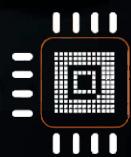


Conceito Sobre Emmc (EMMC, EMCP & UFS)



Mobile Emmc

WWW.MOBILEEMMC.COM.BR



Mobile Emmc



Tópicos

→ Capítulo 1 Conhecimento Gerais

→ Capítulo 2 eMMC / eMCP

→ Capítulo 3 UFS

Cursos EAD
www.mobileemm.com.br



35 99233-1820

CONHECIMENTOS GERAIS

Antes de começar a realizar os procedimentos de eMMC ou algum outro processo, é importante saber como funciona um telefone em si mesmo. Telefone hoje é mais do que isso, não se mais utilizado especificamente para a sua função principal que é fazer e receber chamadas ou enviar e receber mensagens, agora inclui um infinitas funções adicionais, como tirar fotos, tocar sua música favorita, gravar vídeos, armazenar sua agenda, etc... bem, tudo em um único dispositivo. Mas nós realmente sabemos como nosso dispositivo funciona internamente? Devemos entender o funcionamento de uma equipamento tanto em software quanto em hardware, pelo menos os conceitos básicos para ser capaz de realizar procedimentos um pouco mais avançados, como conexões ISP para recuperação de equipamentos mortos devido a danos na boot, por isso Neste primeiro capítulo, vamos analisar um pouco sobre as partições no software que precisamos saber sobre o sistema operacional Android, bem como as principais funções, em termos gerais, do hardware do mesmo, de modo que, ao iniciar a programação da memórias, é mais fácil entender o motivo de cada procedimento e quando é realmente um problema de software e quando é um problema de hardware. Portanto, convido você a dar uma boa leitura e se possível, reler esta parte quantas vezes forem necessárias para poder entender tudo isso sem maiores problemas.

Eletrônica Digital

Antigamente também, todos os equipamentos de telecomunicações trabalhavam diretamente com sinais analógicos vindos de microfones, câmeras de TV e outras fontes. No entanto, atualmente a maioria das transmissões de informações sem fio, por ondas de rádio, e por meios físicos como fibras ópticas e cabos, ocorre na forma digital. Os sinais analógicos são convertidos em digitais e, com isso, transmitidos de forma muito mais eficiente.

Portas-lógicas

Introduzir de maneira breve as portas lógicas digitais, conhecimento fundamental para se avançar no estudo e entendimento de sistemas digitais.

Sistema Digital

Um sistema digital é um sistema matemático que define informações como valores numéricos. Dessa forma, é possível definir operações digitais como cálculos matemáticos. Comumente trabalhamos com valores numéricos na base decimal, mas um sistema digital trabalha de maneira diferente. Em analogia ao sistema decimal, onde cada dígito possui 10 valores possíveis, um sistema digital é um sistema binário, onde cada dígito possui apenas 2 valores possíveis. Esses dois valores são definidos como “níveis lógicos” e adota-se o valor de 0 (zero) ou 1 (um) apenas.

CAPÍTULO I

Transportando esse sistema para um sistema eletrônico, é necessário apresentar esses dois valores como sinais elétricos. Para tanto, podemos entendê-los como:

Ligado ou desligado;

Nível alto ou nível baixo;

Alimentado ou em zero;

VCC ou Terra.

As operações observáveis para esses níveis lógicos são definidas como operações lógicas. Todas as possíveis operações lógicas são baseadas em apenas 3 operações primárias, que são:

Inversão;

Soma lógica;

Produto lógico.

Portas Lógicas

Porta Lógica NOT

A porta NÃO ou inversora (NOT) utiliza o operador de inversão. Para um determinado valor na entrada, a saída possui um valor contrário ao da entrada. Se a entrada for 1, a saída será 0. Se a entrada for 0, a saída será 1. Ou seja, para um valor na entrada a saída será seu complemento, ou o inverso do valor na entrada.

CAPÍTULO I

Porta Lógica AND

Para se explicar o funcionamento da porta E (AND) pode-se fazer um paralelo com um circuito com interruptores, como na figura abaixo. Para que a lâmpada acenda é preciso que os dois interruptores estejam ligados.

Portas Lógicas: Porta Lógica AND

Analogia com a porta lógica AND

A porta lógica E (AND) utiliza-se do operador de produto lógico. A saída é igual a 1 se todas as entradas for 1. A saída é igual a zero se ao menos uma entrada for 0, se todas entradas não forem 1.

Porta Lógica OR

Uma forma simples de se entender o funcionamento da porta OU (OR) é pensar em um circuito com interruptores em paralelo, como na figura abaixo. Para que a lâmpada acenda é preciso que um dos dois interruptores esteja ligado.

Portas Lógicas: Porta Lógica OR

Analogia com a porta lógica OR

A porta lógica OU (OR) utiliza-se do operador de soma lógica. A saída é igual a 1 se pelo menos uma das entradas for 1. A saída é igual a zero se nenhuma entrada for 1, todas forem zero.

CAPÍTULO I

Porta Lógica NAND

A porta lógica NÃO E (NAND) utiliza-se do operador de produto lógico e o de inversão. A saída é igual a 0 se todas as entradas for 1. A saída é igual a 1 se ao menos uma entrada for 0, se todas entradas não forem 1.

Porta Lógica NOR

A porta lógica NÃO OU (NOR) utiliza-se do operador de soma lógica e o de inversão. A saída é igual a 0 se pelo menos uma das entradas for 1. A saída é igual a 1 se nenhuma entrada for 1, todas forem zero.

Porta Lógica XOR

A porta lógica OU EXCLUSIVO (XOR) utiliza-se do operador de soma lógica, com um círculo. A saída é igual a 0 se as entradas forem iguais. A saída é igual a 1 se as entradas não forem iguais, se uma delas diferirem das outras.

Porta Lógica XNOR

A porta lógica NÃO OU EXCLUSIVO (XNOR) utiliza-se do operador de soma lógica, com um círculo e o de inversão. Tem as saídas inversas da operação XOR. A saída é igual a 1 se as entradas forem iguais. A saída é igual a 0 se as entradas não forem iguais, se uma delas diferirem das outras.

CAPÍTULO I

Teorema de De Morgan

O Teorema de De Morgan diz respeito às seguintes afirmações:

Uma operação NAND é igual a uma operação OR com todas as entradas invertidas;

Uma operação NOR é igual a uma operação AND com todas as entradas invertidas.

Com essas duas afirmações podemos fazer diversas simplificações em expressões lógicas, referentes a circuitos digitais.

Sistema de numeração mais usado eletrônica

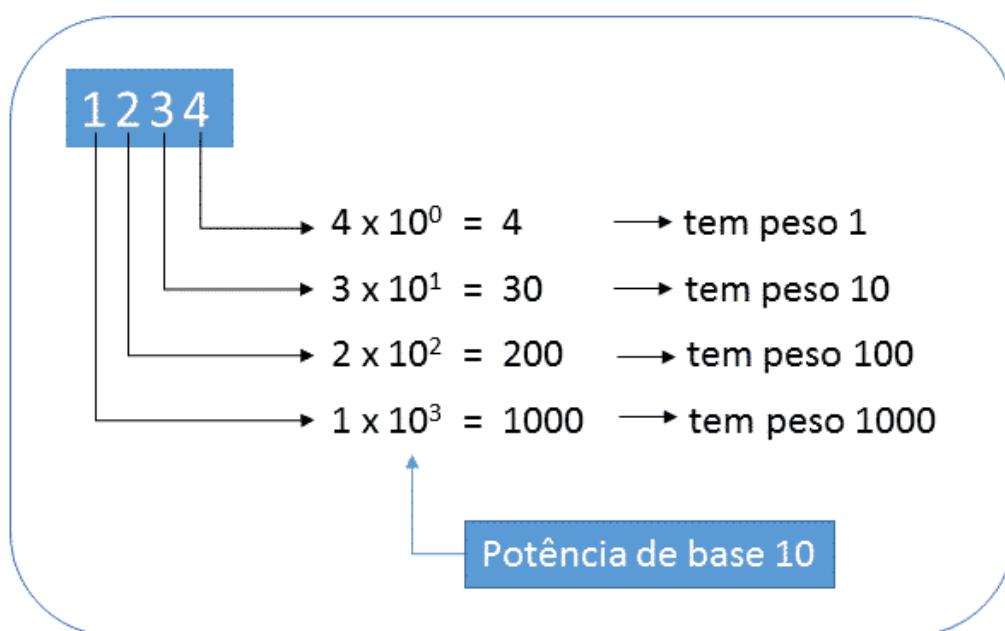
Os sistemas de numeração são usados para representar a quantidade de determinados elementos. O sistema mais usado pelas pessoas é o decimal. Esse sistema é formado por 10 algarismos. Para a eletrônica digital e sistemas de computação os sistemas binário, hexadecimal e octal são muito utilizados.

Entender as diferentes formas de representação numérica é muito importante para se trabalhar com eletrônica e programação. A seguir apresentaremos os detalhes de cada um desses sistemas de numeração mencionados.

Sistema de numeração decimal

O sistema de numeração decimal utiliza 10 algarismos para sua representação: 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9.

Para formar um número, associa-se um ou mais algarismos, e a posição de cada algarismo terá um peso de uma potência de 10. Dessa forma temos as unidades, dezenas, centenas e milhares. Cada posição terá um peso na representação:



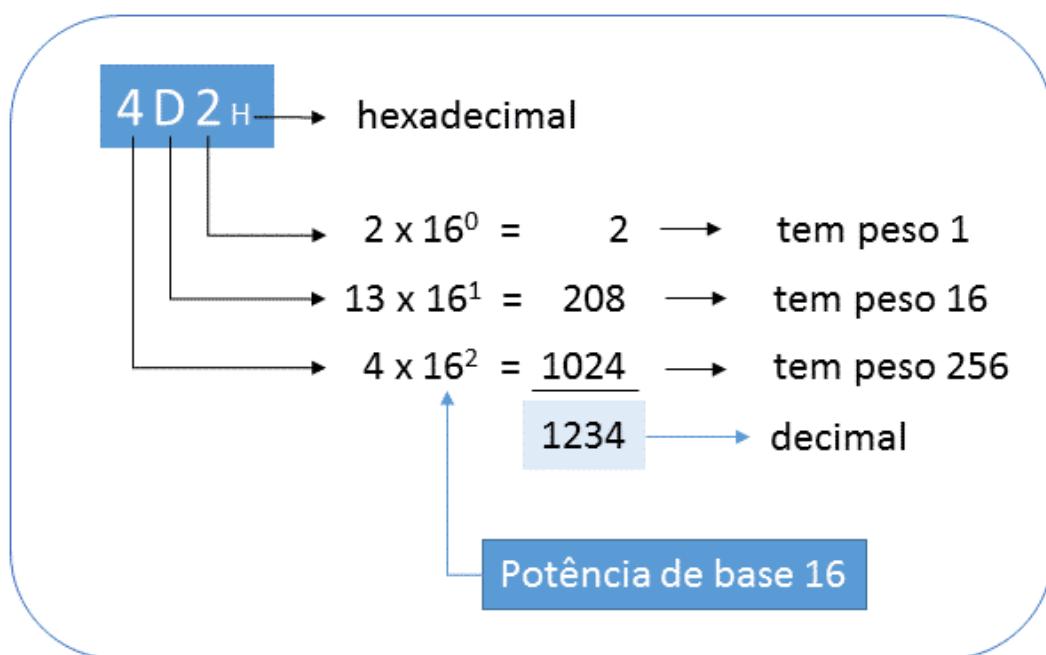
CAPÍTULO I

Figura 1 – Representação de um número em base 10

Como exibido na figura acima, o sistema decimal é representado na base 10 e cada posição é múltiplo de uma potência de 10

Sistema de numeração Hexadecimal

O sistema de numeração hexadecimal utiliza 16 algarismos para sua representação: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E e F. Assim como no sistema decimal, a associação dos algarismos representam diferentes números e a posição do algarismos será um múltiplo de potência de 16. Assim, o sistema hexadecimal é um sistema de base 16. Podemos fazer uma relação entre o sistema hexadecimal e o sistema decimal, como exibido na tabela abaixo:

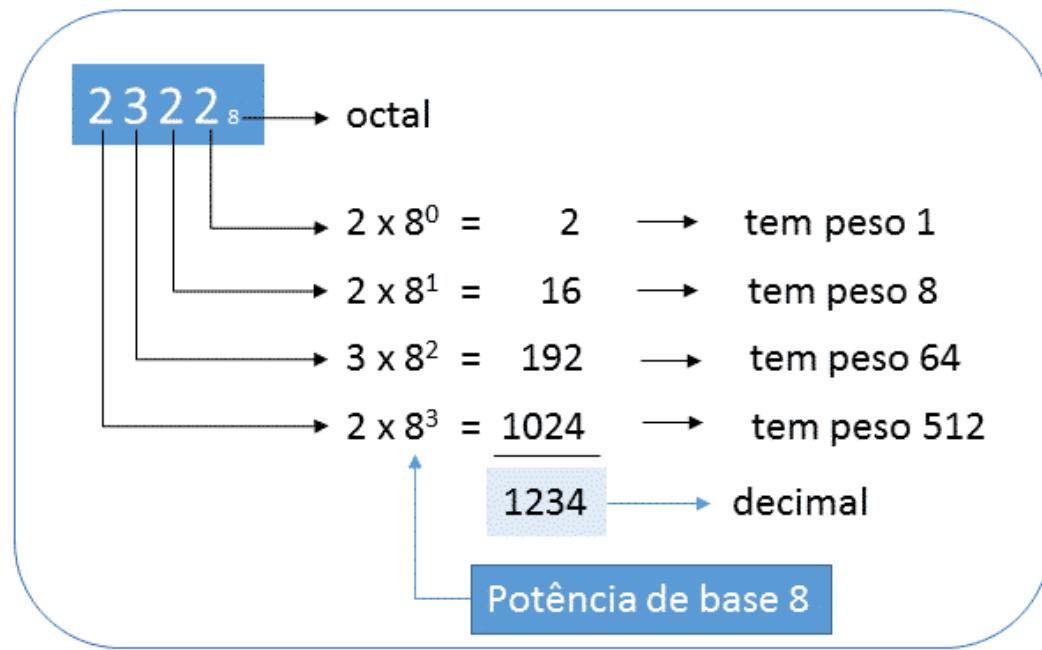


Como exibido figura acima, o sistema hexadecimal é representado na base 16 e cada posição é múltiplo de uma potência de 16.

