Note 2018: much of the information herein is old and the field has changed with many new methods and options. Still I find this useful for historical, and in some ways current, context.

Ideas for methods on dumping memory IC's. The most efficient method for dumping FLASH involves purchasing a highly supported industrial programmer in the range of 10,000eu and support packages around 1,000 each year to receive software updates that allow the programmer to notice new FLASH chips. This allows an analyst to spend one day to dump memory with the ability to also write to it. The most manually method and the method I've used requires 4 to 5 days. The majority of this time is spent debugging the hardware setup which involves many hand connected wires to/from the chip and breakout board and microcontroller. Perhaps one day of this time is actually spent on target specific software. If it were possible to simplify the hardware this task could be reduced to 2 days.

Two attempts in 2007 and 2008 were made to use consumer CF cards to resocket target FLASH by putting it in place of the cards own FLASH. This has worked and been somewhat detailed but few have replicated it without problem. Questions that I'd like to answer are:

1. What types of CF/SD cards have controllers that get in the way of a raw (dd) dump? Show at least one or two known to work. Try on a few targets and document the results.

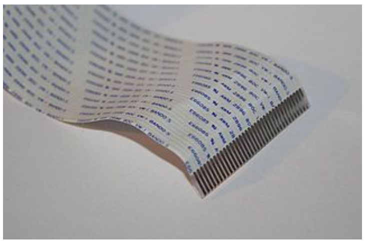
2. The attempts so far have focused on TSOP flash (pins exposed on side) but can this be used for BGA (pins beneath, much more expensive equipment normally) by finding CF and SD cards with BGA chips?

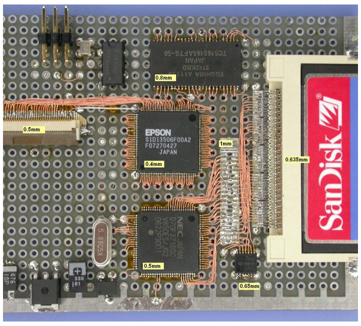
This requires purchasing various components to play with. It is likely that most of this hardware will not work but because it is not clear the shot-gun approach to the bill of materials is necessary.

Index:

Using Flex Cables

Using fpc ffc 0.5mm flex cables. shave cable and solder to it. Yamaichi and many others (see wikipedia link before) sell these. I also remember seeing this technique used with solinoid wireing





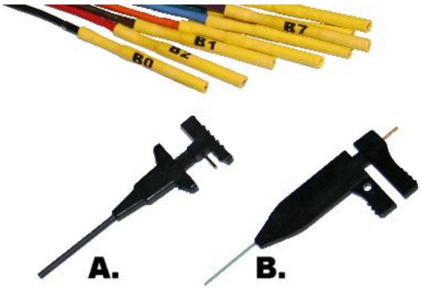
Hand soldered to exposed flex cables

Using IDE Cables

Some IDE cables have spacing that could be used similar to the FLEX cables.

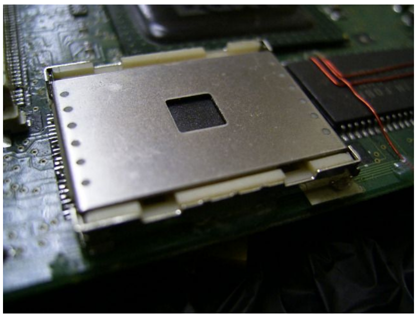
Using Wire Clips

Gologic 0.3mm “Nano clip” probes $9 ea (“b” pictured). Datasheet and same price at digikey. See this and this forum post comparing different clip types.

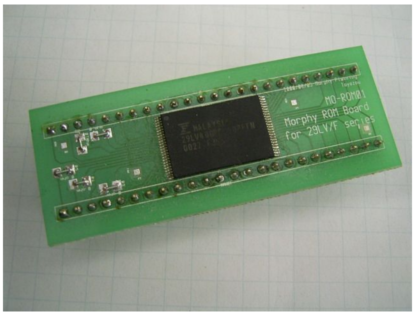


Using Clamshell Socket

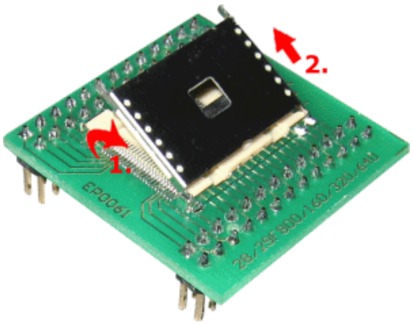
Clamshell TSOP socket (ontop of PCB?): Yamaichi IC197 series. From ib-hoebel but only 40pin, in .pl only 32pin. Yamaichi datasheet says that a 56 pin version exists but im having trouble finding it outside of the chinese sites. They also do not have details of the 197 on their website and it appears it has been replaced by full ZIF sockets (IC51) or a different type of identical footprint insertion technique (IC306, IC307only 0.8mm? IC179 1.27mm but datasheet describes smaller but only up to 44 pin).



