



# **Chip Off Village In-depth Analysis**

# Disclaimer

This talk is ONLY for the Proof of Concept and Educational Purpose

We are not responsible for the liabilities and unexpected outcome regarding the law and ordinance of your country.

Please read the correspondent regulation in your country before using the devices and materials.

I am NOT teaching you how to tear off the devices and breaking the devices as result of damage

# Who am I?

Captain Kelvin

Focusing on

- hardware and drone security
- Penetration Test, Incident Respond and Digital Forensics
- Speaker @ Black Hat, DEFCON, SANS, DFRWS, HITB, SINCON
- Organizer of Chip Off Village, RFID Village and Drone Hacking Village at Black Hat, DEFCON, Hardwear.io, Hack In The Box, Hack In Taiwan, Infosec In the City,

<https://www.youtube.com/watch?v=qIKst7cHsn8&t=2s>

<https://twitter.com/blackhatmea/status/1592588241160482817?s=46&t=-ETzZ6EXupyKXsNgqgrXwg>

# Contact



## Captain Kelvin

立即驗證

OSCE<sup>3</sup>, OSEP, OSWE, OSED, OSCP, OSDA, OSWA, OSWP, KLCP | Black Hat / DEFCON Speaker & Trainer | Penetration Test | Digital Forensics | Incident Response | Hardware and Drone Security Researches & Analysis

手遊特別活動區 手遊 [Web 3.0 資訊](#)

# Black Hat USA Training in Aug 2024

Extraction from the 'Practical Drone Hacking'

- 2 Day Intensive (Zero to Hero)
- 4 Day Advanced Drone Hacking



# Syllabus

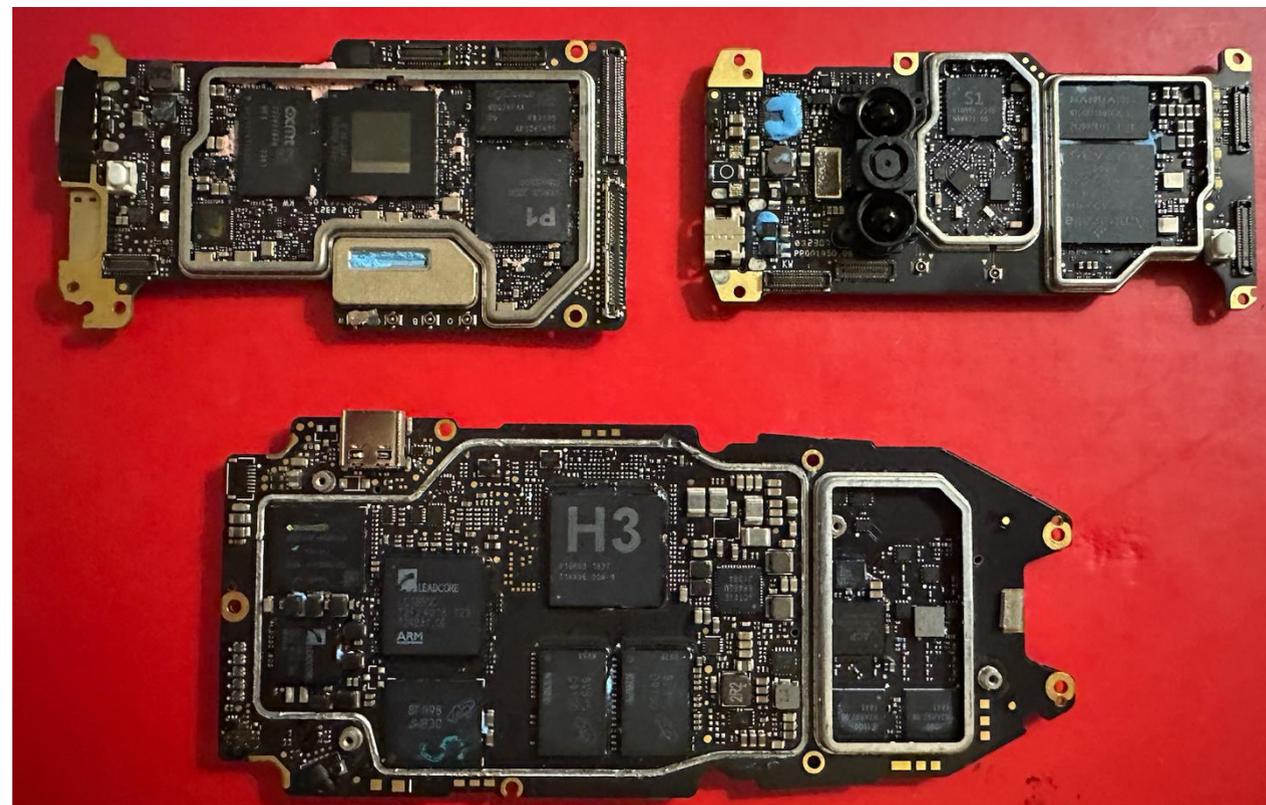
Day 1: Attack Vectors, Drone Communication, Drone Components and Operations

