Software Medusa Pro

Manual de usuário

Conteúdo

Introdução

Medusa Pro Software é uma aplicação que funciona com os programadores Medusa Pro e Medusa Pro II no sistema operativo Windows.

Medusa Pro Software - fornece uma interface fácil de usar para a recuperação de dispositivos danificados por software.

O Software Medusa Pro permite-lhe recuperar dispositivos via USB, eMMC, UFS, interfaces NAND, ligando-se directamente ao processador ou memória, bem como utilizando o firmware original de fábrica para os dispositivos do fabricante.

1. Descrição do programa

A janela principal do programa tem este aspecto.

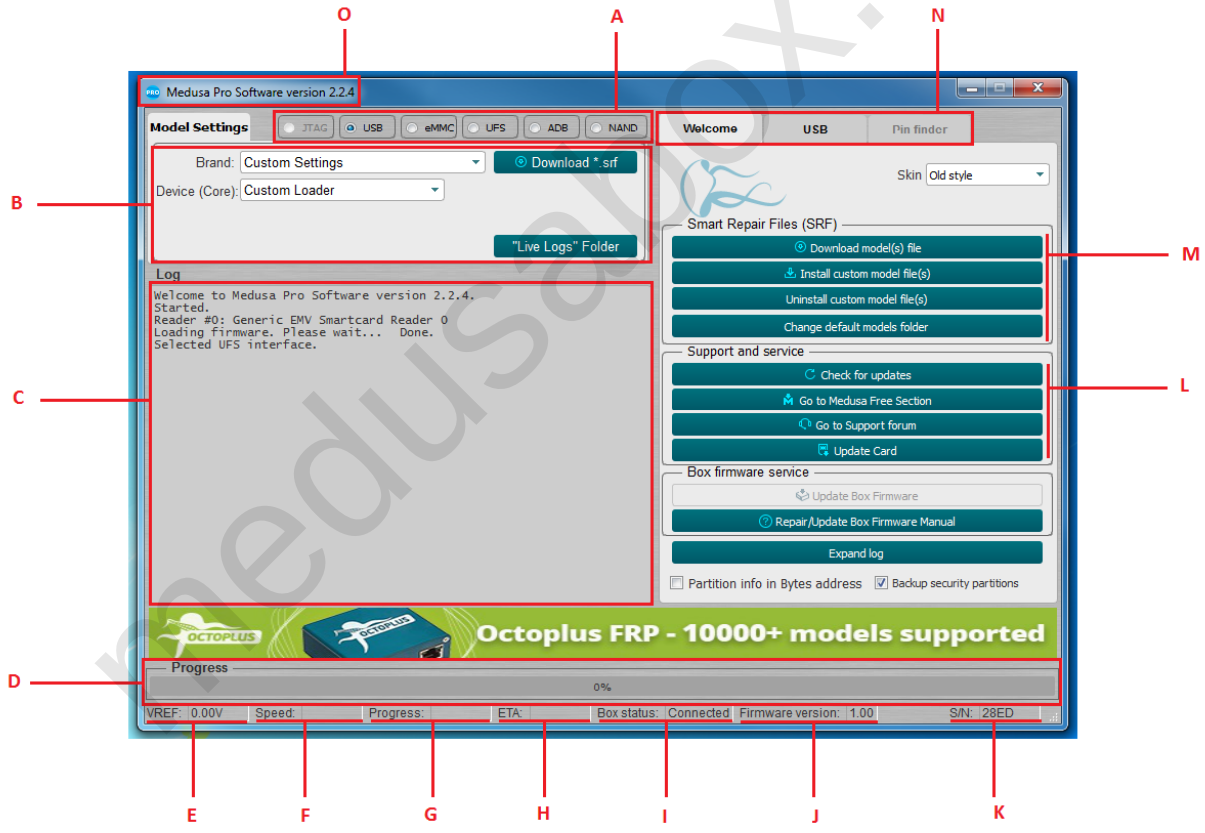

Figura. 1 separador "Bem-vindo" da janela principal

A. Selecção da interface de trabalho através da qual o trabalho com o dispositivo ligado é realizado;
B. Configuração da interface segundo a qual o dispositivo está ligado;
C. Visualização de informações sobre o dispositivo e o progresso das operações;
D. Progresso da operação actual em percentagem;
E. Voltagem de referência;
F. Velocidade em kilobytes por segundo (KB/s), megabytes por segundo (MB/s) e gigabytes por segundo (GB/s);
G. Tempo decorrido desde o início da operação;
H. Tempo aproximado restante até ao fim da operação;
I. Estado do programador: "Conectado" e "Desconectado";
J. Versão actual do firmware da box;
K. Número de série da box;
L. Apoio e serviço;
M. Gestor da SRF;
N. Grupo de separadores para trabalhar com a box. O primeiro separador "Bem-vindo" é mostrado na Figura 1 e foi concebido para gestão SRF, controlo de versão de software e firmware da box. O segundo separador depende da interface seleccionada. 1A. O terceiro separador Pin Finder não é utilizado.
O. Versão actual do software

