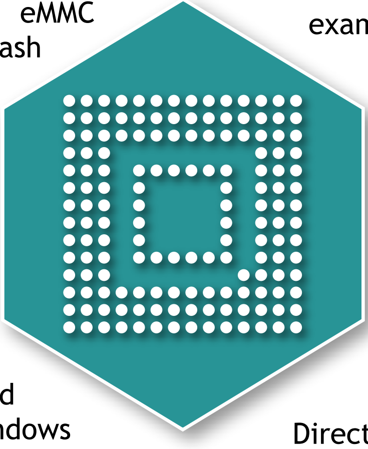
eMMC Device Forensics

ACQUIRE LOCKED & UNSUPPORTED DEVICES



A significant proportion of the locked and/or unsupported mobile devices received by forensic units will contain standards-based eMMC (embedded MultiMedia Card) flash memory chips whose interface is well understood. In many cases, physical extractions of eMMC flash memory chips can be performed by means of connecting to specific points on the printed circuit board of the device. This technique is referred to as 'Direct eMMC' or In-system Programming (ISP) and allows physical extractions to be performed on a wide range of both Android & Windows Phone handsets and tablet computers (regardless of an active lock). The techniques can also be used to perform physical extractions of TomTom units and an ever increasing range of devices which utilise eMMC chips.

> “BY FAR THE LEADER IN MOBILE PHONE FORENSIC TEACHING. FANTASTIC TEACHERS WITH ALWAYS UP TO DATE DOCUMENTATION.”

Course Aims

eMMC Device Forensics is a 4 day course designed to teach existing mobile device examiners how to perform physical extractions of eMMC-based devices which cannot be acquired using established commercial forensic tools & techniques. Delegates will learn how to identify devices which can be safely acquired using Direct eMMC and develop their skills in extracting data from devices of varying complexities. A key component of the course will be teaching delegates how to locate the Direct eMMC points on the circuit board of undocumented devices, such that they can utilise the techniques learned on the widest range of evidential exhibits back in the workplace.

Who should attend?

This course is targeted at existing phone examiners who have at least 6 months experience in mobile device forensics. The course includes close work with small components and therefore requires good eyesight and a steady hand. Previous experience in handset disassembly and soldering would be beneficial but not essential.

Direct eMMC vs. JTAG

Direct eMMC is in some ways similar to JTAG in that it is a non-destructive means of acquiring a physical dump of flash memory via the printed circuit board of a device. Direct eMMC complements, but is not a direct replacement for JTAG; some devices can be extracted using either technique, other devices may only support one of the two methods.

What you will learn

By the end of the course, delegates will be able to:

- Bypass locks on Android & Windows Phone handsets and tablets containing eMMC chips
- Perform physical extractions of unsupported Android & Windows Phone handsets, TomTom units & tablet computers using 'Direct eMMC'
- Locate Direct eMMC points on the printed circuit boards of undocumented devices
- Explain & justify their actions in court

contact

+44 (0)20 8133 8758
info@controlf.net
PO Box 167, Sandy, SG19 9AL

www.controlf.net

Dates & prices are on our website

Control-F®
DIGITAL FORENSICS

'We make it make sense'