CAPÍTULO I

Sistema de numeração Octal

O sistema de numeração octal utiliza 8 algarismos para sua representação: 0, 1, 2, 3, 4, 5, 6 e 7. Assim, o sistema octal possui base 8. A seguir é apresentada a representação de um número octal: o sistema hexadecimal e o sistema decimal, como exibido na tabela abaixo:



Como exibida figura acima, o sistema octal é representado na base 8 e cada posição é múltiplo de uma potência de 8.

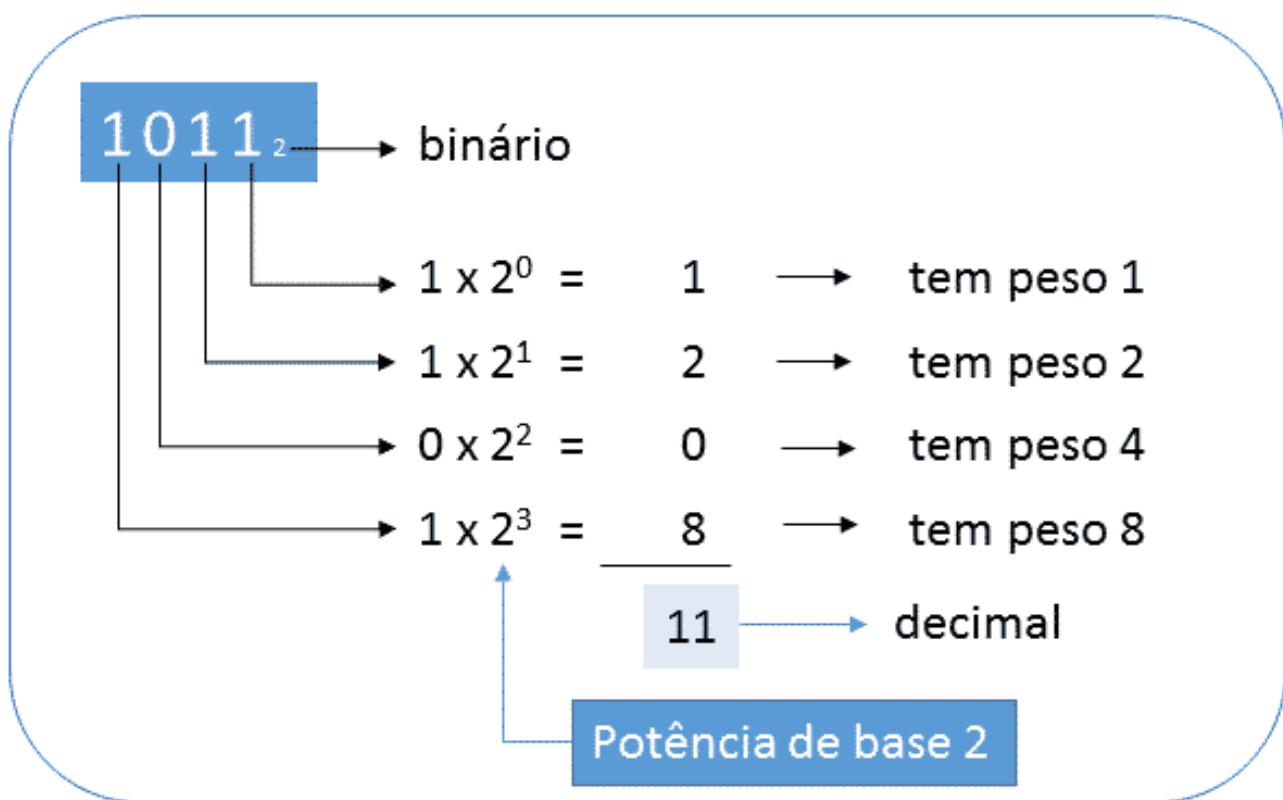
Sistema de numeração binário

O sistema de numeração binário utiliza apenas dois algarismos para sua representação: 0 e 1. Assim é um sistema de base 2. Ele é muito usado para representação de valores em sistemas digitais. O seu conhecimento é muito importante para a área de eletrônica. A seguir é apresentada sua representação:

CAPÍTULO I

Sistema de numeração binário

O sistema de numeração binário utiliza apenas dois algarismos para sua representação: 0 e 1. Assim é um sistema de base 2. Ele é muito usado para representação de valores em sistemas digitais. O seu conhecimento é muito importante para a área de eletrônica. A seguir é apresentada sua representação:



Como exibido figura acima, o sistema binário é representado na base 2 e cada posição é múltiplo de uma potência de 2.

Sistema Binário

Os computadores trabalham com um sistema incrível, que utiliza apenas dois valores para manipular qualquer informação. Isso quer dizer que todas as operações que o computador faz, desde permitir-nos a escrever um simples texto até jogar jogos 3D são realizados utilizando apenas dois valores, que por convenção são os dígitos “0” (zero) e “1” (um). Mas como isso é possível? Como o computador consegue dar andamento a todos os seus processos utilizando apenas os dígitos “0” e “1”? Como que isso tudo funciona na prática? Será que dentro de um processador ou em um CD/DVD veremos, literalmente, uma fileira de “0s” e “1s”?

O que é binário?

De forma geral, binário é um sistema que utiliza apenas dois valores para representar suas quantias. É um sistema de base dois. Esses dois valores são o “0” e o “1”.

Dai podemos concluir que para 0 temos desligado, sem sinal, e para 1 temos ligado ou com sinal.

Vale ressaltar que o sistema que utilizamos diariamente é o sistema de base dez, chamado também por base decimal. Esse sistema utiliza os algarismos indo-árabicos, que são: 0, 1, 2, 3, 4, 5, 6, 7, 8, e 9.

Nós seres humanos fomos “treinados” para trabalhar com a base decimal. Ela é a ideal para nós. Mas, para os computadores a base binária é a ideal.

Nos computadores esses zeros (“0s”) e uns (“1s”) são chamados de dígitos binários ou somente bit (conjunção de duas palavras da língua inglesa binary digit), que é a menor unidade de informação dos computadores. Dessa forma, tanto faz dizer dígito “0” e dígito “1”, ou, bit “0” e bit “1”.

CAPÍTULO I

ormação de informações / O caractere.

São esses bits que formam qualquer informação, porém, um bit sozinho não faz nada, é apenas um sinal qualquer. Para que os bits possam realmente formar uma informação, precisam ser agrupados, reunidos. Esses grupos podem ser de 8, 16, 32 ou 64 bits.

8 bits

10100110

Apesar de parecer ser um sistema limitado, agrupando bits é possível fazer uma infinidade de representações.

Agora vou explicar algo importante a saber: o conceito de “palavras”. Na terminologia dos computadores, palavra é um grupo de algarismos binário (bits) que podem ocupar uma localização na memória, e, que podem ser processados de uma só vez, podendo ser um número binário que é para ser manuseado como um dado, ou, uma instrução que diz ao computador que operação deve ser executada. Pode ser também um caractere ASCII representando uma letra do alfabeto, ou ainda, um endereço que diz ao processador onde se localiza um dado.

Existem tamanhos de palavras diferentes, onde cada um recebe um nome, veja:

• 4 bits = NIBBLE ($2^4 = 16$ variações);

CAPÍTULO I

- $8\text{ bits} = \text{BYTE}$ ($2^8 = 256$ variações);
- $16\text{ bits} = \text{WORD}$ ($2^{16} = 65.536$ variações);
- $32\text{ bits} = \text{DOUBLE WORD}$ ($2^{32} = 4.294.967.296$ variações);
- $64\text{ bits} = \text{QUAD WORD}$ ($2^{64} = 18.446.744.073.709.551.616$ variações).

Para entender melhor, imagine que com palavras de 8 bits, as instruções, os endereços, os números e dados são representados por números binários de 8 bits. Dessa forma o menor número binário é 00000000 (ou 00 em hexadecimal), e, o maior número é 11111111 (ou FF em hexadecimal), o que corresponde de 0 a 256 valores diferentes (variações).

Quanto maior a palavra, maior será o número que se pode trabalhar. Por exemplo: com palavras de 16 bits pode-se trabalhar com números decimais até 65.536. É preciso frisar aqui que apesar de um determinado PC usar palavras de 8 bits, por exemplo, não significa que o processador desse PC ficará restringido a números decimais inferiores a 256. Simplesmente significa que será necessário usar duas ou mais palavras para representar números maiores. Dessa forma é certo dizer que um processador de 32 bits é mais rápido que um de 16 bits, pois, este último será obrigado a dividir números maiores (acima de 65.536) em números menores que sejam possíveis de se manipular com 16 bits, o que levará mais tempo.

CAPÍTULO I

Está confuso?

Atualmente os processadores acessam a memória a 64 bits por vez, porém, continuamos a usar o nome BYTE para referir ao tamanho de uma memória.

O correto seria usar “BYTE” para designar o tamanho de uma memória de 8 bits, e, QUAD WORD para memórias de 64 bits.

Mas, qual seria o lado prático disso? Nenhum, e pior, acaba confundindo, pois, imagine ter que usar BYTE para memórias de 8 bits (SIMM/30), WORD para memórias de 16 bits, e assim sucessivamente. Por isso até hoje o usual é o BYTE para designar o tamanho de uma memória.

Na prática

Agora um ponto importante. Como que isso tudo funciona na prática? Será que dentro de um processador ou em um CD/DVD veremos, literalmente, uma fileira de “0s” e “1s”? Não é assim que funciona.

Infelizmente eu já vi muitas publicações fazerem afirmações totalmente erradas, que só servem para confundir a cabeça de quem está aprendendo. Li uma certa vez que se você pagasse um CD-ROM e “ampliasse” a sua superfície de gravação, viria uma série de “0s” e “1s”. Ora, não é assim que funciona.

Em nível de eletrônica, os bits 0 e 1 são representados através de valores de tensão. Por exemplo: o bit 0 pode ser representado por valores entre 0 e 0,3 volts. Já o bit 1 pode ser representado por valores entre 2 e 5 volts. Esses números são apenas

CAPÍTULO I

exemplos, não estamos afirmando aqui que são exatamente esses valores.

De forma geral, qualquer valor pode ser usado para representar os bits, depende do projeto, da aplicação e da tecnologia empregada. Com o avanço da tecnologia dos computadores, passou a se usar tensões cada vez menores, pois, os dispositivos eletrônicos passaram a trabalhar com tensões menores. Nos computadores são usados valores muito baixos, tais como esses que acabamos de mencionar.

Já o CD/DVD (dispositivos ópticos) armazenam as informações em forma de pequenos pontos denominados Pits e um espaço entre eles denominado Lands, que são interpretados no processo de leitura como “0s” e “1s” (bits).

Era Digital

Em nosso cotidiano é comum ouvir frases do tipo “era digital” ou “sistemas digitais” ou ainda “TV digital”. Mas, o que é digital? Resumidamente, digital é tudo aquilo que pode ser transmitido e/ou armazenado através de bits.

Um dispositivo digital é aquele que utiliza os bits para manipular qualquer tipo de informação (dados).

Círculo que gerencia a energia

Os circuitos integrados de gerenciamento de energia (CIs de gerenciamento de energia ou PMICs ou PMU como unidade) são circuitos integrados para gerenciamento de energia . Embora PMIC se refira a uma ampla gama de chips (ou módulos em dispositivos system-on-a-chip), a maioria inclui vários conversores DC / DC ou sua parte de controle. Um PMIC geralmente é incluído em dispositivos operados por bateria , como telefones celulares e reprodutores de mídia portáteis, para diminuir a quantidade de espaço necessária.