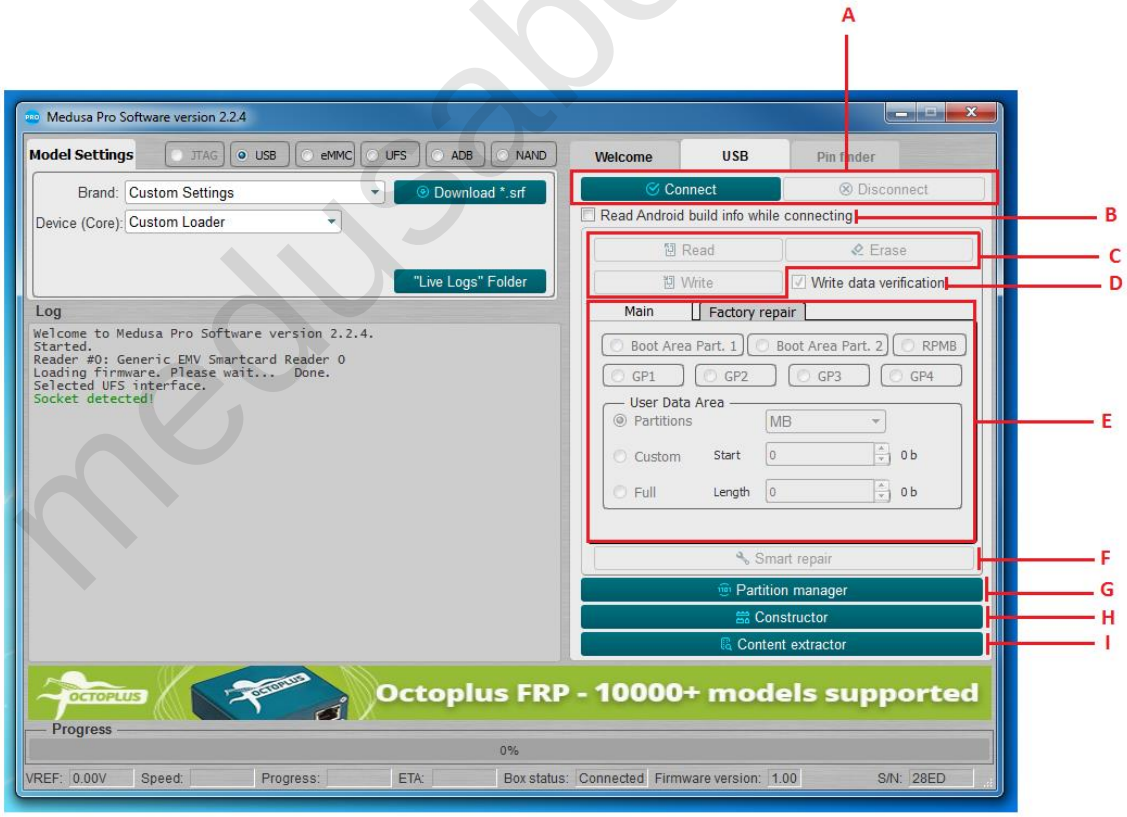

Figura. 2 separador Interfaz da janela principal

A. Inicialização do dispositivo ligado;
B. Pesquisar e ler "Android Info" ao inicializar o dispositivo;
C. Funções standard de leitura, escrita e borramento;
D. Verificação dos dados registados;
E. Ajuste das definições de leitura, escrita e borramento (endereço, tamanho, secções individuais, todo o flash), é possível introduzir valores em bytes, blocos, kilobytes e megabytes (bytes, blocos são introduzidos em hexadecimal; kilobytes, megabytes em forma decimal);
F. Reparação do flash com a ajuda do ficheiro SRF;
G. Trabalho com secções;
H. Criação de ficheiros SRF;
I. Parsing do conteúdo da memoria flash.

1.1. Algoritmo geral de recuperação de dispositivos

Em geral, o processo de recuperação do dispositivo consiste em várias etapas:

1. É necessário ligar fisicamente o dispositivo a uma das interfaces Fig.1A;
2. Seleccione a interface necessária;
3. Configurar a interface no campo Fig.1B;
4. Inicialize o dispositivo clicando no botão "Ligar" (Fig. 2A);
5. Os resultados da inicialização são mostrados na figura 1C do registo. No caso de uma inicialização bem sucedida, o registo pode conter certos parâmetros do dispositivo, por exemplo, fabricante do dispositivo, modelo do dispositivo, número de série, capacidade, etc. Se o dispositivo não pôde ser inicializado, o registo mostra informações sobre a impossibilidade de inicializar o dispositivo;
6. Após uma inicialização bem sucedida, deve seleccionar o método pelo qual planeia restaurar o dispositivo. O método pode ser diferente para cada dispositivo (firmware de fábrica, dumps de dispositivos previamente guardados, utilização de ficheiros SRF originais criados pela equipa Medusa para uma recuperação mais rápida e fácil do dispositivo).

2. Trabalho com memórias flash eMMC

Medusa Pro e Medusa Pro II funcionam em conformidade com EMC 5.1 (JESD84-B51) e são totalmente compatíveis com versões anteriores da especificação.

O software Medusa Pro permite-lhe trabalhar com memória flash seleccionando uma largura de bus de dados de 1, 4 ou 8 bits.

Box	Largura do Bus, bits
Medusa Pro	1, 4
Medusa Pro II	1, 4, 8

Tabela 1 Conformidade da largura do bus eMMC con la box conectada

2.1 Inicialização eMMC

Antes de iniciar a inicialização do eMMC, é necessário configurar os parâmetros básicos de ligação, tais como tensão (Tensão, por defeito 1,8 V), largura do bus (Modo Bus, por defeito 1 bit) e frequência de transmissão (Velocidade do bus, por defeito Auto). Na maioria dos casos, a tensão e a frequência de transmissão podem ser deixadas inalteradas. Se a unidade flash for ligada através dum socket "Medusa", a largura do bus pode ser seleccionada de acordo com a box actualmente utilizada, de acordo com a tabela 1.

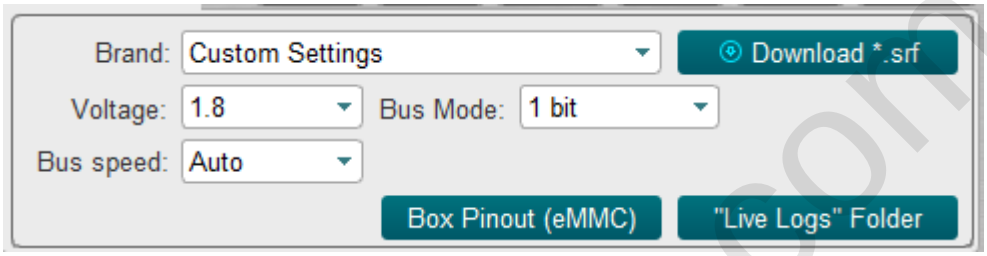

Figura. 3 Configuração dos parâmetros básicos para a inicialização da unidade flash eMMC

Ao clicar no botão "Ligar" (Fig. 4), no caso de uma inicialização bem sucedida, a informação sobre o transportador é apresentada no registo (exemplo em Fig. 5).

