



Smashing the Screen Does Nothing!

Chip-Off Recovery of eMMC Data



Kim Thomson
H-11 Digital Forensics
kim@h11dfs.com

who am I?

- Retired SIGINT Soldier
- Nerd
- I love all things wireless
- My passion is extraction/recovery and decoding of phone/device data
- I teach courses in mobile forensics, chipoff for mobile forensics, JTAG-ISP for mobile forensics, Python for mobile forensics, database analysis for mobile forensics, and sewing
- I settled into mobile forensics because of the variety of areas within the field
- kim@h11dfs.com

chip-off extraction =

Removing the memory chip from a device in order to recover the data from the memory chip. Can be used for digital forensics, reverse-engineering, fun on a Saturday afternoon, etc.

Pros:

data is recovered, bypassing security on the device; still works on damaged/destroyed devices

Cons:

device is usually ruined by the process and encryption is still encryption

the movies lie to you

- Smashing a phone's screen doesn't destroy the flash chip inside
- Snapping off a burner phone's screen does nothing but unplug the phone's monitor
- You really need to go after it to destroy the data

what's the point?

One of the persistent challenges of mobile forensics or mobile data recovery is getting the data. Chip-off extraction of eMMC flash chips has been of great help in that aspect, when the data is more important than the phone hardware itself.

Chip-off can also be used for NAND memories, NOR memories, serial EEPROMs, Universal Flash Storage (UFS) and other types of memories.



mobile forensics challenges

- Finding the data
 - Phone, network, SIM, SD card, cloud?
- Extracting the data
 - Security locks (PINs, passwords, patterns, etc.), port difficulties, USB debugging?
- Decoding the data
 - Character encodings, file formats, database types?
- Analyzing the data
 - What does it mean?

finding the data

- Cloud
 - Many types of data simply aren't found on the phone
 - Depending on the case, may be trivial to obtain
- SIM
 - Not used for much data these days apart from last LAC and account info
 - Can contain old, deleted data from previous phones
- SD Card
 - Apart from the phone, probably the most important piece
 - Full of media and app data
 - May contain data from previously-used phones

finding the data

- Service Provider's Network
 - Tower dumps, subscriber data, call-detail records (CDR), SMS, MMS, data usage, web sites accessed, etc.
 - CDRs continue to be a prime source of location and activity information; must be obtained with proper legal authority
- Synced devices
 - Chrome, iCloud, Firefox, OneDrive, Dropbox, e-mail accounts, etc.
 - Can contain web histories, connected WiFi networks, calls, contacts, e-mail, synced files, etc.

finding the data

- Phone
 - Calls, contacts, messaging, e-mails, media, location data, account info
 - Databases, logs, event histories, connection timelines
 - Connected cells, WiFi nets, application usage history, netstats, synced Bluetooth devices
 - Basically the user's entire life may be found on the phone

The importance of the phone data cannot be overestimated. In 2018, I can personally guarantee that we will never see ALL the info on a device. There's simply too much of it.

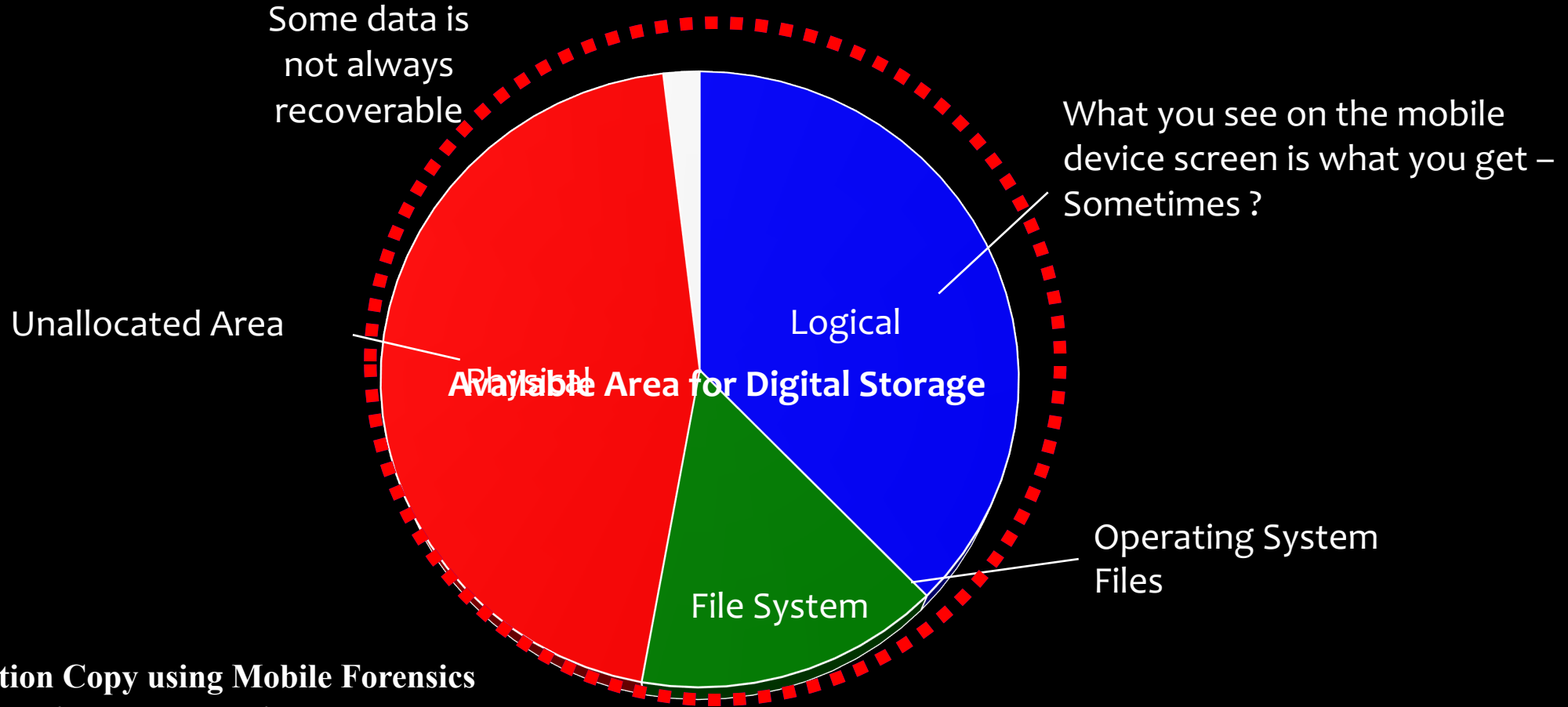
phone data problems

```
</N2>
</N1>
<N2 Tag="Remote">
  <N1 Tag="60:b1:2d:75:95:fd">
    <N1 Tag="Timestamp" Type="int">1451602321</N1>
    <N2 Tag="DevClass" Type="int">7936</N2>
    <N3 Tag="DevType" Type="int">3</N3>
    <N4 Tag="AddrType" Type="int">1</N4>
  </N1>
  <N2 Tag="38:01:95:8d:a2:da">
    <N1 Tag="Timestamp" Type="int">1451602321</N1>
    <N2 Tag="DevClass" Type="int">7936</N2>
    <N3 Tag="DevType" Type="int">3</N3>
    <N4 Tag="AddrType" Type="int">0</N4>
  </N2>
  <N3 Tag="bc:14:85:fa:38:16">
    <N1 Tag="Timestamp" Type="int">1451602321</N1>
    <N2 Tag="DevClass" Type="int">7936</N2>
    <N3 Tag="DevType" Type="int">3</N3>
    <N4 Tag="AddrType" Type="int">0</N4>
  </N3>
</N2>
```

```
B:A3:62:60,1,1424864957046-1000
6:94:62:60,1,1432342510972-1000
C:D6:42:C3,1,1417488961243-1000
5:65:C4:16,1,1430867240965-1000
4:E4:A5:7D,1,1262311175840-1000
B:51:43:3B,1,1408253655409-1000
1:15:02:06,1,1262312973884-1000
chbox/com.google.android.voicesearch/1274-1000
ch.ime.VoiceInputMethodService.?..4160-1000
!+android_idcca7d207f52f397$>..E.s3426-1000
ms_outgoing_check_max_count1000(=.
.I.sms_outgoing_check_interval_ms6
00000&<..I.lock_screen_lock_after_
timeout5000.;..5.auto_swipe_main_u
ser1:...9.lock_screen_quick_note1#
9..I.roam_dial_international_force
d0:8 V roam setting data internat
```

- Straight hexadecimal
- Flash memory storage chaos
- ENCRYPTION!!

phone extraction types



Extraction Copy using Mobile Forensics is not necessarily a **Bit Stream Clone/Image** as with Computer Forensics

logical extraction

- Were originally based on AT commands, talking to the internal modem
- Simple
- Relatively Fast (unless they have loads of media on the phone)
- Will recover no truly deleted data
 - May recover “deleted” database entries (calls, chats, contacts, etc.)
- Excellent choice for a “quick look”
- Can be stymied by different versions of an OS or blocked/disabled USB ports
- For Android and others, usually requires the installation of an extraction client (APK)

file-system extraction

- Usually “good enough” depending on the phone (Android)
- Depending on the phone, may be possible or may not
 - Jailbroken iPhone, rooted Android
 - Other OS, maybe, maybe not
- Analogous to copy-paste all files in the file system
- Can be blocked by security protocols in Android and iOS
- There are “lesser” file-system extractions
 - Android Debug Bridge (ADB) Backup
 - iTunes Backup
 - Partial file system based on MTP for Android

physical extraction

- This has always been the real goal: get ALL the data on the phone... all the 1s and 0s
- Analogous to a physical image of a hard drive
- Requires root permissions in Android, most of the time just a temp root
- After iPhone 4 is impossible (improbable?) in iOS devices
- Gives the examiner the possibility of recovering truly deleted data
 - Media
 - Deleted Files, not just DB entries
- Getting a full physical extraction of a device has sometimes been rather difficult

difficulties with physical extractions

- Locked Devices
 - Pattern, PINs, passwords
- Disabled ports in prepaid devices
 - TracFone, Net10, StraightTalk, etc.
- Android Debug Bridge (ADB) difficulties
 - Android 4.4.4 started it
- Android versions and security protocols
 - Carriers, makes, models
- Locked bootloaders
 - Verizon, ATT, I'm looking at you...

difficulties with physical extractions

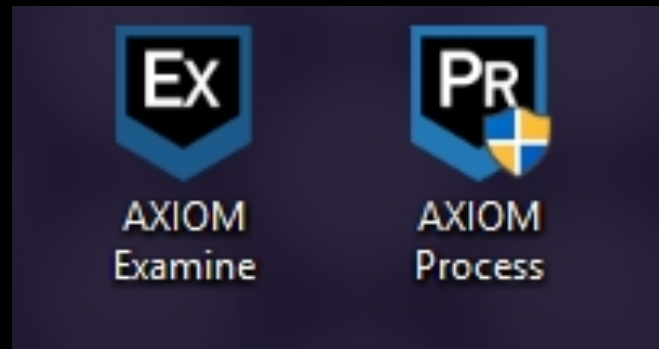
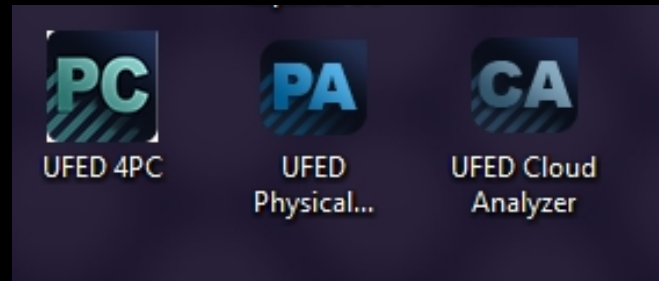
- Factory Reset Protection (FRP) locks
- Inability to root the device, even temporarily
- Inability to flash unsigned code to device (bootloaders)
- Damaged devices
 - Broken screens
 - Broken ports
 - Water damage
 - Destroyed or taced phones

how to get a physical extraction

- Temporary rooting
 - Must be able to push a vulnerability via USB Debugging (ADB) to */data/local/tmp* and execute
 - Must be supported by the device and version of Android
 - Is usually defeated by passcode/PIN/pattern/whatever
 - Newer versions of Android may not allow this
 - May be an app as well (APK)
- Bootloaders
 - Usually pushed to RAM while in fastboot or download mode
 - Bypasses security if it works
 - Others used while in Emergency Download (EDL) mode for Qualcomm processors
 - Very processor and/or manufacturer dependent

automated-tool vendors

- Cellebrite
- MicroSystemation
- Oxygen
- Magnet Forensics
- Paraben
- Guidance/OpenText
- SecureView
- MobilEdit



benefits of automated tools

- Widely used
- Well-funded and researched
- Faster
- Easier
- Require less technical expertise
- In most cases, you only need to follow the instructions

benefits of automated tools

- Besides providing the extraction of data from the mobile device, these tools also do the decoding, or parsing of the data
- Analytical tools are also included
- Reporting tools are also included
- Customer support
- Etc...

