Chapter: Operations		**Section:** 409.17
Subject: Specialized Units		**Topic:** Digital Forensics Unit
Accreditation: ADM. 11.01	**Revised:**	**Reaffirmed:**
Enacted: 07/30/2015	**Last Review:** 05/01/2021	**Review:** 04/01/2022

I. PURPOSE

The purpose of this General Order is to set forth the guidelines concerning the seizure and subsequent analysis of electronic systems to include, but not be limited to: computers, tablets, GPS units, cell phones and any other device able to generate and store electronic data that may constitute evidence of criminal activity. In light of the inherent fragile nature of electronic data, it is imperative that proper care be afforded this media, during both seizure and analysis. Improper attempts to view electronic data will result in alterations to the data, thereby potentially corrupting evidentiary material. Using personnel specifically trained to perform this function will ensure the integrity of the electronic systems and/or data is preserved.

II. POLICY

The Digital Forensics Unit (DFU) is responsible for assisting with the physical seizure of computer or other electronic systems that have been identified or suspected of containing data relating to or constituting criminal acts. The DFU shall be responsible for conducting the subsequent forensic analysis of electronic systems seized during criminal investigations. In addition, the DFU shall assist personnel in the preparation of search warrants relating to the seizure of electronic equipment and may conduct the actual seizure of the equipment, if appropriate.

III. STAFF

The DFU shall serve as a unit under the direction of the Division Commander of the Criminal Investigations Division. The DFU shall be staffed with personnel who have received training specific to the proper seizure and forensic analysis of electronic systems. Recognized training entities include, but are not limited to: The National White Collar Crime Center, IACIS, Guidance Software, Access Data, Cellebrite, XRY, BlackBag, and the United States Secret Service (NCFI).

As a majority of the analytical function is performed within the MAC OS, Windows, Linux, iOS, and Android environments, a prerequisite to joining the DFU, at a minimum, is the possession of an extensive working knowledge of multiple file and operating systems.

IV. EQUIPMENT

The DFU staff requires special and high end seizure, imaging, forensic examination, and storage equipment. This equipment is required to ensure the electronic data seized is collected, analyzed, maintained secure, safe from alteration, and able to be stored long-term. All equipment relevant to the goals and objectives of the DFU will be evaluated by the Division Commander of the Criminal Investigations Division.

V. PROCEDURES

A. Seizures of Electronic Devices and Digital Media

1. To help ensure the eventual admissibility of any potential evidence obtained from electronic systems, it is imperative that the operating or file system of the electronic systems not be accessed. The data within these systems must be preserved and must not be altered in any manner.

2. The DFU has the proper tools, software, and training to both digitally and physically seize electronic systems to prevent any alteration of the data contained therein.

3. Documentation of the seizure location must occur to assist in subsequent court presentations. Items of importance include, but are not limited to, confirmation of electrical service and dial tone availability where applicable, as well as photographic documentation of the system prior to seizure. The DFU is equipped to perform electronic system seizures, and shall be the entity responsible for this task.

4. Agency personnel shall request the assistance of the DFU in all cases where the potential exists for the seizure of an electronic system or electronic generated data. The requesting deputy should be prepared to provide the DFU with detailed information concerning the electronic system to be seized, if possible, and the crime under investigation.

5. Agency personnel should refrain from operating or accessing any electronic system that is related to their investigation and shall request the assistance of the DFU to secure the electronic system(s) and/or data.

B. Forensic Examination

1. The DFU is responsible for conducting the forensic examinations of electronic systems to include, but not be limited to: computers, tablets, GPS units, cell phones and any other device able to generate and store electronic and/or computer generated data.

2. All examinations will be conducted utilizing accepted methods, such as those prescribed by the previous mentioned training entities.

3. Investigating deputies should be prepared to provide the DFU with an overview of their investigation and what type of information they are expecting to locate within the seized system or data.

4. An electronic forensics examination is a slow and tedious process, and the investigating deputy should consider this when managing the investigation.

5. Reports shall be completed by the DFU concerning the examinations performed and the results obtained. Copies of the reports shall be provided to the investigating deputy.

6. Requests from foreign jurisdictions for forensic examinations will be evaluated by the DFU staff and will be accepted whenever possible.

7. Forensic examinations shall be conducted within a secure room, maintaining security at the level of the main property storage area. Once an analysis has been completed on a seized system, the system may be removed to a storage area at the discretion of the DFU. Care must be afforded all seized electronic systems to prevent corruption or inadvertent alteration of data. Under no circumstances shall electronic systems or data be stored or maintained in the general property storage area, due to the prevalence of magnetic fields, dust, dirt and contaminants.

C. Training

1. Due to the evolution of computer system engineering and software development, continuing education is essential for the productivity and continued competence of the DFU.

2. In an effort to maintain a quality unit and expertise for court presentation, DFU staff should obtain and maintain certifications relevant to the electronic forensic field. They should be certified in one or more of the related certifications: A+ Certified, EnCase® Certified Examiner (EnCE®), Seized Computer Evidence Recovery Specialist (SCERS), IACIS Certified Forensic Computer Examiner (CFCE), Cellebrite Certified Examiner, Access Data Certified Examiner (ACE), XRY Certified Examiner, BlackBag Certified Examiner.

3. All training and certification opportunities relevant to the goals and objectives of the DFU will be evaluated by the Division Commander of the Criminal Investigations Division.