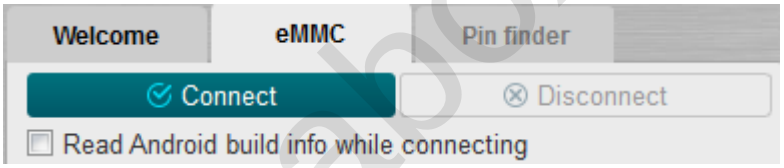

Figura. 4

```
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 Janela com o registo da unidade flash ligada

A partir de agora, a memória flash é considerada inicializada e vc pode trabalhar com ela.

2.2. Funções estandar eMMC (Main)

As funções estandar de leitura, escrita e borramento estão disponíveis no separador "Principal".

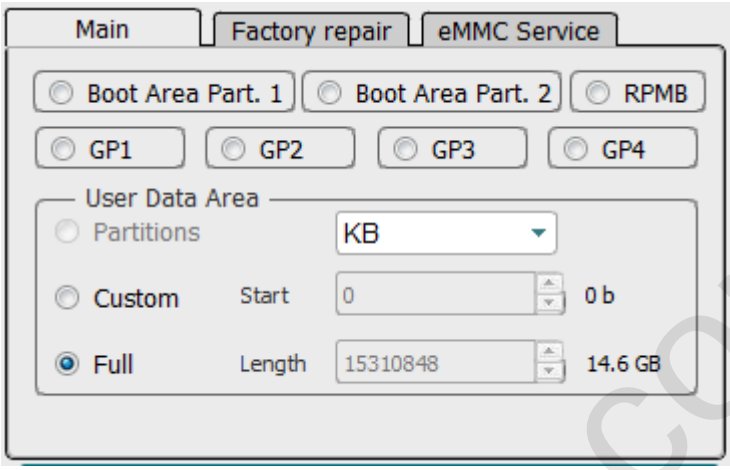

Figura 6

Na parte superior do separador pode seleccionar a área de memória com que deseja trabalhar, desde que a área seleccionada não seja de tamanho zero:

- 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. Trabalho com secções eMMC (Partitions)

Se determinadas secções foram encontradas na memória flash durante a inicialização, é possível seleccionar as secções necessárias para simplificar o trabalho com elas através da pré-selecção do modo "Partições" (Fig. 7) e pressionar o botão "Ler". (Fig. 8), será aberta uma janela com as secções, Fig.9

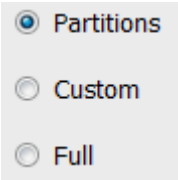

Figura. 7

Figura. 8

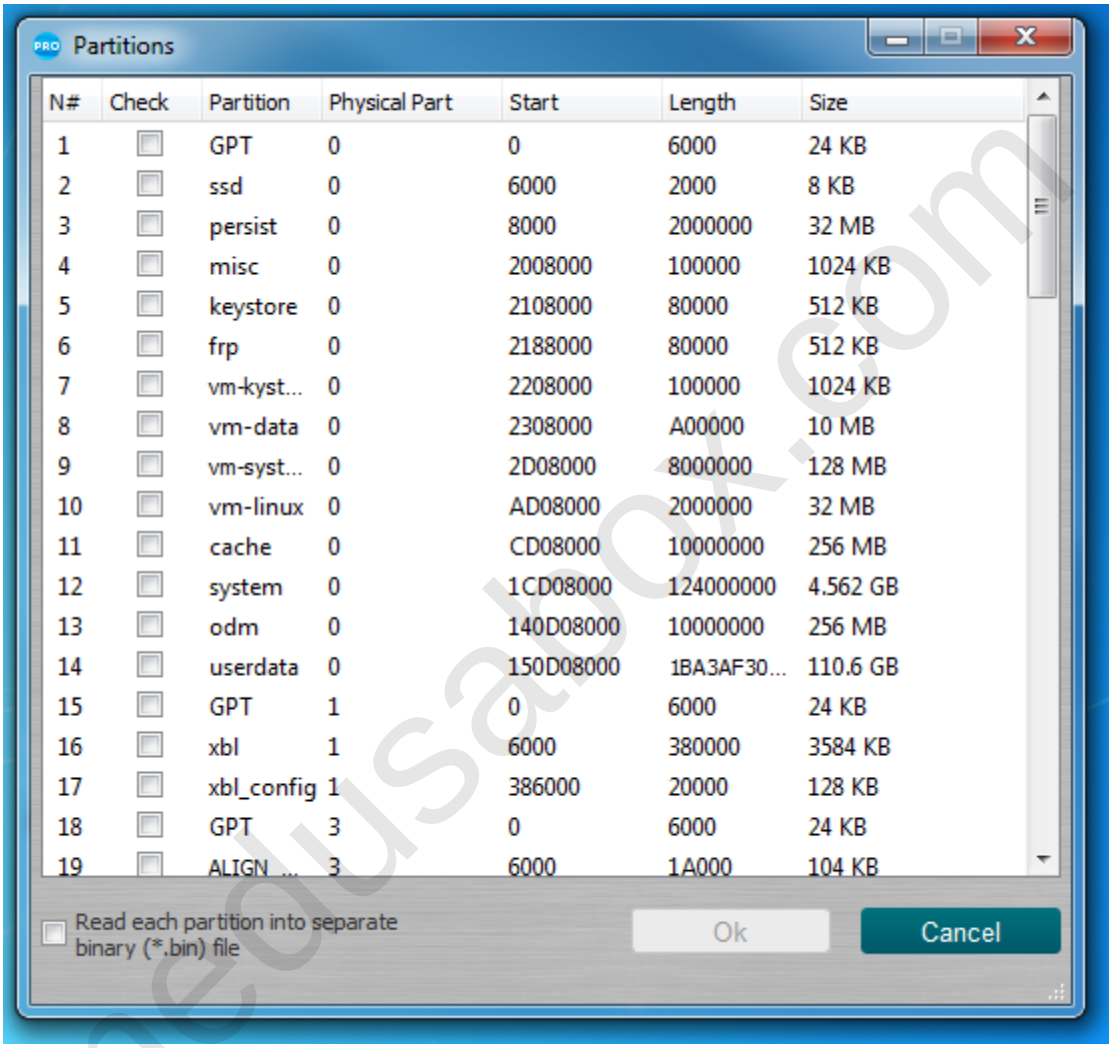

Figura. 9 Janela com secções

Nesta janela, deve seleccionar as secções que deseja ler. Estas partições serão lidas num ficheiro com a extensão *.mpt, também é possível ler partições em ficheiros *.bin separados, para isso deve marcar a opção "Ler cada partição num ficheiro binário separado (*.bin)".

Para escrever partições, seleccione o ficheiro com a extensão *.mpt, que foi lido anteriormente, e clique em "Escrever" (Fig. 8).

2.2.2. Trabalhos em eMMC com endereços e blocos arbitrários (Custom)

Quando é necessário escrever / ler / borrar dados num determinado endereço e numa determinada quantidade, é necessário mudar para o modo Personalizado (Fig. 10), escolher de uma lista de unidades em que os dados serão introduzidos:

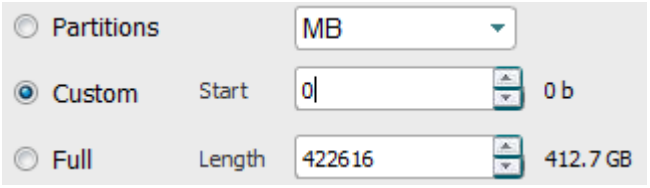

Figura. 10

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

2.2.3. eMMC trabalho com o volume completo da memória flash (Full)

Se precisar de escrever/ler/borrar a informação de toda a memória flash, tem de mudar para o modo **Full** (Fig. 11)

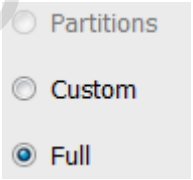

Figura. 11

Em seguida, realizar a operação necessária (Fig. 8).

