ELECTRONIC DEVICES AND COMPUTER EQUIPMENT

STANDARD NO(S): NYSLEAP 50.1

DATE: March 27, 2014
REVIEWED: 03/15/2017

REFER TO: Timothy Thompson

I. OBJECTIVE:

In order to maintain compliance with accepted electronic evidence collection and forensic examination procedures, the SCSO will maintain the equipment, tools and supplies necessary to collect and preserve electronic evidence and to conduct forensic examinations of that electronic evidence. SCSO members will follow the procedures outlined in this policy to guide them through identification and collection of electronic evidence. Furthermore, the member assigned to analyze electronic equipment will follow the procedures outlined in this policy to guide them through forensic examination of electronic evidence.

II. DEFINITIONS:

A. Electronic/Digital Evidence: Any information that is stored or transmitted in digital format that can be of evidentiary value in a criminal or internal proceeding (i.e., internal or external hard drives, thumb drives, compact discs, smart cards, tape media, or other devices designed to hold data in a digital format.)
B. Electronic Evidence Forensics: The use of specialized techniques for recovery, authentication and analysis of electronic data when a case involves issues relating to the reconstruction of electronic equipment usage, the examination of residual data, the authentication of data by technical analysis or explanation of technical features of data and electronic equipment usage.
C. Electronic Evidence Forensic Examiner: A member of the SCSO who has been specifically trained in the techniques of electronic data recovery and seizure.
D. Computer Systems: Computer monitor, CPU, hard drive, modem, CD ROM drive, DVD drive, internal hard drive device configured to work together as a unit or cabled together externally.
E. Hard Drive: Data storage devices that consist of an external circuit board, external data and power connections, and internal magnetically charged glass, ceramic or metal platters that store data.

F. External Hard Drive: Hard drives can also be installed in an external drive case. External hard drives increase the computer's storage capacity and provide the user with portable data. Generally, external hard drives require a power supply and a universal serial bus (USB), FireWire, Ethernet, or wireless connection to a computer system.

G. Removable Media: Cartridges and dis-based data storage devices typically used to store, archive, transfer and transport data and other information.

H. Thumb Drives: Small, lightweight, removable media with USB connections, these devices, also referred to as flash drives are easy to conceal and transport. They can be found as part of, or disguised as, a wristwatch, a pocket size multi tool such as a Swiss Army Knife, a keychain FOB, or any number of common devices.

I. Cellular Telephone: Handheld device capable of transmitting or receiving communications through a cellular network while moving around a wide geographic area. Some of these communications may include voice communications, text or media message communications. Most devices are able to contain personal information management applications such as, a phone book and calendar. Some devices are also capable of receiving internet access or other short range communications such as, Bluetooth, Near Field Communications (NFC), WiFi and hotspots. Some devices are able to install applications (apps) such as games or social media sites, etc. Many of these applications are valuable evidence in an investigation or prosecution.

J. Media Cards: Small data storage devices commonly used with digital camera, computers, cellular telephones, digital music players, video game consoles, and other handheld electronic equipment.

K. SIM Card: Subscriber Identity Module. Often found as a small rectangular chip with one angled corner hidden inside a cellular telephone under the battery. This card may contain the subscriber's profile, including an IMSI.

L. IMSI: International Mobile Subscriber Identity. It is a 14 or 15 digit (depending on location) number on the SIM card. The first three digits represent the Mobile County Code (MCC). The following three digits (in North America; 2 digits in Europe) represent the Mobile Network Code (MNC). The remaining digits represent the Mobile Subscription Identification Number (MSIN) within the network's customer base.

M. GSM cell phones: Global System for Mobile Communications. IT is a communication standard for wireless networks. Mostly used by AT&T and T-Mobile although other networks may use it also. This standard is used globally and it is likely to find a SIM card in devices on this standard.

N. CDMA: Code Division Multiple Access. It is a communication standard for wireless networks. Mostly used by Verizon and Sprint although other networks may use it also. This standard is not used globally as frequently and it is unlikely to find a SIM card in devices on this standard, although some devices may have one.

