A. Purpose:

To outline the steps taken to conduct the chip-off technique and direct physical connection techniques for forensic examination of memory chips.

Chip-off forensics is an advanced digital data acquisition procedure which involves physically removing the non-volatile integrated circuit (*i.e. flash memory chips from a device capable of storing* data). The chip-off process is performed to remove the internal memory chip from damaged or destroyed devices not accessible by extraction tools, devices unsupported by commercial tools and/or unsupported by advanced data extraction methods. The data can be read directly on an external specialized reader. These chips are removed, cleaned and prepared for reading by the compatible reader. Data extraction software and programmers are used to extract the data from the memory chip which can be parsed and examined by mobile forensic software tools.

Other processes can also be employed to access and extract data from devices (i.e. USB Flash drives, SD cards, micro-SD cards, compact flash cards and others) that do not require removal of the memory chip. These methods utilize specialized software and hardware tools to allow for a direct physical connection to the memory chip / PCB (printed circuit board) bypassing damaged controllers and achieving potential data recovery.

B. Responsibility:

Forensic Examiners or other analysts working in the Computer Crimes and Electronic Evidence Unit.

Definitions/Abbreviations:

Refer to CC SOP-26 - Definitions and Abbreviations.

C. Safety:

1. The Chip-off procedure will be conducted in a hood with the Sentry Air System Series 200 Exhaust in operation. The “use log” located in the binder will be updated for the days of use of the Sentry Air System Series 200 to monitor replacement of filters. The filters will be changed in the Sentry Air System Series 200 after 30 uses or after one (1) year, whichever is sooner.
2. If necessary due to the condition of evidence received (i.e. hazardous and/or biological substances), wear appropriate personal protective equipment (e.g., lab coat, gloves, mask, eye protection), while carrying out standard operating procedures.
3. It is up to the examiner to ensure all solvents used during the examination are up to date and dispose of any expired materials appropriately.

D. Destruction of Evidence:

1. Per the Connecticut Practice Book (40-9), the defense must be notified in the event of destructive testing (if the suspect has been arrested).
    a. Refer to guidance from the Case Management Unit.
2. If no arrest has been made, the analyst/technician may proceed with the process.
3. If no suspect is listed on the evidence receipt, the analyst/technician may proceed with the process.
4. Consult with the technical leader or supervisor with any questions or concerns.

E. Procedure:

1. Research the make and model of the evidence to be examined to ensure it is supported for this method. This includes the chip identification number and the ball grid array (BGA).
    a. External resources including, but not limited to http://transition.fcc.gov may be utilized.
2. Based upon best practices, remove the chip from the circuit board using available techniques.
    a. This can include but is not limited to the use of alcohol-based solvents.
    b. If using a hot plate, turn the temperature up high, but start with evidence on at zero degrees, and work while it is heating up. Record final temperature in notes where chip(s) when able to be removed successfully.
3. Ensure the chip is in its best condition before contact with the programmer (i.e.- tin the chip or clean the chip).
4. Acquire the data utilizing the correct programmer, adapter, software, and if necessary, write-blocker.
    a. Ensure an internet connection is present if necessary.
    b. A computer dedicated to this method will be utilized for examinations.
5. Document all processing completed on QR-CC-56 - Chip Off Record
    a. Photographic documentation will be utilized and will be saved to the work product.
6. Due to the possible consumption of evidence in this procedure, two copies of the extraction will be saved for examination.
    a. One original copy, and one working copy.
    b. Refer to CC-SOP-55 for guidance on saving the extraction(s). If the submission is to be examined by someone other than the one performing the extraction, follow procedures regarding virtual evidence storage.
    c. Refer to applicable CCEEU SOP for examination purposes

F. References:

1. Training books and notes from applicable software/hardware.
2. Help files located either online or within the applicable software.
3. SWGDE Best Practices for Chip-Off
4. SWGDE Standards and Controls Positions Paper
5. Training books and notes from applicable hardware and software.