2.3. eMMC trabalho com firmwares do fabricante (Factory repair)

Nesta secção (Fig. 12) é implementada a capacidade de restaurar a memória interna do dispositivo com firmware de fábrica de diferentes fabricantes.

O procedimento de recuperação completa consiste em seleccionar o dispositivo desejado, clicando no botão correspondente no separador e na janela que se abre, seleccionar o ficheiro de firmware com a extensão necessária para este dispositivo e escrever o firmware seleccionado.

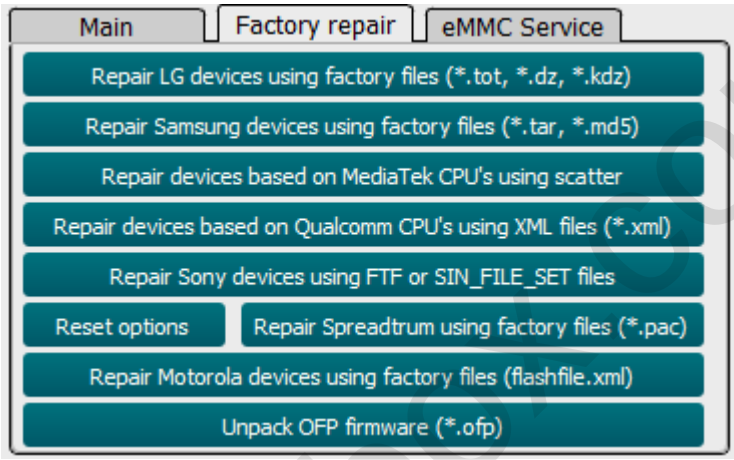

Figura. 12 Separador Factory repair

2.4. eMMC trabalhos com funções de serviço (eMMC Service)

Este modo é utilizado para trabalhar com registos internos eMMC (CID, CSD, EXT_CSD), particionamento de memória flash, comutação do modo de memória flash, leitura de informação adicional, actualizações de firmware.

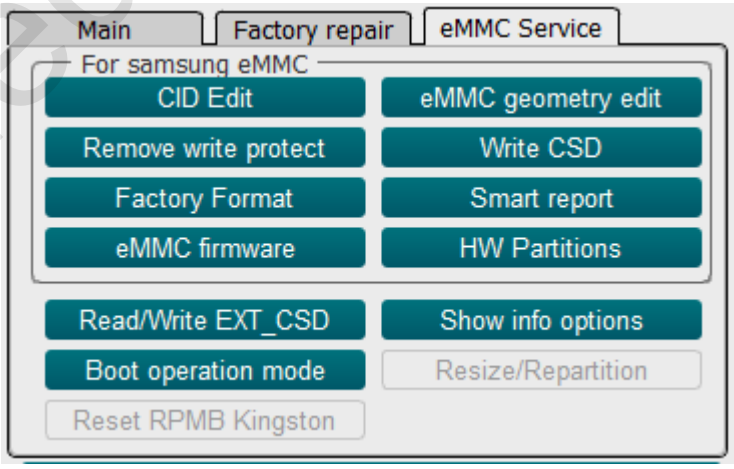

Figura. 13 Separador eMMC Service

«CID Edit» - Utilizado para editar o registo CID;

«Remove write protect» - Remove a protecção de escrita;

«Factory Format» - Borra completamente a memoria flash;

«eMMC firmware» - Actualização do firmware do driver EMMC;

!!! A Medusa Pro Software não é responsável pela perda do dispositivo ao actualizar o firmware do controlador. Todas as operações de actualização de firmware do controlador são realizadas por conta e risco do próprio utilizador.

«eMMC geometry edit» - Estabelecer tamanhos Boot1, Boot2, RPMB;

«Write CSD» - Utilizado para editar o registo CSD;

«Smart report» - Ler informação sobre o recurso da unidade flash;

«HW Partitions» - Utilizado para ajustar os tamanhos de GP1, GP2, GP3, GP4 e área do utilizador;

«Read/Write EXT_CSD» - Trabalhos com EXT_CSD;

«Boot operation mode» - Configuração de boots**;**

3. Trabalho com memórias flash UFS

O software Medusa Pro suporta memória flash UFS com a box Medusa Pro II. **Medusa Pro não suporta UFS!!!** Estándares UFS suportados com Medusa Pro Software:

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

O Medusa Pro II funciona num Lane e suporta os seguintes modos de trabalho de bus: LS PWM G1, LS PWM G2, LS PWM G3, LS PWM G4, HS G1. Trabalhar com meios UFS coincide principalmente com o eMMC, a diferença está nas definições de inicialização, em UFS este separador é parecido com o da Figura. 14, em que no campo "Gear" é seleccionado em qual dos modos a interface UFS irá funcionar (Tabela. 2) e separador **UFS Service**(Fig. 15).

