Digital Forensics

Eff. Date 12/13/2017

Purpose

Enhance the capabilities of Madison Police Department (MPD) personnel in the investigation and prosecution of crimes that involve the use of computers, tablets, cellular phones or other data storage devices.

Goals

1. Properly investigate and assist in the prosecution of cases involving digital evidence.
2. Preserve the integrity of seized digital evidence.
3. Provide expert testimony in court.
4. Act as an educational and training resource for the MPD and the community.

Function

The function of computer forensics includes the investigation of crimes committed involving the use of computers, cellular phones and other data storage devices which may include:

1. Use of electronic devices to commit or facilitate a crime.
2. Any crime outlined in Wisconsin State Statute 943.70 or computer crimes defined by federal code.
3. Perform forensic analysis of digital evidence in felony cases where evidence or information pertinent to an investigation may be stored.
4. Provide technical assistance and guidance in the proper safeguarding and collection of evidence stored in electronic form.

Collection of Devices with Digital Evidence

DESKTOP COMPUTERS

If the computer is shut down, **do not** turn it on. If the computer is powered up, **do not** shut it down. Check the monitor to determine if there is any information that may require photographic documentation and request an investigator for photos if necessary. Unplug the power cable from the rear of the computer, **not from the wall outlet.** Collect the computer tower. There is no need to collect the power cable **unless** the computer is an Apple product. Please collect the power cable for all Apple computers.

LAPTOP COMPUTERS

If the laptop is shut down, **do not** turn it on. If the laptop is powered up, **do not** shut it down. Check the screen to determine if there is any information that may require photographic documentation and request an investigator for photos if necessary. Unplug the power cable from the rear of the computer, **not from the wall outlet.** If the laptop stays powered on after the cable is removed, remove the laptop battery, if possible. If not, close the laptop and leave it powered on. Collect the laptop computer and the power cable for all laptops.

CELL PHONES / TABLETS / MOBILE DEVICES

Once it is determined that the device will require examination, **do not** allow anyone other than L.E. personnel to handle or manipulate the device. If the device is shut down, **do not** turn it on. If the device is powered up, shut it down. Collect the device. If the device is going to be examined on consent, complete the "Consent to Search Cell Phone" form and have the cell phone owner sign the form. Do not forget to ask if the phone has a pass code security lock and indicate the pass code number or pattern on the consent form.

THE HANDLING OF DIGITAL DATA INVOLVING KNOWN OR SUSPECTED CHILD PORNOGRAPHY:

When MPD staff comes across evidence that includes known or suspected child pornography extreme measures must be taken to ensure that this evidence is safely maintained and stored so that it can never be viewed outside of the official scope of the investigation. MPD staff shall also follow federal legislation regarding child pornography prevention, (The Adam Walsh Child Protection and safety act, HR-4472) and Section 3509 of title 18, United States code:

‘‘(m) PROHIBITION ON REPRODUCTION OF CHILD PORNOGRAPHY.— ‘‘(1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.”

‘‘(2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.”

MPD personnel shall adhere to the following operating procedures:

1) MPD personnel not assigned to the Computer Forensics Shared Resources Partnership office (S.R.P) shall never copy or reproduce in any manner items that contain known or suspected child pornography. If MPD investigative personnel, prosecuting attorney’s staff or attorneys or subject matter experts for the defense need to view the material for investigative or trial preparation purposes, arrangements shall be made with the computer forensic investigators assigned to the S.R.P. for viewing to take place in the S.R.P. office with all of the parties present.

2) MPD personnel assigned to the S.R.P. may copy or reproduce and distribute items that contain known or suspected child pornography only at the request of a government agency or for submission to a government agency such as the National Center for Missing and Exploited Children (NCMEC). In such situations the copied material must be delivered by MPD personnel directly to a government agent or delivered in the manner directed by the agency’s submission guidelines.

3) If MPD personnel not assigned to the S.R.P. receive evidence of known or suspected child pornography during the course of an investigation that evidence should be clearly identified as child pornography when packaged and entered into the MPD property system. Digital files such as images and videos should be placed on digital media and labeled clearly on the digital media “CHILD PORNOGRAPHY DO NOT DUPLICATE.”

