Purpose:
To outline the steps taken to conduct the chip-off technique 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 adapters that support specific BGA, eMMC, eMCP and UFS memory chip types. 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. A laboratory report of the data extraction and analysis results is produced and provided to the requesting agency.

Responsibility:
Forensic Examiners or other analysts working in the Computer Crimes Forensic Unit.

Definitions/Abbreviations:
Refer to CC SOP-26 - Definitions and Abbreviations.

Procedure:

Identify the evidence device make and model and confirm that no other full physical memory extraction is possible by other means. When performing the Chip-Off Technique, the information on the device, chemicals and readers used should be recorded on QR-CC-56 (Chip-off Record).

1. To aid in determining the type and location of the flash memory chip, the FCC ID number located on a sticker underneath the battery or on the back of the device should be identified and recorded. The FCC site should be checked to obtain the information specific to the FCCID# at the following address: http://transition.fcc.gov/oet/ea/fccid/.
    a. The information for the device is located within the detail summary.
    b. Select, “Internal Photos” within the attachment list to view image photos of the internal components and their locations for the device. Details about the main

board and the lay out are shown in these photos and can be used as a guide to take apart the phone and access the main board.

2. For devices without FCCID#'s attempt to find information for the device or the flash memory chip once the device is dismantled from internet searches.

   If possible, determine whether the device model employs encryption by default, if so the data stored on the chip will not be readable and the chip-off technique would not be a useful procedure.

2. If the chip-off technique is advisable, dismantle the device to gain access to the main board.
   a. Using the information from above, locate the position of the flash memory chip and begin removing the tin shield covering.
   b. To remove the tin covering, apply liquid solder flux around the entire perimeter of the shield. The solder flux will serve to spread and transmit the applied heat evenly around the edges of the plate.
   c. Heat is applied to the area using a hot air gun. Gently lift the shield up using a metal prying stick until it is completely removed and the chip(s) underneath are visible.
   d. Identify the chip type and determine if a compatible reader adapter/programmer is available.

3. Different methods for removing the chip are used depending on the device and how the chip is set on the board. Factors include the type of chip; the amount of epoxy present around and underneath the chip; and what other parts of the mainboard are in close proximity to the chip.

   Three primary methods can be used to carry out the chip detachment from the board:
   a. Use a heat gun 3-4 inches above the chip being careful not to apply too much heat.
   b. Use heat applied beneath the chip (Gordak 853 High Power ESD BGA Rework Station).
   c. Use Infrared heat (320° C) above the chip with heat applied beneath the chip (200° C)(T-862 BGA Rework Station).

IMPORTANT NOTES AND CONCERNS:
- Carefully score around the chip edges using an exactor knife before heating. When you are heating the chip/board, you need to work away at the epoxy on the side of the chip and open some air pockets. Low heat for longer period of time is better than high heat for short time.
- Do not use force to pry the chip, let the chip come off with light pressure, once the solder and epoxy are broken down, the chip will come off easily. Use a wide flat exactor knife on the sides of the chip to pry the chip loose. If the chip is forced off, some of the BGA pins will be damaged and a read will not be possible.
- Use protective eye glasses or only look at board/chip through the protective screen when using Infrared heating.
- Perform these procedures in a hood with a filtration system and /or venting.

4. Clean the flash memory chip after a successfully removing from the board. Using a solder iron with a chisel tip, apply pressure against the epoxy residue and push forward slightly as the epoxy breaks down. Repeat this process turning chip 90 degrees. A magnifying scope or glasses can be used to view the chip for remaining residues left behind.

IMPORTANT NOTES AND CONCERNS:
- Do not tilt the chisel tip as pressure is applied-this will scratch the chip surface.
- Use short strokes and clean the solder tip between scrapings; during the process, brush with alcohol to check how much epoxy remains on the chip.

5. After the cleanup step has been completed, the chip needs to be re-tinned or re-balled.
   a. Solder paste is applied to the surface of the chip focusing on the BGA pins that the adapter will read from.
   b. Use the hot air from the re-work station and apply hot air to the solder paste for just seconds, until all the solder is attracted to the BGA pins.
   c. Use the solder iron tip to clean away excess solder and large balls that can build up in the previous step.
   d. Use a tooth brush and alcohol 99.9% to clean the chip for reading.

6. Following re-tinning or re-balling, the chip should be readable by a compatible reader adapter programmer. If a read is not achieved repeat the re-tinning/re-balling procedure above and attempt to read the data again.

   The selection of a reader type will depend on the type of memory chip.
   eMMC153 and eMMC169 chips can be read by a Sireda using a SD adapter to a USB interface on the forensic system. A physical acquisition can be conducted using a forensic application such as Encase or FTK Imager.
   Other BGA types or UFS types can be read and imaged using a programmer – the UP828P using the appropriate adapter or the DediProg NuProg-E UFS programmer.

7. The image file produced from the acquisition will be examined using a forensic application (EnCase, FTK, IEF - Refer to CC SOP-08 Case Initiation Protocol) or the image will be examined by a cell phone data analyzer application (Cellebrite's Physical Analyzer-Refer to CC SOP-18 Cell Phone Data Extraction).

8. The Cell Phone Worksheet/Notes (QR-CC-16) should be used to document the evidence device specifics; the chip type identified; the chip-off technique specifics employed; the reader type adapter and /or programmer used; the forensic application or data analyzer application version; and any errors, technical problems, deviations encountered.

9. Produce a report and attachment data of the results following the laboratory reporting protocol (Refer to CC SOP-09 Laboratory Report Protocol).

References:

1. Teel Technologies Advanced Chipoff Training documentation.
2. T-862 BGA Rework Station, Gordak 853 High Power ESD BGA Rework Station, JBC CD-S Soldering Station Kit, Circuit Specialist Digital Hot Air Rework Station w/ soldering iron, UP828P BGA Chip Programmer and adapters, SD Chip Reader Kit instruction manuals and documentation.
3. Cellebrite UFED Touch, UFED4PC software user manual or training documentation.