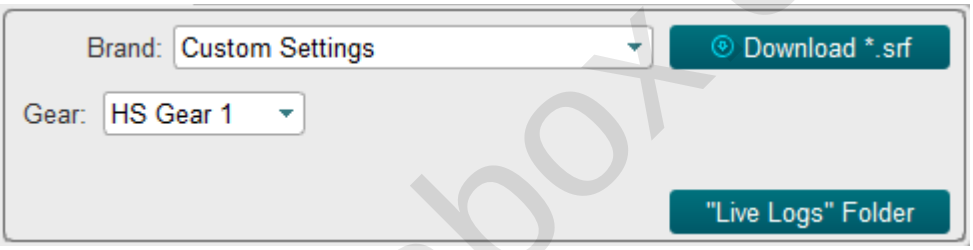

Figura. 14 Configuração dos parâmetros básicos para a inicialização da unidade UFS

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)

Tabela 2 Correspondência da velocidade de transferência de Gear

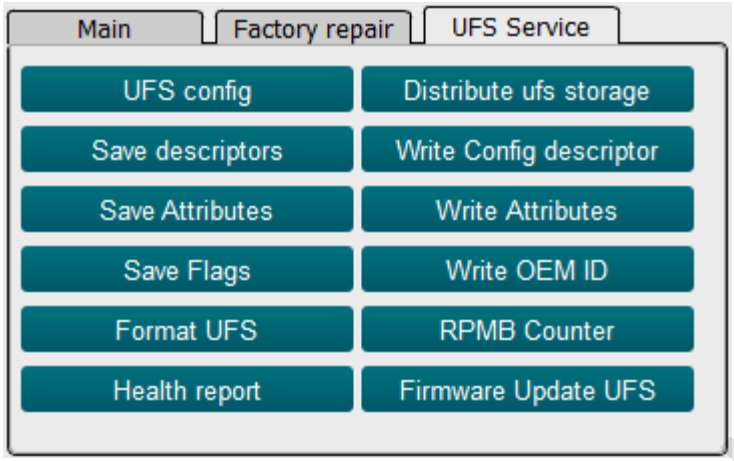

Figura. 15 Separador UFS Service

3.1. UFS trabalhos com funções de serviço (UFS Service)

O botão "UFS config" permite visualizar todos os descritores, indicadores e atributos.

Os botões **"Save descriptors"**, **"Save Attributes"** ou **"Save Flags"** são utilizados para salvar descritores, atributos e bandeiras.

Write Config descriptor - o botão é utilizado para escrever o descritor de configuração. De acordo com a norma UFS, para configurar os medios flash, é necessário escrever o Descritor de Configuração que foi previamente lido. Como o formato Config Descriptor depende da versão da especificação UFS, o Software Medusa Pro converte automaticamente o Config Descriptor para a versão requerida.

Por exemplo: se tentar escrever Config Descriptor versão 2.1 numa memória flash com versão 3.1, o software converte automaticamente o descriptor.

«Format UFS» - Utilizado para apagar todos os LU.

«Distribute UFS storage» - Usado para dividir a memória flash em LU.

«Write Attribute» - Utilizado para registar atributos de um ficheiro guardado.

«Write OEM ID» - Utilizado para registar a identificação OEM do ficheiro guardado.

«RPMB Counter» - Utilizado para ler o contador da RPMB.

«Health report» - Ler informação sobre o recurso da unidade flash.

«Firmware Update UFS» - Utilizado para actualizar o firmware do controlador UFS.

3.1.1 Divisão da unidade UFS em LU (Distribute UFS Storage)

Para dividir a unidade flash no LU, clique em **"Distribute UFS storage"** e a janela abrirá. Fig.16. Os tamanhos LU podem ser introduzidos em blocos, megabytes e gigabytes, para isso é suficiente alterar o modo de entrada. Fig. 17(A). O tamanho LU é introduzido no campo **«LUN Size»** e o volume restante será exibido no campo **«Rest size»**. (Fig. 18), premindo novamente o modo de entrada transfere