement sensitive information thereby establishing proper ownership of such information prohibited by law and should not be distributed or accessed by individuals without proper authority. According to Madison County State's Attorney Thomas Gibbons, by the Illinois Constitutional State Law, the Madison County Administration is a separate entity from other Madison County Elected Offices and the Judiciary Branch. Members of the Madison County Administration do not have authority over other Elected Offices or the Judiciary Branch. Accessing the emails or other work product by the Administration would be beyond the scope of the authority granted to them, without proper permission from the Elected Office or the Judiciary. Evidence indicates that violations of **720 ILCS 5/17-51 Computer Tampering, 720 ILCS 5/33-1 Bribery, 720 ILCS 5/14 Violation of Article 14:Eavesdropping Statute and 720 ILCS 5/33-3 Official Misconduct** could be plausible; however, further investigation was warranted.
16. It was believed that intelligence information could be gleaned from within the network through directory and file structure browsing, account related logs, and server logs to indicate whether or not certain accounts are still active and what activity is occurring within the accounts. Also, it would serve as a tool to determine the location of a specific computer and the office that it may reside within. In addition, by logs and viewing the architecture within the network may also serve to

determine which individual was associated to specific files, data, or computers.

17. Based on the above mentioned information a search warrant was drafted for **“Data within computers and/or servers located at the Madison County Administration building located at 157 N. Main St. in Edwardsville, Illinois, 62025 and the Madison County Sheriff’s Office, 405 Randle St., Edwardsville, Illinois, 62025, which includes the browsing of accounts associated to Robert Dorman, Doug Hulme, Steve Adler to include folder/directory structure within the servers to also include browsing of user activity and user associated logs (logs include: file activity logs, logins, IP logs, associated hardware and MAC address logs, etc.) browsing of any virtual environment activity to also include snapshots, any email associated logs or associated email accounts, any internet related activity reports and with respect to the aforementioned browsing activity also allow the designee conducting the browsing to video, screenshot, capture, export, or digitally seize any files of evidentiary value”**. A search warrant was obtained by the Honorable Judge Neil Schroeder on January 5th, 2018, and was executed at 10:06 p.m. with the assistance of current Madison County IT staff remotely.
18. During the execution pertinent information was gleaned as well as corroborating evidence to the witness information. Limited queries acting in conjunction and within the scope of the warrant were conducted on the three individuals named in the search warrant being Robert Dorman, Steven Adler and Doug Hulme.
19. Specifically, Adler’s account showed that it was created on December 12th, 2016,

and it was active up until the point of July 5th, 2017, when records indicate it was deactivated. This corroborated Hall's statement that Adler's account was left active after he was no longer a Madison County employee. The computer he was associated to is identified using service tag number ID "F4X2VR1". This was identified through ways of querying several different databases. During this query the IP address of 10.0.17.36 was located and associated to hardware Media Access Control (MAC) address of 18:03:73:D0:67:27 (A Dell Optiplex). Next, an IP address query was performed on the first floor switches of the administration building associated to the third Octet subnet of "17" which showed the protocol description of "Support Services Room 158 Dennis Dubbelde's Office". Lt. Vucich is familiar with the office as previously being Dennis Dubbelde's Office which is now Bruce Cooper's Office which was associated to the System name AKA Service Tag F4X2VR1 as recent as December 30th, 2017. A search of Dell's website showed the Service Tag F4X2VR1 is associated to a Dell Optiplex 790. This was also the proximity where Greg Nihiser heard a conversation between Cooper and Ogden about destroying items. Also querying that service tag number through the work order database showed it to be associated to Barry Harris on a previous work order request. Lt. Vucich also knew that to be the same office. Therefore, it is suspected that Adler's computer he previously used is located in the Administrative Services area, which was referred to in IT administrative logs as office number or Room 158. It is further believed that the computer previously used by Steve Adler, would still contain data, files and artifacts, which were created, accessed and viewed

by Steve Adler, during the time of the events in question. As a result of Adler have administrative access to the MailStore and the fact the MailStore application was installed on Adler's computer there reason to believe artifacts of emails or email related queries can be recovered from the computer. It should be noted that Adler's account to include administrative access to the MailStore was still active after the time Steve Adler was no longer a Madison County employee.

