

# Software Medusa Pro

## Manual de usuario



## Contenido

1. Descripción del programa .....	3
1.1. Algoritmo general de recuperación de dispositivos .....	5
2. Trabajo con memorias flash eMMC.....	5
2.1 Inicialización eMMC .....	6
2.2. Funciones estándar eMMC (Main) .....	7
2.2.1. Trabajo eMMC con secciones (Partitions) .....	7
2.2.2. Trabajos eMMC con direcciones y bloques arbitrarios (Custom).....	9
2.2.3. eMMC trabajo con el volumen completo de la memoria flash (Full) .....	9
2.3. eMMC trabajo con firmwares del fabricante (Factory repair).....	9
2.4. eMMC trabajos con funciones de servicio (eMMC Service) .....	10
3. Trabajo con memorias flash UFS.....	12
3.1. UFS trabajos con funciones de servicio (UFS Service) .....	13
3.1.1 División de la unidad UFS en LU (Distribute UFS Storage).....	14
3.1.2 Actualización del firmware del controlador UFS (Firmware update UFS) .....	15
4. Trabajos por USB.....	17
4.1. Inicialización de procesadores Qualcomm vía USB .....	18
4.2. Inicialización de procesadores MediaTek (MTK) vía USB .....	19
5. Trabajo con NAND.....	20
6. Trabajo con ADB (Android Debug Bridge).....	21

# Introducción

**Medusa Pro Software** es una aplicación que funciona con los programadores **Medusa Pro** y **Medusa Pro II** en el sistema operativo **Windows**.

**Medusa Pro Software:** proporciona una interfaz fácil de usar para recuperar dispositivos dañados por software.

**Medusa Pro Software** le permite recuperar dispositivos mediante interfaces **USB, eMMC, UFS, NAND** conectándose directamente al procesador o la memoria, así como utilizando el firmware original de fábrica para dispositivos del fabricante.

## 1. Descripción del programa

La ventana principal del programa se ve así.

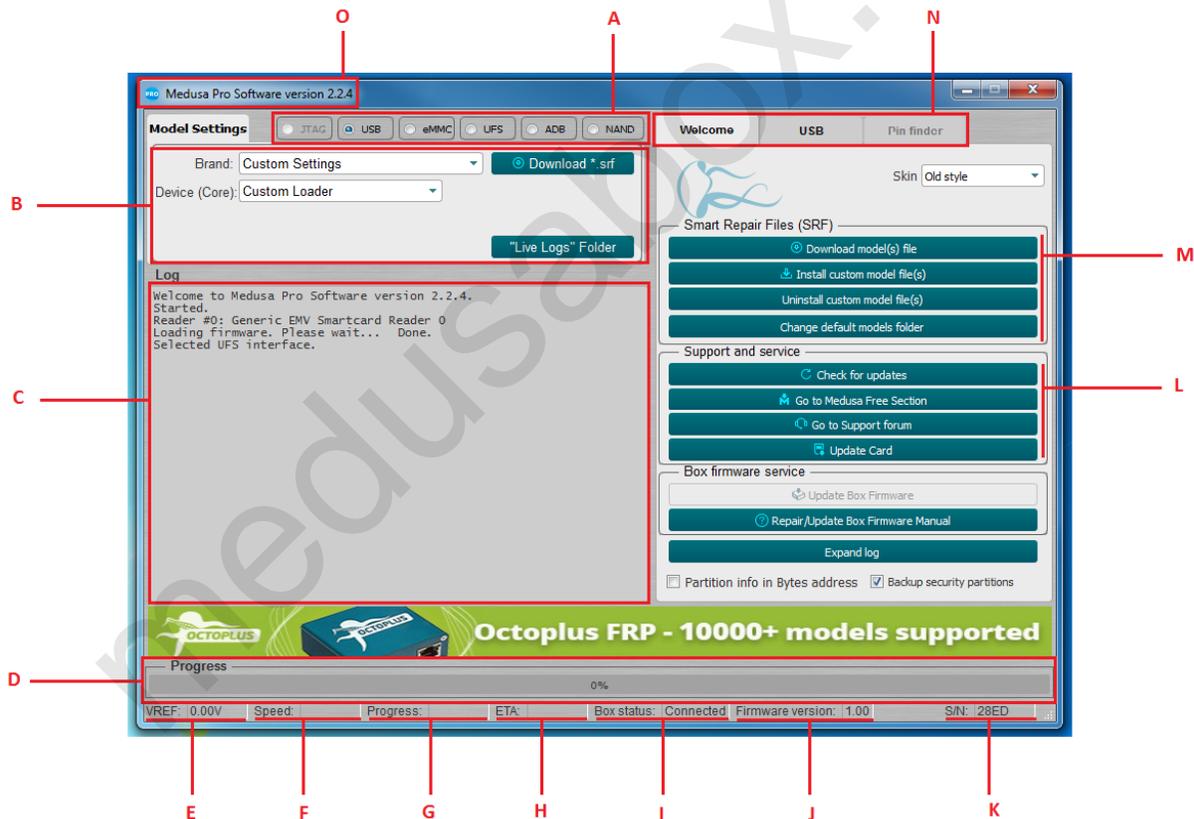


Figura. 1 Pestaña "Bienvenido" de la ventana principal

- A. Selección de la interfaz de trabajo a través de la cual se realiza el trabajo con el dispositivo conectado;
- B. Configuración de la interfaz de acuerdo con qué dispositivo está conectado;

- C. Visualización de la información sobre el dispositivo y el progreso de las operaciones;
- D. Progreso de la operación actual en porcentaje;
- E. Voltaje de referencia;
- F. Velocidad en kilobytes por segundo (KB/s), megabytes por segundo (MB/s) y gigabytes por segundo (GB/s);
- G. Tiempo transcurrido desde el inicio de la operación;
- H. Tiempo aproximado restante hasta el final de la operación;
- I. Estado del programador: "Conectado" y "Desconectado";
- J. Versión actual del firmware de la box;
- K. Número de serie de la box;
- L. Soporte y servicio;
- M. Gerente de SRF;
- N. Grupo de pestañas para trabajar con la box. La primera pestaña de "Bienvenida" se muestra en la Figura 1 y está diseñada para la gestión de SRF, el control de la versión de software y el firmware de caja. La segunda pestaña depende de la interfaz seleccionada. 1A. La tercera pestaña Pin Finder no se utiliza.
- O. Versión de software actual