O termo PMIC se refere a uma classe de circuitos integrados que executam várias funções relacionadas aos requisitos de energia. Um PMIC pode ter uma ou mais das seguintes funções: [1]

- Conversão DC para DC*
- Carregamento de bateria*
- Seleção de fonte de energia*
- Escala de tensão*
- Sequenciamento de energia*
- Funções diversas*

Os CIs de gerenciamento de energia são dispositivos de estado sólido que controlam o fluxo e a direção da energia elétrica. Muitos dispositivos elétricos têm várias tensões internas (por exemplo, 5 V, 3,3 V, 1,8 V, etc.) e fontes de alimentação externa (por exemplo, tomada de parede, bateria, etc.), o que significa que o projeto de energia do dispositivo tem vários requisitos para operação. Um PMIC pode se referir a qualquer chip que seja uma função individual relacionada à energia, mas geralmente se refere a ICs que incorporam mais de uma função, como diferentes conversões de energia e controles de energia, como supervisão de tensão e proteção de subtensão. Ao incorporar essas

CAPÍTULO I

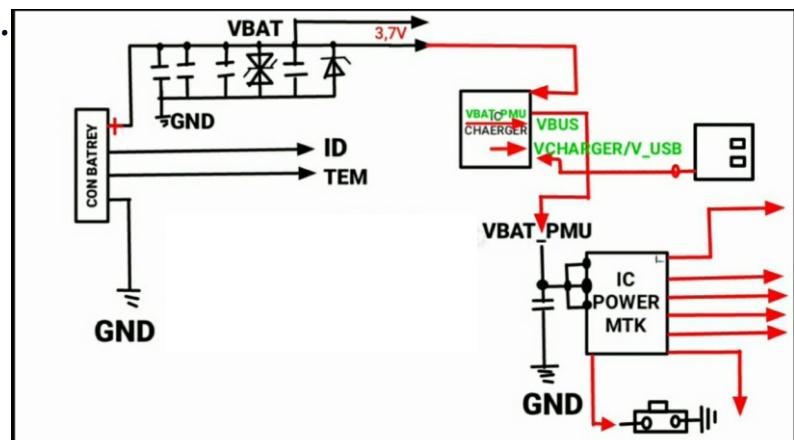
funções em um IC, uma série de melhorias no design geral podem ser feitas, como melhor eficiência de conversão, tamanho de solução menor e melhor dissipação de calor.

Um PMIC pode incluir gerenciamento de bateria, regulação de tensão e funções de carregamento. Pode incluir um conversor DC para DC para permitir a escala de tensão dinâmica. Alguns modelos são conhecidos por apresentarem eficiência de conversão de energia de até 95%. Alguns modelos se integram com escala de frequência dinâmica em uma combinação conhecida como DVFS (voltagem dinâmica e escala de frequência).

Pode ser fabricado usando o processo BiCMOS. Eles podem vir como um pacote QFN. Alguns modelos apresentam interface de comunicação de barramento serial I²C ou SPI para E/S.

Alguns modelos apresentam um regulador de baixa queda (LDO) e um relógio em tempo real (RTC) cooperando com uma bateria de reserva.

Um PMIC pode usar modulação por frequência de pulso (PFM) e modulação por largura de pulso (PWM). Ele pode usar um amplificador de comutação (amplificador eletrônico Classe-D).



CAPÍTULO I

PROCESSADOR

O processador é basicamente o cérebro do nosso dispositivo. Ele é responsável por executar todas as ordens ou instruções que dá para os outros circuitos distribuídos em todo o SoC. Ele pode realizar tarefas aritméticas, como adicionar, subtrair, dividir ou multiplicar, bem como instruções lógicas, como adicionar, remover e colocar, usando portas lógicas e flip-flops (discutido anteriormente). Existem diferentes tipos de processadores, os mais comuns recentemente são: Qualcomm, Exynos, MediaTek, Broadcom, Spreadtrum, HiSilicon. Cada um deles lida com um chipset, por exemplo, na Qualcomm podemos encontrar o chipset "MSM8909" ou "MSM8953", "MSM8974" etc. Quando nos referimos a MSM (Mobile Station Modem), nós queremos dizer que dentro do circuito físico de nosso processador, nossa BaseBand também se encontra, portanto, não vamos encontrar nenhum circuito extra com esta função.



CAPÍTULO I

Memória volátil

Quando nos referimos à memória volátil, estamos nos referindo ao Memória RAM do nosso dispositivo. Como em um computador, encontramos diferentes tipos de RAM, mais um novo que o outro, bem como DDR3 e DDR4, em nossos dispositivos encontramos nossa memória RAM identificada como Low-Power Taxa de dados dupla (LPDDR). Desta forma, podemos encontrar LPDDR1, LPDDR2, LPDDR3, LPDDR4 e os mais recentes LPDDR5. Sendo o mais novo, obviamente mais atualizado e com muitas novas melhorias. No caso do nosso trabalho, não precisamos saber muito sobre ele, pois, as que usaremos, eles só se concentram na memória não volátil

Memória não volátil

Quando nos referimos à memória não volátil, obviamente estamos nos referindo a para a memória de armazenamento interno do nosso dispositivo, o memória onde nosso sistema operacional e os dados do usuário, entre outras coisas. Na evolução normal do sistema de armazenamento interno dos dispositivos móveis, o que se busca é reduzir o consumo de energia e aumentar a velocidade de transferência de arquivos, além de acelerar a leitura e a gravação, por isso, os fabricantes estão constantemente criando novos protocolos de memória. Atualmente, encontramos três tipos de memória; eMMC, eMCP e UFS. Mas antes deles, houve outros, o primeiro foi o ROM (Read Only Memory), que é traduzido como Read Only Memory, uma vez que não pôde ser modificado, armazenou as informações permanentemente sem a necessidade de energia, ao contrário do

CAPÍTULO I

energia, ao contrário do RAM, portanto, tornou-se uma memória ideal para armazenar dados, no entanto, não são mais usados hoje, apesar disso, Continuamos a nos referir à memória ou sistema operacional como ROM como tal, sendo que isso é incorreto.

Depois disso, a memória PROM (leitura programável Apenas memória), ao contrário da ROM, não está programada no Caso contrário, é programado pelo usuário apenas uma vez e em um permanente.

A próxima memória foi a EPROM (Erasable Programmable Read Only Memory), a característica desta memória é que você pode apagar e escrever novamente, por meio de um processo um tanto tedioso, mas funcional. A luz ultravioleta foi usada para apagar as informações.

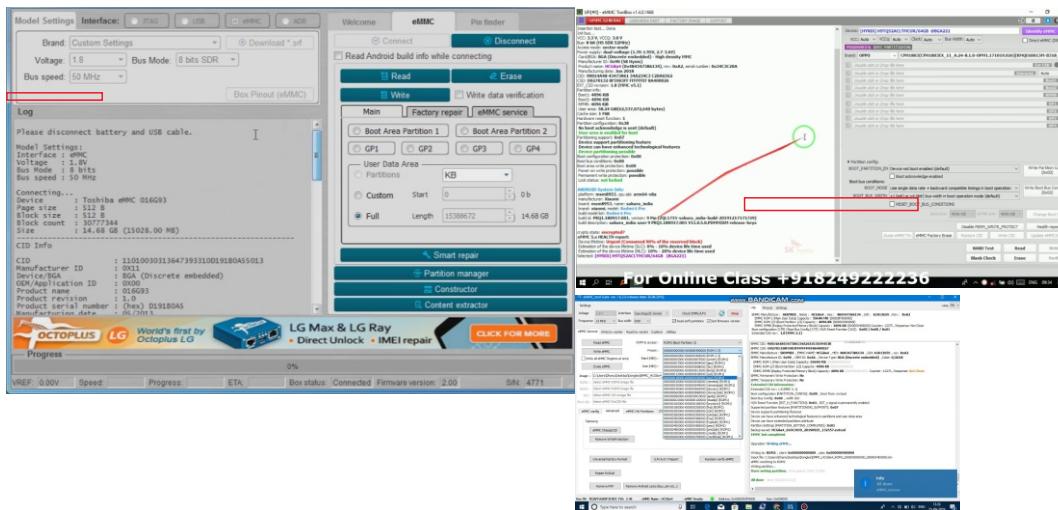
O protocolo que se seguiu foi o EEPROM (Electrical Erasable Memória somente leitura programável), que pode ser programada, apagados e reprogramados eletricamente e não por raios ultravioleta como seus predecessores, EPROMs.

Depois vieram as memórias FLASH, que revolucionaram o sistema de armazenamento de dispositivos eletrônicos. Especialmente no campo em que nos concentrarmos; celular. A vantagem e a diferença deste tipo de memória é que pode armazenar mais dados do que as anteriores. Possui características semelhantes, pois foi fruto de sua evolução, é claro Está. Ele usa duas variantes, o NOR e o NAND, isso baseado nas portas lógicas que usa, a combinação de algumas delas ou flipflops. A memória NOR é composta pelas portas lógicas NOT-OR e a memória NAND, pelas portas lógicas NOTAND. As primeiras, memórias flash NOR, eram muito populares, sem No entanto, eles tinham pouco espaço de armazenamento e expandem isso é

CAPÍTULO I

pouco espaço de armazenamento e expandem isso é o espaço era muito caro e não lucrativo, pelo que se acha uma nova tecnologia, que foi chamada de NAND.

Uma das principais diferenças entre as memórias NOR e NAND, é que no NOR, você pode acessar um byte ou bit específico, fazer a tarefa de programar ou deletar muito eficiente, pois se houvesse um erro em um setor ou célula de memória, era fácil encontrar porque você estava indo direto para o problema, mas também representava perda de tempo e dinheiro, pois quando surgiram sistemas operacionais muito maiores, essa tarefa tornou-se gigantesca. Por outro lado, as memórias NAND não acessam bytes, se não, um grupo destes, chamado de “bloco” (512 bytes, que é o menor grupo de unidade de dados que pode ser acessada por um sistema operacional em um Memória NAND de forma física, visto que, de forma virtual, um sistema operacional pode acessar a menor unidade de dados denominada “página” (4 bytes).



Este tipo de memória é composto por vários tipos de células, das quais que existem:

-SLC (Célula de Nível Único)

CAPÍTULO I

-MLC (*célula multinível*)

-TLC (*célula de nível triplo*)

-QLC (*célula de nível quádruplo*)

Que, como o nome indica, se refere ao número de bits que você pode armazenar em cada uma de suas células. Os SLCs armazemam 1 bit, MLC 2 bits, TLC 3 bits e QLC 4 bits.

As memórias NAND são divididas em dois grupos ou famílias; RAW NAND e MANAGED.

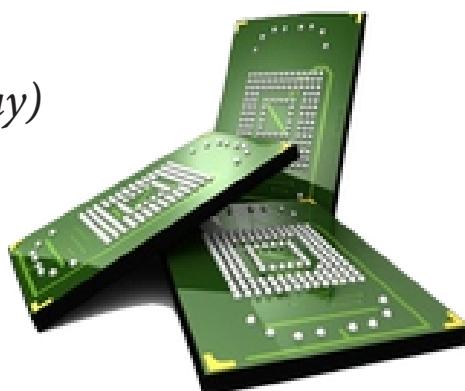
Em RAW NAND, é necessário um controlador externo à memória, ou seja, ao circuito, para poder gerenciar o setor de NAND. Para o qual é necessário pontos de conexão mais altos e maior desgaste do processador, pois, era este o encarregado de toda aquela administração.

Por outro lado, o MANAGED NAND, já contém um controlador dentro do mesmo circuito onde a área NAND está localizada, para o que reduz os pontos de conexão ou comunicação com o processador e remove responsabilidades dele.

É aqui que encontramos as duas memórias principais que veremos na primeira fase deste livro: eMMC e eMCP.

Circuitos BGA (Ball Grid Array)

Este tipo de circuito é composto de bolas de solda em sua superfície, que será soldada na placa em cada passagem configuração. É um encapsulamento comum em dispositivos que usam componentes SMD, exatamente como telefones.



CAPÍTULO I

Componentes SMD

Em dispositivos móveis é muito comum a utilização de componentes SMD (Surface Mounting Device) (por razões de espaço), ou seja, componentes que são soldados na superfície da placa, já que tradicionalmente os componentes passavam pelo cartão para poder ser soldados, como nas velhas televisões ou outros equipamentos eletrônico usaremos basicamente capacitores e resistores, que são o que veremos no dia a dia de nosso trabalho.

O importante é saber como são medidos. Por exemplo, no caso de capacitores, são medidos em farads. São os que encontraremos em maior quantidade em uma placa lógica, pois são os encarregados de filtrar o ruído gerado pelos bucks e LDOs do pmic, gerenciar os picos de tensão que ocorrem enviando-os para o aterramento e proteger a linha ou circuito de que são responsáveis. É um encapsulamento comum em dispositivos que usam componentes SMD, exatamente como telefones.



Isto é o que um capacitor ou capacitores SMD

O outro componente que usaremos constantemente é a resistência, esta é responsável por se opor ao fluxo de elétrons, por isso é eles chamam de resistores. Eles são medidos em ohms. Encontraremos estes em as linhas CMD e CLK.



SOFTWARE

Significado de Android

O que é Android:

Android é o nome do sistema operacional baseado em Linux que opera em celulares (smartphones), netbooks e tablets. É desenvolvido pela Open Handset Alliance, uma aliança entre várias empresas, dentre elas a Google.

O funcionamento do Android é idêntico a outros sistemas operacionais (como Windows, Mac OS, Ubuntu, entre outros), cuja função é gerenciar todos os processos dos aplicativos e do hardware de um computador para que funcionem perfeitamente.