20. Robert Dorman's computer location was also identified through several different databases which yielded positive results. A Media Access Control (MAC) Address associated to him was R90NP2F0 which returns to a Lenovo laptop. Witnesses identify Dorman to commonly use and be in possession of two Lenovo laptops. The other service tag number is "PFOUVVNQ". It was further reported that Dorman received a Lenovo laptop in furtherance of a bid that was submitted to Lenovo during his time as IT Director. Performing a keyword of "Dorman" across the network yielded a file path of "Network\tech1\images\Information Technology" with a folder called "hp-dorman arc_18071719502154" with a creation date of 7/19/2017. IT staff advised that this is a network directory that commonly stores backups of hard drives. There is suspected evidence on Dorman's computers based on interviews conducted with the previous IT staff. Specifically, they indicated that Dorman would hand them "index" cards for email query lookups on other employees from other departments in Madison County Government. This was outside normal procedures and past practices. In addition, he specifically requested to obtain all emails from the MailStore for the email

account of Frank Miles. It should be noted during Frank Miles' time with the Madison County Government, he held the Elected Office of Madison County Treasurer, which would be beyond the scope and authority of Madison County Administration to review said emails. In addition, Dorman would often have the IT staff copy them to USB drives and external media and/or copy the email files to his desktop computer. It was also learned that Dorman had logged into the county domain network with Lenovo laptop(s). It is further believed that the computers used by Robert Dorman, would still contain data, files and artifacts, which were created, accessed and viewed by Robert Dorman, during the time of the events in question. During the course of interview with IT staff, investigators were informed that Robert Dorman previously had a HP Laptop that he commonly used. Contained in the Tech1 backups under a subdirectory labeled Information Technology is a directory of backup files or backup disk images as it relates to **hp-dorman arc_18071719502154**, which is consistent of belonging to Robert Dorman.

21. Former employee John Doll was interviewed and knew the computer name of "Okra" to be the previous IT director's computer. A search of computer associated to Robert Dorman (redorman) showed that his user account has accessed the computer "Okra." Additionally the computer, "Okra", accessed by Dorman has a Media Access Control (MAC) address of 98:90:96:e4:73:33. Doll stated Timothy Renick chose this name because he was a vegetarian. He told investigators that this computer should still be within Dorman's office.

22. Hulme's computer location was also identified through several different databases which yielded atypical results. Specifically, the computer he was associated to is identified using service tag number ID 55R7KB2 (Associated MAC 18:66: DA: 21:82:CE). This system name AKA service tag was consistently used and associated to an internal IP of 10.0.17.37 from November 3^{0th}, 2017, through December 1^{9th}, 2017; however, on January 4th, 2017, a new IP address of 10.0.14.59 was shown as logging into this computer. This third octet set was recognized by IT staff at being in their office(s). A user name initials of "MCH" was associated to these logins meaning this computer was plugged into an internet IP connection and located in the IT office as recent as of 1/5/2018 10:39 AM. "DEHULME" was seen logging into it from the IT office as recent as of 1/5/2018 3:09:01PM. The initials of "MCH" were recognized to be employee, Matt Huntley. Next, a query was performed on the work order database for this hardware and Hulme. It revealed an issue with the hard drive but details were limited. Also, performing a keyword of "Hulme" across the network yielded a file path of "**Network\tech1\images\County Board**" **containing a folder called "dehulme"** with a creation date of 1/27/2017. It is further believed that the computers previously used by Doug Hulme, would still contain data, files and artifacts, which were created, accessed and viewed by Doug Hulme, during the time of the events in question. As a result of Hulme having administrative access to the MailStore and the fact the MailStore application was installed on Hulme's computer there reason to believe artifacts of emails or email related queries can be recovered from the computer. It should be noted that

according to IT staff, Hulme's account to include administrative access to the MailStore is still active.