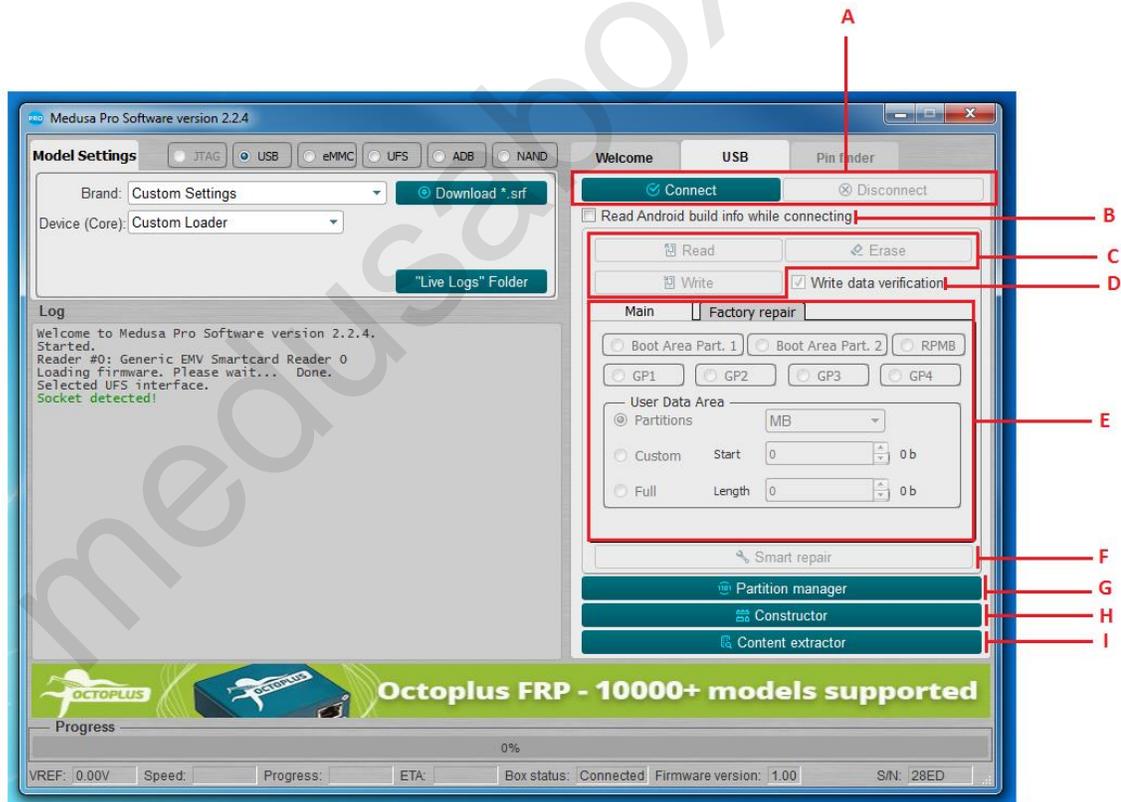


Figura. 2 Pestaña Interfaz de la ventana principal

- A. Inicialización del dispositivo conectado;
- B. Búsqueda y lectura de «Android Info» al inicializar el dispositivo;

- C. Funciones estándar de lectura, escritura y borrado;
- D. Verificación de datos registrados;
- E. Ajuste de la configuración de lectura, escritura y borrado (dirección, tamaño, secciones individuales, la flash completa), es posible ingresar valores en bytes, bloques, kilobytes y megabytes (los bytes, los bloques se ingresan en hexadecimal; kilobytes, megabytes en forma decimal);
- F. Reparación de la flash con ayuda del archivo SRF;
- G. Trabajo con secciones;
- H. Creación de archivos SRF;
- I. Розпаршування вмісту флешки.

## 1.1. Algoritmo general de recuperación de dispositivos

En general, el proceso de recuperación del dispositivo consta de varias etapas:

1. Es necesario conectar físicamente el dispositivo a una de las interfaces Fig.1A;
2. Seleccione la interfaz requerida;
3. Configure la interfaz en el campo Fig.1B;
4. Inicialice el dispositivo haciendo clic en el botón "Conectar" (Fig. 2A);
5. Los resultados de la inicialización se muestran en el registro Fig.1C. En caso de una inicialización exitosa, el registro puede contener ciertos parámetros del dispositivo, por ejemplo: fabricante del dispositivo, modelo del dispositivo, número de serie, capacidad, etc. Si no se pudo inicializar el dispositivo, el registro muestra información sobre la imposibilidad de inicializar el dispositivo;
6. Después de una inicialización exitosa, debe seleccionar el método por el cual planea restaurar el dispositivo. El método puede ser diferente para cada dispositivo (firmware de fábrica, dumps de dispositivos guardados previamente, uso de archivos SRF originales creados por el equipo de Medusa para una recuperación más rápida y sencilla del dispositivo).

## 2. Trabajo con memorias flash eMMC

Medusa Pro y Medusa Pro II funcionan de acuerdo con EMC 5.1 (JESD84-B51) y son totalmente compatibles con versiones anteriores de la especificación.

Medusa Pro Software le permite trabajar con memorias flash seleccionando un ancho de bus de datos de 1, 4 u 8 bits.

Box	Ancho de bus, bits
Medusa Pro	1, 4
Medusa Pro II	1, 4, 8

Tabla 1 Conformidad el ancho del bus eMMC con la caja conectada

## 2.1 Inicialización eMMC

Antes de iniciar la inicialización del eMMC, es necesario configurar los parámetros básicos de conexión, como el voltaje (**Voltage**, predeterminado 1,8 V), el ancho del bus (**Bus Mode**, predeterminado 1 bit) y la frecuencia de transmisión (**Bus speed**, predeterminado **Auto**). En la mayoría de los casos, el voltaje y la frecuencia de transmisión se pueden dejar intactos. Si la unidad flash está conectada mediante un enchufe "Medusa", el ancho del bus se puede seleccionar según la caja que se use actualmente, de acuerdo con la tabla 1.

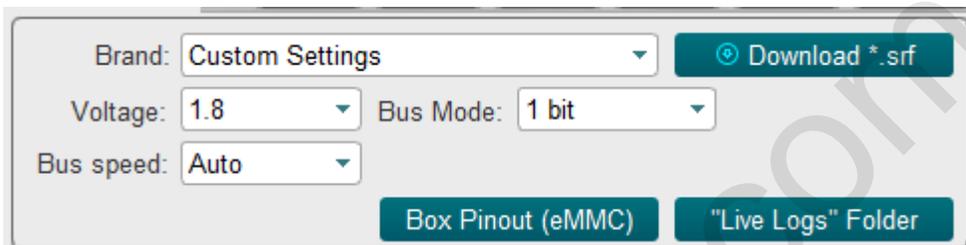


Figura. 3 Configuración de los parámetros básicos para inicializar la unidad flash eMMC  
Al hacer clic en el botón "Conectar" (Fig. 4), en el caso de una inicialización exitosa en el registro se muestra información sobre el portador (ejemplo en la Fig. 5).

