Digital Investigation 26 (2018) S77–S86

Contents lists available at ScienceDirect

Digital Investigation

journal homepage: www.elsevier.com/locate/diin

DFRWS 2018 USA — Proceedings of the Eighteenth Annual DFRWS USA

Digital forensic investigation of two-way radio communication equipment and services

Arie Kouwen [a], Mark Scanlon [b, *], Kim-Kwang Raymond Choo [c], Nhien-An Le-Khac [b]

[a] *School of Computer Science, University College Dublin, Ireland*
[b] *Forensics and Security Research Group, University College Dublin, Ireland*
[c] *Department of Information Systems and Cyber Security, University of Texas at San Antonio, USA*

Keywords:
Digital radio
Ham
Push-to-Talk
Forensic process
Digital forensics

ABSTRACT

Historically, radio-equipment has solely been used as a two-way analogue communication device. Today, the use of radio communication equipment is increasing by numerous organisations and businesses. The functionality of these traditionally short-range devices have expanded to include private call, address book, call-logs, text messages, lone worker, telemetry, data communication, and GPS. Many of these devices also integrate with smartphones, which delivers Push-To-Talk services that make 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 only using smartphones. To date, there is little research on the digital traces in modern radio communication equipment. In fact, increasing the knowledge base about these radio communication devices and services can be valuable to law enforcement in a police investigation. In this paper, we investigate what kind of radio communication equipment and services law enforcement digital investigators can encounter at a crime scene or in an investigation. Subsequent to seizure of this radio communication equipment we explore the traces, which may have a forensic interest and how these traces can be acquired. Finally, we test our approach on sample radio communication equipment and services.

1. Introduction

Since Guglielmo Marconi (1874–1937) made a radio connection over a few kilometres in 1895, there have been many developments in the world of radio equipment. Over the past decade, a trend is noticeable in commercial radio-equipment increasingly switching from analogue to digital. When speaking of digital two-way radios, this digital equipment has several facilities which are commonly found on cellphones, such as address books, short message services, call logs, GPS, telemetry (the automatic measurement and wireless transmission of data from remote sources), etc. Today, telemetry applications include measuring and transmitting data from sensors located in vehicles, smart meters, power sources, robots, and even wildlife in what is commonly referred to as the Internet of Things.

Two-way radio is often referred as “professional mobile radio”, “private mobile radio” (PMR), or “land mobile radio” (LMR), and colloquially referred to as walkie-talkies. Two-way radios most often use the Very High Frequency (VHF) and Ultra High Frequency (UHF) bands. Portable two-way radios have a communication distance of a few kilometres when directly transceiving to/from each other but when they make use of radio repeaters or Radio over IP (RoIP) the distance is almost unlimited. Overby and Cole outlines a comparison of telephony and two-way LMR services and a comparison of radio over IP and LMR IP trunking (Overby and Cole, 2008). Radio technologies are also used in Public Protection and Disaster Relief (PPDR) emergency response systems (Barbatsalou et al., 2014).

Push-To-Talk (PTT) services are increasingly used to communicate between different kinds of devices and radio equipment. There are numerous smartphone applications designed specifically for this purpose. One example of this is the WAVE Communicator application from Motorola, which uses their “WAVE Work Group Communications Solution”. This makes it possible to directly communicate between two-way radios and smartphones. Some smartphones have a special PTT button, a soft-button on the screen,

* Corresponding author.
E-mail addresses: arie.kouwen@ucdconnect.ie (A. Kouwen), mark.scanlon@ucd.ie (M. Scanlon), raymond.choo@fulbrightmail.org (K.-K. Raymond Choo), an.lekhac@ucd.ie (N.-A. Le-Khac).

https://doi.org/10.1016/j.diin.2018.04.007

or reassigns an existing button, e.g., using the volume down to act as a PTT button. This makes radio communication equipment more popular among organisations that need group communication facilities that are independent of public communication infrastructures in case of an outage of this public infrastructure.

