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

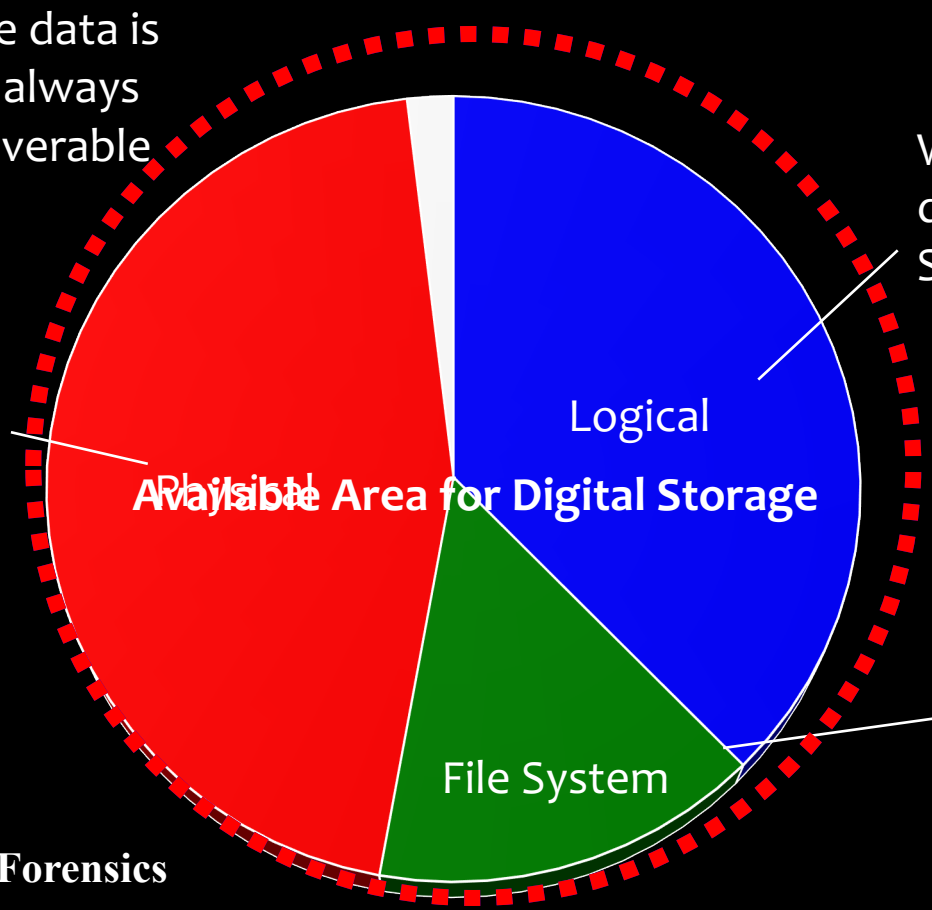
```
    </N2>
</N1>
<N2 Tag="Remote">
    <N1 Tag="60:b1:2d:75:95:fd">
        <N1 Tag="Timestamp" Type="int">1451602321</N1>
        <N2 Tag="DevClass" Type="int">7936</N2>
        <N3 Tag="DevType" Type="int">3</N3>
        <N4 Tag="AddrType" Type="int">1</N4>
    </N1>
    <N2 Tag="38:01:95:8d:a2:da">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

```
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
1274-1000
4160-1000
3426-1000
```

```
chbox/com.google.android.voicesear
ch.ime.VoiceInputMethodService.?..
!+android_idcca7d207f52f397$>..E.s
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
```

- Straight hexadecimal
- Flash memory storage cha
- 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 possibly 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

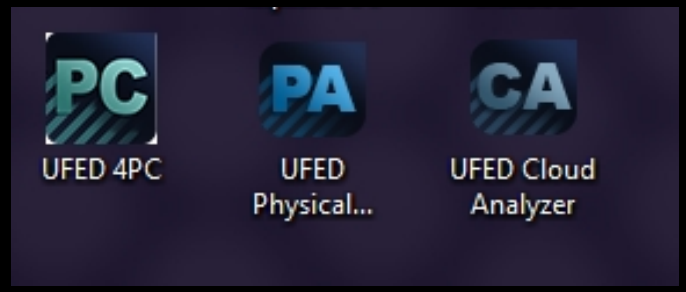
- Factory Reset Protection (FRP) locks
- Inability to root the device, even temporarily