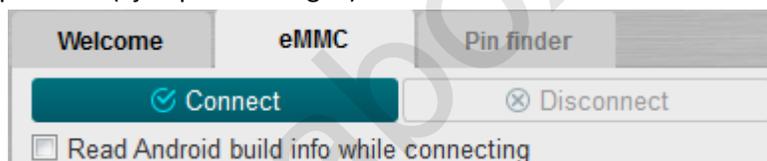


Figura. 4

```
Connecting...
Device       : Kingston eMMC IB2916
Page size   : 512 B
Block size  : 512 B
Block count : 30621696
Size        : 14.60 GB (14952.00 MB)
-----
CID Info
CID          : 70010049423239313690334EA34D47B3
Manufacturer ID : 0X70
Device/BGA   : BGA (Discrete embedded)
OEM/Application ID : 0X00
Product name : IB2916
Product revision : 9.0
Product serial number : (hex) 334EA34D
Manufacturing date : 04/2020
-----
CSD Info
CSD          : D04F01320F5903FFFFFFFFEF8A400061
CSD structure : CSD version No. 1.2
SPEC version  : 4.1, 4.2, 4.3, 4.4, 4.41, 4.5,
               4.51, 5.0, 5.01, 5.1
```

Figura. 5 Ventana con el registro de la unidad flash conectada

A partir de ahora, la unidad flash se considera inicializada y se puede trabajar con ella.

## 2.2. Funciones estándar eMMC (Main)

Funciones estándar de lectura, escritura y borrado están disponibles en la pestaña "**Principal**".

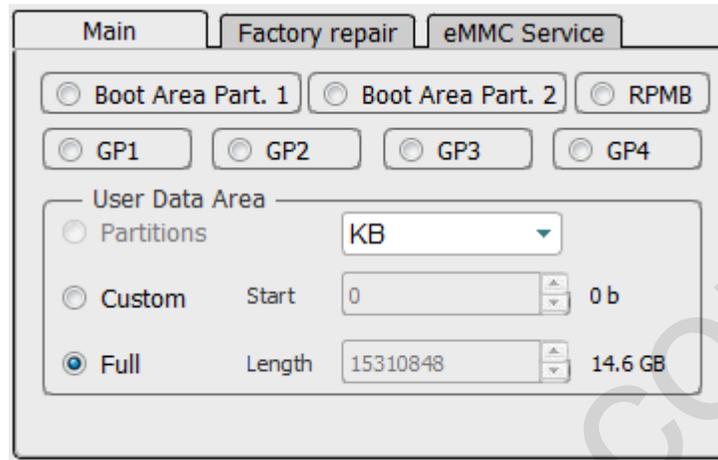


Figura 6

En la parte superior de la pestaña puede seleccionar el área de memoria con la que desea trabajar, siempre que el área seleccionada no sea de tamaño cero:

- Boot Area Part. 1;
- Boot Area Part. 2;
- RPMB;
- GP1 (General purpose 1);
- GP2 (General purpose 2);
- GP3 (General purpose 3);
- GP4 (General purpose 4);

### 2.2.1. Trabajo eMMC con secciones (Partitions)

Si se encontraron ciertas secciones en la unidad flash durante la inicialización, es posible seleccionar las necesarias para simplificar el trabajo con ellas preseleccionando el modo "**Particiones**" (Fig. 7) y presionando el botón "**Leer**". (Fig. 8), se va a abrir ventana con las secciones, Fig.9

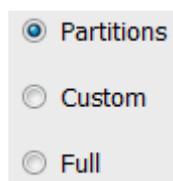


Figura. 7



Figura. 8

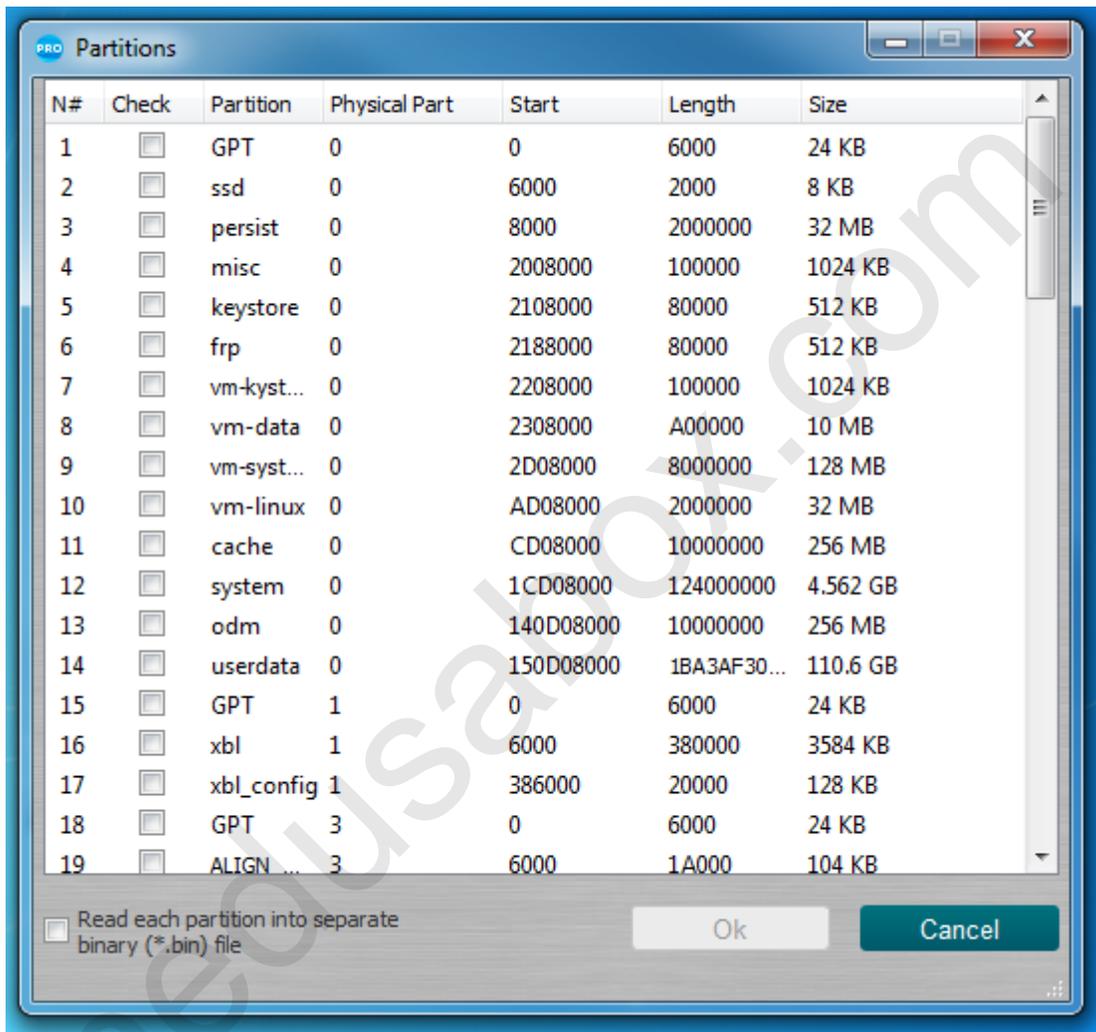


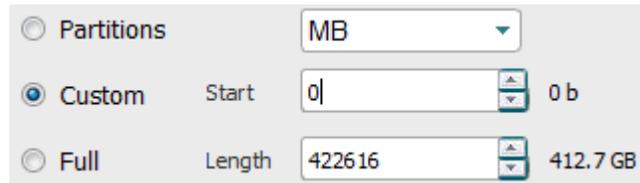
Figura. 9 Ventana con secciones

En esta ventana, debe seleccionar las secciones que desea leer. Estas particiones se leerán en un archivo con la extensión \* .mpt, también es posible leer particiones en archivos \* .bin separados, para esto debe marcar la opción "**Leer cada partición en un archivo binario (\* .bin) separado**".