BREVE INTRODUÇÃO

O conteúdo das partições do Android pode ser parcial ou completamente modificado com o flash de uma imagem (sistema de arquivos .img ou binário executável ou um zip flash) para eles. Mas nunca precisamos modificar a maioria deles e qualquer que seja o fabricante que escreveu neles, permanecerá lá sem modificações (somente leitura) por toda a vida útil do dispositivo. Um usuário usa apenas uma partição / dados para salvar dados pessoais como fotos, música, etc. Todos os outros são para o dispositivo funcionar. Normalmente existem cerca de 50 partições em um dispositivo Android, mas apenas algumas partições são modificadas com o objetivo de adicionar novos recursos ou atualizar o dispositivo. Uma ROM personalizada ou atualização secundária também está limitada a modificar partições / boot, / system e / data normalmente. A maioria das partições está quase intacta, contendo bootloaders, firmwares, configurações etc. Aqui está um detalhe "resumido" dessas partições que são importantes para um usuário comum, mas

CAPÍTULO I

interessado.

Na maioria dos dispositivos / sistema e / dados são partições maiores (em alguns dispositivos / personalizados ou uma partição semelhante também) cobrindo quase 90% do eMMC. Todos os outros são menores, com alguns KB ou MB.

PARTIÇÕES RELACIONADAS COM SoC / CHIPSET / PROCESSORS

SoC é o primeiro componente quando iniciamos um PC ou telefone móvel que inicializa hardware e processadores e carrega bootloaders na memória para inicializar o SO. É um chip integrado contendo várias coisas, por exemplo, CPU, GPU, modem, wi-fi etc. Varia de acordo com os fabricantes de dispositivos e fornecedores de SoC (chipset mais processador).

Algumas partições são específicas para SoC, a maioria delas são blobs binários executáveis de código fechado (como aboot, sbl, rpm, tz, cmnlib, devcfg, keymaster, lksecapp e outros em um dispositivo Qualcomm), carregados passo a passo por bootloaders.

MODEM ou RADIO - o rádio do telefone

Também chamado de banda base, ele é responsável por sinais e em dispositivos mais antigos pode controlar wi-fi, bluetooth e GPS (na maioria dos dispositivos mais novos, eles são controlados pelo kernel e ROM). As atualizações dependem do país e podem melhorar ou diminuir o desempenho da bateria, a intensidade do sinal da rede e a capacidade de roaming. Às vezes, também é necessário ter uma versão mínima de banda base para usar uma ROM para que o RIL funcione bem com a banda base.

CAPÍTULO I

O firmware do modem é um mini-sistema operacional para o chip de rádio celular que possui seu próprio processador. Firmware é um termo geral, o firmware existe para muitas coisas no telefone. O chip sem fio para WiFi, GPS e Bluetooth geralmente tem um firmware, assim como o núcleo da GPU, entre outras coisas. Esses arquivos de firmware geralmente estão localizados dentro da partição do SISTEMA ou do VENDOR. O firmware do modem é especial porque tem seu próprio processador de banda base (BP) separado, de modo que o firmware é deixado de fora da imagem do sistema em sua própria partição. O modem não é uma partição específica do Android. Ele está vinculado ao hardware do telefone, mas o kernel possui um código que permite ao Android interagir com o hardware. Mas o processador de banda base (BP) - que opera o modem e é responsável por toda a comunicação por meio de redes móveis, por exemplo, chamada, SMS e internet - é totalmente isolado do Processador de Aplicativo (aquele que chamamos de CPU) e não é governado pelo kernel Android; ele roda um RTOS independente.

Para conhecer mais sobre as partições da memoria flash adquira o nosso curso na plataforma www.mobileemmc.com.br

MDM

Gerenciamento de Dispositivos Móveis: Este tipo de bloqueio é o que está muito na moda, pelo menos no ano de 2019, já que é um bloqueio de negócios que impede o usuário de acessar o modo de recuperação ou modo de download, portanto, você não pode redefini-lo ou flash, e você não pode acessar o menu do dispositivo ou algumas funções dele. Este tipo de bloqueio também pode ser removido diretamente memória, por conexão isp ou, removendo a memória docartão

O que significa MDM (Mobile Device Management)

Mobile Device Management significa Gestão de Dispositivos Móveis. Ou seja, é a tarefa de não somente ter um inventário de quantos e quais celulares, smartphones e tablets uma empresa possui, mas também catalogar informações (modelos de aparelhos, utilizados em quais áreas, por quais colaboradores, entre outras) e configurar esses celulares/tablets de forma correta.

Já muito popular em países como os Estados Unidos, o MDM ainda é pode ser considerado algo recente no Brasil em alguns segmentos, assim como a própria mobilidade corporativa – recentemente impulsionada pela prática do BYOD (Bring Your Own Device, ou traga o seu próprio dispositivo). Mas enquanto em outros locais a gestão de aparelhos móveis é focada principalmente na segurança de dados, por aqui definir o que é MDM na prática pode ser mais amplo.

Aqui, esse tipo de solução também agrupa diversas outras funcionalidades. Bloqueio de recursos, personalização da interface (tela inicial), geolocalização e atualização remota de apps são alguns exemplos. Portanto, no Brasil pode-se dizer que uma das grandes funções do MDM, além da segurança e transmissão de dados corporativos, é aumentar a produtividade e, além disso, evitar o uso indevido dos aparelhos.

Sequência de inicialização do Android

Depois de alguma pesquisa, meu conhecimento atual da sequência de inicialização do Android (pelo menos em um dispositivo Qualcomm) é o seguinte:

PBL -> XBL (substitui SBL) -> Aboot -> Kernel

PBL:

Primary Boot Loader (às vezes chamado de bootROM).

Primeiro trecho de código executado após o dispositivo ser ligado (portanto, PBL é a raiz da confiança)

Construído e distribuído no SoC pela própria Qualcomm

Verdadeiramente é ROM (não pode ser atualizado)

Contém uma chave pública que é usada para verificar a integridade de XBL. A chave privada correspondente está em posse da Qualcomm.

Tem acesso a uma chave de autenticação de 256 bits exclusiva do dispositivo que é necessária para gravar na partição RPMB (link)

XBL:

Extendiam Boot Loader

XBL substitui o SBL mais antigo (link)

Solução proprietária da Qualcomm (ou seja, fornecida e assinada pela Qualcomm)

Em alguns casos, pode ser personalizado pelo OEM por um preço (link)

Mora no eMMC (nas partções de hardware booto?)

*Contém uma chave pública que é usada para verificar a integridade do Aboot
Pode ser atualizado*

Como ele reside no eMMC, um usuário com privilégios de root pode modificá-

CAPÍTULO I

Como ele reside no eMMC, um usuário com privilégios de root pode modificá-lo e potencialmente bloquear o dispositivo:

Aboot

Android Boot Loader

Fornecido pelo OEM

Depende assinado (presumo pelo OEM e não pela Qualcomm, o que significa que a chave pública em XBL deve ser a chave pública do OEM?)

Vive no eMMC (na partição de hardware boot0 ou boot1? Ou talvez na partição de hardware de dados do usuário)

Contém uma chave pública que é usada para verificar a integridade do kernel / sistema operacional (também conhecido como ROM) antes de carregá-lo. No entanto, se Aboot estiver "desbloqueado", qualquer ROM pode ser carregada)

Pode ser atualizado no OEM, pode ser parcialmente de código aberto ou fechado (por exemplo, Samsung)

Devo

Como ele reside no eMMC, um usuário com privilégios de root pode modificá-lo e potencialmente bloquear o dispositivo.

CAPÍTULO I

Primary BootLoader

Como mencionamos anteriormente, isso está dentro processador, especificamente dentro de uma área chamada bootrom, NÃO PODE ser danificado por software, apenas hardware. Em que casos? Pode ser devido a um golpe, devido à umidade ... bem, por qualquer motivo no hardware. Este PBL é responsável por gerar o Porta EDL em smartphone Qualcomm.

Secondary BootLoader)

Esta boot, como mencionamos, está alojada em nossa memória interna, seja eMMC ou eMCP, algumas marcas a salvam no RAM, isso está no nível do software, portanto, pode ser danificado por alguma má manipulação do software do smartphone, seja que você tente fazer o downgrade para um dispositivo com memória anti-rollback, se você carregar uma partição do sistema operacional que danificar o dispositivo ou por muitos outros motivos. No caso dos dispositivos Samsung, encontramos o bootloader secundário com o nome de Sboot, onde, dentro dele, encontramos o boot 1 e 2. No caso do MTK, vamos encontrá-lo com o nome de "preloader» e nas demaisarcas, simplesmente como "boot".

Dependendo da marca do dispositivo

CAPÍTULO I

TABELA DE PARTIÇÃO

A memória interna do telefone (eMMC ou UFS; não o cartão SD) é uma memória de estado sólido (flash), também conhecida como NAND. Raw NAND, como é chamado, é basicamente uma memória flash pura dependente da CPU para controlá-la. Mas, para usar a memória flash como um disco rígido tradicional (dispositivo de bloco), o NAND é equipado com um microcontrolador (multimídia integrado). É chamado eMMC.

O eMMC pode ser particionado como um disco rígido no PC. Os PCs são tradicionalmente particionados com o esquema Master Boot Record (MBR) compatível com BIOS, no qual o primeiro setor do disco contém os detalhes das partições chamadas Tabela de Partição. O tamanho limitado do setor de inicialização (512 bytes) coloca uma limitação de no máximo 4 partições (primárias) listadas no MBR. A partição estendida foi usada para mais de 4 partições.

A tabela de partição GUID (GPT) foi introduzida com o sistema de inicialização UEFI que não depende do primeiro setor de inicialização e, portanto, pode conter até 128 partições. O GPT também faz a verificação CRC, tem GPT de backup, identifica as partições por GUID e as partições têm um rótulo.

Dispositivos Android usam GPT. Podemos visualizar e manipular GPT usando ferramentas Linux, como `parted` e `gdisk`, enquanto `fdisk` é a ferramenta tradicional para partições MBR.

Para visualizar a tabela de partição na memória interna:
fácil de identificá-los pelo nome. No entanto, no
a maioria dos dispositivos, encontramos uma combinação de ambos.

CAPÍTULO I

No entanto, no a maioria dos dispositivos, encontramos uma combinação de ambos para o bom funcionamento do mesmo.

No caso dos equipamentos mais recentes da Huawei, com processadores Kirin, eles não usam GPT ou MBR, senão usam EFI, um sistema além dos mencionados acima.

CAPÍTULO I

O que é EDL?

Os fabricantes de celulares SoC (System on Chip) geralmente fornecem modos especiais projetados para depuração, diagnóstico ou recuperação. Nesse caso, os dispositivos baseados na Qualcomm têm um modo EDL (modo de download de emergência). Nesta interface de teste integrada, é possível obter acesso às funções de leitura e gravação de memória de baixo nível. Esse acesso se aplica tanto à ROM quanto à RAM.

A conexão do dispositivo a um conector USB é suficiente para iniciar a extração?

Para colocar um dispositivo no modo EDL, não existe uma abordagem única; geralmente está em todo lugar. Com várias maneiras de alternar o dispositivo para o modo de download de emergência (EDL), o investigador geralmente é relegado a digitalizar as páginas da Internet devido aos vários métodos, geralmente diferentes para cada dispositivo. Existem abordagens de software e de hardware.

Abordagens de software:

ADB (Android Debug Bridge). Se o dispositivo estiver desbloqueado e o modo adb estiver ativado, você poderá emitir o comando “adb reboot edl” em uma linha de comando.

Mude o dispositivo para o modo de inicialização rápida, mantendo Power e Vol- ao mesmo tempo (a combinação de teclas pode ser diferente para cada dispositivo) e execute o comando “fastboot oem edl”.

CAPÍTULO I



Método de combinação de teclas (a combinação depende do modelo do dispositivo). Você precisa desligar o dispositivo, conectar o cabo USB ao PC, mas não o dispositivo. Pressione e segure Vol- e Vol + ao mesmo tempo e, enquanto os segura, conecte a outra extremidade do cabo USB ao dispositivo. Mantenha as teclas pressionadas por 3-5 segundos, o dispositivo deve entrar no modo EDL. Além disso, manter pressionado o botão “#” e conectar o dispositivo via USB é suficiente para mudar muitos telefones de botão Qualcomm para o modo EDL. Este método funciona em muitos dispositivos KaiOS Qualcomm, incluindo o Jio Phone 1.

Abordagens de hardware:

Cabo EDL. Cabos especializados podem ser usados para mudar o dispositivo para o modo EDL. Esses cabos estão disponíveis on-line ou, se você tiver um kit de cabos forenses do Oxygen, eles serão incluídos.

Curto-circuito dos pinos. Esse método, também conhecido como “curto-circuito”, requer experiência técnica e, geralmente, desmontagem do telefone. Para alternar o telefone para EDL, pinças metálicas para reparo de telefones celulares ou um pedaço de fio são frequentemente usadas para fazer curto/conectar os pontos de teste. Isso não é recomendado, a menos que o investigador tenha experiência em montagem/desmontagem de componentes elétricos.

É possível encontrar conselhos sobre como reduzir os pontos de teste na Internet. Para fazer isso, digite o seguinte no campo de pesquisa:

<nome do dispositivo>, pontos de teste, ponto de teste, 9008, EDL.

