

FLASH数据恢复

一、FLASH简介 | 二、FLASH存储结构 | 三、常见故障分类 | 四、实际案例



公司简介

公司致力于FLASH数据恢复设备的研发生产和销售，在U盘、SD卡、TF卡、固态硬盘的数据恢复方面，拥有自己的科研团队和业内专家，拥有核心技术和自主知识产权，并长期为国内外数据恢复行业的难题提供技术支持与服务，始终掌握最前沿技术。

主打产品：MDR-Flash 移动存储设备数据恢复系统

前言

QIAN YAN

FLASH存储设备包含很多产品, 只要其存储部分采用的是FLASH芯片制作的均是, 常见的有U盘, SSD, TF卡, SD卡, CF卡, MS (记忆棒), MP3, MP4, 手机, 平板电脑, 录音笔等。

FLASH存储技术其包含电源处理芯片, 数据处理芯片和数据存储芯片三大部分, 简单故障的数据恢复也许就是维修电源转换电路或更换晶振就能够解决。但不断更新发展的存储技术集成度已变的更高, 目前大部分主控都已集成晶振, 且主控损率非常低。主控损坏后即使更换也不能访问用户数据。

所以我们只能通过读取数据存储芯片底层资料, 解密重组后还原用户数据。

FLASH存储器

1



我们研究的方向是针对所有FLASH存储设备的数据恢复，日常生活中经常使用的U盘 TF卡CF卡 SD卡 MS卡 SSD EMMC 录音笔 MP3 MP4 平板电脑各种嵌入式产品等等，都是我们的研究对象。



111010101110 10101010 10 10 101010101

111010101110

10101010

NAND FLASH大致分为三类



单层存储

•**SLC** (Single-Level Cell) 即1bit/cell, 速度快寿命长, 价格昂贵 (约MLC 3倍以上的价格), 约10万次擦写寿命



故障盘比例



多层存储

•**MLC** (Multi-Level Cell) 即2bit/cell, 速度一般寿命一般, 价格一般, 约5000---10000次擦写寿命

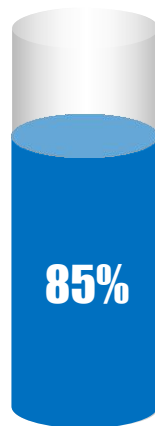


故障盘比例



三层存储

•**TLC** (Trinary-Level Cell) 即3bit/cell, 速度慢, 寿命短, 价格便宜, 约500次擦写寿命



故障盘比例



111010101110 10101010 10 10 101010101

111010101110

10101010

物理镜像中包含以下这些概念

PAGE

Page是NAND Flash的最小读写单位，一个Page包含若干个Byte

BLOCK

Block是NAND Flash的最小擦除单位，一个Block包含了若干个Page

PLANE

PLANE就是一个存储矩阵，包含若干个Block

LUN

LUN是晶圆上的小方块，一个芯片里可能封装若干个LUN，由于flash的工艺不一样，技术不一样，由此产生了LUN的概念一个chip包含N个LUN。

2

FLASH的存储结构

每个主控厂商都有自己独立的存储方式与加密算法，例如磨损平衡（动态/静态），XOR加密（动态/静态）与AES加密等。

我们只要根据芯片参数正确读出物理镜像，按照物理镜像的存储结构来分析即可。



111010101110

10101010

10 10 101010101

111010101110

10101010

例如：某芯片物理镜像中，**一个页包含2112字节**，区域划分如下：

512字节	16字节	512字节	16字节	512字节	16字节	512字节	16字节
用户数据	服务区+ECC	用户数据	服务区+ECC	用户数据	服务区+ECC	用户数据	服务区+ECC



111010101110

10101010

10 10 101010101

111010101110

10101010

每个**PLANE**又包含**1024**个块
一个物理镜像包含**2**个**PLANE**

	物理镜像
PLANE0	0块
PLANE1	1块
PLANE0	2块
PLANE1	3块
PLANE0	4块
PLANE1	5块
PLANE0	6块
PLANE1	7块
PLANE0	8块
PLANE1	9块
PLANE0	10块
...	...
PLANE1	2037块
PLANE0	2038块
PLANE1	2039块
PLANE0	2040块
PLANE1	2041块
PLANE0	2042块
PLANE1	2043块
PLANE0	2044块
PLANE1	2045块
PLANE0	2046块
PLANE1	2047块



