Título: Guía de procedimientos para la extracción de datos en dispositivos móviles dañados

Autor: Fernando Ferrari

POSGRADO ESPECIALIZACIÓN EN INFORMÁTICA FORENSE

Facultad de Ingeniería

Director: Ing. Sergio Appendino

Fecha de publicación: 18/08/2022

UNIVERSIDAD FASTA | FACULTAD DE INGENIERÍA

Índice

Tabla de ilustraciones

Resumen

El objetivo de este trabajo es elaborar una guía para investigadores forenses especialistas en dispositivos móviles, que los capacite en la extracción de datos de dispositivo que se encuentren dañados. En primer lugar se describe la extracción de datos mediante técnica "JTAG", luego se aborda la extracción mediante una conexión "ISP" y por último se ve la más invasiva, conocida como "chip-off". Luego desarrollan las recomendaciones y herramientas necesarias para la solución de los problemas más comunes que podemos encontrar a la hora de intentar extraer datos de un dispositivo móvil. Por último se presenta una introducción a las nuevas tecnologías de memorias y las principales herramientas para su lectura. La presente guía también aporta conocimientos de electrónica práctica para poder utilizar las técnicas de extracción de datos propuestas para los distintos tipos de dispositivos móviles. El especialista forense obtendrá una introducción a las técnicas básicas de reparación de dispositivos móviles que lo ayudaran a llegar a una extracción de datos exitosa. Esta guía servirá de apoyo a quien se inicie en estas técnicas. Por otro lado, al usuario avanzado, le será útil a la hora de avanzar más rápido a la extracción de datos en memorias modernas.

Palabras claves

Forense – Extracción – Chip-off – JTAG - ISP

Introducción

Muchas veces la extracción de datos fracasa por un problema en el hardware periférico al elemento que contiene realmente la información digital de interés. Como ya veremos la información relevante se encuentra en un único componente: la memoria de datos.

Si bien lo que describe esta guía puede parecer demasiado esfuerzo para ser aplicado solo en algunos casos, con solo lograr el acceso a los datos de un solo dispositivo que contenga la única prueba existente para encontrar la verdad en una causa, todo el esfuerzo valdrá la pena, aunque solo se aplique una vez.

Debido a la amplia gama de dispositivos móviles, existen múltiples métodos de adquisición. No hay ningún método de adquisición universal único disponible para todos los modelos.

En lo que interesa a este trabajo tampoco hay un método de extracción único cuando se trata de dispositivos móviles dañados.

Algunos métodos de adquisición dependen del estado del teléfono, la versión del sistema operativo, el tipo de almacenamiento, etc.

Es necesario investigar y estudiar para descubrir qué métodos de adquisición están disponibles para un dispositivo en particular.

Esta guía describe distintos métodos de adquisición disponibles para las diferentes plataformas de los dispositivos móviles y analiza la posibilidad de aplicar estos métodos cuando la integridad del dispositivo se encuentra comprometida.

Dada la gran variedad de dispositivos móviles, sus diferentes tecnologías, el avance constante de estos y la necesidad de acotar esta guía, se abordaran las generalidades en lo que respecta a técnicas y herramientas en electrónica aplicada y las técnicas de extracción de datos para un solo tipo de memorias, dando al final de la guía un vistazo a la extracción de datos en memorias más modernas.

Objetivos

Objetivo general

Elaborar una guía para investigadores forenses especialistas en dispositivos móviles, que los capacite en la extracción de datos de dispositivo que se encuentren dañados.

Objetivos específicos

Para esto el lector deberá incorporar conocimientos básicos sobre el funcionamiento de los distintos medios de almacenamiento utilizados en los dispositivos móviles de tipo Smartphone, memorias externas, pen drive, etc. para que luego pueda decidir qué técnica deberá aplicar para llegar a una extracción de datos exitosa.

La guía también aportara conocimientos de electrónica práctica para poder utilizar las técnicas de extracción de datos propuestas para los distintos tipos de dispositivos móviles.

El especialista forense obtendrá una introducción a las técnicas básicas de reparación de dispositivos móviles que lo ayudaran a llegar a una extracción de datos exitosa.

Guía de procedimientos:

Capítulo 1 - Extracción de datos

Extracción de datos mediante conexión al puerto "JTAG"

La extracción de datos a través de este método es del tipo invasiva pero no destructiva y permite realizar un volcado completo de la memoria aunque el dispositivo este parcialmente dañado (placa principal parcialmente dañada, pantalla rota, conector USB dañado), la única condición es que el microprocesador y la memoria funcionen con el circuito de alimentación propio del dispositivo. También posibilita la extracción de datos aunque el dispositivo posea algún tipo de seguridad con clave de usuario (patrón, contraseña, etc.). Es condición para que el volcado de memoria sea legible, que la memoria de datos no este encriptada.

Para dar una introducción al tema, diremos que JTAG (Joint Test Action Group) se estandarizó alrededor de los años 90 como la norma IEEE 1149.1-1990. En el año 94 se publicó un documento que contiene la descripción del lenguaje de comunicación (boundary scan description language (BSDL)). Es ahí cuando esta norma fue adoptada por las compañías electrónicas de todo el mundo para la prueba de circuitos impresos y la prueba de sub módulos de circuitos integrados. También es muy útil como mecanismo para depuración de aplicaciones embebidas, puesto que provee una puerta trasera para acceder al sistema. Esta puerta trasera es la que permite acceder a la memoria de datos del sistema.

Respecto a la parte física de una interfaz JTAG, podemos describirla como una interfaz de cuatro o cinco pines. Los pines del bus son:

- TDI (Entrada de Datos)
- TDO (Salida de Datos)
- TCK (Reloj)
- TMS (Selector de Modo)
- TRST (Reset) es opcional

Además, se deberán conectar las alimentaciones correspondientes para que el circuito del celular y el del lector estén al mismo potencial y así poder leer correctamente las señales. Para esto el puerto JTAG, generalmente incluye los pines:

- VREF (Alimentación positivo)
- GND (Alimentación negativo)

Ya que posee una sola línea de datos, el protocolo es necesariamente serial, esto hace que el volcado de la memoria sea bastante lento. La entrada de la señal de reloj es por el pin TCK. La configuración del dispositivo se realiza manipulando una máquina de estados de un bit empleando el pin TMS. Un bit de datos es cargado en TDI y otro sacado en TDO por cada pulso de reloj de la señal TCK. Se pueden cargar diferentes modos de instrucción, tales como como leer el ID del chip, muestrear el valor de pines de entrada/salida, manejar pines de salida,

manipular funciones del chip, y otras. La frecuencia de trabajo de la señal de reloj del pin TCK varía en función de cada chip, pero típicamente está en el rango de 10-100 MHz (10-100ns/bit).

El pin TRST es una señal opcional para reseteo o reinicio. Si no se dispone de dicho pin, puede reiniciarse mediante una instrucción reset.

Existen algunos celulares que tienen un puerto JTAG integrado, por lo que las conexiones están a menudo disponibles en la placa de circuito impreso en adelante PCB, como parte de la fase de prototipado del producto, tal como se observa en las ilustraciones 1 y 2, en las cuales se pueden ver los pads para soldar las conexiones o como se ve en la figura 2, un puerto de conexión ya incorporado. Estas conexiones pueden proporcionar una sencilla forma de realizar ingeniería inversa y en lo que interesa a esta disciplina, el volcado de la memoria de datos.

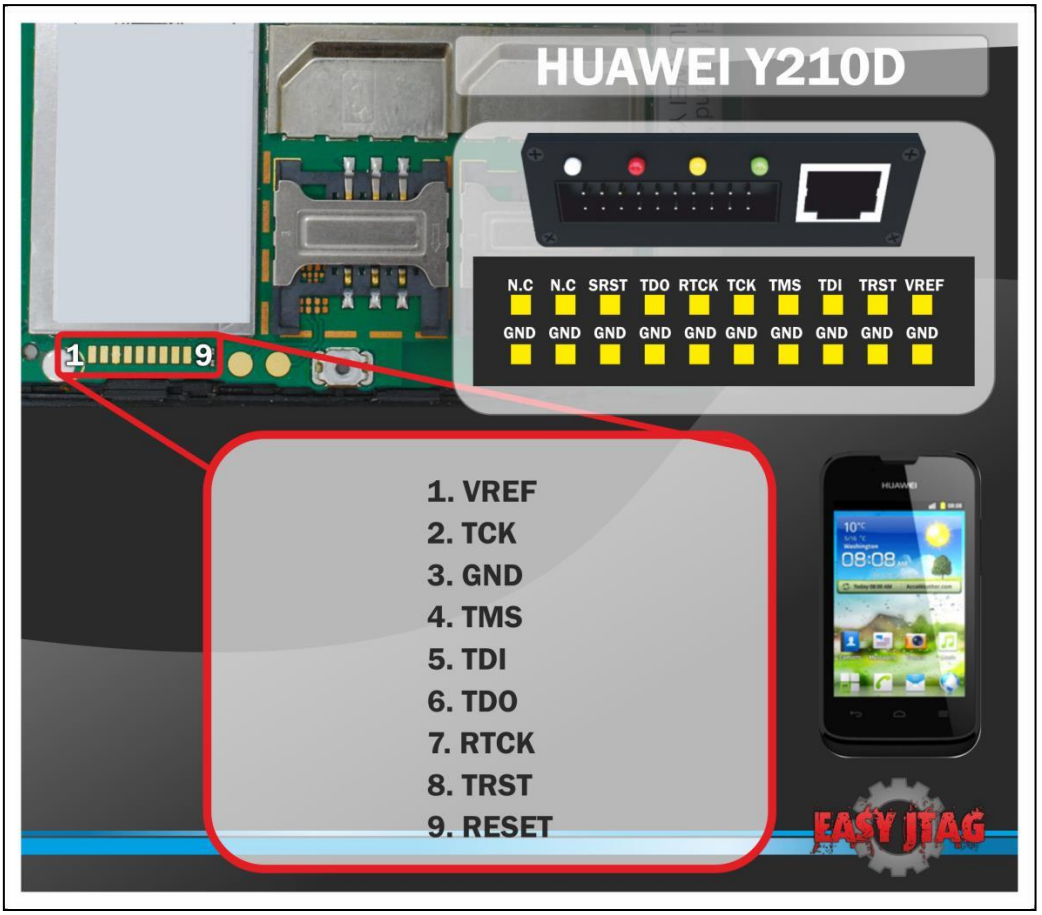


Figura 1 – Puerto JTAG para soldar disponible en el PCB – Fuente: https://easy-jtag.com/

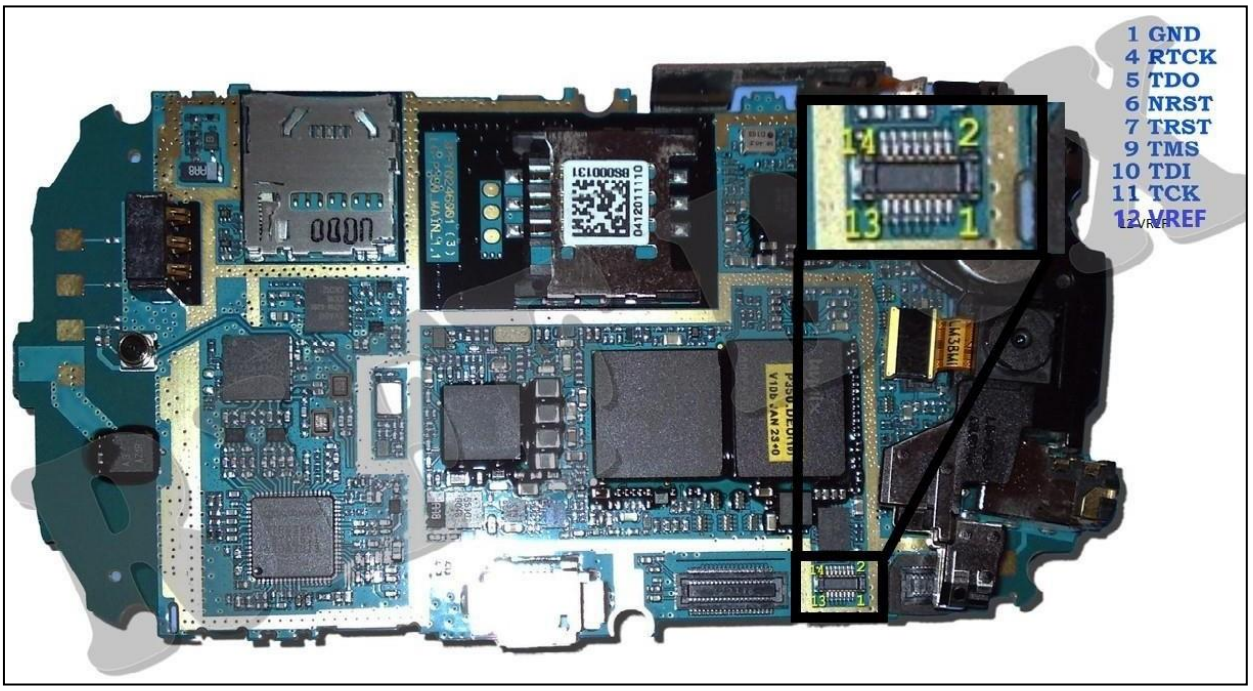


Figura 2 – Puerto JTAG con conector disponible en el PCB – Fuente: https://www.riffbox.org/

En otros casos, el puerto no estará disponible y todo dependerá de contar con información extra sobre el dispositivo que se desea analizar, tal como los esquemáticos (diagrama de conexionado de los componentes) o diagramas del PCB (ubicación de los componentes en el circuito impreso) en los cuales se pueda encontrar donde interceptar las conexiones del puerto JTAG.

Respecto al hardware y software para realizar este procedimiento, si bien los protocolos son públicos, la implementación escapa a la profundidad que aborda este trabajo. También, dada la gran cantidad de equipamiento disponible en el mercado para este fin, no tendría sentido abordar la implementación del hardware y el protocolo de lectura para poder establecer una conexión JTAG. A continuación se listan algunos de los equipos JTAG disponibles en el mercado:

- Easy Jtag Box
- Riff Box
- OCTOPLUS
- ATF BOX
- ORT JTAG TOOL

Las características de estos equipos son similares, todas ofrecen casi las mismas opciones. La principal diferencia radica en la información que ofrecen con respecto a los dispositivos que soporta, tales como diagramas de conexionado en el PCB, velocidades de lectura, etc.

Figura 3 – EASY JTAG BOX - Fuente: https://easy-jtag.com/

Figura 4 – RIFF BOX - Fuente: https://www.riffbox.org/

Figura 5 – OCTOPLUS - Fuente: https://octoplusbox.com/es/

Figura 6 – ATF BOX - Fuente: https://gsmserver.es/atf-gold-box/

Figura 7 – ORT JTAG TOOL - Fuente: https://www.ort-jtag.com/home

Las cajas vienen con variedad de conectores y placas con "pad" para soldar las conexiones, en caso que se lo requiera. A continuación se muestra un ejemplo de conexión típico, utilizando la caja de lectura "RIFF Box", para un celular marca Samsung, modelo SM-i8260L, este celular posee disponible los pad del puerto JTAG para soldar:

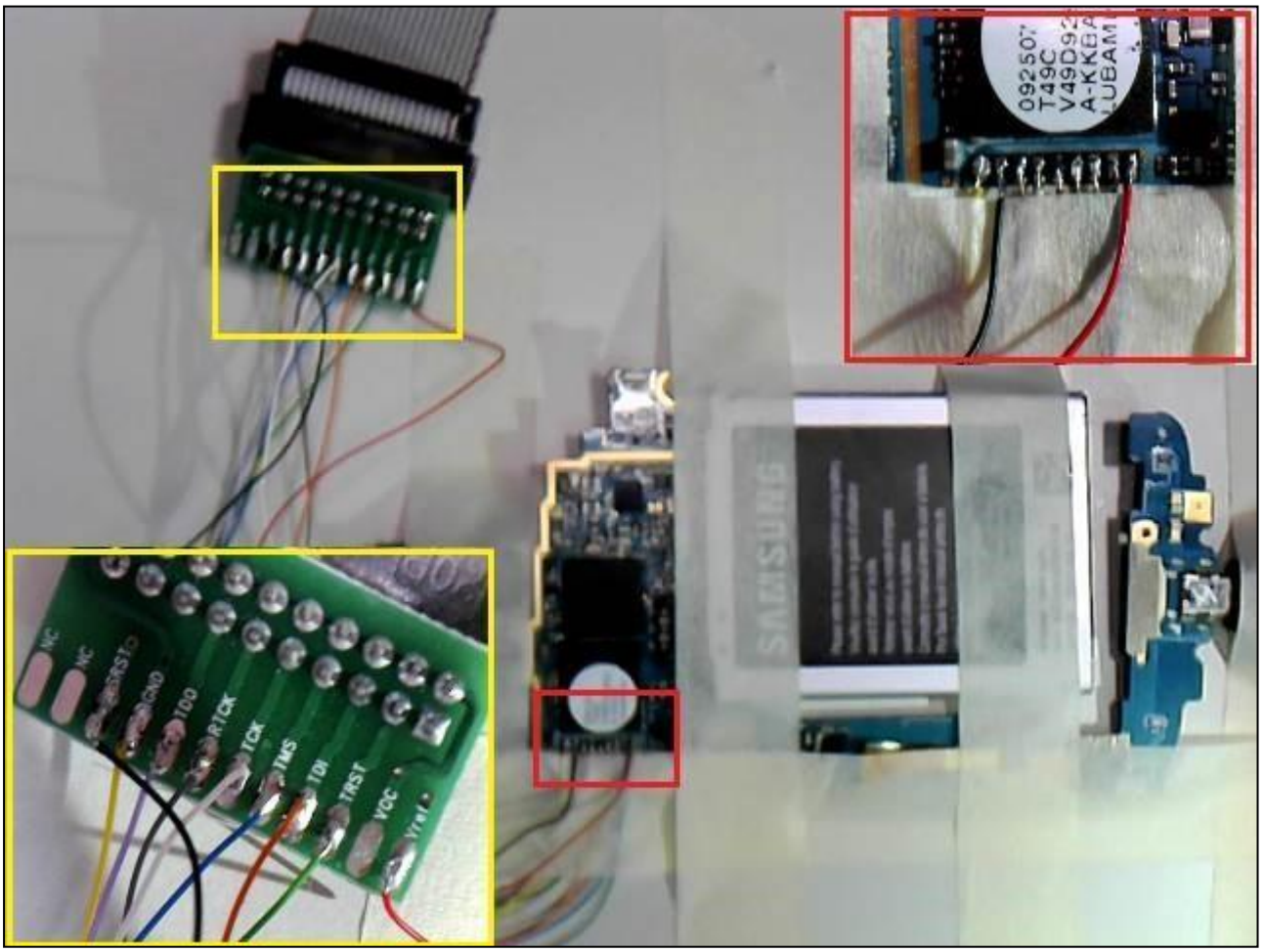


Figura 8 – Conexionado JTAG con RIFF Box – Fuente: Producción Propia

Una vez realizado el conexionado, se debe alimentar el celular, ya sea mediante batería o alimentación externa. Se recomienda utilizar ambas alimentaciones ya que el proceso de lectura es largo, esto aumenta el éxito de la extracción en caso de que alguna de las alimentaciones falle.