Para escribir particiones, seleccione el archivo con la extensión \* .mpt, que se leyó previamente, y haga clic en "**Escribir**" (Fig. 8).

## 2.2.2. Trabajos eMMC con direcciones y bloques arbitrarios (Custom)

Cuando sea necesario escribir / leer / borrar datos en una dirección determinada y en una cantidad determinada, debe cambiar al modo personalizado **Custom** (Fig. 10), elija de una lista de unidades en las que se ingresarán los datos:



<input type="radio"/> Partitions	MB
<input checked="" type="radio"/> Custom	Start 0 0 b
<input type="radio"/> Full	Length 422616 412.7 GB

Figura. 10

- **Hex value** (en bytes, HEX);
- **Hex blocks** (en bloques, HEX);
- **KB** (en kilobytes, DEC);
- **MB** (en megabytes, DEC).

## 2.2.3. eMMC trabajo con el volumen completo de la memoria flash (Full)

Si necesita escribir/leer/borrar información de toda la memoria flash, debe cambiar al modo **Full** (Fig. 11)



<input type="radio"/> Partitions
<input type="radio"/> Custom
<input checked="" type="radio"/> Full

Figura. 11

Luego realice la operación requerida (Fig. 8).

## 2.3. eMMC trabajo con firmwares del fabricante (Factory repair)

En esta sección (Fig. 12) está implementada la capacidad de restaurar la memoria interna del dispositivo con firmware de fábrica de diferentes fabricantes.

El procedimiento de recuperación completa consiste en seleccionar el dispositivo deseado haciendo clic en el botón correspondiente en la pestaña y en la ventana que se abre, seleccionar el archivo de firmware con la extensión requerida para este dispositivo y escribir el firmware seleccionado.

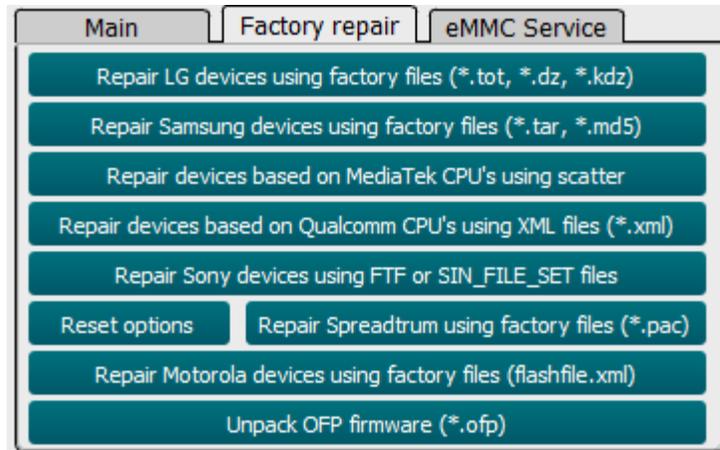


Figura. 12 Pestaña Factory repair

## 2.4. eMMC trabajos con funciones de servicio (eMMC Service)

Este modo se utiliza para trabajar con registros internos de eMMC (CID, CSD, EXT\_CSD), partición de la memoria flash, cambio de modo de la memoria flash, lectura de información adicional, actualizaciones de firmware.

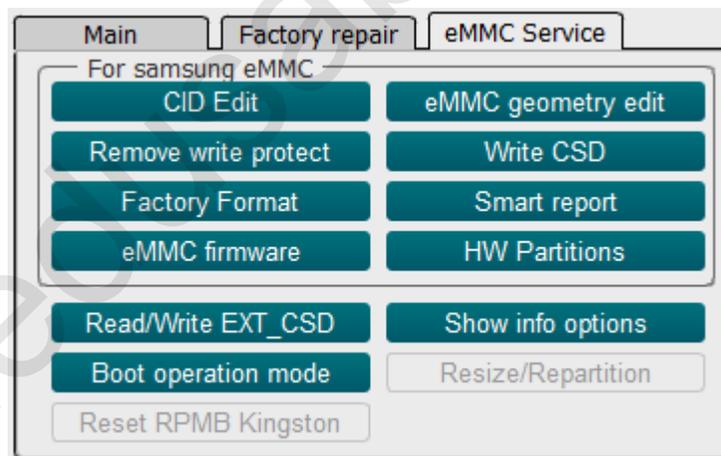


Figura. 13 Pestaña eMMC Service

«CID Edit» - Se utiliza para editar el registro CID;

«Remove write protect» - Elimina la protección contra escritura;

«Factory Format» - Borra completamente la memoria flash;

«eMMC firmware» - Actualización del firmware del controlador EMMC;

**!!! Medusa Pro Software no es responsable de la pérdida del dispositivo cuando se actualiza el firmware del controlador. Todas las operaciones de actualización del firmware del controlador se realizan por cuenta y riesgo del usuario.**

«eMMC geometry edit» - Establecer tamaños Boot1, Boot2, RPMB;

«Write CSD» - Se utiliza para editar el registro CSD;

«Smart report» - Lee información sobre el recurso de la unidad flash;

«HW Partitions» - Se utiliza para ajustar los tamaños de las áreas GP1, GP2, GP3, GP4 y User area;

«Read/Write EXT\_CSD» - Trabajos con EXT\_CSD;

«Boot operation mode» - Configuración de boots;

medusabox.com

### 3. Trabajo con memorias flash UFS

Medusa Pro Software es compatible con memorias flash UFS con la box **Medusa Pro II**. **Medusa Pro no es compatible con UFS!!!** Estándares UFS soportados con Medusa Pro Software:

- UFS 2.0
- UFS 2.1
- UFS 3.0
- UFS 3.1.

Medusa Pro II se ejecuta en un Lane y soporta los siguientes modos de trabajo de bus: LS PWM G1, LS PWM G2, LS PWM G3, LS PWM G4, HS G1. Trabajo con medios UFS coincide principalmente con eMMC, la diferencia está en la configuración de inicialización, en UFS esta pestaña se ve como en la Fig. 14, donde en el campo "Gear" se selecciona en cuál de los modos funcionará la interfaz UFS (Tabla. 2) y pestaña **UFS Service**(Fig. 15).