23. On January 9, 2018 sometime after 9:00AM, in accordance with a court issued overheard Chris Slusser met with Doug Hulme in the Administrative Offices area of the Madison County Government. The meeting was video and audio recorded. Portions of the audio were distorted due to the nature of the placement of the overheard device. During the conversation Hulme and Slusser are heard discussing emails and how the Hulme has full access to all Madison County emails. Hulme makes mention of how easy it is to query emails. He specifically mentions performing key word searches, which will often populate several hits. Hulme further details on if he searches "fundraiser" he will find other hits on the system. Hulme mentions having access to all of the system. Hulme provides information on how the MailStore works and the functionality of the system. Hulme referenced having information as it related to the system on a Madison County Judge. Rob Dorman's name was also mentioned in the context of the conversation during the conversation about the emails. The overheard corroborated Slusser's previous statements to investigators and the Grand Jury.
24. IT staff advised that the Tech1 Server and associated network directories commonly stores backups drive images or backup user information of hard drives from user computers. IT staff further advised that the Tech1 Server containing the **backup disk image files and backup user files** is not backed up and the data can be easily removed.

25. On January 7, 2018 Matthew Huntley, who worked on Hulme's computer was interviewed. He indicated that he was told by Hulme that he (Hulme) had his android based phone plugged into the computer and it subsequently malfunctioned when he re-booted it. Huntley performed some diagnostic tests on it which yielded a possible corrupt boot sector. Huntley advised that IT technicians commonly make images of Huntley advised that he removed Hulme's defective hard drive, later fully identified as **Toshiba MQ02ABD100H 1TB hard drive, SN: 56MQT57JT**. IT staff told investigators that technicians commonly make disk images and/or backups of computers during the process of replacing computers. Disk images can constitute an exact copy of file structure or a copy of the contents of the disk at the time the image was acquired. commonly referred to a of computers during the process of intended on shipping the defective drive off to Dell for repair, exchange, etc. thereby establishing a relinquishment in ownership. Huntley said the drive is currently at his desk and he would work with authorities to locate and retrieve it. Huntley advised that he then placed a new drive into Hulme's desktop computer and reinstalled a new operating system. On January 8, 2018 at approximately 8:28AM, I met with Huntley and secured the drive, **Toshiba MQ02ABD100H 1TB hard drive, SN: 56MQT57JT**, as evidence pending warrant application.
26. The decision was made to seize the hard drive as a measure of preservation so any possible evidence would not be destroyed. The decision was made based on the following circumstances. The investigation began on January 3rd, 2018; however,

Grand Jury testimony was provided on or about December 21st, 2017. Some investigators were informed of the investigation as early as December 21st, 2017. I believed in good faith evidence would destroyed, lost, or damaged because of our interest in the hard drive. It is unknown at this time if Hulme is aware of this investigation; however, evidence gleaned from his hard drive would substantiate or refute claims made by Slusser that Hulme was bragging about having emails that he may not be legally entitled to possibly in violation of the aforementioned offenses. Due to the fact a limited number of individuals had access to the MailStore, it is believed that Hulme's computer and/or associated images will contain evidence of such.

27. It is my belief that any number of items sought in this affidavit may be found which are stored electronically. There is a fair probability that contraband or instrumentalities of a crime may be found on the digital device(s) based on the following information that is known to me.

Basis for scope to search areas within the digital device

Based on my experience and training as, I know that electronic files can be easily moved from one digital device or electronic storage medium to another. Therefore, electronic files downloaded to or created on one device can be copied on or transferred to any other computer or storage medium at the same location. In addition, based upon my experience and training, I know that searching

computerized information for evidence of crimes often requires investigators to seize most or all computer equipment.