O. IMEI: International Mobile Equipment Identifier. This is a unique number on GSM phones.

P. MEID: Mobile Equipment Identifier. This is a unique number on CDMA phones.

Q. U.F.E.D.: is an acronym for: Universal Forensic Extraction Device.
R. Operator: is a member, certified to conduct a forensic downloading of a device.
S. Exam: means the forensic download of a device and any subsequent analysis by the operator.
T. Device: means, but is not limited to a cellular telephone, computer tablet, or other instrument that contains electronic digital data.

III. RESPONSIBILITES:

A. The initial member(s) on scene where the possibility exists that electronic/digital evidence may be present should not attempt to analyze electronic evidence unless specially trained to do so. Members should secure the scene and request assistance from a SCSO member who, or outside law enforcement agency that have persons specially trained in collection and examination of these devices.
B. The Sheriff will assign certain members of the Office of Sheriff to be trained and certified in forensic electronic evidence examination. While these members will be the main electronic forensic examiners for electronic equipment, other Department members may also be trained in the proper procedures for collection of these devices.

IV. PROCEDURES:

A. Computer systems and other electronic equipment are inherently fragile by nature. It is imperative that proper care be afforded to electronic equipment, during both seizure and analysis. Improper attempts to view electronic data could result in alterations to the data, thereby potentially corrupting evidentiary material. The integrity of the electronic device and/or data is preserved by using personnel specifically trained to perform the computer seizures and subsequent analysis.
B. The SCSO member(s) trained and certified to handle electronic equipment are responsible for assisting with the physical seizure of electronic equipment that have been identified as or suspected of containing data relating to or constituting criminal offenses which are the subject of a criminal investigation. This member(s) shall be responsible for conducting the subsequent forensic analysis of all electronic media that he is certified to examine.
C. The following procedures will apply only in those cases where data residing on any electronic media is being sought as evidence in a criminal investigation. Any electronic media seized as recovered/stolen property will not be examined, unless there is an open criminal investigation and only done so under authority of an in-force search warrant for the particular device that has been recovered.
D. No member of the SCSO, except those under the direction of a certified electronic forensic examiner shall power on or access a computer system, digital recording device, storage media, or cellular telephone that is or has been seized. These devices may contain destructive programs that can alter, encrypt, or destroy evidence. Accessing files and programs can alter file access dates and other data which may be critical as evidence.

E. Seizing Desktop Computers:
    a. Immediately isolate any suspects from the computer. Consider the possibility of latent prints or DNA on the keyboard, mouse, and other peripheral devices.
    b. Photographs will be taken of all evidence prior to disassembly and collection.
    c. If the computer is off, leave it off.
    d. If the computer is on, leave it and photograph the screen as you found it.
    e. Unplug the computer from the back of the computer first, then the wall.
    f. All cables and hardware they belong to are to be labeled.
    g. All evidence collected will be documented pursuant to SCSO property and evidence collection procedures.
    h. All evidence collected shall be packaged in suitable evidence containers/bag(s).
F. Seizing Laptop Computers:
    a. Immediately isolate any suspects from the computer. Consider the possibility of latent prints or DNA on the keyboard, mouse, and other peripheral devices.
    b. Photographs will be taken of all evidence prior to disassembly and collection.
    c. If the computer is off, leave it off.
    d. If the computer is on, leave it and photograph the screen as you found it.
    e. Unplug the computer from the back of the computer first, then the wall.
    f. All cables and hardware they belong to are to be labeled.
    g. All evidence collected will be documented pursuant to SCSO property and evidence collection procedures.
    h. All evidence collected shall be packaged in suitable evidence containers/bag(s).
G. Seizing Large Network Computers – Mainframes:
    a. Immediately request assistance from the New York State Police Computer Forensic Unit.
    b. Isolate suspects from the computers. Remember, it is possible for them to access these remotely utilizing other hand held devices.
    c. Do not disconnect the power or take any other action, as doing so may severely damage the system and/or cause the loss of evidentiary data.
    d. All evidence collected will be documented pursuant to SCSO property and evidence collection procedures.
H. Seizing Cellular Telephones:
    a. If the cell phone is off, leave it off and remove the battery if possible.
    b. If the cell phone is on and not password protected, put the phone into airplane mode and turn it off. Then remove the battery if possible.
    c. If the cell phone is on and password protected, try to get the password from the owner, then follow step b.
    d. If the cell phone is on and password protected and you can't get the password from the owner, remove the battery if possible. Do not try to guess at a password, it could lock the device and a forensic examination will not be possible.

e. All available cables and chargers should be collected.
f. Each cell phone and it's chargers should be packaged as one item in a paper evidence bag. Do not package multiple phones as one item.
g. Write the password (if applicable) and owner's name on the outside of paper evidence container. If the password is a 9 dot pattern code, be sure to label the top left corner as such and draw arrows showing flow of pattern marking start and end locations.
h. All evidence collected will be documented pursuant to SCSO property and evidence collection procedures.

