Digital Forensic Traces in Radio Communication Equipment

UCD Forensics and Security Research Group

Arie Kouwen, Nhien-An Le-Khac and Mark Scanlon
School of Computer Science, University College Dublin, Ireland.
arie.kouwen@ucdconnect.ie, an.lekhac@ucd.ie, mark.scanlon@ucd.ie

Motivation

Historically, radio-equipment has solely been used as a two-way analogue communication device. Today, the use of radio communication equipment is increasing. The functionality of these traditionally short-range devices have expanded to include smartphone level functionality including private calls, address books, call-logs, text messages, data, lone worker, telemetry, data communication, GPS, etc. Many of these devices also directly integrate with smartphones, which delivers Push-To-Talk services. This makes it possible to setup connections between users using a two-way radio and a smartphone. In fact, these devices can be used to connect users solely using smartphones. To date, there is little research on the digital traces in modern radio communication equipment, which is often considered critical infrastructure [1]. Increasing the knowledge base about these radio communication devices and services can be valuable to law enforcement as these devices are already being discovered in cases. The market for two-way radio is growing worldwide. According to Hytera (one manufacturer of Private Mobile Radios), there was a 100% market growth from 2014 to 2015. The market for Land Mobile Radio (LMR) Systems is expected to grow to $42 billion by 2022.

Figure 1. Digital Two-Way Radio Equipment

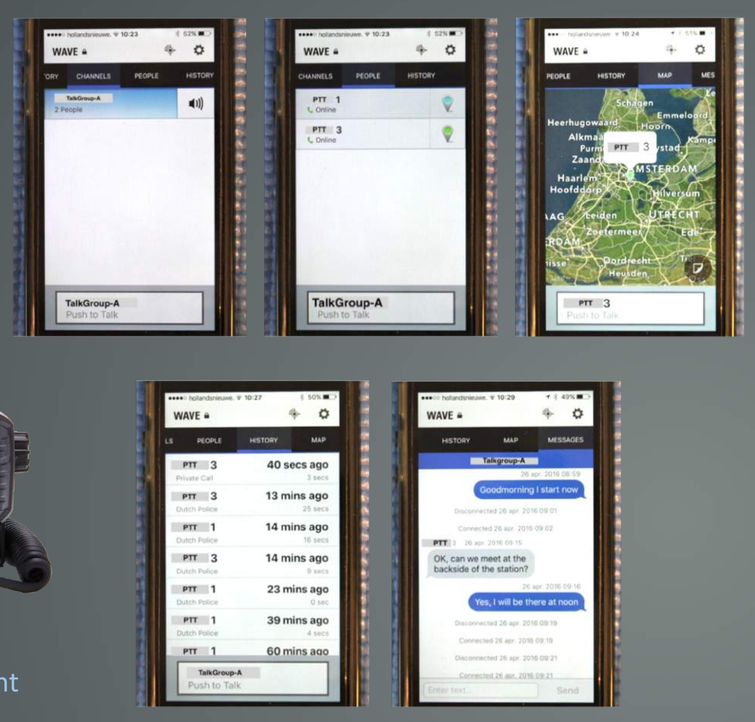

Figure 2. Example Smartphone Functionality over Radio

Problem Statement

Radio communication equipment is migrating from analogue devices to digital devices with new features commonly found in smartphones, such as call logs, address books, short messages, data communication and GPS. If digital investigators encounter digital radio communication equipment, it is necessary to have knowledge about the radio communication equipment, radio infrastructure, and associated services. However, there is little literature available on the topic. It is also often difficult to expand digital forensic capability when dealing with the current backlogs [2].

To get a general insight into the existing knowledge of law enforcement digital experts, a questionnaire was sent out to Dutch Experts eXchange (DEX) members. Of the 47 respondents, 12 had previously encountered radio communications in their cases; Digital two-way radios were encountered in 7 cases, analogue two-way radios in 6 cases, smartphones with Push-To-Talk features in 4 cases, VHF/UHF transceivers in 3 cases, shortwave transceivers in 2 cases, WiFi two-way radios in 2 cases, data communication modem connected to a radio transceiver in 1 case, and Software Defined Radio in 1 case. This leads to the following problems to be addressed for an investigator:

- Who are the users of radio communication equipment?
- Which equipment used for radio communication is worthy for investigation and which digital forensic traces may exist in radio communication equipment?
- Is it possible with popular digital forensic tools to acquire radio communication equipment?
- How can forensically interesting data in the radio communication equipment be acquired?
- Where can other possible traces of evidence be found?

Evidence Acquisition

Popular mobile-focused digital forensic tools on the market are Cellebrite's UFED Physical Analyzer, Magnet Acquire, MSAB's XRY and Blackbagtech's Blacklight. These are used to acquire GSMs, smartphones, and navigation equipment. However, we could not find support for two-way radio devices from any of the above-mentioned applications. Requests for information were sent to Cellebrite, MSAB and Magnet Forensics and all three companies replied that they do not have any experience with two-way radio and do not plan to invest in it in the future.

In the daily work of a digital investigator, it is not always possible to do an extraction of every mobile device encountered. Sometimes, a mobile device is not supported by forensic software or there may be a risk of losing data when performing an extraction. In these cases, a manual extraction with the help of photography based device investigation software, e.g., Fernico's ZRT3. This is the case with most two-way radios. With ZRT3, digital photos are taken from the screen contents of the mobile device.