- a. Volume of evidence: Electronic media and storage devices such as cell phones, SD cards, hard disks, CD-ROMs, DVDs, diskettes, tapes and laser disks can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. This may require searching authorities to examine all of the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks to months, depending on the volume of data stored. It would also be impractical to attempt this type of data search on site.
- b. Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert and examiner is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected, or encrypted files. Since computer evidence is vulnerable to inadvertent or intentional modification or destruction (either from external sources or from destructive code embedded in the system such

as a “booby traps”), a controlled environment is essential to its complete and accurate analysis.

23. Imaging and Acquisition, Processing, Analysis and Examination:

- a. Imaging and Acquisition: The reviewing and examination of files acquired from computer hard disks or cellular devices can vary based on the type of “copy” made from the original evidence commonly referred to as a “forensic image”. These images are usually “read only” files that cannot typically be altered and will come in different file formats depending on the type of software used to make the acquisition. Producing a “forensic image” is the most important process in any method. The most preferred method would be to obtain a “full”, “bit by bit”, or “physical image”. This is because it is the least intrusive way to alter or change the data and obtaining a “full, bit by bit and/or physical image” is considered the preferred method. At this point in the process, the data is usually “raw “and unreadable and needs to be processed. Due to rapid technology advances of digital devices, a “full, bit by bit and/or physical image” may not always be able to be performed; therefore, other examination or extractions methods may need to be implemented.
- b. Processing: The type of software that is used to process the forensic image(s) will ultimately parse through the data in an automated manner in which the programmer of the software has intended. The processing phase allows the raw data to be read. The later review of this readable data allows the

examiner to recover artifacts so he/she can parse through the data and interpret the evidence and later present the finding which is referred to as the analysis/examination phase.

- c. Analysis and Examination: The analysis of electronically stored data, whether performed on site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file formats and areas within the processed files. This is similar to looking inside a dresser in furtherance of searching for narcotics. There are several layers and drawers within the dresser and possibly other containers that must be opened. In order to locate the evidence and instrumentalities authorized for seizure by the warrant one must be allowed to browse different file containers and areas because of their various naming conventions and/or locations within the digital device. These containers and areas can commonly be described as “search history, images, communications, videos, calendar, audio, deleted data, encryption, operating system files, emails, documents, and programs” and the individual files they contain. These areas can also include sub categories within them and some of these areas are often intertwined with one another and require the examiner to parse through each area to determine if the artifact(s) is relevant for inculpatory or exculpatory evidence through due diligence. Depending on the type of acquisition and processing performed, it will delineate what the examiner can see from the

extraction. Examiners use various types of examination software. In almost all instances, the forensic examiner is unable to predict the types of data that will populate the viewing gallery during an examination. This also includes the technique of "keyword" searching. This technique and the "containers and areas" described above are further defined and articulated to search based on the following:

- i. Conducting Keyword Searches: A full and comprehensive examination consists of performing electronic "keyword" searches. These "keyword" searches may scan through all electronic storage areas (but sometimes not databases) to determine whether occurrences of language contained in such storage areas exist. These keyword searches are pertinent and are usually related to the subject matter of the investigation. This may require "opening" or reading the first few "pages" or "entries" of such directory, folder, and/or database in order to determine their precise contents. Furthermore, "scanning" storage areas to discover and possibly recover recently deleted data for deliberately hidden files.
- ii. Search History: The search history of a phone and/or computer is pertinent to any investigation to determine possible intent and/or research conducted on a particular topic to either prove or disprove motive. Search history is relevant to any case involving images, videos, location based information for addresses of victim(s), scene(s) of crimes, etc. It is also

intertwined into programs because often times a user will search for certain names within an application or program and these programs will keep track of search history within their own application container. A user also has the ability to interact with any internet based search function on a device. This can be whether it is a 3rd party search engine or search engine native to the device exists. Reviewing of this information contained in the searches on these applications is vital in determining intent, knowledge, and possible motive of a crime.