- Inability to flash unsigned code to device (bootloaders)
- Damaged devices
  - Broken screens
  - Broken ports
  - Water damage
  - Destroyed or tacoed phones

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 mmcblko 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?

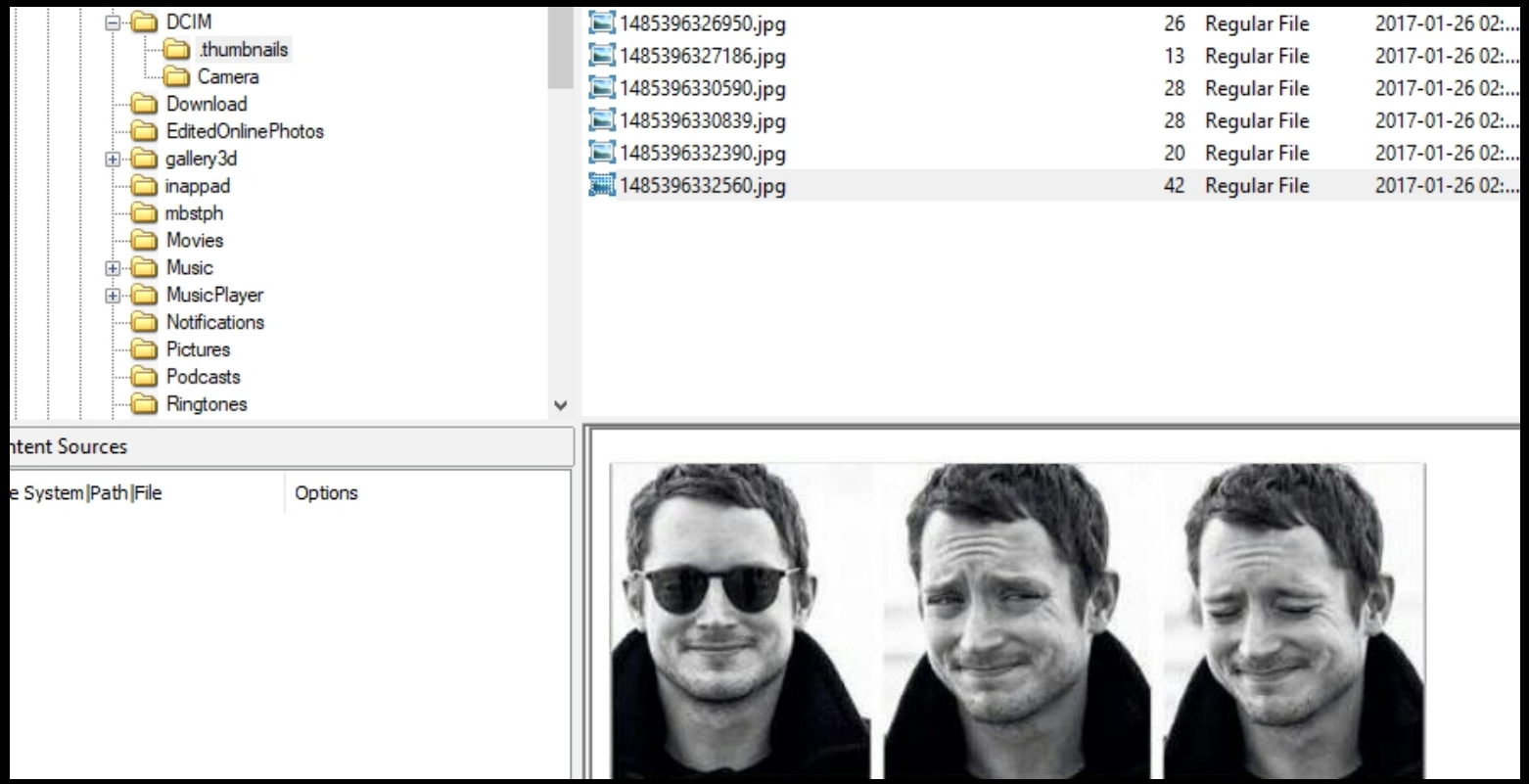
- AccessData FTK Imager (free)
  - http://marketing.accessdata.com/ftkimager4.2.0
- Medusa Pro or Octoplus Pro Software (about 160 bucks)
- Autopsy and Sleuthkit (FOSS)
- Cellebrite Physical Analyzer (paid)
- Oxygen Detective (paid)
- Magnet Axiom (paid)

how do we see 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 Axiom (paid)

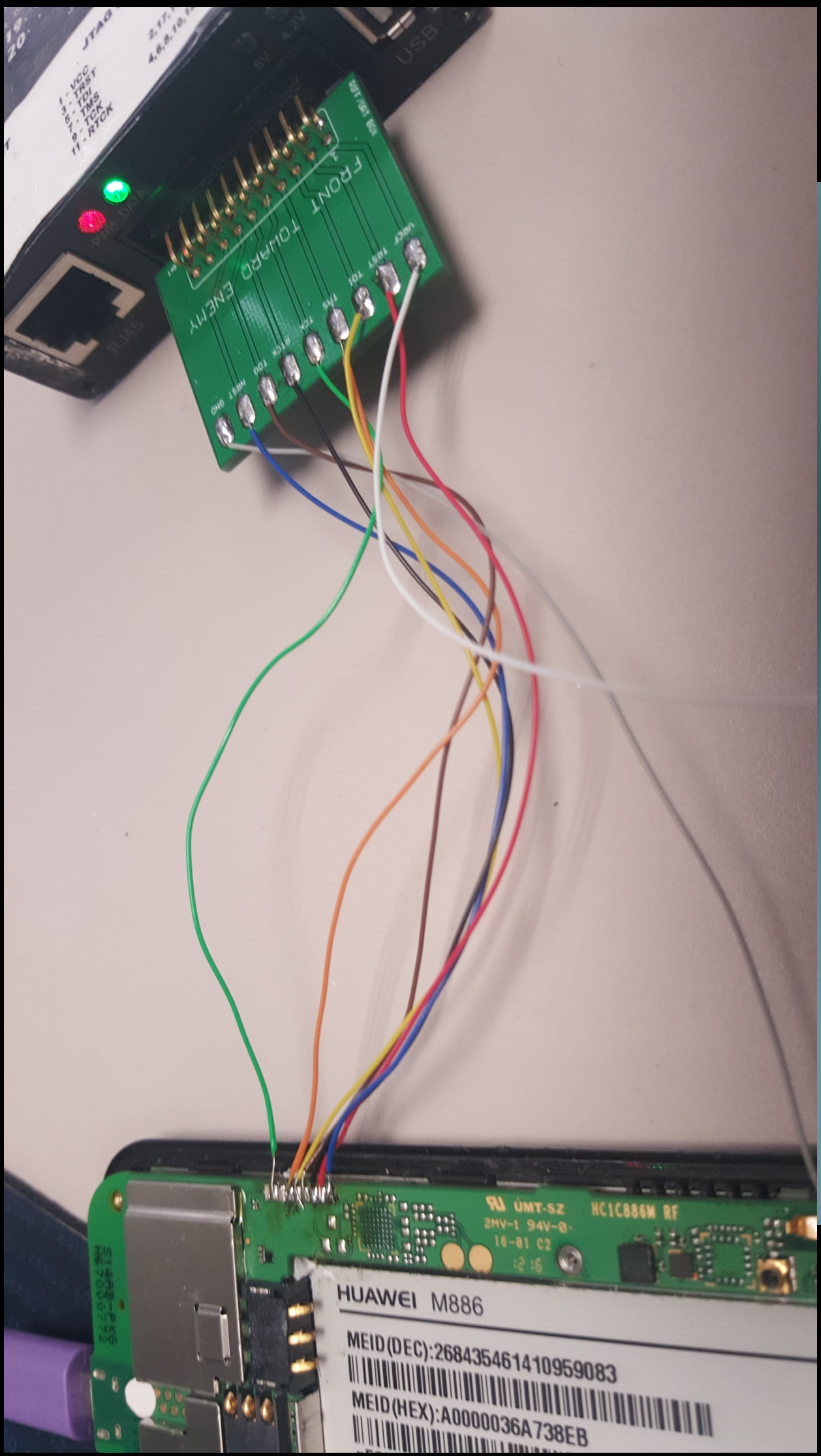
user data

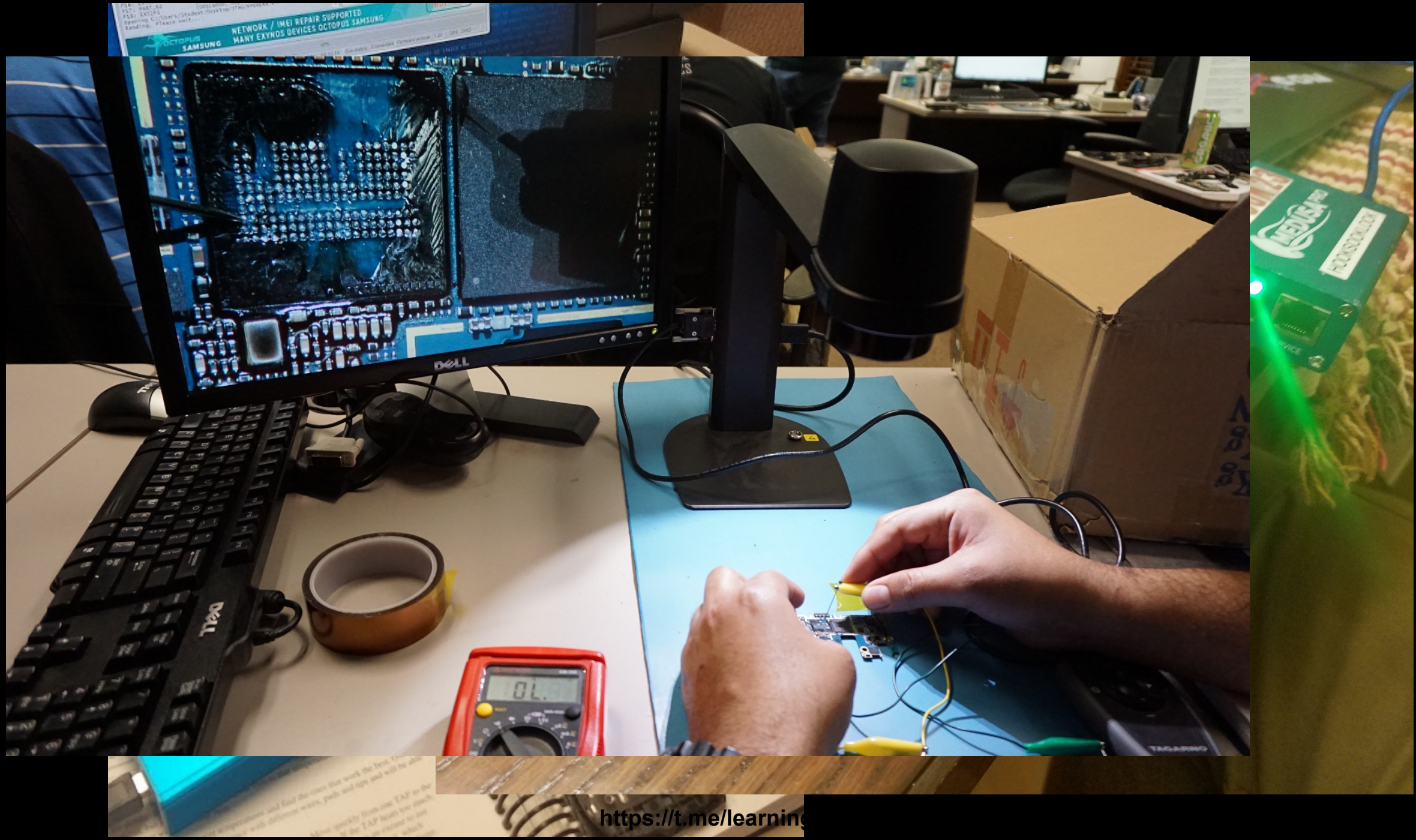
- Calls
- Contacts
- Messaging
- Location data
- E-mails
- Paired devices
- WiFi networks
- Cookies, web history, videos, music, recordings, images, cell towers, account data, visited web pages, bookmarks, notes, notifications, open apps, usage history, powering events, network statistics, a compromising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