Luego se inicia el software de lectura, el cual se incluye con la caja de lectura adquirida. A continuación se puede ver una captura del software correspondiente a la caja Riff Box mientras inicia la lectura de este celular en particular:

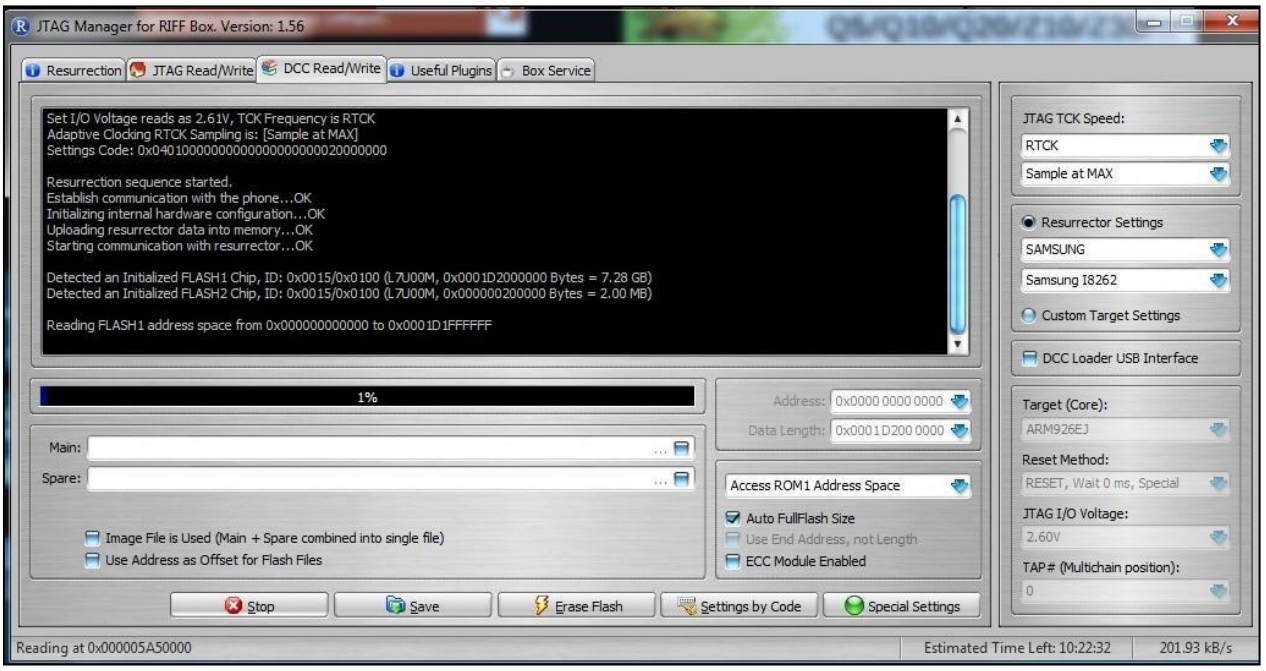


Figura 9 – Software de lectura para Riff Box – Fuente: Producción Propia

Extracción de datos utilizando una conexión "ISP"

Al igual que el método JTAG, la extracción de datos a través del método ISP (In-system programming) o también llamado ICSP (in-circuit serial programming) es del tipo invasiva pero no destructiva, tales como las que veremos más adelante (chip-off), y permite realizar un volcado completo de la memoria aunque el dispositivo este dañado (placa principal, pantalla rota, conector USB dañado, microprocesador, circuito de alimentación), la única condición es que la memoria de datos funcione. También posibilita la extracción de datos aunque el dispositivo posea algún tipo de seguridad con clave de usuario (patrón, contraseña, etc.).

Es condición para que el volcado de memoria sea legible, que la memoria de datos no este encriptada.
Este método explota la capacidad de algunos dispositivos programables, tales como microcontroladores o memorias, para programarse mientras están instalados en un sistema completo, en lugar de requerir extraer el chip para programarse antes de instalarlo en el sistema.
También permite enviar actualizaciones de firmware a la memoria sin necesidad de circuitos de programación especializados en la placa de circuito y simplifica el trabajo de diseño. Esta capacidad es la que permite leer la memoria de datos sin necesidad de extraerla del circuito.
La condición principal para poder aplicar este método es poder localizar los pines necesarios en el circuito. Estos son:

- Vpp o Vddf: Tensión de programación
- Vdd: Alimentación positiva
- Vss: Alimentación negativa
- CLK: Reloj
- DAT0: Bus datos serie
- CMD: Bus de comandos

Estos son los mismos pads o contactos que deberemos conectar en el método que se verá más adelante (chip-off), los cuales serán fácilmente localizables en la hoja de datos de la memoria que queremos leer, dado que en el método chip-off, la memoria es retirada de la placa (PCB) del dispositivo. Para ejemplificar esto, se describirá a continuación la configuración de pines de una memoria muy común utilizada en dispositivos móviles, la memoria Samsung KLMAG2WEMB-B031 de 16 Gigabyte de capacidad:

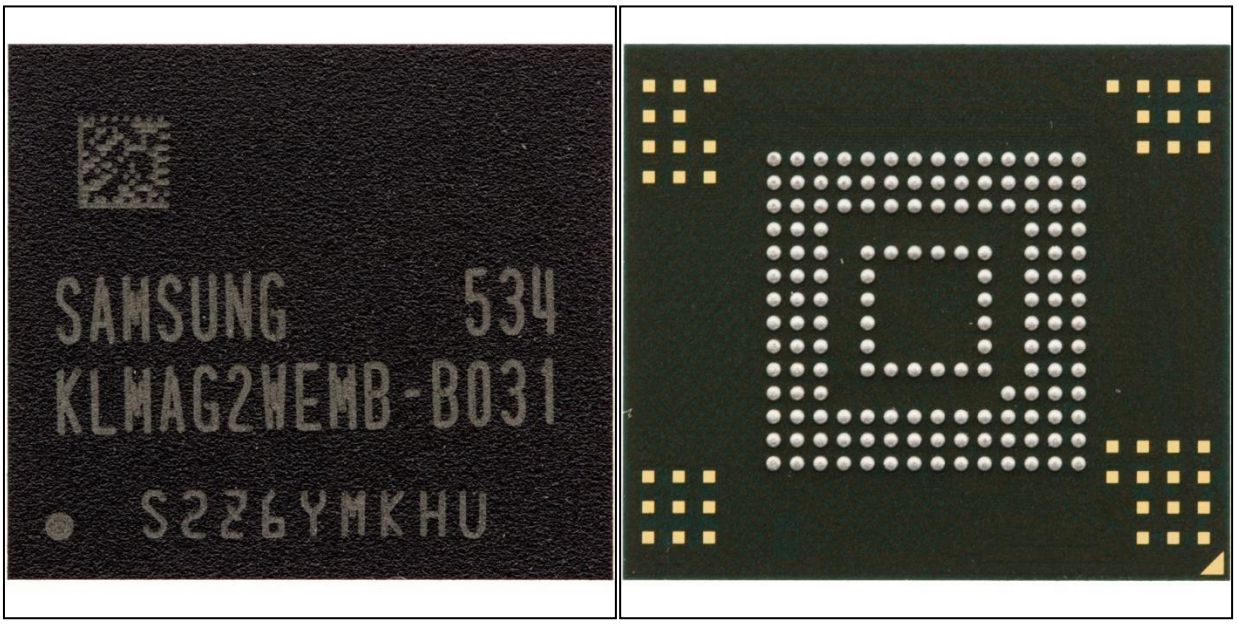


Figura 10 – Memoria e-MMC - Fuente: Producción Propia

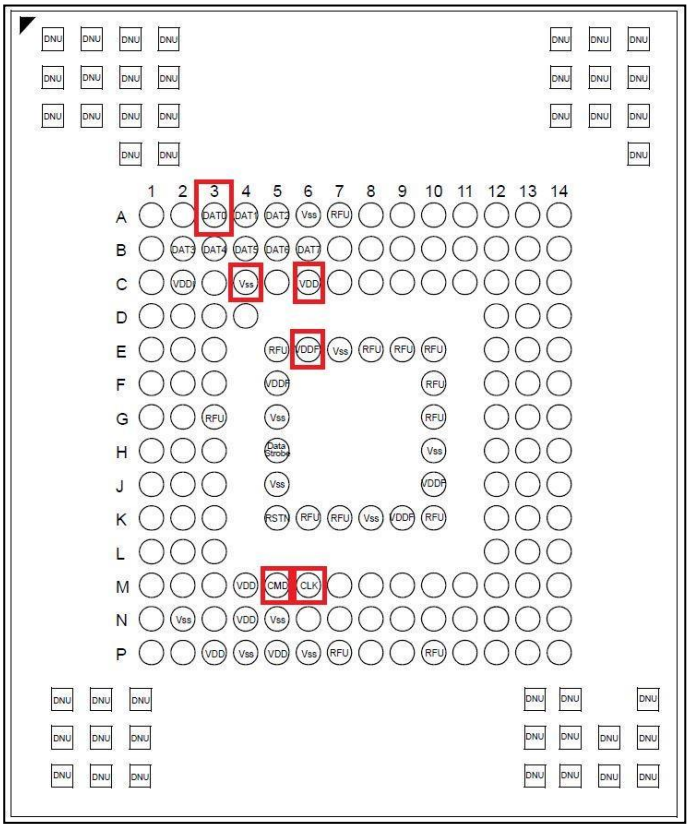


Figura 11 – PinOut - Fuente: Producción Propia

En los recuadros rojos se resaltan los pines de interés.

Esta memoria es del tipo e-MMC (embedded MultiMediaCard). Este tipo de memoria no es más que una memoria MMC (MultiMediaCard) que se encuentra soldada (o incorporada) en el dispositivo, a diferencia de las MMC que generalmente son removibles.

Ambas memorias utilizan tecnología NAND Flash, son no volátiles, y se pueden borrar y reprogramar eléctricamente.

Sin profundizar en el tema, podemos decir que las memorias NAND, reciben su nombre de las puertas lógicas NAND, las cuales producen una salida falsa solamente si todas sus entradas son verdaderas:

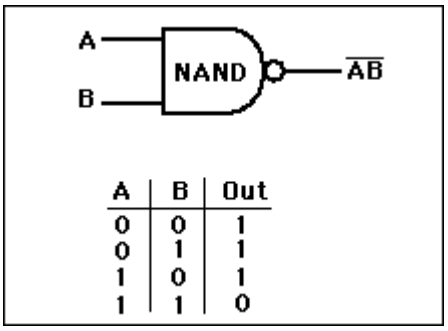


Figura 12 – Compuerta NAND - Fuente: Producción Propia

Respecto a la tecnología "flash", diremos que permite borrar de a bloques mediante impulsos eléctricos, a diferencia de las antecesoras EEPROM (Electrically Erasable Programmable Read Only Memory), que permiten solo el borrado byte a byte y aún más antiguas, las EPROM (Erasable Programmable Read Only Memory), que solo permiten el borrado completo mediante la exposición a rayos ultravioletas.
Las memorias Flash son más densas (más capacidad de almacenamiento, en menos espacio) y baratas que las anteriores. Es por esto que se han convertido en las más utilizadas en este tipo de dispositivos.

Volviendo a lo que interesa en este capítulo, y recordando lo que dijimos al inicio, "*La condición principal para poder aplicar este método es poder localizar los pines necesarios en el circuito*", y dado que la memoria se encuentra soldada en el PCB y no hay acceso a los pines de conexión, debemos conocer el recorrido de las conexiones de estos pines de interés.
Esto se podrá hacer de dos o tres maneras.

La primera y más rápida, es conocer el esquemático o diagrama de conexiones del dispositivo y la ubicación de los componentes, pistas y test point en el PCB, tal como se muestra en el dispositivo siguiente:

Ejemplo para un Samsung GT-S5360:

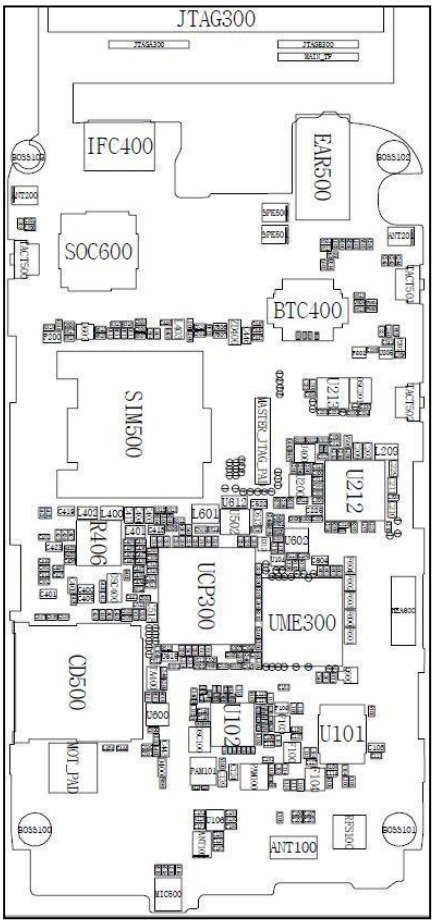


Figura 13 – PCB con la ubicación de los componentes – Fuente: Producción Propia

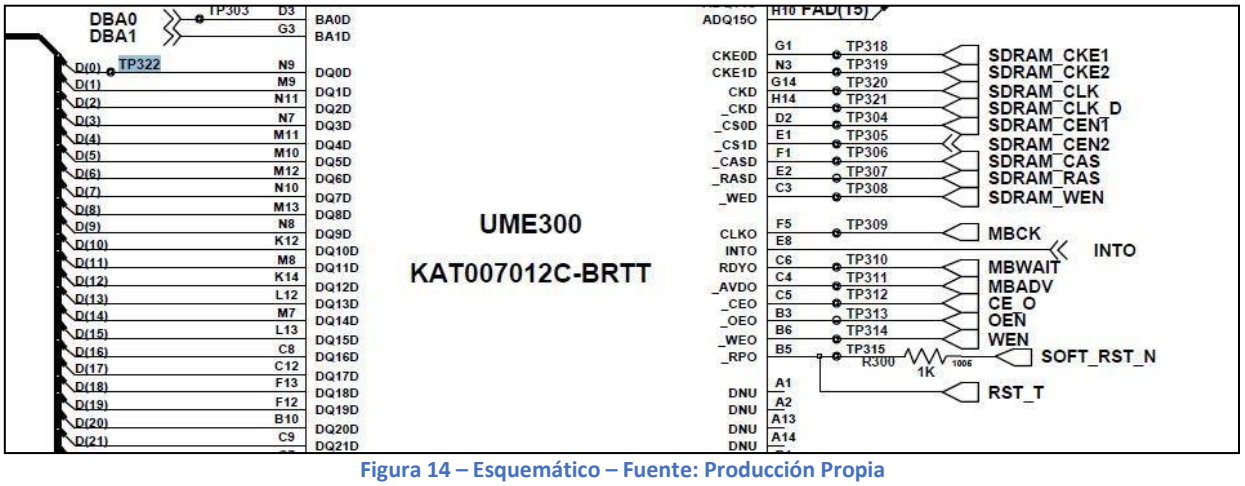


Figura 14 – Esquemático – Fuente: Producción Propia

En la figura 13 podemos ver el PCB con la ubicación de los componentes. En ella debemos ubicar la memoria de datos, esto lo podemos hacer desde el esquemático o directamente leyendo el código impreso que permite acceder a la hoja de datos con la información, la cual podemos encontrar en internet.