problems with automated tools

- When they don't work, they don't work
- If a device isn't supported, then you may not be able to find support at all for it
 - It may be possible, but sometimes it's difficult to figure out which other method may work
- They are, depending on your background and point of view, insanely expensive
- Automated tools produce... and there is no nice way to put this... the script kiddies of the mobile-forensics world
- They don't exactly produce a "technically-advanced user" necessarily

moving beyond automated tools

- Custom Recoveries
 - Odin, Fastboot, etc. (go hit up XDA Developers)
- Engineering Bootloaders
- Flasher Boxes
 - Octoplus – Medusa
 - Z3X
 - Furious Gold
 - CS-Tool
 - BST Dongle
 - Etc.

moving beyond automated tools

- Custom ADB scripts
 - dd your mmcblk0 through tcp-forwarded adb via nc
 - Use *df* and *mount* to figure out which is your
 - Usually require a rooted device, at least temporarily
- HID devices attacks to unlock phones
 - Teensy, Rubber Duck, Cellebrite, SecureView, etc.
- Man-in-middle (MITM) attacks
 - WiFi or cell

moving beyond automated tools

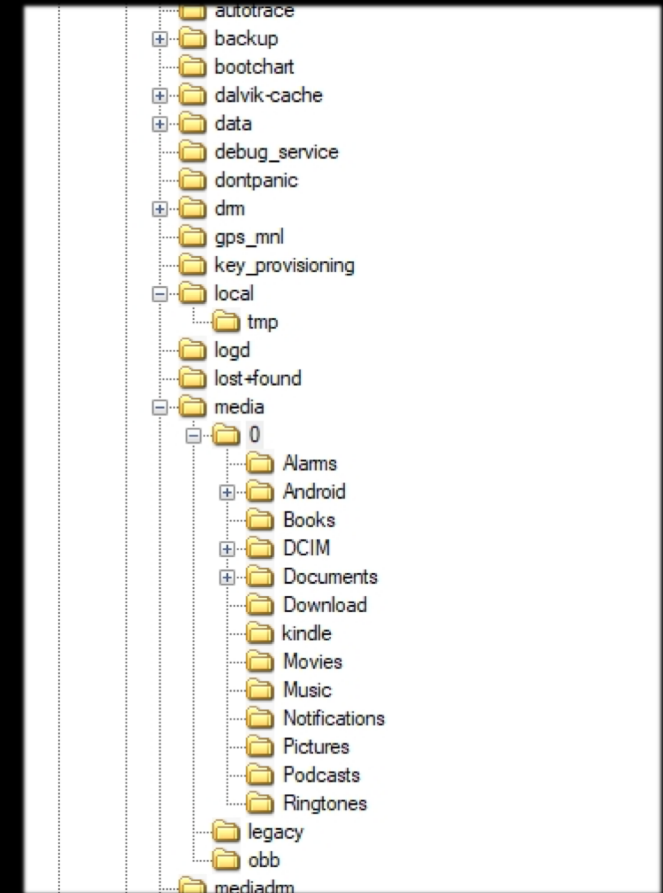
- Joint Test Action Group (JTAG) extraction
 - Currently limited to older or cheaper phones
- In-System Programming (ISP) or eMMC chips
 - Limited to phones with eMMC or eMCP chips
- Chip-Off Extraction
 - Can be NOR, NAND, eMMC, eMCP or UFS chips

what do we do with the data?

- AccessData FTK Imager (free)
 - <http://marketing.accessdata.com/ftkimager4.2.0>
- Medusa Pro or Octoplus Pro Software (about 160 bucks)
- Autopsy and Sleuthkit (FOSS)
- Cellebrite Physical Analyzer (paid)
- Oxygen Detective (paid)
- Magnet Axion (paid)

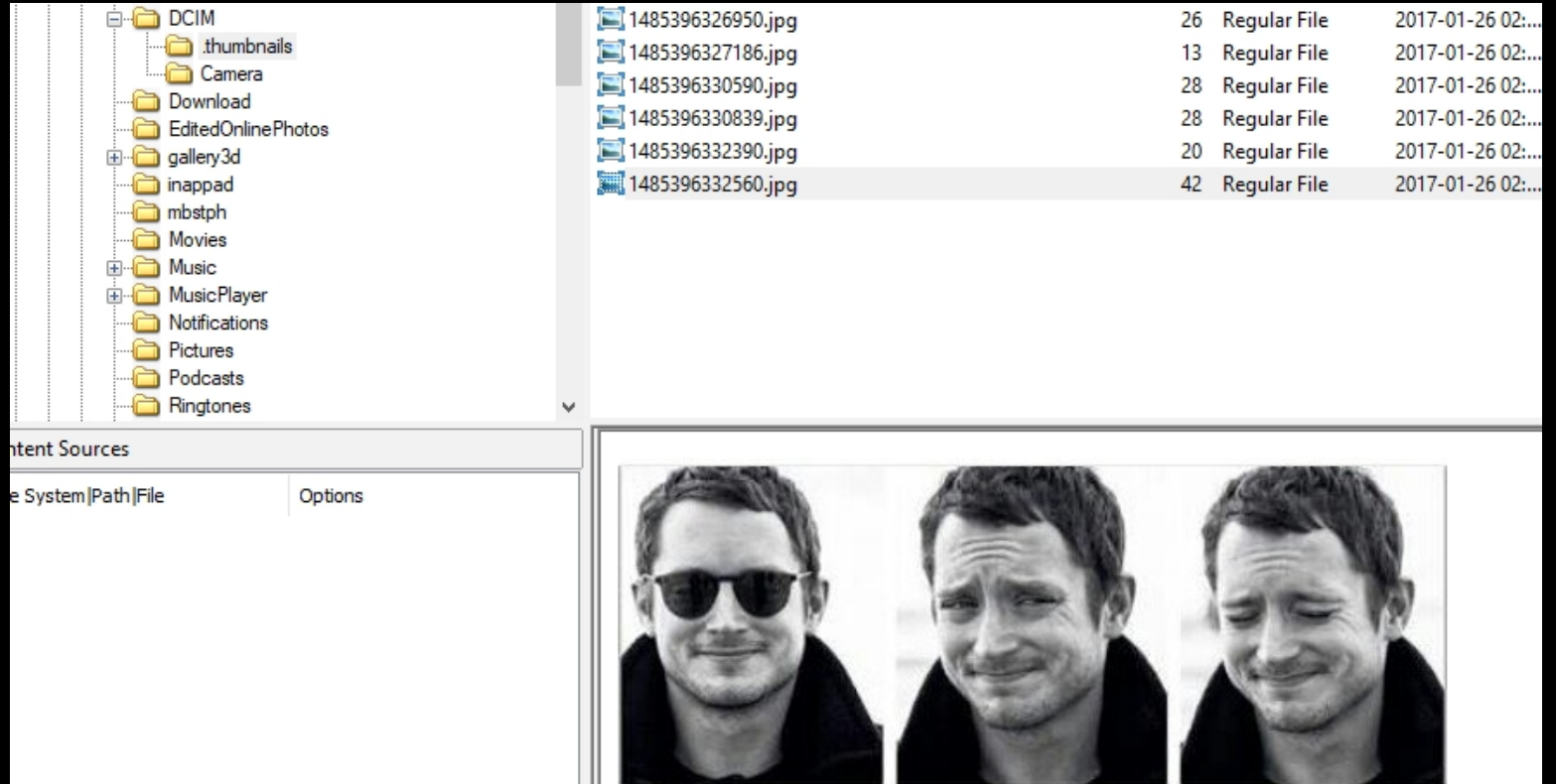
how do we see the data?

- AccessData FTK Imager (free)
 - <http://marketing.accessdata.com/ftkimgager4.2.0>
- Medusa Pro or Octopus Pro Software (about 160 bucks)
- Autopsy and Sleuthkit (FOSS)
- Cellebrite Physical Analyzer (paid)
- Oxygen Detective (paid)
- Magnet Axion (paid)



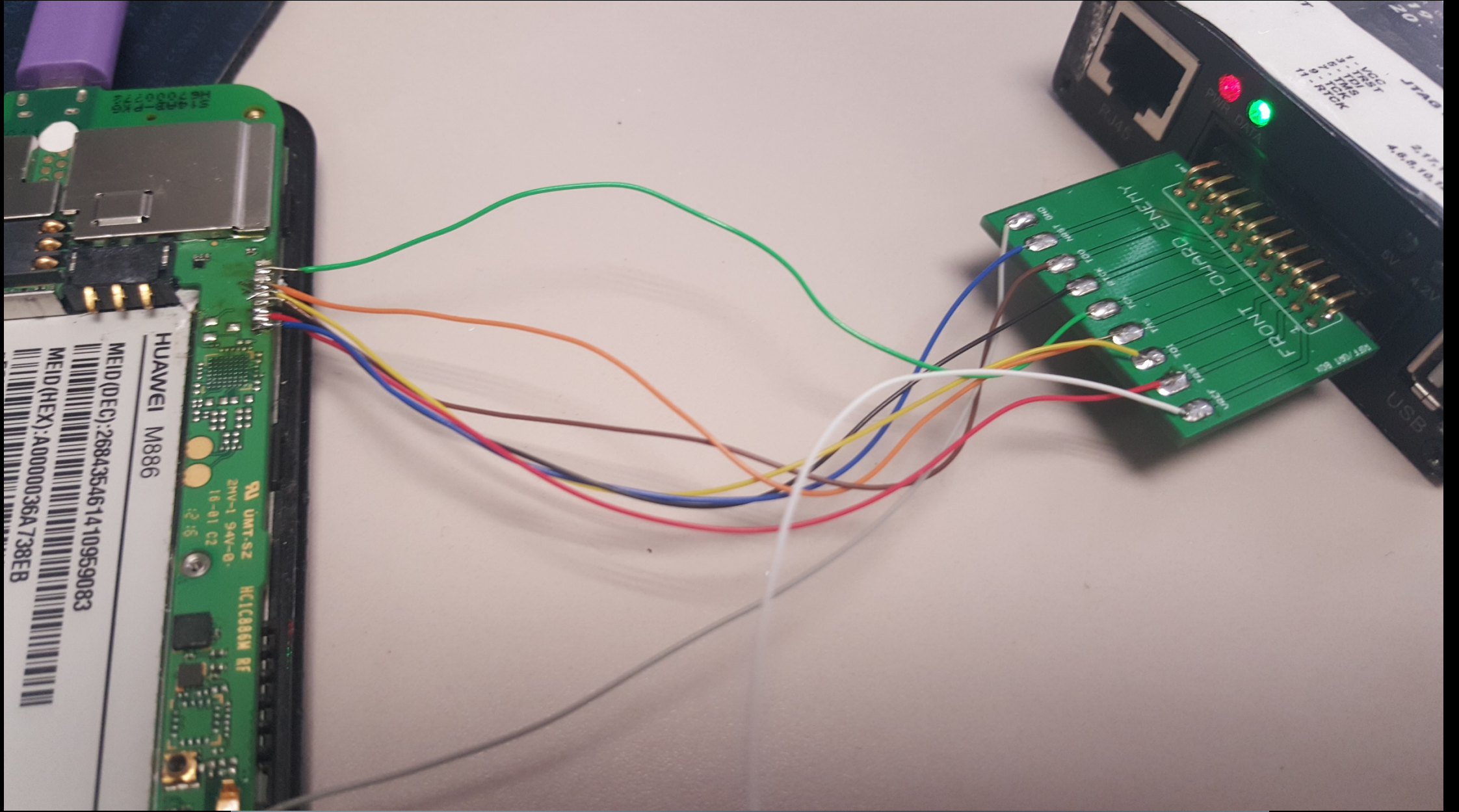
user data

- Calls
- Contacts
- Messaging
- Location data
- E-mails
- Paired devices
- WiFi networks
- Cookies, web history, videos, music, recordings, images, cell towers, account data, visited web pages, bookmarks, notes, notifications, open apps, usage history, powering events, network statistics, a compromising picture you took then deleted, etc...



so you convinced me.. i want the dataz

- JTAG Extraction
- In-System Programming (ISP)
- Chip-Off
 - Originally designed for debugging and testing
 - Dependent on the device's processor
 - Most modern devices can't be dumped with JTAG
 - Mostly limited to feature (burner) and cheaper/older devices
 - Can be quite slow