JTAG
1 - VCC
3 - TRST
5 - TDI
7 - TMS
9 - TCK
11 - RTCK
USB
PWR
DATA
FRONT TOWARD ENEMY
HUAWEI M886
MEID(DEC):268435461410959083
MEID(HEX):A0000036A738EB


OCTOPUS
SAMSUNG
NETWORK / IMEI REPAIR SUPPORTED
MANY EXYNOS DEVICES OCTOPUS SAMSUNG
DELL
OL.
https://t.me/learning

chip-off extraction

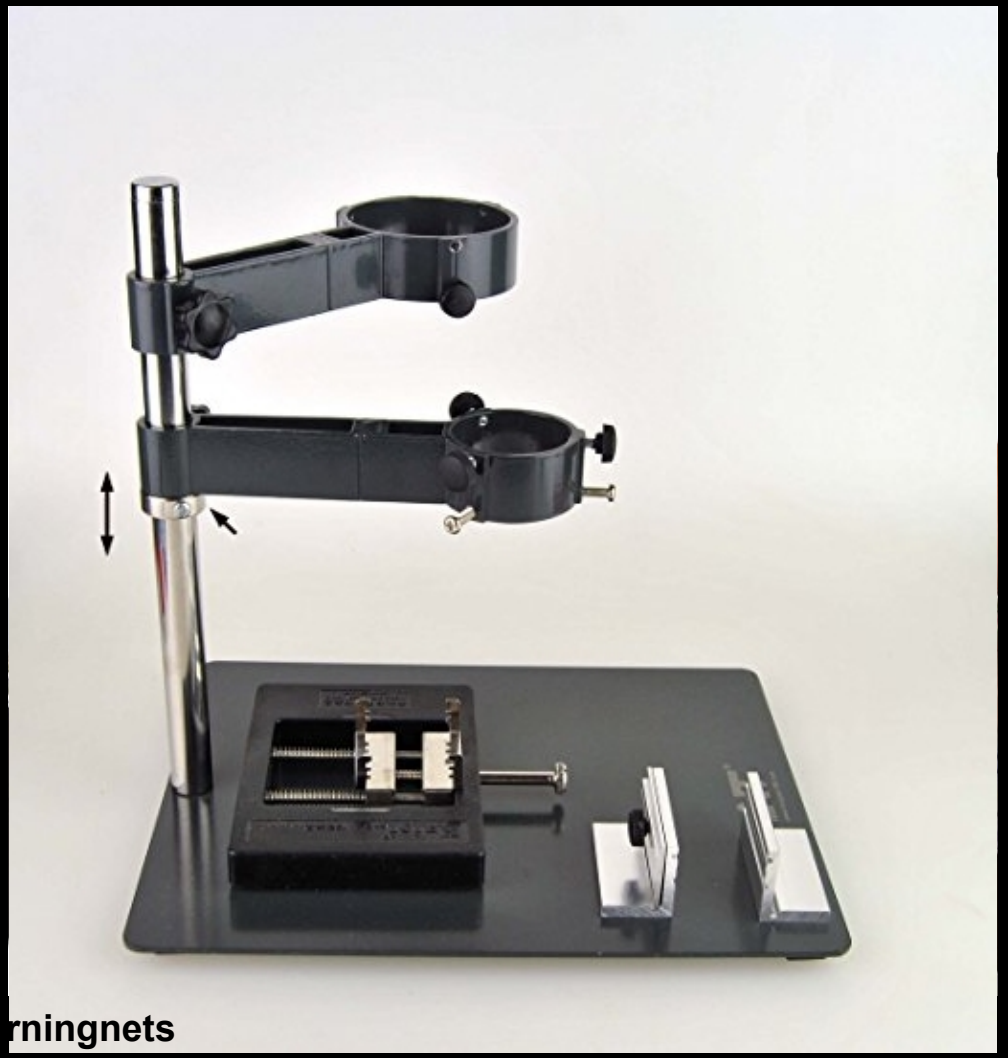
- Most of the time this is the end of the road for a phone
- Phone doesn’t have to be working
- Phone can have water damage
- Phone can be almost totally destroyed and still be recoverable
- Thousands of investigators and data-recovery experts are doing chipoff

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

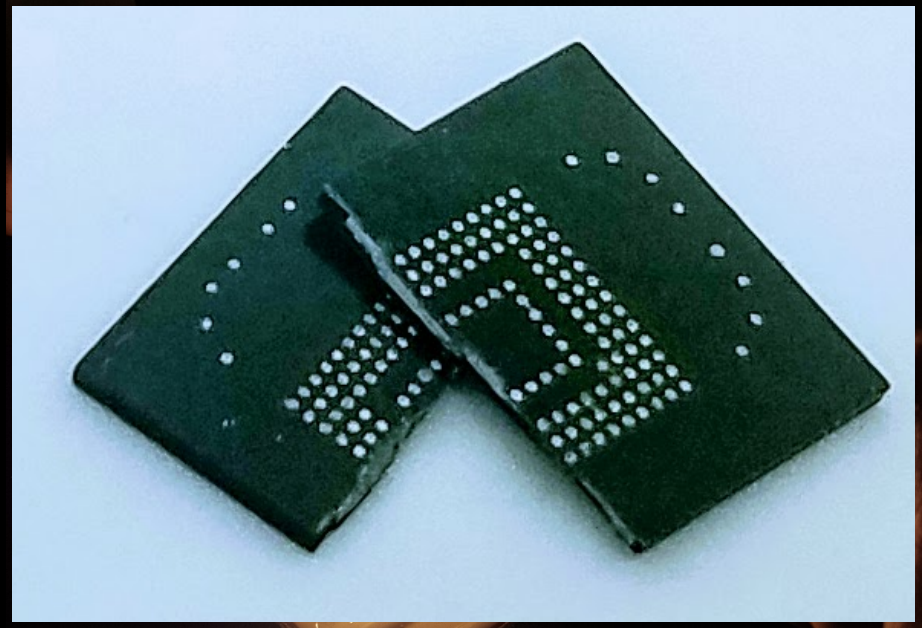
- Inexpensive
- Can be fairly safe if done carefully
- Most of us started here
- Can be reversible if you are careful
