E22 The Examination of Non-Functional Data-Storing Electronic Devices

Peter V. Mosher, Scott Thompson, BSc, and Greg Hudson, BSc, Centre of Forensic Sciences, 25 Grosvenor Street, Toronto, Ontario M7A2G8, Canada*

The goal of this presentation is to describe the types of damage and approaches to repair as well as details regarding the extraction of data from severely damaged devices, with emphasis on cellular telephones. This presentation will provide information and techniques to forensic examiners which will enable them to assess options when faced with the need to examine damaged devices.

The conventional forensic examination of fully functional data-storing electronic devices such as cellular telephones can be an involved and time consuming task with its own set of technical challenges. However, when confronted with a device that has been rendered non-functional due to physical or electronic damage, the examiner must weigh the potential evi- dentiary value of such an examination against the time and expertise that will be required to bring the device to a point where data acquisition can take place.

The Centre of Forensic Sciences Digital Evidence Unit has been exam- ining non-functional and/or damaged electronic devices, with particular emphasis on cellular telephones, since 2003. This approach to case item repair and data extraction was borne out of necessity, as although it could be argued that repairs could most easily be done by the manufacturer, chain of custody issues and the lack of local service representatives often made such an approach either unacceptable or simply infeasible. These inconve- niences led to the development of damaged device repair techniques, which range from correcting basic power-related problems to the imaging of data directly from non-volatile memory chips that have been physically removed from the circuit board of a device.

The thought of attempting a repair of a device as small and as techno- logically advanced as a cellular telephone may be intimidating to many examiners, but the majority of causes that render these devices non-func- tional are relatively straightforward to correct, requiring little more than a small amount of work and an identical phone, i.e. an exemplar, from which parts can be harvested. Examples of such causes of malfunction include broken or dirty connectors, corrosion from liquids such as water or blood, cracked or defective displays, fatigued solder joints, and defective batteries, among others. While it is sometimes impossible or impractical to repair a severely damaged device, experience at the Centre of Forensic Sciences laboratory suggests that basic repair of damaged devices could fall well within the existing capabilities of many forensic laboratories, and that damaged items should be considered for inclusion in evidence collection and examination policies.

Even when a device has been damaged to the point where it is beyond repair, it may still be possible to extract usable data. Should the memory “chips” themselves on the phone’s circuit board be undamaged, it is some- times possible to physically remove the chips from the board and perform a bit-level examination. While being more technically involved than a con- ventional examination, as well as being time consuming, this is an option that can be explored should the data need to be retrieved at any cost.

This presentation first examines the types and extent of damage that have been encountered in routine casework, and the level of technical training required to perform each type of repair. Discussion will include potential difficulties, information and material resources, data recovery techniques and related success rates. Particular emphasis will be placed on basic repair of cellular telephones, with examples of specific techniques being given. This will be followed by an overview of the process used to extract data from more severely damaged devices, and will include a dis- cussion of the details of populating the memory of an exemplar, removing and imaging the memory chip, building a memory map using a hexa- decimal editor, creating a procedure, and carrying out the examination on the submitted device.

Digital Evidence, Electronic Device, Cellular Telephone

 ** Presenting Author*