Day 2: Drone Programming with Python, Drone Detection with SDR

Day 3: Drone Firmware Analysis and Reverse Engineering

Day 4: Drone Forensics

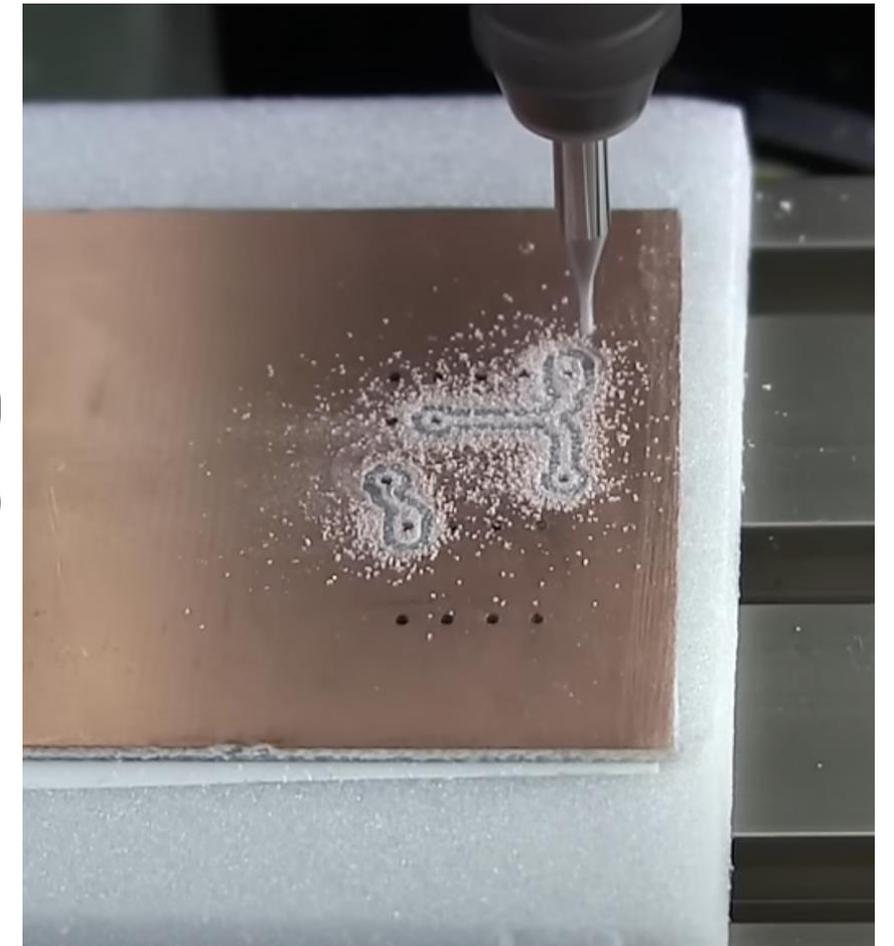
- recover black box, data and flight log analysis from the chip





