CHAMPAIGN POLICE DEPARTMENT

POLICY and PROCEDURE

POLICY NUMBER: 43.2

SUBJECT: HIGH TECHNOLOGY CRIME UNIT

EFFECTIVE DATE: 2/01/13
REVISED DATE:

REFERENCE ILEAP:

INDEX AS:

43.2.1 BACKGROUND
43.2.2 PROCEDURES
43.2.3 CASES INVOLVING CHILD PORNOGRAPHY

PURPOSE:

The Champaign Police Department is committed to serving all segments of the public in the highest possible capacity. To accomplish that mission, specialized training has been provided in the areas of digital evidence and online investigations for the investigation of crimes that are high-tech in nature. This policy will provide guidelines regarding the investigation, seizure, and subsequent analysis of digital evidence.

DEFINITIONS:

Chain of Evidence: The continuity of custody of materials and other items collected as evidence.

Computer Equipment: The physical components of a computer system. Also referred to as hardware.

Software: Programs that have been or can be installed in a computer.

Storage Media: Digital storage devices that include but may not be limited to computer diskettes, flash memory cards, Universal Serial Bus (USB) thumb drives, compact disks (CD/DVD), and hard disk drives used to store data.

High Technology Crime Unit (HTCU): A specialized unit consisting of officers designated by Investigations supervisors who are trained to investigate crimes involving the use of the Internet and/or digital devices.

POLICY:

43.2.1 BACKGROUND

A. The Champaign Police Department recognizes that digital evidence may present itself in many forms. Various crimes are committed with electronic devices such as computers, cell phones, gaming systems, tablet readers, and media centers. It shall be the policy of the Champaign Police Department to proactively investigate and prosecute computer and other high-tech related crimes.

43.2.2 PROCEDURES

A. In light of the inherently fragile nature of computer data, it is imperative that proper care be afforded to electronic storage media, during both seizure and analysis. Improper attempts to view computer data will result in alterations to the data, thereby potentially corrupting evidentiary material. The integrity of the computer system and/or data is preserved through the use of personnel who have been specifically trained to perform computer seizures and subsequent analysis.

1. When officers become aware or suspect that computer equipment, storage media, software, or other device capable of storing data in an electronic format may contain evidence of criminal activity, they shall:

   a. Immediately take the action(s) necessary to prevent the removal or alteration of such evidence.

   b. Prevent the removal, shut down, or start-up of computer equipment.

   c. Prevent the computer equipment from connecting to or disconnecting from a power source, telephone line, or other computer or peripheral equipment.

   d. Prevent the removal, destruction, or alteration of computer storage media and software.

   e. Protect the computer equipment, storage media, software, or other device capable of storing data in an electronic format free from magnetic fields and strong radio frequency signals such as those that may be found in the trunks of vehicles with trunk mounted radio equipment.

   f. Make proper notifications to command staff in cases involving serious felonies and/or child abduction.

2. Search of computer equipment, storage media, software, and other devices capable of storing data in electronic format.

   a. Computer equipment, storage media, software or other devices capable of storing data in an electronic format cannot be searched without a search warrant or the consent of the owner.

   b. The search of computer equipment, storage media, software, or other devices capable of storing data in an electronic format will be

conducted only by a person specifically trained in computer forensics. This computer forensic training will be of a type and from a source authorized by an Investigations Division supervisor.

B. The HTCU may also conduct forensic analysis of computer systems, networked computer systems, electronic recording and storage devices, and electronic storage media seized by outside agencies where the offense committed affects the citizens of the County of Champaign or when otherwise authorized by the Chief of Police.

C. Due to the type of work that is conducted in the HTCU, it is imperative that physical security be maintained in and around the lab facility. Personnel in the lab are involved in the investigation of criminal activity and handle the processing of original evidence involved in criminal cases. Therefore, it is necessary to restrict areas to HTCU personnel only unless escorted by HTCU personnel. The lab will be considered a restricted access area. A sign-in log shall be maintained to document the entry of any non-HTCU member into the secure computer forensics lab.

