H-11 DIGITAL FORENSICS

Advanced ISP–EDL–JTAG Cell Phone Data Recovery

The new updated H-11 Advanced ISP–EDL–JTAG Cell Phone Data Recovery is a certified 5-day course where students learn how to recover mobile data from embedded systems that are locked, damaged or unsupported. This recovery method works on newer devices that store data on eMMC or eMCP flash memory chips and recovered through the device's test points. Students will also learn how to properly identify test points and then create ISP pin-out diagrams that can be used for future digital forensic cases. Students will also learn how to use EDL to bypass device locks and encryption and identify JTAG connections. These techniques and methods are used in order to bypass security and perform full memory acquisitions for complete analysis of evidence. This course will use, and cover tools included in the ***H-11 ISP–EDL–JTAG Forensics Lab Kit***.

ISP	In-System Programming	Learn how to perform In-System Programming techniques to extract data from flash memory chips
EDL	Emergency Download Mode	Learn how to perform EDL steps to acquire physical and logical evidence from locked devices
JTAG	Joint Test Action Group	Learn the proper steps to extract memory data and create pin-out views of integrated circuits

Day 1

Module 1: Overview and Flash Memory

- Mobile Forensics Overview and the Forensic Process
- NAND and NOR and Flash Memory
- Mobile Device File and Operating Systems

Module 2: Phone Research

- Purpose of Online Research
- What you are NOT going to find
- Websites and types of data they provide for ISP, EDL, and JTAG. What do we need?
- Ways to obtain internal images of a device
- LAB: Researching technical characteristics of phones
- LAB: Phone research – which path to follow

Module 3: Binary Image Types, Analysis and Troubleshooting

- AXIOM; Oxygen; UFED; BlackLight; and FTK Imager
- Data Checks and Image Conversion
- Creating a Hash Value
- Other open-source tools (7zip and HEX Editors)
- LAB: Open a NAND flash phone dump
- LAB: Open an eMMC phone dump

Module 4: Soldering

- Types of solder and soldering irons
- Types and styles of soldering
- Soldering to the test points for JTAG and ISP
- Equipment for soldering
- Soldering for JTAG LAB
  - Preparing wires for JTAG soldering
  - Soldering to JTAG TAPs
- Soldering for ISP LAB
  - Preparing 40-gauge wire for soldering
  - Soldering to Surface-Mount Components

Day 2

Module 5: Origin and Purpose of JTAG

- JTAG origin and purpose
- JTAG overview
- Types of devices we can perform JTAG on
- Tools used for JTAG
- LAB: Researching support for phones in JTAG software (Medusa, Octoplus or RIFF2)

Day 3

Module 6: JTAG for Mobile Forensics

- LAB: Researching phones for JTAG extraction
- LAB: Performing JTAG extractions on mobile phones

Module 7: ISP for Mobile Forensics

- What is In-System Programming?
- ISP overview
- Type of Devices we can perform ISP examination
- Tools used for direct eMMC and eMCP reading
- LAB: Researching support for phones in ISP software (Medusa, OctuplusRIFF2, Z3X)
- LAB: Introduction to ISP Extraction

Day 4

Module 8: Tracing ISP Test Points

- Proper ISP Chip Removal
- Cleaning the PCB
- Identifying the Test Points
- LAB: Finding test points on a known phone
- LAB: Finding test points on an unknown phone

Module 9: Medusa Pro Software

- Putting tools together and defining a forensic method
- LAB: Multiple ISP extractions of different types of phones

Day 5

Module 10: Emergency Download (EDL) Mode Extractions

- What is EDL?
- How to get a phone into EDL Mode
- Test Points
- ISP-point grounding
- LAB: Performing EDL Extraction on Android phones using test points
- LAB: Performing EDL Extraction on Android phones using ISP-point grounding

Final ISP- EDL-JTAG Written and Hands-on Exam

Join our Mobile Forensic User Group: https://groups.google.com/forum/#!forum/mobile-device-forensics-and-analysis