

# SPECIAL ORDER



Title	
<b>Computer Crime and Forensic Unit</b>	
Series / Number	
<b>SO – 01-11</b>	
Effective Date	Distribution
<b>March 23, 2001</b>	<b>A</b>

DISTRICT OF COLUMBIA

I. Background.....Page	1	IV. Regulations.....Page	: 2
II. Policy.....Page	1	V. Procedural Guidelines.....Page	2
III. Definitions.....Page	1		

## I. Background

Members of our Department are encountering computers in increasing numbers during the course of their criminal investigations. These computers may contain valuable evidence and leads that can aid in the investigation of crimes. Further, computer crime has increased dramatically in the last few years, and is expected to continue this growth for the foreseeable future. Therefore, the Department has created a Computer Crime and Forensic Unit (“CCFU”) to aid in the retrieval, preservation, and processing of information obtained through computers near or at the crime scene. This unit is a part of the Special Investigative Division’s Investigative Support Branch.

## II. Policy

The policy of the Metropolitan Police Department is to retrieve and preserve all evidence, and to pursue all leads, stored on the computer system.

## III. Definitions

When used in this directive, the following term shall have the meaning designated:

**Evidence** – computers and electronic devices that are believed to be associated with, related to, or an instrument of the crime itself, or which may have recorded or documented the crime; or which may have supported or facilitated the accomplishment of the crime at a crime scene or search warrant location.

#### **IV. Regulations**

- A. The CCFU shall provide technical and forensic expertise to members regarding computer technology and computer related investigations.
- B. The CCFU staff shall have the appropriate training, skills, and tools necessary to safely preserve and thoroughly examine and analyze evidence on computer systems.
- C. The CCFU staff shall coordinate their activities with the Mobile Crime Lab, and Crime Scene Search, as appropriate.

#### **V. Procedural Guidelines**

- A. The primary duties of the CCFU are:
  - 1. Conducting forensic examinations of computer systems and electronic digital devices seized by members and assisting in the seizure of those computer systems. This includes:
    - a. Responding on search warrants for the purpose of seizing, processing, and transporting computer systems and other digital electronic devices;
    - b. Responding to crime scenes to conduct thorough searches and limited forensic analysis, on site, of computer systems and other digital electronic devices;
    - c. Conducting forensic analysis on computer systems and other digital devices seized by members; and
    - d. Providing an on-call member to respond to requests for assistance after normal working hours. The on-call member will be responsible for carrying the CCFU on-call pager at all times and responding to all pages. Communications Division will have the number of the CCFU on-call pager and use it to contact the on-call member when requested.
  - 2. Providing members of the Department with investigative support and expertise regarding computers, the Internet, and networks as they relate to their specific criminal investigations. This includes:
    - a. Identifying and tracing suspects through e-mail and other Internet protocols, such as chat rooms, newsgroups, and file transfers;
    - b. Providing assistance with the technical and legal aspects of search warrants as they relate to computer systems, networks, and digital electronic devices; and

3. Responding to and investigating complaints regarding computer and computer-related crimes.
- B. Members encountering computers or electronic devices that are suspected to contain evidence shall contact the Computer Crime and Forensic Unit. After hours, members shall contact Communications and advise them to notify the on-call member of the Computer Crime and Forensic Unit.
- C. To ensure that possible evidence is not tainted or destroyed at the scene of a crime or on the site of a search warrant, members shall:
1. Not turn on any computer or digital device that is turned off.
  2. Not turn off a computer that is turned on unless they have been directed to, while on-site, by a member of the CCFU. Once given direction to turn off the computer, members may then seize the computer to take to the CCFU.
  3. At no time shall a member of the department who is not assigned to the CCFU conduct a search and/or analysis of a computer system.
    - a. When the courts require that a search of a computer system be done on-site, the member shall contact the CCFU as soon as possible requesting its assistance.
    - b. When members encounter computers during the course of their duties that need to be searched and/or analyzed on-site, they shall contact the CCFU. If, after hours, they shall call the Communications Department to have the on-call CCFU member respond to the scene.
- D. When it has been determined that a search warrant will be executed at a location where computers are likely to be involved, members shall notify the CCFU. Notification to the CCFU shall be made as early as possible so that preparations can be made to ensure proper and lawful seizure of evidence.
- E. Once a decision has been made to seize a computer system as specified in section IVC2 above, the member shall:
1. Complete the appropriate paperwork per General Order 601.3 (Handling and Accounting for Seized and Forfeited Property); and

2. Deliver the computer system to the Computer Crime and Forensic Unit at 300 Indiana Avenue, NW, Room 3019 for processing.

// SIGNED //  
Charles H. Ramsey  
Chief of Police

CHR:NMJ:rsk