I. POLICY

This policy establishes procedures for the seizure and storage of computers, personal communications devices (PCD’s), digital cameras, and other electronic devices that are capable of storing digital information; and for the preservation and storage of digital evidence. All evidence seized and/or processed pursuant to this policy shall be done so in compliance with clearly established Fourth Amendment and search and seizure provisions.

II. PROCEDURE

A. Seizing Computers and Related Evidence

Computer equipment requires specialized training and handling to preserve its value as evidence. Members should be aware of the potential to destroy information through careless or improper handling, and utilize the most knowledgeable available resources. When seizing a computer and accessories the following steps should be taken:

1. Photograph each item, front and back, specifically including cable connections to other items.
2. List all items connected to the unit (ie; webcam, printer, scanner, external hard drive, thumb drives).
3. Look for a phone line, cable to a modem, or for wireless access for Internet access. Photograph and document the type of connection or device.
4. Do not overlook the possibility of the presence of physical evidence on and around the hardware relevant to the particular investigation such as fingerprints, biological or trace evidence, and/or documents and seize in an appropriate manner to maintain the physical evidence.
5. If the computer is off, **LEAVE IT OFF**
6. If the computer is ON:
   a. **DO NOT** manipulate the mouse or pointer or access anything or examine any files.
b. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.

c. Do NOT shut it down normally.

d. Disconnect the power cable from the back of the computer box or if a portable notebook style, disconnect any power cable from the case and remove the battery.

e. If you are unable to locate the laptop battery or are unable to access it, perform a hard shutdown by holding down the “On” button until the screen goes blank.

f. If the case involves child porn, internet chat, Instant Messaging, hacking, or a network intrusion, contact the on duty supervisor to ascertain the feasibility of contacting a computer forensic expert to perform a RAM dump prior to turning off the computer. A RAM dump will collect information such as running processes, network connections and data stored in temporary memory.

7. Label each item with case number, evidence sheet number, and item number.

8. Handle and transport the computer and storage media (e.g., tape, discs, memory cards, flash memory, and external drives) with care so that potential evidence is not lost.

9. Properly book the computer into evidence. Do not store computers where normal room temperature and humidity is not maintained.

10. At minimum, members should document the following in related reports:

   a. Where the computer was located and whether or not it was in operation.
   b. Who was using it at the time?
   c. Who claimed ownership?
   d. If it can be determined, how it was being used.
   e. Who else uses the computer or has access to it.
   f. If possible, obtain passwords or access codes.

11. In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all storage devices (hard drives, tape drives, and disk drives) should be seized along with all media. Accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should not be seized unless as a precursor to forfeiture.

B. Business and Network Computers

If the computer belongs to a business, is used as part of the business, or is connected to a network, it may not be seized unless the computer itself is the crime scene and not just a repository for possible evidence of a crime. The Department and the member may be held liable if the business suffers a loss of revenue or customers from having the computer seized.

Cases involving businesses and/or networks require specialized handling. Members will contact a certified forensic computer examiner for instructions or a response to the scene. Most cases will require an on-site acquisition or to parse out the information from the network drives or to image only the suspects hard drive of the involved computer. This shall only be done by someone specifically trained in processing computers for evidence.

C. Forensic Examination of Computers

If an examination of the contents of the computer’s hard drive, or floppy disks, compact discs, or any other storage media is required, forward the following items to a computer forensic examiner:
1. Copy of report(s) involving the computer, including the Evidence/Property sheet and a copy of the Yolo County Hi Tech Submission Form containing a brief explanation of the case and the analysis requested.

2. Copy of search authorization: the search warrant used or a copy of the consent form signed by the property owner or indicate if it was a Probation/Parole search. Include the court the Probation/Parole was from and if possible a copy of the Terms and Conditions of the Probation/Parole. Refer to the Sac Hi-Tech Task Force Web page for the most current search warrant verbiage. The warrant must include the wording to allow the search of the data as well as seizing the item.

3. A listing of the items or terms to search for (e.g., names, screen names, email addresses, Social Security numbers, DL numbers, check numbers, photographs, financial records, e-mail, and documents).

4. IF NEEDED or REQUESTED an exact duplicate of the hard drive or disk will be made using a forensic computer and a forensic software program by someone trained in the examination of computer storage devices for evidence.

D. Digital Storage Media

Digital storage media, including loose or external hard drives, floppy discs, CD’s, DVD’s, tapes, memory cards, or flash memory devices, should be seized and stored in a manner that will protect them from damage.

1. If the media has a write-protection tab or switch, it should be activated.

2. Do not review, access, or open digital files prior to submission. If the information is needed for immediate investigation request the Evidence Tech copy the contents to an appropriate form of storage media.

3. Many kinds of storage media can be erased or damaged by magnetic fields. Keep all media away from magnetic devices, electric motors, radio transmitters or other sources of magnetic fields.

4. Do not leave storage media where they would be subject to excessive heat or cold such as in a parked vehicle on a hot or cold day.

5. Use plastic cases designed to protect the media, or other protective packaging, to prevent damage.

E. Seizing Personal Communication Devices (cell phones)

Personal communication devices such as cell phones, PDAs or other hand-held devices connected to any communication network must be handled with care to preserve evidence that may be on the device including messages, stored data and/or images.

1. Unless verifiable exigent circumstances exist and evidence will be lost if examination is delayed, Officers should not attempt to access, review or search the contents of such devices prior to examination by a forensic expert. Unsent messages can be lost, data can be inadvertently deleted and incoming messages can override stored messages.