# What is Chip Off?

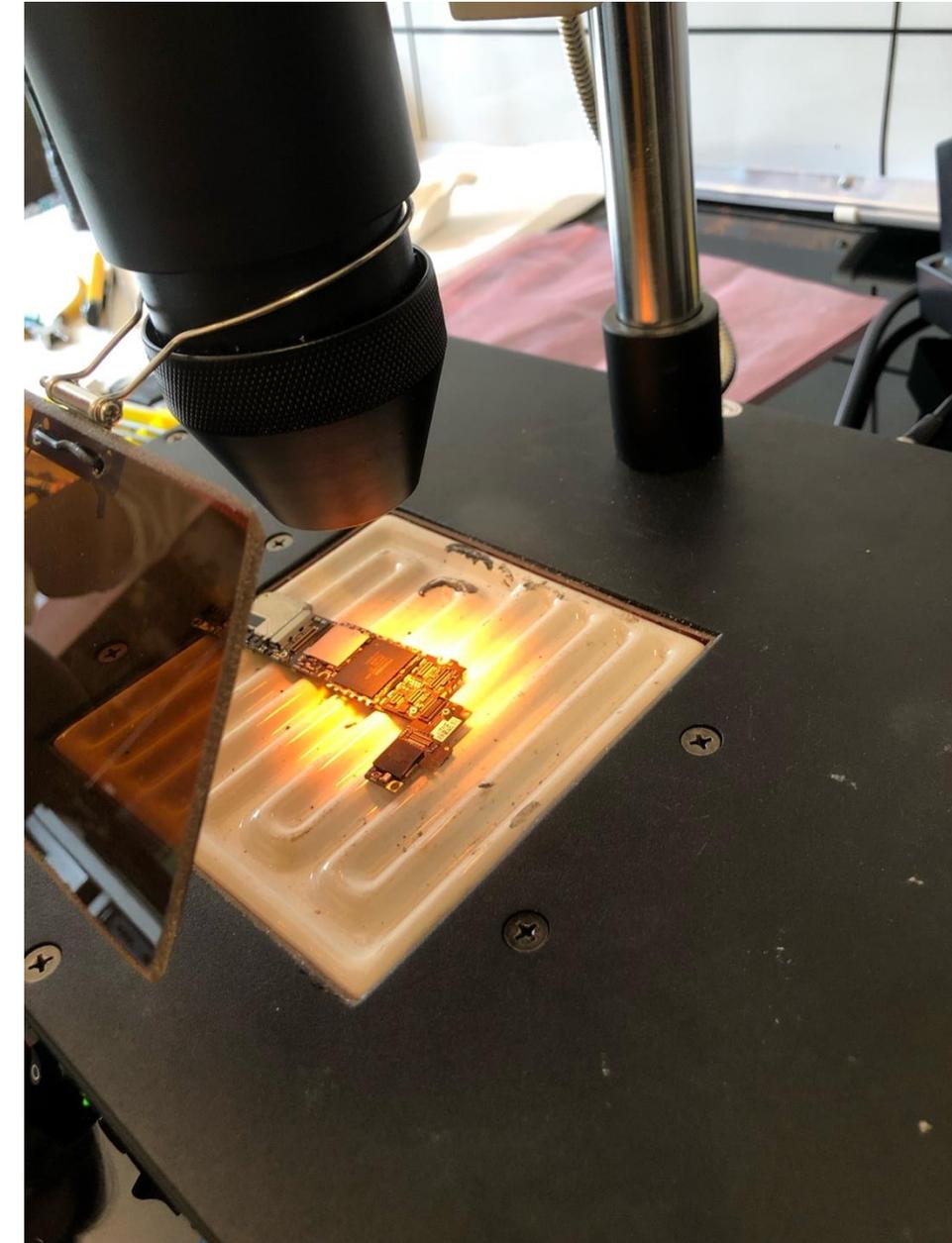
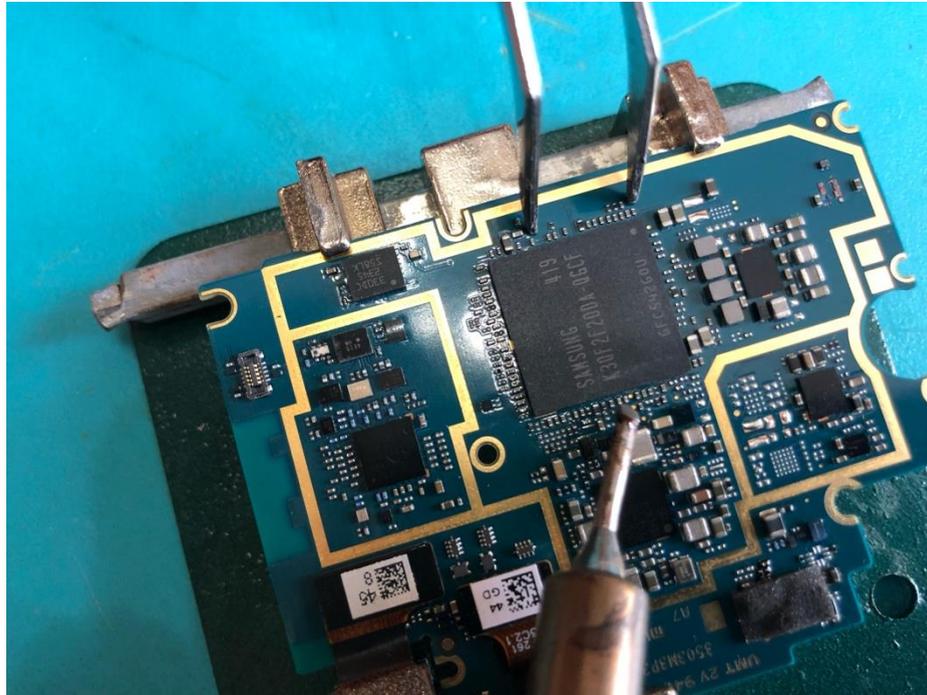
# Hot Air, Infra-Red or Milling ?