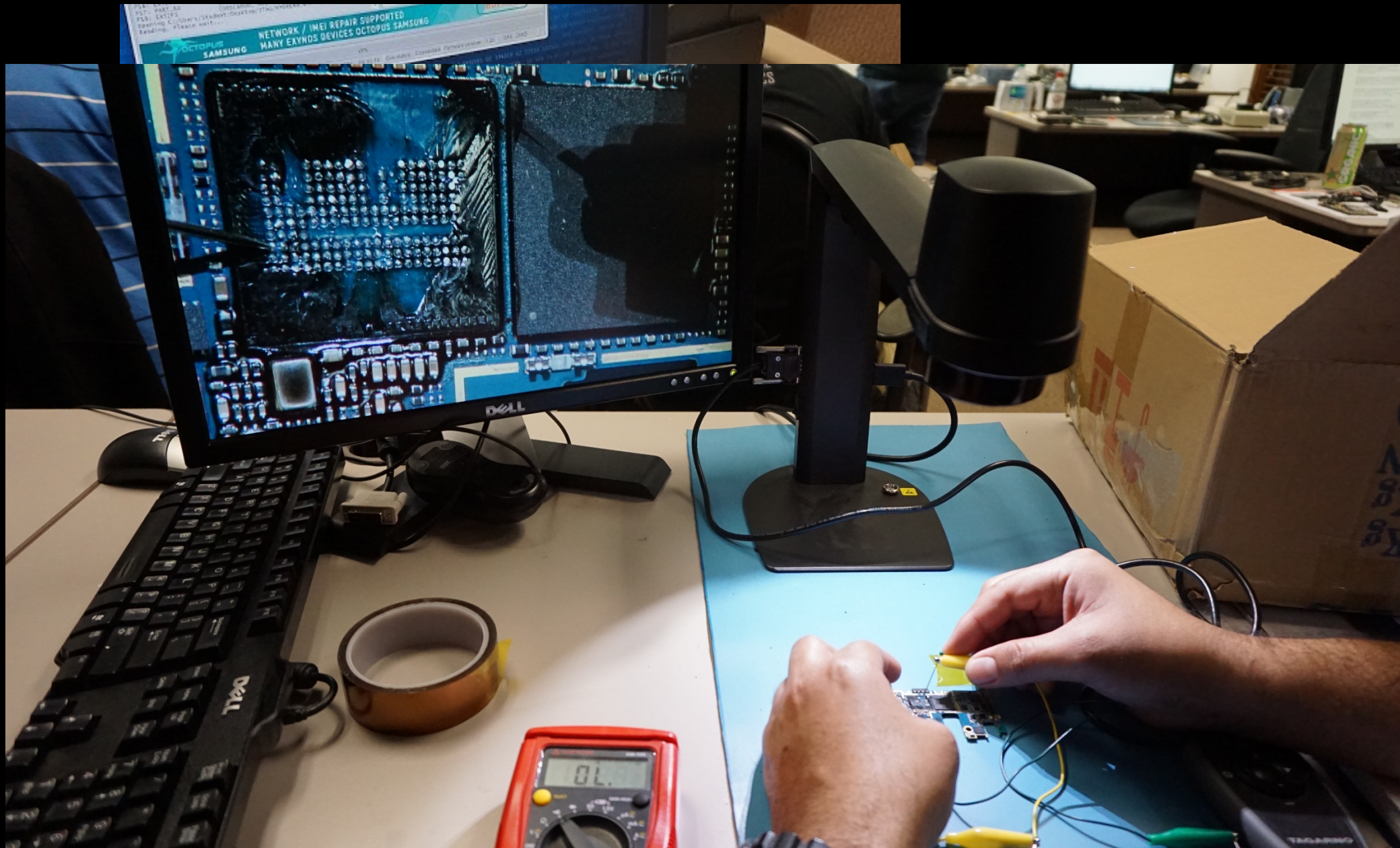
HUAWEI M886
MEID(DEC):268435461410959083
MEID(HEX):A0000036A738EB

UMT-SZ
2HV-1 94V-0
16-01 02

HC1C886W RF

1 - VCC
2 - TXD
3 - RXD
4 - GND

FRONT TOWARD ENETTY
VCC TXD RXD GND



chip-off extraction

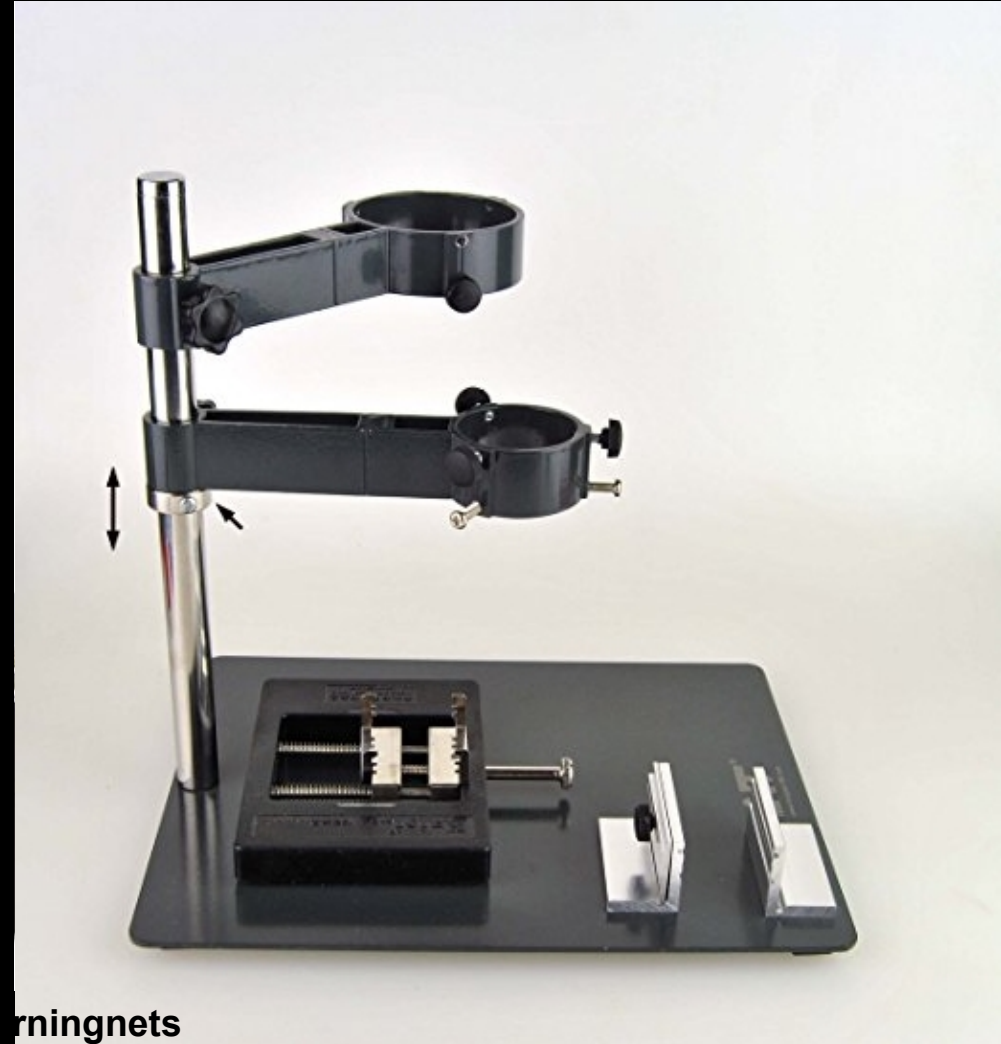
- Most of the time this is the end of the road for a phone
- Phone doesn't have to be working
- Phone can have water damage
- Phone can be almost totally destroyed and still be recoverable
- Thousands of investigators and data-recovery experts are doing chipoff

chip-off extraction methods

- Heat
 - Heat gun
 - Infrared workstation (SMD rework station)
 - Hot air or infrared preheater
- No-Heat (matter subtraction for the intellectuals)
 - Milling
 - Polishing

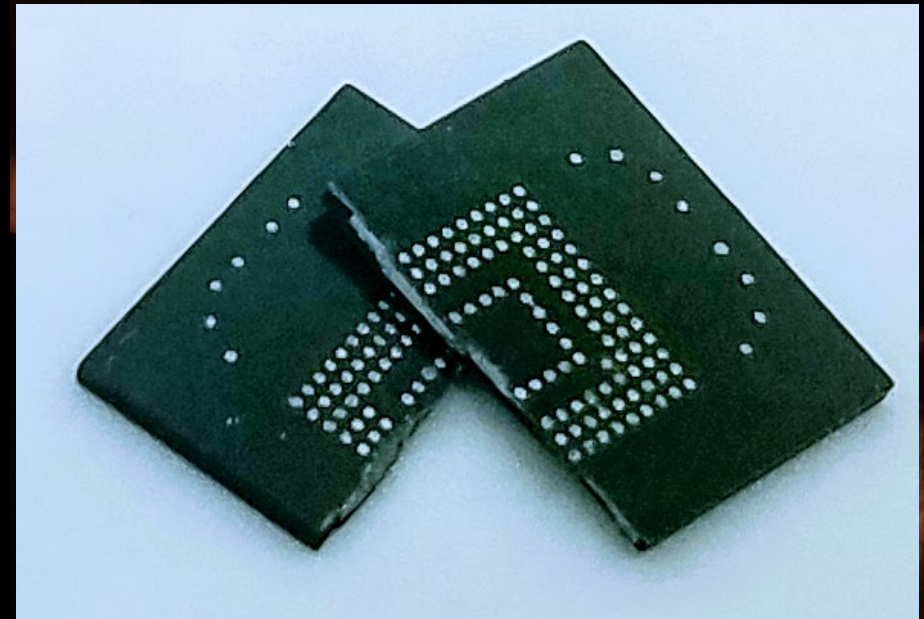
chip-off extraction methods – hot air

- Inexpensive
- Can be fairly safe if done carefully
- Most of us started here
- Can be reversible if you are careful
- Preheat with around 400 deg F, 200 C on the bottom for 5-8 minutes, then hit it with about 850/450 on the top, use a $\frac{3}{4}$ inch flat Xacto blade to lift chip off
- Clean with knife-blade soldering tip with flux, then clean with alcohol, retin if necessary



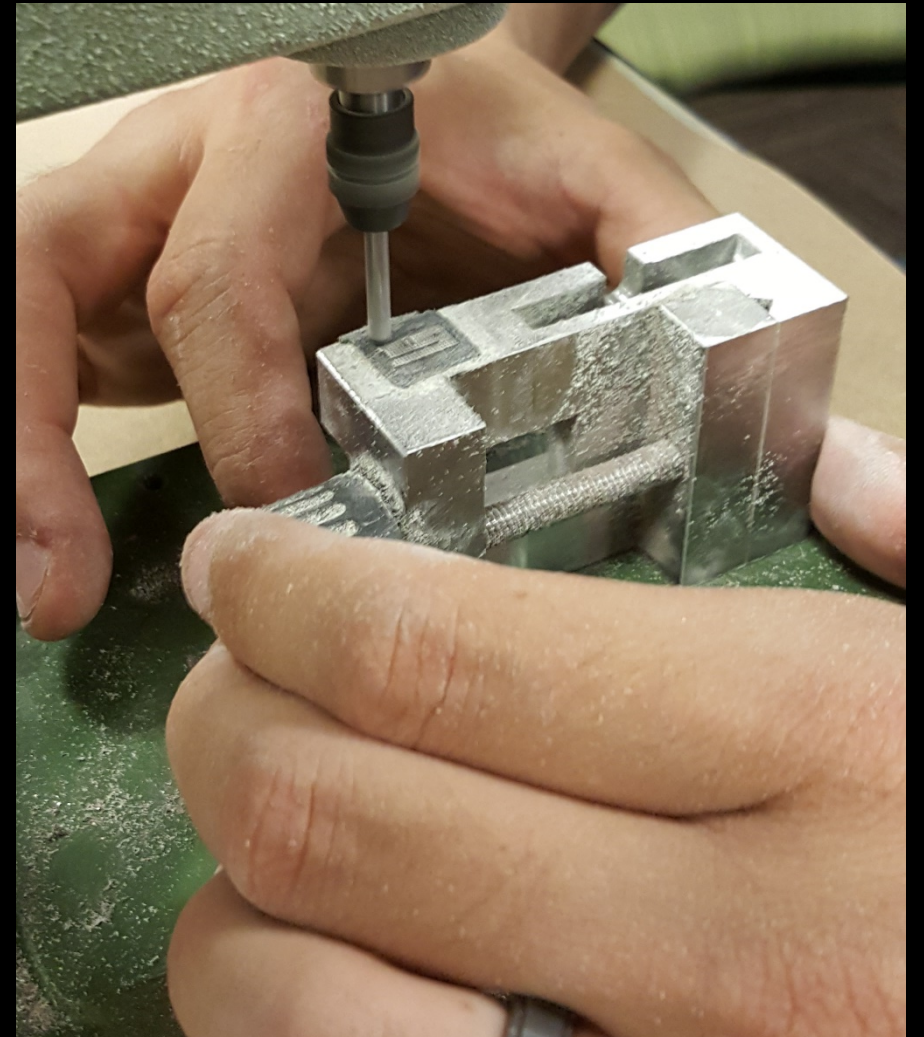
chip-off extraction methods – infrared

- Inexpensive or very expensive
- Is relatively safe with practice
- Can be reversible if you are careful
- Preheat with 200C on the bottom plate for 5-6 minutes, then hit it with top light at about 285C directly on the chip.
- Use Xacto blade to lift off. Don't force it. If you force it... it may break.
- Clean with knife-blade and flux, then alcohol (99% isopropyl or denatured), re-tin if necessary
- T862++ SMD rework station



chip-off extraction methods – milling

- Fairly inexpensive
- Very safe with practice
- Not reversible without some magic
- Can be done with an inexpensive mill
- Cut the board around the chip, then turn it upside down, stick the chip to your milling block with double-sided carpet tape.
- Use 1/8 inch flat-nose milling bit to slowly mill away the PCB material from the backside. Clean up at the end if need be.
- Proxon MF70 mill