Capítulo 2



eMMC/eMCP

→ Capítulo 1 Conhecimento Gerais

→ Capítulo 2 eMMC / eMCP

→ Capítulo 3 UFS



CAPÍTULO 2

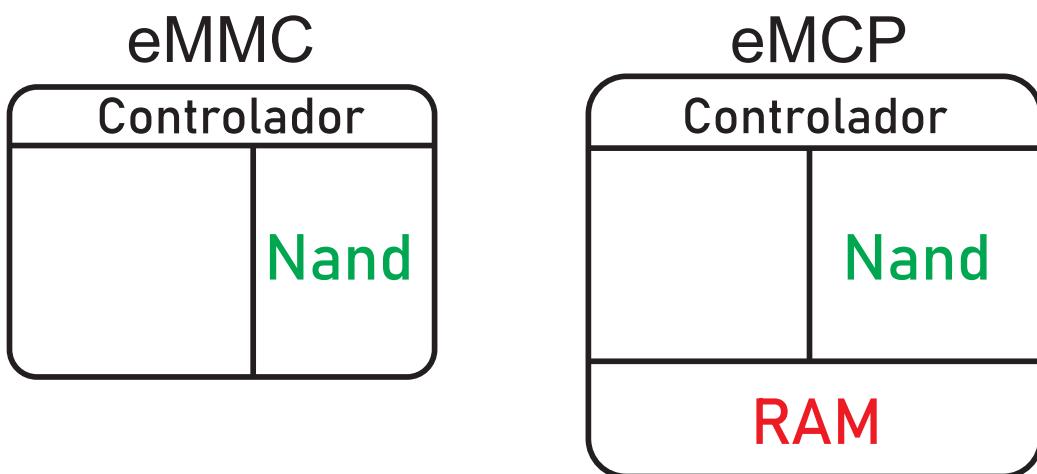
Um MultiMediaCard (eMMC) incorporado é um pequeno dispositivo de armazenamento feito de memória flash NAND e um controlador de armazenamento simples . O padrão eMMC para aplicativos de memória flash embutidos foi desenvolvido em 2006 pela JEDEC e a MultiMediaCard Association.

A tecnologia é destinada ao uso em dispositivos portáteis, como telefones celulares e, mais recentemente, em sensores conectados à Internet das Coisas (IoT). A memória flash e o controlador estão contidos em um único circuito integrado (IC) que é incorporado permanentemente em um dispositivo.

Um eMMC atua como o armazenamento primário para dispositivos portáteis como telefones celulares ou tablets , o que pode aumentar esse armazenamento com um cartão Secure Digital removível ou cartão multimídia microSD. É o único armazenamento para sensores muito pequenos conectados à IoT. A conexão com a placa principal do dispositivo é paralela, mas a especificação eMMC mais recente (versão 5.1) permite uma taxa de transferência de até 400 megabytes por segundo (MBps), que é comparável a uma unidade de estado sólido usando uma conexão SATA .

CAPÍTULO 2

Aqui vemos nesta imagem a diferença entre um e outro.

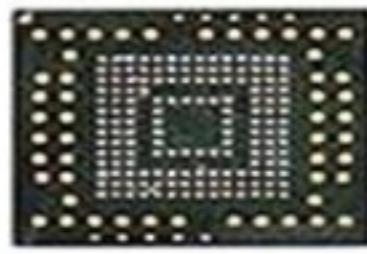
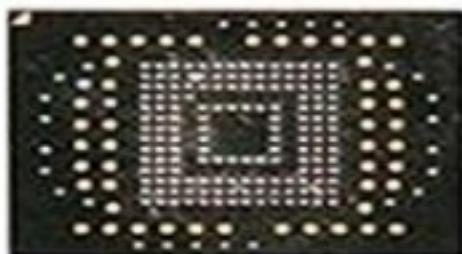


Cada memória, independentemente de ser eMMC ou eMCP, como mencionamos, ele é encapsulado em um circuito do tipo BGA, os mais conhecidos são;

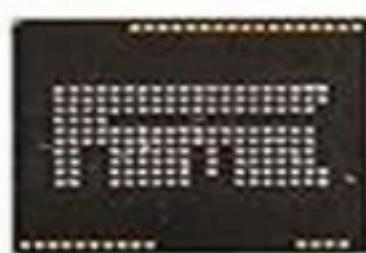
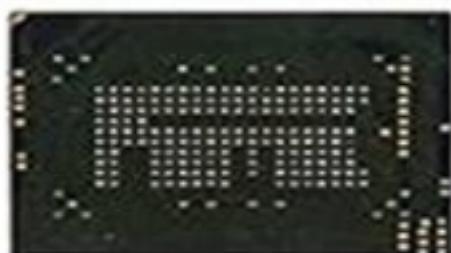
-BGA221 -BGA153 / 169 -BGA186 / 162 -BGA254

CAPÍTULO 2

BGA-153/169



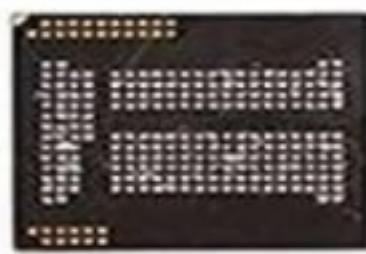
BGA-162 /186



BGA-529



BGA-221



1. BGA 153 (used as eMMC and eMCP products)

2. BGA 169 (used as eMMC and eMCP products)

3. BGA 162 (used as eMCP and UFS products)

4. BGA 186 (used as eMCP and UFS products)

5. BGA 221 (used as eMCP and UFS products)

6. BGA 529 (used as eMCP and UFS products)

7. BGA 254 (used as eMCP and UFS products)

CAPÍTULO 2

RAM O que?

Isso é usado no circuito de telefones celulares para armazenar dados de memória. É feito de milhões de transistores e capacitores que são embalados em circuito integrado (IC)

Transistores e capacitores são emparelhados para criar uma célula de memória, que representa um único bit de dados.

O capacitor mantém os dados de bit de informação, um 0 ou um 1.

O transistor atua como uma chave que permite que o circuito de controle no chip de memória leia o capacitor ou mude seu estado

Tipos de celula RAM

Memória dinâmica de acesso aleatório (DRAM)

Na maioria dos casos, a forma comum de memória de telefones celulares é uma memória dinâmica de acesso aleatório (DRAM)

Isso é usado para armazenar temporariamente informações em telefones celulares

Serial Dynamic Random access memory (SAM)

O oposto de RAM é a memória serial dinâmica de acesso aleatório (SAM). SAM armazena dados

SDRAM

SDRAM significa Synchronous Dynamic Random Access Memory. DDR é a abreviação de "DDR SDRAM" e significa Double Data Rate DDR RAM (ou memória de acesso aleatório de dupla taxa de dados) Isso faz o mesmo, mas o faz duas vezes a cada contagem de relógio. Isso torna DDR RAM duas vezes mais rápido que SDRAM.

“In-System Programming” aplicada à ciência forense, é a prática de se conectar a um eMMC ou chip de memória flash eMCP com a finalidade de baixar o conteúdo completo da memória de um dispositivo. A memória eMMC e eMCP são o padrão nos smartphones de hoje, e a prática do ISP permite que os examinadores recuperem diretamente os dados completos sem remover o chip e destruir o dispositivo. O ISP beneficia o examinador que enfrenta os desafios de orçamentos apertados, mas deseja expandir sua experiência na recuperação de evidências de smartphones bloqueados. Uma técnica econômica, o ISP fornece aos examinadores os mesmos resultados de um chip-off a um preço mais baixo. E, assim como com JTAG e Chip-Off, sua agência ainda pode usar sua linha atual de software de análise forense para recuperar a prova definitiva. Não há necessidade de adquirir software de análise adicional.

Por que precisamos do ISP?

ISP Permite que os examinadores contornem os códigos de bloqueio e recuperem uma coleção completa de dados de telefones não suportados por JTAG ou ferramentas comerciais.

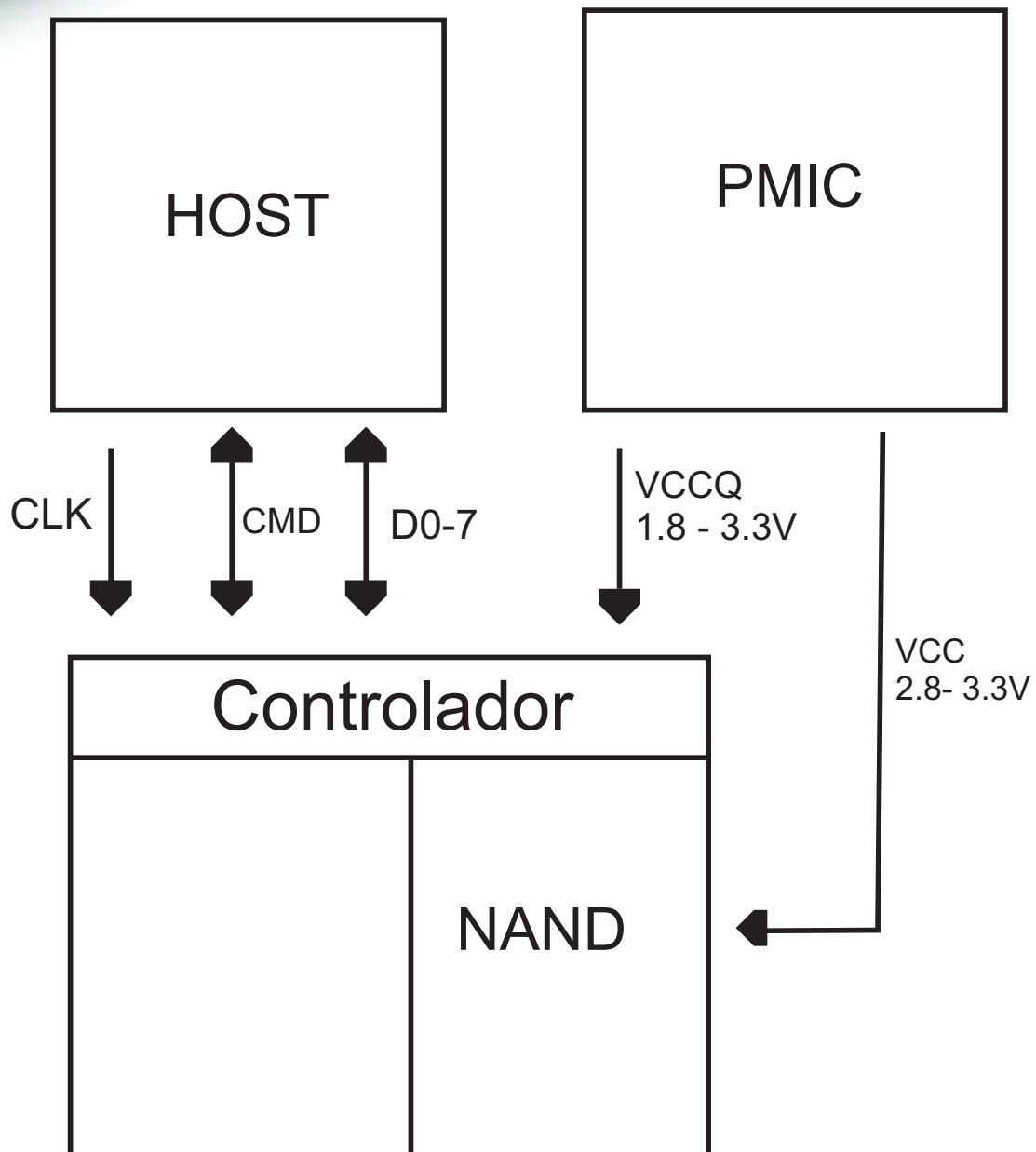
ISP Permite que os examinadores contornem os códigos de bloqueio e recuperem uma coleção completa de dados de telefones não suportados por JTAG ou ferramentas comerciais.

É uma prática não destrutiva que alcança os mesmos resultados que um chip-off, enquanto deixa a evidência original intacta.

Adquire dados muito mais rápido do que JTAG, permitindo que os examinadores processem mais telefones com mais rapidez.

Menos recursos e ferramentas são necessários para realizar um download do ISP em comparação com Chip-Off.

CAPÍTULO 2



Conexão com ISP

1.VCC (Voltage Common Collector)

1. VCC é a entrada de energia de um dispositivo
2. Pode ser positivo ou negativo em relação ao GND.
3. VCC na maioria dos dispositivos, este pino está vinculado ao VCC do dispositivo
4. Pode ser usado para alimentar um chip IC buffer
5. provavelmente será 3.3v e 2.8v.
6. 2,8 ... 3,3 V que são valores mínimos e máximos
7. Poder da memória NAND dentro do eMMC
8. Interface de E / S NAND e fonte de alimentação NAND Flash.

Para conhecer melhor sobre ISP e Chip-Off, e tudo sobre memoria flash nand, etc..

Mobile Emmc tem maior parte em conhecimento em ferramenta emmc e ufs do mercado como UFI BOX, EASY JTAG PLUS, MEDUSA PRO, MEDUSA PRO 2, MIRACLE NINJA E OUTRA.

Conhecer cada partição e cada painel de ferramenta, facilita cada trabalho e sabe qual box é a melhor para se trabalha elimina gastos desnecessário.

eMMC REGISTERS

- Card Identification (CID) register
- Operations Conditions Register (OCR)
- Card-Specific Data (CSD) register
- Extended Card-Specific Data (Ext_CSD) register

Como você deve saber, o chip eMMC tem registros diferentes - Registro CID, Registro CSD, Registro CSD estendido. A maioria dos bits nesses registros são somente leitura e apenas alguns deles podem ser alterados. O registro de identificação de cartão (CID) tem 128 bits de largura. Ele contém as informações de identificação do dispositivo (ID do fabricante, nome do produto, revisão do produto, número de série do produto, data de fabricação e alguns outros) usadas durante a fase de identificação do dispositivo (protocolo eMMC).