- Preheat with around 400 deg F, 200 C on the bottom for 5-8 minutes, then hit it with about 850/450 on the top, use a ¾ inch flat Xacto blade to lift chip off
- Clean with knife-blade soldering tip with flux, then clean with alcohol, retin if necessary



rningnets

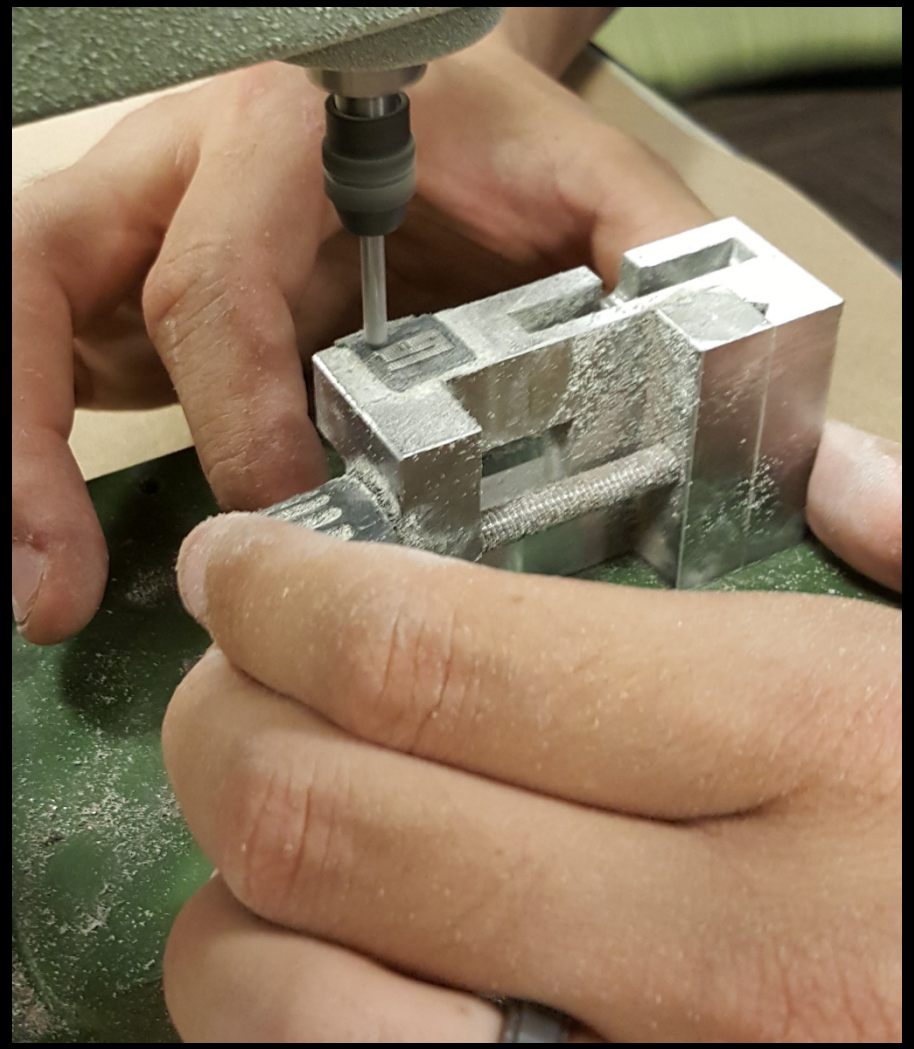
chip-off extraction methods – infrared

- 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), retin 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

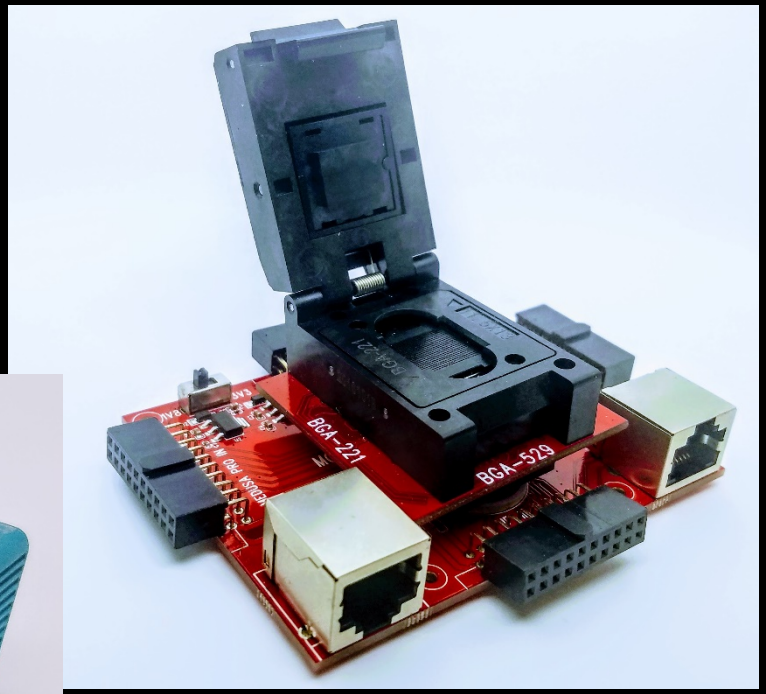
- UP828P Universal Programmer
- E-Mate Pro eMMC Adapter with Medusa Pro or Octoplus Pro Box
- KLD or Sireda Adapters (convert eMMC or eMCP to SD Card slot)
- Dediprog NuProg-E (eMMC and UFS chips)
- Allsocket and others
- Many different brands (Chinese) of readers and programmers

chip-off programmer – UP828P

up48.com

Purpose-built software
downloadable and included

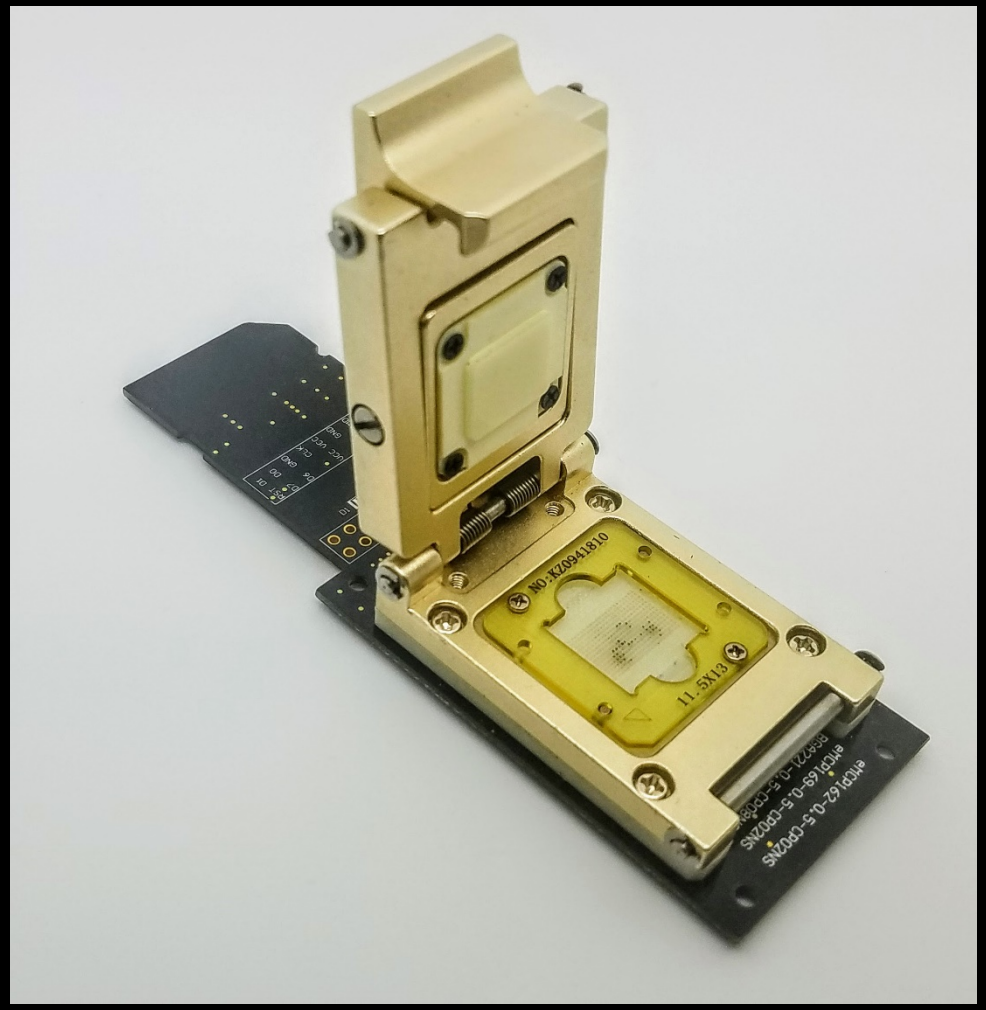
chip-off/ISP box – Medusa Pro & E-mate



medusabox.com

Purpose-built software
downloadable and included

