Case Number: 00000-00

## **AFFIDAVIT FOR SEARCH WARRANT**

STATE OF MISSOURI	)
	) ss
COUNTY OF CLAY	)

I, <u>Det. Sqt.John Doe</u>, affiant and applicant herein, being duly sworn, appears now before the undersigned Judge authorized to issue Warrants in criminal cases and makes this Affidavit in support of the issuance of a Search Warrant.

FURTHER, for the purpose of showing probable cause that a crime has been or is being committed and that the above described items exist and are located at the above described place, Affiant states the following facts which he has reasonable grounds to believe and does believe to be true; to wit:

My name is John Doe I have been employed at the Clay County Sheriff's Department for 17 years. I am currently assigned as a Det. Sgt. with the Clay County Sheriff's Department.

On June 30, 2009, at approximately 11:05 P.M., Overland Park Police Officers were dispatched to 1313 Mockingbird Lane, Overland Park, Johnson County, KS on a report of disturbance in progress.

Upon arrival, Overland Park Police Officers spoke with Deak Roose and Shelly Smith. Shelly Smith stated she was using the home computer when she came upon several files with explict file names consistent with child pornography. She confronted her live-in boyfriend, Deak Roose about the files. During the confrontation, Roose struck her in the head. Roose was arrested for battery and transported. Smith turned off the laptop and gave it to the arresting officers.

On July 1, 2009, Detective Joe Friday interviewed Deak Roose. Roose denied knowledge of the child pornographic files and stated he had no idea how they would have been on the computer.

During the search of the residence, a Blue Dell Inspiron laptop computer (Model: 6500U, Serial Number: BR549) was located in the basement office.

The laptop computer and power cord were packaged as evidence and transported to the Heart of America Regional Computer Forensics Laboratory (4150 N. Mulberry Drive, Suite 250, Kansas City, Clay County, Missouri) on June

2, 2009 by Detective Irving Smith where it was submitted for storage in the laboratory's evidence control facility.

Based on the affiant's knowledge, training, and experience, the affiant knows that 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 forensics 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 - that is, in 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 of 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 browser 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. Thus, the ability to retrieve residue 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 search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password protected or encrypted files. Searches and seizures of evidence from computer systems commonly require the seizure of all computer items to be processed by a qualified computer expert in a laboratory or other controlled environment. The high volume of the contents and intentional concealment of criminal activity through random ordering and deceptive file names requires search authorities to examine all the stored data. This sorting process may take weeks or months depending on the volume of the data stored.

A forensic examination of the computer is needed to check for other file variations, which may be erased, hidden, encrypted, compressed, or password protected.

Page 2 of 2