Os chips Samsung eMMC permitem a alteração dos dados CID. Os chips eMMC de outros fornecedores não permitem (ou o método é desconhecido) alterar o CID.

Quando precisamos mudar o cid?

Você pode precisar alterar o CID se quiser alterar ou reparar alguns dados nele, por exemplo, se o dispositivo (eMMC) danificou o nome do produto e deve ser corrigido. Ou frequentemente, quando você deseja alterar o chip eMMC no dispositivo para outro semelhante (Samsung) eMMC, pode ser necessário alterar o CID do novo Samsung eMMC para semelhante, que estava no antigo eMMC.

eMMC REGISTERS

E em todas as cpu precisamos disso?

Isso não depende da CPU do dispositivo, depende do problema.

Registro de Condições de Operações (OCR)

O registro de dados específicos do cartão (CSD) fornece informações sobre como acessar o conteúdo do dispositivo. • O registro CSD define o formato dos dados, o tipo de correção de erros, o tempo máximo de acesso aos dados e a velocidade de transferência de dados, bem como se o registro DS pode ser usado. • A parte programável do registro (entradas marcadas com W ou E na tabela a seguir) pode ser alterada pelo comando PROGRAM_CSD (CMD27).

Registro de dados específicos do cartão (CSD)

Registro de dados específicos do cartão estendido (Ext_CSD)

O registro de dados específicos do cartão estendido (ECSD) de 512 bytes define as propriedades do dispositivo e os modos selecionados.

Os 320 bytes mais significativos são o segmento de propriedades.

Este segmento define os recursos do dispositivo e não pode ser modificado pelo host.

Os 192 bytes inferiores são o segmento de modos.

O segmento de modos define a configuração na qual o dispositivo está funcionando.

O host pode alterar as propriedades dos segmentos de modos usando o comando SWITCH.

CAPÍTULO 2

EMMC CID: 90014A484347386134A261013659453B

EMMC CSD: D02701328F5903FFFFFFEF8A400027

EMMC Manufacture : SKHYNIX , EMMC NAME: HCG8a4 , HEX: 484347386134 , S/N: 61013659 , rev. 0xA2

EMMC Manufacture ID: 0x90 , OEM ID: 0x4A , Device Type: BGA (Discrete embedded) , Date: 4/2018

EMMC ROM 1 (Main User Data) Capacity: 59640 MB (000E8F800000)

EMMC ROM 2/3 (Boot Partition 1/2) Capacity: 4096 KB (000000400000)

EMMC RPMB (Replay Protected Memory Block) Capacity: 4096 KB (000000400000) Counter: 13275 , Response: Not Clean

EMMC Permanent Write Protection: No

CID Info

CID	:	110100303136473933100191B0A55013
Manufacturer ID	:	0X11
Device/BGA	:	BGA (Discrete embedded)
OEM/Application ID	:	0X00
Product name	:	016G93
Product revision	:	1.0
Product serial number	:	(hex) D191B0A5
Manufacturing date	:	05/2013

VCC: 3.3 V, VCCQ: 3.0 V

Bus: 8 bit (HS SDR 52MHz)

Access mode: sector mode

Power supply: dual-voltage (1.70-1.95V, 2.7-3.6V)

Card/BGA: BGA (Discrete embedded) - High density MMC

Manufacturer ID: 0x90 (SK Hynix)

Product name: HCG8a4 (0x484347386134), rev: 0xA2, serial number: 0x34C3C20A

Manufacturing date: Jun 2018

CID: 90014A48 43473861 34A234C3 C20A6562

CSD: D0270132 8F5903FF FFFFFFFF 8A400026

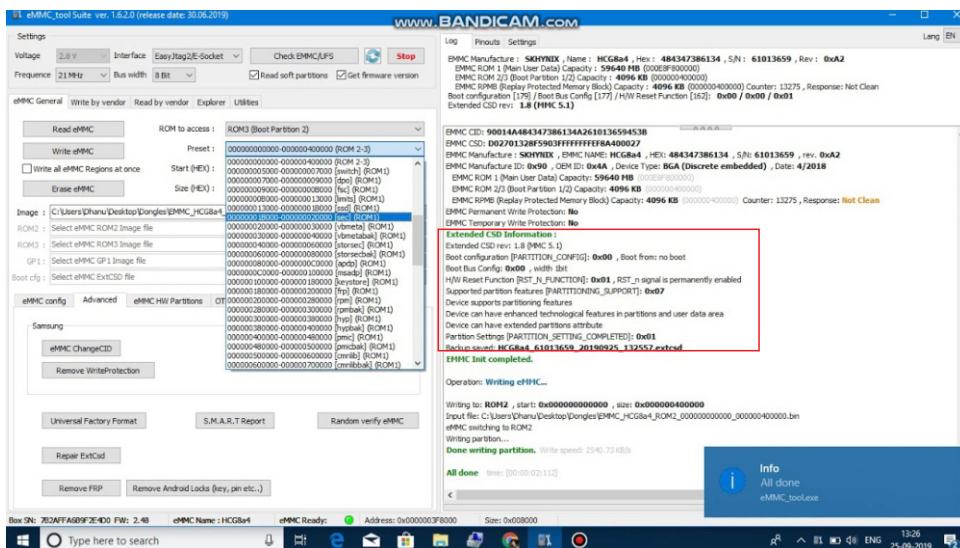
EXT_CSD revision: 1.8 (MMC v5.1)

Partition info:

A cima temos uma ilustrações do cid, csd, ext_csd nas interface das box Easy Jtag, Medusa pro 1 ou 2 ou Octoplus Pro e Ufi Box.

CAPÍTULO 2

EXT_CSD (Extended Card Specific Data)



Tevemos ter muito atenção no ext_csd, porque ele vai toda a informações na memoria flash nand. Caso técnico não tenha conhecimento pode danificar o aparelho, o ‘boot’ e não inicia mais o aparelho.

CAPÍTULO 2

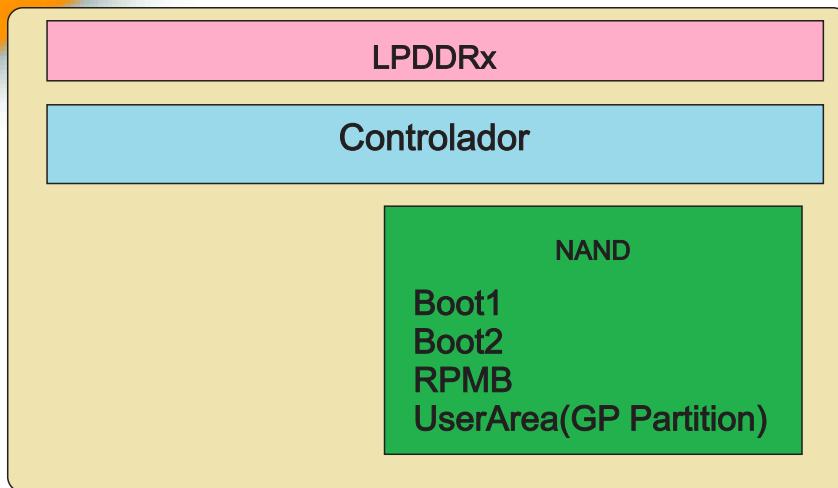
Boot Configuration (Partition Config): Esta parte nos fala de qual partição está inicializando o equipamento ou se não inicializa de nenhuma. Lembre-se de que cada memória pode hospedar o arquivo de inicialização em um partição dos quatro que tem, dependendo de onde inicializa ou se não inicializa de nenhuma partição e com base no envio ou não de confirmação de inicialização, nós irá gerar uma configuração hexadecimal que nos referirá a Qual marca de processador tem nosso aparelho, se essa configuração estiver errada, o equipamento não liga. Aqui a tabela de configuração hexadecimal para cada processador.

CONFIGURAÇÃO DE BOOT

<i>Qualcomm</i>	<i>Configuracion Hexadecimal</i>
<i>UserArea</i>	
<i>No envía ACK</i>	<i>ox00/ox38</i>
<i>MTK/Exynos</i>	
<i>Boot 1</i>	
<i>Si envía ACK</i>	<i>ox48</i>
<i>Hi-Silicon/Broadcomm</i>	
<i>Boot 1</i>	
<i>No envía ACK</i>	<i>ox08</i>

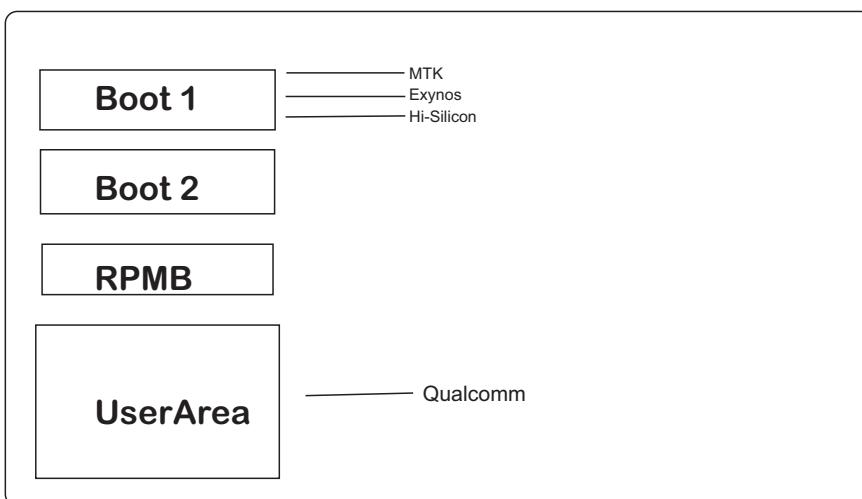
CAPÍTULO 2

eMCP



As partições *Boot 1* e *Boot 2* são destinadas a hospedar dentro eles o bootloader ou o arquivo de boot que faz nosso dispositivo ligar. No entanto, nem todos os fabricantes decidem hospedar seus inicializar, por exemplo, a Qualcomm o hospeda em *UserArea* e não em qualquer estes dois.

MTK por sua vez, como Exynos, Hi-Silicon e Broadcom, se eles usam uma dessas partições para inicializar de lá, eles usam especificamente a partição *Boot 1* para inicializar a partir dela.



CAPÍTULO 2

O tamanho dessas duas partições pode variar de 128 kb a 16 MB, embora geralmente os encontramos em 4096kb, ou seja, 4 MB.

As duas partições devem ser sempre do mesmo tamanho, não você pode variar o tamanho de qualquer um deles independentemente, eles sempre serão os mesmos.

```
EMMC Manufacture : SKHYNIX , Name : HCG8a4 , Hex : 484347386134 , S/N : 61013659 , Rev : 0xA2
EMMC ROM 1 (Main User Data) Capacity : 59640 MB (000E8F800000)
EMMC ROM 2/3 (Boot Partition 1/2) Capacity : 4096 KB (000000400000)
EMMC RPMB (Replay Protected Memory Block) Capacity : 4096 KB (000000400000) Counter: 13275 , Response: Not Clean
Boot configuration [179] / Boot Bus Config [177] / H/W Reset Function [162]: 0x00 / 0x00 / 0x01
Extended CSD rev: 1.8 (MMC 5.1)
```

Como podemos ver na imagem anterior, descobrimos que ambos As partições têm o mesmo tamanho, 4096kb.

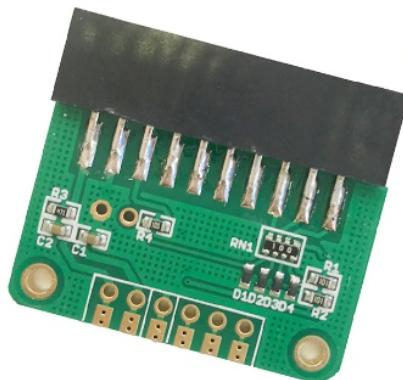
O RPMB, por sua vez, é responsável por hospedar os arquivos de segurança do dispositivo, como configurações de impressão digital, Knox entre outros arquivos de segurança. Esta partição não pode ser modificada porque é criptografada com um Segurança SHA-256 e é necessário ter a chave de criptografia para ser capaz de acessá-lo. Seu tamanho é independente do Boot 1 e 2 e da UserArea, este se podemos modificar (o tamanho), mas não o conteúdo

```
EMMC Manufacture : SKHYNIX , Name : HCG8a4 , Hex : 484347386134 , S/N : 61013659 , Rev : 0xA2
EMMC ROM 1 (Main User Data) Capacity : 59640 MB (000E8F800000)
EMMC ROM 2/3 (Boot Partition 1/2) Capacity : 4096 KB (000000400000)
EMMC RPMB (Replay Protected Memory Block) Capacity : 4096 KB (000000400000) Counter: 13275 , Response: Not Clean
Boot configuration [179] / Boot Bus Config [177] / H/W Reset Function [162]: 0x00 / 0x00 / 0x01
Extended CSD rev: 1.8 (MMC 5.1)
```

Aqui podemos ver que, neste caso, o tamanho RPMB é o mesmo que O Boot 1 e 2, no entanto, não tem necessariamente que ser assim, às vezes podemos encontrá-lo com um tamanho de 512kb ou 16mb. UserArea, por sua vez, é onde o sistema operacional Android está hospedado, neste caso. Seu tamanho depende da capacidade de armazenamento memória física, ou seja, pode ser 1gb, 4gb, 8gb, etc. Está o tamanho não pode ser alterado simplesmente com alguma configuração, uma vez que é físico.