# Chip Off Village



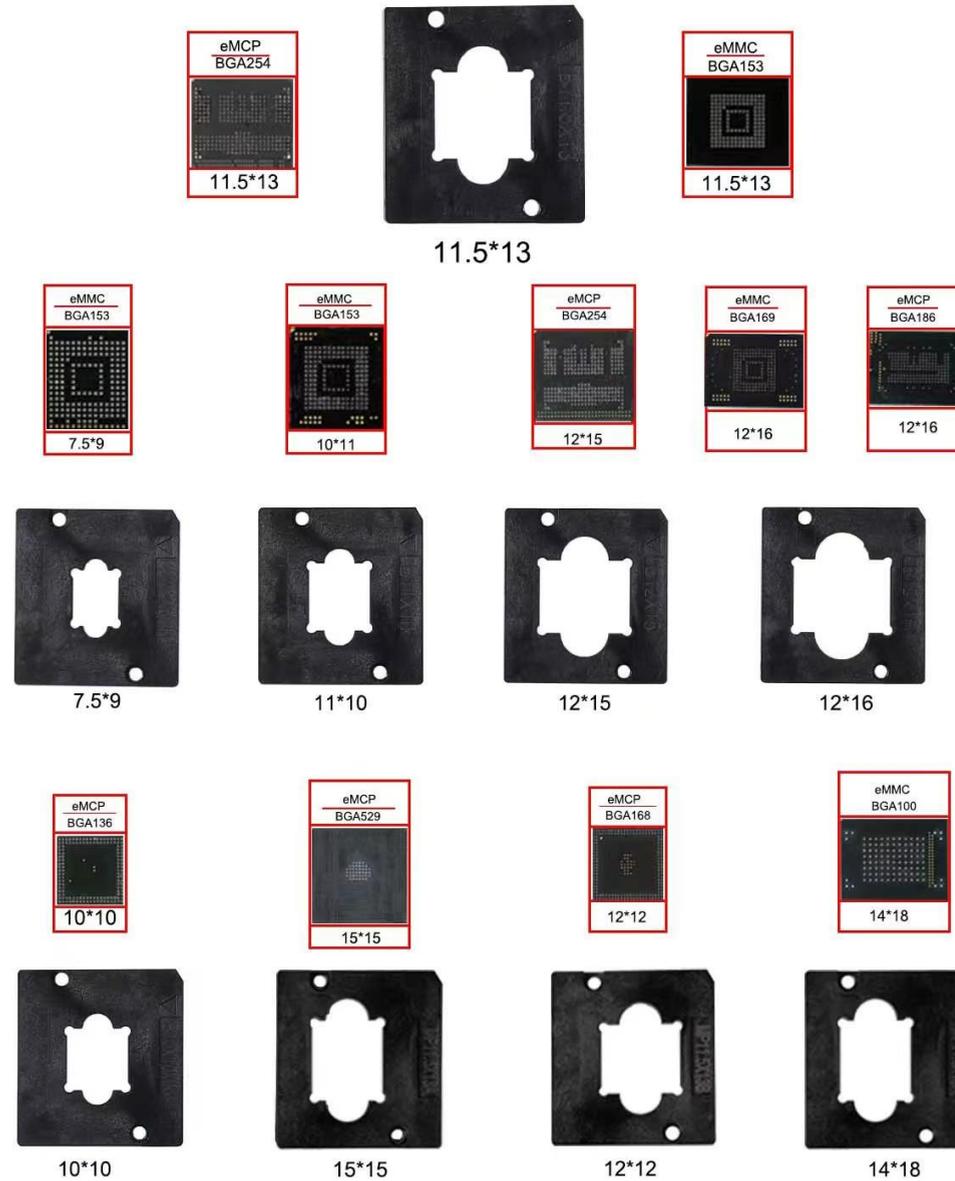
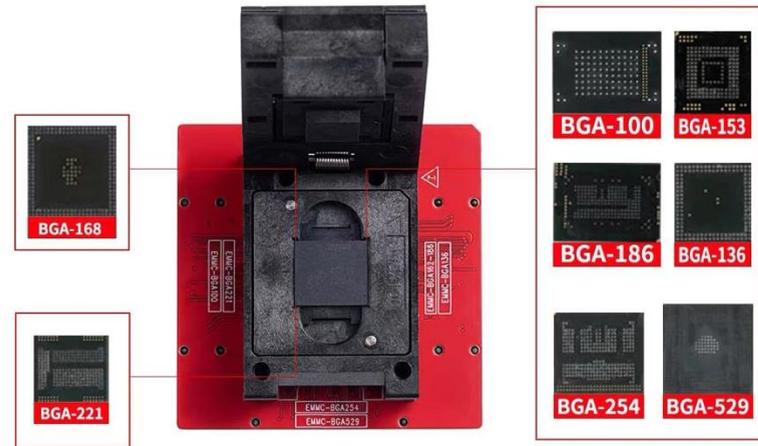
# eMMC / UFS