111010101110

10101010

10 10 10101010

111010101110

10101010

ECC错误

ECC校验错误与
芯片质量相关,
有部分**可以修正**
但不能在损坏的
存储设备上修正。
可以通过算法来
修正读取物理镜
像中的BIT错误。

	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	0123456789ABCDEF
0x000	EB	58	90	4D	53	57	49	4E	34	2E	31	00	02	40	10	6D	.X.MSWIN4.1..@.m
0x010	02	00	00	00	00	F8	00	00	3F	00	80	00	80	1E	00	00	?.....
0x020	80	7A	53	07	98	3A	00	00	00	00	00	00	02	00	00	00	.zS.....
0x030	01	00	08	00	00	00	00	00	00	00	00	00	00	00	00	00	
0x040	00	00	29	87	9C	D4	E0	4B	49	4E	47	53	54	4F	4E	20	..)....KINGSTON
0x050	20	20	46	41	54	73	32	20	20	20	FA	33	C9	8E	D1	BC	FATs2...3....
0x060	F8	7B	8E	C1	BD	78	00	C5	76	00	1E	56	16	55	BF	22	{.....V.V.U."
0x070	05	89	7E	00	89	4E	00	91	0B	FC	F3	A4	8E	D9	BD	00	N.....
0x080	7C	C6	45	FE	0F	8B	46	18	88	45	F9	38	4E	40	7D	25	.E...F...E.8N@ %
0x090	8B	C1	99	BB	00	07	68	97	00	72	1A	83	EB	3B	66	A1	h...r...f.
0x0A0	1C	7C	66	3B	07	9A	57	FC	75	06	00	CA	02	88	56	02	...W.u....V.
0x0B0	81	C3	30	73	ED	BF	02	00	83	7E	16	00	75	45	8B	4E	.0s.....uE.N
0x0C0	1C	8B	56	1E	B9	03	00	49	40	75	01	42	BB	00	7E	E8	.V....Iou.B...~.
0x0D0	5F	04	73	26	B0	F8	4F	74	7E	02	0E	75	33	D2	B9	03	.s&...Ot..F"3...
0x0E0	00	3B	C8	77	1E	8B	76	0A	91	F7	76	18	0B	F1	03	46	...W.v...s...F
0x0F0	1C	13	56	1E	EA	D1	73	0B	EB	27	83	7E	2A	00	77	03	.V...s...~*..w.
0x100	E9	FD	02	BE	7E	7D	AC	98	03	F0	AC	84	C0	74	17	30	...~}.....t.<
0x110	FF	74	09	B4	0E	BB	07	00	CD	10	EB	EF	BE	81	7D	E8	.t.....}.
0x120	E5	AE	7F	7D	EB	E0	98	CD	12	5E	1F	66	87	04	CD	19	..I}.....^f....
0x130	41	56	66	6A	00	52	50	06	53	6A	81	6A	10	8B	F4	60	AVfj.RP.Sj.j...
0x140	80	7E	02	0E	75	04	B4	42	EB	1D	91	92	33	D2	F7	76	~..u..B....3..v
0x150	18	91	F7	76	18	42	87	CA	F7	76	1A	8A	F2	8A	C8	CD	...v.B...B....
0x160	CC	02	0A	CC	B8	00	02	8A	56	40	CD	13	61	8D	64	10	V@...a.d.
0x170	5E	72	0A	40	55	01	42	03	5E	0B	49	75	B4	C3	03	18	^r.@U.B.^Iu....
0x180	01	27	0D	0A	49	6E	74	61	6C	69	64	20	73	79	73	74	!..Intalid syst
0x190	65	6D	20	64	69	73	6E	FF	0D	0A	44	69	73	6B	20	49	em disk...Disk I
0x1A0	2F	4F	20	65	72	72	6F	72	FF	0D	0A	52	65	70	6C	61	/O error...Repla
0x1B0	63	65	20	74	68	65	20	84	69	73	6E	2C	22	61	6E	64	ce the disk,"and
0x1C0	20	74	68	65	6E	20	72	72	65	73	73	20	61	6E	79	20	then rress any
0x1D0	6B	65	79	0D	0A	00	00	00	49	4F	20	20	20	20	20	20	key.....IO
0x1E0	52	59	53	4D	13	44	4F	53	20	20	20	53	59	53	7E	01	RYSM.DOS SYS~.
0x1F0	00	57	49	4E	C2	4F	4F	54	20	53	59	53	00	00	75	AA	.WIN.OOT SYS..u.