V. AUTHORIZATION FOR CELLULAR TELEPHONE EXAMINATIONS

A. All U.F.E.D. exams conducted pursuant to a SCSO criminal investigation will be authorized by either the CID Lt, or the Sheriff, Undersheriff or Chief Deputy prior to the examination.
B. All requests for a U.F.E.D. exam made by an outside agency will be authorized by either the CID Lieutenant, Sheriff, Undersheriff or Chief Deputy prior to the exam being conducted and will follow the procedures outlined in Section VI.
C. Any exam conducted pursuant to an internal SCSO investigation will be authorized by the Sheriff prior to any exam being conducted.

VI. PROCEDURES FOR U.F.E.D. EXAMINATIONS:

A. All electronic devices in which a U.F.E.D. examination has been requested should have been properly examined first for physical evidence such as: DNA, latent fingerprints, gunshot or blood residue or other trace evidence.
B. All devices in which a U.F.E.D. examination is requested will be accompanied with either a copy of an in-force criminal search warrant or a fully executed consent to search form signed by the owner of such device. The only exceptions are:
   a. Exams conducted on devices for training purposes which are County property or have been turned over to the SCSO as donations.
   b. Exams on devices that are SCSO property and the exam has been authorized by the Sheriff.
C. The certified U.F.E.D. operator will generate a SJS number and accompanying report listing all pertinent information and results of such logical or physical forensic examination.
D. The investigator requesting such forensic examination will complete the SCSO Forensic Exam of Electronic Device Spreadsheet (SCSO-LE-015) which will be provided to the operator and maintained in a binder located in the UFED office in the Criminal Investigation Division.
E. Seneca County Sheriff's Office cases:
   a. The operator will make a pristine evidence copy of the forensic download to a Thumb drive, memory card, compact disc (CD) or a digital disc (DVD). The

pristine evidence copy will be packaged and secured into evidence by the operator following procedures outlined in SCSO policy 5-1 "Collection & Preservation of Evidence. The operator will make a "Working Copy" of the forensic download which will be turned over to the Investigating Officer.

F. Outside Agency cases:
    a. The requesting officer from the outside agency will complete SCSO-LE-015 and will provide a thumb drive of sufficient memory size to the operator prior to conducting the examination.
    b. The operator will make a pristine evidence copy of the forensic download to a thumb drive (provided by the outside agency). This evidence copy will be turned over to the outside agency requesting officer after it has been placed into an evidence container and the operator has completed a SCSO Property Evidence Form. The operator will make a "working copy" of the forensic download to a media device (provided by the outside agency). Both the pristine copy and the working copy will be turned over to the requesting officer from the outside agency. It is the responsibility of the outside requesting agency to maintain the evidence and document the chain of custody.

VII. REQUEST FOR ANALYSIS OF NON-CELLULAR ELECTRONIC EQUIPMENT

A. All non-cellular electronic equipment submitted for analysis will be accompanied with a copy of the search warrant or consent to search form authorizing the search.
B. The member conducting the analysis must be familiar with the scope of the search warrant or any limited consent before performing any forensic analysis. If the member finds evidence of a separate crime in plain view during a forensic analysis, the member will stop the search immediately and notify the case investigator who will apply for a secondary search warrant for any material observed outside of the scope of the original search warrant or consent.
C. Specific information detailing the accepted methods of collecting electronic evidence can be found in the Special Report published by the National Institute of Justice titled; "Electronic Crime Scene Investigation: An Guide for First Responders" Second Edition dated April 2008. A PDF version is available for reference at http://www.nij.gov/publications/ecrime-guide-219941/Pages/welcome.aspx