Investigation

During the course of their investigation, MPD personnel are strongly discouraged from interacting directly (or allowing victims or witnesses to do so) with computers or other electronic devices that will subsequently be seized as digital evidence, unless they have been specifically trained to do so or there are exigent circumstances requiring such interaction. All activities on a computer or cell phone will be reflected in a forensic examination, and interacting with the device may overwrite or alter digital evidence or otherwise complicate a forensic examination. If it is necessary to interact with the digital evidence, document the date, time and activity involved. All examination, retrieval and analysis of digital evidence is to be done by FSU forensics examiners unless otherwise authorized by command staff.

Transport all devices to a district property intake room and package the item in the manner described in the Evidence Packaging Manual. If the device is going to be transported and released directly to a forensic examiner, the device must have an assigned property tag number prior to the examiner taking custody of the device.

Examination and Analysis of Electronic Evidence

EVIDENCE INTAKE

1. All evidence submitted to computer forensics must have a property tag and must be accompanied by an electronic lab request.
2. The forensic examiner will verify and document by description, serial number and condition, any evidence submitted.
3. The forensic examiner will ensure the legal authority for the search of the evidence is in place and documented; a complete copy of the search warrant or consent form shall be submitted during intake.

PRESERVATION OF EVIDENCE

1. Digital evidence in the custody of computer forensic examiners will be handled in a manner consistent with the preservation of evidence.
2. Computer forensic examiners shall ensure the chain of custody of any evidence submitted for forensic examination is maintained and documented during the examination process. Evidence will be properly secured while in the custody of computer forensic examiners.

DIGITAL EVIDENCE ACQUISITION

1. Whenever possible, write-blocking tools are to be used during the acquisition of forensic images to prevent original evidence from being modified.
2. All analysis (beyond a forensic preview using write-blocking tools) shall be conducted using a forensic copy of the drive. In some circumstances, including the acquisition of data from mobile devices and solid state hard drives, changes to the original evidence may be unavoidable due to the nature of these devices.
3. Forensic copies shall be obtained using hardware and software specifically designed to capture a forensic copy of the original media. When it is not possible to obtain a validation hash, the computer forensic examiner will document the circumstances in their report.
4. All items may not need to be forensically imaged provided the media has been previewed and no evidence was found. Lack of a forensic copy will be documented in the examiner's report.

ARCHIVING OF EVIDENCE

All forensic image files containing data of evidentiary value shall be archived. Archived media shall be maintained with the same level of security as the original evidence.

RELEASE OF EVIDENCE

Evidence released from computer forensic examiners will be done in accordance with MPD policies. No media shall be released from law enforcement custody which contains contraband (child pornography).[1]

Prosecution

The case detective shall provide direction to the forensic examiner regarding the preparation and presentation of electronic evidence throughout the prosecution process.

The forensic examiner shall assist in the presentation and preparation of digital evidence for court to include training and an explanation of the findings to the assigned District Attorney.

Regarding release of information as part of the discovery process:

[1] Any evidence recovered during a child pornography investigation should be property tagged and placed in evidence–no photocopies of any images, emails, etc. should be sent to Records as attachments.

1. The forensic examiner shall, at the direction of the lead investigator, prepare evidence to be released or presented to the defense (copies of media, evidence files, EnCase reports, etc.).
2. The forensic examiner shall coordinate with the case detective regarding access or release of evidence and other information to the defense.
3. Contraband, child pornography images, or 3rd party information in any format, written or electronic, shall not be released to the defense without a valid court order. Access to this type of data, or forensic examination of the evidence by the defense, can be arranged by appointment through the forensic examiner.

Reporting

MPD personnel shall document all actions and observations in regard to the handling of computer or electronic evidence, consistent with MPD procedures relating to reporting, such as:

1. Collection of computers and electronic evidence.
2. Any specific actions related to interaction with digital evidence.
3. Chain of custody.

Original SOP: 02/25/2015
(Revised: 01/19/2017, 12/13/2017)