111010101110 10101010 10 10 101010101

111010101110

10101010

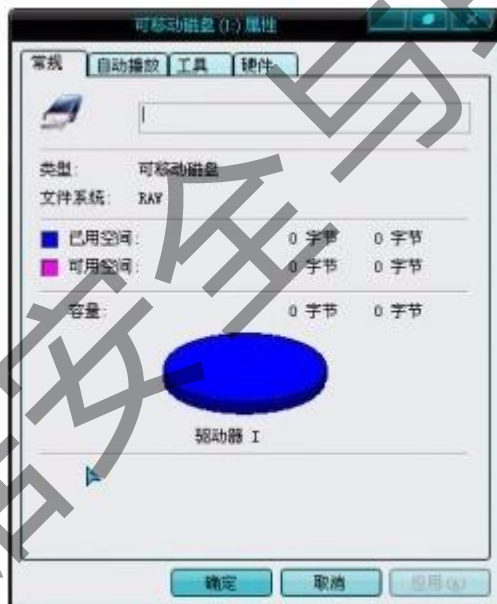
常见的故障现象

故障盘大部分都是**固件**损坏导致的，**U盘固件存储在FLASH中**。由于各种原因导致主控不能正确访问固件区。比如缺陷列表损坏，编译表损坏，密钥损坏等。

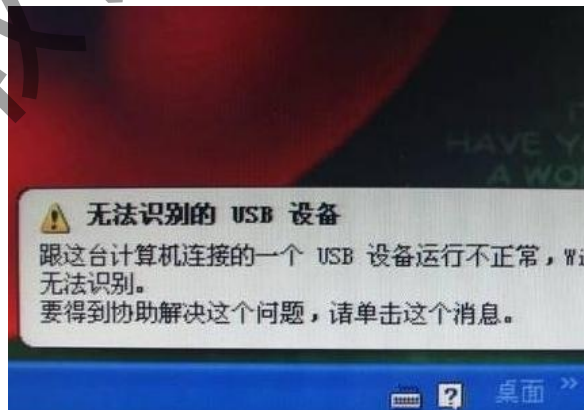
故障现象：**物理损坏**多为无法识别的USB设备，或者链接电脑后在**设备管理器中不能发现新硬件**；

逻辑损坏则是可以检测到设备但是**提示格式化**，提示插入磁盘或**无法访问**等，不能对设备进行读写。常规方法不能修复设备，不能读取数据部分，只能通过**读取FLASH底层数据**进行恢复。