- iii. Images or Graphic Files: Almost every digital device will contain images. These images can be indicia of many different things. They can contain certain icons of programs that either are installed or were installed on a device which can be instrumentalities of a crime. Images can also have been generated or taken from the same device, which they were found on or a different device. This is important because images contained metadata commonly referred to as EXIF data. This data can contain vital information about when the photo was taken, the location where the photo was taken, and the device which took the photo; therefore, location based information is often intertwined with the examination of images and it is pertinent to examine both entities. Graphic files can exist on a computer device in several different ways. It can exist in its native/raw undeleted form. Graphic files can also exist as a thumbnail which is indicative that

the image may have been resident on certain portions of the device even if the graphic file was deleted or is still resident. Also, graphic files in the form of thumbnails can be generated if a video file is existent or was existent on the device. These video thumbnail images are commonly referred to as thumbnails or preview images.

Moreover, graphic files, video preview files, and/or thumbnails files can be resident in communication messages over many different forums. These forums can include chat messages, instant messages, Multi-Media messages (MMS Messages), application based messaging (also known as app messaging) which can also aid in the investigation. They may also serve as a "contact" photo in an individual's phonebook or contact(s) section. In summary, graphic/image files, video files, location based data, database information and communications are intertwined with one other.

- iv. Communications: With regards to communications, they can exist in a vast array of different forums. Communication commonly exists as emails and application based communications. Certain text communications can be fruits of contraband or instruments of an offense. Accordingly, people often choose different forums to convey their conversations via text messaging. Commonly, the native text messaging application that comes installed on the device can be used; however, numerous other chat platforms also exist. Examples

of these chat applications are Snapchat, Whatsapp, tigertext, etc. The correspondence can be screen captured which is stored in the form of graphic files. Application based communication assists investigators in determining the suspect's intent and / or knowledge of accessing, acquiring or disseminating illegal material. Another component of the communications area is the phonebook/contact section. This section contains names, email address(es), and phone numbers of individuals that the user of the phone has programmed into the phone. It can establish whether or not a suspect knew a victim or had prior contact. It can also contain a "contact photo" of an individual. They are also essential to examine to correlate call logs to compare against other numbers listed for an individual. In summary, call logs and the phonebook/contact list along with the messaging services are all interconnected with one another. Other examples of this would be applications like Facetime on iOS device(s) and various Facebook messenger components that allow phone calls and chat capability.

- v. Videos: Videos and graphic images on a digital device are often related. Almost every digital device will contain videos. These videos can be indicia of many different things. Videos can also have been generated or taken from the same device which they were found on or a different device. This is important because videos contain metadata as well. This data can contain vital information about when

the photo was taken, the location where the photo was taken, and the device which took the photo; therefore, location based information is often intertwined with the examination of images and it is pertinent to examine both entities. Video files can exist on a cell phone or computer device in several different ways. It can exist in its native/raw undeleted form. They can also be generated from different applications. In summary, graphic/image files, video files, location based data, and communications are intertwined with one another.

Another example to how these two entities are intertwined is a function within iOS device(s) referred to as live-video. When a user takes a picture it will actually take a video capture for several seconds thereby making a video and later allowing the user to select a preferred picture within the video frame feed.

- vi. Calendar: A calendar is a component of the phone that is pertinent to any investigation. The calendar will serve a possible timeline for an individual in an investigation whether or not he/she is the suspect, victim, and/or witness to a crime. It can provide information about a probable location during, before, or after a crime. It is also related to the contacts and communications of a cellular device because individuals will often "share" their calendar with one another thereby establishing a nexus to other devices and/or email addresses.

- vii. Audio: Audio files are not limited to music but also encompasses voicemails which are tied to the communication's aspect of devices. They can also be indicative of voice based searches on various forums which can be intertwined to the search history of a device. An example of this would be the Cortana search bar which stores the voice of some searches conducted and it is interlace into the Microsoft Edge browser.
- viii. Deleted data: Deleted data can be relevant to any data within the phone because any type of data can be deleted (e.g. call logs, communications, audio files in the form of voicemails, calendar entries, images, videos, etc.) Deleted files can still reside on the device in other areas depending on how the user accessed the files. The files may be logged in databases associated to when the user accessed the file of interest. The files may be "cached" on the device even through the original file(s) had been deleted. Digital related "caching" is a software component that stores data so future requests for that data can be served faster; the data stored in a cache might be the result of an earlier computation, or the duplicate of data stored elsewhere. Deleted files may be recovered from the forensic image through a process commonly referred to as "data carving". Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital

investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values. If files have been deleted or accessed by alternative applications on the device the analysis of the applications and file structure can potentially recover the file even though the user thought they deleted it from the device. In the event a file is recovered through a cached copy or a carved out of the data, it may be stripped of date and time related metadata or the "date and time" related information to the file from when the file was originally created on the device.