Como mencionamos anteriormente, alguns fabricantes decidem hospedar dentro do userarea sua bota, como no caso da Qualcomm.

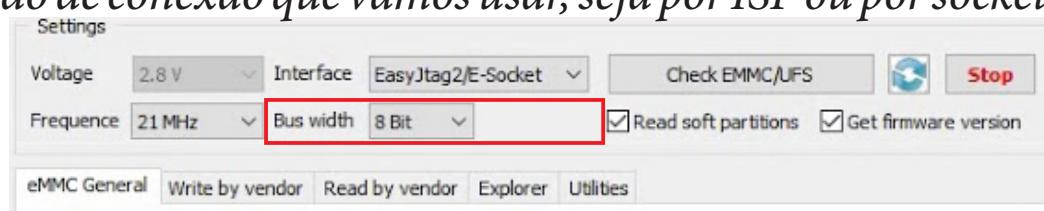
CAPÍTULO 2



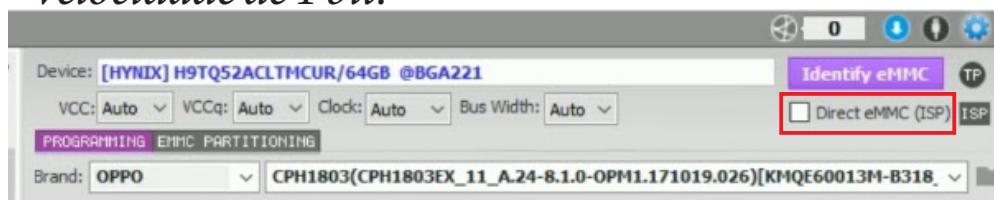
Quando se refere ao ISP não é nada mais do que o que muitos chamam de "jtag", é a ligação de cada um dos pontos com os quais o processador se comunica com a memória, e que sempre encontramos nas pinagens de qualquer caixa.

Como na imagem acima, é o adaptador ISP de UFI box, onde encontramos 2.8v e 1.8v como VCC e VCCQ respectivamente, no entanto, nas pinout, normalmente os encontramos como 1.8 e 2.8.

É importante conhecer a definição de ISP porque em alguns casos, como quando se usa easy jtag ou UFI box, nos obriga a escolher o método de conexão que vamos usar, seja por ISP ou por socket.



Se escolhermos o ISP, em automático deixa-nos a opção de trabalhar apenas com uma linha de dados, que é Dados 0, e com velocidade de 1 bit.



CAPÍTULO 2

Em ambas as imagens anteriores, podemos ver que tanto Easy Jtag como caixa UFI pedimos que você seja específico no tipo de conexão que você vai usar por ISP ou eMMC direto. Ao contrário da Medusa Pro, Medusa não pede essa especificação.



O próximo modo de conexão é direto para a memória ou chip-off, que Nada mais é do que remover a memória do cartão para colocá-la no socket, dependendo do tipo de BGA, ou soldando os cabos ISP direto para o circuito

Na imagem anterior, podemos ver um exemplo de como o circuito eMMC ou eMCP seria conectado através de uma conexão ISP. A vantagem disso é que não precisamos comprar o socket para poder trabalhar a memória, a desvantagem é que trabalharemos devagar, já que a conexão ISP só pode funcionar em 1 bit ou 4 bits, ou seja, com uma única linha de dados ou quatro no máximo, não as oito que temos disponível ao trabalhar no socket.

1 bit (dados 0)

4 bits (dados 0, dados 1, dados 2 e dados 3)

8 bits (Dados 0, Dados 1, Dados 2, Dados 3, Dados 4, Dados 5, Dados 6 e Dados 7)

Por outro lado, no socket podemos trabalhar em uma velocidade diferente já que trabalhamos com todas as linhas de dados.

CAPÍTULO 2

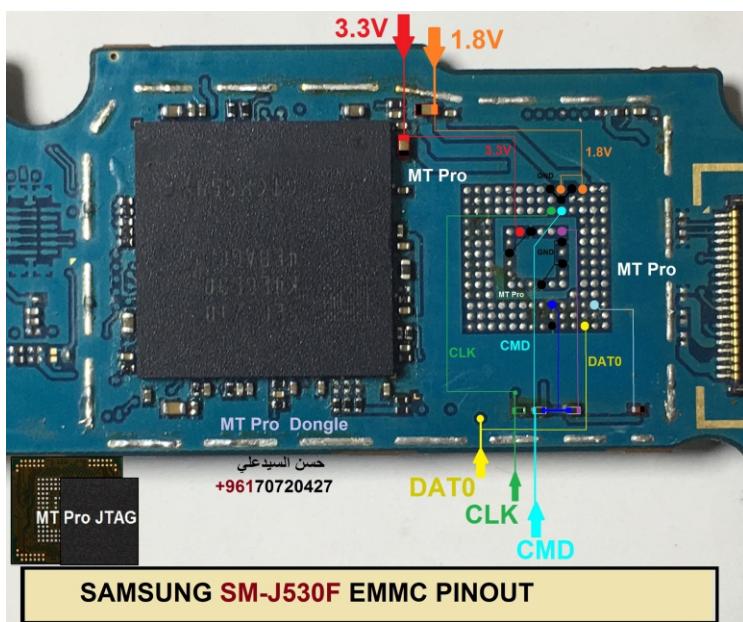
Cada box vem com seu socket regularmente, exceto Medusa Pro (medusa pro 2 ja vem com seu socket para emmc e ufs), que Vem à parte, tem que comprar à parte.

UFS BGA254&eMMC254 2 in 1 Socket
UFS BGA 254&eMMC 254 2 in 1 for Z3x Easy Jtag Plus Box



Agora, para poder funcionar por conexão ISP, precisamos de uma pinout, como já mencionamos, mas; Qual é a pinout?

Tenho certeza de que todos nós vimos pinout em uma box ou na web, que nada mais é do que a imagem onde nos diz onde soldar o cabos no cartão



CAPÍTULO 2

NAND, UFS, eMMC, USB e ISP.

O fato de uma box não ter este ou aquele modelo em seu suporte, ou que a pinagem de uma equipe não apareça no suporte, não significa que não é suportado, simplesmente que os desenvolvedores não dito modelo chegou para poder retirar a pinagem, lembre-se que estes as caixas funcionam com memórias, NÃO com marcas ou modelos de telefone dos mesmos.

CHIP-OFF

Outra forma de trabalha seria Chip-off se vai utilizar adaptadores soket seria remover a memoria flash nand da placa.

Cada técnico chegara na sua temperatua e ar da própria estação e manuseio.

Capítulo 3



UFS

→ Capítulo 1 Conhecimento Gerais

→ Capítulo 2 eMMC / eMCP

→ Capítulo 3 UFS



Universal Flash Storage

Armazenamento Flash Universal (UFS) é uma especificação de armazenamento flash para câmeras digitais , telefones celulares e dispositivos eletrônicos de consumo . Ele foi projetado para trazer maior velocidade de transferência de dados e maior confiabilidade ao armazenamento de memória flash, enquanto reduz a confusão do mercado e remove a necessidade de diferentes adaptadores para diferentes tipos de cartões. [3] O padrão abrange pacotes permanentemente anexados a um dispositivo (eUFS) e cartões de memória UFS removíveis.

Essas memórias, até agora, lançaram apenas três tipos de

BGAs diferentes, estes são:

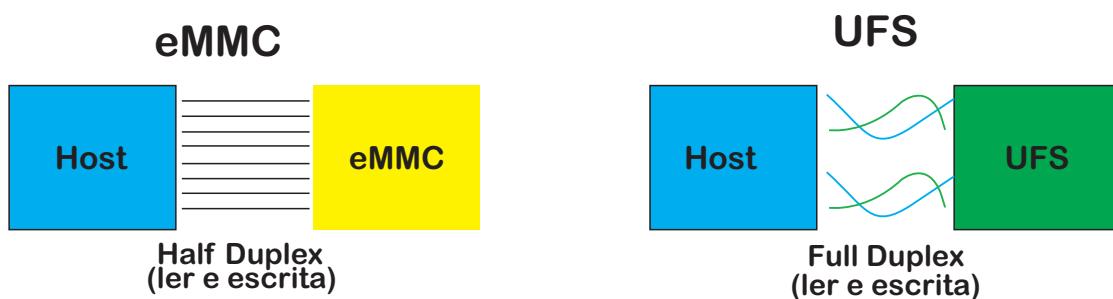
- BGA95
- BGA153
- BGA254

A principal diferença entre uma memória eMMC e um UFS, é que eMMC tem transferência e ISP. vamos ver a seguir:

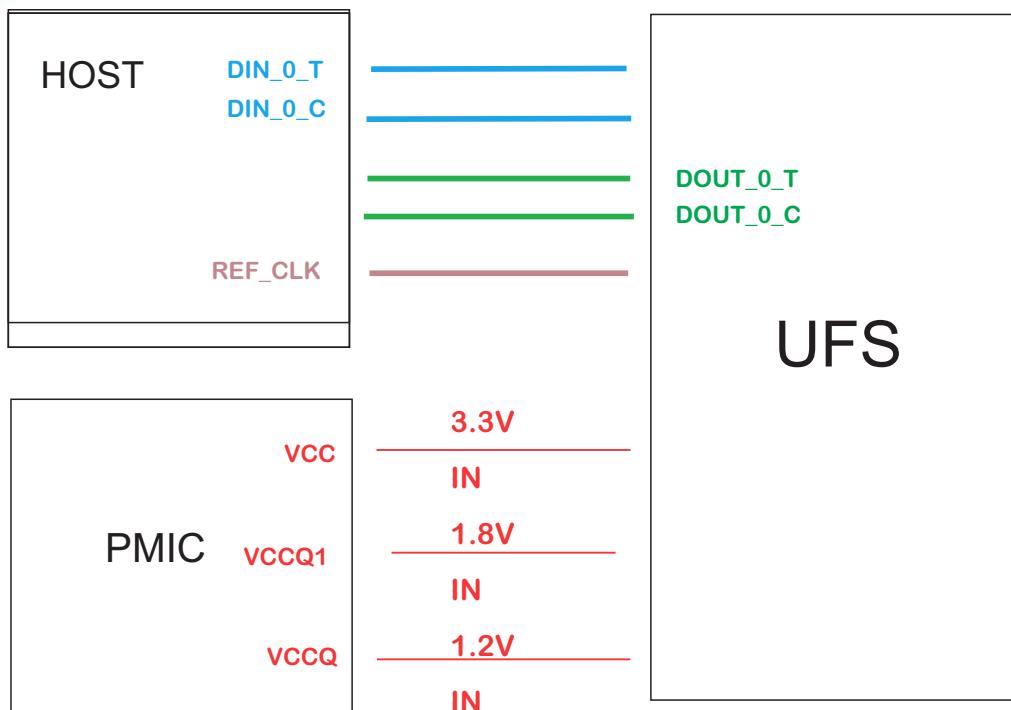
CAPÍTULO 3

O UFS suporta filas de comando, ou seja, o host pode enviar vários comandos de uma vez, e os dispositivos UFS suportam execução paralela e fora de ordem. Quem conclui primeiro retorna ao estado primeiro. Este método de processamento de comando é denominado processamento de comando assíncrono. Seu predecessor, eMMC, não suporta filas de comando. Os comandos são executados um por um, ou um pacote por pacote (cada pacote contém vários comandos). Se o comando anterior não for executado, os comandos subsequentes não podem ser enviados. Este método de processamento de comando é denominado processamento de comando síncrono.

Vamos comparar os métodos de processamento de comando e a eficiência de execução de comando entre "full duplex + processamento de comando assíncrono" e "half duplex + processamento de comando síncrono".



CAPÍTULO 3



Podemos ver que as linhas de dados tratam do sistema de recepção e transmissão, RX e TX, vão aos pares, duas entradas e duas saídas. Também podemos ver as três tensões de alimentação que são fornecidas pelo pmic, essas tensões são inseridas, é claro.

Ao contrário do eMMC, onde o VCC conduz uma tensão entre 2,8 V para 3,3v, no UFS ele lida apenas com a tensão mais alta, ou seja, 3,3v O VCCQ, por sua vez, vai para 1,2v, enquanto o VCCQ2 é o rolamento mais importante de com 1,8v, a mesma tensão que o VCCQ manipula no eMMC

CAPÍTULO 3

Diferença de software, vamos descobrir que UFS gerencia um sistema semelhante ao eMMC, partições, porém, aqui muda algo, não encontramos mais Boot 1 e 2 como tal, RPMB e UserArea, caso contrário, encontramos unidades lógicas.