chip-off extraction methods - milling



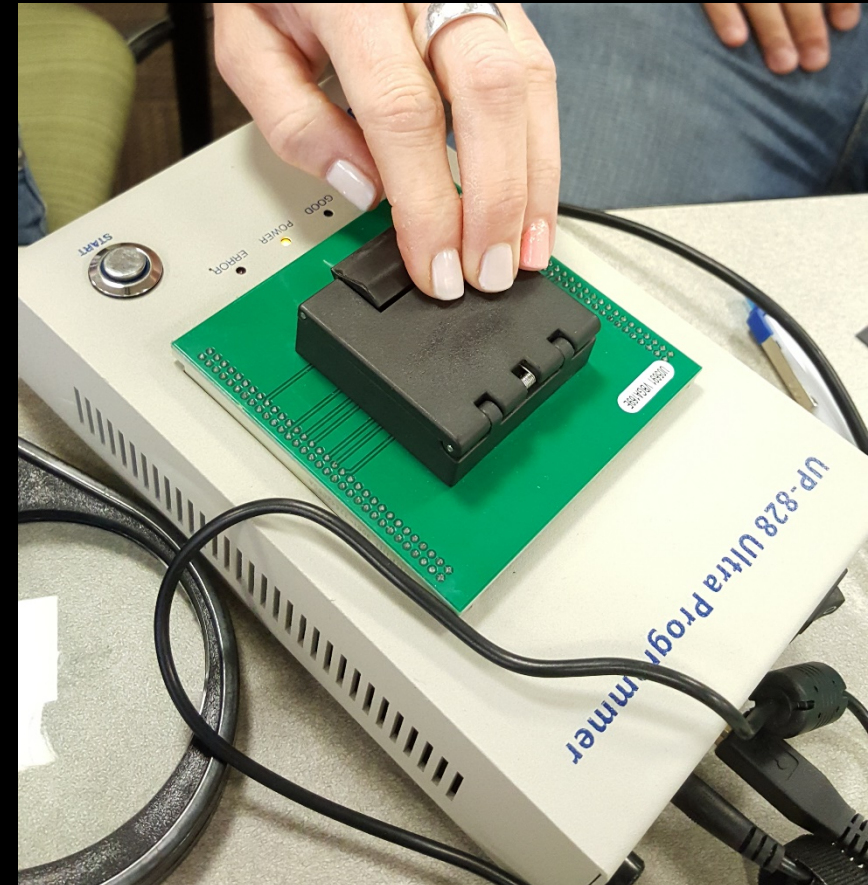
chip-off extraction methods - milling



chip-off readers/adapters/programmers

- UP828P Universal Programmer
- E-Mate Pro eMMC Adapter with Medusa Pro or Octopus Pro Box
- KLD or Sireda Adapters (convert eMMC or eMCP to SD Card slot)
- Dediprog NuProg-E (eMMC and UFS chips)
- Allsocket and others
- Many different brands (Chinese) of readers and programmers

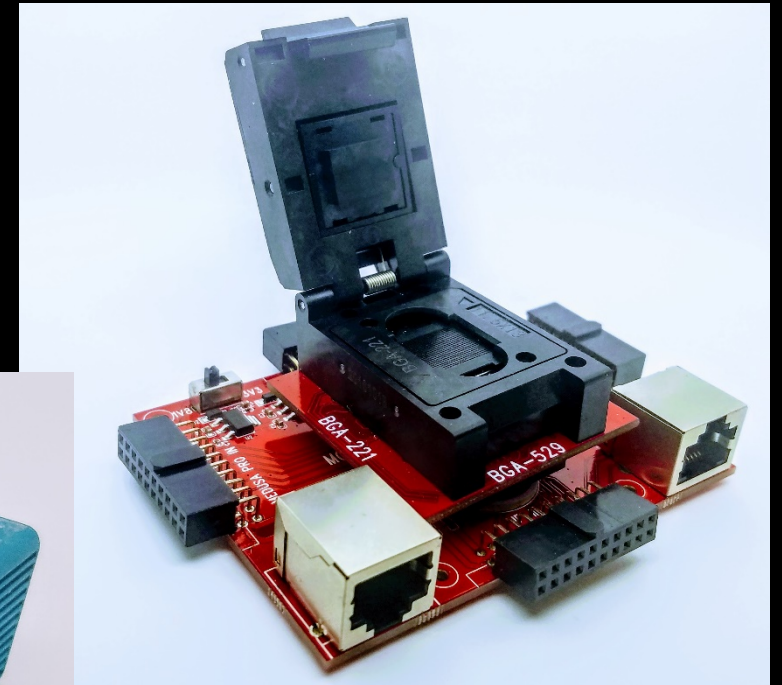
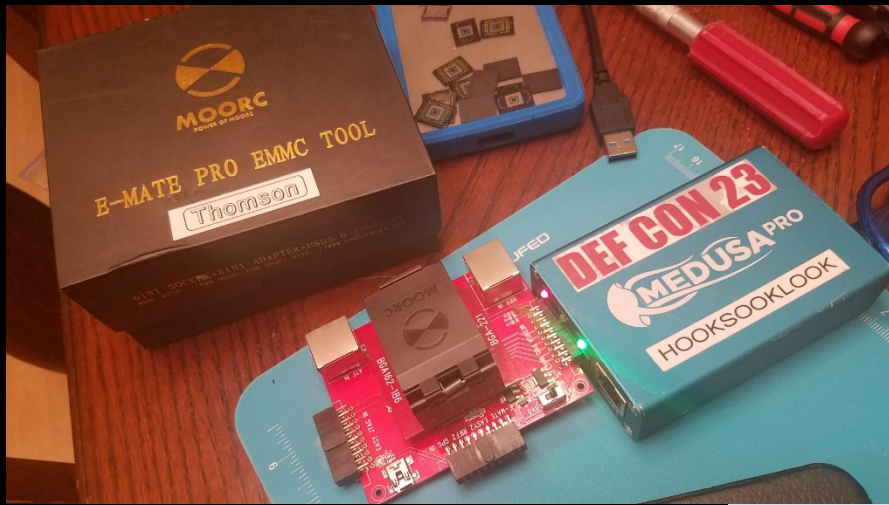
chip-off programmer – UP828P



up48.com

Purpose-built software
downloadable and included

chip-off/ISP box – Medusa Pro & E-mate



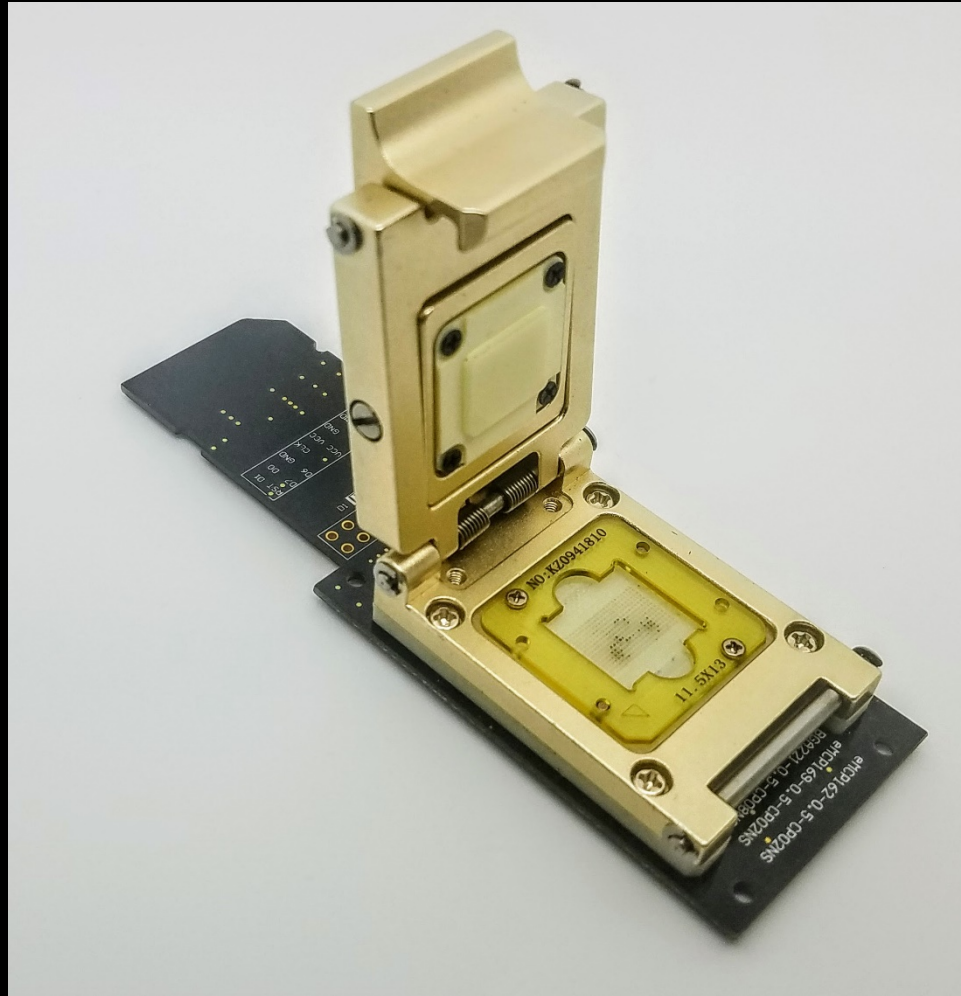
medusabox.com

Purpose-built software
downloadable and included



<https://t.me/learningnets>

chip-off reader/adaptor – KLD - KXT



Uses any disk-imaging software that can read SD cards.

AccessData's FTK Imager is great for this. Use a write blocker if possible too.

chip-off programmer– NuProg-E



www.dediprogram.com

Purpose-built software
downloadable and
included. eMMC and UFS
only (S6 and Note 5)

chip-off equipment

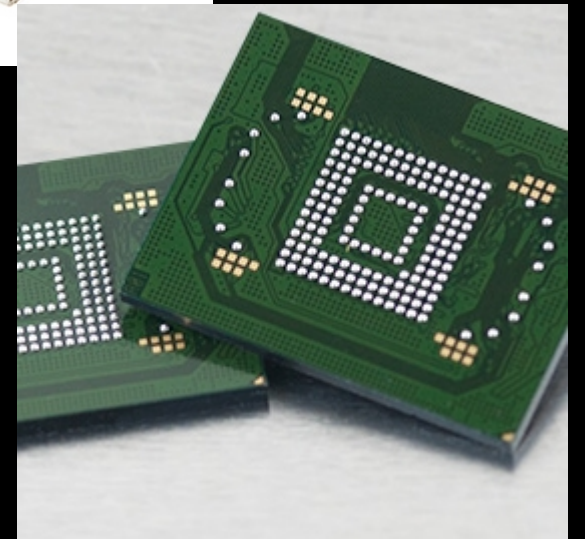
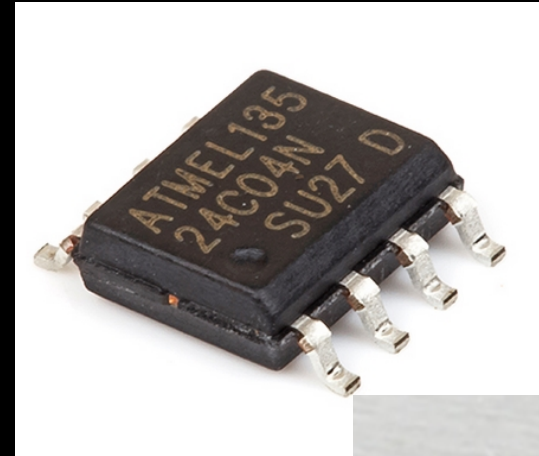
- Call me. I'll sell you all sorts of stuff... seriously. 😊
- gsmserver.com
- fonefunshop.co.uk
- cellcorner.com
- vipprogrammer.com
- amazon.com
- aliexpress.com
- h11dfs.com

The screenshot shows the H-11 Digital Forensics website. The header includes the logo 'H-11 DIGITAL FORENSICS' and navigation links: Home, Solutions, Certified Training, About H-11, and Contact. The main banner features the text 'H-11 Chip-Off Tool Kit' over a dark background with glowing blue lines. Below this, the 'H-11 Mobile Device Chip-Off Standard Lab' is detailed with four categories of equipment:

- ISP JTAG Adapters & Jigs:** Medusa Pro, Micro UART Cable, Optimus Cable, Medusa Pro JIG Adapter, USB AB Cable, and solder boards.
- Readers:** Emate pro EMMC TOOL all in 1 support BGA153/169, BGA162/186, BGA529, BGA-221+SD reader.
- Milling Tools:** Micro Mill, Machine Block, and Milling Bits.
- IR Rework Station:** (Image of the station).

what kinds of chips?