- ix. Encryption: In the context of searches of electronic devices, there is an inherent risk that criminals can easily "hide, mislabel, or manipulate files to conceal criminal activity". This is often done in the form of encryption. This can also include password protected files. Encryption is often difficult to break because the encryption key itself is often encrypted; however, sometimes known passwords stored in plain text is found within the operating system files or other programs that keep the encryption key in plain text. A parallel example to this would be when a locked safe exists in the house; however, the key to the safe is in plain view or found in an area allowed in the search which can easily unlock to combination.

- x. Operating system files: I know through training and experience that Windows based devices and Apple iOS devices commonly keep artifacts of user activity. There may also be backup or shadow copies of user based activity or associated devices actives. They can also contain information of when a program was installed, the frequency of use, etc. This section also logs powering events when a device was powered on or off by a user which can aid in any criminal investigation.
- xi. Emails: Emails serve as a traditional form of communications. They can contain information pertinent to location, images, videos, and contacts shared. Emails are also intertwined into some text messaging techniques for cellular phones and computers. Emails can be backed up in a variety of platforms, to include Personal Storage Table (PST), message format (MSG), text (TXT) format, digital images, and additional storage formats. Backups of emails can commonly be opened and accessed through a variety of programs, leaving potential artifacts within said application or within the file system. In order to determine the origin of an email and/or how it was accessed a full analyses of the drive is required to include; search history, images, communications, videos, audio, deleted data, encryption, operating system files, emails, documents, and programs. The information as it relates to an email can leave any

number of a variety of artifacts on the device. The MailStore can be accessed through a web based portal or through an application based platform. The Madison County Government stores voicemails (audio files) through an email based system.

xii. Documents: Individuals will keep correspondence from others that may be pertinent to an investigation in the forms of notes. They will also keep a list of tasks. An example of this is when people view or collect illegal images. Subjects have been known correspond and/or meet others to share information and materials. They sometimes maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests or activities. Documents come in a variety of platforms to include word documents, spread sheet documents, Portable Document Format (PDF), and a variety of formats which can store text based data. When keyword searches are conducted during examinations it will often receive positive hits in documents, notes, and tasks contained on the digital devices. These hits are essential to be examined.

xiii. Programs: These are software additions to the digital device that may or may not have come a factory installed. Often times users will install additional programs for activities they are involved. These programs have the ability to take photos, share information,

contained location based data, and provide an overall view of the what the user's activity is around him/her. Application based communication assists investigators in determining the suspect's intent and / or knowledge of accessing, acquiring or disseminating illegal material. Another component of programs can include the databases related to the program that store pertinent information. System and application database files commonly store information pertaining to file or user activity to include registry files and/or application based databases or logs. This may provide investigators with how the user obtained, accessed or disseminated said files or contraband. Each system or application can independently store databases related information that the developer programmed into the function of the application. The information contained in the database can provide for the users knowledge, intent and motive as it relates to the files of interest. In fact, most programs installed on a phone or digital device will ask permission to access or utilize other functions of the phone (e.g. device location information, contacts, photos, etc.).

Based on the aforementioned information, it is believed that a relationship to the criminal offenses described within have also established a nexus to all the containers and files named in this request for search warrant for said digital device(s). Thus, it is impossible for a

thorough examination to be conducted without intrusion into other arenas of a hard drive analysis.

Further the Affiant sayeth not.