Luego, en el esquemático buscaremos las líneas de conexión de interés. En este caso encontramos las líneas de interés leyendo las referencias. Por ejemplo para la línea de datos "DAT0", encontramos la referencia D(0) y vemos que el PCB incluye un test point para esta línea, así que ubicamos dicho test point en el PCB y ya tenemos una de nuestras conexiones. A continuación se ilustra esto en las figuras siguientes:

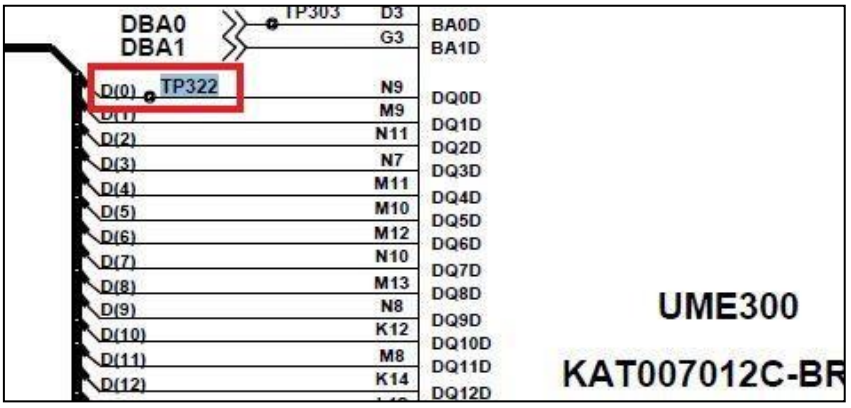


Figura 15 – Línea DAT0 en el esquemático – Fuente: Producción Propia

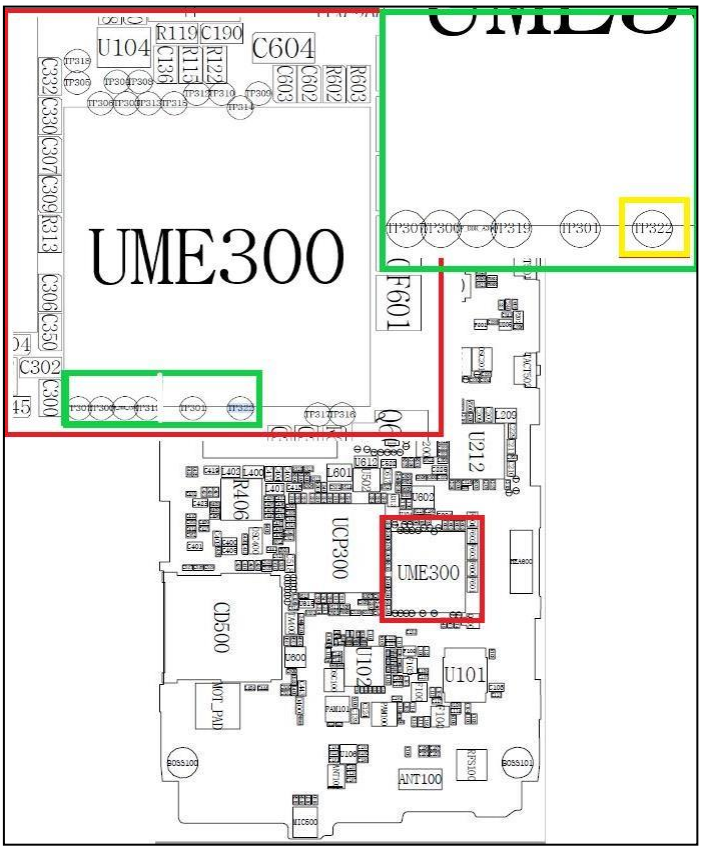


Figura 16 – Ubicación del test point correspondiente a DAT0 en el PCB – Fuente: Producción Propia

En otros casos no encontraremos test point y deberemos conectar nuestras líneas de interés en una pista del PCB, el borne de una resistencia, bobina, capacitor, etc. A continuación se ilustra una conexión típica de este método:

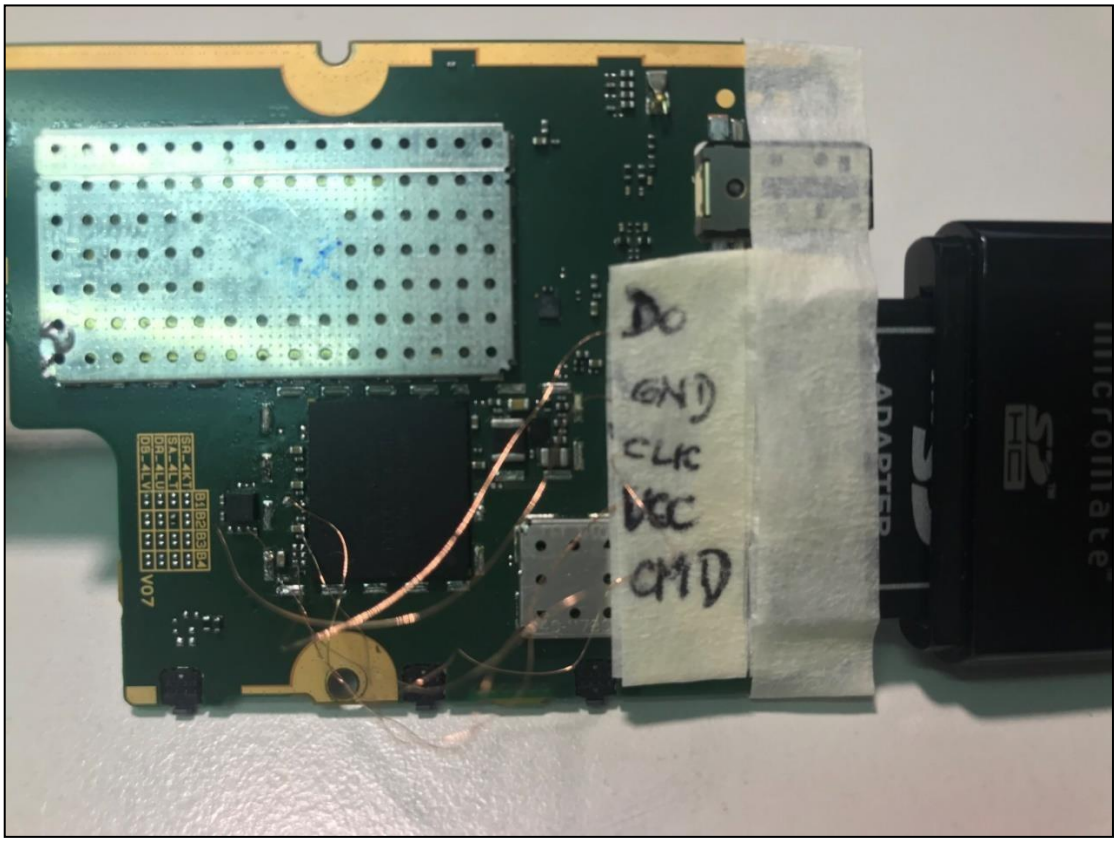


Figura 17 – Nokia Lumia 530 conectado para volcado de memoria por método ISP – Fuente: Producción Propia

En este caso se obtuvo el diagrama de conexión realizando una búsqueda en internet (*Sitio web de Forensics Wiki. Disponible en: https://forensicswiki.xyz/wiki/index.php?title=JTAG_and_Chip-Off_Tools_and_Equipment. Accesible: 21/04/2022*). Varios de estos diagramas son ofrecidos por las mismas empresas que fabrican las cajas ya descriptas en el capítulo anterior. En este caso, el diagrama se encuentra como imagen, tal como se muestra en la figura siguiente:

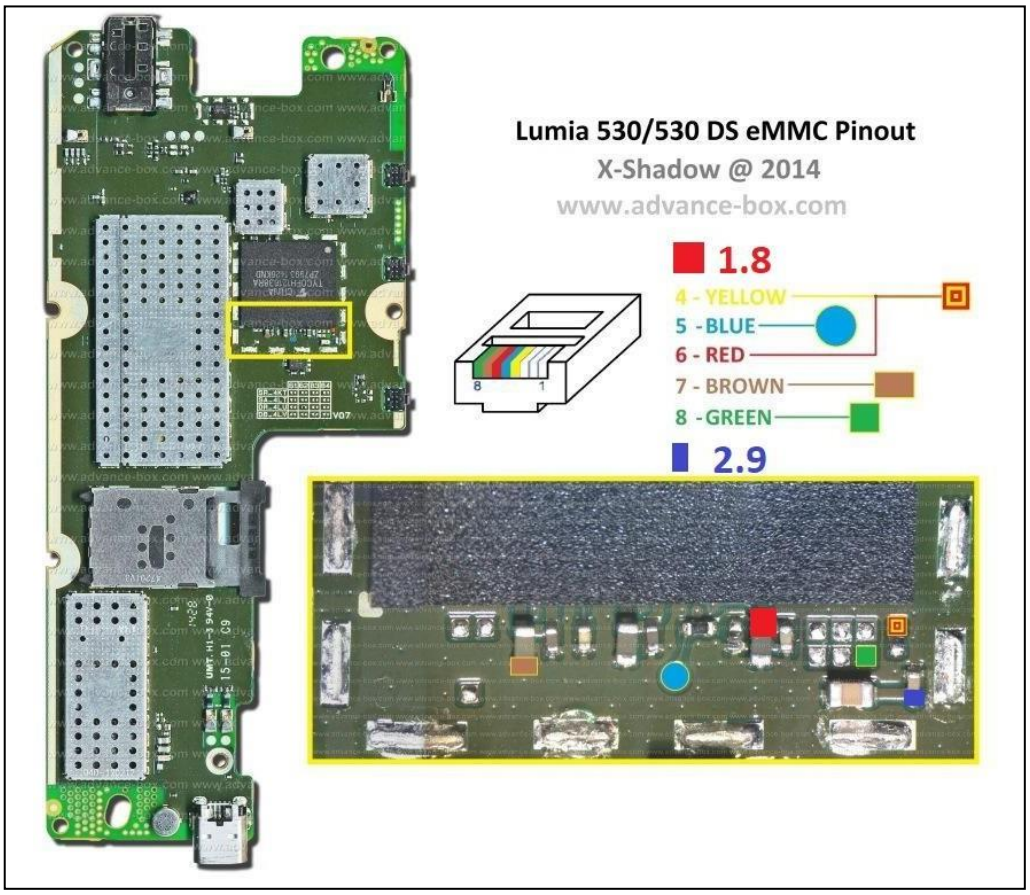


Figura 18 – Diagrama de conexión para lectura de memoria por método ISP – Fuente: https://gsmserver.es/

Notar en este caso que antes de poder acceder a los lugares de conexión se debió retirar el blindaje de la memoria. Esto se realiza con una estación de soldadura por aire caliente:

Figura 19 – Estación de soldado por aire caliente - Atten ST862D – Fuente: https://mtkargentina.com.ar

También es posible desoldarla con un soldador convencional, aunque necesita un poco más de esfuerzo y práctica. Otra opción es cortar con cuidado el blindaje. Esto puede realizarse con un "cutter" o torno tipo "Dremel" con un disco de cote delgado.

Para la lectura se puede utilizar una de las cajas antes descriptas, con el accesorio para este fin. La mayoría posee compatibilidad para realizar esta tarea y también incluyen los diagramas de conexión en el software de adquisición.

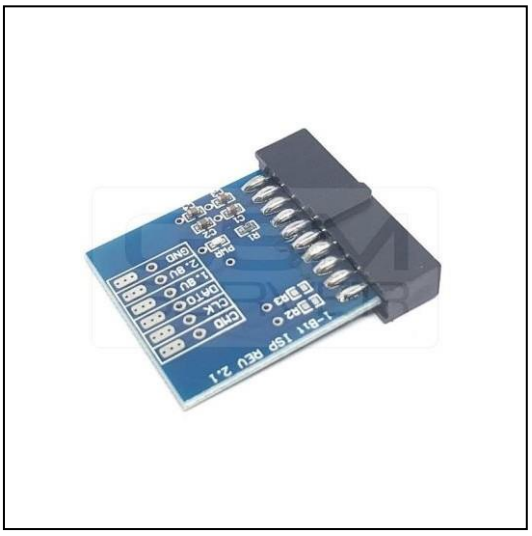
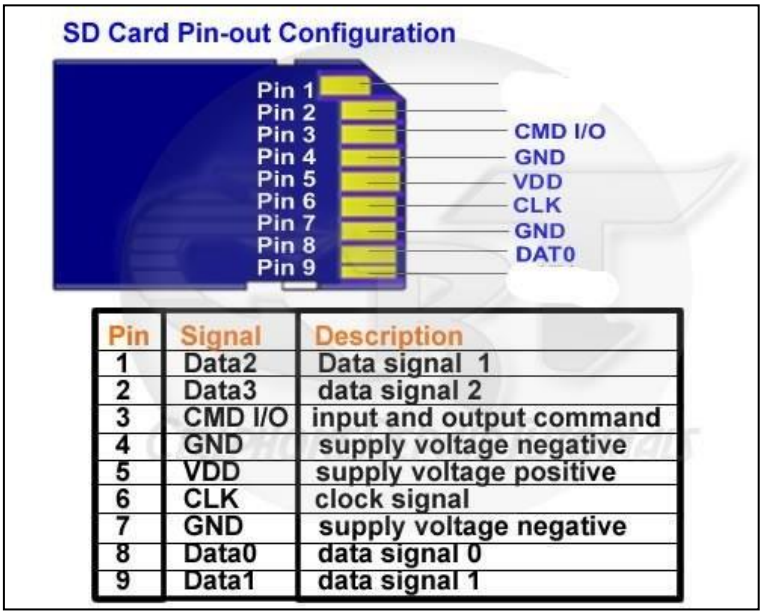


Figura 20 – Accesorio ISP para EASY JTAG BOX – Fuente: Producción Propia

En caso de no contar con una caja de este tipo, es posible leer este tipo de memorias con un lector convencional de memorias SD.
Los lectores de este tipo de memorias poseen el siguiente pinout:



Pin	Signal	Description
1	Data2	Data signal 1
2	Data3	data signal 2
3	CMD I/O	input and output command
4	GND	supply voltage negative
5	VDD	supply voltage positive
6	CLK	clock signal
7	GND	supply voltage negative
8	Data0	data signal 0
9	Data1	data signal 1

Figura 21 – Pinout lector de tarjetas SD – Fuente: Producción Propia

Como se ver, aquí tenemos los conectores necesarios para conectarnos al PCB del dispositivo para realizar el volcado de memoria por método ISP.