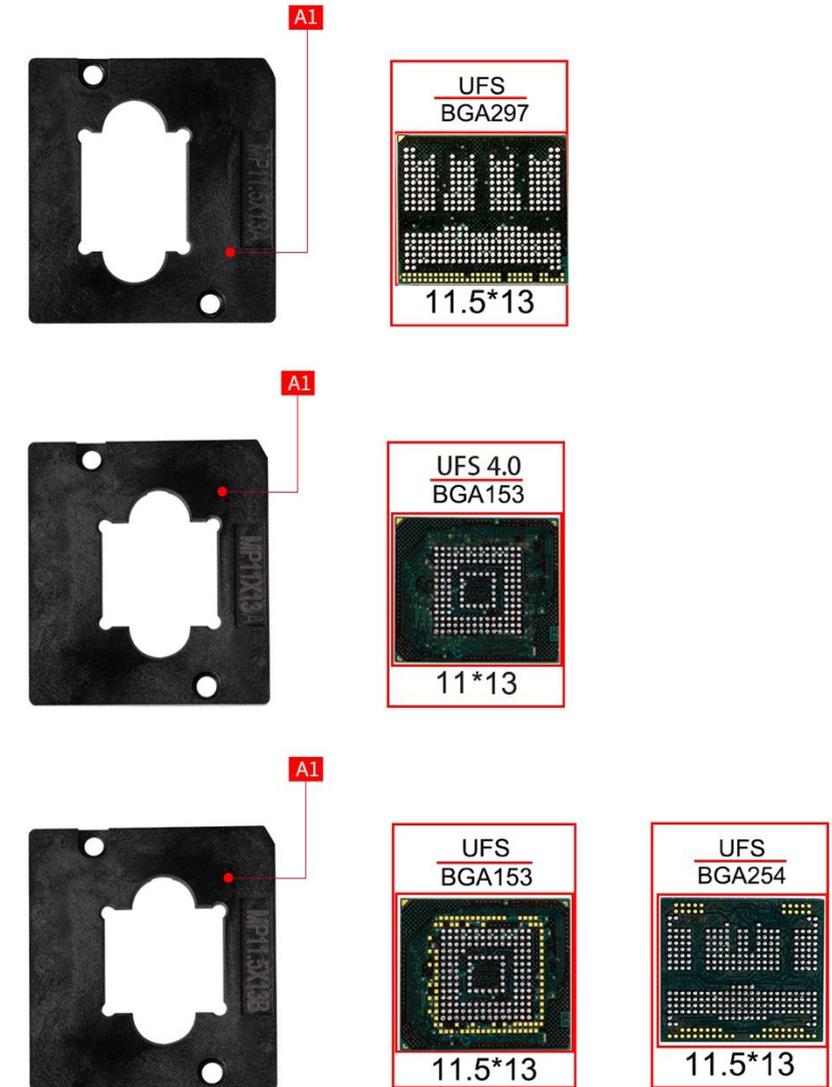
Mobile Phone  
IoT Device e.g. router  
Drone and Car