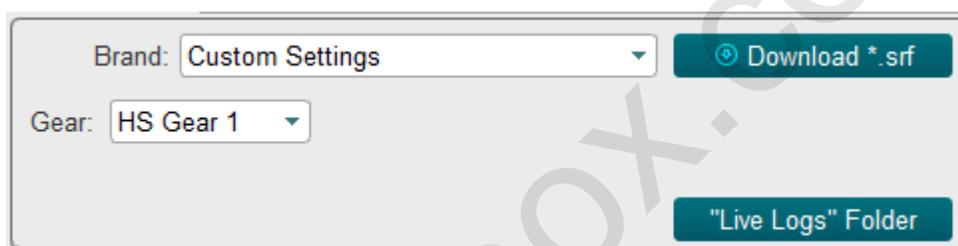


Figura. 14 Configuración de los parámetros básicos para inicializar la unidad flash UFS

Gears	Min (Mbps)	Max (Mbps)
LS PWM-G1	3 (300KB/s)	9 (900KB/s)
LS PWM-G2	6 (600KB/s)	18 (1.8MB/s)
LS PWM-G3	12 (1.2MB/s)	36 (3.6MB/s)
LS PWM-G4	24 (2.4MB/s)	72 (7.2MB/s)
HS G1		1248 (124.8MB/s)

Tabla 2 Correspondencia de la velocidad de transferencia de Gear

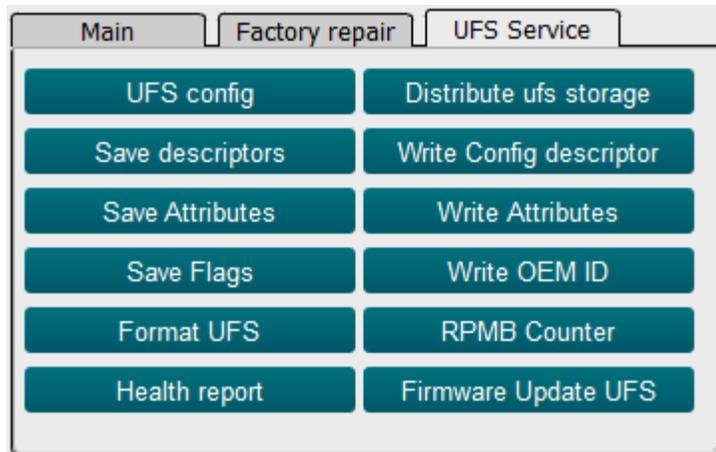


Figura. 15 Pestaña UFS Service

### 3.1. UFS trabajos con funciones de servicio (UFS Service)

El botón «**UFS config**» le permite ver todos los descriptores, indicadores y atributos.

Los botones «**Save descriptors**», «**Save Attributes**» o «**Save Flags**» se utilizan para guardar descriptores, atributos y flags.

**Write Config descriptor** - el botón se utiliza para escribir el descriptor de configuración. De acuerdo con el estándar UFS, para configurar medios flash, debe escribir el Descriptor de configuración que se leyó previamente. Debido a que el formato Config Descriptor depende de la versión de la especificación UFS, Medusa Pro Software convierte automáticamente el Config Descriptor a la versión requerida.

*Por ejemplo: si intenta escribir Config Descriptor versión 2.1 en una unidad flash con la versión 3.1, el software convierte automáticamente el descriptor.*

«**Format UFS**» - Se utiliza para borrar todas las LU.

«**Distribute UFS storage**» - Se utiliza para dividir la unidad flash en LU.

«**Write Attribute**» - Se utiliza para registrar atributos de un archivo guardado.

«**Write OEM ID**» - Se utiliza para registrar el ID de OEM del archivo guardado.

«**RPMB Counter**» - Se utiliza para leer el contador RPMB.

«**Health report**» - Lee información sobre el recurso de la unidad flash.

«**Firmware Update UFS**» - Se utiliza para actualizar el firmware del controlador UFS.

### 3.1.1 División de la unidad UFS en LU (Distribute UFS Storage)

Para dividir la unidad flash en la LU, debe hacer clic en «**Distribute UFS storage**» y se abrirá la ventana Fig.16. Los tamaños de LU se pueden ingresar en bloques, megabytes y gigabytes, para esto es suficiente cambiar el modo de entrada. Fig. 17(A). El tamaño de LU se ingresa en el campo «**LUN Size**» y el volumen restante se mostrará en el campo «**Rest size**». (Fig. 18), al pulsar de nuevo el modo de entrada se transfiere el tamaño residual al campo de tamaño. Fig. 17(B). Al hacer clic en el botón «**Add LUN**», la sección aparecerá en la lista, creando así una lista de todas las LU. Para crear estas LU en la unidad flash, debe hacer clic en el botón "**CreateLUNs**". Aparecerá un mensaje en el registro que indica que la configuración se guardó correctamente. El software verifica el número de LU creadas, si el número excede el máximo posible, el botón «**Add LUN**» se vuelve inactivo.