o tamanho residual para o campo de tamanho. Fig. 17(**B**). Ao clicar no botão **"Add LUN"**, a secção aparecerá na lista, criando assim uma lista de todos os LU. Para criar estes LU na memória, deve clicar no botão **"CreateLUNs"**. Uma mensagem aparecerá no registo indicando que a configuração foi guardada com sucesso. O software verifica o número de LU criado, se o número exceder o máximo possível, o botão "Add LUN" fica inactivo.

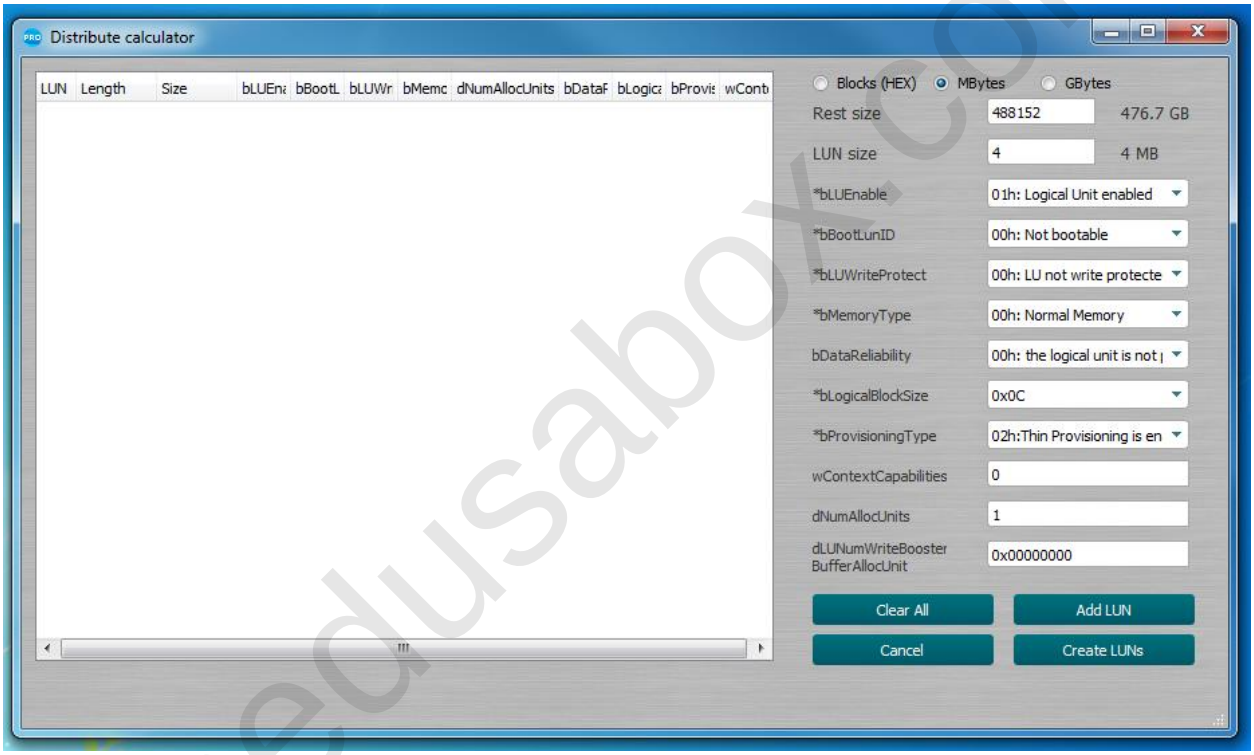

Figura. 16 Janela Distribute UFS storage

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

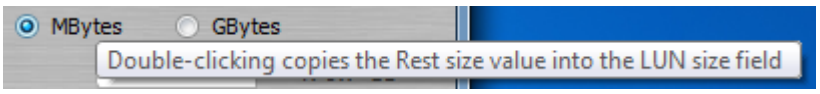

Figura. 17 (B) Pressionando duas vezes o modo de entrada do tamanho LU

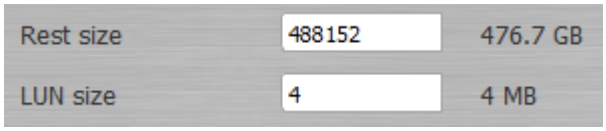

Figura. 18 Campos remanescentes e tamanho do actual LU

3.1.2 Actualização do firmware do controlador UFS (Firmware update UFS)

Se precisar de actualizar o firmware do controlador UFS, pode fazê-lo clicando no botão **"Firmware Update UFS"** (Fig. 15) e a janela de recuperação de firmware será aberta (Fig. 19). No topo da janela encontrará o fabricante, o nome e a revisão actual da unidade flash ligada. Em baixo pode ver o fabricante, nome e revisão do firmware para o qual se pretende actualizar. Se o firmware estiver na base de dados do Software Medusa Pro, todos os campos na parte inferior da janela serão automaticamente preenchidos e o botão **"Update to"** será activado; caso contrário, os campos serão marcados como **«Not supported»**.

O utilizador pode actualizar o driver UFS com o "seu" firmware clicando no botão **"Open file..."** para especificar o caminho para o firmware do utilizador. Se o firmware falhar, o botão **"Update to"** (Actualizar para) será activado.

!!! A Medusa Pro Software não é responsável pela perda do dispositivo ao actualizar o firmware do controlador. Todas as operações de actualização de firmware do controlador são realizadas por conta e risco do próprio utilizador.

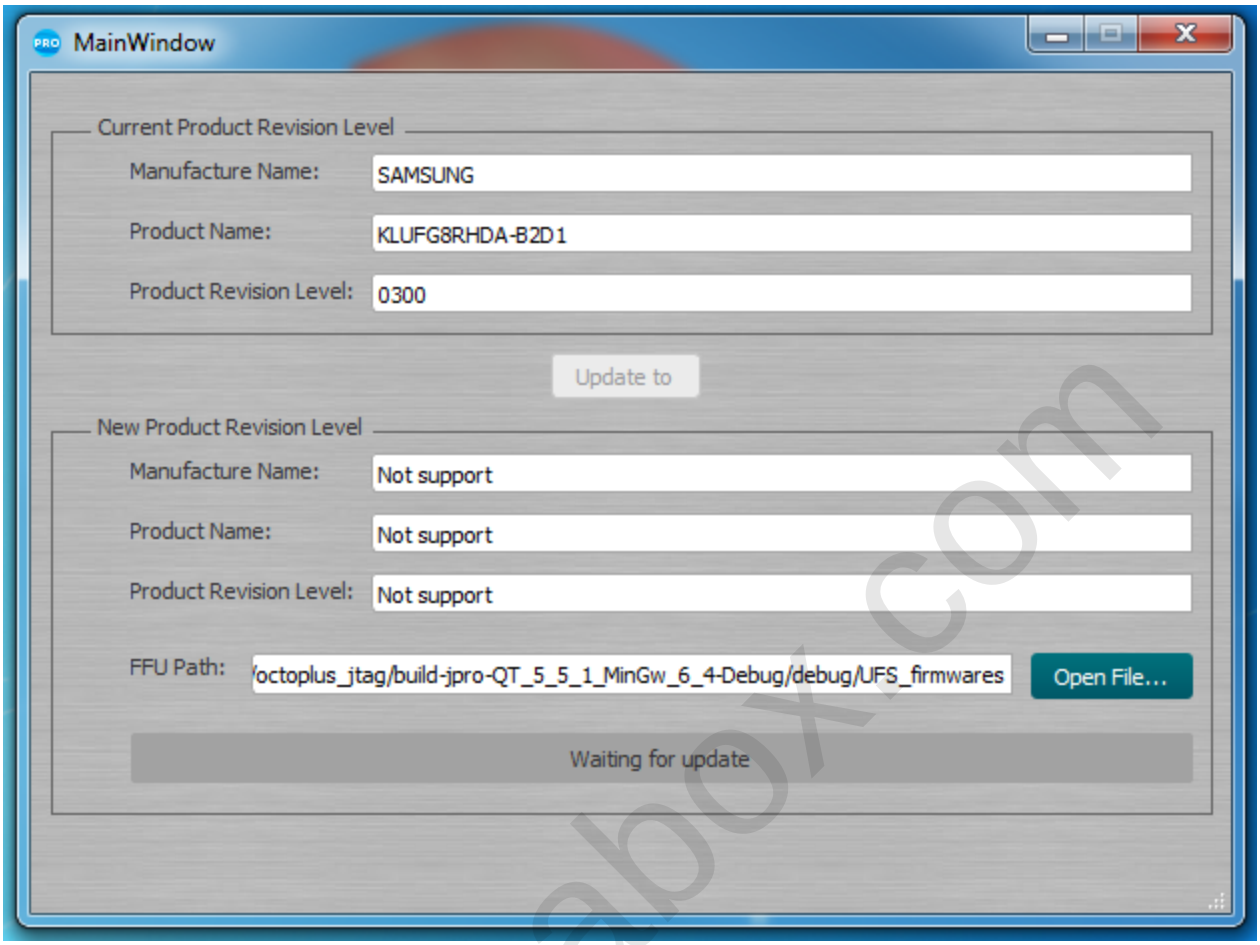

Fig.19 Janela Firmware Update UFS

4. Trabalhos por USB

O software Medusa Pro é compatível com USB com dispositivos com processadores Qualcomm ou MediaTek (MTK) instalados.