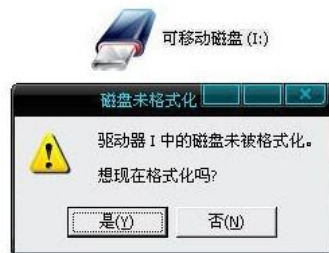
逻辑损坏



物理损坏



逻辑损坏



FLASH常见故障分类

物理损坏

1

- 1、电路板断裂
- 2、接口断裂
- 3、电路开路 短路
- 4、摔坏
- 5、进水
- 6、各种外界因素导致

逻辑损坏

2

- 1、ECC校验错误
- 2、固件损坏

3

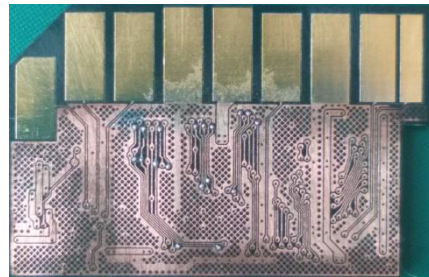
实际案例

4

目前FLASH数据恢复根据难度和设备封装形式分为两种：



普通封装的SD卡



一体化封装的SD卡



111010101110

10101010

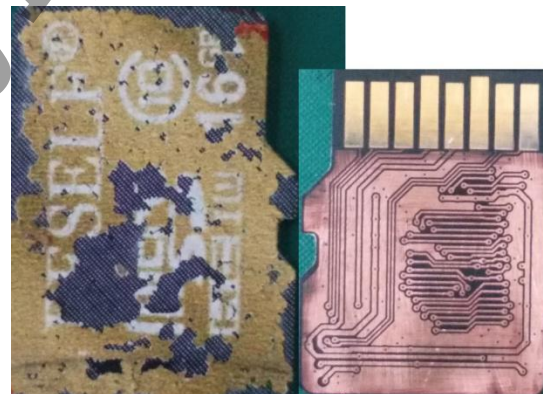
10 10 10101010

111010101110

10101010

一体化封装恢复难度高成本大

一体化封装的FLASH存储设备引脚定义各不相同，只有根据**逻辑分析仪**具体分析每条线路波形综合判断，最终确定哪些是**正确的引脚定义**。只有分析出正确的引脚定义才能**读取物理镜像**做下一步分析。