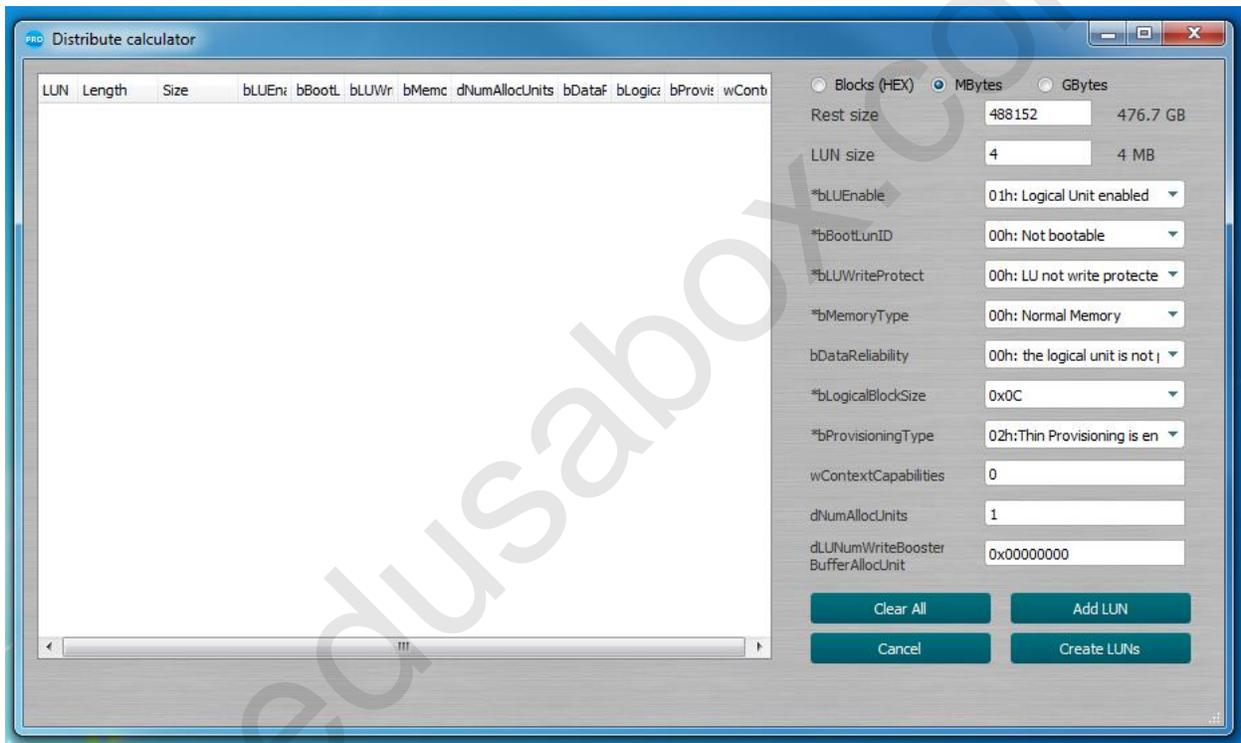


Figura. 16 Ventana Distribute UFS storage



Figura. 17 (A) Modo de entrada de tamaño de LU



Figura. 17 (B) Pulsando dos veces el modo de entrada de tamaño LU

Rest size	488152	476.7 GB
LUN size	4	4 MB

Figura. 18 Campos de restos y tamaño de la LU actual

### 3.1.2 Actualización del firmware del controlador UFS (Firmware update UFS)

Si necesita actualizar el firmware del controlador UFS, puede hacerlo haciendo clic en el botón **«Firmware Update UFS»** (Fig. 15) y se abrirá la ventana de recuperación de firmware (Fig. 19). En la parte superior de la ventana se encuentran el fabricante, el nombre y la revisión actual de la unidad flash conectada. En la inferior se muestra el fabricante, el nombre y la revisión del firmware al que desea actualizar. Si el firmware está en la base de datos de Medusa Pro Software, todos los campos en la parte inferior de la ventana se completarán automáticamente y el botón **«Update to»** se activará; de lo contrario, los campos se marcarán como **«Not supported»**.

El usuario puede actualizar el controlador UFS con "su" firmware haciendo clic en el botón **«Open file...»** para especificar la ruta al firmware del usuario. Si el firmware falla, el botón **«Update to»** se activará.

**!!! Medusa Pro Software no es responsable de la pérdida del dispositivo cuando se actualiza el firmware del controlador. Todas las operaciones de actualización del firmware del controlador se realizan por cuenta y riesgo del usuario.**

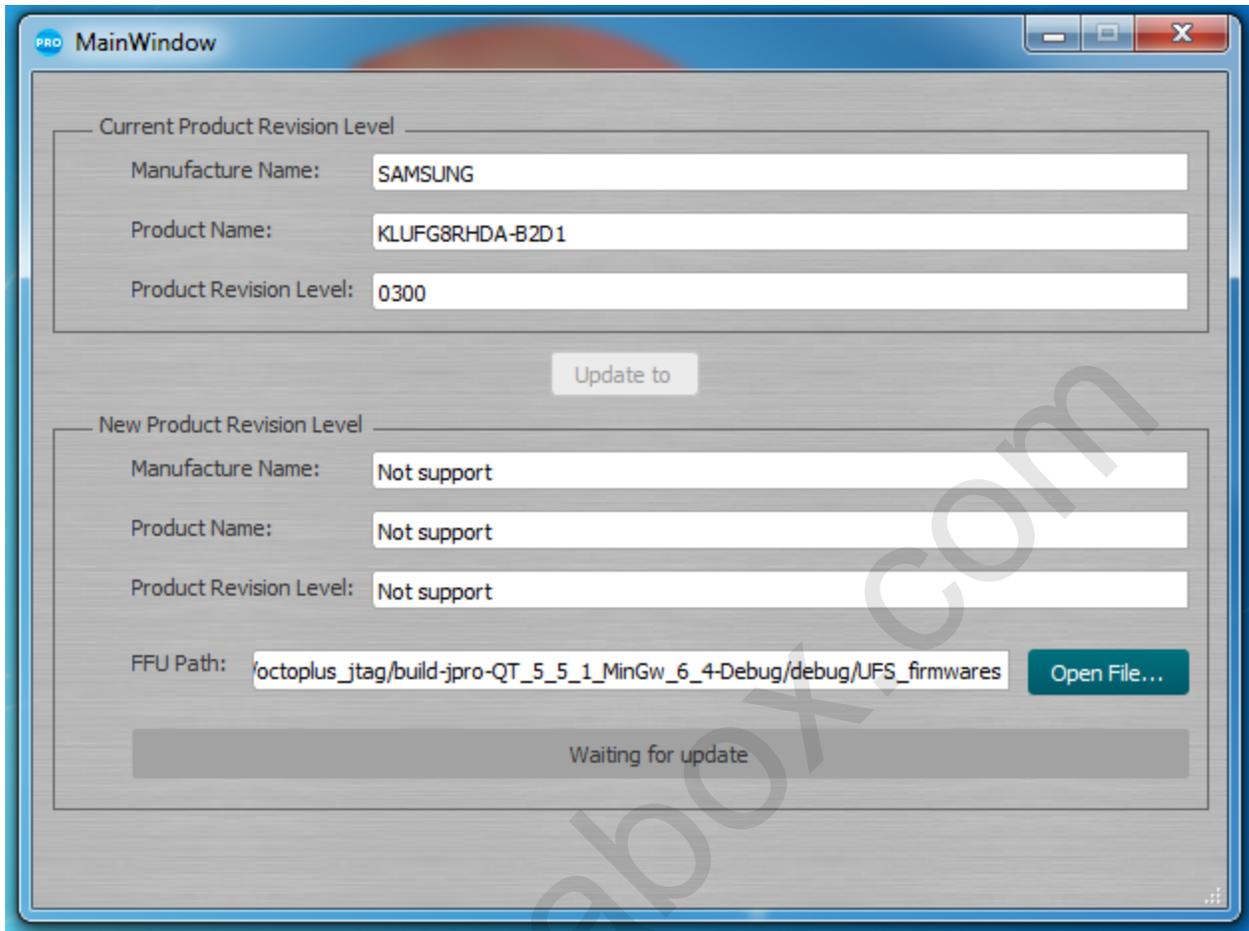


Fig.19 Ventana Firmware Update UFS

## 4. Trabajos por USB

Medusa Pro Software es compatible con USB con dispositivos que tengan instalados procesadores **Qualcomm** o **MediaTek (MTK)**.

Para inicializar el dispositivo, debe estar en EDL (Emergency Download Mode). Es posible cambiar al modo EDL de diferentes maneras, la forma más efectiva es cerrar los puntos correspondientes (**test points**) en la placa del dispositivo. Para realizar este procedimiento, debe desmontar parcialmente el dispositivo.

En algunos otros casos, puede cambiar el dispositivo al modo EDL con un comando especial de Android u otros modos como **Recovery**, **Fastboot**, etc. Una vez que el dispositivo entra en modo EDL, queda disponible en el sistema como un puerto COM, a través del cual se lleva a cabo la interacción en modo EDL.