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.Land Mobile Radio (LMR) Systems (TETRA, Project 25, dPMR, DMR and TETRAPOL) market is expected to grow to $42 billion by 2022 (Acute Market Reports, 2016). Although communication possibilities such as cellphones, smartphones, phone lines, leased lines, and Internet exist, the infrastructure needed for these communication methods can experience blackouts. Certain parts of a nation's infrastructure are often considered critical as a failure or disruption can have serious consequences (Klaver et al., 2013). Because of this, mission-critical organisations resort to two-way radio, with which they can continue communication in case of infrastructural issues (Baldini et al., 2014).

Law enforcement agencies do not have much expertise with radio-equipment such as HF-, VHF- and UHF-Transceivers, Packet Radio, Digital Mobile Radio, Software Defined Radio (SDR), etc. Traditionally, this did not present a problem as radio equipment did not have much forensic value. However, modern systems use a variety of digital techniques such as digital speech- and data-channels, programming, and GPS. Data communication such as email, chat, location tracking or telemetry are also possible and have long showed promise for vehicular communication (Feher, 1991). Digital Mobile Radio can connect to backbone-equipment, which can further connect radio-transceivers with each other or, via internet-links, to other remote areas anywhere in the world. Furthermore, telecom operators and radio equipment rental companies in European countries are also offering PTT services.

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. The knowledge of the Dutch digital experts gives a mixed view. There are digital experts who have already encountered radio communication equipment and/or services at a crime scene and a number of cases where criminals used it to aid in the execution of their crimes, and those who have not. 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. 68.1% of the respondents “do not know” or “have little knowledge” of the intricacies of modern radio communication equipment. The majority of respondents (82.6%) identified that they would like to know more about the subject. Furthermore, the answers showed that radio communication is in use by criminals who obviously use it to hide their communication from being picked up by law enforcement. There were also cases in which radio communication was used in normal business situations. The overall results showed that more research for the subject was needed.

Because of the existence of this equipment and these services, it is likely that police will encounter this equipment in more and more cases, especially with the opportunity for criminals to leverage the technology in combination with other devices. Law enforcement are continuously battling to keep up with new technologies and devices (Lillis et al., 2016), while dealing with current digital evidence backlogs (Scanlon, 2016) However, there is very little research both in literature and by practitioners on digital forensic traces in radio communication devices. Therefore, in this paper, we present the forensic acquisition and analysis of radio communication equipment and services, and a workflow to aid investigation. We also evaluate the possibility of using popular forensic tools to acquire artefacts from radio communication equipment. We also test our approach with different scenarios and propose a workflow for radio device investigation.

1.1. 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. Because of these digital features and other benefits, radio communication equipment is increasingly used today. In addition, telemetry applications can make use of radio communication equipment and is in use by companies and organisations that need control data for their objectives. 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.

When digital experts do not investigate digital radio communication equipment, valuable evidence may be neglected. This can be the case when a digital expert is not aware of the features of radio communication equipment and their networks. The following research questions are defined to get an insight into the current general knowledge level of digital investigators, the radio communication equipment and its users, where evidence can be found and how to get this evidence.

1. Who are the users of radio communication equipment?
2. Which equipment used for radio communication is worth to be investigated and which digital forensic traces may exist in radio communication equipment?
3. Is it possible with popular digital forensic tools to acquire radio communication equipment?
4. How can forensically interesting data in the radio communication equipment be acquired?
5. Where can other possible traces of evidence be found?
6. Forensic acquisition and analysis

2. Background

There are several manufacturers of digital radio communication equipment and software. The common brands are Motorola, Hytera, Sepura, Kenwood, ICOM, Vertex, Yeasu, Harris, Tyt Radio, amongst others. They offer portable and mobile two-way radios, repeaters and all kind of accessories such as headsets and remote speaker microphone (RSM) sets.

2.1. Features of digital radio equipment

Digital two-way radios both mobile and portable make use of one of the aforementioned standards. These digital standards make it possible, besides regular voice communication, to use many additional features and options. The features and options include:

- Radio-ID: This identifies the radio unit in the network. With TETRA it is called an Individual Tetra Subscriber Identity (ITSI) and consists of 3 individual numbers: Tetra Mobile Country Code (TMCC), Tetra Mobile Network Code (TMNC) and the Short Subscriber Identity (SSI). With DMR a Radio-ID and optionally a Radio Alias can be programmed.
- Talkgroups: Users/radios connected to the same talkgroup can communicate with each other. A user can switch to another