chip-off reader/adapter – 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.

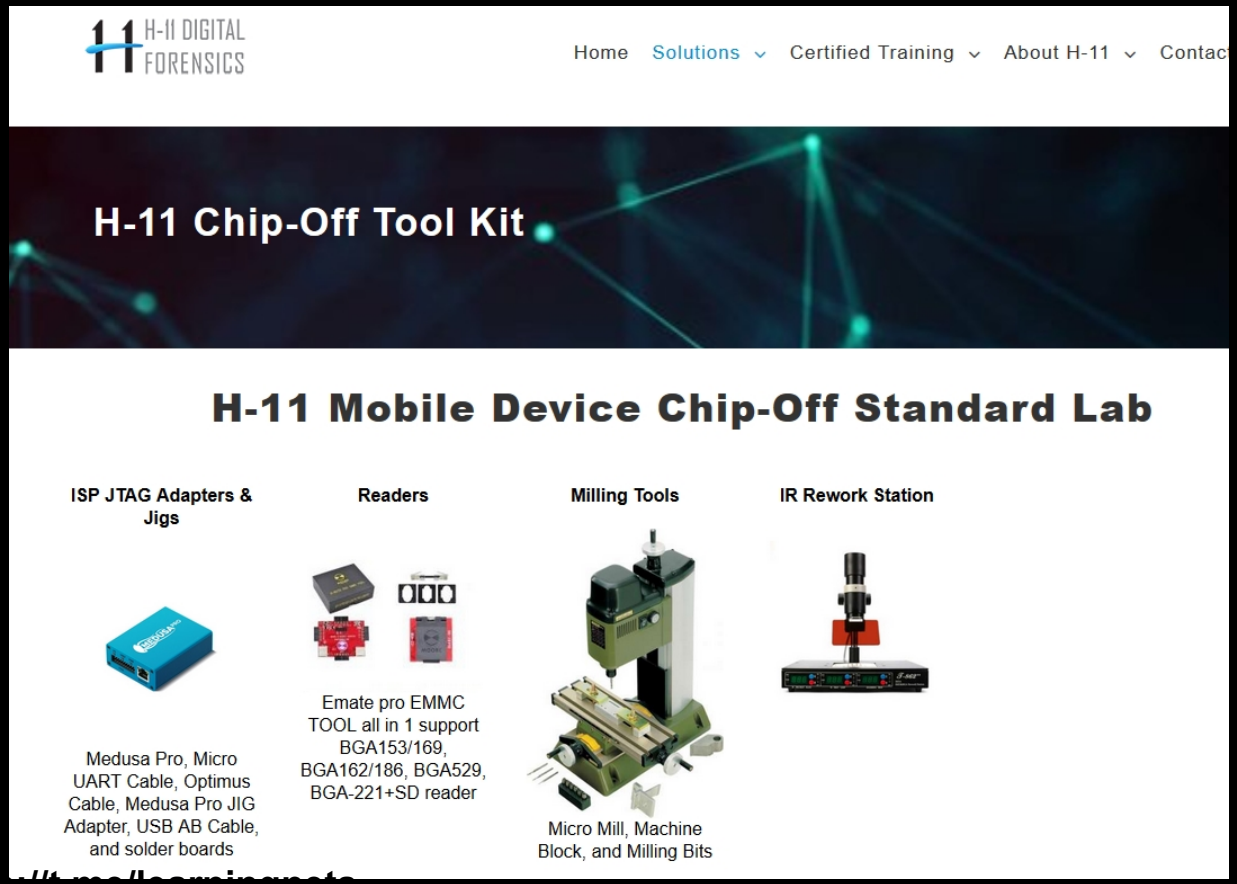
chip-off programmer– NuProg-E

www.dediprog.com

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

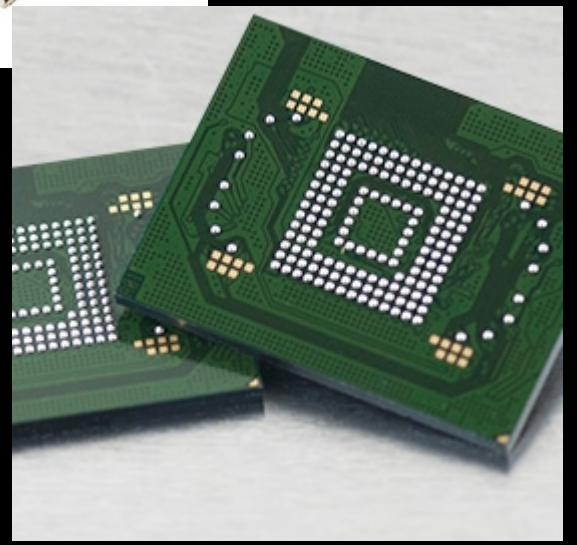
chip-off equipment

- 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



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**

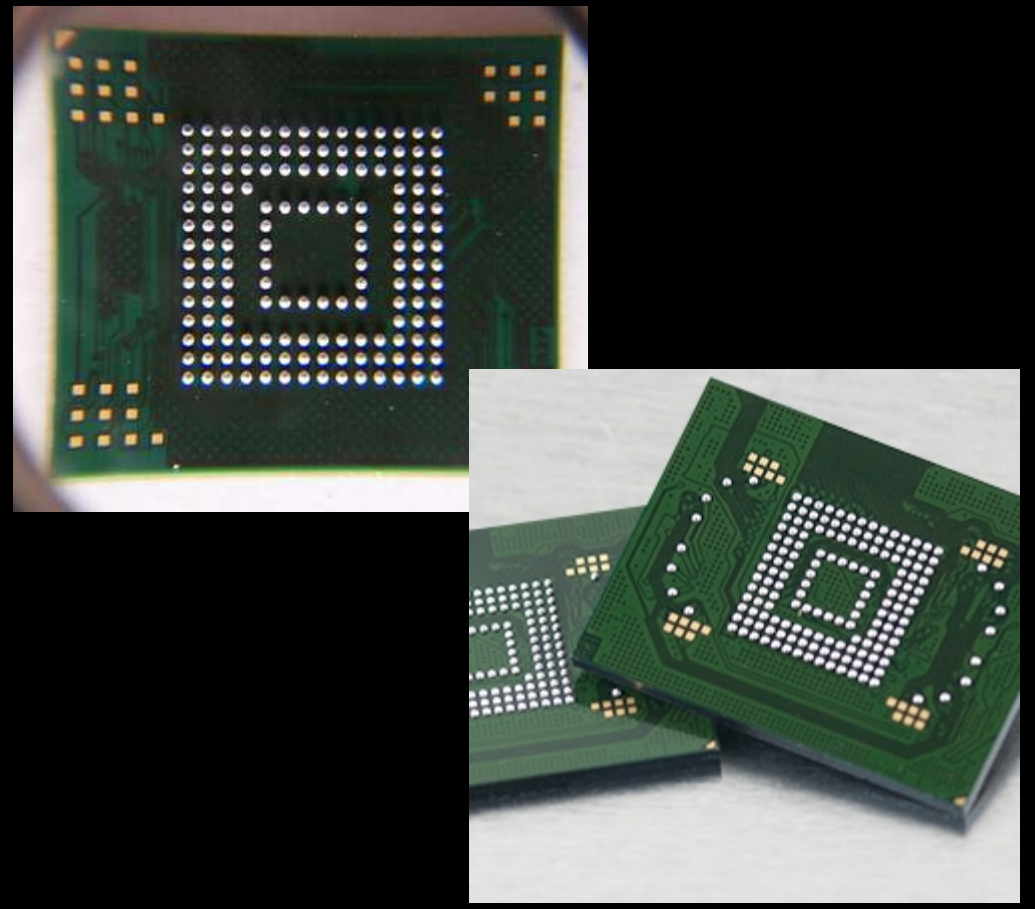


embedded multimedia controller (eMMC)

- 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

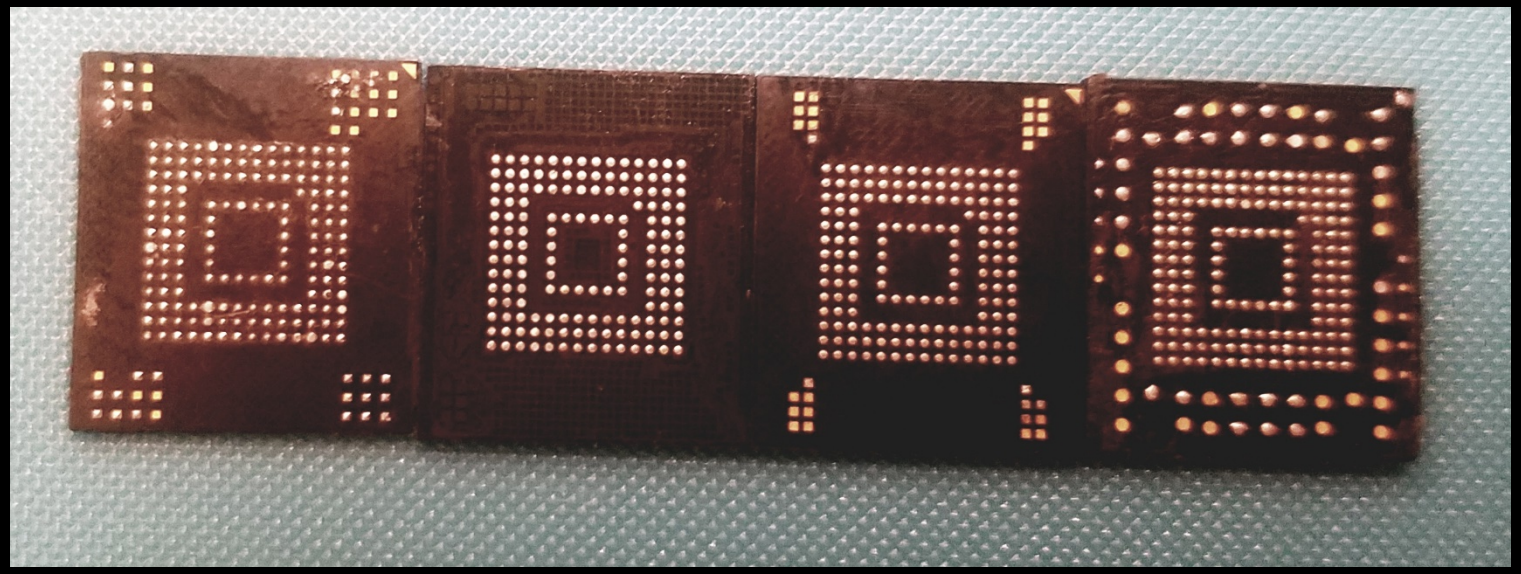
types of eMMC and eMCP – BGA153/169

- 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

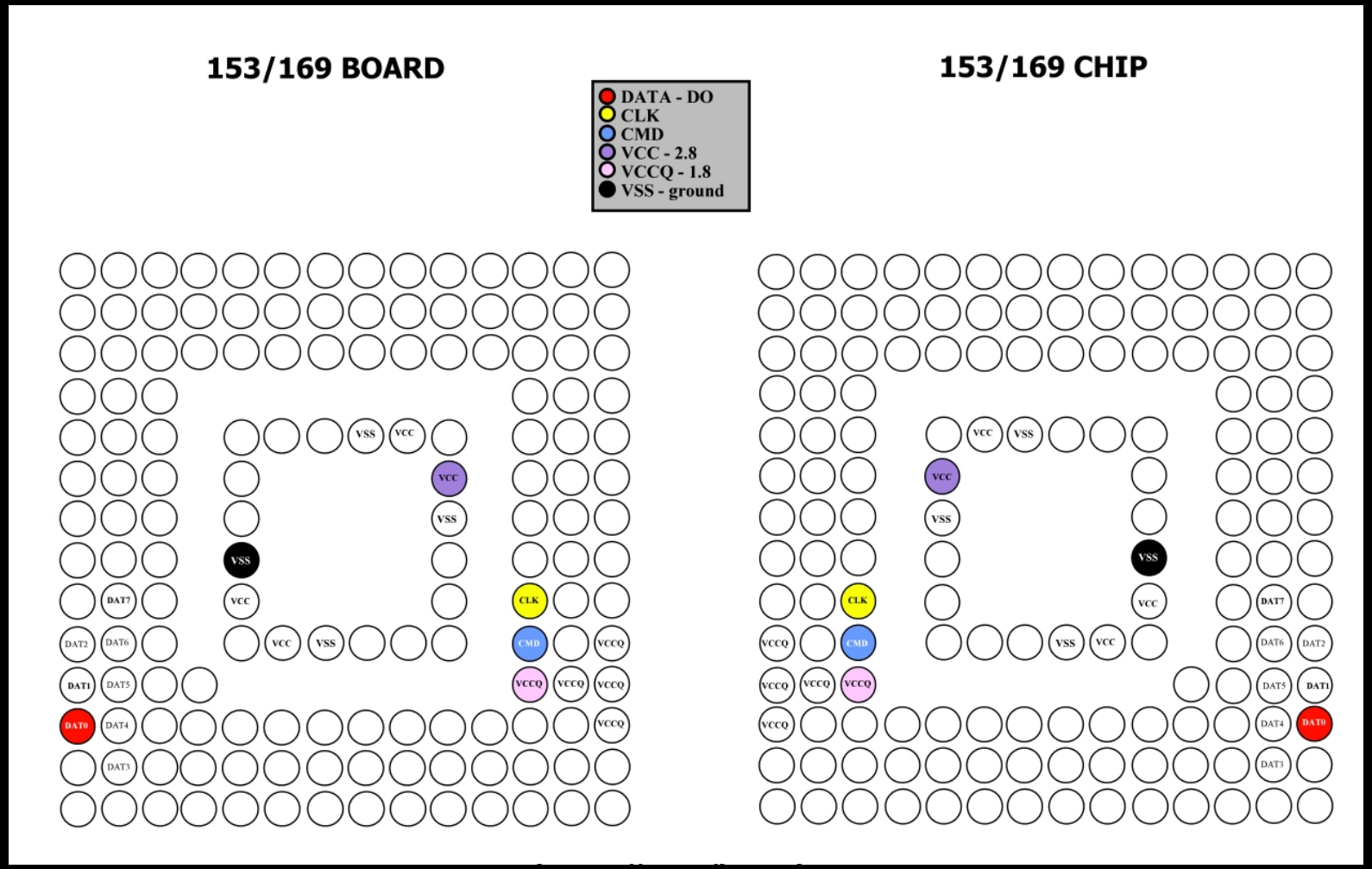


types of eMMC and eMCP – BGA153/169

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

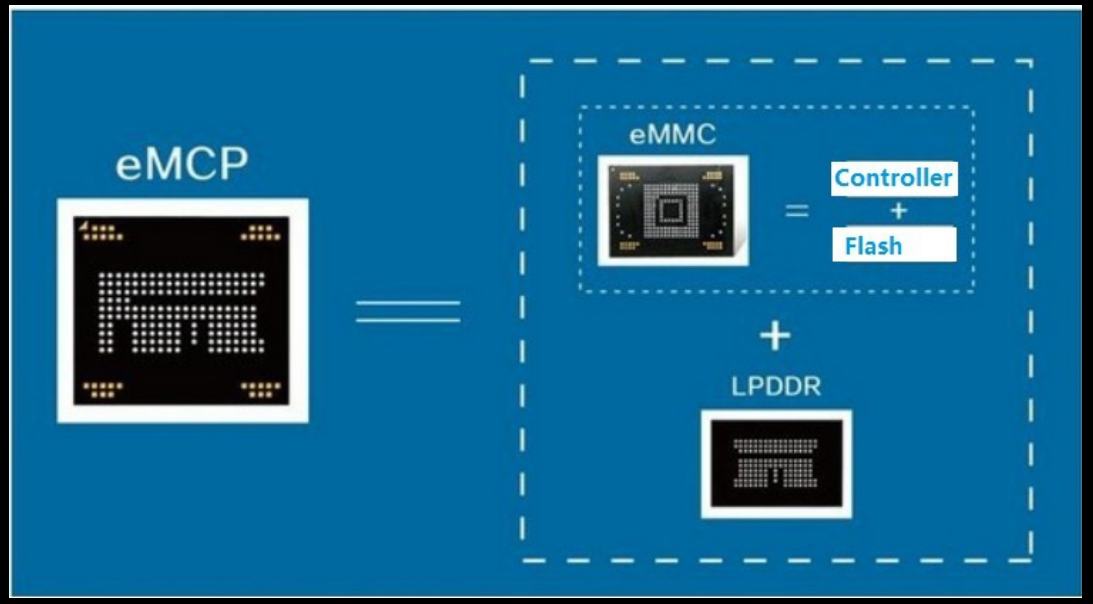


types of eMMC and eMCP – BGA153/169



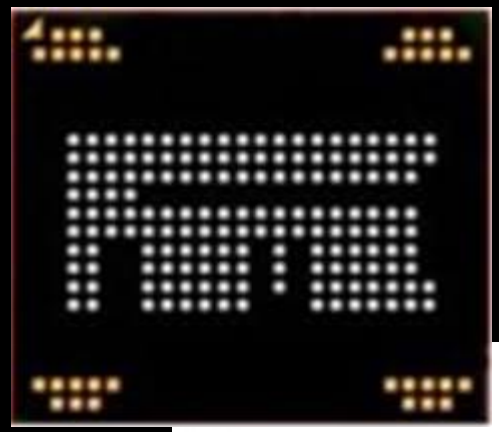
embedded multi-chip package (eMCP)

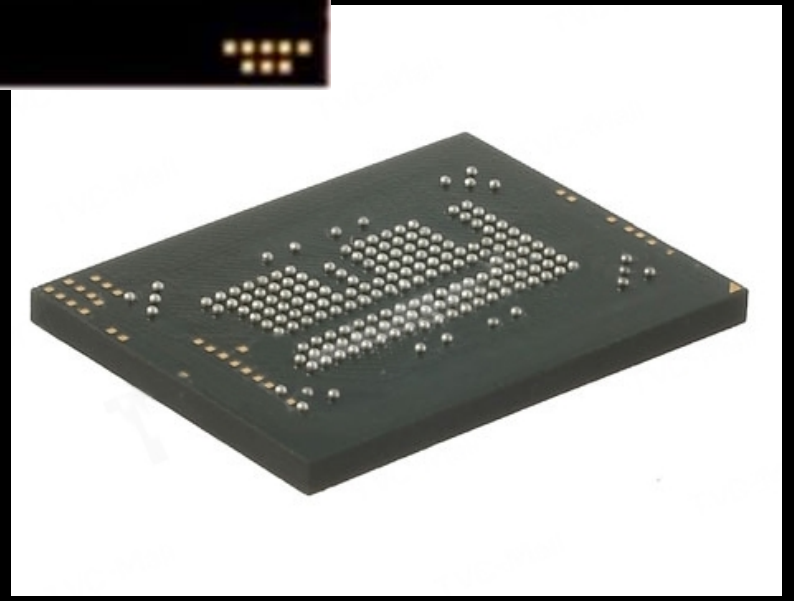
- Is an eMMC and DDR RAM in one package (MCP)