# 90% Coverage

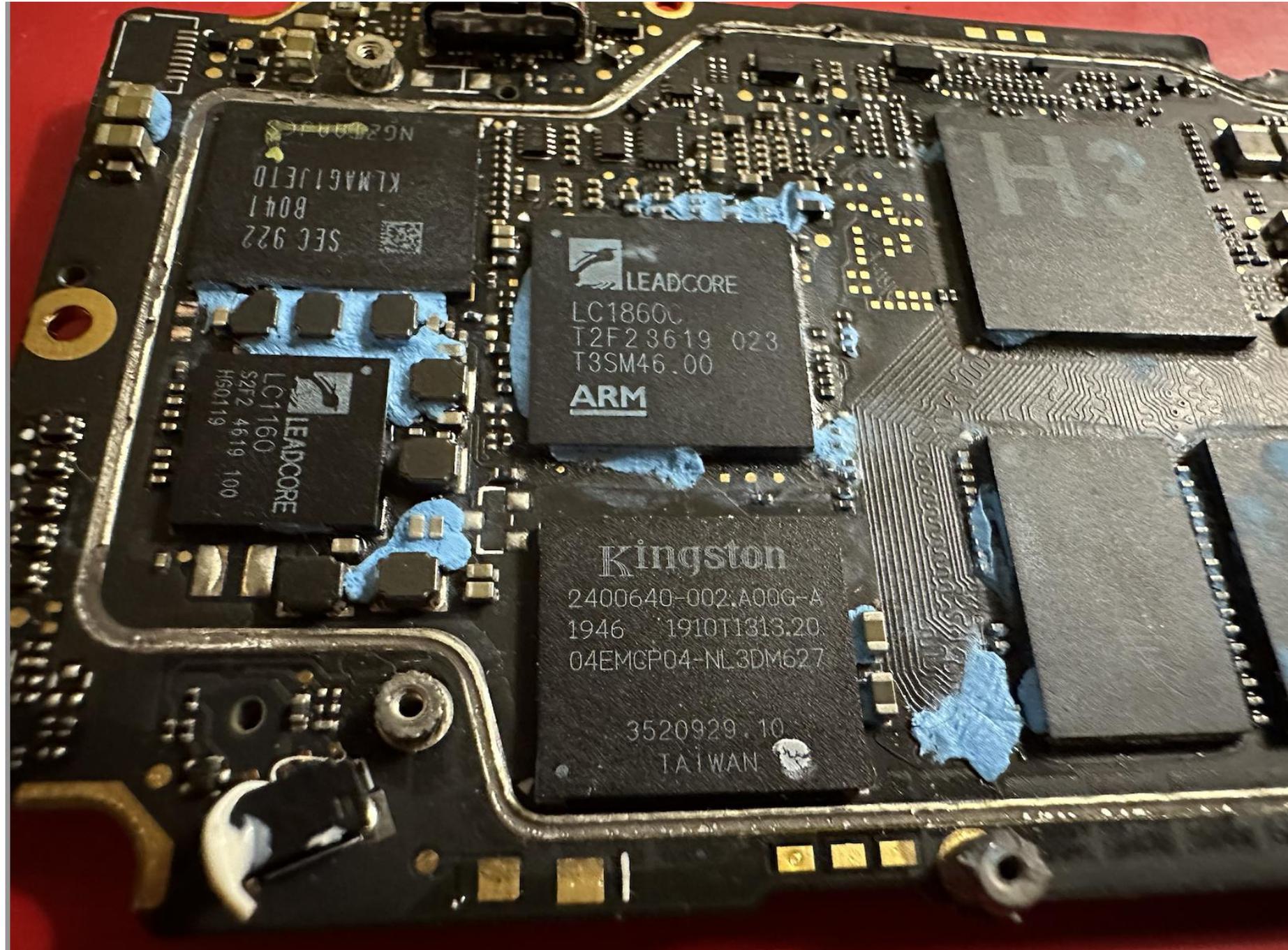
## 支持芯片&Support BGA