Yamaichi IC197



Typical breakout PCB that such a socket could be used with.



48pin in breakout from Epsilon.pl (20eu)

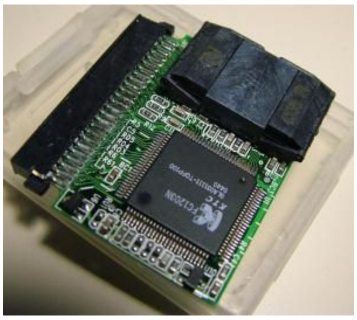
Using Clamp Socket

Using Spring Socket

Using Special Flex boards

Some of the WII and XBox mods included flex boards cut in a way that they could be placed over and around the target flash or ic and then soldered easily (or without soldering even, it could just clamp snuggly around the target chio). Not sure where to purchase these.

Using Repurposed CF

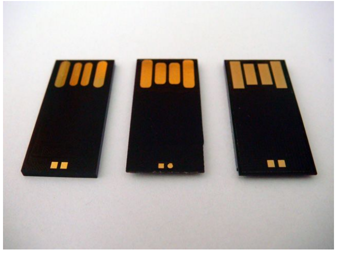


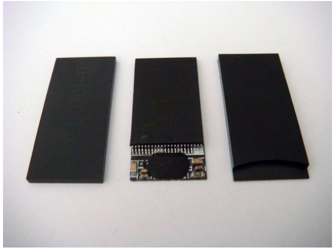
Using a Socket on CF or PCB. Notice the KTC FC1203N (Kingston?) can also be found in Kingwolf cards so perhaps they also have TSOP inside (rather expensive though). The sockets themselves can be purchased from distrelec.de or ebay (.de&com) but we cover that above.

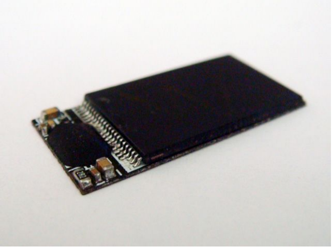
Need to find a series of CF, USB and Memory cards to take apart. Look for TSOP and BGA versions.

Using Repurposed UDP SD/CF/USB

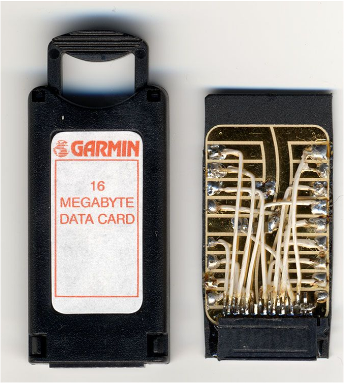
Nice detail on how FLASH is used (from a data recovery perspective so decent depth) in the first 3 images on the right. The others are from a document on “UDP [ultradense?] USB drives”.

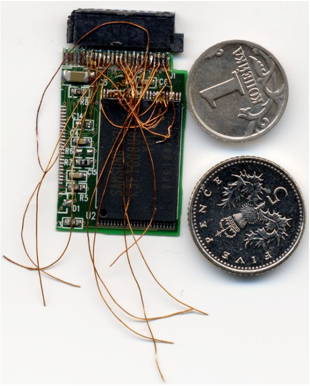


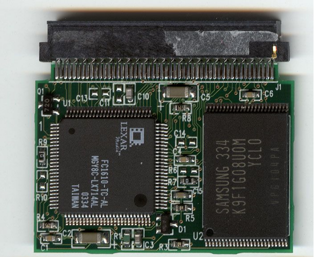




These resources do not give full detail of the cards shown. Another resource describing changing the memory with more details on the exact cards used:

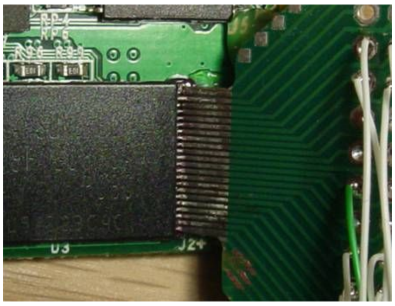






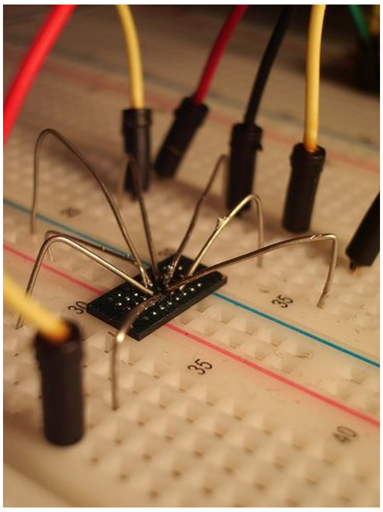
Using Shaved Breakoutboard + Reader

It is possible to use breakout boards cut to form and carefully soldered to the chip. There is some discussion in the description concerning problems when doing this to a chip in place. The author also explains that Readers can work better than CF/SD/USB controllers because it is passive and some controllers attempt to handle/massage the FS (look for FAT, etc).