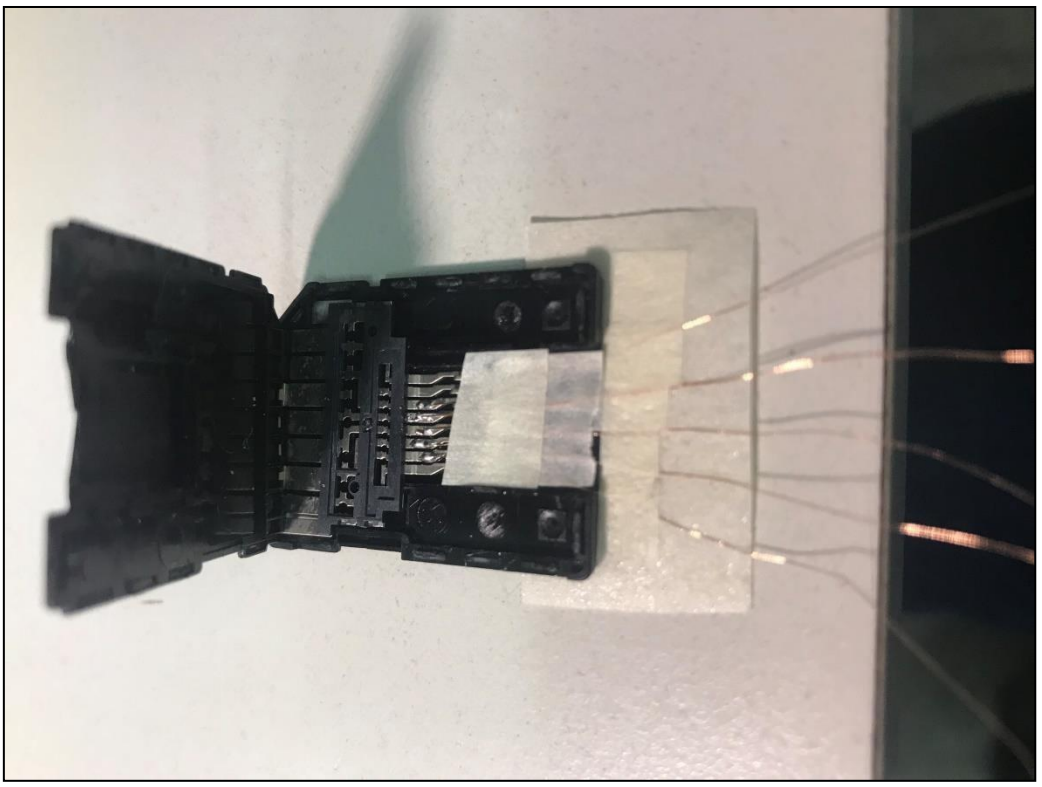


Figura 22 – Lector casero ISP – Fuente: Producción Propia

En la figura anterior se ve cómo fabricar un lector para ISP con un adaptador de memoria de micro SD a SD. Este adaptador se utiliza con un lector convencional USB de tarjetas SD, tal como se ve en la figura siguiente:

Figura 23 – Lector USB con adaptador para micro SD modificado para ISP – Fuente: Producción Propia

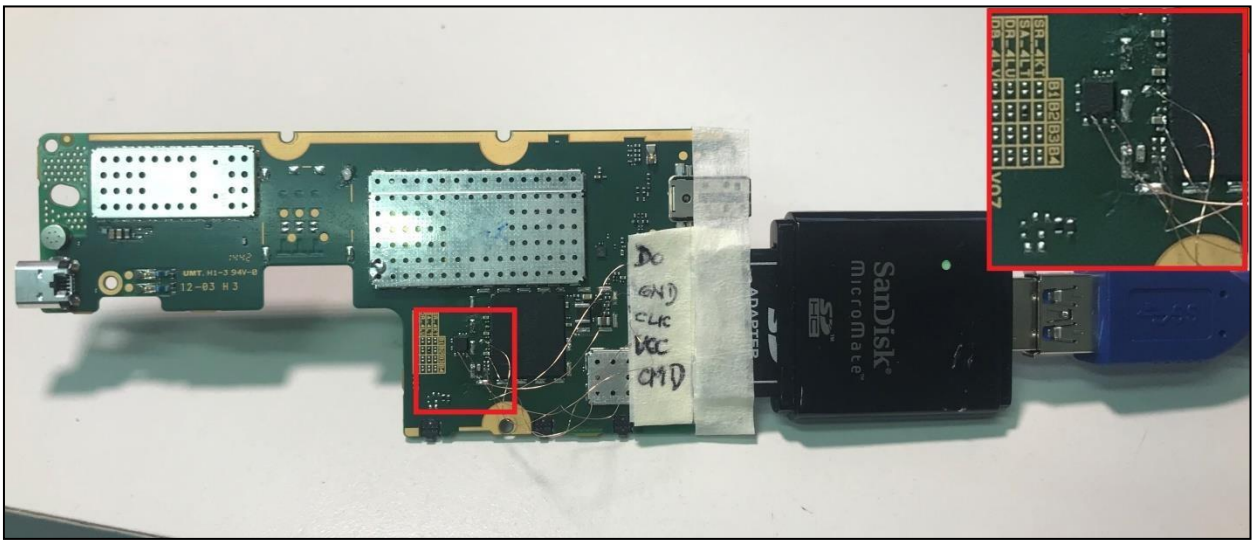


Figura 24 – Placa conectada con el lector ISP casero – Fuente: Producción Propia

Para realizar este tipo de soldaduras en el PCB se recomienda usar un soldador con temperatura regulada para evitar dañar el PCB. Un ejemplo de esto es la estación de soldado GOOT-RX-802AS:

Figura 25 – Estación de soldado GOOT-RX-802AS – Fuente: Producción Propia

El alambre de conexionado deberá ser muy delgado y barnizado, para proporcionar aislación eléctrica. Este tipo de alambre barnizado es muy cómodo de trabajar ya que al estañar la punta el aislante desaparece, evitando así tener que quitar manualmente la aislación para estañar las puntas. La figura siguiente muestra un rollo de este tipo de alambre:

Figura 26 – Alambre barnizado – diámetro 0.09 mm – Fuente: Producción Propia

Para realizar las soldaduras se recomienda el uso de una lupa o microscopio analógico o digital con una distancia focal de al menos 10 cm, para poder trabajar cómodamente debajo del objetivo. Estos son algunos ejemplos de lupas o microscopios:

Figura 27 – Lupa digital y analógica – Fuente: https://www.gadnic.com.ar/

Otra opción para realizar las conexiones en el PCB sin soldaduras es utilizar un dispositivo llamado “CODED” el cual posee varios brazos regulables que en su extremo poseen un

electrodo de conexión que se apoya en el contacto de interés del PCB. A continuación se muestran algunas imágenes de este dispositivo:

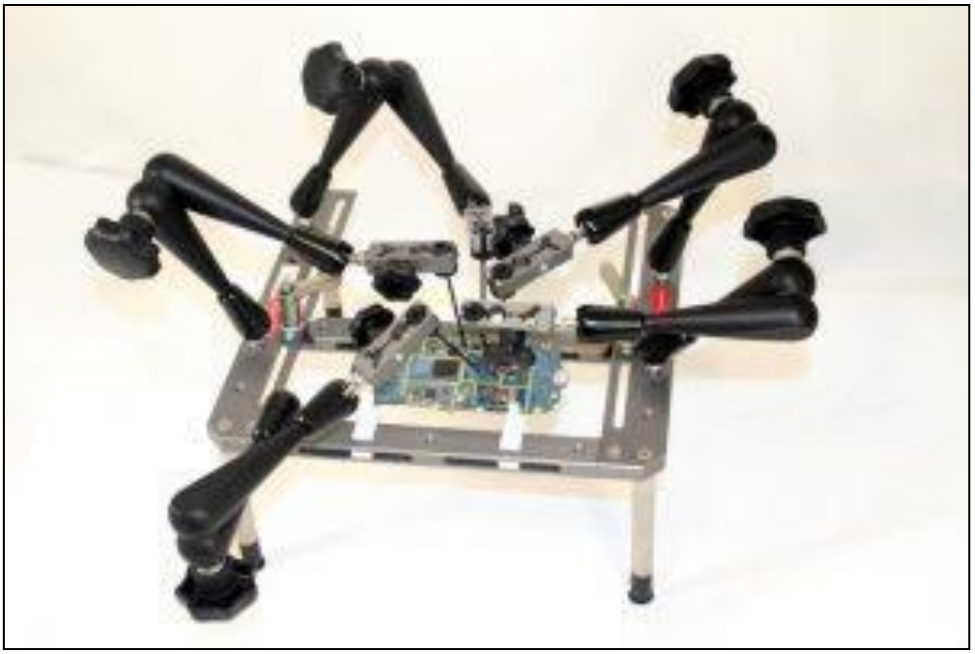


Figura 28 – CODED – Fuente: Producción Propia

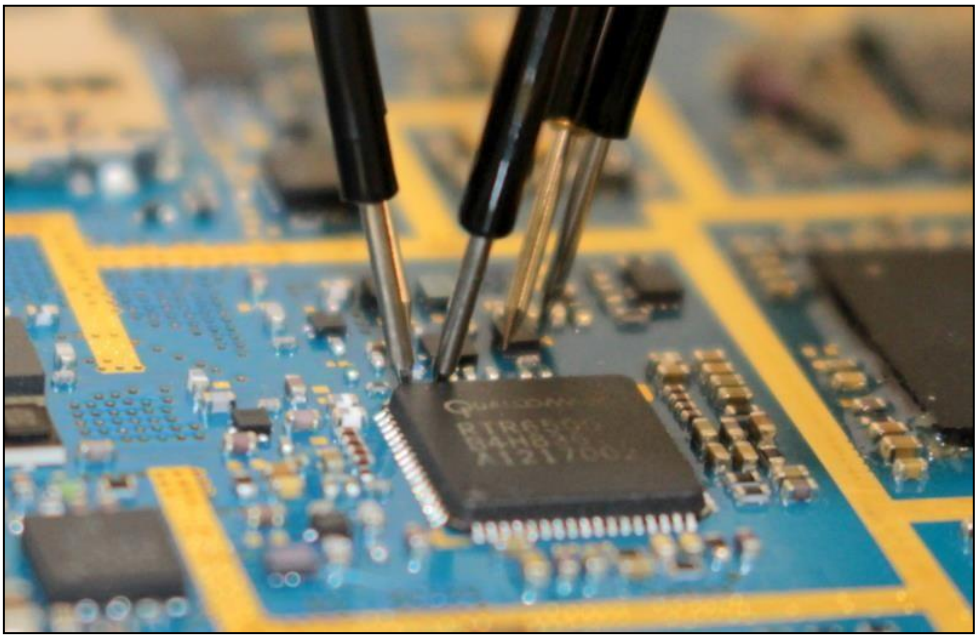


Figura 29 – CODED – Fuente: Producción Propia

Una vez realizadas las conexiones en el PCB, procedemos al volcado de la memoria. Esto lo podemos hacer desde la caja “Box” que estemos usando, de la misma manera que lo hicimos en el capítulo anterior con el método “JTAG”.

En el caso de que estemos usando el lector casero propuesto, fabricado con un lector de memorias SD, al conectar éste al puerto USB de una PC con Windows nos aparecerá un mensaje de Windows que pregunta si deseamos formatear la unidad, por supuesto que no debemos aceptar este mensaje.
A continuación debemos realizar el volcado de la memoria, una buena opción es utilizar el "FTK Imager" ya que es un software muy potente y libre.
Debemos ir al menú "File" luego a "Create Disk Image" y elegir la opción "Physical Drive", aquí debemos buscar el lector que estemos usando y verificar con el tamaño de la memoria que estamos por leer:

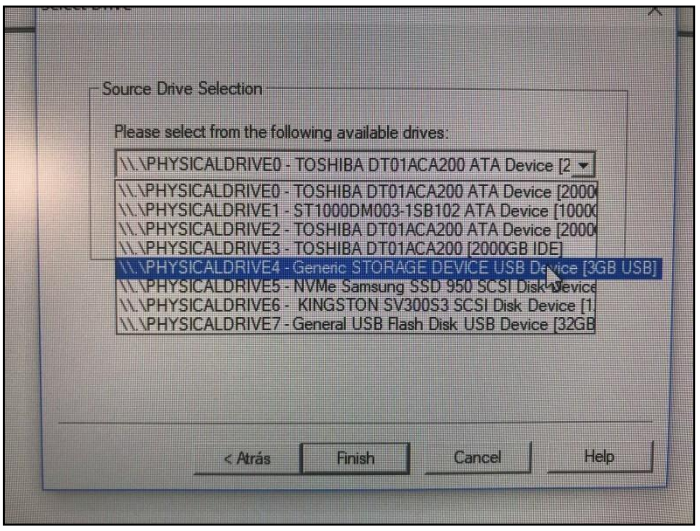


Figura 30 – Selección disco físico para el volcado de memoria – Fuente: Producción Propia

Una vez realizado este paso debemos especificar qué tipo de formato y dónde queremos guardar la imagen. El formato recomendado es sin compresión o más conocido como RAW. También existen otros que utilizan algún tipo de compresión como el E01 (formato de archivo de imagen EnCase, utilizado por el software EnCase). Hecho esto, ya podemos iniciar la lectura de la memoria:

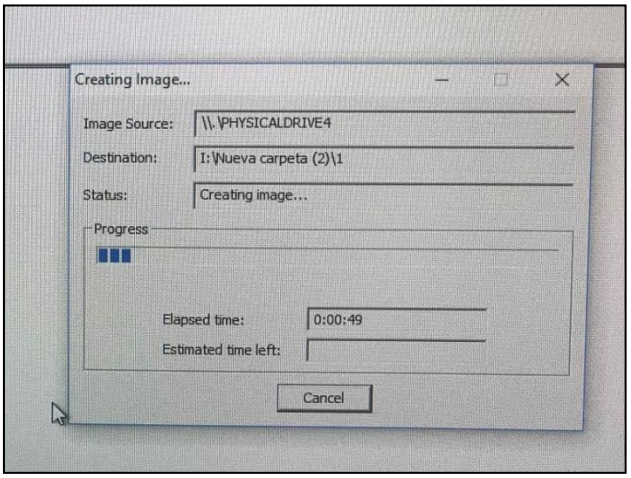


Figura 31 – Volcado de memoria con FTK Imager – Fuente: Producción Propia

Extracción de datos utilizando la técnica "Chip-Off"

En este caso la extracción de datos es del tipo invasiva y destructiva. Es utilizada cuando el método ISP no es posible, generalmente porque no fue posible hallar las conexiones necesarias en el PCB. Al igual que los dos métodos anteriores, permite realizar un volcado completo de la memoria aunque el dispositivo este dañado (placa principal, pantalla rota, conector USB dañado, microprocesador, circuito de alimentación). La única condición es que la memoria de datos funcione. También posibilita la extracción de datos aunque el dispositivo posea algún tipo de seguridad con clave de usuario (patrón, contraseña, etc.). Al igual que antes, es condición para que el volcado de memoria sea legible, que la memoria de datos no esté encriptada.

Consiste en extraer el chip en el que residen los datos desoldándolo de la placa para posteriormente leerlo y conseguir una imagen. Con ese sistema es posible recuperar archivos (incluso archivos borrados) de dispositivos dañados físicamente.

Para desoldar la memoria de datos del PCB se deberá, en primer lugar, retirar los blindajes en caso de que posea. Si bien la memoria se puede desoldar con una estación de aire caliente como la descripta anteriormente, se recomienda usar una herramienta diseñada para este fin, la misma consta de un calefactor inferior que calienta el PCB, ayudando a que el estaño funda más rápido que si solo calentamos el chip desde arriba. Esto disminuye las probabilidades de dañar la memoria por exceso de temperatura. Además, esta herramienta posee una luz infrarroja que se enfoca sobre el chip de interés y lo calienta. A continuación se muestra una estación de soldado infrarroja básica como ejemplo (Fuente: http://www.tech168.cn/Item/Show.asp?m=1&d=3086):

Figura 32 - Estación de Soldado Infrarroja Yaxun YX-862D++ – Fuente: Producción Propia

Se deberá retirar completamente el PCB del dispositivo, también desconectar todos los periféricos que sea posible, tales como cámaras fotográficas, sensores, pantalla, etc. Luego se configura la temperatura del calefactor inferior, este calentará todo el PCB, deberá ser una temperatura suficiente pero no demasiada como para fundir el estaño y otros componentes del PCB. Se recomienda una temperatura cercana a los 150 grados centígrados. Una vez que la temperatura del PCB se estabilice se procederá a encender el calefactor infrarrojo, configurado entre 250 y 350 grados. Se recomienda calentar tiempos cortos e ir verificando cuando la memoria se suelte, para evitar sobrecalentamiento y reducir la probabilidad de daño de la memoria. No obstante, se recomienda leer las especificaciones de cada estación de soldadura y seguir los pasos que el fabricante recomiende.

Una vez retirada la memoria se deberá retirar el exceso de estaño con un soldador de estaño y el agregado de flux, también nos podemos ayudar utilizando una “cinta de desoldar”.

El flux para soldar, también conocido como fundente para soldar es un producto químico, generalmente en forma de pasta fluida, que al ser aplicado sobre los componentes que vamos a soldar elimina el óxido existente entre ellos aumentando sustancialmente la calidad de la soldadura. Además facilita mucho el trabajo de soldar ya que concentra el calor y lo reparte de forma uniforme en la zona de trabajo. Existen diferentes composiciones del flux y siempre se trata de mezclas de agentes químicos activos (ej.: cloruro de zinc, cloruro de amonio, etc.) con otros elementos que actúan como disolventes, aditivos y componentes protectores contra el oxígeno.

Luego deberá limpiar con algún solvente, tal como puede ser alcohol Isopropílico. Ahora si estamos en condiciones de proceder a la lectura. Para esto podremos usar diversos zócalos de lectura que vienen diseñados para este fin y se conectan directamente a un lector de memorias tipo “SD”.

A continuación se puede ver un ejemplo de este zócalo:

Figura 33 - Adaptador SIREDA BGA a SD – Fuente: Producción Propia

Estos adaptadores vienen para todos los tipos de memorias. En caso de no contar con el adaptador, es posible soldar los pines necesarios directamente sobre el chip y conectarlos al lector casero que vimos en el capítulo anterior.