- Serial EEPROMs (CC skimmers, BT headsets, etc.), usually I2C or SPI
- NAND memories (mostly burner phones)
- NOR memories (really cheap Chinese burners)
- UFS memories (S6, Note 5, S7, etc... new phones)
- **eMMC or eMCP memories (still most phones)**
 - also smart devices of other sorts
 - probably 85-90 percent of the devices of interest



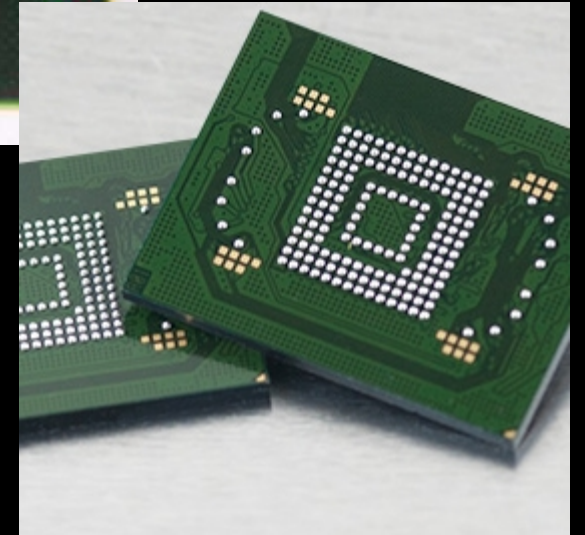
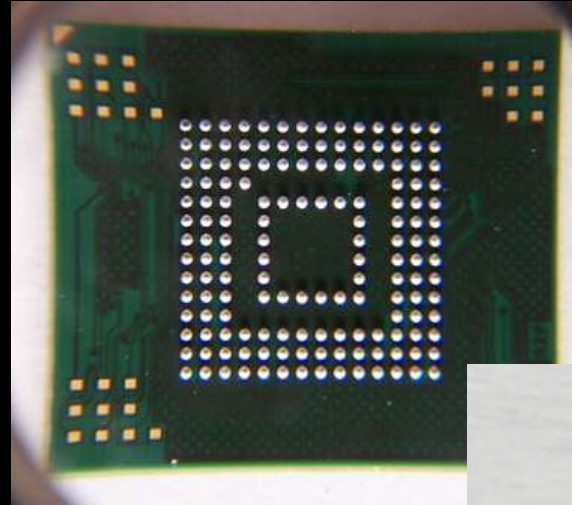
embedded multimedia controller (eMMC)

- Contain a NAND core and an internal (embedded) flash controller
- Easy to use, built to the JEDEC eMMC standard
- For forensics examiners they are easy to decode and parse
- The extraction (dd image) looks just like any other block device, like a hard drive or sd card
- Very similar to monolithic sd cards
- Easy to open the dump in basically any computer-forensics tool, even some of them in 7-zip



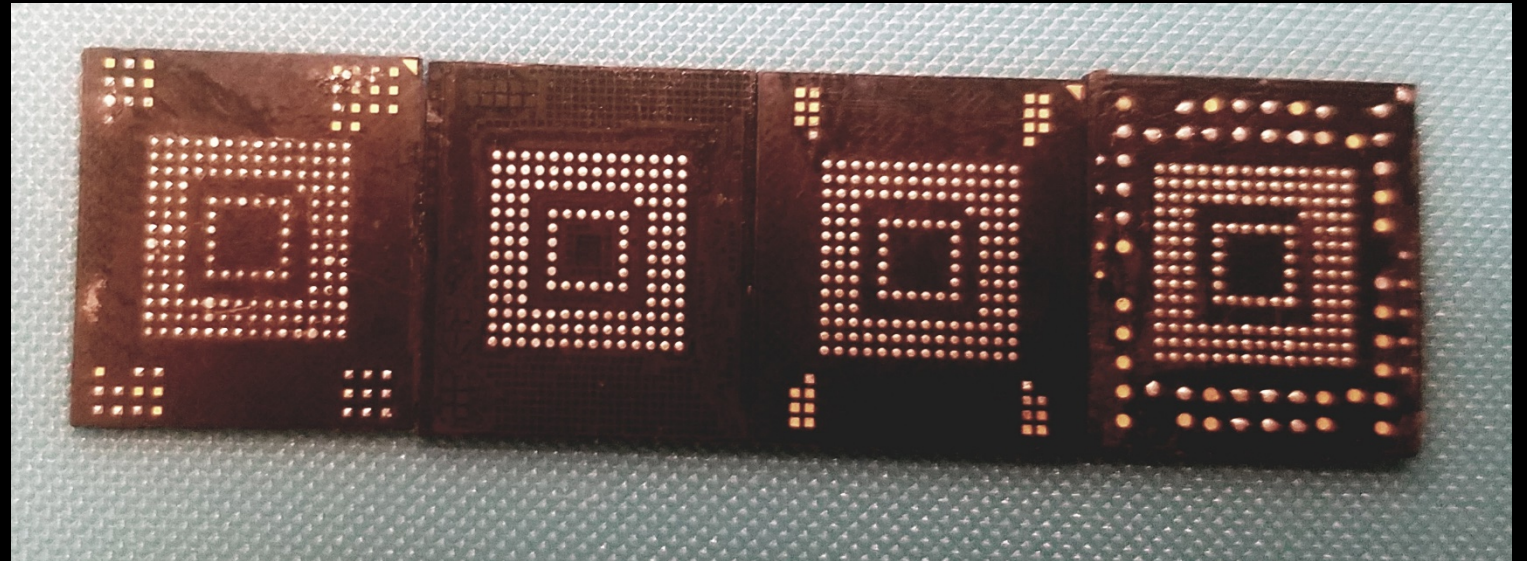
types of eMMC and eMCP – BGA153/169

- Ball-grid Array chip
 - balls of solder on the new chips used to solder the chip to the board
- 153 contacts
 - Only about twenty ish are used
- 169 chip has two semi-arcs of eight pads on each side



types of eMMC and eMCP – BGA153/169

- By far the most common in phones and smart devices
- Five physical sizes; 11.5mmx13mm is the most common

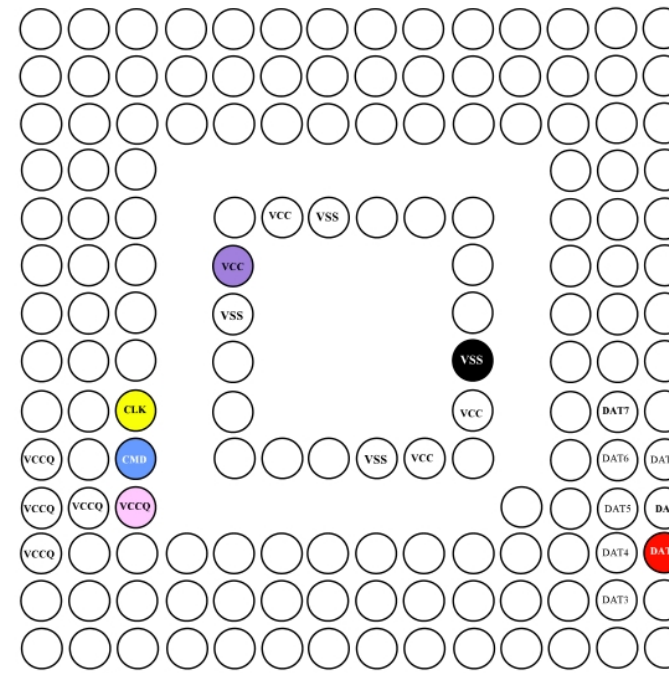
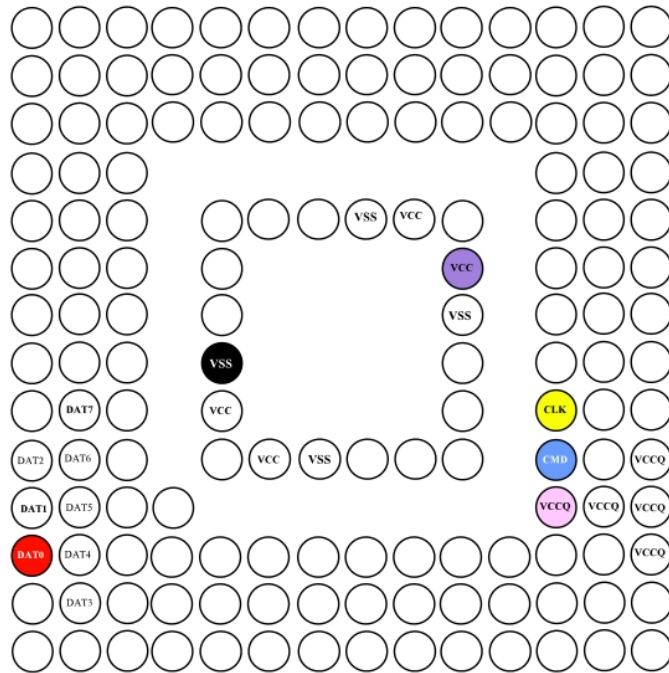


types of eMMC and eMCP – BGA153/169

153/169 BOARD

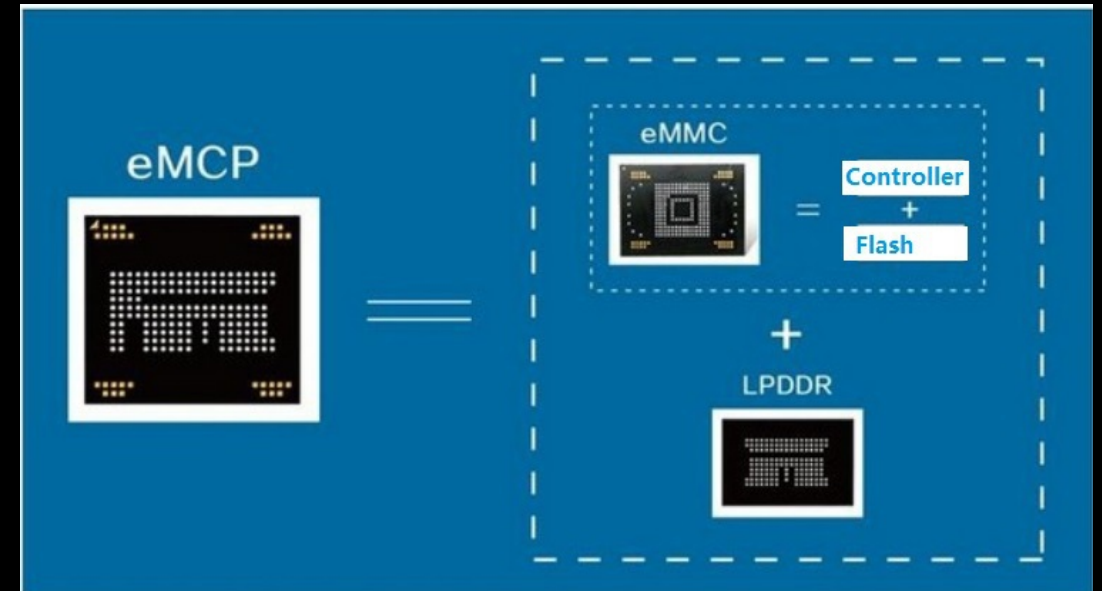
153/169 CHIP

- DATA - DO
- CLK
- CMD
- VCC - 2.8
- VCCQ - 1.8
- VSS - ground



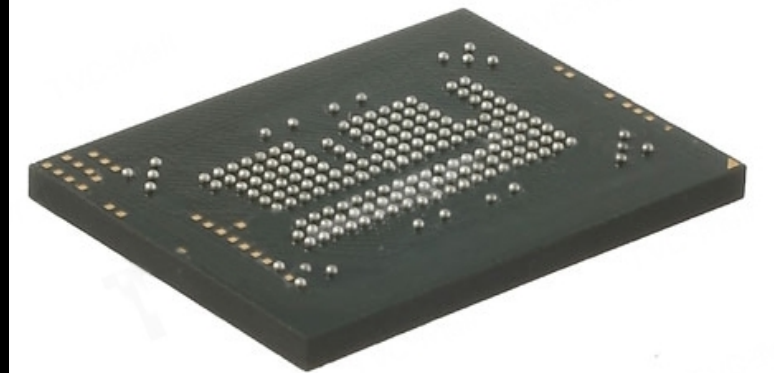
embedded multi-chip package (eMCP)

- Is an eMMC and DDR RAM in one package (MCP)
- Usually found in cheaper phones, such as Chinese garbage phones
- Consists of the BGA162/186 and the BGA221
- The BGA529, while still an eMCP, is super swank, found in nice phones, but not many

