

Chip-Off Forensics for Mobile Devices v3.0

The Chip-Off Forensics for Mobile Devices v3.0 is a new, updated, and exciting H-11 Digital Forensics certified 5-day training course for cell phone examiners and digital forensic experts. This course teaches our innovative No Heat chip removal technique, in addition to the Hot Air and Infrared Heat removal methods. New tools and techniques continue to show high rates of success while significantly lowering the risk of damage to the evidence. Students will leave this course with the knowledge and advanced skills needed to perform a successful Chip-Off on mobile devices, USB drives, SD drives and other devices for forensic extraction, examination, and investigations. This course will use tools from the [H-11 Mobile Device Chip-Off Lab Kits](#).

Day 1

Module 1: Course Overview and Flash Memory

- Overview
- The Forensic Process
- NAND and NOR Memory
- NAND Flash vs. eMMC Memory
- Mobile Device File and Operating Systems

Module 2: Introduction to Chip-Off

- What is Chip-Off?
- What type of devices use flash memory
- Flash Memory and Flash Memory Packages
- Small Outline vs. Multi-Chip Packages
- How do you remove the flash memory?
- Can the chip be damaged as it is removed?
- Can Chip-Off be used on iOS devices?
- Considerations

Module 3: Phone Research

- Purpose of Online Research
- What are you not going to find?
- Websites and types of data they provide
- Finding the FCC Grantee Code

Day 2

Module 4: Chip-Off for Mobile Forensics

- E-Mate Chip Reader and Adapters (All sizes):
 - eMMC 169
 - eMCP 162
 - eMCP 221
 - eMCP 529
- UP-828P Programmer and Adapters
 - UP-169P
 - UP-162P
 - UP-221P
 - UP-137P
- Medusa Pro Flasher Box
- Write Blocker
- Disk Management

Module 5: Cleaning the Chip

- Tools
- Types of Epoxy
- Cleaning the Chip
- Retining the Chip

Day 2 - Continued

Module 6: Removing the Flash Memory

- Hot Air Heat Removal
 - Hot Air Station
 - Preheater
 - Steps
- IR Heat Removal
 - T-862 IR Rework Station
 - IR Settings
 - Steps
- Micro Milling Removal
 - Micro Mill
 - Additional Tools
 - Steps
- Removing the Heat Shield
- Hands-on Exercises and Reality Check

Day 3

Hands-on Exercises from Modules 4, 5, and 6

Day 4

Module 7: Binary Image Types

- NAND Dumps
- Forensic Tools and Raw NAND Flash
- Generic Master Boot Record (MBR)
- Why an examiner should understand dump types

Module 8: Back Up and Evidence File Conversion

- Overview
- Create Forensic Image
- Drive Hash Verification Result

Day 5

Module 9: Bootloader Extractions

- Review Android Partitions
- How to install and use Android SDK, ADB and Fastboot tools
- Obtaining Root Permissions on a phone
- The recovery Partition on a Huawei Phone
- Command Line techniques for access and extractions

Final Practical and Hands-on Exam