Para inicializar o dispositivo, este deve estar em EDL (Emergency Download Mode). É possível mudar para o modo EDL de diferentes maneiras, a maneira mais eficaz é fechar os pontos de teste correspondentes na placa do dispositivo. Para realizar este procedimento, é necessário desmontar parcialmente o dispositivo.

Em alguns outros casos, pode mudar o dispositivo para o modo EDL com um comando especial Android ou outros modos, tais como **Recovery**, **Fastboot**, etc. Assim que o dispositivo entra em modo EDL, torna-se disponível para o sistema como uma porta COM, através da qual a interacção em modo EDL tem lugar. Visualização de dispositivos em modo EDL ligados via USB, Qualcomm (Fig. 20) e MTK (Fig. 21)

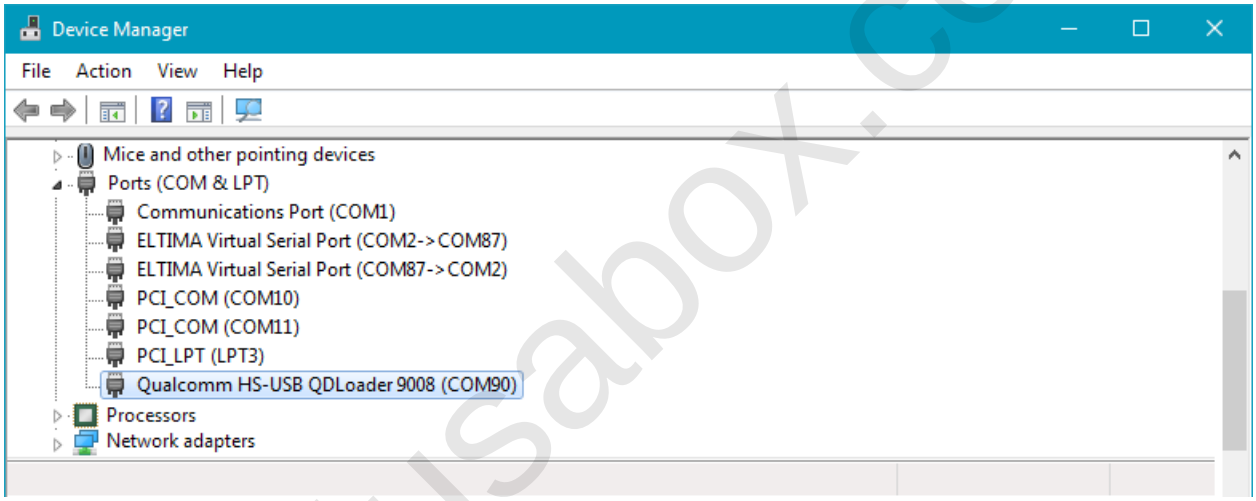

Fig. 20 Dispositivo com processador Qualcomm em modo EDL, ligado via USB

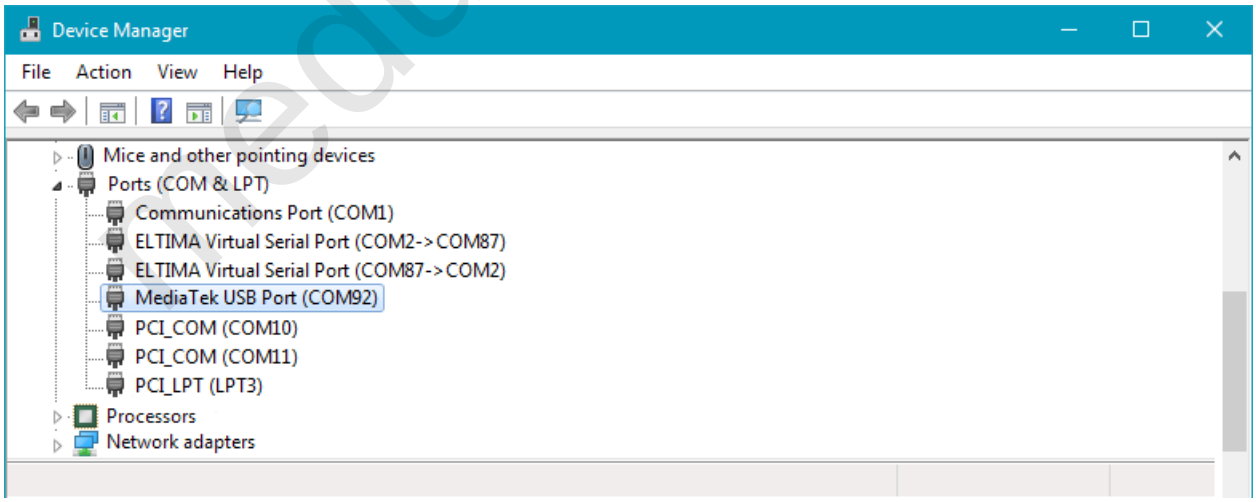

Fig. 21 Dispositivo com processador MTK em modo EDL, ligado via USB.

4.1. Inicialização de processadores Qualcomm via USB

Após certificar-se de que o dispositivo está em modo EDL e definido no sistema como "Qualcomm HS-USB QDLoader 9008" (Fig. 20), selecione da lista **"Device (Core")** (Fig. 22) o processador instalado no dispositivo e pressionar **Connect**.

Se não souber o nome do processador no dispositivo, pode usar a função de detecção automática do processador seleccionando **"Detecção automática"** na lista **"Device (Core)"** e clicando em **"Connect"**.

Se a inicialização for bem sucedida, o registo exibirá informações sobre o dispositivo e poderá trabalhar com ele a partir de agora. Utilizando as funções padrão de leitura/gravação/escrita/apagamento do separador **"Main"** (Fig. 23) e trabalhar com o firmware de fábrica no separador "Factory repair" (Fig. 24).

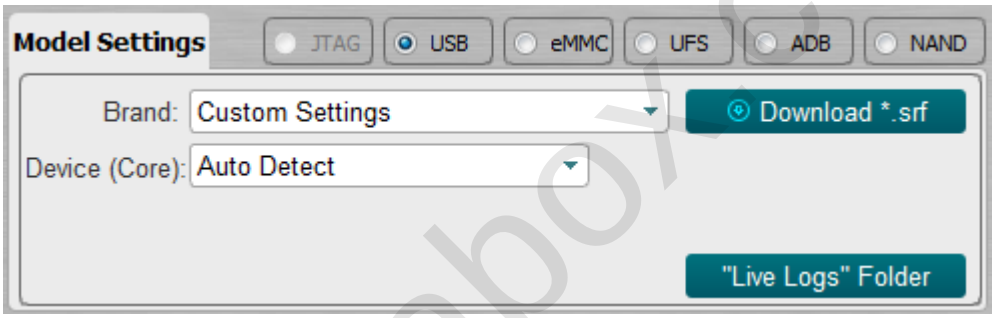

Fig.22

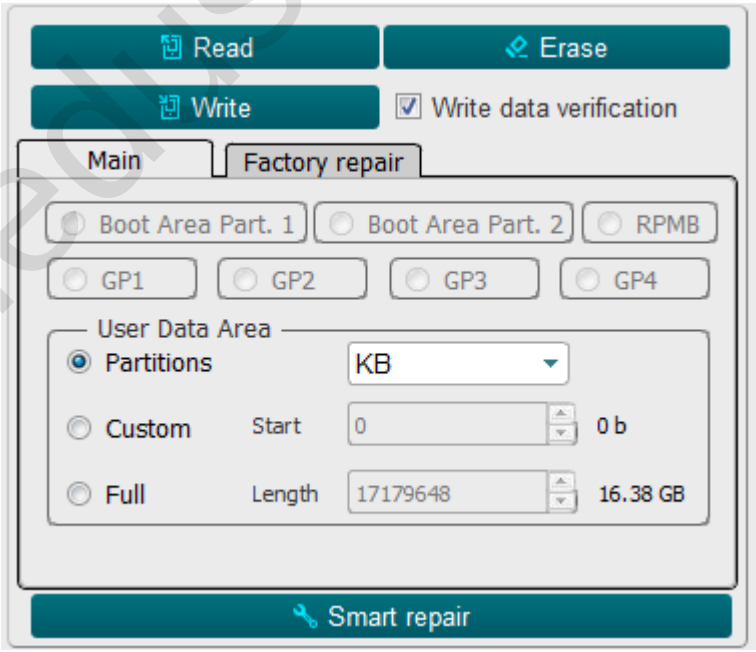

Figura. 23

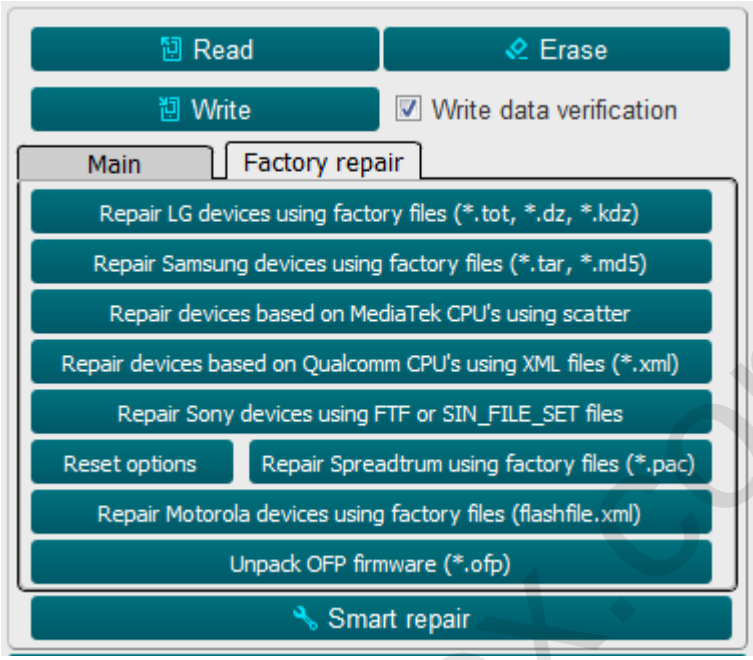

Figura. 24

4.2. Inicialização de processadores(MTK) via USB

Depois de se certificar que o dispositivo está em modo EDL e definido no sistema como **"MediaTek USB Port"** (Fig.21), seleccionar na lista **"Device (Core)"** (Fig.22) uma das duas opções **"MTK Custom"** ou **"MTK General"**.

A diferença entre estas duas opções é que no **MTK Custom** é necessário seleccionar 3 ficheiros para inicializar o dispositivo: **"Download Agent (DA)", "Preloader" e "Authentication File"** (**ficheiro AUTH**) (Fig. 25).