Investigation Methodology

To guide investigators, we propose a novel workflow that could be followed in case of encountering radio equipment, as outlined in Figure 3.

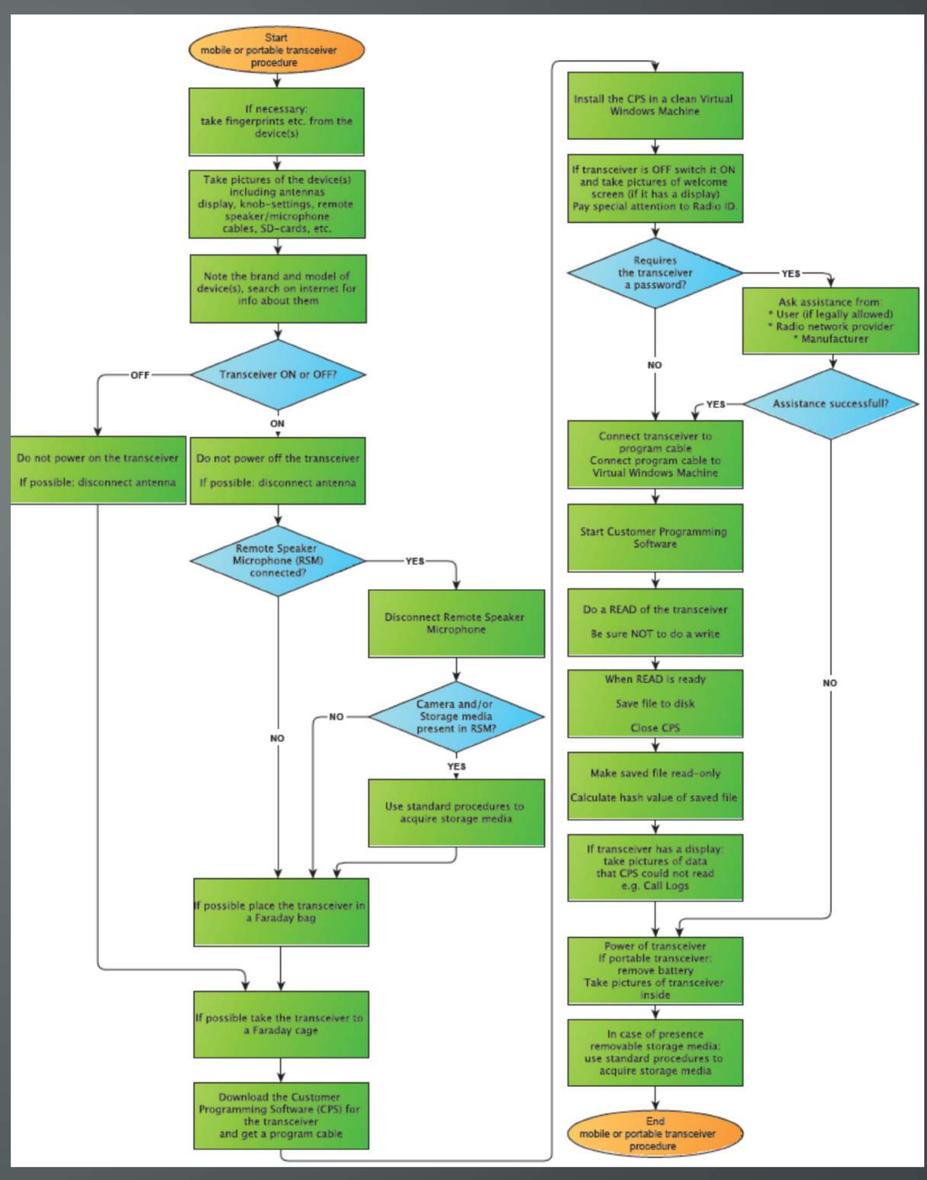

Figure 3. Investigative Workflow for Processing Mobile or Portable Two-Way Transceiver

Conclusion and Future Work

Law enforcement digital experts must investigate digital radio equipment. Industry is moving towards integrated devices, so it is to be expected that increasingly often radio communication equipment, combined with smartphone connectivity, will be encountered at crime scenes. Therefore it is important to get access to the radio devices with forensic tools. That is why API possibilities, JTAG and chip-offs must be researched and developed, in a similar manner to mobile phone forensics [3].

References

[1] Baldini G.,Karanasios S., Allen D., Vergari F., Survey of Wireless Communication Technologies for Public Safety. IEEE Communications Surveys & Tutorials 2014;16(2):619–641.

[2] Scanlon M. *Battling the Digital Forensic Backlog through Data Deduplication*. In: Proceedings of the 6th IEEE International Conference on Innovative Computing Technologies (INTECH 2016), Dublin, Ireland, 2016.

[3] Alghafli K.A., Jones A., Martin T.A., Forensics Data Acquisition Methods for mobile phones. In: International Conference for Internet Technology and Secured Transactions. IEEE; 2012:265–269.

Scan to download a preprint of our DFRWS USA paper on this topic

www.ForensicsAndSecurity.com