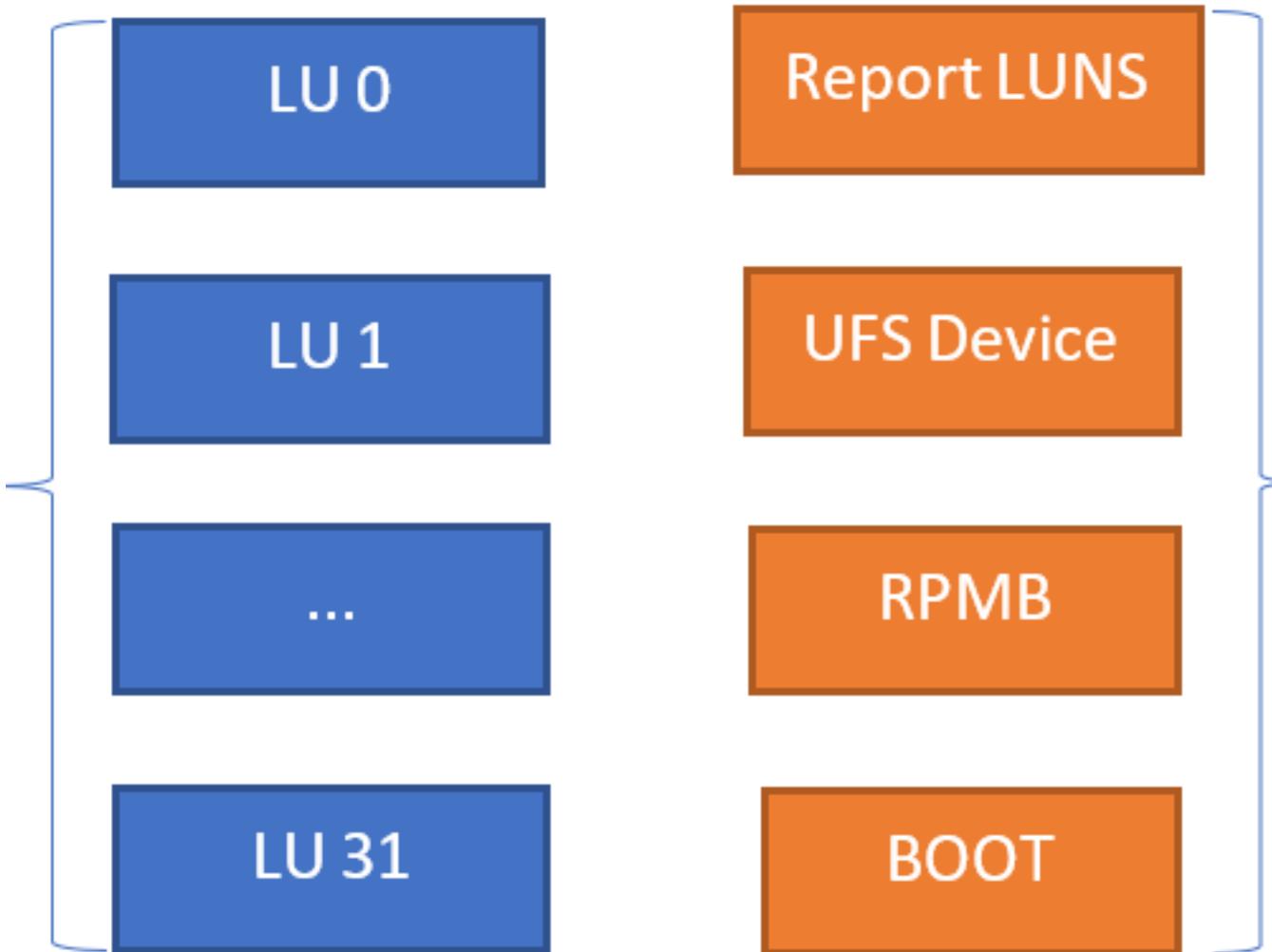
Lembre-se de que no eMMC / CP temos quatro partições principais mas podemos adicionar mais quatro adicionando um total de oito partições. Em UFS é semelhante, cada memória suporta até oito unidades lógicas ou LUNs (Logical Unit Number), estes são listados a partir de Lu0 até Lu7.

No armazenamento do computador, um número de unidade lógica , ou LUN, é um número usado para identificar uma unidade lógica , que é um dispositivo endereçado pelo protocolo SCSI ou por protocolos de rede de área de armazenamento que encapsulam SCSI, como Fibre Channel ou iSCSI. [1]

Um LUN pode ser usado com qualquer dispositivo que ofereça suporte a operações de leitura / gravação, como uma unidade de fita , mas é mais frequentemente usado para se referir a um disco lógico criado em uma SAN . Embora não seja tecnicamente correto, o termo "LUN" é freqüentemente usado para se referir ao próprio disco lógico . [2]

Encontraremos muitas semelhanças com eMMC desde, analisando o log de operações do easy jtag plus, medusa pro 2 e hypobox , que é atualmente as únicas caixas que suporta este protocolo de memória, podemos perceber dos quais, LU0 é equivalente a UserArea. Mas vamos colocar uma imagem para tornar a comparação mais clara.

CAPÍTULO 3

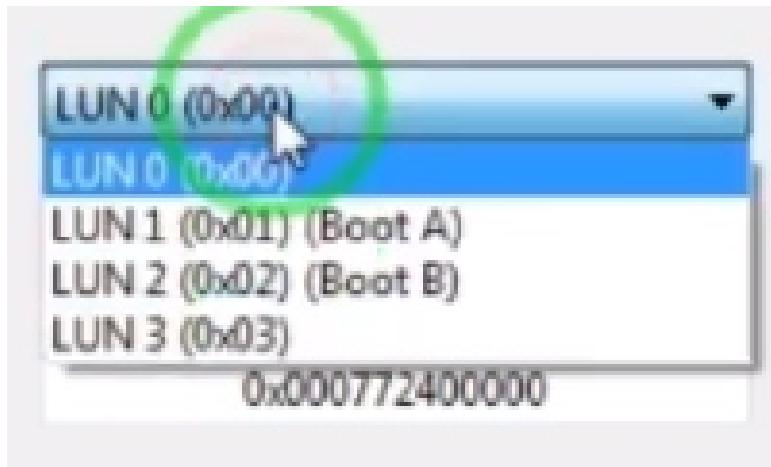


CAPÍTULO 3

Pode ver uma leitura Ufs easy jtag e suas partições . na imagem a baixo

```
----- Detected 19 partitions -----  
LUN0 (BOTA0) [0x400000 0x400000] Size: 4.0MB  
LUN0 (BOTA1) [0x800000 0x400000] Size: 4.0MB  
LUN0 (EFS) [0xc00000 0x1400000] Size: 20.0MB  
LUN0 (PARAM) [0x2000000 0x800000] Size: 8.0MB  
LUN0 (BOOT) [0x2800000 0x2800000] Size: 40.0MB  
LUN0 (RECOVERY) [0x5000000 0x2e00000] Size: 46.0MB  
LUN0 (OTA) [0x7e00000 0x800000] Size: 8.0MB  
LUN0 (RADIO) [0x8600000 0x2a00000] Size: 42.0MB  
LUN0 (TOMBSTONES) [0xb000000 0x100000] Size: 1.0MB  
LUN0 (DNT) [0xb100000 0x100000] Size: 1.0MB  
LUN0 (PERSISTENT) [0xb200000 0xc0000] Size: 768.0KB  
LUN0 (STEADY) [0xb2c0000 0x40000] Size: 256.0KB  
LUN0 (PERSDATA) [0xb300000 0x900000] Size: 9.0MB  
LUN0 (SYSTEM) [0xbc00000 0x10cc00000] Size: 4.199GB  
LUN0 (CACHE) [0x118800000 0xc800000] Size: 200.0MB  
LUN0 (HIDDEN) [0x125000000 0x9600000] Size: 150.0MB  
LUN0 (CP_DEBUG) [0x12e600000 0x500000] Size: 5.0MB  
LUN0 (USERDATA) [0x12eb00000 0x643400000] Size: 25.50GB  
LUN3 (CPEFS) [0x6000 0x600000] Size: 6.0MB
```

Leitura e a re- programação e totalmente diferente que vamos ver a seguir



CAPÍTULO 3

UFS

Maximum Number of LUs: 8

Number of LUs found: 5

LUN 0:

Size: 0xEE4800000 / 59,584,000,000B / 59GB

LUN 1 (Boot A):

Size: 0x400000 / 0,004,000,000B / 4MB

LUN 2 (Boot B):

Size: 0x400000 / 0,004,000,000B / 4MB

LUN 3:

Size: 0x800000 / 0,008,000,000B / 8MB

LUN 4:

Size: 0x800000 / 0,008,000,000B / 8MB

Number of W-LUs found: 1

W-LUN 0xC4 (REPORT LUNS):

Size: 0x1000000 / 0,016,000,000B / 16MB

Full size: 0x0F6800000 / 59,616,000,000B / 59GB

As partições LUN1 e LUN2 são equivalentes ao Boot 1 e 2, mesmo podemos observar que ao lado de cada um, entre parênteses podemos observe que nos indica como (Boot A) e (Boot B) e o tamanho é como no eMMC, sempre 4096kb ou 4mb.

Maximum Number of LUs: 8

Number of LUs found: 5

LUN 0:

Size: 0x0F4800000 / 59,584,000,000B / 59GB

LUN 1 (Boot A):

Size: 0x400000 / 0,004,000,000B / 4MB

LUN 2 (Boot B):

Size: 0x400000 / 0,004,000,000B / 4MB

LUN 3:

Size: 0x800000 / 0,008,000,000B / 8MB

LUN 4:

Size: 0x800000 / 0,008,000,000B / 8MB

Number of W-LUs found: 1

W-LUN 0xC4 (REPORT LUNS):

Size: 0x1000000 / 0,016,000,000B / 16MB

Full size: 0x0F6800000 / 59,616,000,000B / 59GB

CAPÍTULO 3

Então encontramos o W-LUN 0xC4 que é equivalente à partição RPMB.

Number of W-LUs found: 1

W-LUN 0xC4 (REPORT LUNS):

Block size: 0x100

Size: 0x400000 / 0,004,000,000B / 4MB

Full size: 0x773C00000 / 29,828,000,000B / 29GB

As memórias UFS são OTP regularmente configuradas (One Time Programming), então o tamanho não pode ser alterado de suas partições, há muito poucas memórias que o permitem.

Agora vamos falar sobre socket, temos em mente que pinagens de leitura não são compatíveis com emmc e emcp, devemos adquirir adaptadores específico para ufs

Para isso, exigimos um socket especial. No momento apenas Easy Jtag Plus, medusa pro 2 e hypobox, que suporta.

Existem socket, original e o genérico. O original era desenvolvido pela mesma equipe e lançado apenas para dois BGAs, BGA95,254 e 153.

Estes são os soquetes originais para UFS

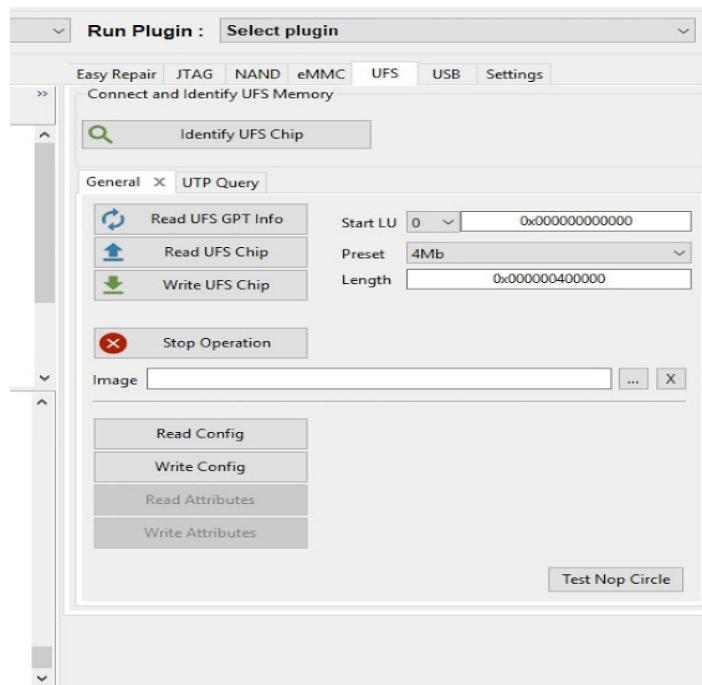


CAPÍTULO 3

Aqui temos os genéricos do fabricante do X-Mate IC chega FRIEND 3 em 1. Como você pode ver, a grande diferença é que este socket suporta os três BGAs existentes no mercado até agora, o BGA95, 153 e 254.



CAPÍTULO 3



Como podemos ver, a opção de VCC ou CLK não aparece mais. nem os Bits, já que essas linhas não existem mais no UFS, só nos permite modificar para alta ou baixa tensão ainda há muito desenvolvimento sobre a UFS, porém, Medusa Pro, por exemplo, já está trabalhando no Medusa Pro 2, que já vai incluir o UFS também e em alta velocidade de transferência de arquivos, pois atualmente esse é o problema do UFS, que é muito comunicação lenta e despejo LUNo, por exemplo, leva muito tempo, então vamos esperar e resolver esse problema no futuro

CAPÍTULO 3

Isp UFS NEW

Vamos fala um pouco do sistema novo que esta saindo, sistema de isp ufs, para vamos fala um pouco sobre esse sistema e mostra alguns adaptadores para isso. no momento so a easy jtag e a medusa pro 2 tem os adaptadores para reconhecer leitura pra isp, igual vimos no tópico anterior o sistema de dados e diferente de emmc, isso inclui um sistema de leitura totalmente diferente, por isso os socket e totalmente diferenciado e não pode ser usado.

na imagem abaixo tem um sistema mostra dos adaptadores que suporte isp ufs



easy jtag plus ufs



medusa pro 2 ufs



Mobile EMMC
WWW.MOBILEEMMC.COM.BR

PRIMEIRO EMMC & UFS

TEMOS SERVIDOR ARQUIVOS
WWW.MOBILEEMMC.COM