Para **"MTK General"** só precisa de seleccionar um ficheiro: "**Precarregador**" (Fig. 26) e clicar em " **Connect** ". Se a inicialização for bem sucedida, o registo exibirá informações sobre o dispositivo e poderá trabalhar com ele a partir de agora. Utilizando as funções padrão de leitura/escrita/apagamento do separador **"Main"** (Fig. 23) e trabalhar com o firmware de fábrica no separador **"Factory repair"** (Fig. 24).

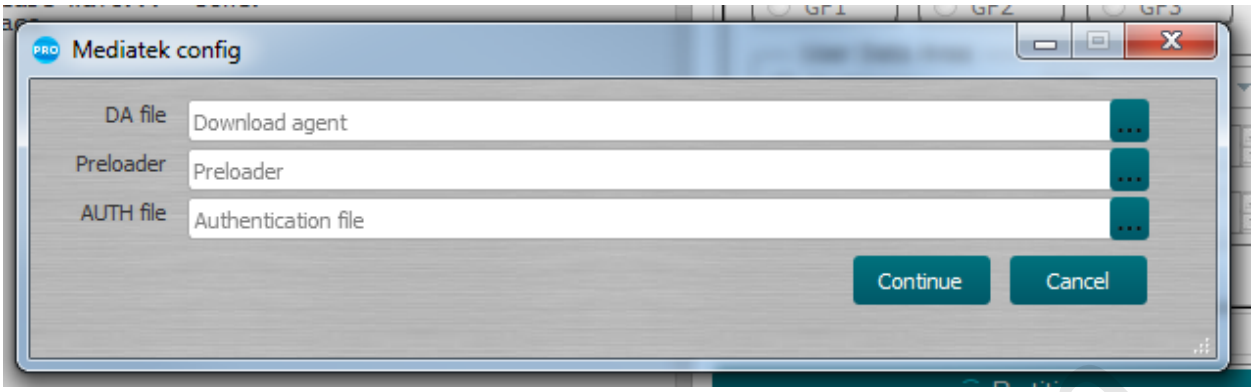

Figura. 25

Figura. 26

5. Trabalho com NAND

O software Medusa Pro suporta unidades flash JEDEC ONFI NAND de 8 bits e 16 bits de largura e 32/64 bits Apple PPN. Fisicamente, a unidade flash é ligada através de um socket (conector) **Medusa** ou soldada ao **conector pin**. Dependendo do tipo de unidade de flash, é seleccionado o modo **PPN** ou **ONFI** (Fig. 27)

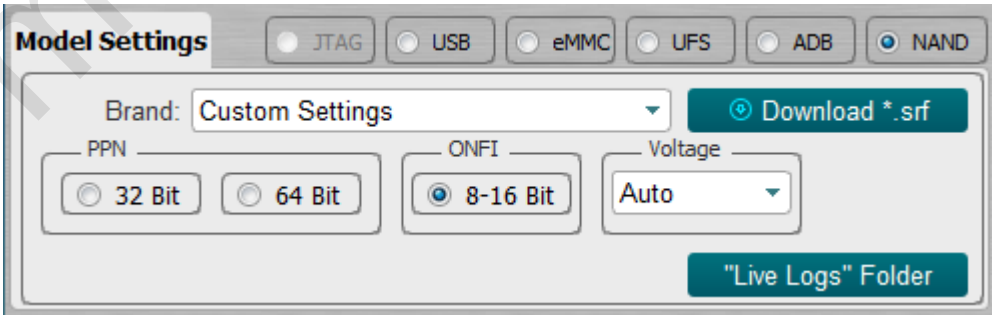

Figura. 27

Apenas funções de leitura/escrita/erase padrão estão disponíveis no modo **ONFI**.

No modo **PPN**, para além das funções padrão, estão disponíveis funções adicionais no separador **Serviço NAND** (Fig.28).

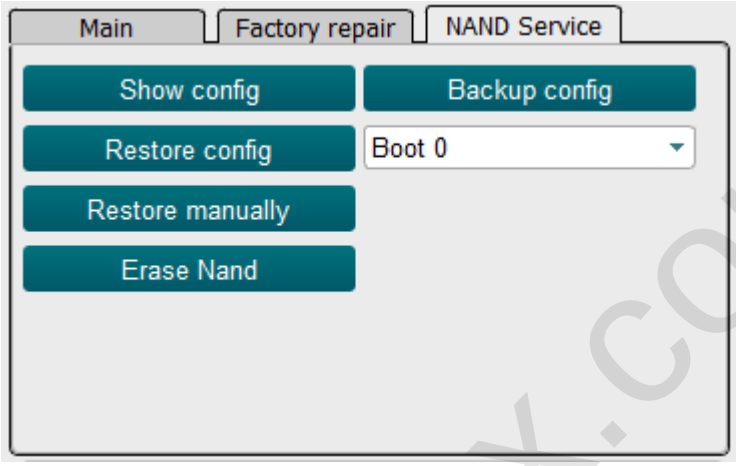

Figura. 28

- **Show config** - Destacar a informação de configuração no registo;
- **Backup config** - Guardar configurações em ficheiros separados;
- **Restore config** - Restaura a configuração do ficheiro guardado no "Boot" seleccionado;
- **Restore manually** - Fornece acesso a correcções de configuração manualmente;
- **Erase NAND** - Eliminar o armazenamento NAND.

6. Trabalho com ADB (Android Debug Bridge)

`O dispositivo deve ter o ADB activado.` Para activar o ADB no seu dispositivo Android, siga estes passos:

- Entrar em **Settings** → **About phone** → **Software information**;
- Clicar em **Build number** seis vezes (até a mensagem **You are now a developer**);
- Entrar no menu **Settings** e encontrar novo item **Developer options**;
- Mover o interruptor de **USB Debugging** para a posição activa;
- Deve então ligar o dispositivo a um PC e clicar em **Connect**. Se a inicialização for bem sucedida, a informação sobre o dispositivo deve ser exibida no registo. Só leitura está disponível no modo ADB.