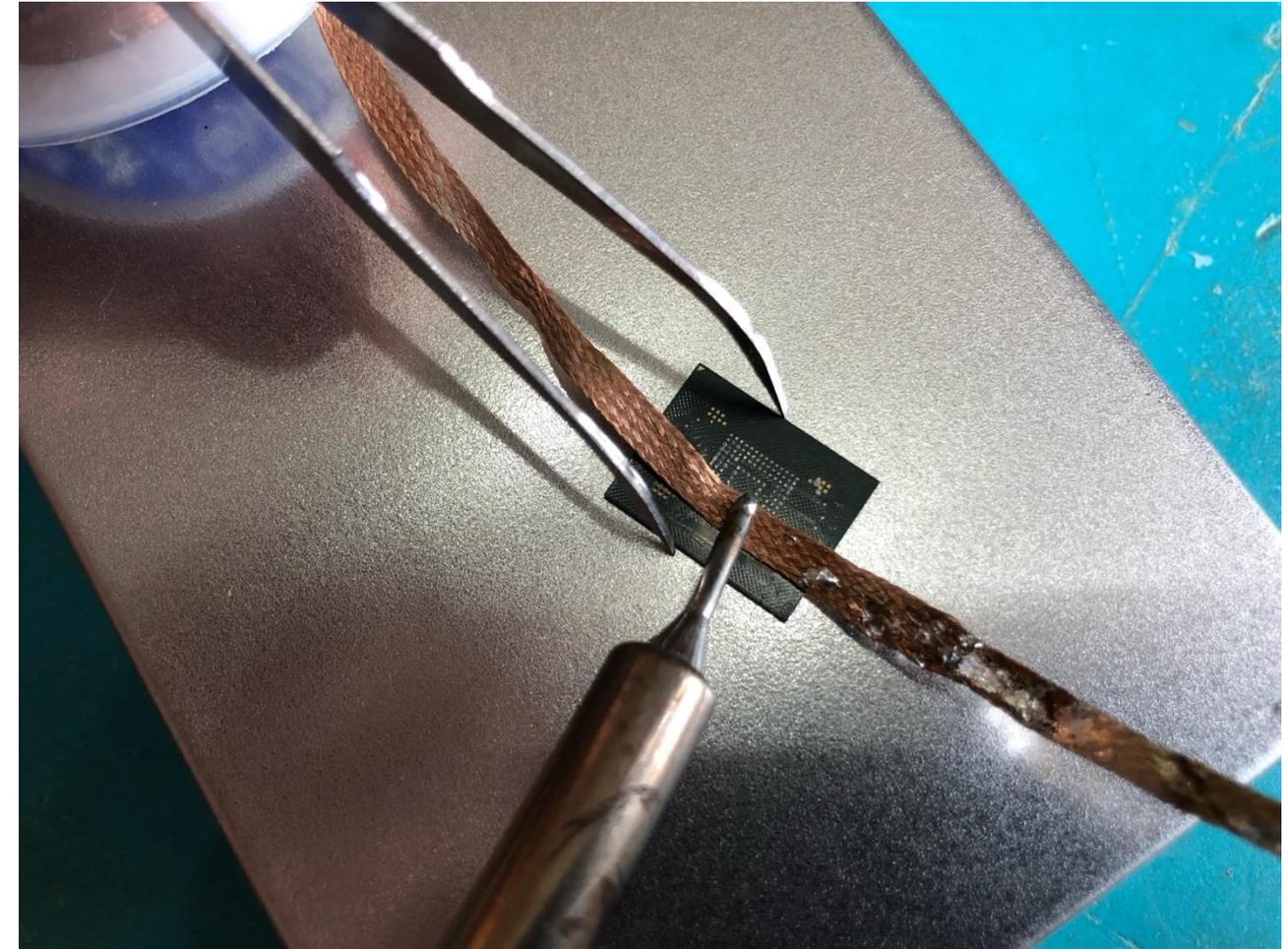
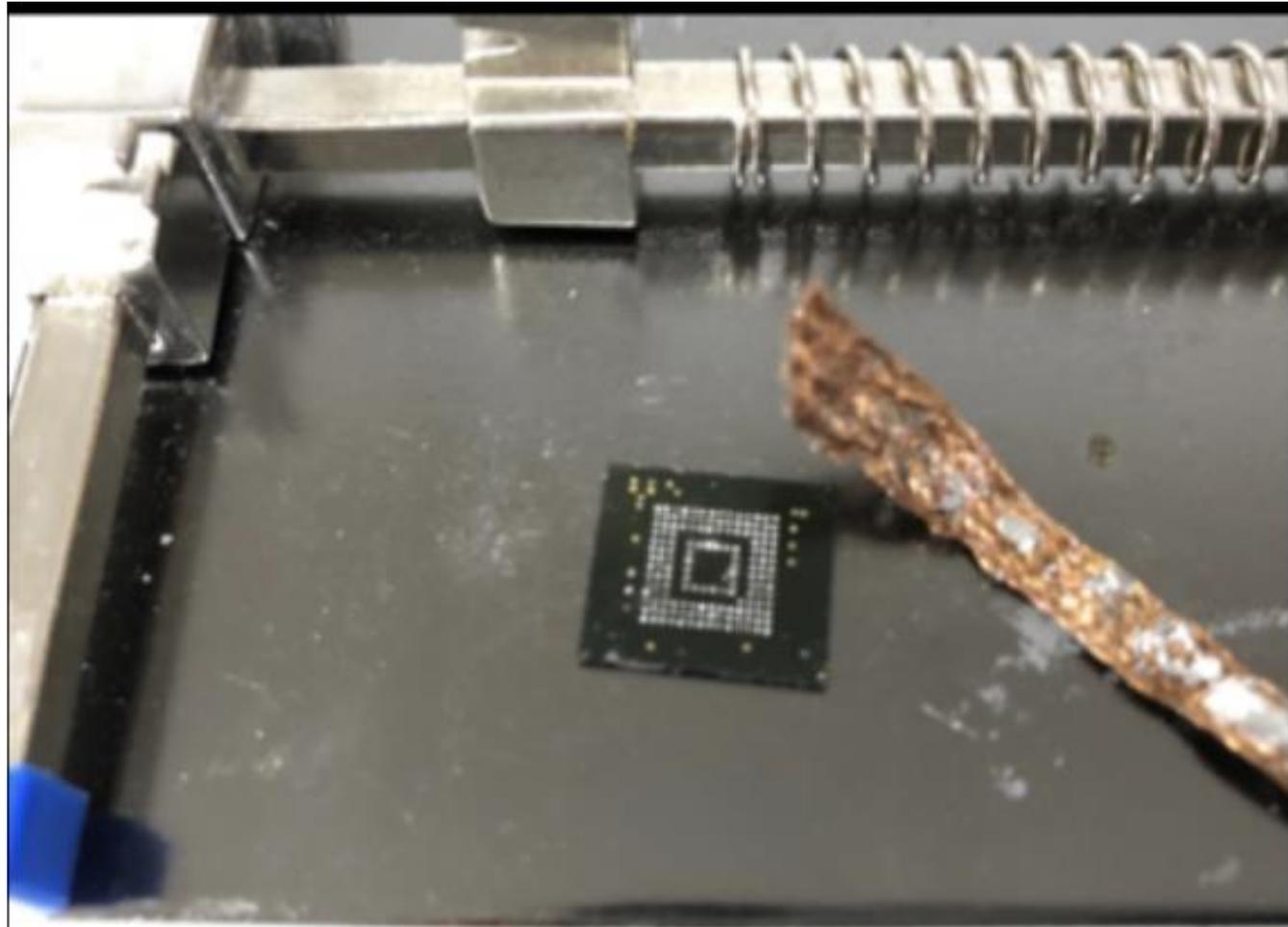
## 支持芯片&Support BGA