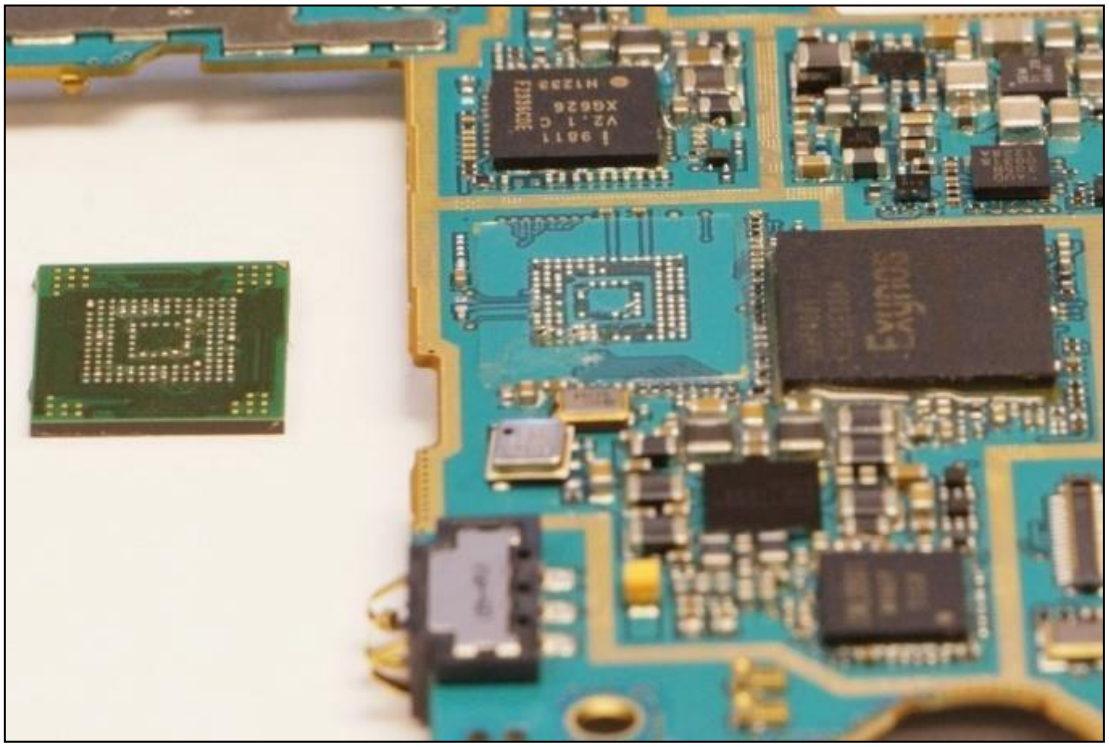


Figura 34 – Memoria desoldada del PCB y lista para ser leída – Fuente: Producción Propia

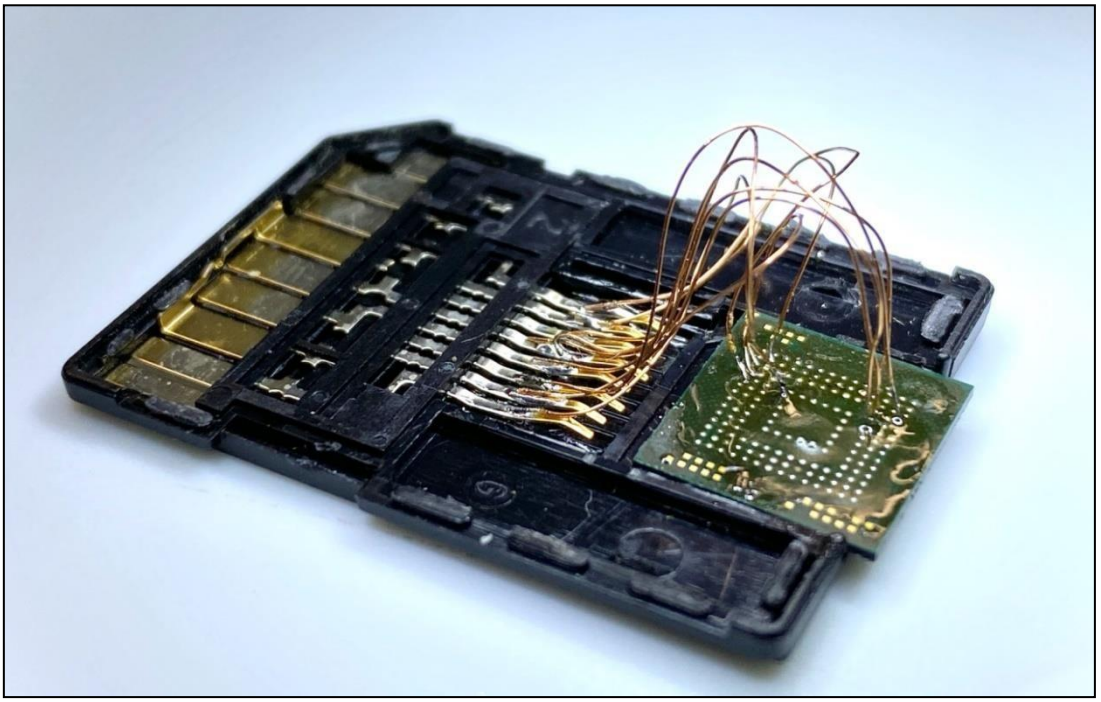


Figura 35 – Lectura directa sin zócalo con lector SD convencional – Fuente: Producción Propia

Al ver la figura 35, queda claro que esta tarea se debe realizar con una lupa o microscopio y un soldador de buena calidad y que posea una punta lo bastante delgada como para poder realizar las soldaduras. El alambre, al igual que antes, debe ser muy delgado y barnizado.

Los pines de conexión necesarios se deberán obtener de la hoja de datos de la memoria en cuestión.

Al igual que antes, el volcado de la memoria lo podemos realizar con “FTK Imager”.

Recomendaciones y herramientas necesarias para acceder al puerto de conexión cuando este no funciona

Este problema en los celulares y otros dispositivos móviles que poseen puerto de conexión es, sin dudas, el problema más común, dado que es el mismo puerto que se usa para cargar la batería del dispositivo.

El uso constante de este puerto, y muchas veces la utilización del mismo en el momento que está conectado, hace que el conector comience a hacer falso contacto, y luego a desoldarse del PCB. Otro problema común es la falla solo en la conexión de datos, muchas veces el dispositivo carga normalmente pero al conectarlo al puerto USB de la PC ésta no lo reconoce.
Esta falla puede deberse simplemente a que los contactos del puerto de datos están dañados o, lo más común, es la intervención de algún servicio técnico que realizo la reparación del conector USB pero que solo dejo conectado los pines de carga y no los de datos.

Como primera medida debemos evaluar la posibilidad de obtener datos por otros medios que no sea el puerto de conexión USB. A veces es posible obtener datos a través de una conexión Bluetooth.

La primera intervención que debemos hacer para solucionar un problema de conexión en el puerto es la limpieza. Muchas veces se acumula polvo, fibras textiles, etc. en el conector, y al insertar el cable de carga se va compactando en el fondo del conector, que hace que la ficha de conexión no se inserte completamente. Podemos "rascar" cuidadosamente el fondo del conector con un alfiler, retirando de a poco los residuos. Luego podemos utilizar aire comprimido para soplar y retirar la suciedad que se liberó. En lo posible el aire debe estar libre de humedad, se recomienda utilizar algún removedor de partículas con aire inerte, el más común es nitrógeno. A continuación se muestra un producto que se consigue en nuestro país:

Figura 36 – Aire inerte comprimido "Compitt OR" marca DELTA - Limpieza puerto USB con alfiler – Fuente: Producción Propia

La limpieza se debe hacer progresiva, esto significa que debemos limpiar lo suficiente para que funcione el conector y disminuir al máximo las probabilidades de dañar el conector al estar realizando la limpieza. Recordemos que la finalidad es lograr la extracción de datos y no la reparación del dispositivo.

En caso de que la limpieza no funcione, el próximo paso será la limpieza con algún solvente que no deje residuos de humedad en el conector. Se recomienda usar algún limpiador de contactos tipo “Contacmatic ® Super” de la empresa DELTA:

Figura 37 - Contacmatic ® Super” de la empresa DELTA – Fuente: Producción Propia

Se deberá rociar siempre el conector de tal manera que éste se encuentre en la parte más baja, para evitar que el líquido ingrese dentro de la carcasa del dispositivo. Este proceso y el anterior se pueden repetir alternadamente hasta lograr que el puerto funcione.
Cuando ninguno de estos métodos funcione, deberemos desarmar el dispositivo para lograr llegar al PCB en la parte donde se encuentra soldado el conector:

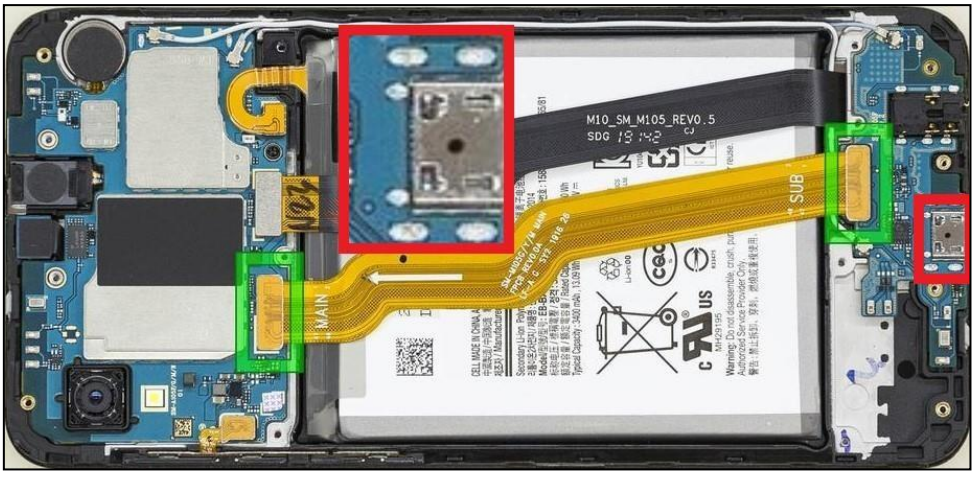


Figura 38 – Identificación del conector una vez desarmado el dispositivo. – Fuente: Producción Propia

Para lograr llegar al conector deberemos desarmar el dispositivo en cuestión. Esta tarea varia ampliamente entre distintos dispositivos, desde algunos que solo se deben quitar algunos tornillos, hasta los que requieren una herramienta especial para lograr despegar la tapa trasera, o hasta en algunos casos, despegar la pantalla para poder llegar al PCB.

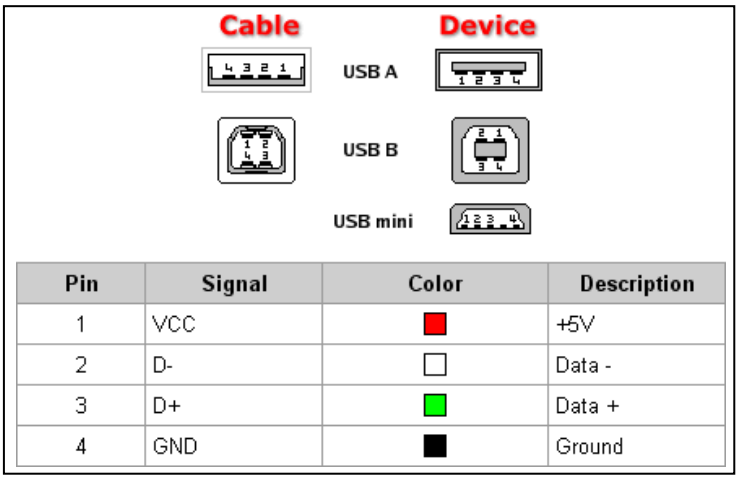
Una herramienta muy útil para despegar las pantallas de los dispositivos móviles es lo que se conoce como "estación separadora de pantallas", esta herramienta consiste en una plancha perforada con temperatura controlada y una bomba de vacío que fija la pantalla:

Figura 39 – Estación separadora de pantalla "Vaxun 943" – Fuente: Producción Propia

Una vez que se logró llegar a la parte interna del dispositivo y se ubicó el puerto USB, intentaremos en primer lugar retocar las soldaduras del conector.
Si esto aún no resuelve el problema, significa que el conector puede estar roto, para lo cual, en vez de cambiar el conector, soldaremos un chicote de cable que posea en un extremo un conector USB:

Figura 40 – Chicote USB – Fuente: Producción Propia

Para saber dónde soldar cada cable, consultaremos el pinout del puerto USB y micro USB:



Pin	Signal	Color	Description
1	VCC		+5V
2	D-		Data -
3	D+		Data +
4	GND		Ground

Figura 41 – Tipos de puerto USB y sus pinout - Fuente: Producción Propia

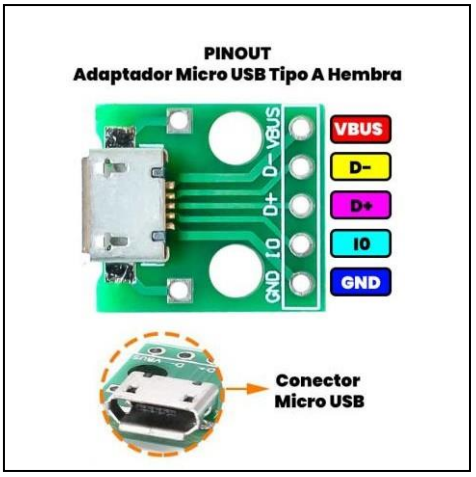


Figura 42 – Pinout Micro USB – Fuente: Producción Propia

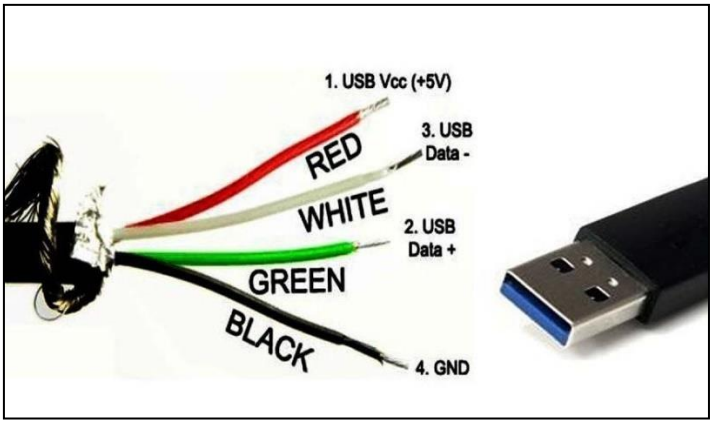


Figura 43 – Pinout USB – Fuente: Producción Propia

Ahora debemos soldar los cables del chicote USB a la placa madre o PCB del dispositivo. Esto los podemos hacer directamente en la patas del conector, utilizando un trozo de alambre delgado. También es posible localizar algún componente, tal como una bobina de choque o capacitor por donde pasen las pistas que van al conector USB. Esto se puede hacer utilizando un multímetro. Los multímetros son instrumentos de medición de magnitudes eléctricas, tales como diferencia de potencial (se mide en volt), corriente eléctrica (se mide en amperios), resistencia eléctrica (se mide en ohm), y otras.
Muchas veces esto es más sencillo que soldar directamente en los pads del conector (*ver la figura siguiente*).

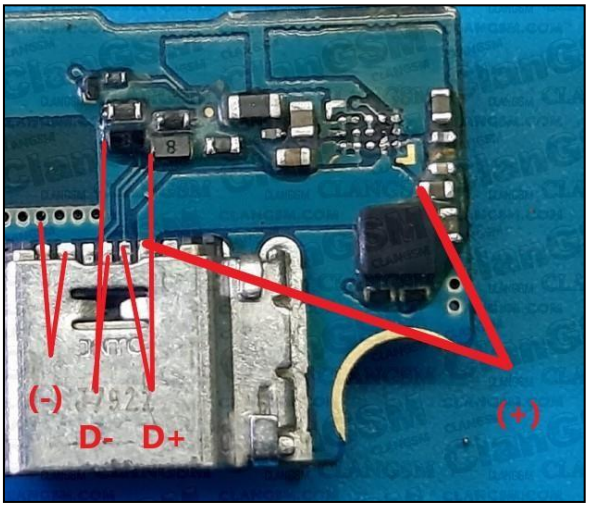


Figura 44 – Sitios de conexión para chicote USB – Fuente: Producción Propia

Recomendaciones y herramientas necesarias para energizar el dispositivo cuando la batería o circuito de carga no funcionan

Muchas veces los dispositivos móviles llegan sin batería, o la batería no carga a través del puerto USB, o la batería se encuentra dañada.

Para estos casos es fundamental contar con un Multímetro y una fuente de alimentación regulada con control de corriente, tal como la siguiente:

Figura 45 – Fuente de alimentación digital Yihua 1502D+ – Fuente: Producción Propia

Una de las primeras pruebas que podemos realizar, en caso de que el dispositivo lo permita (en los dispositivos con baterías internas no será posible), es conectar la fuente directamente en los bornes de conexión de la batería, respetando las indicaciones que están impresas en la batería:

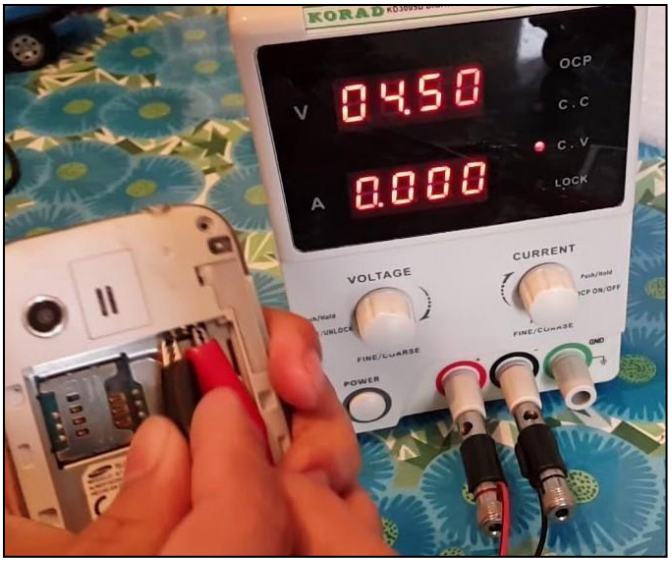


Figura 46 – Alimentación directa a los bornes de conexión – Fuente: Producción Propia

A continuación, calibramos la tensión de salida de la fuente un valor por encima de 4 volt y no más de 4,5 volt. Una vez conectados los cocodrilos a los bornes, procedemos a encender el dispositivo mirando el indicador de corriente. Si el circuito de alimentación del dispositivo está en funcionamiento veremos un incremento en el indicador de corriente. Una vez que soltamos el botón de encendido este consumo se debe mantener, e ira variando al iniciarse el sistema operativo.
En caso de que el dispositivo no posea batería, podemos averiguar la polaridad de los bornes buscando en internet (buscar la batería correspondiente y observar la polaridad en las imágenes) o realizando una medición de continuidad con un multímetro. Con esto podremos encontrar fácilmente el polo negativo en la mayoría de los dispositivos, ya que estará unido a las partes metálicas del dispositivo, tal como el conector USB, el zócalo de la memoria SIM, el zócalo de la tarjeta de memoria, etc. En general el polo positivo, será el opuesto.
En caso de que no se tenga una fuente de alimentación, también es posible utilizar una batería de litio cargada de cualquier otro dispositivo y conectarla a los bornes de la misma manera.