- Usually found in cheaper phones, such as Chinese garbage phones
- Consists of the BGA162/186 and the BGA221
- The BGA529, while still an eMCP, is super swank, found in nice phones, but not many



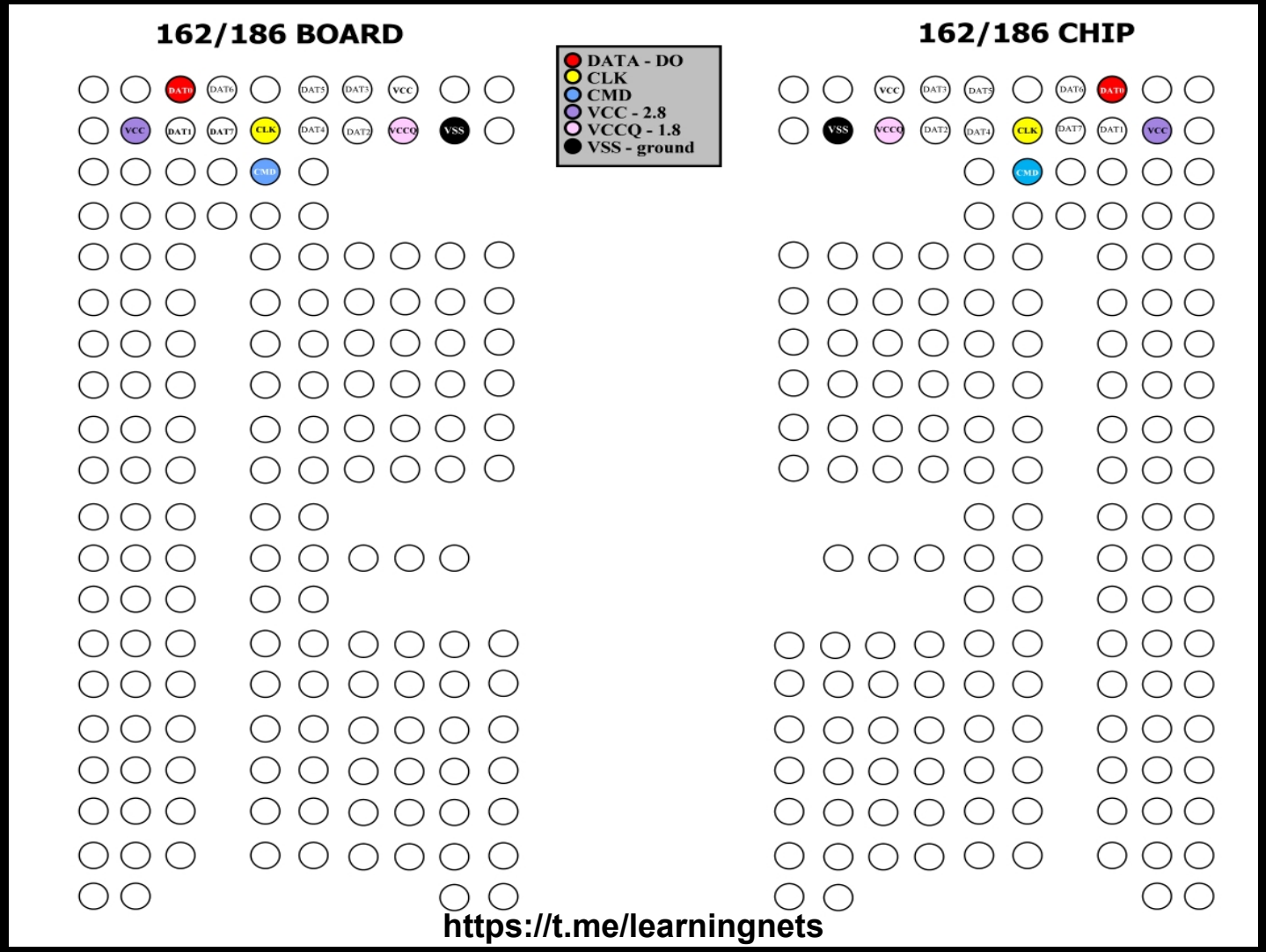
types of eMCP – BGA162/186

- 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)



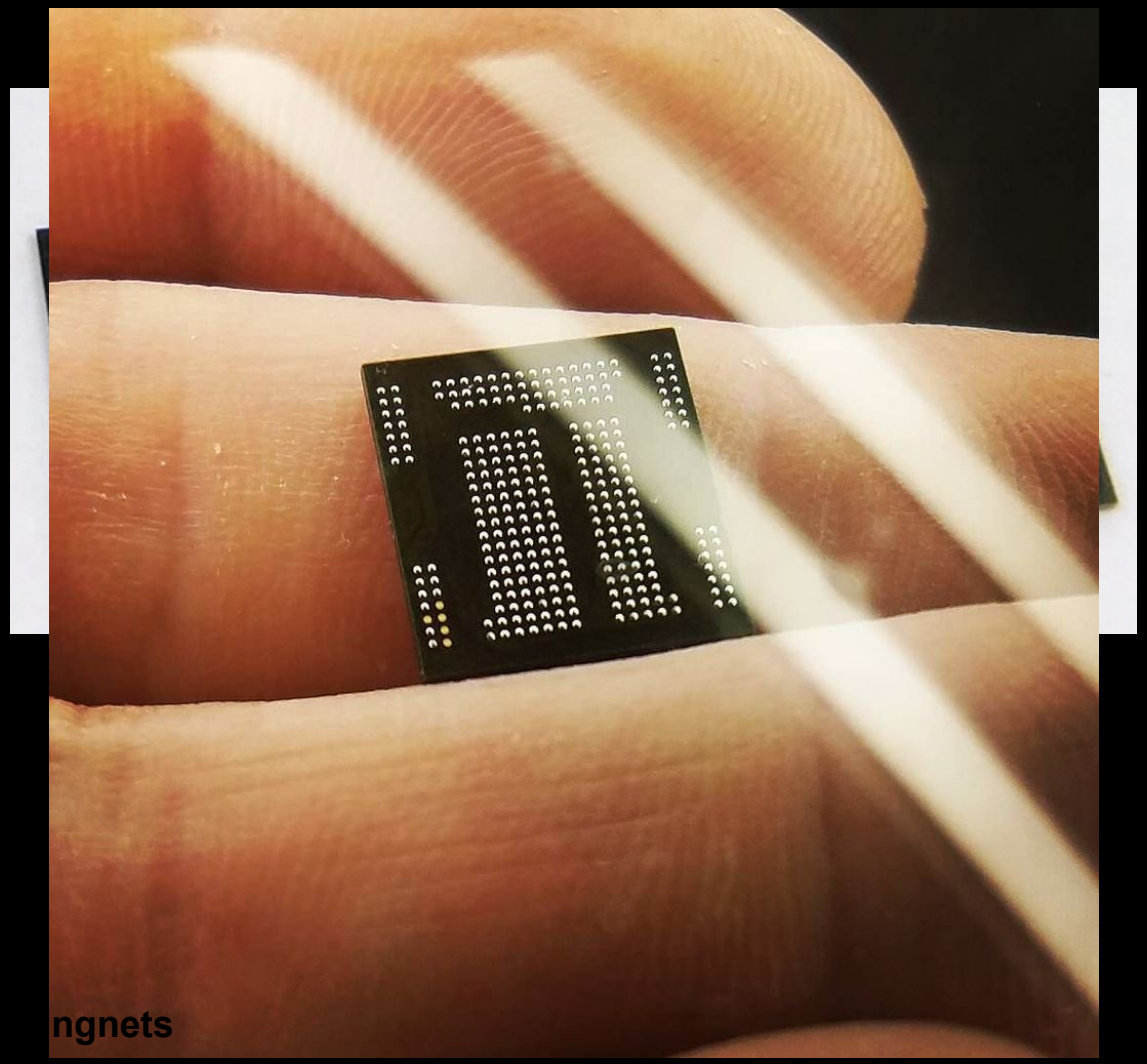


types of eMCP – BGA162/186

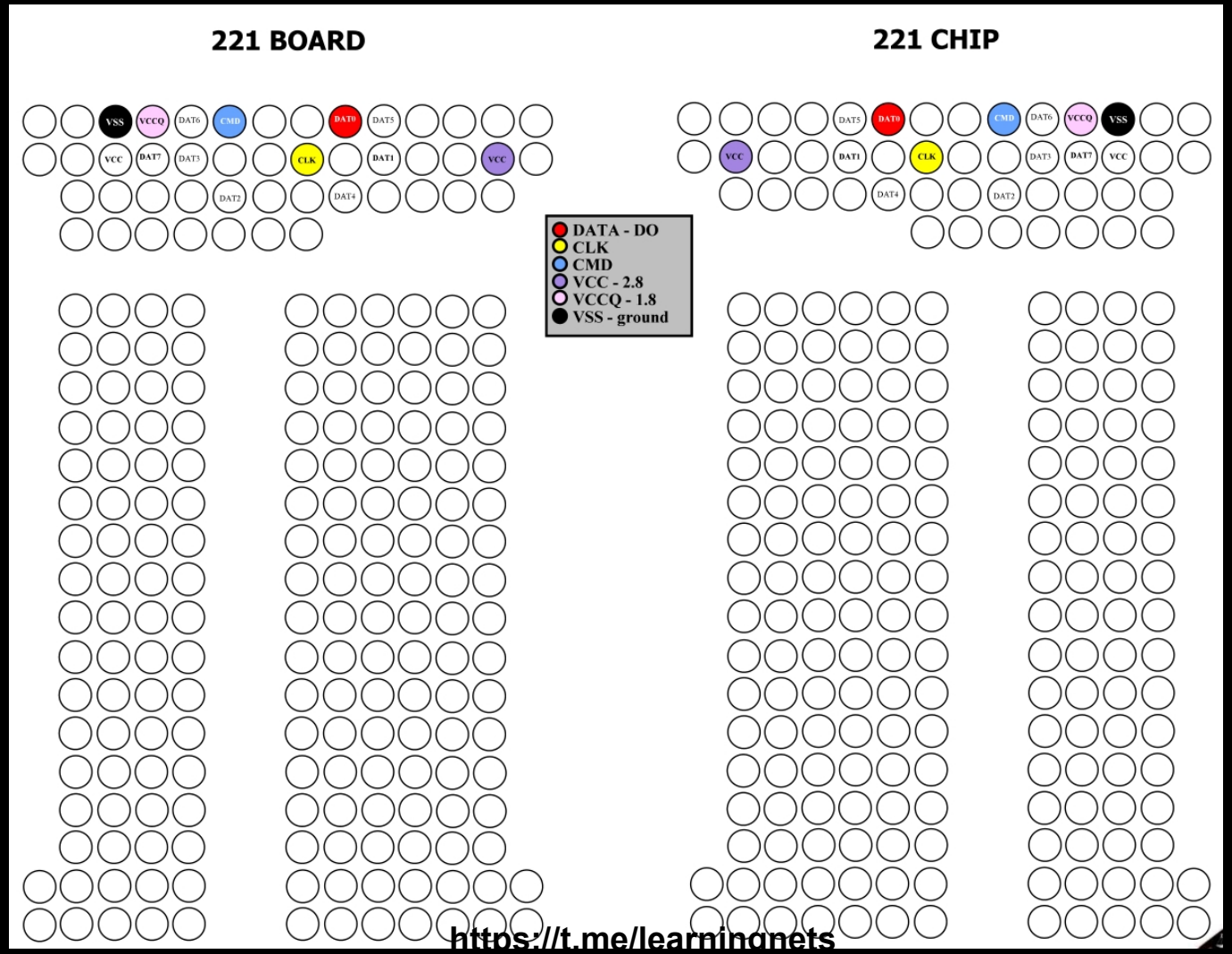


types of eMCP – BGA221

- 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

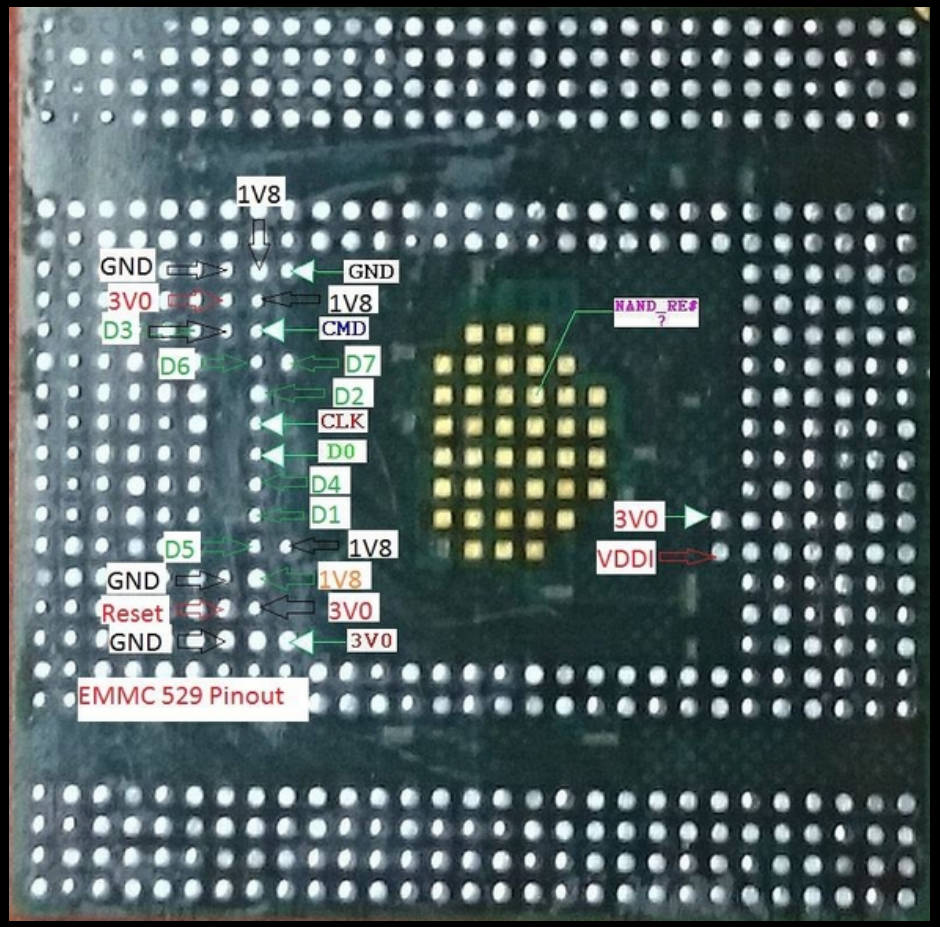


types of eMCP – BGA221

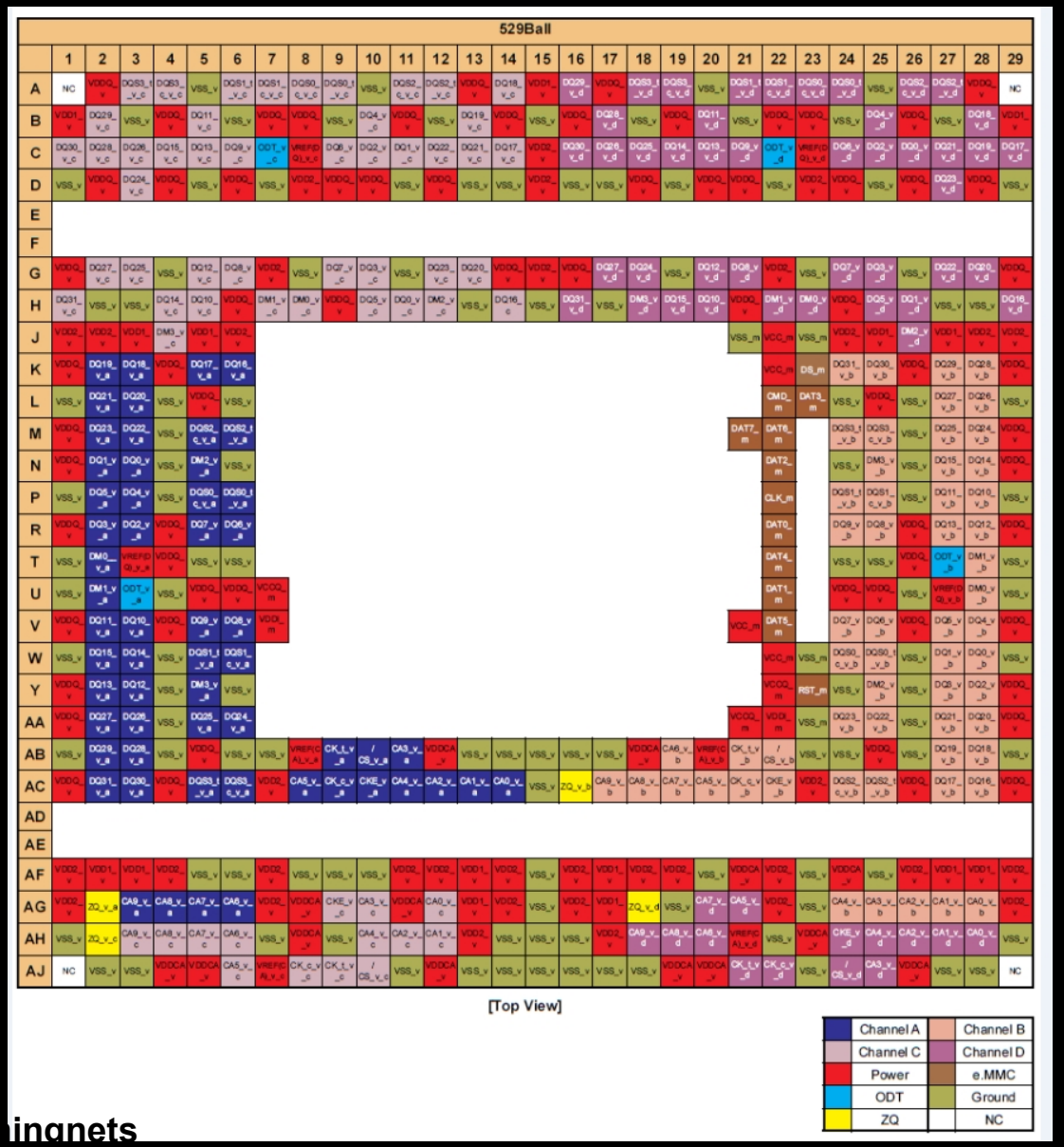


types of eMCP – 529

- Least common eMCP chip in mobile devices (Note 4 era)
- I've only ever seen one physical size
- Looks like all the pads (529 of them)

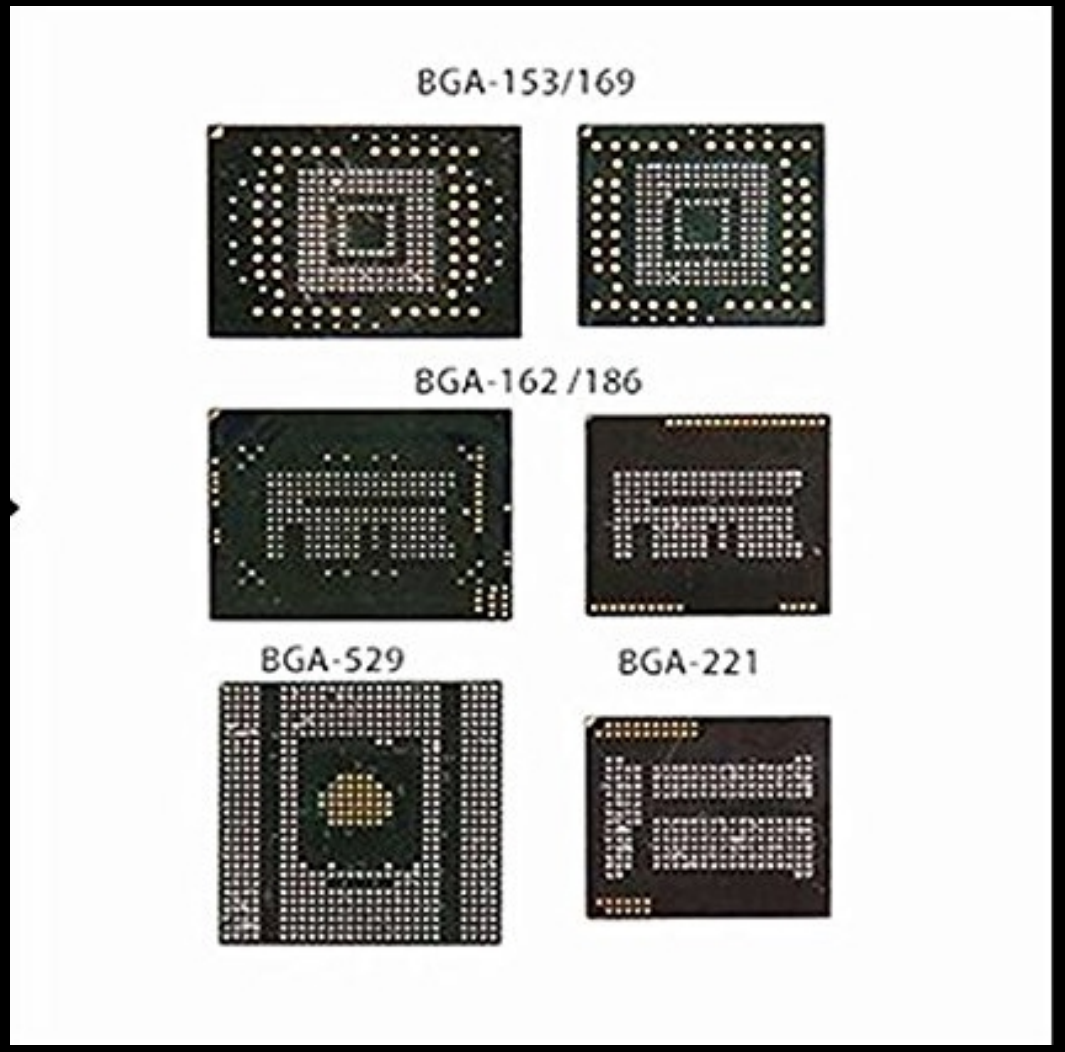


types of eMCP – 529



ingnets

all the culprits

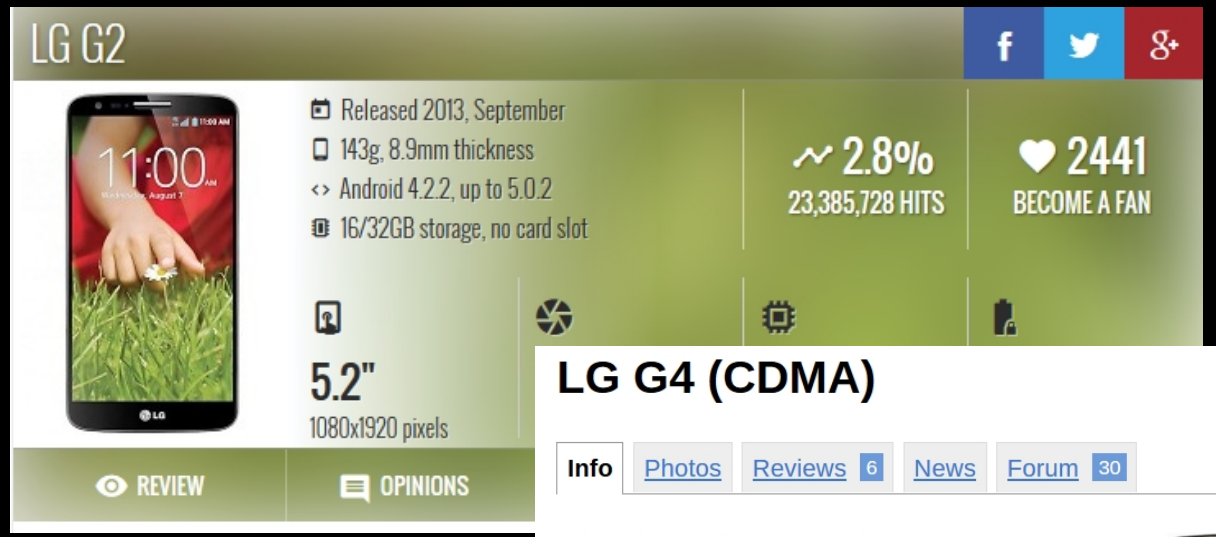


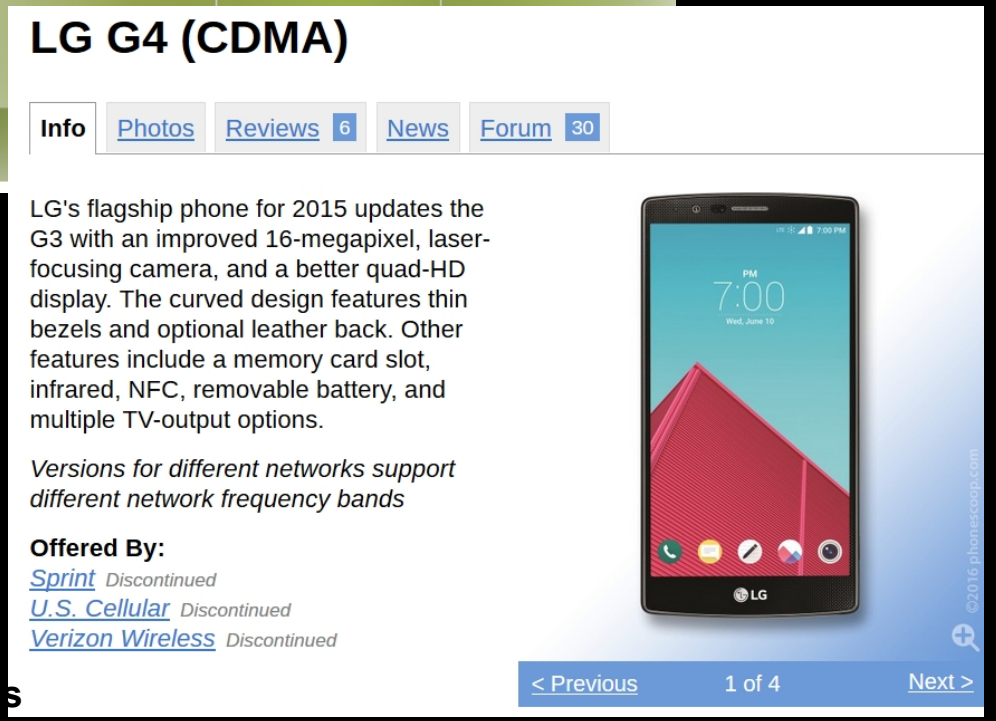
so how's it done?

