DISTRICT COURT. STATE OF WASHINGTON, COUNTY OF SPOKANE

FILED
MAY 19 2009
SPOKANE COUNTY DISTRICT COURT

STATE OF WASHINGTON)
)
Plaintiff,) NO. 07-356136

vs SEARCH WARRANT -

Brian L. Moore w/m 5/8/66) RETURN, INVENTORY & RECEIPT
)
)
Defendant.

1. DATE AND TIME OF EXECUTION OF SEARCH WARRANT:

7/15/09 0900

2. PREMISES AND FILES SEARCHED:

Computers - HP laptop SN. CNF8144Q33- H/P SN. 2CE52303XT
Generic CPU, SN.- 050007213 - Dell CPU - 721DR11

3. PERSONS PRESENT DURING EXECUTION OF SEARCH WARRANT:

Kip Hollenbeck Ty Snider

4. INVENTORY LIST OF INFORMATION SEIZED: Search of computer files - In process

(SEE ATTACHED SEARCH WARRANT PROPERTY SHEET ADDITIONAL)

5. METHOD OF ENTRY: N/A

Kip Hollenbeck
Seizing Officer

COPY OF RECEIPT RECEIVED:

N/A
Recipient

CERTIFICATE OF RETURNEE:

I certify that on this 19th day of May, ~~19~~ 2009, at 3:09, (AM/PM) the above captioned search warrant and written inventory were returned to the District Court Judge who signed the search warrant by delivery to the Spokane County District Court Clerk.

SPD NO. 07-356136

IN THE DISTRICT COURT OF THE STATE OF WASHINGTON

IN AND FOR THE COUNTY OF SPOKANE

STATE OF WASHINGTON, Plaintiff,	)	
v.	)	No.
Brian L. Moore, WM, 5/08/66	)	
	)	AFFIDAVIT FOR SEARCH WARRANT
Defendant.	)	FOR EVIDENCE OF:

First Degree Murder

(Name of Felony Herein)

Detective Kip Hollenbeck #240, being first duly sworn on oath, deposes and says:

(1) Background of affiant:

Your affiant was previously employed as a police officer by the City of Ellensburg, WA from March 1987 through September 1989. Your affiant currently holds the rank of detective with the Spokane Police Department and is assigned to the Major Crimes Unit.

Your affiant has been trained and continuously educated in all aspects of law enforcement including murder and robbery investigations.

During the course of the affiant's law enforcement career, he has investigated to successful conclusion several homicide cases, as well as crimes against persons including child abuse, assaults, robbery, burglary, all forms of theft, domestic violence and rape. Affiant as prepared and executed numerous search warrants in both patrol and investigative capacities.

(2) Crime being investigated:

First Degree Murder

(3) Circumstances supporting probable cause:

On 4/27/09, Spokane County Deputy Prosecuting Attorney Mark Cipolla charged Brian Moore with one count of First Degree Murder and one count of First Degree Conspiracy to Commit Murder.

On 4/27/09 Brian Moore was arrested in Anaheim, CA on the Spokane warrant for First Degree Murder and First Degree Conspiracy to Commit Murder.

On 4/27/09 investigators with the Spokane Police Department and the Anaheim Police Department served a California Superior Court search warrant at Brian Moore's residence at 2100 E. Howell, Ave., Suite #207 in Anaheim, CA. During the execution of that search warrant, four computers, two lap tops and two PC computers were seized as evidence. Based on the above information, your affiant believes probable cause exists to search these computers for evidence related to this investigation.

On 4/27/09 private investigator Ted Pulver provided Det. Hill with a zip drive that had previously been given to Pulver by Brian Moore. The contents of this zip drive allegedly contain a conversation between Brian Moore and state's witness Michael Kendall. Moore later filed an alleged extortion complaint against Kendall in an attempt to prevent Kendall from cooperating with the police investigation. Your affiant believes probable cause exists to search this zip drive to examine the contents for any evidence related to this investigation.

Based upon your affiant's knowledge, training and experience, and that of the Spokane Police Department's Computer Forensic Unit, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily-available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear, rather, that data remains on the hard drive until it is overwritten by

new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space (space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block or storage space) for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The Internet browser (i.e. Microsoft Internet Explorer) typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. As a result, the ability to retrieve evidence of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity and computer habits.

The purpose of this warrant is twofold. First, to search and seize computer evidence (hardware, software, storage devices and peripheral devices) related to the crime of First Degree Murder.

> **Computer Hardware** is the physical equipment of a computer. Computer hardware consists of the components that can be physically handled. The function of these components is typically divided into three main categories: input, output, and storage. Computer hardware consists of all equipment, which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar data. Hardware includes file servers, desktop computers, laptop computers, mainframe computers, hard drives, peripheral devices and data storage devices.
>
> **Computer Software** is a general term used to describe a collection of computer programs, procedures and documentation that perform some task on a computer system. The term includes application software such as word processors which perform productive tasks for users, system software such as operating systems, which interface with hardware to provide the necessary services for application software.
>
> **Peripheral Device** is any computer hardware device that can attach to a computer in order to expand its functionality. Some of the more common peripheral devices are printers, scanners, disk drives, tape drives, microphones, speakers, DVD and/or CD players, flash card readers and cameras.
>
> **Data Storage Device** is a device for recording or storing information (data). Data Storage Devices include hard drives, Zip Disks, DVDs, compact disks, flash memory devices and floppy disks.

The second purpose is to examine and analyze the computer related digital evidence after the items are seized to collect the evidence contained there-in. A commissioned

officer of the Spokane Police Department will make forensic copies of the information contained on the defendant's computer related digital storage devices.