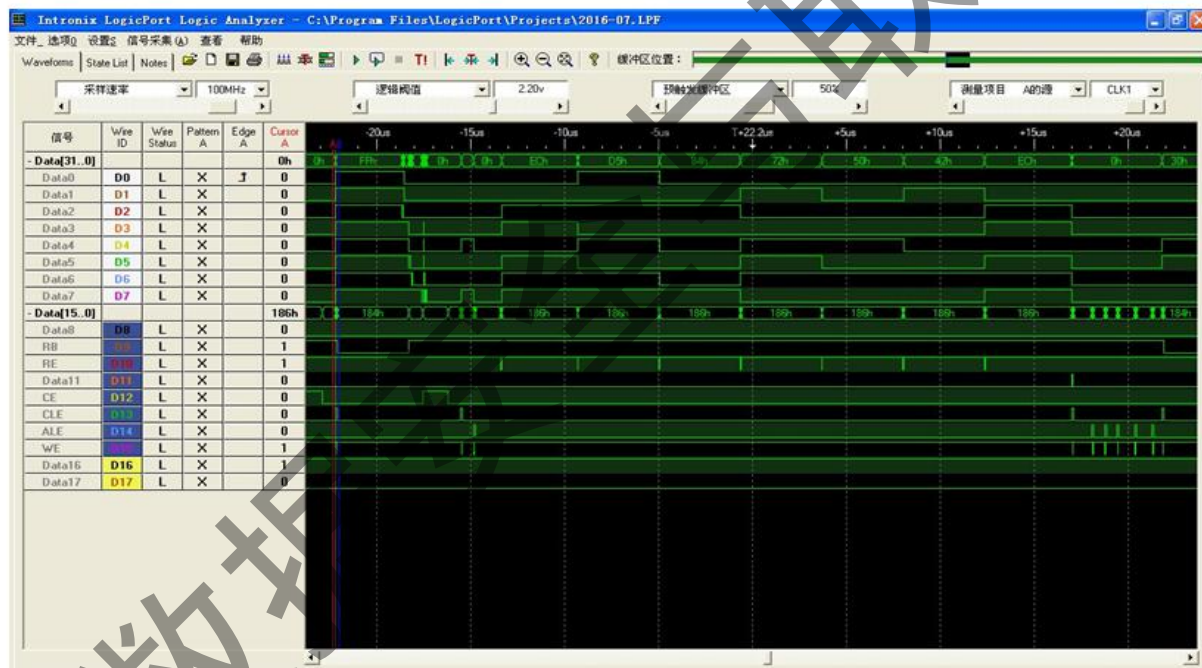


111010101110 10101010 10101010101

111010101110

10101010

逻辑分析仪分析





111010101110

10101010

10 10 10101010

111010101110

10101010

我们已经拥有
的一体U盘定义
164种



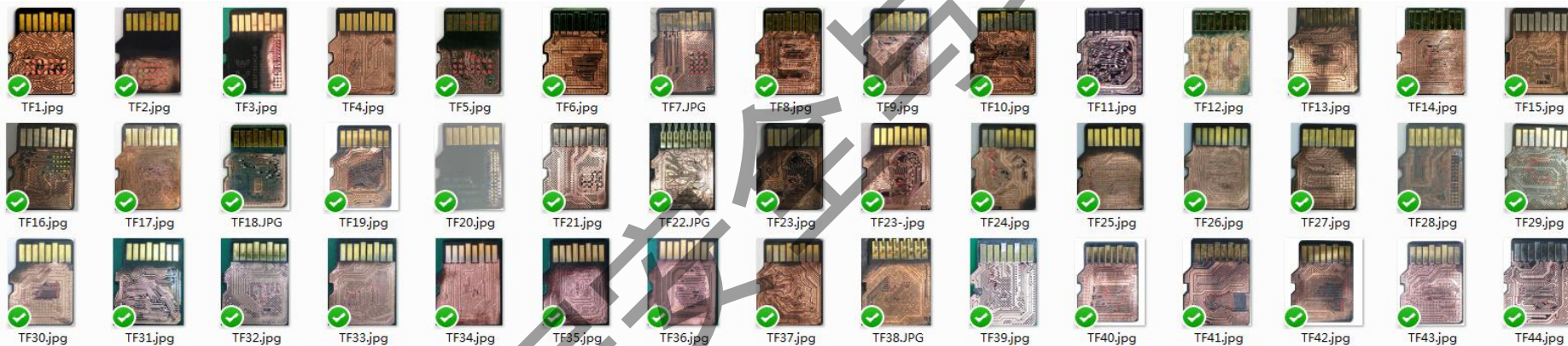


111010101110 10101010 1010 101010101

111010101110

10101010

TF卡 44种



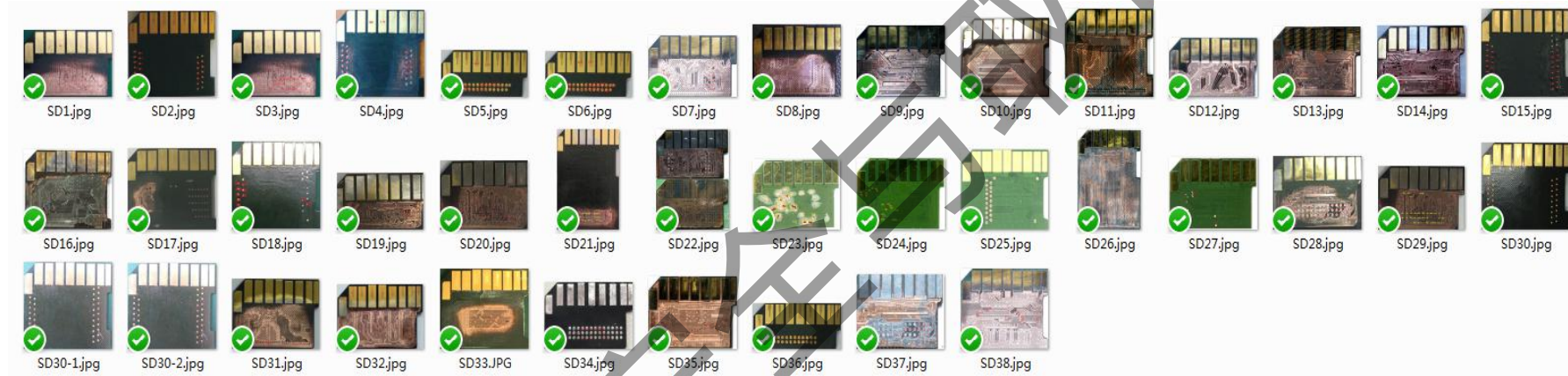


111010101110 10101010 10101010101

111010101110

10101010

SD卡40种



EMMC 9种





111010101110

10101010

10 10 101010101

111010101110

10101010

FLASH数据恢复
的大致流程

- 1、判断故障类型
- 2、无法修复的故障需要读取物理镜像
- 3、物理镜像的分析
- 4、建立逻辑镜像
- 5、分析逻辑镜像
- 6、导出正确数据

分类

读取

分析

解密

重组

验证



111010101110

10101010

10 10 10101010

111010101110

10101010

普通U盘数据恢复

故障现象为插入电脑提示格式化。利用工具检测可以识别到主控型号与FLASH的ID，但是无法修改格式化也会报错。这样的现象就是固件损坏导致的，通过更换电路板或主控是不能修复的。只能通过读取物理镜像才能恢复其内容。



案例一



111010101110

10101010

10 10 101010101

111010101110

10101010

普通U盘数据恢复

故障盘信息:

厂家: 金士顿16G USB2.0U盘

主控型号: TC58NC6623

FLASH丝印: TC58TEG6DDKTA

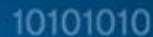
FLASH ID: 0x98DE9892 7650

物理镜像为8G×2 2CE 单通道 每个芯片对应一个通道

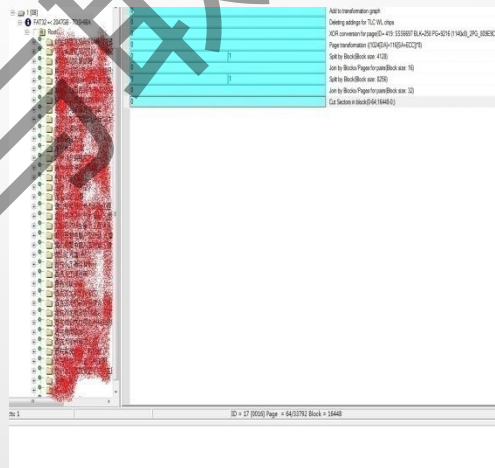
通过FLASH ID 可以知道这款芯片是东芝14nm **TLC芯片**
属于SDR 芯片包含4个PLANE

The screenshot shows a software interface for identifying a USB device. The 'Identifier (ID)' field displays '983AA892' and '76500000'. The 'Manufacturer' is 'Toshiba'. The 'Microchip' is 'TC58TEG7D0KTA00'. The 'Microchip capacity' is '16384'. The 'Page size' is '9216'. The 'Bus width' is '8 bit/100x0'. The 'Block size (in pages)' is '258'. The 'Reading algorithm' is '9' and 'TLC w/L8 SDR'. The 'Power scheme' is 'TSOP-48' and 'TLGA-52'. The 'Read Params' is '529'. The 'Planes number' is '4'. The 'Read Retry type' is '23'. The 'Pair Page type' is '0'. The 'Active all CE' checkbox is unchecked. The 'Specific Interleave' is 'Block (Page Size: 16 sectors)'. The 'Interleave value' is '4128'. The 'Core (VCC)' is '3.300 V'. The 'ID buffer (VCCQ)' is '3.300 V'. The interface includes 'Quit', 'Import', and 'Apply' buttons at the bottom.

案例一



案例一





111010101110 10101010 10 10 10101010

111010101110

10101010

一体化封装SD数据恢复

故障现象是插入到读卡器中计算机没有任何反应



案例二



111010101110 10101010 10 10 101010101

111010101110

10101010

一体化封装SD数据恢复

故障盘信息:

厂家: SONY 128G SD

主控型号: 未知 (可以通过物理镜像中的数据分析出是什么主控)