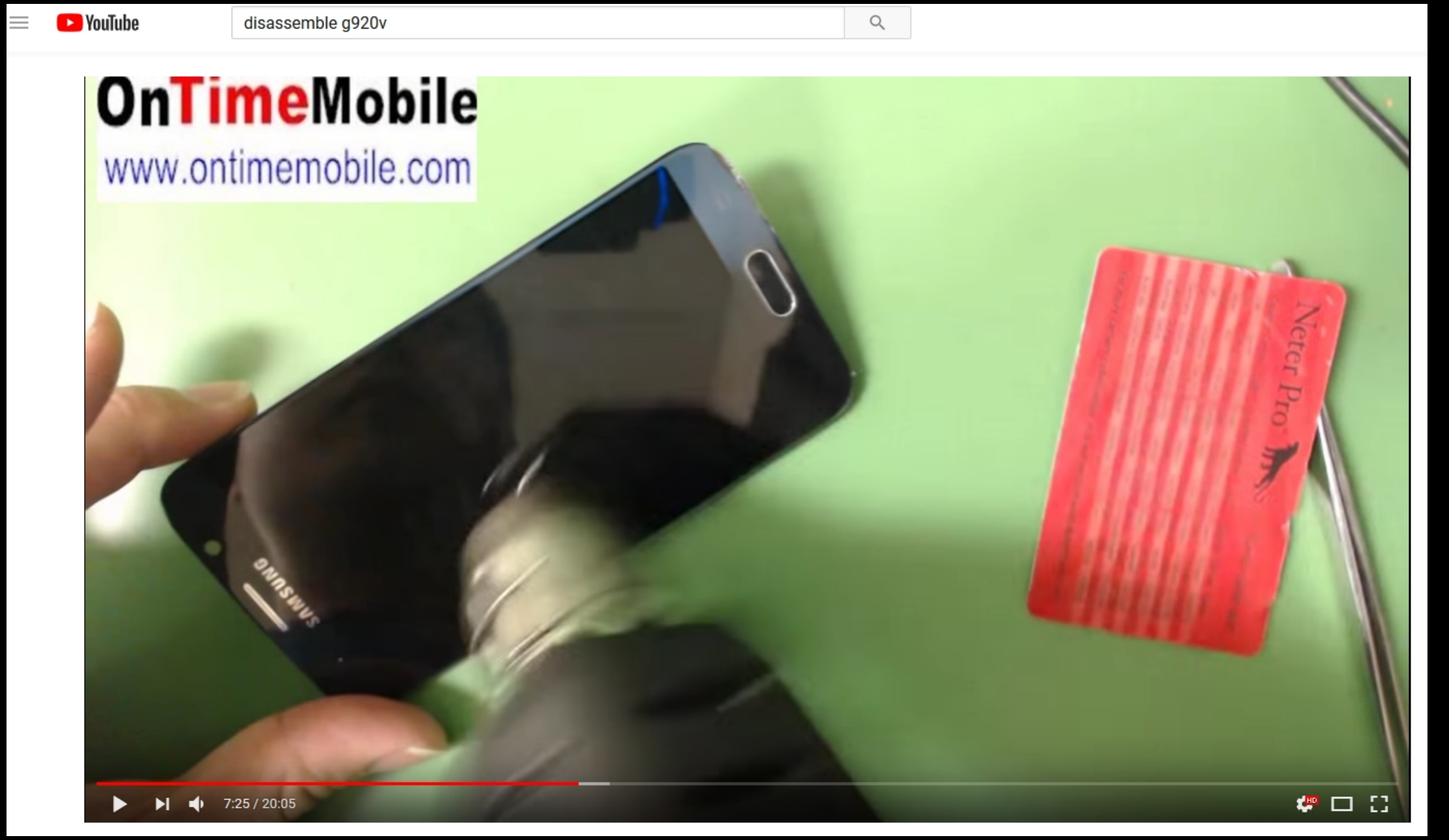
- Try the automated tools first and other methods that don't involve destruction
- Research the phone
  - Memory type
  - Memory package style (FCC filing, internal photos)
  - Size of the memory (4GB or more it's likely an eMMC or eMCP)
- Disassemble the phone carefully and precisely in order to not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

phone research?

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






YouTube
disassemble g920v
OnTimeMobile
www.ontimemobile.com
SAMSUNG
Neter Pro
7:25 / 20:05

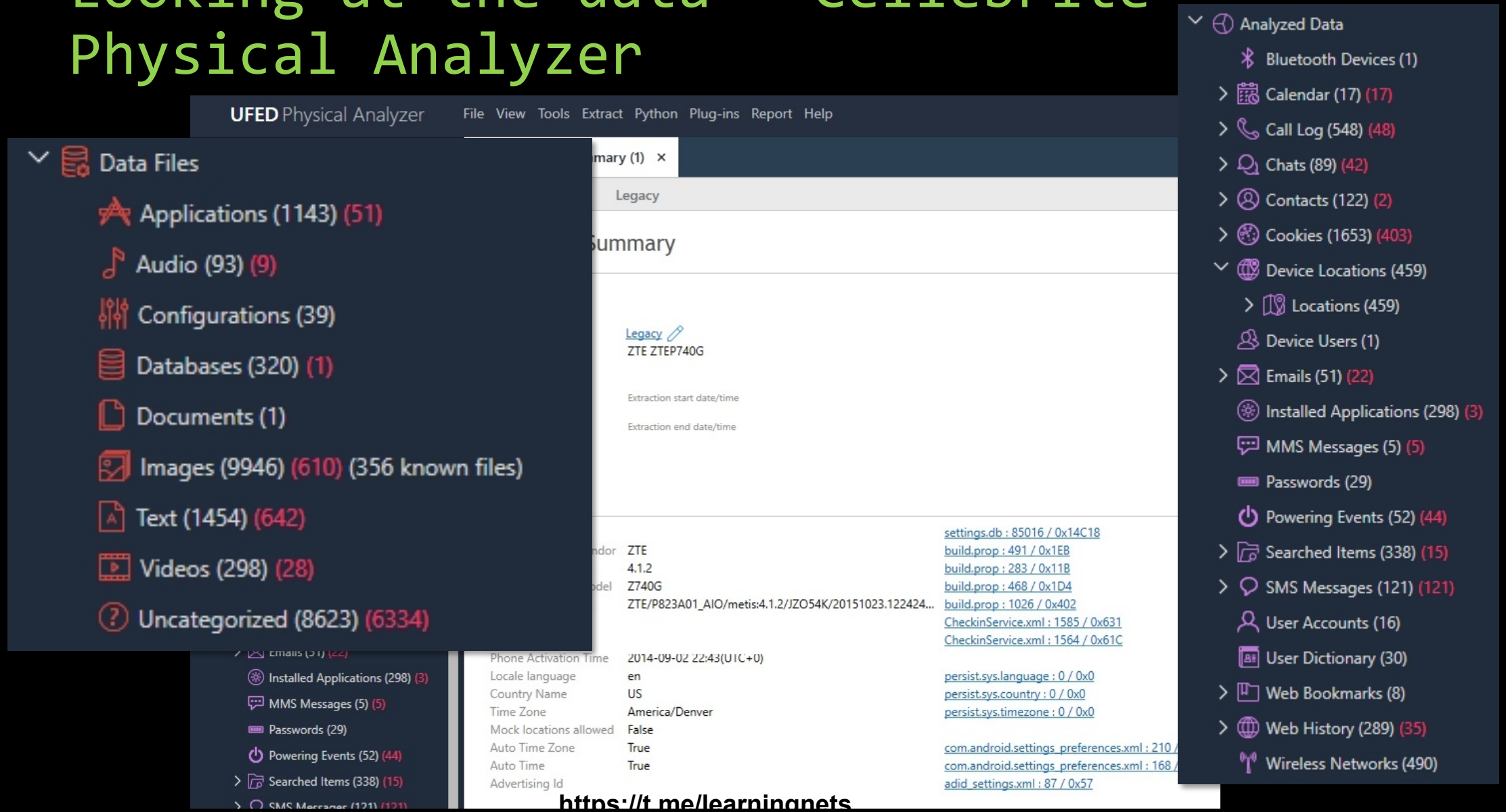
video demo of proper technique

Edit and sick beatz:
Nick Thomson

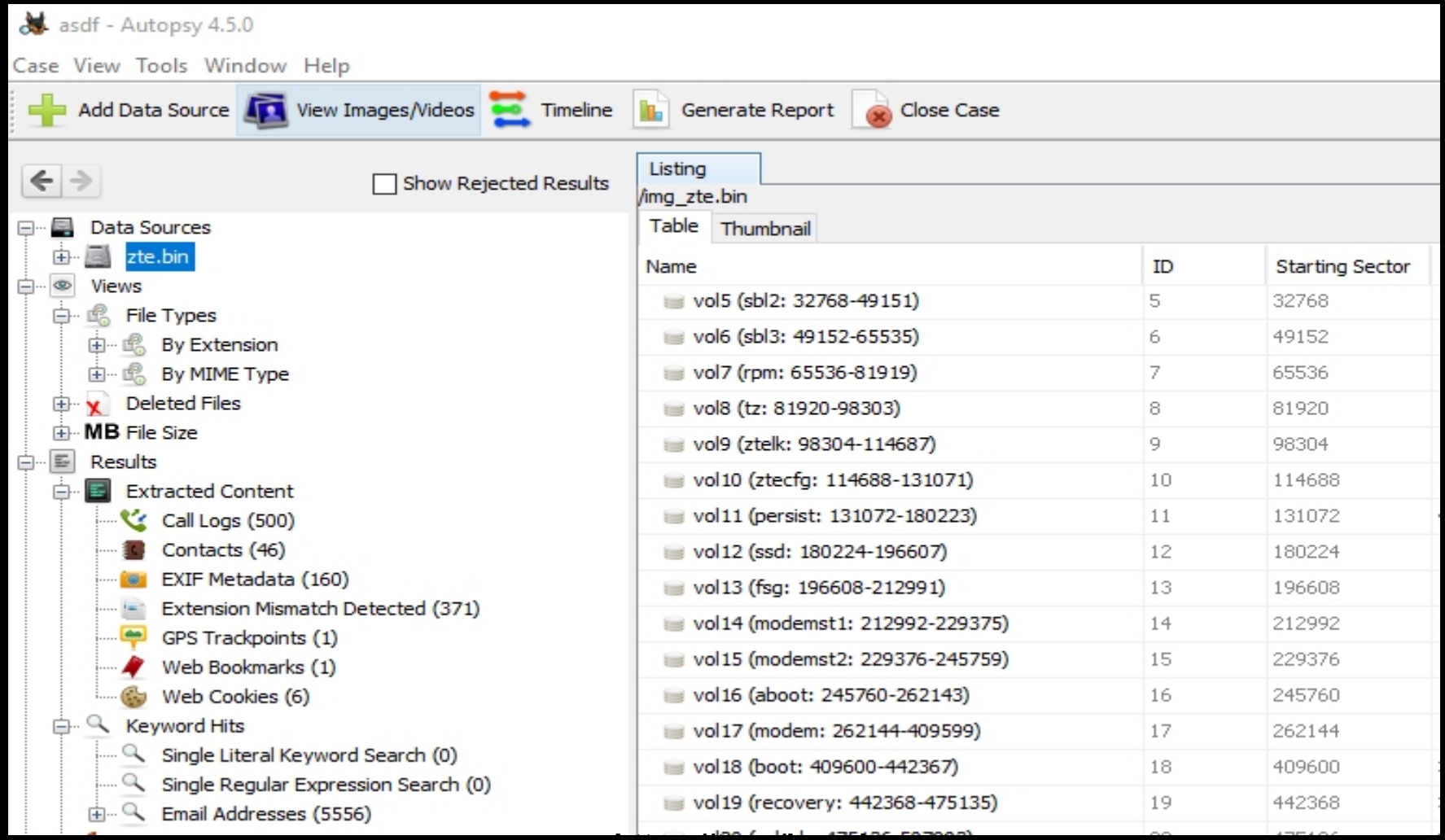
Looking at the data – Tools