Det. Sgt. D. K. 321
Affiant

Subscribed and sworn to before me on this 9 day of JAN, 20 18.

Wm D. Schneider
Judge

IN THE CIRCUIT COURT
THIRD JUDICIAL CIRCUIT
MADISON COUNTY, ILLINOIS

18 MR 500/18

FILED

JAN 25 2018

SEARCH WARRANT

CLERK OF CIRCUIT COURT #31
THIRD JUDICIAL CIRCUIT
MADISON COUNTY, ILLINOIS

ALL PEACE OFFICERS OF THE STATE OF ILLINOIS, SPECIAL AGENTS OF THE UNITED STATES GOVERNMENT, AGENTS OF THE FEDERAL BUREAU OF INVESTIGATION, or ANY DESIGNEE DIRECTED FROM A PEACE OFFICER AND/OR FEDERAL SPECIAL AGENT:

This day, **Detective Sergeant Brian Koberna DSN 321**, having subscribed and sworn to Complaint for Search Warrant, I have under oath examined the Complainant, and am satisfied that probable cause exists.

THEREFORE, IN THE NAME OF THE PEOPLE OF THE STATE OF ILLINOIS, I command that you search the following described premise(s) or item(s):

The Madison County Administration building located at 157 N. Main St., Edwardsville, IL 62025 to specifically include the backup disk image files and backup user files located on a network server, Network\tech1\images\Information Technology, with a folder called "hp-dorman arc_18071719502154" and Network\tech1\images\County Board, with a folder called "dehulme" Madison County Computer network/server located with the Informational technology (IT) Department

and there to seize, secure, analyze, tabulate and make return thereof according to law, the following property or things:

respect to the above seized backup disk image files and backup user files to analyze any or all search history, images, communications, videos, calendar, audio, email, deleted data, encryption, operating system files, emails, documents, and programs

or things which have been used in the commission of or which may constitute evidence of the offense(s) in connection with which this warrant is issued, being **720 ILCS 5/17-51 Computer Tampering, 720 ILCS 5/33-1 Bribery, 720 ILCS 5/14 Violation of Article 14:Eavesdropping Statue and 720 ILCS 5/33-3 Official Misconduct.**

The following facts have been sworn to by Complainant in support of the issuance of this Warrant. (See attached Complaint for Search Warrant, which is made a part of this Search Warrant by incorporation and express reference).

ISSUED AT MADISON COUNTY, ILLINOIS, UNDER MY HAND THIS 9 DAY
OF JAN, 2018 AT THE HOUR OF 4:18 pm


JUDGE

18 MR 500118

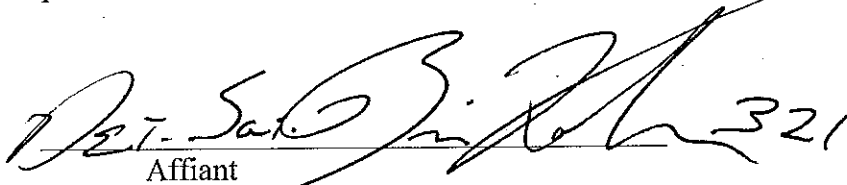
RETURN

STATE OF ILLINOIS)
) SS
COUNTY OF MADISON)

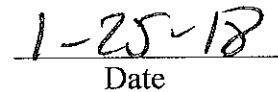
I, Sgt. Brian Koberna DSN 321 via designee, have executed the within Search Warrant by searching and seizing the within described data from the Madison County network server located at 157 N. Main St., Edwardsville, Illinois, this 10th day of January, 2018, at the hour of 8:30 a.m., and seizing the following property, to-wit:

Backup User files under the path of Network\tech1\images\Information Technology with a folder called "hp-dorman arc_18071719502154" and Network\tech1\images\County Board with a folder called "dehulme".

and by giving a duplicate copy of the Search Warrant to Madison County Board Chairman, Kurt Prenzler, from whom the property was seized, all in accordance with the provisions of Article 8 of the Code of Criminal Procedure of 1963.


Affiant


Judge


Date