Cuando la batería no sea extraíble, la tarea se complica un poco más, dado que primero deberemos desarmar el dispositivo, y en la mayoría de los casos deberemos despegar la pantalla para poder acceder.
Una vez que se logre acceder a la batería, procedemos a verificar si la misma posee algo de carga, para esto necesitaremos un multímetro. Si la tensión es 0 (cero), es posible que el circuito de carga no funcione. En algunos casos el circuito de carga no logra comenzar la carga porque la batería consume más de lo que el circuito de carga puede aportar. En este caso podemos desconectar la batería y cargarla con una fuente externa, directamente en los bornes del conector:

Figura 47 – Conector batería interna celular – Fuente: Producción Propia

Si no tenemos la hoja de datos de la batería, podemos identificar el polo negativo al igual que antes, midiendo continuidad con un multímetro en el conector del PCB del dispositivo, buscando cuál de los contactos tiene continuidad a masa.
Una vez hecho esto podemos conectar la fuente de alimentación a los contactos a través de unos alfileres o directamente soldando unos chicotes de cable al conector.

En caso que la batería no funcione o no esté, es posible alimentar al igual que antes, conectando una fuente de alimentación directamente al conector de la placa, con la dificultad de que ahora no podremos usar los cocodrilos como antes dado el tamaño del conector:

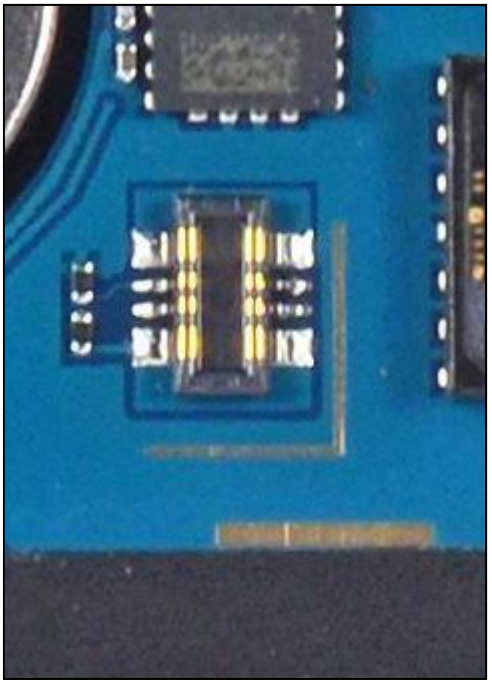


Figura 48 – Conector bacteria – lado del PCB – Fuente: Producción Propia

Aquí deberemos encontrar el polo negativo, al igual que antes, utilizando el multímetro. En este caso deberemos soldar unos chicotes de cable para poder conectar la fuente de alimentación externa. Los contactos más grandes son los correspondientes a los polos negativo y positivo. El resto generalmente son de algún control de carga o temperatura.

Recomendaciones y herramientas necesarias para extraer datos de memorias Flash del tipo “USB” o “Pen Drive” y memorias externas del tipo “SD” o “micro SD”, “MMC”, “Memory Stick”, etc. dañadas.

Dado que este tipo de memorias poseen dentro una memoria del mismo tipo que las vistas anteriormente, es posible aplicar los mismos métodos que antes (Chip.Off e ISP) para leer directamente la memoria. Esto es útil cuando la interfaz USB o la de lectura están dañadas.

Para los pendrive y memorias flash que poseen una estructura "clásica", con partes separadas, tales como un controlador, una PCB y un chip de memoria NAND con encapsulado, la tarea se simplifica mucho, dado que debemos preocuparnos solo por desoldar la memoria para luego llevar a cabo la lectura con las técnicas antes vistas, ya sea, soldando directamente chicotes de cables en las patas o pads correspondiente o utilizando un zócalo de lectura para el tipo de menoria que deseamos leer:

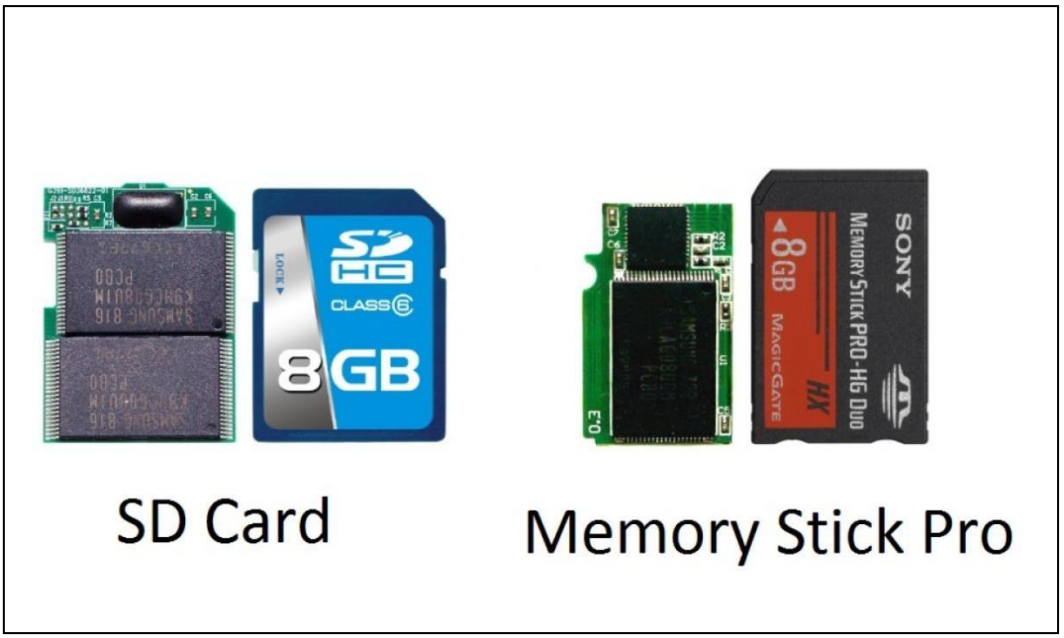


Figura 49 – Interior memoria “SD Card” y “Memory Stick Pro” luego de quitar el encapsulado – Fuente: Producción Propia

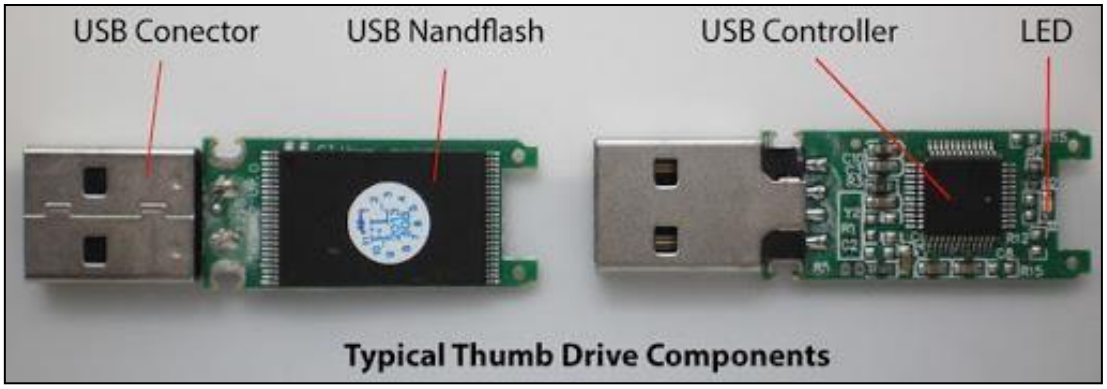


Figura 50 – Interior de un Pendrive “clásico” – Fuente: Producción Propia

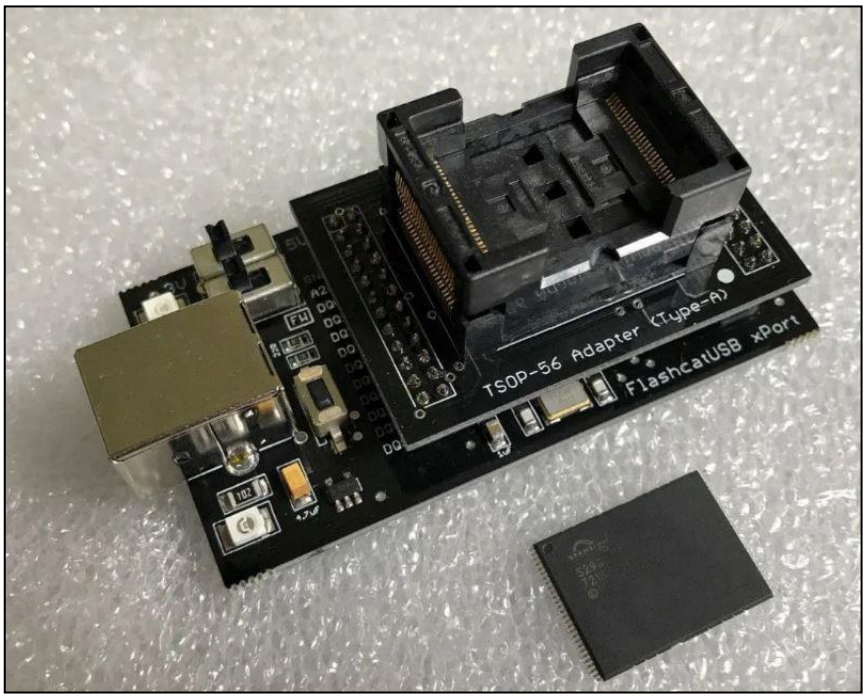


Figura 51 – Lector TSOP-48 – Fuente: Producción Propia

Dependiendo el tipo de memoria podremos adquirir un lector comercial para cada tipo de encapsulado. Para desoldar la memoria utilizaremos el método visto anteriormente en la sección "Extracción de datos utilizando la técnica "Chip-Off".
Esta técnica elimina cualquier falla que pueda tener la interfaz USB o el controlador de la memoria o pendrive.

La recuperación de datos se vuelve más complicada en los dispositivos flash NAND modernos, los cuales utilizan un tipo de arquitectura donde la interfaz, el controlador y los chips de memoria están integrados en una capa de cerámica común, esto se conoce como estructura monolítica:

Figura 52 – Memoria micro SD – Fuente: http://www.pc3000flash.com/

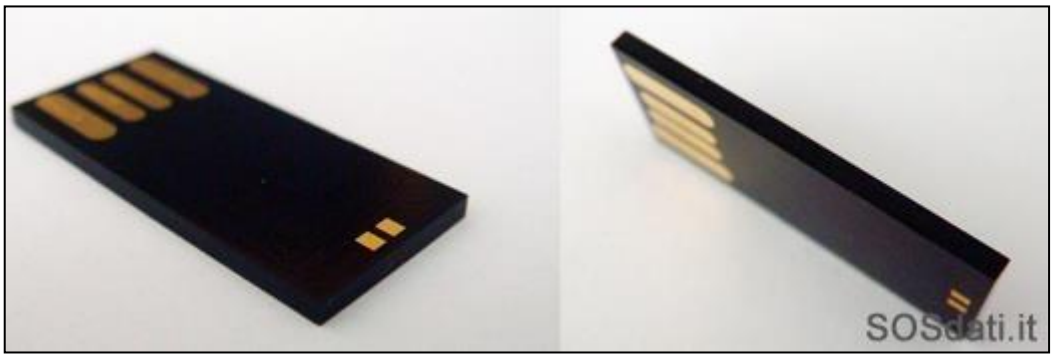


Figura 53 – Pendrive en formato monolítico – Fuente: http://www.pc3000flash.com/

En este tipo de dispositivos solo tenemos disponible los contactos de la interfaz de datos, aunque en su interior tiene los mismos componentes vistos anteriormente:

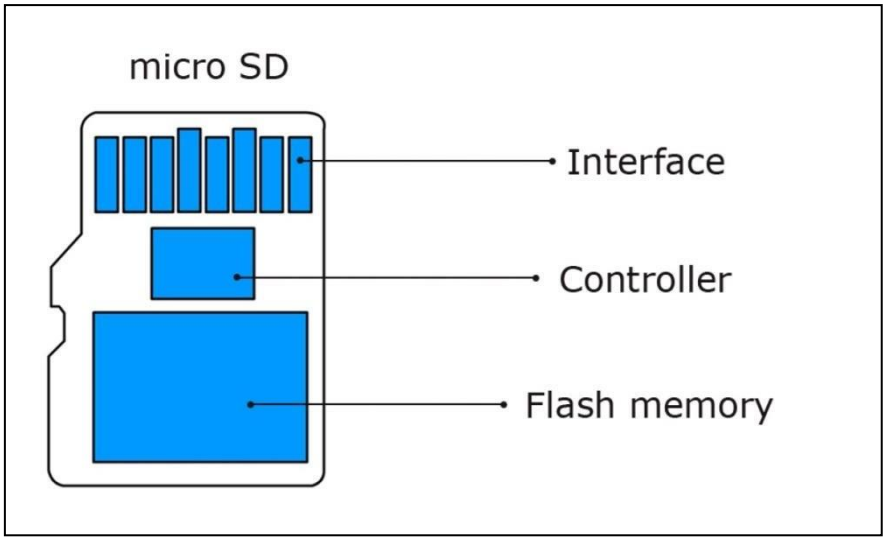


Figura 54 – Componentes internos memoria SD – Fuente: http://www.pc3000flash.com/

El primer paso es acceder al circuito impreso de la memoria, para esto es necesario quitar el encapsulado. Esta tarea es artesanal y requiere de paciencia. Se realiza lijando la cubierta de la memoria hasta que aparezcan las pistas de la placa.

En primer lugar, tomamos nuestro dispositivo monolítico. En este ejemplo, se trata de una pequeña tarjeta micro SD. Necesitamos fijar esta tarjeta en la mesa con una cinta adhesiva de doble cara:

Figura 55 – Memoria micro SD fijada a la mesa con cinta doble faz – Fuente: http://www.pc3000flash.com/

Después de eso, comenzamos a borrar la capa de cerámica del lado inferior. Esta operación requiere algo de tiempo, por lo que debe tener mucha paciencia y cuidado. Si daña la capa de pinout, la recuperación de datos será imposible:

Empezamos con la lija gruesa (el tamaño más grande de grano) – 1000 o 1200:

Figura 56 – Proceso de quitar la capa de cerámica de la memoria micro SD – lija gruesa (1000) – Fuente: http://www.pc3000flash.com/

Cuando se elimina la primera parte del revestimiento (la mas grande), es necesario cambiar el papel de lija al tamaño de grano más pequeño:

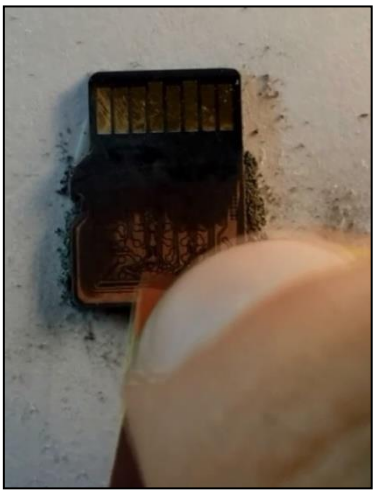


Figura 57 - Proceso de quitar la capa de cerámica de la memoria micro SD – lija intermedia (2000) – Fuente: http://www.pc3000flash.com/

Finalmente, cuando la capa de cobre de los contactos se vuelve visible, debemos usar el tamaño de grano más pequeño:

Figura 58 - Proceso de quitar la capa de cerámica de la memoria micro SD – lija fina (2500) – Fuente: http://www.pc3000flash.com/

Finalmente, luego de limpiar con alcohol isopropílico, deberíamos obtener algo así:

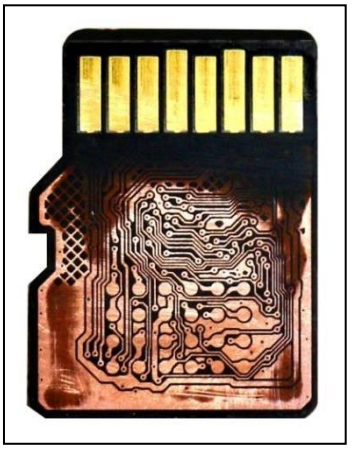


Figura 59 – Memoria micro SD sin la capa cerámica – Fuente: http://www.pc3000flash.com/

Ahora que tenemos a la vista los pads y pistas del PCB se presenta otra dificultad, la de que no es tan fácil conseguir los pinou de las memorias. Es por esto que para esta técnica se recomienda adquirir una herramienta especialmente diseñada para este fin, la cual, además de incluir todo el hardware y software necesario, suministra una gran base de datos con varios pinout de distintas memorias.

