COLLECTION OF DIGITAL EVIDENCE

INDEX CODE: 1831
EFFECTIVE DATE: 07-01-23

Contents

I. POLICY

It is the policy of the Anne Arundel County Police Department to preserve, collect, and examine any computer related or digital evidence linked to criminal activity.

II. DEFINITIONS

A. Computer Forensic Examiner

An investigator specifically trained in computer seizures and with forensic software to conduct analysis of computer data for the purpose of investigating criminal violations of law where computer systems are used as instruments in the commission of crimes, or the subject of a crime.

B. Computer Seizure Specialist

An employee specifically trained to seize computers and related equipment during criminal investigations.

C. Digital Evidence

Digital evidence, also known as electronic evidence, is any probative information stored, in binary form, or transmitted in digital form that a party to a court case may use at trial.

Examples of digital evidence include, but are not limited to, e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

Examples of where digital evidence is found include, but are not limited to, hard drives, floppy drives, Zip disks, Jaz disks, Flash Memory cards, magnetic tapes, cellular telephones, Personal Data Assistants (PDA) and any memory developed for the storage of electronic data or information.

III. RESPONSIBILITIES

The Criminal Investigation Division, Economic Crimes Section, Economic Crimes Unit, Digital Forensic Lab has been established to provide specially trained examiners to conduct forensic examination and evidence recovery from collected items that contain digital evidence.

The Computer Seizure Specialist, if available, conducts collection of computer system components that contain potential evidence in the field.

The investigating detective, officer, or on scene supervisor is responsible for determining probable cause if the item or computer is subject to seizure. All rules of search and seizure apply to seizures of computer and digital evidence. Digital evidence can easily be destroyed so the application of the "exigent circumstances" exception may apply in some cases to secure computers and digital evidence to prevent destruction of said evidence. If there are any questions related to the seizure of computer or other digital evidence, the State's Attorney's Office and/or Digital Forensics Lab personnel should be consulted.

NOTE: As it is likely to cause damage or modify stored data, **under no circumstances** will employees (including Computer Seizure Specialists) access or review data on a seized computer system or review data on media to be seized. Only Computer Forensic Examiners, or other approved examiners, may conduct physical examinations on computer systems and/or storage media.

IV. COLLECTION METHODS

NOTE: When computers are seized that have not been used as instruments in committing crimes, they shall be treated as routine evidence. The following procedures apply only when data stored on computer equipment is being sought as evidence during an investigation.

A. The items collected are evidence and as such should be collected with great care to preserve the item for later use in your investigation or subsequent criminal proceeding. Chain of custody must be documented as per Index Code 1203, Section VI.

B. Suspects or other persons will not be allowed to touch or be in close proximity to the computer, or come into contact with a power supply cut off switch (including wall sockets, light switches, breaker panels, etc.). Seizing personnel should be aware that computers may be equipped with destructive software or other defense schemes.

C. Utilize the On/Off Rule. If the device is 'on' do not turn it off because this could enable a 'lock-out' feature or delete data from a computer system. If the device is 'off' do not turn it on because this could change the evidence. When in doubt (stand-alone home computer) – just pull the plug out. Pull the plug out from the rear of the device – not the wall. Remove the battery from laptop computers and collect the power adapters.

D. Under no circumstances should any personnel attempt to 'look around' in the file structure of a computer to see if any evidence is present. Do not attempt to copy out any files to removable media such as floppy disks or CD-R disks. Only trained forensics examiners conduct evidence recovery.

E. Fingerprint processing, **if needed**, can be conducted on the external parts of a computer system before collection at a crime scene.

V. SEIZING A STAND-ALONE HOME COMPUTER

There are three basic scenarios. Photograph the computer system in place. Take overall, medium, and specific pictures of the front and rear of the machine. Note connections at the rear. Look around the monitor and desk for any passwords, IP addresses, email addresses and note them. Take medium and close-up pictures of these passwords if possible.

A. Scenario #1: The computer is Off or in Sleep mode. First, take pictures of the system front and rear. Second, turn on power to the monitor only. Third, move the mouse only and watch for screen activity. If there is none, press the space bar only one time and watch for screen activity. If the monitor does not display a screen, pull the plug from the rear. If you see screen activity, photograph and take notes of what you see. If you see a 'chat program' you may see a screen name or e-mail address – photograph and note this information. Note other connections and unplug from the rear. Collect and package as needed.

B. Scenario #2: The computer is On and the monitor is in Screen Saver mode. First, take pictures front and rear. Second, move the mouse only. If there is no on screen activity, press the space bar only. Take photographs of the screen and note what you see with special attention to any 'chat program' indicating a screen name or e-mail address. Pull the plug, collect and package as needed.

C. Scenario #3: The computer is On and work product is on the screen. Take photographs of what is on the screen and make a note of any programs that are running with special attention to any 'chat program' indicating a screen name or e-mail address. Pull the plug, note connections and package as needed.

NOTE: When dealing with an Apple-Macintosh OS 7 through 9, the power plug can be pulled from the rear such as in a Windows-based PC. However, when dealing with OS X and 'file vault' is engaged, do not pull the power. Attempting to turn off or disengage 'file vault' or the home directory where user data is stored could cause permanent loss due to file encryption. Contact the Digital Forensics Lab for assistance if needed.