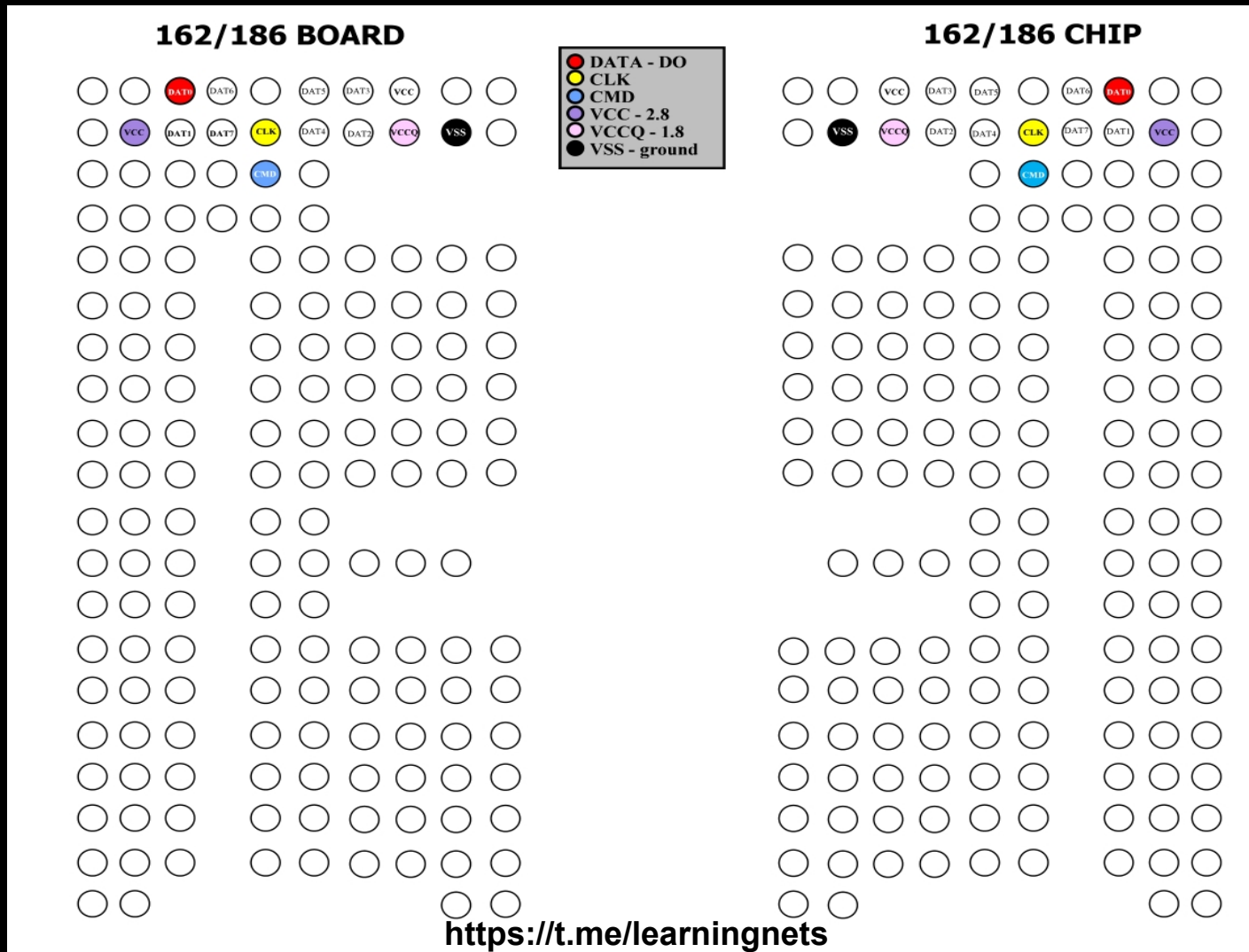


types of eMCP – BGA162/186

- Second most common type of chip
- Two physical sizes, 11.5mmx13mm is the most common, and 12x16 less common
- The smaller one is the 162; the larger one is the 186 (has 24 extra pads in groups of four)

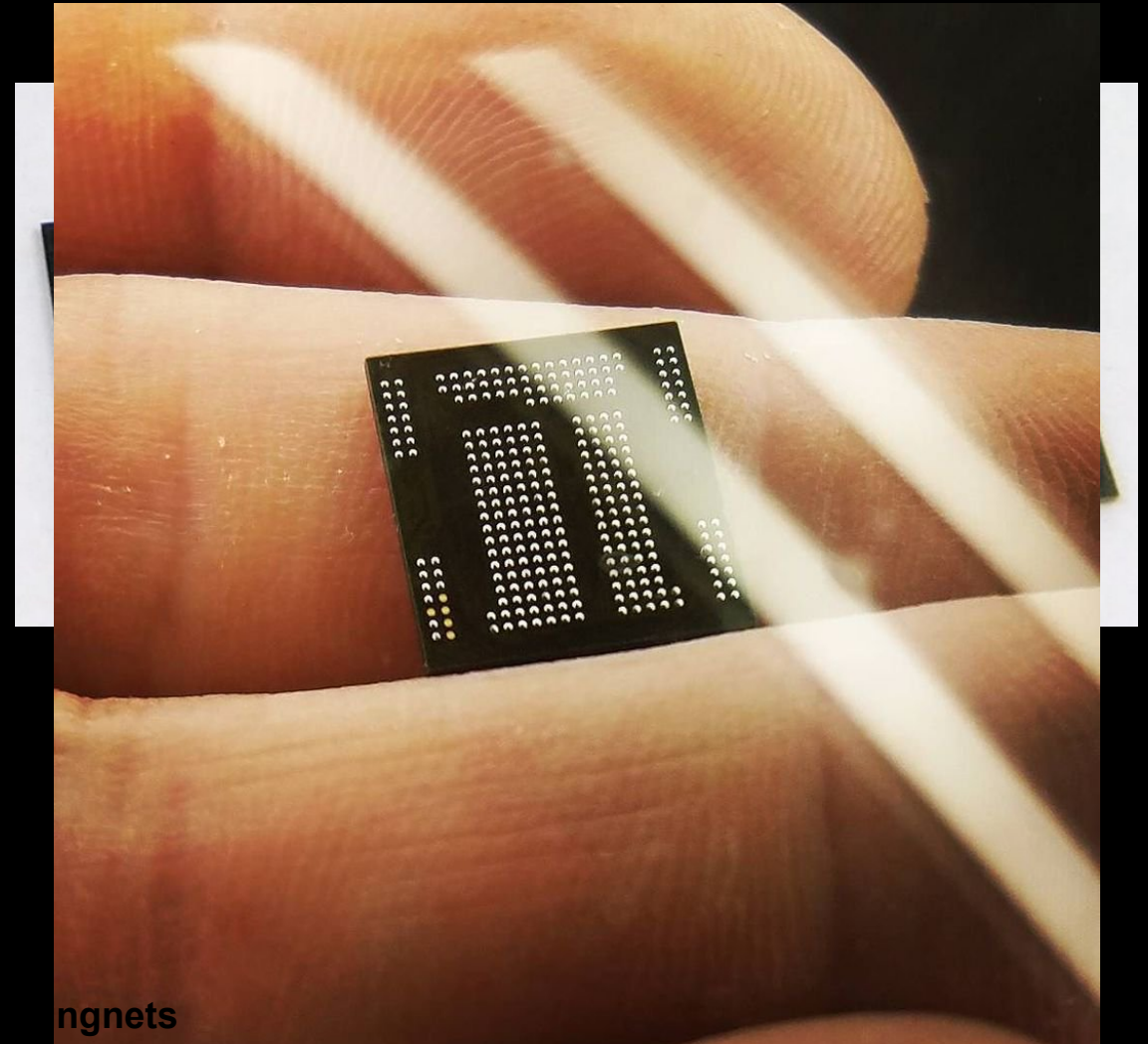


types of eMCP – BGA162/186

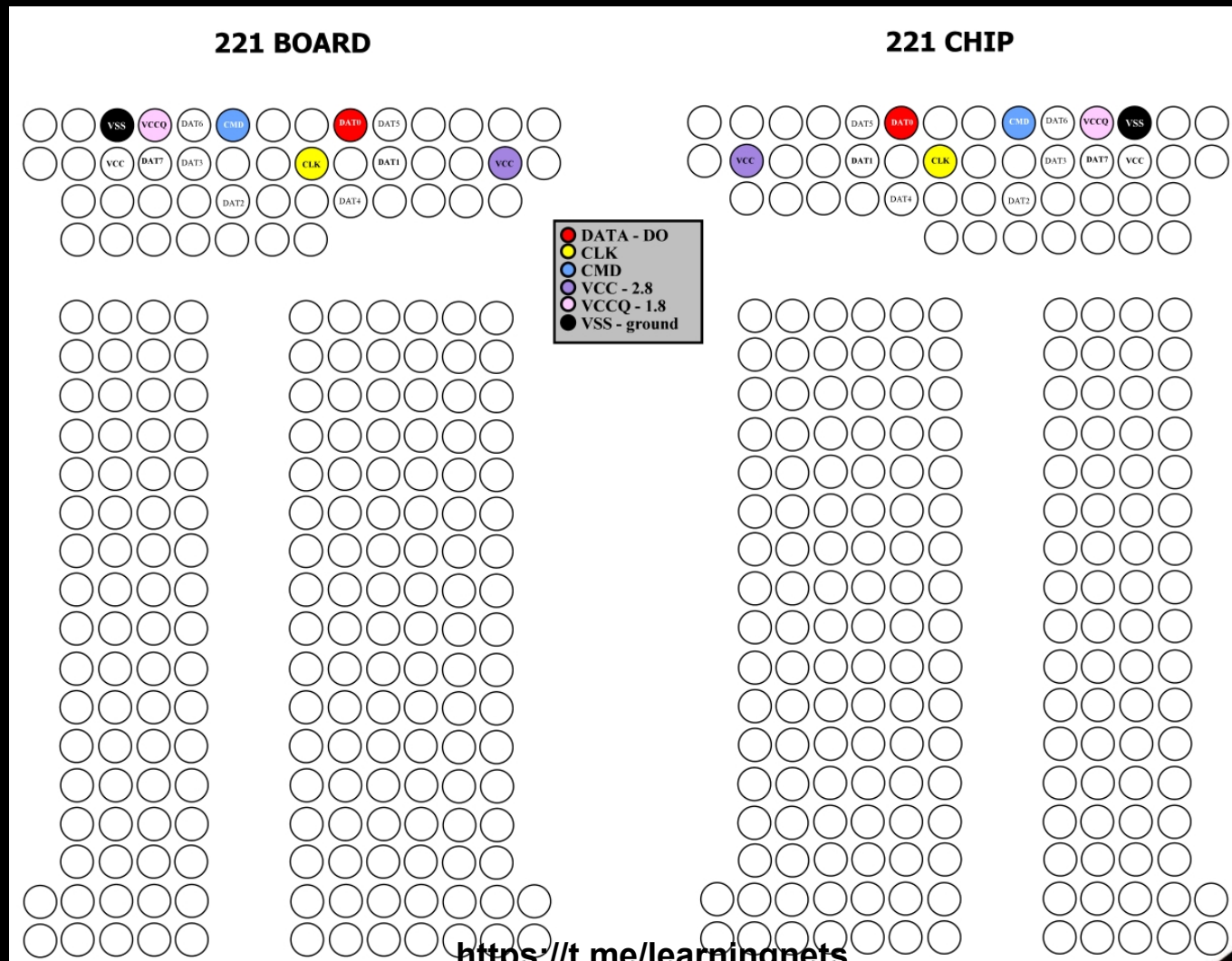


types of eMCP – BGA221

- Third most common chip type in mobile phones and smart devices (Echo Dot for example)
- I've only ever seen one physical size in phones (11.5mmx13mm)
- Looks a Pi or a section of Stonehenge