Un equipo comercial destinado a este fin es el "PC-3000" de la empresa ACELab:

Figura 60 – PC-3000 y accesorios de la empresa ACELab – Fuente: http://www.pc3000flash.com/

Con la compra del equipo tendremos acceso al "Centro de Soluciones Globales", en el cual encontraremos el pinout de nuestra memoria:

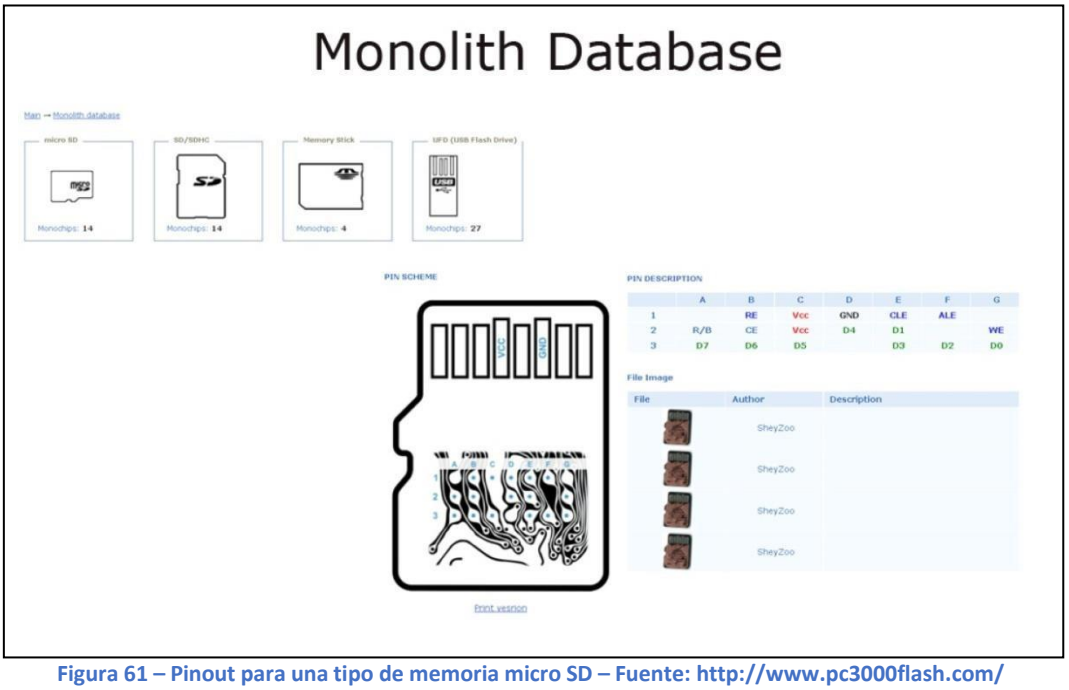


Figura 61 – Pinout para una tipo de memoria micro SD – Fuente: http://www.pc3000flash.com/

A continuación debemos localizar y soldar 3 grupos de contactos:

1 - Contactos de E/S de datos: D0, D1, D2, D3, D4, D5, D6, D7
2 - Contactos de mando: ALE, RE, R/B, CE, CLE, WE
3 - Contactos de alimentación: VCC, GND

Después de eso, debemos fijar la tarjeta microSD en el adaptador de la placa adaptador para una soldadura más conveniente:

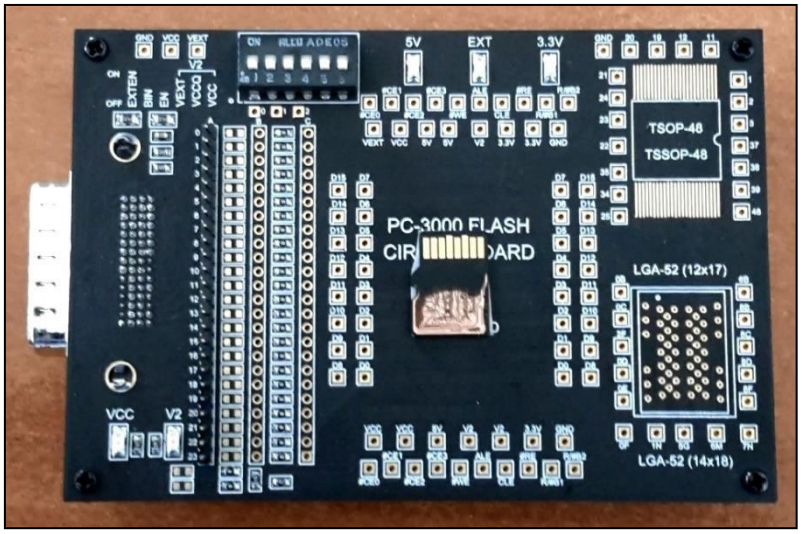


Figura 62 – Memoria micro SD sobre placa accesorio del PC-3000 – Fuente: http://www.pc3000flash.com/

Se recomienda imprimir el esquema de pines de la memoria antes de soldar para que esté a mano cuando se necesite verificar la matriz de pines.

Bajo el microscopio deberíamos ver una imagen como la siguiente:

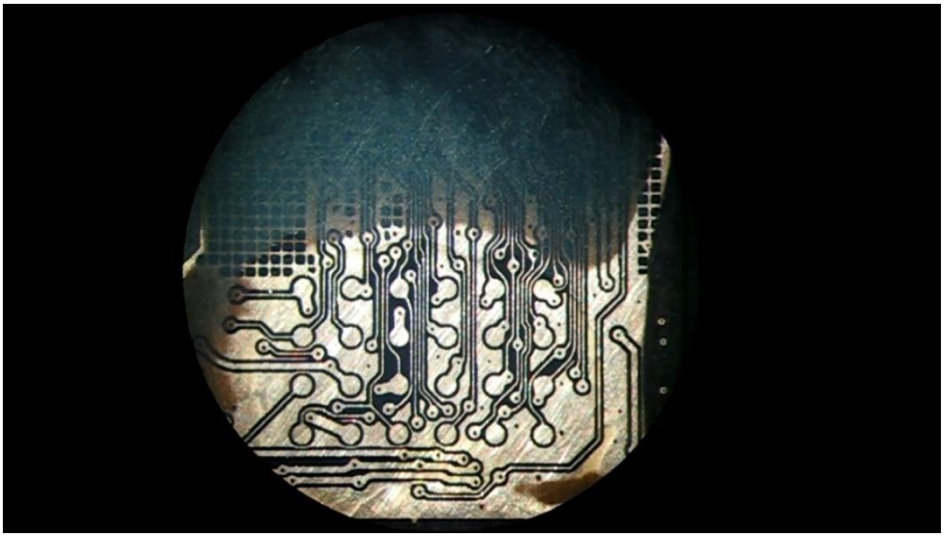


Figura 63 – Imagen bajo el microscopio de una memoria micro SD decapada – Fuente: http://www.pc3000flash.com/

Se debe colocar un poco de flux para soldar en los contactos con la ayuda de un cepillo pequeño.

Ahora, con la ayuda de un palillo humedecido con flux, debemos colocar todas las esferas de estaño en los contactos de los pines de cobre que están marcados en el esquema del pinout. Se recomienda usar las esferas de estaño con un tamaño de aproximadamente 75% del diámetro de nuestros contactos. El flux nos ayudará a fijar las esferas de estaño en la superficie de la tarjeta microSD:

Figura 64 – Esferas de estaño – Fuente: https://multi-com.eu/

Cuando todas las esferas de estaño estén colocadas en los pines, debemos usar un soldador para derretir estaño:

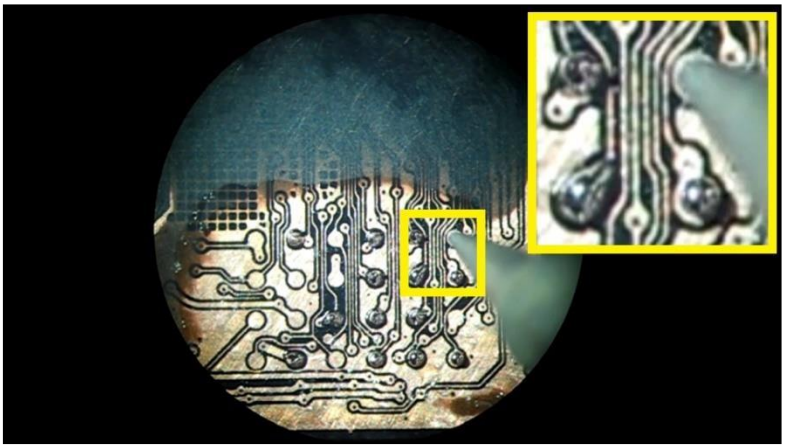


Figura 65 – Esferas de estaño fundidas en los contactos de la memoria – Fuente: http://www.pc3000flash.com/

Luego, usando una pistola de aire caliente, debemos calentar nuestros pines con la temperatura de +200C. El flux ayudará a distribuir el calor entre todos los contactos y fundirlos con cuidado. Después del calentamiento, todos los contactos y las esferas de estaño tomarán una forma de semiesfera:

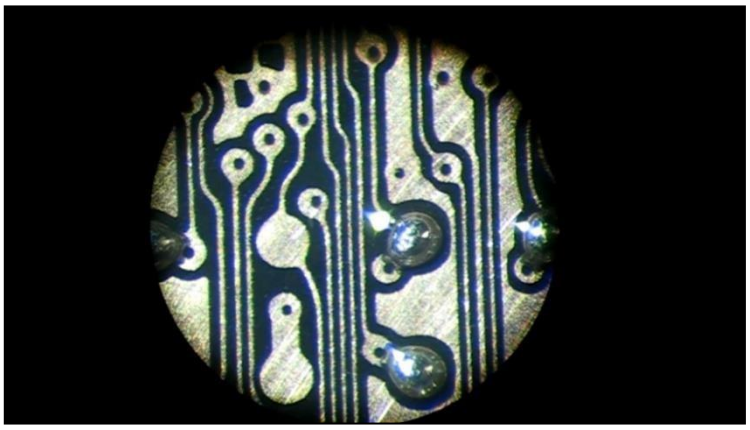


Figura 66 – Esferas de estaño luego de ser calentadas con la pistola de calor – Fuente: http://www.pc3000flash.com/

El siguiente paso es preparar los hilos de cobre. Deben tener la misma longitud (aproximadamente – 5-7 cm):

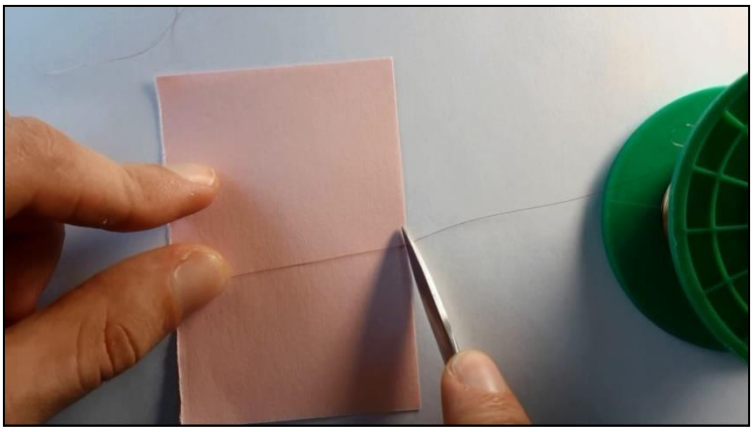


Figura 67 – Hilos de cobre para realizar la conexión – Fuente: http://www.pc3000flash.com/

Ahora debemos estañar las puntas de los alambres y comenzar el proceso de soldado. Primero lo haremos del lado de la placa:

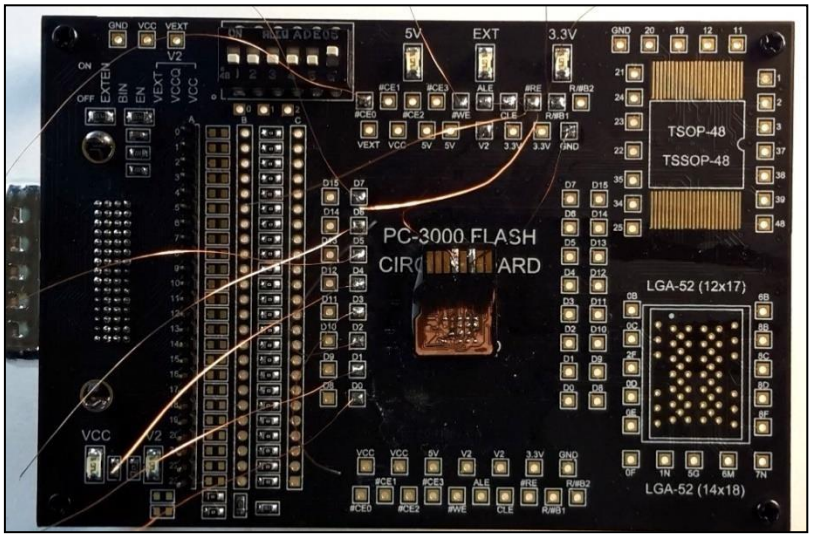


Figura 68 – Alambres soldados del lado de la placa – Fuente: http://www.pc3000flash.com/

Finalmente, ahora todos los cables están soldados a la placa de circuito y estamos listos para comenzar a usar un microscopio para soldar los cables a la tarjeta microSD. Esta es la operación más complicada y requiere mucha paciencia, una vez finalizada debería quedar de la siguiente manera:

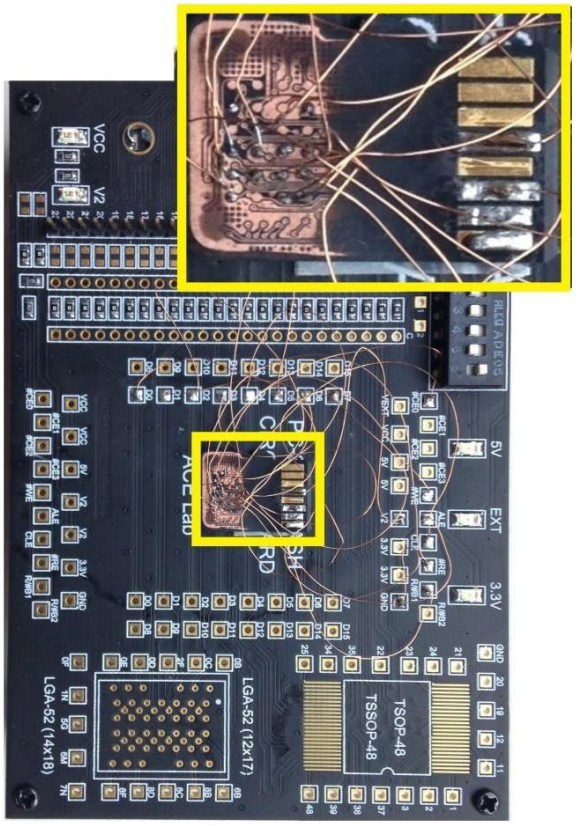


Figura 69 – Memoria microSD ya conectada a la placa adaptador del PC-3000 – Fuente: http://www.pc3000flash.com/

Ahora estamos listos para conectar nuestra placa de circuito al PC-3000 y comenzar el proceso de lectura:

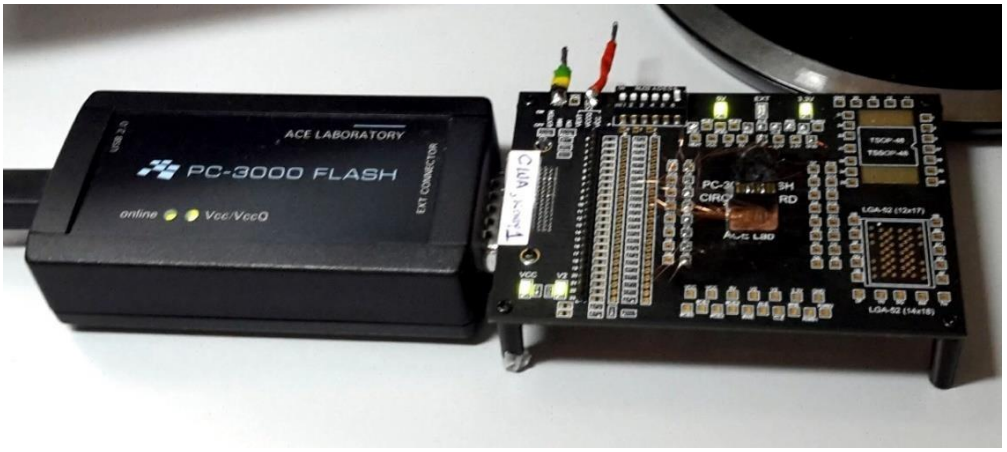


Figura 70 – PC-3000 conectado a la placa que contiene la memoria microSD – Fuente: http://www.pc3000flash.com/

