



WRITTEN DIRECTIVE	No. PD17-1102	Page: 1 of 3
Search and Seizure of Computer-Related Equipment	Effective Date:	2-6-2017
	Supersedes/ Amends:	PD16-1102
	Reference:	83.2.5



I. Purpose

The purpose of this policy is to establish procedures for seizing or recovering information from computers and computer-related equipment.

II. Policy

It shall be the policy of the Lynchburg Police Department that officers should adhere to all guidelines and laws governing search and seizure as set forth by the *Code of Virginia* and departmental directives.

III. Procedure

A. Definitions

1. For purposes of this policy, a computer is defined as a high-speed electronic device that processes, retrieves, and stores programmed information, typically in binary form, according to instructions given to it in a variable program. These devices usually consist of a Central Processing Unit (CPU), external drive(s), server(s), and smart phones.
2. Computer-related equipment and peripherals may include keyboard, monitor, printer, external driver(s), thumb drives or other portable storage drives, external drives, CD's / DVD's, diskettes, wireless routers, scanners, microphones, external speakers, and other computer related components.

B. In the event that a computer is connected to a mainframe or network system (such as in a factory or business) a Forensics Unit supervisor will determine whether outside resources, including the Virginia State Police Computer Evidence Recovery Unit, should be contacted prior to any search warrant being issued.

C. If a search warrant is obtained, or consent to search is obtained, the items to be listed in the warrant as "items to be searched for"

should include “all computer hardware, and its components to include, but not limited to, peripherals, cables, manuals, data, digital storage devices, diskettes, CD(s) and programs, and all data contained therein.”

- D. Seized items will be examined by properly trained personnel within the department’s Forensics Unit.
- E. The primary responsibility for the seizure of a computer or computer-related equipment will be with the investigating officer.
- F. Members of this department will follow protocol as established in the Best Practices for Seizing Electronic Evidence A Pocket Guide for First Responders guide published by the U. S. Department of Homeland Security United States Secret Service to ensure that the maximum amount of data being searched for in the seizure of a computer is not lost and the equipment is not damaged.
- G. All seized evidence will be transported to the police department and entered into the Property and Evidence system, in accordance with *PD1201 Evidence, Recovered, or Found Property* prior to any examination taking place.
 - 1. The investigating officer will be responsible for the transportation and vouchering of all seized items.
 - 2. The investigating officer should complete and submit a Digital Forensics Service Request to the department’s Forensics Unit prior to any examination taking place. The request should include the following information:
 - a) Evidence item number and a description of the evidence.
 - b) Legal authority for the search.
 - c) Any privileged information contained within the evidence.
 - d) Detail whether or not the evidence has been previously viewed or accessed by anyone.
 - e) Provide user names, screen names, passwords or pattern locks, and e-mail addresses.
 - 3. The investigating officer will leave a copy of the police report and search warrant or consent to search form with the evidence.

- H. Outside agency requests will be approved in advance by a Forensics Unit supervisor and all evidence will be handled as previously stated. The outside agency investigating officer should complete and submit a Digital Forensics Service Request Outside Agency form to the department's Forensics Unit prior to any examination taking place. The request will include all information outlined in section III, G, 2, a through e of this directive.

- I. Technical information and support may be obtained prior to and after executing a search warrant from personnel within the department's Forensics Unit who have received specialized training on the recovery of evidence from computer and computer-related equipment.

Original Signed

Raul M. Diaz
Chief of Police

February 6, 2017

Date