types of eMCP – BGA221



types of eMCP – 529

529Ball																															
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29		
A	NC	VDDQ_v,c	DQ81_v,c	DQ83_v,c	VSS_v	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	DQ81_v,c	NC		
B	VDD1_v	DQ29_v,c	VSS_v	VDDQ_v	DQ11_v,c	VSS_v	VDDQ_v	VSS_v	DQ4_v,c	VDDQ_v	VSS_v	DQ18_v,c	VDDQ_v	VSS_v	VDDQ_v	DQ28_v,c	VSS_v	VDDQ_v	DQ14_v,c	VSS_v	DQ11_v,c	VSS_v	VDDQ_v	VSS_v	DQ4_v,c	VDDQ_v	VSS_v	DQ18_v,c	VDDQ_v		
C	DQ30_v,c	DQ28_v,c	DQ16_v,c	DQ13_v,c	DQ8_v,c	DQ1_v,c	VREFB_q1,c,d	DQ8_v,c	DQ2_v,c	DQ1_v,c	DQ22_v,c	DQ21_v,c	DQ17_v,c	VDDQ_v	DQ20_v,c	DQ16_v,c	DQ3_v,c	DQ14_v,c	DQ13_v,c	DQ9_v,c	DQ1_v,c	VREFB_q1,c,d	DQ6_v,c	DQ2_v,c	DQ0_v,c	DQ1_v,c	DQ18_v,c	DQ17_v,c			
D	VSS_v	VDDQ_v	DQ24_v,c	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	VSS_v		
E																															
F																															
G	VDDQ_v	DQ27_v,c	DQ25_v,c	VSS_v	DQ12_v,c	DQ8_v,c	VDDQ_v	VSS_v	DQ7_v,c	DQ3_v,c	VSS_v	DQ23_v,c	DQ20_v,c	VDDQ_v	VDDQ_v	VDDQ_v	DQ27_v,c	DQ31_v,c	VSS_v	DQ12_v,c	DQ8_v,c	VDDQ_v	VSS_v	DQ7_v,c	DQ3_v,c	VSS_v	DQ23_v,c	DQ20_v,c	VDDQ_v		
H	DQ31_v,c	VSS_v	VSS_v	DQ14_v,c	DQ10_v,c	VDDQ_v	DM1_v,c	DM0_v,c	VDDQ_v	DQ5_v,c	DQ0_v,c	DM2_v,c	VSS_v	DQ16_v,c	VSS_v	DQ31_v,c	VSS_v	DM5_v,c	DQ15_v,c	DQ10_v,c	VDDQ_v	DM1_v,c	DM0_v,c	VDDQ_v	DQ5_v,c	DQ1_v,c	VSS_v	DQ18_v,c	DQ16_v,c		
J	VDDQ_v	VDDQ_v	VDDQ_v	DM3_v,c	VDDQ_v	VDDQ_v																VSS_m	VCC_m	VSS_m	VDDQ_v	DQ3_v,c	VSS_v	DQ22_v,c	DQ20_v,c		
K	VDDQ_v	DQ19_v,c	DQ18_v,c	VDDQ_v	DQ17_v,c	DQ16_v,c																	VCC_m	D8_m	DQ31_v,c	DQ30_v,c	VDDQ_v	DQ29_v,c	DQ28_v,c	VDDQ_v	
L	VSS_v	DQ21_v,c	DQ20_v,c	VSS_v	VDDQ_v	VSS_v																	DM0_m	DM1_m	VSS_v	VDDQ_v	VSS_v	DQ27_v,c	DQ26_v,c	VSS_v	
M	VDDQ_v	DQ23_v,c	DQ22_v,c	VSS_v	DQ82_v,c	DQ82_v,c																	DAT7_m	DAT6_m	DQ83_v,c	DQ81_v,c	VSS_v	DQ25_v,c	DQ24_v,c	VDDQ_v	
N	VDDQ_v	DQ1_v,c	DQ0_v,c	VSS_v	DM2_v,c	VSS_v																	DAT2_m	VSS_v	DM3_v,c	VSS_v	DQ15_v,c	DQ14_v,c	VDDQ_v		
P	VSS_v	DQ8_v,c	DQ4_v,c	VSS_v	DQ80_v,c	DQ80_v,c																	CLK_m	DQ81_v,c	DQ81_v,c	VSS_v	DQ11_v,c	DQ10_v,c	VSS_v		
R	VDDQ_v	DQ5_v,c	DQ2_v,c	VDDQ_v	DQ7_v,c	DQ6_v,c																	DAT0_m	DQ9_v,c	DQ8_v,c	VDDQ_v	DQ13_v,c	DQ12_v,c	VDDQ_v		
T	VSS_v	DM0_v,c	VREFB_q1,c,d	VDDQ_v	VSS_v	VSS_v																	DAT4_m	VSS_v	VSS_v	VDDQ_v	DQ7_v,c	DM1_v,c	VSS_v		
U	VSS_v	DM1_v,c	DQ1_v,c	VSS_v	VDDQ_v	VDDQ_v	VDDQ_v																DAT1_m	VDDQ_v	VDDQ_v	VSS_v	VREFB_q1,c,d	DM0_v,c	VSS_v		
V	VDDQ_v	DQ11_v,c	DQ10_v,c	VDDQ_v	DQ9_v,c	DQ8_v,c	VDDQ_v																VCC_m	DAT5_m	DQ7_v,c	DQ6_v,c	VDDQ_v	DQ6_v,c	DQ4_v,c	VDDQ_v	
W	VSS_v	DQ15_v,c	DQ14_v,c	VSS_v	DQ81_v,c	DQ81_v,c																	VCC_m	VSS_m	DQ80_v,c	DQ80_v,c	VSS_v	DQ1_v,c	DQ0_v,c	VSS_v	
Y	VDDQ_v	DQ13_v,c	DQ12_v,c	VSS_v	DM3_v,c	VSS_v																	VCC_m	RST_m	VSS_v	DM2_v,c	VSS_v	DQ8_v,c	DQ2_v,c	VDDQ_v	
AA	VDDQ_v	DQ27_v,c	DQ26_v,c	VSS_v	DQ25_v,c	DQ24_v,c																	VDDQ_v	VDDQ_v	VSS_m	DQ23_v,c	DQ22_v,c	VSS_v	DQ21_v,c	DQ20_v,c	VDDQ_v
AB	VSS_v	DQ29_v,c	DQ28_v,c	VSS_v	VDDQ_v	VSS_v	VREFB_q1,c,d	CK_L1_v,c	/	CA3_v,c	VDDCA_v,c	VSS_v	VSS_v	VSS_v	VSS_v	VSS_v	VDDCA_v,c	CAB_v,c	VREFB_q1,c,d	CK_L1_v,c	/	VSS_v	VSS_v	VDDQ_v	VSS_v	VDDQ_v	DQ19_v,c	DQ18_v,c	VSS_v		
AC	VDDQ_v	DQ31_v,c	DQ30_v,c	VDDQ_v	DQ29_v,c	DQ28_v,c	VDDQ_v	CA5_v,c	CK_L2_v,c	CA4_v,c	CA2_v,c	CA1_v,c	CA0_v,c	VSS_v	ZQ_v,c	CAB_v,c	CAB_v,c	CAT_v,c	CAT_v,c	CK_L3_v,c	CK_L3_v,c	VDDQ_v	DQ28_v,c	DQ28_v,c	VDDQ_v	DQ27_v,c	DQ26_v,c	VDDQ_v			
AD																															
AE																															
AF	VDDQ_v	VDD1_v	VDD1_v	VDD2_v	VSS_v	VSS_v	VDDQ_v	VSS_v	VSS_v	VSS_v	VDDQ_v	VDDQ_v	VDD1_v	VDDQ_v	VSS_v	VDDQ_v	VDD1_v	VDDQ_v	VDDQ_v	VDDQ_v	VSS_v	VDDCA_v,c	VDDQ_v	VSS_v	VDDCA_v,c	VSS_v	VDDQ_v	VDD1_v	VDD1_v	VDDQ_v	
AG	VDDQ_v	ZQ_v,c	CAB_v,c	CAB_v,c	CAT_v,c	CAB_v,c	VDDQ_v	VDDCA_v,c	CK_L1_v,c	CA3_v,c	VDDCA_v,c	CA0_v,c	VDD1_v	VDDQ_v	VSS_v	VDDQ_v	VDD1_v	ZQ_v,c	VSS_v	CAT_v,c	CAS_v,c	VDDQ_v	VSS_v	CA4_v,c	CA3_v,c	CA2_v,c	CA1_v,c	CA0_v,c	VDDQ_v		
AH	VSS_v	ZQ_v,c	CAB_v,c	CAB_v,c	CAT_v,c	CAB_v,c	VDDCA_v,c	VSS_v	CA4_v,c	CA2_v,c	CA1_v,c	VDDQ_v	VSS_v	VSS_v	VSS_v	VDDQ_v	CAB_v,c	CAB_v,c	VREFB_q1,c,d	VSS_v	VDDCA_v,c	CK_L1_v,c	CK_L1_v,c	/	CA3_v,c	VDDCA_v,c	CA2_v,c	CA1_v,c	CA0_v,c	VSS_v	
AJ	NC	VSS_v	VSS_v	VDDCA_v,c	VDDCA_v,c	CA5_v,c	VREFB_q1,c,d	CK_L1_v,c	/	CA3_v,c	VSS_v	VSS_v	VSS_v	VSS_v	VSS_v	VDDCA_v,c	VDDCA_v,c	CK_L1_v,c	CK_L1_v,c	/	CA3_v,c	VDDCA_v,c	VSS_v	VSS_v	VSS_v	VSS_v	VSS_v	VSS_v	VSS_v	NC	

[Top View]

Channel A	Channel B
Channel C	Channel D
Power	eMMC
ODT	Ground
ZQ	NC

all the culprits

BGA-153/169



BGA-162 /186



BGA-529



BGA-221




so how's it done?

- Try the automated tools first and other methods that don't involve destruction
- Research the phone
 - Memory type
 - Memory package style (FCC filing, internal photos)
 - Size of the memory (4GB or more it's likely an eMMC or eMCP)
- Disassemble the phone carefully and precisely in order to not damage the flash-memory chip

phone research?

- fccid.io
- fcc.io
- phonescoop.com
- gsmarena.com
- phonedb.net
- google.com

LG G2



Released 2013, September
143g, 8.9mm thickness
<> Android 4.2.2, up to 5.0.2
16/32GB storage, no card slot

2.8%
23,385,728 HITS

2441
BECOME A FAN

5.2"
1080x1920 pixels

REVIEW OPINIONS


LG G4 (CDMA)

Info Photos Reviews 6 News Forum 30

LG's flagship phone for 2015 updates the G3 with an improved 16-megapixel, laser-focusing camera, and a better quad-HD display. The curved design features thin bezels and optional leather back. Other features include a memory card slot, infrared, NFC, removable battery, and multiple TV-output options.

Versions for different networks support different network frequency bands

Offered By:
[Sprint](#) Discontinued
[U.S. Cellular](#) Discontinued
[Verizon Wireless](#) Discontinued



< Previous 1 of 4 Next >



YouTube

disassemble g920v



OnTimeMobile
www.ontimemobile.com



video demo of proper technique



Edit and sick beatz:
Nick Thomson

Looking at the data – Tools

- These tools will parse the file system of most eMMC/eMCP extractions
 - Cellebrite
 - FTK Imager (Free)
 - Magnet Axion
 - Autopsy (FOSS)
 - Medusa Pro or Octopus Pro Software
 - 7-zip... not kidding (Free)

Looking at the data – Cellebrite Physical Analyzer

The screenshot displays the Cellebrite Physical Analyzer interface. At the top, the menu bar includes 'UFED Physical Analyzer', 'File', 'View', 'Tools', 'Extract', 'Python', 'Plug-ins', 'Report', and 'Help'. The main window is divided into several sections:

- Data Files:** A sidebar on the left lists various data categories with their counts and sub-counts:
 - Applications (1143) (51)
 - Audio (93) (9)
 - Configurations (39)
 - Databases (320) (1)
 - Documents (1)
 - Images (9946) (610) (356 known files)
 - Text (1454) (642)
 - Videos (298) (28)
 - Uncategorized (8623) (6334)
- Summary:** A central pane showing a 'Legacy' report for 'ZTE ZTEP740G'. It includes fields for 'Extraction start date/time' and 'Extraction end date/time'. Below this, a table lists device details:

Vendor	ZTE	settings.db : 85016 / 0x14C18
Model	4.1.2	build.prop : 491 / 0x1EB
	Z740G	build.prop : 283 / 0x11B
	ZTE/P823A01_AIO/metis:4.1.2/JZO54K/20151023.122424...	build.prop : 468 / 0x1D4
		build.prop : 1026 / 0x402
		CheckinService.xml : 1585 / 0x631
		CheckinService.xml : 1564 / 0x61C
- Device Information:** A table at the bottom provides system details:

Phone Activation Time	2014-09-02 22:43(UTC+0)
Locale language	en
Country Name	US
Time Zone	America/Denver
Mock locations allowed	False
Auto Time Zone	True
Auto Time	True
Advertising Id	
- Analized Data:** A sidebar on the right lists analyzed data categories:
 - Bluetooth Devices (1)
 - Calendar (17) (17)
 - Call Log (548) (48)
 - Chats (89) (42)
 - Contacts (122) (2)
 - Cookies (1653) (403)
 - Device Locations (459)
 - Locations (459)
 - Device Users (1)
 - Emails (51) (22)
 - Installed Applications (298) (3)
 - MMS Messages (5) (5)
 - Passwords (29)
 - Powering Events (52) (44)
 - Searched Items (338) (15)
 - SMS Messages (121) (121)
 - User Accounts (16)
 - User Dictionary (30)
 - Web Bookmarks (8)
 - Web History (289) (35)
 - Wireless Networks (490)

Looking at the data – Autopsy

The screenshot shows the Autopsy 4.5.0 interface. The top menu bar includes 'Case', 'View', 'Tools', 'Window', and 'Help'. Below the menu is a toolbar with buttons for 'Add Data Source', 'View Images/Videos', 'Timeline', 'Generate Report', and 'Close Case'. The main window is divided into three panes. The left pane shows a tree view of 'Data Sources' with 'zte.bin' selected, and 'Views' including 'File Types', 'Deleted Files', 'MB File Size', and 'Results'. The 'Results' pane is expanded to show 'Extracted Content' with various categories like 'Call Logs (500)', 'Contacts (46)', 'EXIF Metadata (160)', 'Extension Mismatch Detected (371)', 'GPS Trackpoints (1)', 'Web Bookmarks (1)', 'Web Cookies (6)', 'Keyword Hits', and 'Email Addresses (5556)'. The right pane shows a 'Listing' for '/img_zte.bin' with a table view. The table has columns for 'Name', 'ID', and 'Starting Sector' and lists 19 volumes.