Otra opción para reemplazar el proceso de soldadura es utilizar una herramienta fabricada por la misma empresa llamada “Spider Board Adapter”, que permite apoyar una serie de agujas conductoras en los contactos de interés de la memoria:

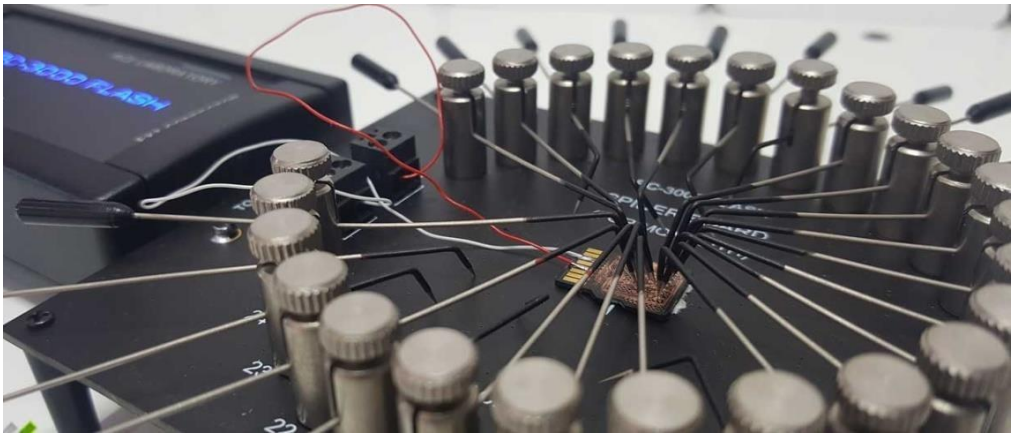


Figura 71 – Spider Board Adapter – PC3000 – Fuente: http://www.pc3000flash.com/

Figura 72 – Ampliación agujas Spider Board Adapter – PC3000 – Fuente: http://www.pc3000flash.com/

Para las memorias que estén dañadas mecánicamente, el éxito de la recuperación de datos dependerá del lugar donde este dañada:

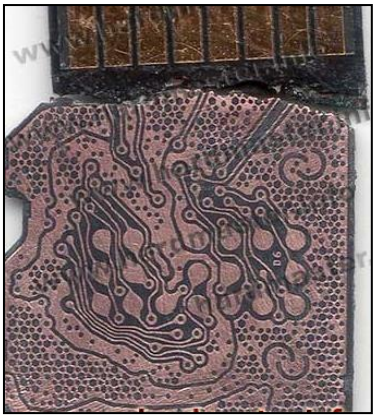


Figura 73 – Memoria dañada mecánicamente con buena probabilidad de recuperación de datos – Fuente: http://www.pc3000flash.com/

Figura 74 - Memoria dañada mecánicamente con escasa/nula probabilidad de recuperación de datos – Fuente: http://www.pc3000flash.com/

Recomendaciones y herramientas necesarias para extraer datos de celular que posee la placa principal dañada

En estos casos, si el dispositivo lo permite, se pueden aplicar las técnicas antes descriptas de JTAG, ISP o Chip-Off. No obstante, y antes de probar estas técnicas o en los casos que los dispositivos no permitan aplicar estas técnicas, siempre intentaremos reparar el equipo,

Una de las fallas más comunes es la humedad en las placas debido a que han estado en un lugar húmedo o en algunos casos el dispositivo móvil fue recuperado del agua o quedo enterrado en algún lugar con humedad.

La difícil reparación en estos casos se debe a que la mayoría de este tipo de equipos posee baterías incorporadas, que por lo general están con carga. Al humedecerse la circuitería comienza un proceso de electrolisis entre los distintos componentes, dada la cercanía de ellos y la conductividad del agua. En los casos que el agua sea salada el proceso se acelera.

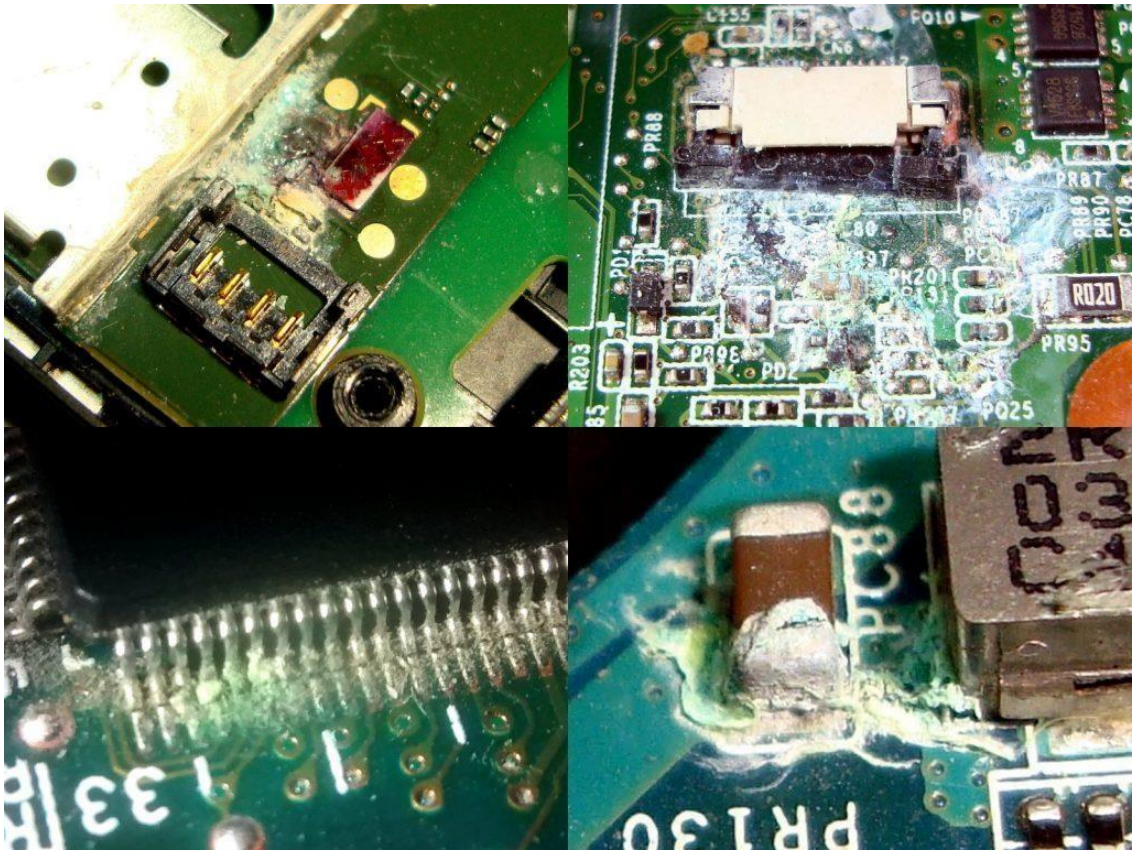


Figura 75 – Aspecto de placas "sulfatadas" por electrolisis – Fuente: Producción Propia

En estos casos la probabilidad de éxito en la reparación dependerá del tiempo que estuvo el dispositivo energizado y húmedo, también de la parte afectada y por último, pero no menos importante, de cuanta información (datasheet, manuales de servicio, etc.) y repuestos podamos conseguir de ese dispositivo en particular.

El primer paso será desarmar el equipo lo antes posible y desconectar la batería para detener el proceso de electrólisis.

A continuación retiraremos todos los periféricos tratando de dejar la placa base o la placa que contiene el circuito “sulfatado” lo más libre posible. Ahora comenzamos a limpiar la placa con alcohol isopropílico y un cepillo de cerdas blandas. También se puede usar un limpiador ultrasónico y sumergir la placa. Este tipo de equipo también es utilizado para el soldado de componentes que poseen conexiones débiles:

Figura 76 – Limpiador ultrasónico Fuente: Producción Propia

Luego de este proceso debemos realizar una inspección minuciosa bajo el microscopio en la zona afectada y comenzar a medir continuidad de pistas, valores de resistencias y capacitores, integridad de los conectores, etc.

A partir de aquí, como dijimos antes, todo dependerá del grado de conocimientos en electrónica que tenga el lector de esta guía, la información y repuestos que se tengan del dispositivo en cuestión y el grado de daño que se haya producido.

Capítulo 3 – Nuevas tecnologías

Nuevas tecnologías de memoria - Memorias UFS (Universal Flash Storage) y herramientas necesarias para su lectura.

Dada la necesidad de incorporar cada vez más almacenamiento, aumentar la velocidad de lectura/escritura y reducir cada vez más el consumo de los dispositivos móviles, los equipos más modernos incorporan memorias que utilizan el estándar UFS, el cual es un tipo de memoria NAND Flash con una interfaz full dúplex. Esto quiere decir que este tipo de memorias pueden leer y escribir de forma simultánea.

Esta tecnología empezó a incorporarse en los dispositivos de más alta gama en el año 2015, con el estándar UFS 2.0, que llegaba hasta los 128 GB, hasta el presentado en el 2022 por Samsung, el UFS 4.0 que duplica la velocidad del estándar anterior (UFS 3.1) y llega hasta los 1.000 GB de almacenamiento.

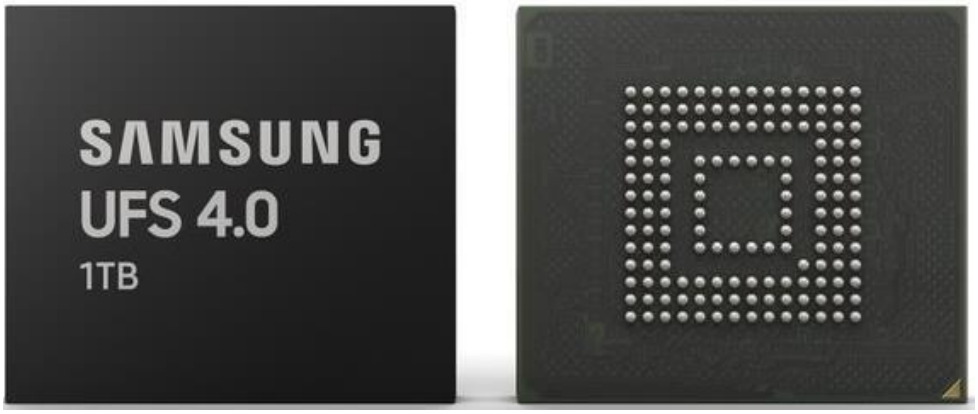


Figura 77 – Memoria Samsung UFS 4.0 de 1TB Fuente: Producción Propia

Para poder leer este tipo de memoria deberemos adquirir una herramienta específica, tal como la fabricada por la empresa “DediProg” de origen Taiwanés, el programador “NuProg-E” que es compatible con los protocolos Universal Flash Storage (UFS), eMMC y eMCP, que son ampliamente utilizados en dispositivos móviles tales como teléfonos inteligentes y tabletas.

A continuación se puede ver una imagen del programador y sus accesorios para dos tipos de encapsulados de memoria:

Figura 78 – Programador NuProg-E para memorias UFS – Fuente: https://www.dediprog.com/

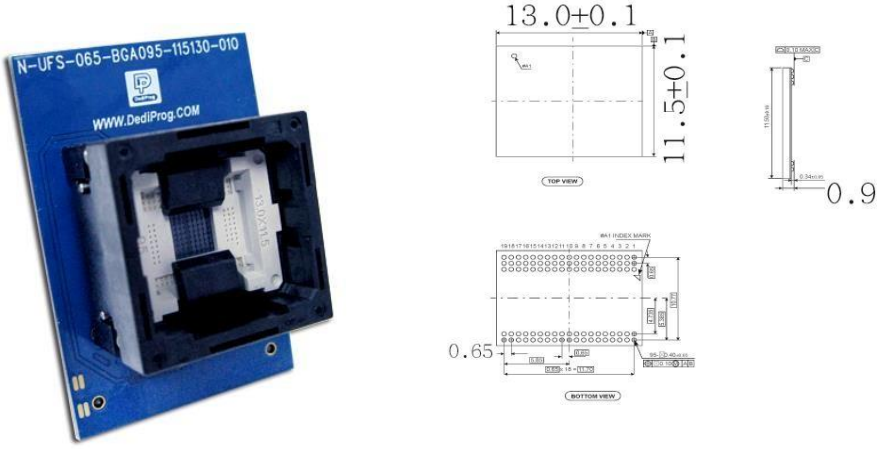


Figura 79 – Zócalo NuProg-E para encapsulado BGA095 – Fuente: https://www.dediprog.com/

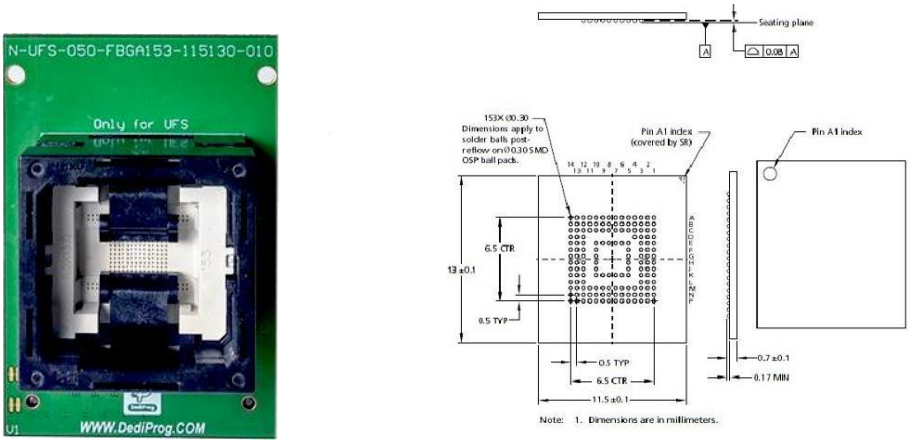


Figura 80 - Zócalo NuProg-E para encapsulado FBGA153 – Fuente: https://www.dediprog.com/

Recomendaciones

El analista forense deberá investigar constantemente para estar a la vanguardia de la tecnología si desea acceder a dispositivos que parecería imposible acceder.

Aunque parezca demasiado esfuerzo, estudio e inversión, aplicar una técnica específica para un determinado dispositivo, que tal vez aplicaremos una sola vez en mucho tiempo, es posible que la prueba obtenida sea la única para poder llegar al fondo de una investigación. En este caso la inversión estará más que justificada.

Siempre se deberán aplicar primero las técnicas menos invasivas y solo aplicar las más invasivas o destructivas como último recurso (chip-off).

Es recomendable, siempre que sea posible, probar la extracción en un dispositivo muleto, para así aumentar el porcentaje de éxito en la extracción de datos del dispositivo que contiene los datos de interés.

Conclusiones

Si bien el trabajo recorre varias técnicas de extracción avanzadas, estas son solo algunas y requieren una permanente actualización en la temática debido a la actualización constante y a la aparición de nuevas tecnologías.

Esta guía se desarrolló investigando técnicas y probándolas luego con celulares y memorias de prueba. El lector podrá avanzar junto a esta guía de la misma manera, probando y sacando sus propias conclusiones con dispositivos de prueba e ir avanzando desde las técnicas más sencillas hasta las más complejas, hasta poder aplícalas con seguridad en un dispositivo secuestrado con datos sensibles de una causa real.

Cada Investigador podrá utilizar esta guía de recomendaciones como un puntapié inicial de alguien que ya recorrió este camino. Así podrá avanzar más rápido a la extracción de datos en dispositivos que utilizan tecnologías más nuevas.

Bibliografía

Oleg, Afonin & Vladimir, Katalov. (2016) - Mobile Forensics Advanced Investigative Strategies. Birmingham, UK: Packt Publishing Ltd.

Colin, O'Flynn & Jasper, van Woudenberg. (2021). The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks. San Francisco, United States: No Starch Press.

Igor Sestanj. (2016). NAND Flash Data Recovery Cookbook. Belgrade, Serbia: Len Rorke.

Sitio web de ALLDATASHEET. Disponible en: https://www.alldatasheet.es/datasheet-pdf/pdf/1132297/SAMSUNG/KLMAG2WEMB-B031.html. Accesible: 21/04/2022

Sitio web de Forensics Wiki. Disponible en: https://forensicswiki.xyz/wiki/index.php?title=JTAG_and_Chip-Off_Tools_and_Equipment. Accesible: 21/04/2022

Sitio web de Emmc Pinouts. https://emmcpinouts.com/Default.php. Accesible: 21/04/2022

Sitio web de JTAG FINDER. Disponible en: http://www.jtagfinder.com/. Accesible: 21/04/2022

Sitio web de Teel Technologies. Disponible en: https://teeltech.com/. Accesible: 23/04/2022

Sitio web de Access Data. Disponible en: https://accessdata.com/. Accesible: 23/04/2022

Sitio web de Sireda. Disponible en: http://www.sireda.com/. Accesible: 23/04/2022

Sitio web de Electroquímica Delta: https://www.edelta.com.ar/. Accesible: 25/04/2022

Sitio web de ACELab. Disponible en: https://www.acelab.eu.com/. Accesible: 28/04/2022

Sitio web de ACELab. Disponible en: http://www.pc3000flash.com/solbase/monochips.php?lang=eng. Accesible: 28/04/2022

Sitio web de DediProg. Disponible en: https://www.dediprog.com/. Accesible: 28/04/2022