VI. SEIZING A BUSINESS NETWORKED COMPUTER

Contact the Digital Forensics Lab prior to any Search Warrant execution at a business. If practical, give at least one weeks notice to allow for preparation.

Prior to the warrant execution, attempt to obtain as much intelligence as possible about the business computer(s) type, operating system(s), and network set-up. This information will help in prior planning and make the warrant execution as trouble-free as possible.

VII. SEIZING REMOVABLE MEDIA

External storage devices come in a variety of shapes and sizes. Examples are 'thumb drives' or 'external hard drives.' Take photographs of the device and make notes about the device type and model. If the device is plugged into a computer system, collect the computer as mentioned above, then collect the external device. If the device is externally powered, unplug this first before disconnecting the device from the computer. Be aware of wireless devices including wireless network storage devices. Collect power adapters if present and package as needed.

VIII. SEIZING COMPUTER RELATED ITEMS

A. Digital Cameras

Digital cameras can be collected as any other item of evidence. These devices have internal memory that can hold data. They also usually have an additional expansion flash memory card. Collect, remove the batteries, and package as needed. Make notes of the make, model, serial number and card type if any is present. The memory card has a file system just like a computer's hard drive and can be imaged and examined for digital evidence. Leave the memory card in the camera.

B. Cell Phones

Cell phones can have digital forensic value in that many newer models have cameras and add-in memory cards. The memory card has a file system just like a computer's hard drive and can be imaged and examined for digital evidence. If the phone should need to be examined for other information such as address books or dialed numbers, it should be left turned 'On' and placed inside a protective radio interference bag (available from the Digital Forensics Lab); and/or placed in "Airplane Mode" and submitted to the Digital Forensics Lab for examination as soon as possible. The power adapter should be collected if present and used to charge the device battery as needed. If needed, contact the Digital Forensics Lab for assistance.

IX. DIGITAL VIDEO SURVEILLANCE SYSTEMS

These systems capture suspects engaged in all types of criminal activity. Evidence from these systems is extremely important in criminal investigations. First, watch the digital video to see if there is evidence on the video. Do not assume that evidence is present.

A. The preferred method of collecting digital video surveillance evidence from a business or community member is by utilizing Axon Citizen. Officers/detectives can send an invitation to a business owner/ representative or community member through the application or from the Evidence.com web browser.

B. If Axon Citizen does not work, see if the clerk or store manager can copy the video files to a CD or DVD with viewing software. The preferred file format is AVI or MPEG.

When not using Axon Citizen an officer/detective must thoroughly complete the Video Evidence Recovery Request Form (PD 1831) when obtaining video as evidence. Although this form is used to make a request of the Evidence Collection & Identification Section Photo Lab Unit, it should also be fully completed if the officer/detective/crime scene technician is recovering video evidence themselves. The person recovering the video evidence is responsible for uploading the form as a PDF attachment in the records management system. The information that would otherwise be captured on this form must also be obtained when receiving video evidence from a citizen, business or organization even if the video is extracted from a video surveillance system outside the presence of police personnel (i.e. video files sent via email or video media sent via regular mail/delivery service). This information may be obtained by personal contact with the person providing the video, by telephone or by electronic communication. The information obtained and person providing the information must be documented in the incident or supplement report.

If video evidence is obtained from a business or organization, the investigating officer/detective is responsible for having the business owner/employee fill out and sign the AAPD Certification of Custodian of Records form (PD 1831.1). The officer/detective obtaining the certification will sign and date the form as the witness and will ensure the form is thoroughly completed. The officer/detective is responsible for uploading the form as a PDF attachment in the records management system. This form must also be used when the video is extracted from a video surveillance system outside the presence of police personnel (i.e. video files sent via email or video media sent via regular mail/delivery service). For businesses or organizations that are out of the area, the investigating officer/detective should provide this form to the business or organization at the time of making the request for the video and have the signed form returned with the video. If the signed form is not received at the time the video is received, the signed form may scanned and emailed; or faxed from the custodian of the video to the investigating officer/detective.

To assist in any later processing or video enhancement, include in your report the brand, model, and type of Digital Video Recorder device. Further, look for and note any 'tech support' phone numbers. Determine the software program information if possible. These notations can be made on the Video Evidence Recovery Request Form. The incident report or supplement report documenting the recovery of the video should also include a general description of what is captured on the video, including the identity of anyone seen in the video, and who can identify those persons (i.e. the person providing the video or other witness). Any person involved in the recovery of video evidence or providing video evidence must be fully identified in the incident or supplement report. As a last resort, take photographs of the suspect images on the screen. If you need to recover the entire item, photograph and collect all parts of the device and package as needed.

The Digital Forensics Lab, the Evidence Collection & Identification Section, and the CID Commercial Robbery Unit have personnel and equipment that can assist in the assessment, recovery and enhancement of digital video images.

X. PACKAGING AND SUBMITTAL FOR STORAGE

All collected items of evidence should be collected and labeled as per Index Code 1201 and submitted to the Property Management Section for storage. Refer to Index Code 1832 for instructions on submitting collected items to the Digital Forensics Lab for examination.

XI. PROPONENT UNIT: Digital Forensics Lab.

XII. CANCELLATION: This directive cancels Index Code 1831, dated ***02-03-23***.