Visualización de dispositivos en modo EDL conectados vía USB, Qualcomm (Fig. 20) y MTK (Fig. 21)

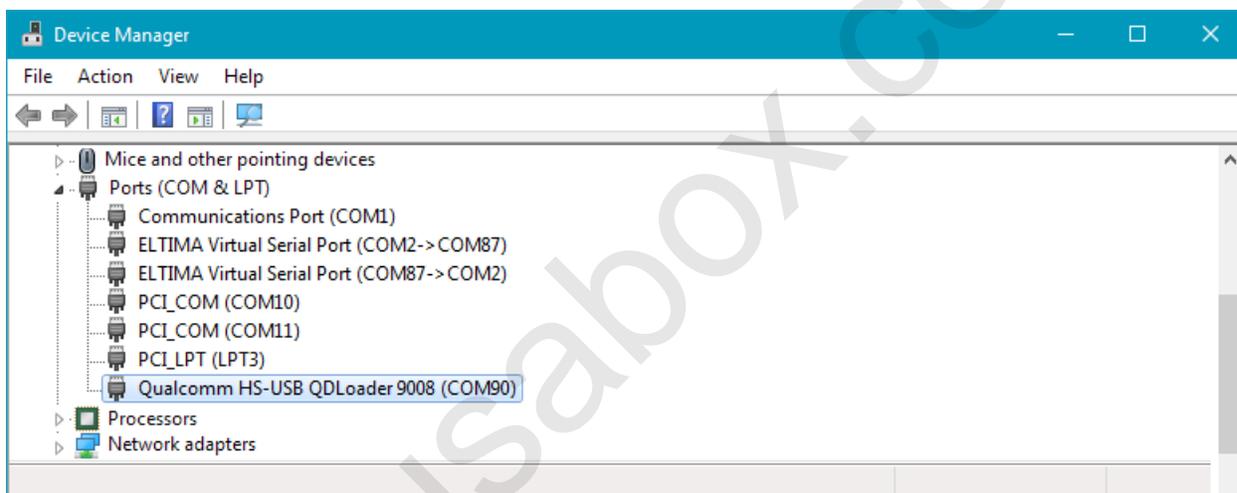


Fig. 20 Dispositivo con procesador Qualcomm en modo EDL, conectado vía USB

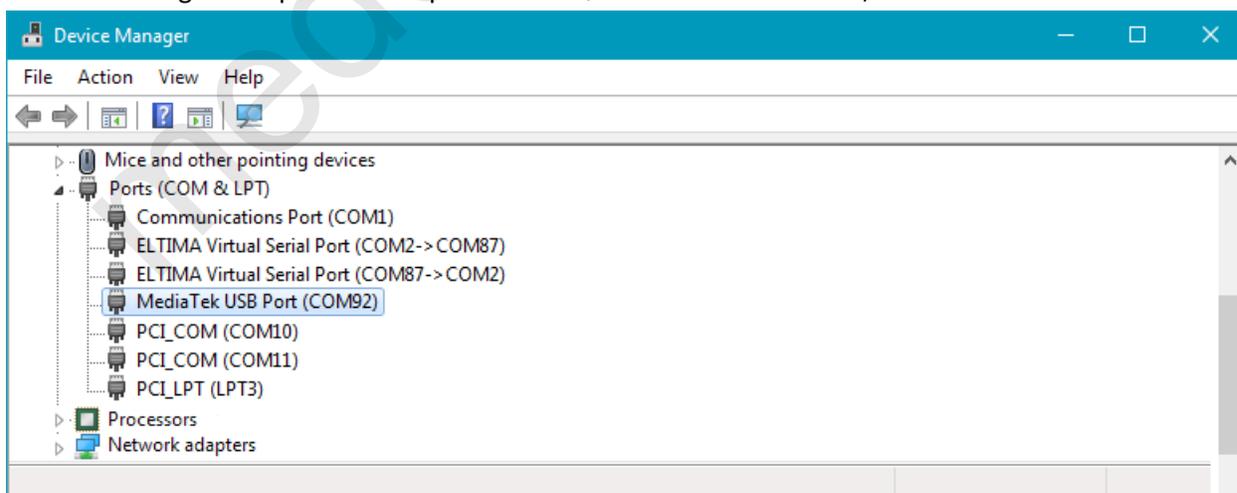


Fig. 21 Dispositivo con procesador MTK en modo EDL, conectado vía USB.

## 4.1. Inicialización de procesadores Qualcomm vía USB

Después de asegurarse de que el dispositivo está en modo EDL y definido en el sistema como "Qualcomm HS-USB QDLoader 9008" (Fig. 20), seleccione de la lista "**Device (Core)**" (Fig. 22) el procesador instalado en el dispositivo y presione **Connect**.

Si no conoce el nombre del procesador en el dispositivo, puede utilizar la función de detección automática del procesador seleccionando "**Detección automática**" en la lista «**Device (Core)**» y haciendo clic en "**Conectar**".

Si la inicialización es exitosa, el registro mostrará información sobre el dispositivo y, a partir de ahora, podrá trabajar con él. Usando las funciones estándar de lectura / escritura / borrado de la pestaña "**Main**" (Fig. 23) y trabaje con el firmware de fábrica en la pestaña «**Factory repair**» (Fig. 24).