# Model / Version ?

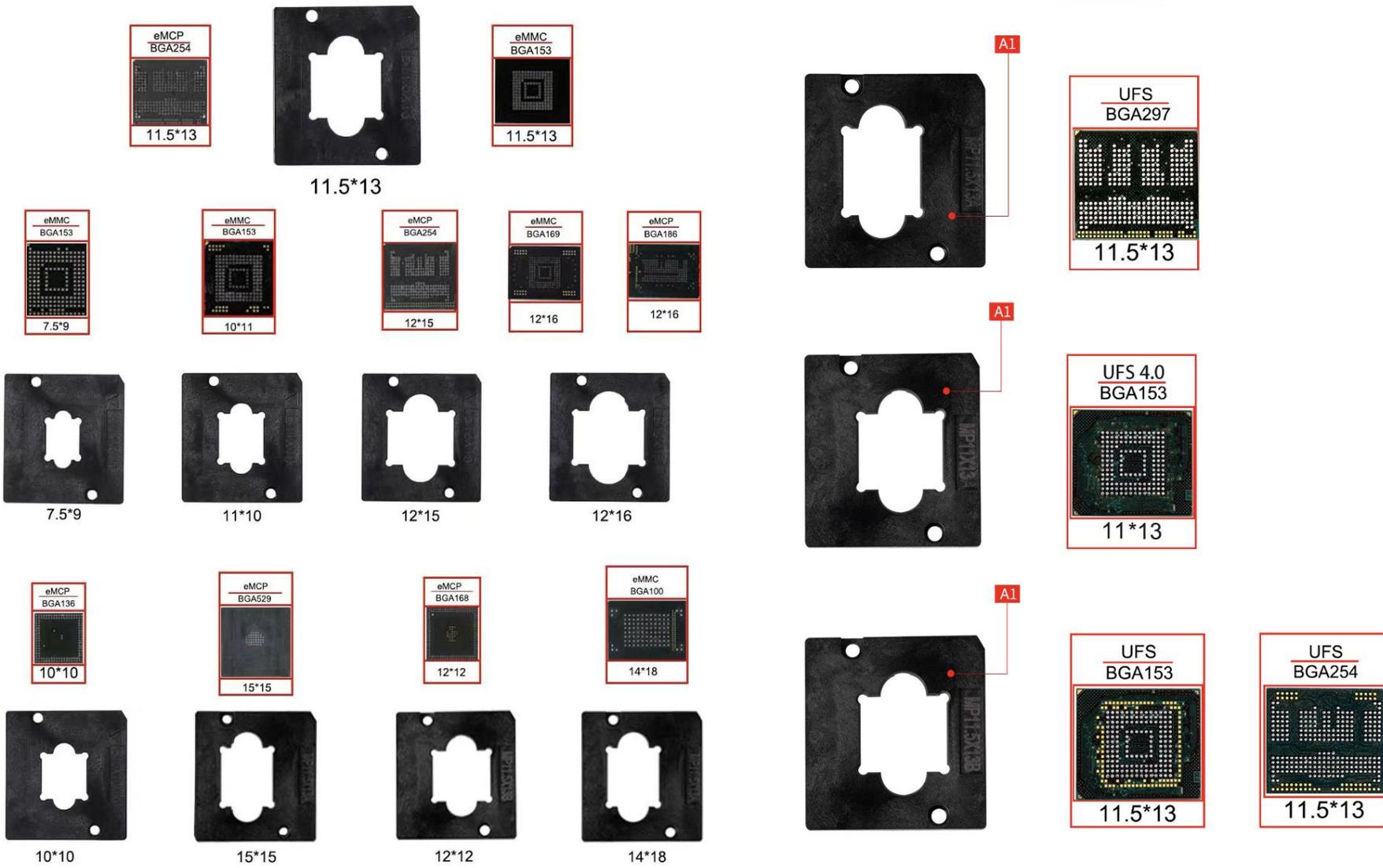


# Make Up



DC27 DEFCON – Chip Off Village  
<https://www.vxrl.hk/dcvxv/>

# PIN 1 / Indicator / Pointer



# Pointer



# MiPi Tester

<https://en.mipitester.com/>



# Other Box



# Demo

# Hardware Hacking Village



MALHAM  
SAUDI ARABIA

26-28 NOVEMBER 2024

# BLACK HAT

# MEA

REGION'S LARGEST CYBERSECURITY EVENT

# Question?



**Captain Kelvin** 立即驗證

OSCE<sup>3</sup>, OSEP, OSWE, OSED, OSCP, OSDA, OSWA, OSWP, KLCP | Black Hat / DEFCON Speaker & Trainer | Penetration Test | Digital Forensics | Incident Response | Hardware and Drone Security Researches & Analysis