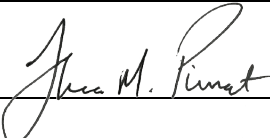


LEESBURG POLICE DEPARTMENT REGULATIONS AND GENERAL ORDERS MANUAL		
General Order Number: 308	Section: CRIMINAL INVESTIGATIONS	Effective Date: SEPTEMBER 2022
Title: DIGITAL EVIDENCE		
Accreditation Standards: ADM.16.01		
Review Date: JANUARY 2024	Total Pages: 3	Chief of Police: 

I. Policy

It is the policy of this Department to use digital evidence processing methods in accordance with industry standards when handling digital evidence. Digital evidence is defined as information and data of value to an investigation that is stored on, received, or transmitted by an electronic device. This evidence can be acquired when electronic devices are seized and secured for examination, for use in criminal investigations, administrative investigations, to support training, and critical incident responses. Digital evidence can cross jurisdictional borders quickly, and can be altered, damaged, or destroyed with little effort. Officers should be able to recognize and protect potential digital evidence for proper collection and subsequent examination.

There are many sources of digital evidence, but for the purposes of this general order, the topic is divided into three major forensic categories of devices where evidence can be found: Internet-based, stand-alone computers or devices, and mobile devices. These areas tend to have different evidence gathering processes, tools and concerns, and different types of crimes tend to lend themselves to one device or the other.

II. Procedure

- A. In light of the inherently fragile nature of computer data it is imperative that proper care be afforded to digital storage media during both seizure and analysis. Improper attempts to view data will result in alterations to the data, potentially corrupting evidentiary material. The integrity of the media and / or data is preserved by using personnel specifically trained to perform digital evidence seizure and analysis (hereafter referred to as digital forensic examiners).
- B. Examinations will be conducted primarily in the digital forensic laboratory. Due to the nature of the work conducted in the laboratory area and the fact that evidence items may be stored in the laboratory for extended periods of time access shall be restricted only to digital forensic examiners and evidence/property technicians. Any other persons accessing the laboratory area shall be escorted by authorized personnel.
- C. In collecting digital evidence the following procedures shall apply only in those cases where data residing on digital media is being sought as evidence in a criminal investigation. Digital media seized as evidence or recovered stolen property that will not be analyzed by a digital forensic examiner will be handled in accordance with other department policies.
 1. No personnel, except those under the direction or guidance of a digital forensic examiner, shall power on or access any piece of digital media which has been or shall be seized with the intention of analysis being conducted. Computers can contain destructive programs capable of altering, encrypting, or destroying evidence. Accessing files and programs can also alter file access dates and other potentially critical data.
 2. In many cases the case agent, if trained, will be able to handle the seizure of digital evidence without the assistance of a digital forensic examiner. There may be occasions that a case agent or supervisor deems it appropriate to call a digital forensic examiner to a scene to conduct the seizure including, but not limited to:
 - a. The case agent is unfamiliar with the type of evidence and the appropriate way to seize it.
 - b. Special tools or knowledge are required for the seizure.
 - c. It is believed that the computer system is part of a business system or server.

- d. It is believed that the suspect has made use of some type of encryption.
3. Evidence will be seized in accordance with current industry best practices. Digital forensic examiners are responsible for conducting periodic departmental training in device seizure techniques and are available for consultation on an as needed basis.
4. All evidence seized will be packaged and secured in accordance with General Order 114, Property and Evidence Control.

D. Request for Digital Forensic Examinations

1. The case agent or their designee will complete a Request for Digital Forensic Analysis (LPD Form 453) and submit it to an examiner or the Criminal Investigations Commander for assignment.
2. Search authority must be established prior to an examination being initiated. Search authority will most often be derived from consent of the device owner or the issuance of a search warrant. If consent is obtained from the device owner, the case agent should submit LPD Form 434-A, consent to search digital media, in addition to the request for analysis. Any other circumstances must be discussed with and approved by a digital forensic examiner prior to the examination beginning.
3. If it is determined by a digital forensics examiner that a device submitted for examination has been accessed by the case agent or other personnel outside of the guidance / direction or the examiner they may at their discretion refuse to conduct analysis of the device(s).
4. Generally, an item of evidence which has already been analyzed will not be “re-examined” by a different examiner. Any re-examination of this nature will be done only under extenuating circumstances and with the authorization of the Criminal Investigations Section Commander or their designee. This does not preclude an examiner from conducting further analysis on a device they previously examined at the request of the case agent.

E. Forensic Imaging Guidelines

1. Every effort possible will be made to never work on original evidence. It is understood that in some circumstances original evidence may need to be examined due to circumstances beyond the examiners control. When actions are taken on original evidence the examiner will thoroughly document their actions to clarify any changes which may have been made. This does not preclude an examiner from capturing an image of the memory on a live system.
2. Device imaging will be done in a forensically sound manner consistent with current industry best practices. Only hardware, software, and procedures which has been validated by a digital forensic examiner will be used on items of evidence.

F. Forensic Analysis Guidelines

1. Analysis may be conducted with validated forensic software of the examiner’s choosing.
2. Analysis will be conducted within the scope of the established search authority. If during the course of examination evidence of crimes outside of the established scope is discovered the examination will cease and the case agent will be consulted to determine proper course of action.

G. Case Priority

1. Examinations will generally be conducted in the order they are received.
2. “Rush Service” may be requested in order to have a device examined as soon as possible. Rush requests require justification from the case agent which will be documented on the request for analysis form.

H. Requests from Outside Agencies

1. Agencies other than the Leesburg Police Department may request the assistance of an LPD digital forensic examiner with device seizure or analysis.
2. Outside of exigent circumstances any requests for assistance by another agency shall be approved by the Criminal Investigations Section Commander or designee before the examiner begins work.
3. Assistance provided to other agencies shall be documented by the examiner through the creation of a case report.

III. Responsibility

This general order is in accordance with current best practices and procedures in this ever-changing technical environment. Because laws continually evolve, this general order recognizes that its recommendations may not apply in all circumstances; but aims to keep pace with the rapid changes involving digital evidence. Criminals continually alter their methods in an effort to disguise criminal activity. In addition to being familiar with these

changes, law enforcement must stay abreast of the applicable laws regarding digital evidence. To that end, the Criminal Investigations Commander, or designee, shall review this general order on an annual basis to insure it is consistent with best practices and procedures.