H-11 DIGITAL FORENSICS

Advanced ISP-JTAG Cell Phone Data Recovery

Advanced ISP – JTAG Cell Phone Data Recovery is a certified 5-day course where students lean how to recover 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 access JTAG connections and apply techniques and methods in order to bypass security and perform memory acquisitions and analysis of this evidence. This course will use and cover tools included in the ***H-11 ISP-JTAG Forensics Lab Kit***.

Course Topics and Learning Points:

- Flash Memory | NAND vs. NOR
- ISP – JTAG Phone Research Methods
- Binary Image Types, Analysis and Troubleshooting
- Soldering to test points for JTAG and ISP
- ISP for Mobile Forensics
- Tracing ISP Test Points
- Using a phone's recovery partition to access device memory
- Command line tricks and instruction to obtain data from filesystem and physical extractions on a device

H-11 ISP-JTAG Forensics Lab Kit:

- Medusa Pro Box
- Hot Air / Soldering Station
- HDMI Microscope w/Monitor
- Digital Multi-meter
- Safety Goggles
- Safety Mask
- Anti-Static Mat
- ISP Tools
- JTAG Tools
- Soldering Tools
- Supplies

Cost:

H-11 Advanced ISP – JTAG Forensics Training and Lab Kit **$4,995**

H-11 Advanced ISP – JTAG Forensics Training Only **$3,795**

*Must have access to forensic tools similar to the ones included in the *H-11 ISP-JTAG Forensics Lab Kit*

H-11 ISP – JTAG Forensics Lab Kit - Standalone **$2,195**

Required Equipment:

Laptop – Windows 7, Windows 10, or Mac: Boot Camp Windows 7

Contact H-11 Digital Forensics today

Phone: +1.801.596.2727 Email: training@h11dfs.com Web: www.h11dfs.com

H-11 DIGITAL FORENSICS

Advanced ISP-JTAG Cell Phone Data Recovery

Advanced ISP – JTAG Cell Phone Data Recovery is a certified 5-day course where students lean how to recover 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 access JTAG connections and apply techniques and methods in order to bypass security and perform memory acquisitions and analysis of this evidence. This course will use and cover tools included in the ***H-11 ISP-JTAG Forensics Lab Kit***.

ISP → In-System Programming	Learning how to perform In-System Programming techniques to extract data from flash memory chips
JTAG → Joint Test Action Group	Learning the proper steps to extract memory data and create pin-out views of integrated circuits

Day 1

Module 1: Mobile Forensics Overview and Flash Memory

- Overview
- The Forensic Process
- NAND and NOR Memory
- Mobile Device File and Operating Systems

Module 2: Phone Research

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

Module 3: Binary Image Types, Analysis and Troubleshooting

- Axiom
- Cellebrite
- 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: JTAG for Mobile Forensics

- 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 and /or RIFF)
- LAB: Practical exercises for JTAG

Day 3

- LAB: Continues hands-on exercises for JTAG

Module 6: JTAG probing

- LAB: Using JTAG probing to find JTAG pinouts

Day 4

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 programming
- LAB: Researching support for phones in ISP software (Medusa, RIFF, Z3X)

Module 8: Tracing ISP Test Points

- Proper ISP Chip Removal
- Cleaning the PCB
- Identifying the Test Points
- LAB: Practical Exercises for ISP

Module 9: Medusa Pro Software and putting the tools together and defining a forensic method

Day 5

- LAB: Continued hands-on exercises for ISP
- Using a phone's recovery partition to access device memory
- Learning command line instruction to obtain filesystem and physical extractions on a device

Final ISP – JTAG Written and Hands-on Exam

H-11 DIGITAL FORENSICS

H-11 ISP-JTAG Forensics Lab Kit (136 pcs.) $2,195

Medusa Pro, Micro UART Cable, Optimus Cable, Medusa Pro JIG Adapter, USB A-B Cable, and solder boards

Hot Air / Soldering Station

14MP HDMI Microscope

22” Monitor for Microscope with HDMI Cable

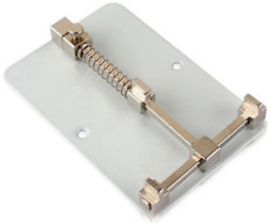
Digital Multi-meter with Sound and Multi-meter Probes

Personal Protective Equipment (PPE): Goggles, Dust Mask, Anti-Static Mat

iFixit Pro Tech Toolkit

Wire Cutters, Wire Strippers, and Assorted Solder Tips

Fiber Glass Pen, and Rosin Flux Pen



Cellphone PCB Holder

Dual USB Charger, Two Micro USB Cables, and USB Power Cable

Lead Solder Spool, Soderon 40 Gauge Wire, and Fine Braid Solder Wick

*Hardware tools and toolkits are subject to change, a comparable/equivalent tool will be substituted