2. If the device is off: LEAVE IT OFF.
3. If the device is on, leave it on. Do not turn it off. The device should be placed in a solid metal container, such as a paint can, to prevent the device from sending or receiving information from its host network.

4. If possible, obtain PIN numbers, passwords or access codes to the unit.

5. When seizing the devices, also seize the charging units and keep them plugged in to the chargers until they can be examined. If the batteries go dead all the data may be lost.

6. If a cell phone/PDA is placed into evidence, the member should notify, via email, the Evidence Tech and the Investigations Supervisors of that fact so it can be taken care of properly (i.e.: plugged in/charged) in a timely manner in order not to expire the battery. If the device is collected afterhours/weekends the Watch Commander should be consulted on how to best preserve the evidence.

F. Collection of Evidence

Once digital evidence is recorded it shall not be erased, deleted or altered in any way prior to submission. All digital evidence, including photographs, video or audio files will be preserved regardless of quality, composition or relevance. First generation copies of digital evidence shall be considered as “original” and be handled the same as any other original evidence. Viewing, copying, printing or any other use of the original is not permitted.

1. Surveillance Video

   a. Video from surveillance cameras should be copied onto a digital medium in order to transfer it into evidence. CD-ROM discs or thumb drives are preferred. If unable to transfer the images to one of the listed devices, photographs or video will be taken of the monitor showing the surveillance video. Once the images are obtained they are to be treated as original evidence and logged into evidence.

   b. Digital evidence placed on a storage medium (USB device or SD memory card), including digital photos and videos, shall be booked into evidence and the files shall be downloaded to the department computer storage system by personnel assigned to the Evidence Unit only, which includes the Deputy Director of Police Services, and the Fiscal Analyst Manager. After the files are downloaded, they shall be removed from the storage medium by the person who downloaded the digital evidence. The storage medium device will be returned to the officer for later use.

2. Internet Evidence

   a. Evidence relating to crimes committed on the internet can pose numerous problems. Internet crimes have a time critical element in that the evidence itself could easily be changed or deleted. If it is possible to seize the computer, do so. If not, a screen capture with date and time should be performed. If necessary, the entire web page should be “ripped” to show the content in its original environment.

   b. Internet evidence should be copied onto some other medium for preservation, such as a CD-ROM disc or a thumb drive. If that is not possible a photograph or video should be taken of the relevant material. If that is not possible a hard copy print out may suffice. A computer specialist should be contacted to assist if needed.
3. E-Mail

One of the most common internet areas for evidence is e-mail. In order for e-mail to be used as evidence, FULL HEADER information is required. Full header information is not usually visible to the reader of the e-mail, but it can be viewed through the user’s e-mail client program. Full header is available on all e-mail. The full header information contains information about the sender, receiver, dates, times and IP address of the sender, which is required for a search warrant. Printed copies of the full header information will suffice if a digital copy is unavailable. If you are unable to locate the full header information, contact a computer forensic expert for assistance.

4. Chat room/IM (instant messages)

A ram dump will need to be executed in order to preserve the chat room log or IM’s in most cases as the data is held in temporary memory. Turning off the computer prior to getting a ram dump will result in the loss of that data forever. A computer expert will be required to perform the ram dump.

5. Social Networks

Social networking sites are very common communication source with people and are a good source of information. The information found in social networking pages can be very time sensitive as the information can easily be changed or deleted. Obtain a copy of the page digitally or photograph or hard copy printout as soon as possible and enter it into evidence. Re-checking the page periodically may reveal additional information or that certain information has been removed. Again, obtain a copy of the page if it has been modified.

6. Online sales/auctions (i.e.; Craigslist, E-Bay)

On line sales and auctions are a constant source of crime. The same rules that are used for other digital evidence should be followed in these types of cases (i.e., screen capture, photograph, and hard copy). A copy of all the correspondence should be collected. Full headers should be collected also if correspondence is through e-mail. Most on line auctions or sellers have an ID number that will need to be part of the information collected as most of the companies require it to track the transaction. Additional information regarding the account should be obtained such as: date account opened, name of people on account, account activity, and account passwords.

7. Phishing scam/ID theft

Scams involving banks should be handled the same as other digital evidence. A digital capture of the web page, photograph or hard copy printout should be obtained as soon as possible to preserve the evidence as it was seen by the victim. If the victim did supply personal identifying information, banks, credit cards and other financial business should be notified of the breach.

8. Web cams

A copy of the video should be collected. It may be prudent to collect any videos that were sent and/or received in regards to the case. The copy of the video should be treated as original evidence and handled as such. The type of web cam, the program the web cam uses, and how it was sent, needs to be noted.
G. Copying of Digital Evidence

1. Only the Evidence Tech, or a qualified person at their direction, is authorized to copy original digital media that is held as evidence. The original digital media shall remain in evidence and shall remain unaltered. A note shall be made on the RIMS evidence entry explaining why a copy of the digital media was made and for whom.

2. Digital images that are enhanced to provide a better quality photograph for identification and investigative purposes must only be made from a copy of the original media.

3. If any enhancement is done to the copy of the original, it shall be noted in the corresponding incident report.

Darren Pytel
Police Chief

07/10, 10/11, 08/17, 12/17, 05/19, 06/19

10/11 added II C 1 (pg 3) Yolo County Hi Tech Submission Form and II G 1 (pg 6) note re: copy made.
07/19 Permanent storage on CD rom disc removed.
   Deputy Director of Police Services and Fiscal Analyst Manager added
   Copy of digital evidence made for whom required