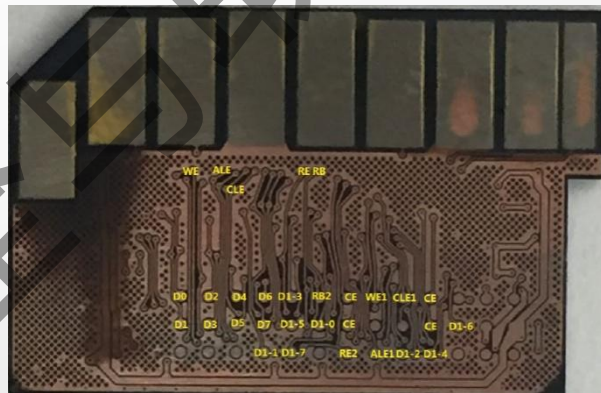
FLASH 丝印: 未知

FLASH ID: 未知

未作出定以前很多信息都是未知的。

对于一体化封装我们有完整的恢复流程。

1打磨, 2侦测定义, 3读取FLASH, 4分析数据, 5组合数据



案例二



111010101110

10101010

10 10 10101010

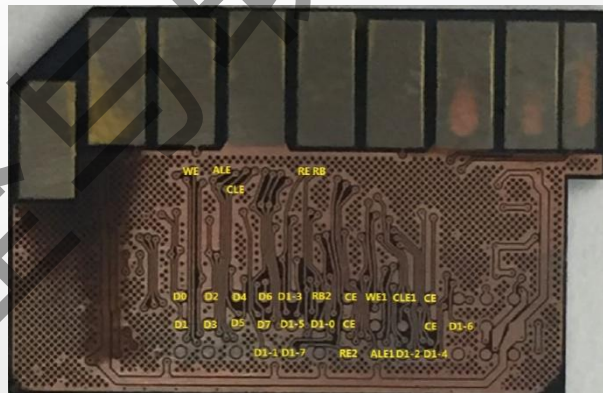
111010101110

10101010

一体化封装SD数据恢复

除折断、短路、FLASH芯片损坏外。一体SD
卡恢复成功几率90%

支持任意类型照片、文档及视频。



案例二



111010101110

10101010

10 10 101010101

111010101110

10101010

一体化封装TF数据恢复

故障现象插入读卡器中计算没有任何反应。



案例三



111010101110 10101010 10 10 101010101

111010101110

10101010

一体化封装TF数据恢复

除折断、短路、FLASH芯片损坏外。TF卡恢复成功几率70%

支持任意类型照片、文档及视频。



案例三

TF卡恢复的难点一个是焊点非常小，另一个就是加密方式大多是动态加密。我们可以解决大部分动态加密的问题。



111010101110 10101010 1010 101010101

111010101110

10101010

录音笔

故障现象是可以开机 但是定格
在开机画面 链接电脑没有反应



案例四



111010101110

10101010

10 10 101010101

111010101110

10101010

录音笔

录音笔数据存储格式特殊，加密方式也比较特殊。
(FLASH存储底层数据都有加密)

故障盘信息:

厂家: 清华同方

主控型号: ATJ3315B

FLASH 丝印: 29F64G08AAMEI

FLASH ID: 0x8988244B 0900

物理镜像为8G×1 1CE 单通道 每芯片对应一个通道



案例四



111010101110

10101010

10 10 10101010

111010101110

10101010

录音笔

物理镜像读取完毕后重点在于解密数据和重组数据。

录音笔数据恢复在逻辑镜像建立后。需要把固件部分剔除。剔除时可能会把文件系统中重要的部分一并去掉。所以录音笔的恢复50%是没有文件结构的。

除FLASH芯片损坏外，录音笔恢复成功率85%以上。
支持已知任意类型录音文件



案例四



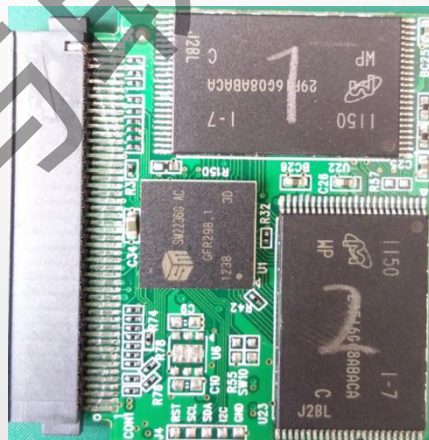
111010101110 10101010 10 10 101010101

111010101110

10101010

CF卡

故障现象是插入读卡器中计算机没有任何反应



案例五



111010101110 10101010 10 10 101010101

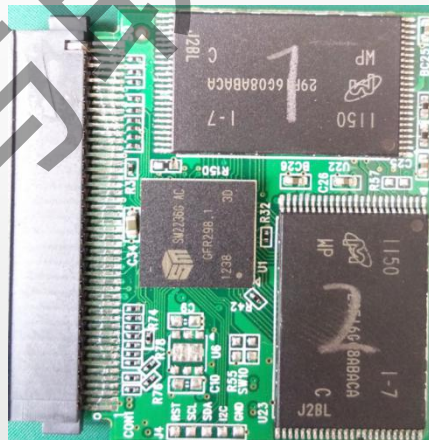
111010101110

10101010

CF卡

除FLASH芯片损坏外。CF卡恢复成功几率95%

支持任意类型照片、文档及视频。



案例五

CF卡恢复的难点在于芯片的逻辑顺序排列，每页数据交换最小为8个字节。
经过分析与重组最终恢复出客户想要的照片



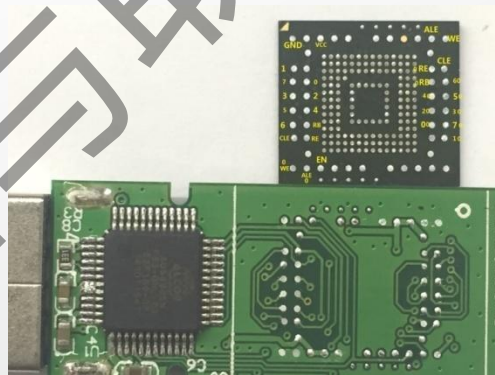
111010101110 10101010 1010 101010101

111010101110

10101010

EMMC

故障现象提示格式化



案例六



111010101110

10101010

10 10 10101010

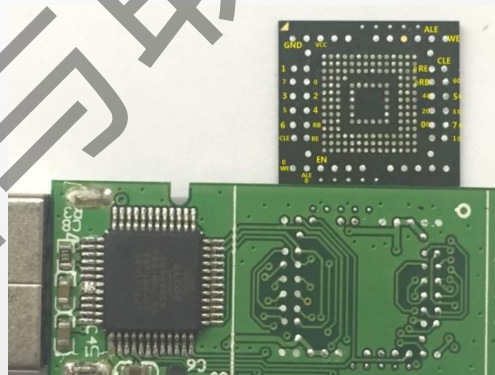
111010101110

10101010

EMMC

经过研究发现 EMMC芯片通常存在两个接口，一个是MMC接口，就是手机用到的。另一种就是NAND FLASH接口 也就是我们要读取的物理层数据接口。

当EMMC接口损坏无法读取数据的情况下，可以直接通过NAND FLASH接口直接读取底层数据，然后解密重组。



案例六



111010101110

10101010

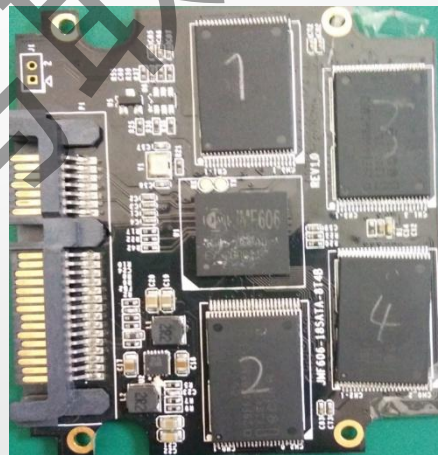
10 10 10101010

111010101110

10101010

SSD

故障现象是系统下不认盘，在BIOS
中可以认到8M



案例七



111010101110 10101010 10 10 10101010

111010101110

10101010

SSD

故障盘信息:

厂家: 未知

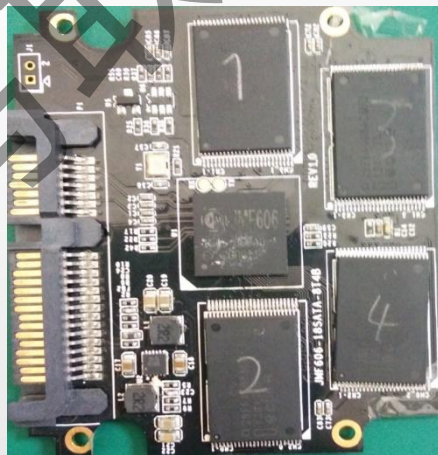
主控型号: JMF606

FLASH 丝印: MT29FxxG08CxxAx

FLASH ID: 0x2C88244B

物理镜像为 $8\text{G} \times 4$ 4CE 单通道 每芯片对应一个通道

固态硬盘与U盘 SD TF CF 不同, 数据块小, 重复率高, 编译方式特殊。一部分使用AES加密。



案例七

111010101110

10101010

案例七

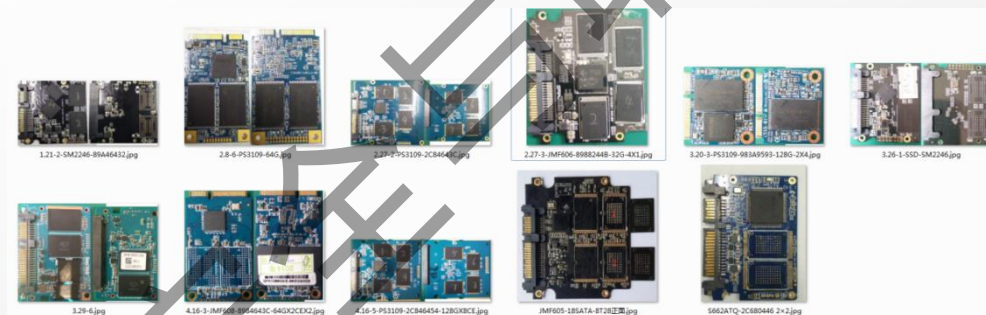


111010101110 10101010 1010 101010101

111010101110

10101010

SSD已成功
的方案



THANKS



- 张彬
- 手机号： 13942001139
- 深圳市云帆赢通信息技术有限公司