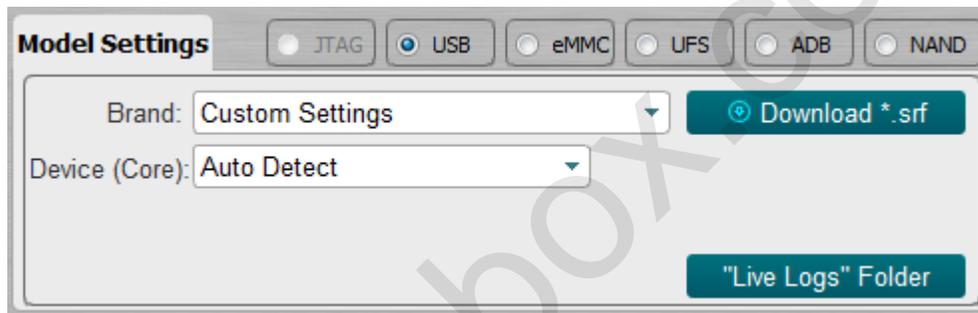


Fig.22

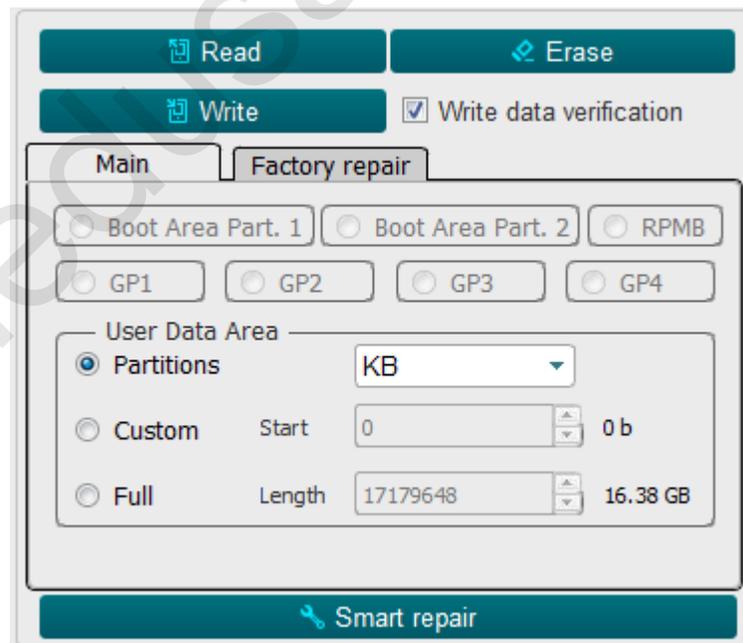


Figura. 23

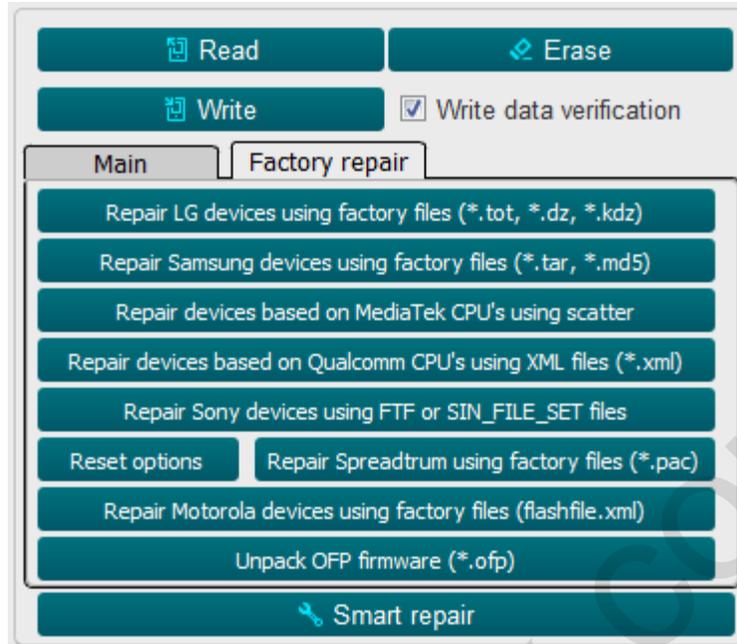


Figura. 24

## 4.2. Inicialización de procesadores MediaTek (MTK) vía USB

Después de asegurarse de que el dispositivo está en modo EDL y definido en el sistema como «**MediaTek USB Port**» (Fig.21), seleccione de la lista de " **Device (Core)**" (Fig.22) una de las dos opciones «**MTK Custom**» o "**MTK General**".

La diferencia entre estas dos opciones es que en **MTK Custom** es necesario seleccionar 3 archivos para inicializar el dispositivo: "**Download Agent (DA)**", "**Preloader**" y "**Authentication File**" (archivo **AUTH**) (Fig. 25).

Para "**MTK General**" solo necesita seleccionar un archivo: "**Precargador**" (Fig. 26) y hacer clic en "**Connect**". Si la inicialización es exitosa, el registro mostrará información sobre el dispositivo y, a partir de ahora, podrá trabajar con él. Usando las funciones estándar de lectura / escritura / borrado de la pestaña "**Main**" (Fig. 23) y trabajo con el firmware de fábrica en la pestaña "**Factory repair**" (Fig. 24).



Figura. 25



Figura. 26

## 5. Trabajo con NAND

Medusa Pro Software soporta unidades flash JEDEC ONFI NAND con anchos de 8 y 16 bits y Apple PPN de 32/64 bits. Físicamente, la unidad flash se conecta a través de un conector **Medusa** o se suelda al **conector pin**. Dependiendo del tipo de unidad flash, se selecciona el modo **PPN** u **ONFI** (Fig. 27)

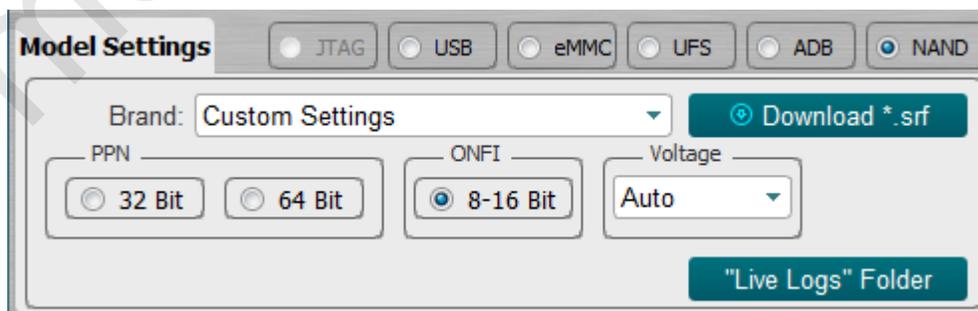


Figura. 27

Solo las funciones estándar de lectura/escritura/borrado están disponibles en el modo **ONFI**.

En el modo **PPN**, además de las funciones estándar, hay funciones adicionales disponibles en la pestaña **Servicio NAND** (Fig.28)

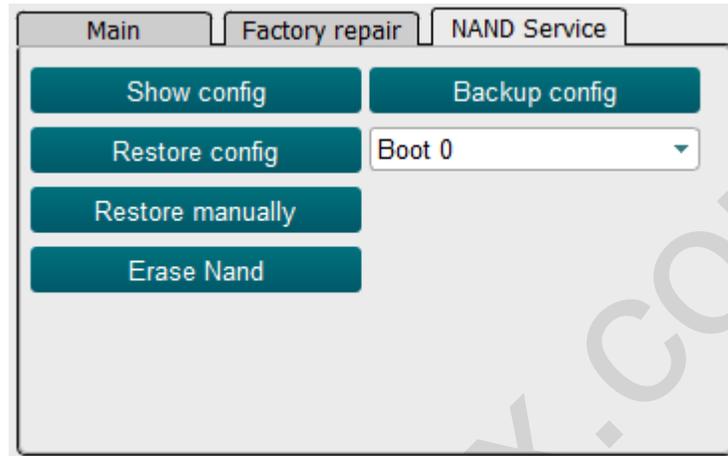


Figura. 28

- **Show config** - Resalta en el registro la información de configuración;
- **Backup config** - Guarda configuraciones en archivos separados;
- **Restore config** - Restaura la configuración desde el archivo guardado en el "Boot" seleccionado;
- **Restore manually** - Proporciona acceso a arreglos de configuración manualmente;
- **Erase NAND** - Borra el almacenador NAND.

## 6. Trabajo con ADB (Android Debug Bridge)

El dispositivo debe tener ADB habilitado. Para habilitar ADB en su dispositivo Android, siga estos pasos:

- Entrar en **Settings** → **About phone** → **Software information**;
- Clicar en **Build number** seis veces (hasta que aparezca el mensaje **You are now a developer**);
- Entrar en el menú **Settings** y encontrar nuevo punto **Developer options**;
- Mover el interruptor **USB Debugging** en la posición activa;
- Luego, debe conectar el dispositivo a una PC y hacer clic en **Conectar**. Si la inicialización es exitosa, la información sobre el dispositivo se mostrará en el registro. Solo lectura está disponible en el modo ADB.