D. Due to the length of time that may be required for a Computer Forensic Examiner to image and examine digital evidence, it is inevitable that evidence will be left in the secure computer forensic laboratory while it is actively being worked on. The computer forensic laboratory is a secured and restricted area, with very limited access. Only members of the HTCU and the Investigations Commander have access to this area. Evidence may be stored in the lab on a temporary basis until it is no longer needed. However, as soon as the original evidence is no longer needed, it shall either be signed back into the Evidence Room or, when appropriate, released. All original evidence and hardware will be maintained in the Evidence Room for storage.

E. All forensic images created during the examination of digital evidence will be maintained in the secure computer forensic laboratory in a locked evidence storage area if saved onto DVD's, CD's, or other media. If the forensic images are too large to be placed on media it will be stored on external hard drives or the network attached storage within the secure computer forensic laboratory.

F. The Computer Forensic Examiner (CFE) shall produce a report detailing the work done in each case. This report may be different than a standard Champaign Police Department Report, and can be written in a format chosen by the Forensic Computer Examiner. At the conclusion of forensic examinations the examiner will provide the original case agent with the report and copies of digital images recovered. This information may be provided to the case agent via printed casebook or CD/DVD. Further restriction of case materials may occur in cases involving child pornography in accordance with 720 ILCS 5/11-20.1.

43.3.3 CASES INVOLVING CHILD PORNOGRAPHY

A. During Champaign Police Department investigations where images possibly depicting Child Pornography are discovered, employees shall take the following steps to ensure that there is no accidental distribution or unnecessary reproduction of the images.

1. The HTCU will maintain the original evidence as required by Champaign Police Department policy. Upon completion of the examination, the original evidence will be securely stored within the secure computer forensic laboratory.

2. If the images of child pornography are needed for court or grand jury, the HTCU will only supply investigators with the number of images necessary to obtain the desired outcome in the proceeding. If the images are printed, they will be sealed in an envelope with evidence tape, clearly marked as child pornography, and signed out.

3. If the HTCU Supervisor deems it appropriate, images of child pornography may be electronically duplicated for the purposes of sending them to the National Center for Missing and Exploited Children, the FBI Innocent Images program, the Department of Homeland Security, and/or Immigration and Customs Enforcement.

4. Any law enforcement representative, investigator, or prosecuting attorney that is provided with copies of child pornography for prosecutorial purposes is responsible for the destruction of such images at the conclusion of prosecution. Proper destruction shall include shredding printed images and/or destroying CD/DVD copies.

5. Upon request from the prosecuting attorney, HTCU personnel will produce a forensic image of digital evidence containing suspected child pornography for review by a defense attorney or defense expert. The exam shall take place at the Champaign Police Department in the presence of HTCU personnel. At no time will suspects be allowed access into the Champaign Police Department secure computer forensic laboratory during the review of derivative evidence containing suspect child pornography.

B. If the HTCU searches a computer system and/or any electronic media that contains suspected child pornography for an outside agency, the HTCU will adhere to the following requirements:

1. The HTCU will retain a copy of the case file, images, and archives. The material will be stored in the secured areas of the secure computer forensic laboratory.

2. The examiner will return the original computer and original storage media to the outside agency for safekeeping. The outside agency will be responsible for maintaining the integrity of the original evidence once it is returned to them.

3. The HTCU will provide to the submitting agency or investigator a case report that includes the suspected child pornography files in electronic format.

4. If the HTCU Supervisor deems it appropriate, images of child pornography may be

electronically duplicated for the purposes of sending them to the National Center for Missing and Exploited Children, the FBI Innocent Images program, the Department of Homeland Security, and/or Immigration and Customs Enforcement.

5. The HTCU may prepare presentations and other material for court room testimony as needed. The HTCU shall maintain custody of any presentations that contain suspected child pornography files until the conclusion of trial and/or other proceedings. Once the case is adjudicated and evidence is allowed to be destroyed per the prosecutor, all presentations containing child pornography will be properly destroyed.