Based upon your affiant's knowledge, training and experience, your affiant knows that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals). This is true because of the following:

- Transferability. Digital files are easily transferred from one device to another. For example, images taken on a digital camera are typically downloaded to a computer or other digital storage device (i.e. Sony PlayStation). These files can then be transferred to other digital storage device (i.e. USB drive, CD, DVD, etc.).

Based upon your affiant's knowledge, training and experience, your affiant also knows that examining and analyzing electronic storage devices requires a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

- The volume of evidence. Computer storage devices (hard drives, USB drives, diskettes, tapes, digital video disks) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. In order to identify files, which may be concealing evidence and / or instrumentalities of the crime, a computer forensic examiner will have to examine all the stored data. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

- Technical requirements. Searching computer systems for criminal evidence is a highly technical process requiring specialized skills 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 is qualified to analyze the system and its data. In any event, however, 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 extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and/or from destructive code imbedded in the system as a "booby traps), a controlled environment is essential to its complete and accurate analysis.

The forensic copies will be made by the Spokane Police Department, using programs developed for performing data acquisition and analysis. One program, called "Encase" from Guidance Software, will make a copy or forensic image of the Defendant's computer. It is completely non-invasive so that the original computer evidence is never

changed. EnCase authenticates and verifies all copies of the original evidence to ensure that the integrity of the evidence is protected and that it can meet foundation and authentication challenges.

Investigators can then perform an analysis upon the copied evidence without any chance of altering the original evidence. Then data searching procedures can recover hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and/or from destructive code imbedded in the system), a controlled environment is essential to its complete and accurate analysis. Due to the capability of computers and computer related storage devices to store a large number of files, this process is often slow. As a result, it could be several weeks for the forensics examination to be completed.

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 facts that I believe are necessary to establish probable cause to believe that evidence of the crime of First Degree Murder is presently located within the aforementioned items and location.

WHEREFORE, affiant requests that a Search Warrant issue for the purpose of searching:

(x) COMPUTERS, described as follows:

1. Hewlett Packard lap top, serial # CNF8144Q33
2. Hewlett Packard Pavillion lap top, serial # 2CE52303XT
3. Generic CPU, serial #050007213
4. Dell CPU, serial # 721DR11
5. Zip drive unit

( ) VEHICLE(S), described as follows:

( ) PERSON(S), described as follows:

to seize (list property to be named in Search Warrant):

Forensic copies of the data contained with

1. Hewlett Packard lap top, serial # CNF8144Q33
2. Hewlett Packard Pavillion lap top, serial # 2CE52303XT
3. Generic CPU, serial #050007213
4. Dell CPU, serial # 721DR11
5. Zip drive unit

Affiant Police Officer

SUBSCRIBED AND SWORN TO before me this 14th day of May, 2009.

Judge, Spokane County District Court

IN THE DISTRICT COURT OF THE STATE OF WASHINGTON

IN AND FOR THE COUNTY OF SPOKANE

STATE OF WASHINGTON, Plaintiff,	)	
v.	)	No.
Brian L. Moore, WM, 5/08/66	)	
Defendant.	)	

TO ANY PEACE OFFICER OF THE STATE OF WASHINGTON:

WHEREAS, Detective Kip Hollenbeck #240, has this day signed an affidavit on oath before the undersigned, one of the District Court Judges in and for the County of Spokane that he believes that a felony has been or is being committed, to wit:

First Degree Murder, and that evidence of said felony is located:

(x) COMPUTERS, described as follows:

1. Hewlett Packard lap top, serial # CNF8144Q33
2. Hewlett Packard Pavillion lap top, serial # 2CE52303XT
3. Generic CPU, serial #050007213
4. Dell CPU, serial # 721DR11
5. Zip drive unit

( ) upon or in the vehicle(s) described as follows:

( ) on the following person(s):

WHEREAS, the undersigned finds that there is probable cause to believe said facts contained in the affidavit to be true:

THEREFORE, in the name of the State of Washington, you are commanded within ___x___ days (not to exceed ten [10] days) to:

(x) enter into the aforementioned computers

(x) enter the aforementioned vehicle(s)

( ) detain the aforementioned person(s)

with the necessary and proper assistance, and diligently search for and seize:

Forensic copies of the data contained with

1. Hewlett Packard lap top, serial # CNF8144Q33
2. Hewlett Packard Pavillion lap top, serial # 2CE52303XT
3. Generic CPU, serial #050007213
4. Dell CPU, serial # 721DR11
5. Zip drive unit

and make a return of said warrant promptly, no later than three (3) days from the execution of the Search Warrant to the undersigned Judge, showing all acts and things done thereunder, with a written inventory of any properties taken, and the name of the person(s) in whose possession the same were found, if any, and if no person(s) be found in the possession of said articles, the inventory shall so state.

The peace officer taking property under the warrant shall give to the person from whom or from whose premises the property is taken a copy of the warrant and a receipt for the property taken. If no such person is present, the officer may post a copy of the Search Warrant and Receipt.

The inventory shall be made in the presence of the person from whose possession or premises the property is taken, or in the presence of at least one (1) person other than the seizing officer. This person may be another officer.

5/14/09 3:15 pm _____

Date/Time

Judge, Spokane County District Court

The subject of the search may request that a search warrant and accompanying papers not be filed. Unless there is an objection within seven (7) days after the execution of the Search Warrant, the Search Warrant and all accompanying papers will be filed and become available for public inspection.

The State objects to the filing of this Search Warrant and accompanying papers:

( ) YES (x) NO