Directly Soldering

Directly attack to pads. Also see the flex cable and other wiring methods above.



Purchase Plan

We are only going to target TSOP 48 and 56 pin at 0.5mm for now. Might venture into TSSOP packages as well. All items are 0.5mm TSOP unless otherwise noted.

Clamp sockets:

Distrelec.de 48@17eu 56@18eu

Eliptor.pl easy zif 32@16

Spring sockets

All 56 boards appear to convert to 48 for programmers

Epromirok.hu 48@41eu

56downto48@67 Equinox 56downto48@77

Eliptor 48@70eu

Breakout boards:

Distrelec.de 48@9eu

60 0.4mm@9 TSSOP 56 0.5mm@7

Assorted 0.5 0.6 0.8 1.2 @42

Epromirok.hu 48@9eu 56@14eu

48 0.?mm@14

Eliptor.pl 48to42pin@5eu 48@4eu 56@4eu 48@3eu 48@2eu 48@3eu

Flex cables:

Digikey 30pin@19eu 40pin@9eu

Flex connector:

Newhaven 40pin 0.5mm@8eu

Reader

As mentioned in the attempt from 2007:

Amazon.com DazzlSmartMedia/XD type1@$10 type2@$10

Bill of Materials

Store	Purchase link and cost	Qty	Total
Distrelec.de	Socket 48@17eu	3	51
	Socket 56@18eu	3	54
	Board 48@9eu	2	18
Epromirok.hu	Spring Socket 48@41eu	1	41
	Board 48@9eu	2	18
	Board 56@14eu	2	28
Eliptor.pl	Spring Socket 48@70eu	1	70
	Board 48to42pin@5eu	2	10
	Board 48@4eu	2	8
	Board 56@4eu	2	8
	Board 48@3eu	2	6
	Board 48@2eu	2	4

	Board 48@3eu	2	6
Digikey	Cable 30pin@19eu	2	38
	Cable 40pin@9eu	2	18
Newhaven	Cable connector 40pin 0.5mm@8eu	4	32
Amazon.com	Reader type1@$10	1	10
	Reader type2@$10	1	10
		Total	430

Why are some types of boards or items purchased from different sellers?
Because they are different footprints. These boards will be cut and attached to a chip in place. Depending on how thick the board is, how much solder it already has on the traces, will determine how successful this technique is.

Why purchase multiple items?
Techniques might fail and result in the item being destroyed or in less than optimal shape. To avoid having to spend extensive effort to repair, better to move onto the spare and save repairing for later if required (when/if the spare is also damaged).
When an item is expensive though only 1 is purchased.

Notes

I believe all the Distrelec boards could be found at farnel (but not digikey)

disrelec prototyping boards

https://www.distrelec.com/ishopWebFront/catalog/node.do/para/keywords/is/Prototyping_Boards/and/language/is/en/and/shop/is/YY/and/id/is/01/and/node/is/DC-56139.html

Like what is at conrad but for 20eu

https://www.distrelec.com/ishopWebFront/catalog/product.do/para/keywords/is/Prototyping_Boards,_Eurocard,_SMD_for_QFP,_SOP,_SSOP,_SDIP/and/language/is/en/and/shop/is/YY/and/series/is/1/and/id/is/01/and/node/is/DC-26964.html

massive prototyping board for 42

https://www.distrelec.com/ishopWebFront/catalog/product.do/para/keywords/is/Prototyping_Boards,_SMD_Multi-adapter/and/language/is/en/and/shop/is/YY/and/series/is/1/and/id/is/01/and/node/is/DC-19624.html

Other connector sites:

http://www.wellsconn.com/en_listclassproducts.asp?product_class=005&class_name=%A1%EFConnect%A1%A2Scoket (hundreds of brands) most made by weilei.com (tons of adapters but no prices, meant for their programmer)

BGA

http://www.hddworld.com/tqfp.html but no clear pricing, have to contact but they are in asia and have a lot of spring based sockets for various bga footprints

http://www.epromirok.hu/index.php?route=product/product&path=36_56_62&product_id=206

ebga64 for 172eu (wellon programmer rated). made by weilei.com

A bga breakout board plus tsop and others for 90eu:

http://ucables.com/ref/EBGA64-SOCKET-ADAPTER-R320519

Might be able to buy the boards with the programmer here:

http://www.wholesale-in-china.org/articles/article-140143.htm

can also find some sockets on ebay but they are not cheap

http://www.ebay.co.uk/sch/i.html?_nkw=up2008+programmer