Name	ID	Starting Sector
vol5 (sbl2: 32768-49151)	5	32768
vol6 (sbl3: 49152-65535)	6	49152
vol7 (rpm: 65536-81919)	7	65536
vol8 (tz: 81920-98303)	8	81920
vol9 (ztelk: 98304-114687)	9	98304
vol10 (ztecfcg: 114688-131071)	10	114688
vol11 (persist: 131072-180223)	11	131072
vol12 (ssd: 180224-196607)	12	180224
vol13 (fsg: 196608-212991)	13	196608
vol14 (modemst1: 212992-229375)	14	212992
vol15 (modemst2: 229376-245759)	15	229376
vol16 (about: 245760-262143)	16	245760
vol17 (modem: 262144-409599)	17	262144
vol18 (boot: 409600-442367)	18	409600
vol19 (recovery: 442368-475135)	19	442368

Looking at the data – FTK Imager

The screenshot displays the AccessData FTK Imager 4.2.0.13 interface. The 'Evidence Tree' on the left shows a hierarchy starting with 'cache (21) [304MB]' and 'userdata (22) [2088MB]'. Under 'userdata', there is a folder 'NONAME [ext4]' containing a '[root]' folder. The '[root]' folder contains several subfolders: 'anr', 'app', 'app-asec', 'app-private', 'audio', 'backup', 'bms', 'dalvik-cache', and 'data'. The 'data' folder is expanded, showing a list of application-specific folders such as 'cn.com.zte.settings.patch', 'cn.wps.moffice_i18n', 'cn.zte.music', 'cn.zte.recorder', 'com.android.backupconfirm', 'com.android.bluetooth', and 'com.android.browser'.

The 'File List' on the right shows a table of files and folders. The columns are 'Name', 'Size', and 'Type'. The files listed are all folders with a size of 4 and a type of 'Direct'.

Name	Size	Type
cn.com.zte.settings.p...	4	Direct
cn.wps.moffice_i18n	4	Direct
cn.zte.music	4	Direct
cn.zte.recorder	4	Direct
com.android.backupc...	4	Direct
com.android.bluetooth	4	Direct
com.android.browser	4	Direct
com.android.calculat...	4	Direct
com.android.calendar	4	Direct
com.android.Calenda...	4	Direct
com.android.certinsta...	4	Direct
com.android.chrome	4	Direct
com.android.contacts	4	Direct
com.android.Contact...	4	Direct
com.android.defcont...	4	Direct
com.android.email	4	Direct

Looking at the data – Octopus/Medusa

The screenshot shows the 'Content extractor' application window. The main area displays a file tree under 'Image content'. The tree is expanded to show the 'misc' directory, which contains several sub-directories and files. The 'bluetooth' directory is expanded, showing the 'bt_config.xml' file selected. The file properties panel on the right shows details for 'bt_config.xml'.

Image content

Parse user data only (uncheck it for non-Android OS) Show empty volumes Show deleted data

Name	Size	Type
misc		Directory
adb		Directory
bluetooth		Directory
bt_config.xml	1377	file
bluetooth		Directory
keystore		Directory
keychain		Directory
net		Directory
radio		Directory
sms		Directory
zoneinfo		Directory
vpn		Directory
shared_relo		Directory
systemkeys		Directory
wifi		Directory
sockets		Directory
wpa_supplicant		Directory
softap.conf	45	file
p2p_supplicant.c...	445	file
wpa_supplicant.c...	365	file
entropy.bin	21	file

Image

Cancel

Read from file...

Close

Actions

Extract...

Find...

Search contacts...

Search SMS...

Search media...

File properties

Name: bt_config.xml

Path: userdata/misc/bluetooth

Size: 1377

Type: File

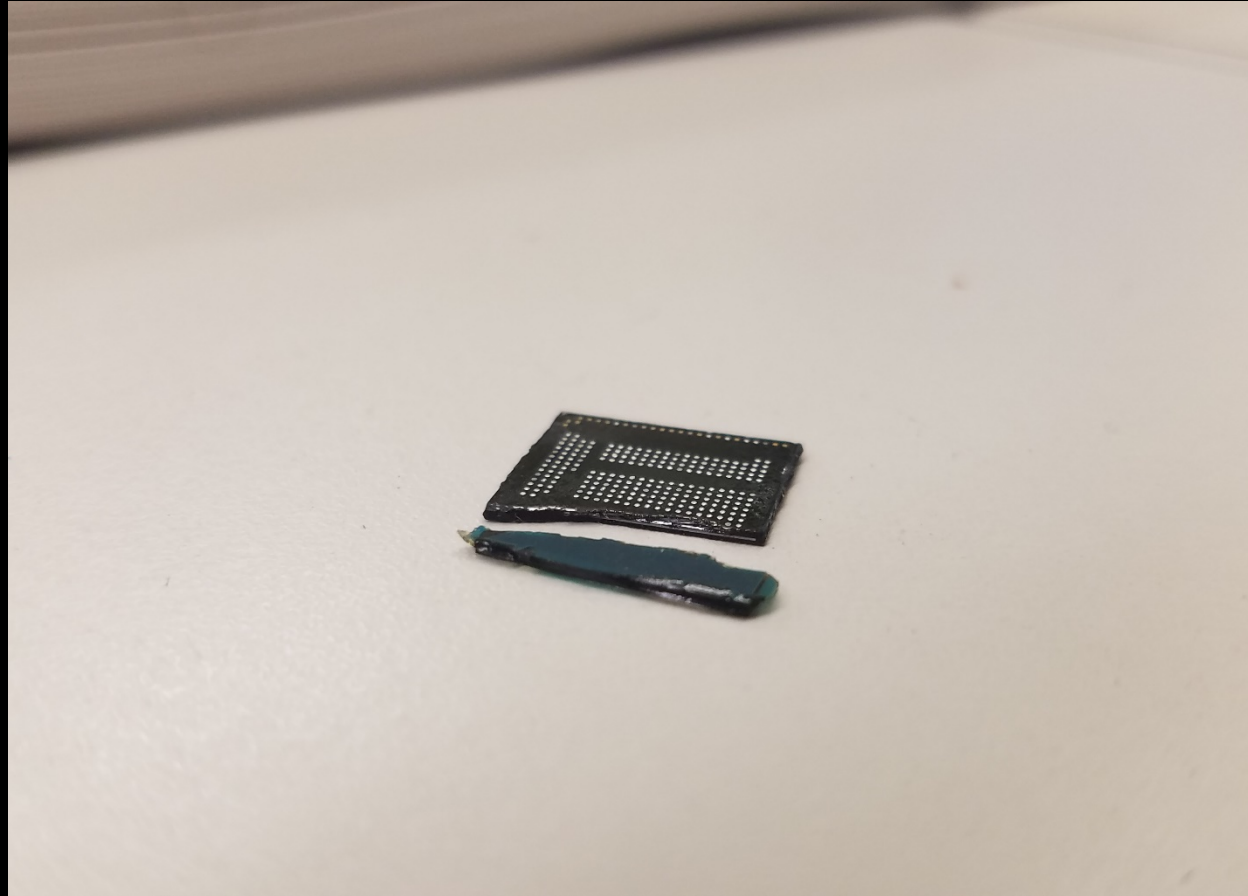
success stories

- Suspect “tacoed” his phone while being arrested for burglary and aggravated assault – HTC Desire 510



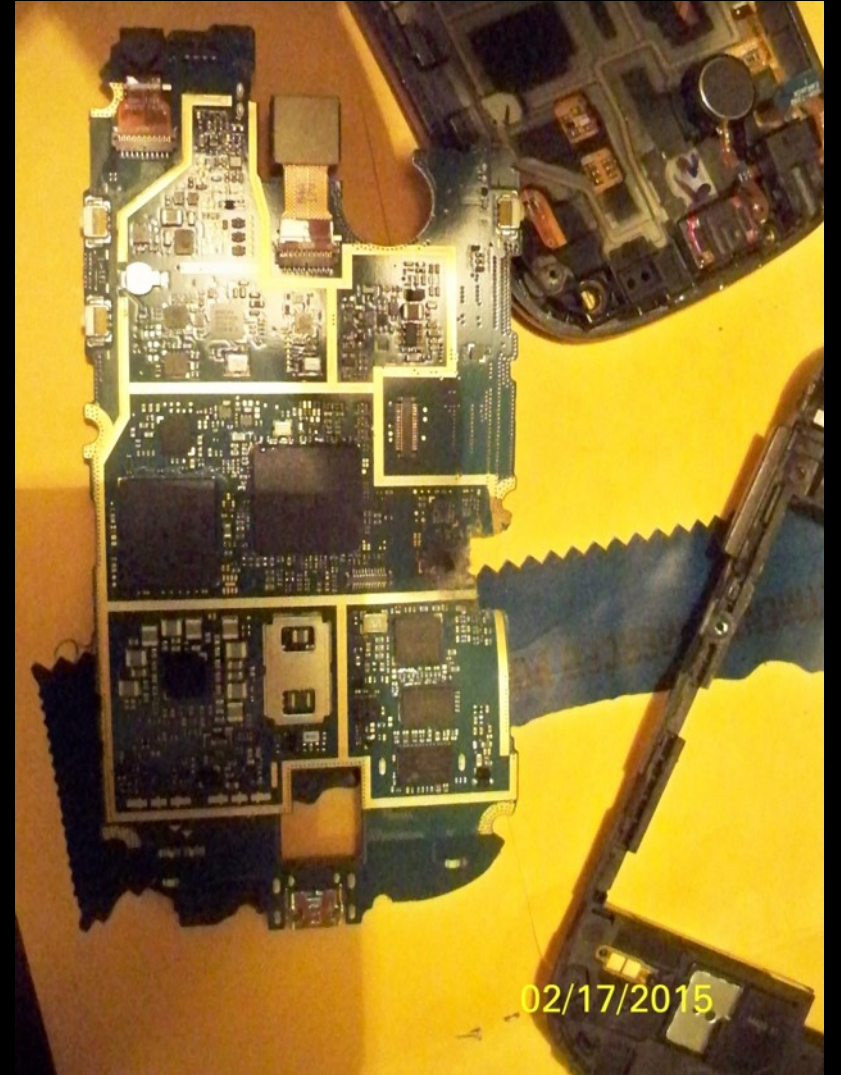
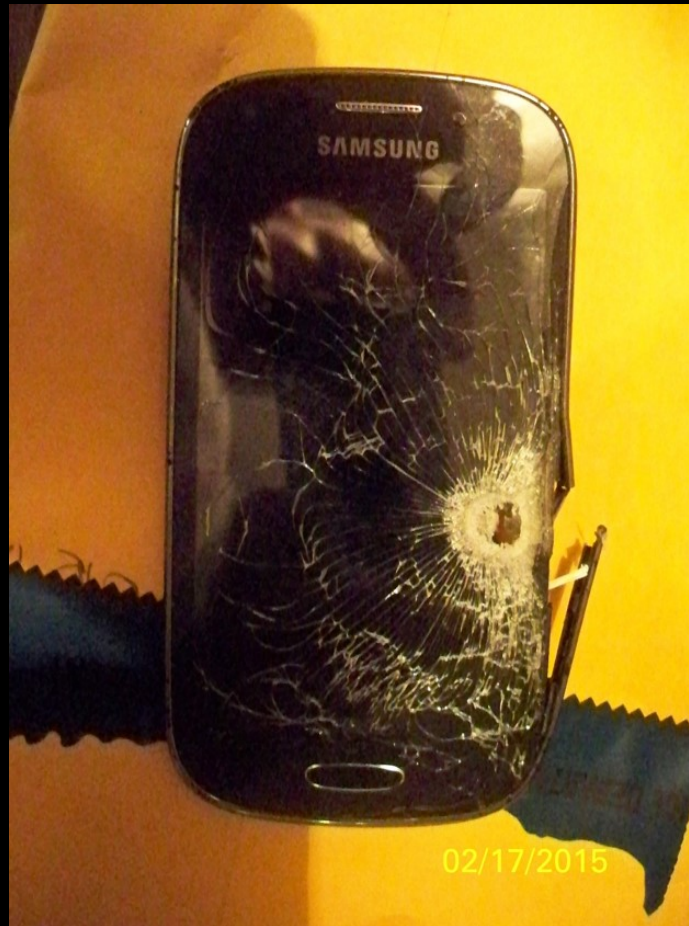
success stories

- Suspect was behaving inappropriately with his stepdaughter. He broke her phone to avoid the data falling into authorities' hands.
- He almost did a good job destroying the phone. Almost.
- ZTE Z828



success stories

- Armed robbery with an Uzi. Phone was shot through. Good thing the bullet missed the chip.
- Samsung SGH-T599N





recommended equipment to do it cheap

- Wagner HT3500 hot-air gun - \$45
- Weber Displays hot-air gun holder - \$60 (or get a friend)
- Medusa Pro Box / E-mate Pro Adapter Combo \$239 (gsmserver.com)
- Variable-temp soldering iron for chip cleaning with knife-tip \$40-\$200
- Autopsy, FTK Imager and DB browser for SQLite \$0
- Solder paste, flux, etc...
- Buy yourself a lot of broken phones on eBay or find a recycler or “borrow” your friends’ phones

Summary

- Smashing the screen does little to nothing to destroy the data on the screen
- Most phones, assuming they aren't encrypted, can be extracted using chip-off techniques
- You can do chip-off for a couple hundred bucks
- TV and movies lie
- @ArdJect on Twitter
- kim@h11dfs.com for official things