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

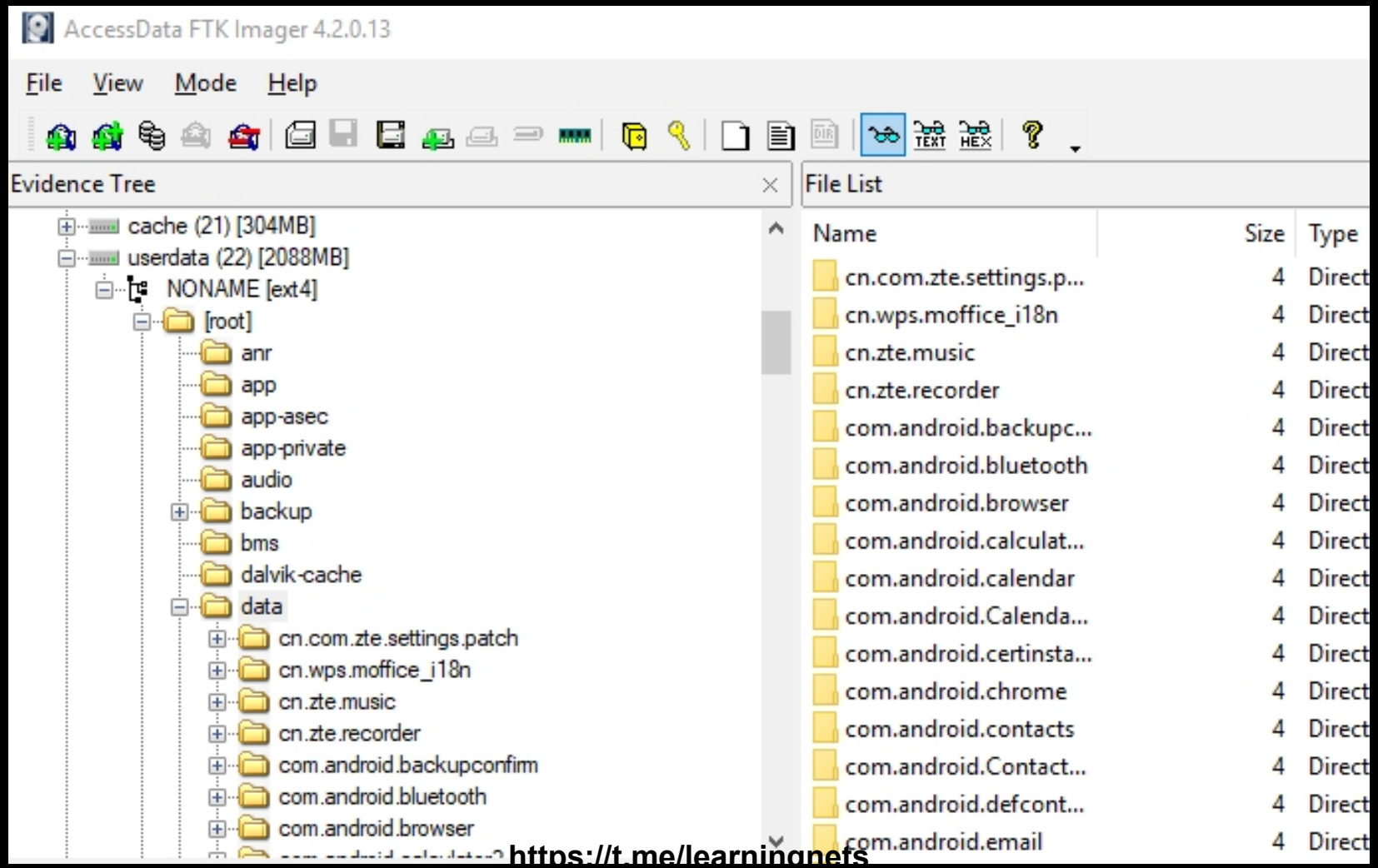
Looking at the data – Cellebrite Physical Analyzer



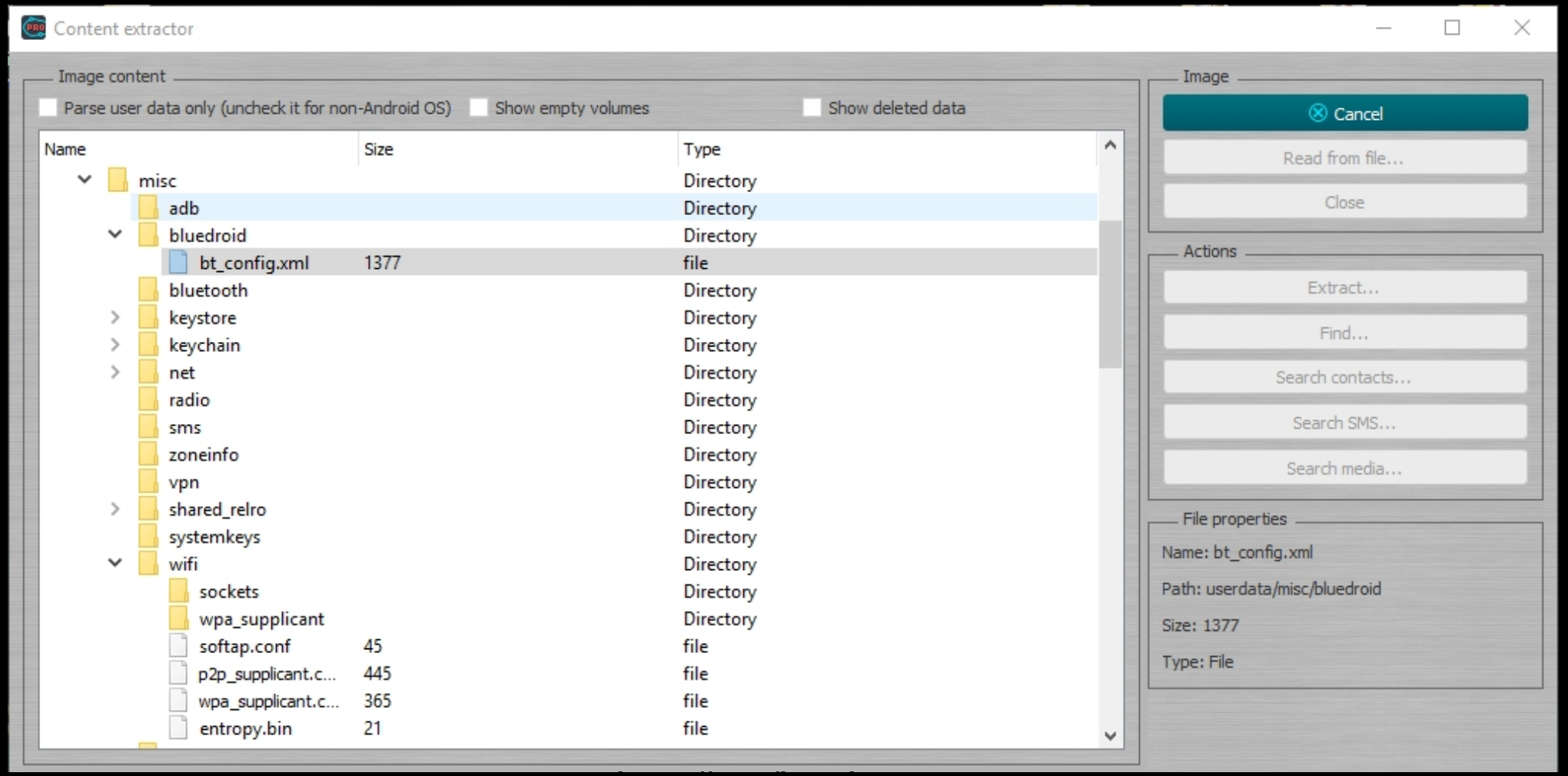
Looking at the data – Autopsy



Looking at the data – FTK Imager



Looking at the data – Octoplus/Medusa

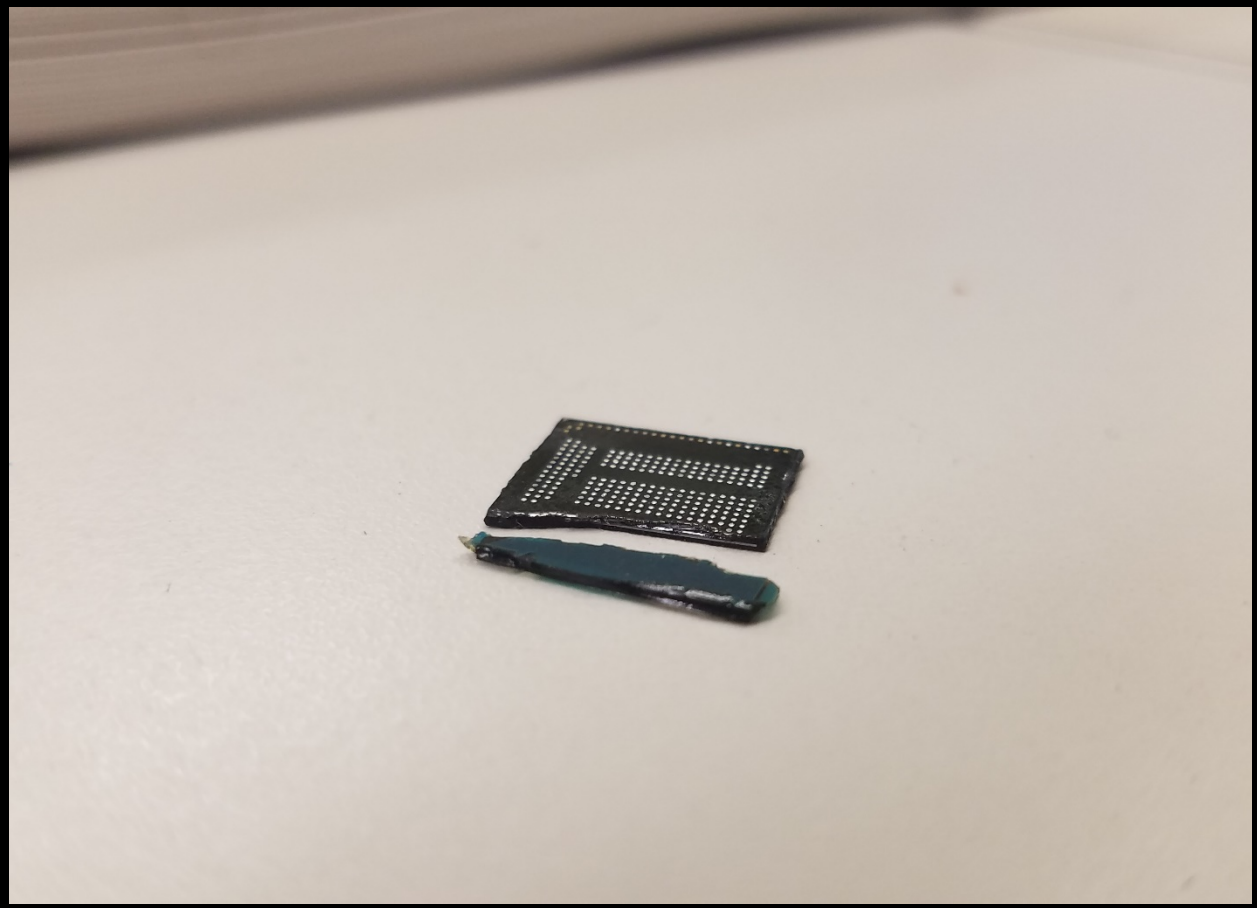


success stories

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

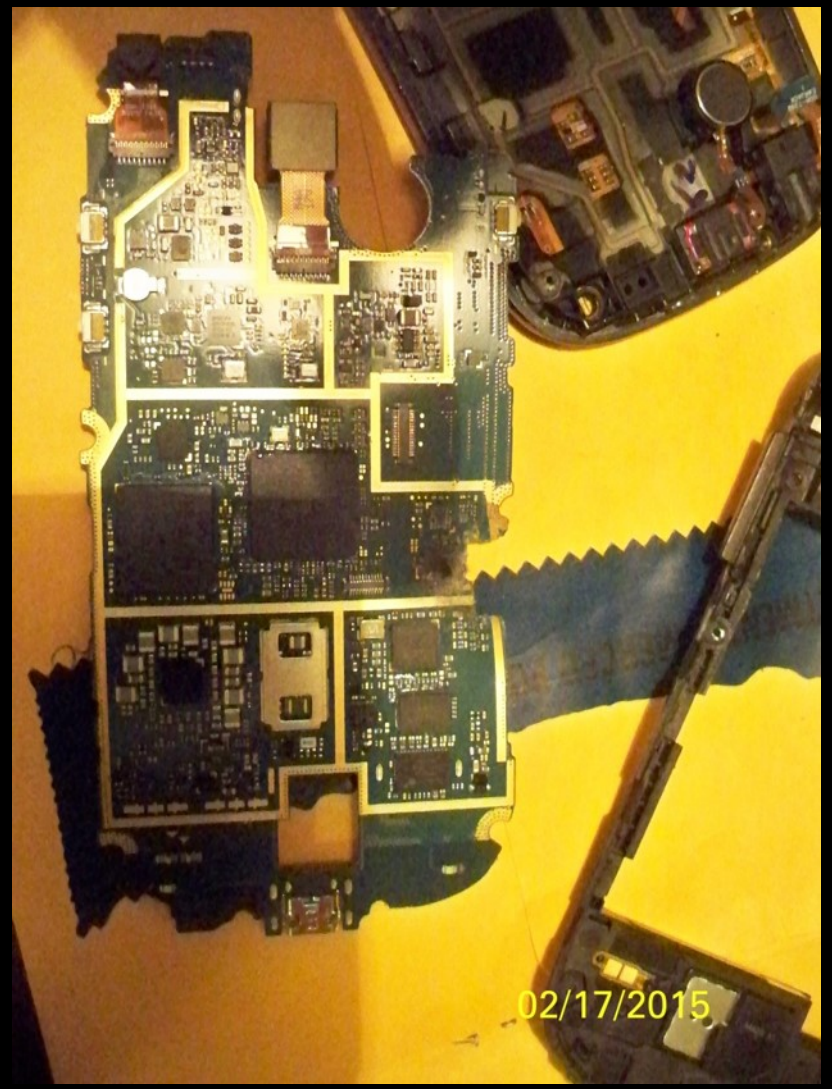
success stories

- 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




BSIDES
Symantec
OpenWest Conference · Utah Open Source
CISCO SYSTEMS
Kevina McLean
Cisco
GENERAL
STAFF
Ultimate Insider Threat
MERC with a MOUTH
Since 1991
El Guero TAQUERIA
44

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