Procedure 3.21	Eugene Police Department
EFFECTIVE DATE 2-12-02	

Computer-Related Evidence

3.21.1 PURPOSE AND SCOPE

PART I - Responsibilities and Procedures for All Personnel

A. Seizing a computer as evidence
B. Forensic examination of computers
C. Business or networked computers
D. Reporting

3.21.2 RESPONSIBILITIES AND PROCEDURES ALL PERSONNEL

A. Seizing a computer as evidence

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. Look for a phone line or cable to a modem for Internet access.

2. If the computer is off, do not turn it on.

3. If the computer is on, do not shut it down normally and do not click on anything or examine any files.

    a. Photograph the screen, if possible, and note any programs or windows that appear to be open and running.

    b. Disconnect the power cable from the back of the computer box. (For laptops, disconnect any power cable from the case and remove the battery.)

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

5. Handle and transport the computer and storage media (e.g., floppy disks, CDs) with care so that potential evidence is not lost.

6. Lodge all computer items in the Property Control Unit in the basement of City Hall. Do not lodge computers in the parking level cage.

7. Document in the report where the computer was located, if it was in operation, who was using it at the time, who claimed ownershi8p, and how it was being used if that can be determined.

8. In most cases when a computer is involved in criminal acts and is in the possession of the suspect, the computer itself and all accessories (printers, monitors, mouse, scanner, keyboard, cables, software and manuals) should be seized.

B. Forensic examination of computers

1. 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 the Computer Forensic Examiner in the Financial Crimes Unit:

- Copy of report(s) involving the computer, including the Evidence/Property sheet.

- Copy of a consent to search form signed by the computer owner or the person in possession of the computer, or a copy of a search warrant authorizing the search of the computer hard drive for evidence relating to investigation.

- A listing of the items to search for (e.g., photographs, financial records, e-mail, documents.)

2. 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.

C. Business or networked computers

1. If the computer belongs to a business or is part of a network, it may not be feasible to seize the entire computer. Contact the Financial Crimes Unit for instructions or a response to the scene. It may be possible to perform an on-site inspection, or to seize only the hard drive of the involved computer.

2. This should only be done by someone specifically trained in processing computers for evidence. Cases involving networks require specialized training not currently available at this department.

D. Reporting

Once the forensic examination has been completed, the examiner will prepare a report showing the findings that will be copied to the officer investigating the case.