Digital Forensic Investigation of Two-Way Radio Communication Equipment and Services

ARIE KOUWEN, **MARK SCANLON**, KIM-KWANG RAYMOND CHOO, AND NHIEN-AN LE-KHAC

UCD Forensics and Security Research Group

Agenda

- Brief overview of two-way radios
- Motivation of this work
- Case Studies with Investigative Workflows:
  - Radio Email (radio transceiver connected to a modem)
  - Device Investigation (Hytera PD785G)
  - Smartphone Push-to-Talk application
- Conclusion and Future Work

Two-Way Radios

- a.k.a. Professional Mobile Radio, Private Mobile Radio, Land Mobile Radio, or just "walkie-talkies"
- Popularly used across several application areas, including:
  - Public Safety Organisations – Police, Ambulance, Fire
  - Private Security Companies
  - Enterprise and Business
  - Marine and Aviation
  - Military
  - HAM Radio Amateurs

Digital Two-Way Radios

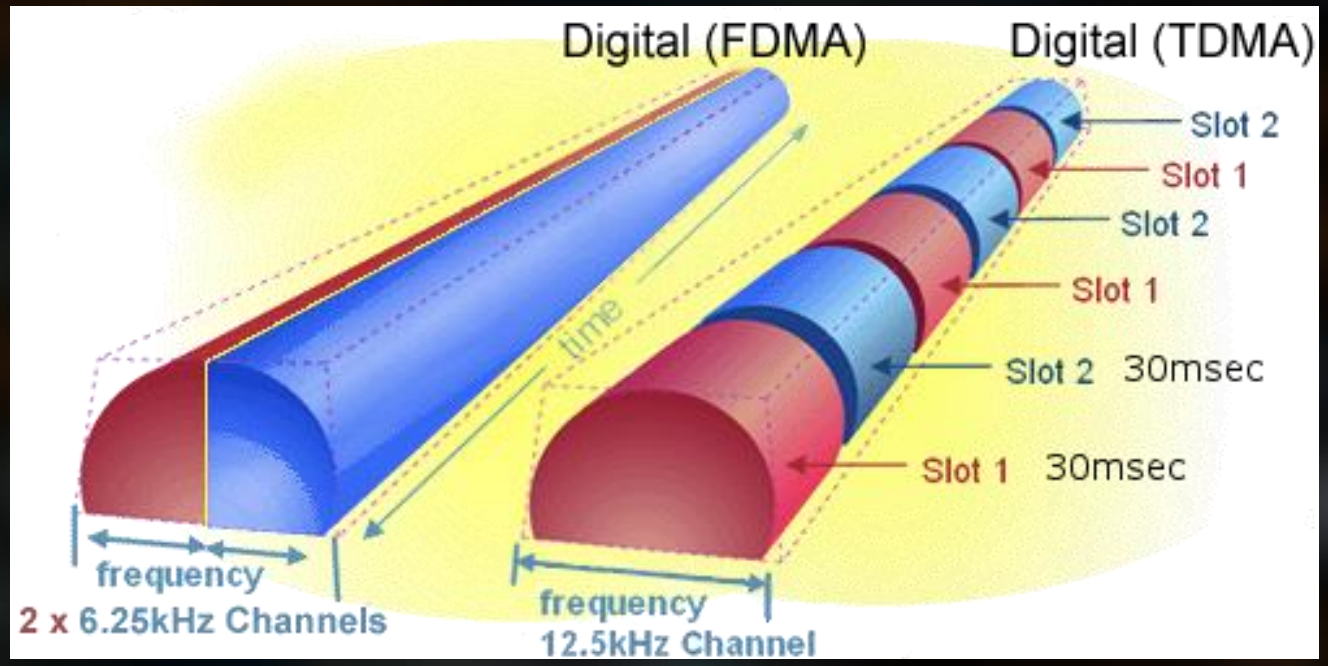
- Enhanced functionality
  - Radio-ID is used to identify each radio on the network
  - Talkgroups
  - Private call
  - Roaming - automatic channel switching
  - Address Book
  - Short Message Service
  - Encryption – voice, text and data
  - Remote Monitoring – operator can listen in remotely
  - GPS
  - Smartphone Tethering

Communication Range

- Typically have a communication range of a few kilometres for handheld devices
- Tower based radios can have a range up to 50km
- Radio repeaters or Radio over IP (RoIP) can result in almost unlimited distances

Communication Channels

- With Frequency Division Multiple Access (FDMA), a piece of the radio spectrum is divided into different channels with a certain bandwidth.
  - Every user on the same channel can communicate with each other.
- With Time Division Multiple Access (TDMA), a channel is divided into time slots
  - Users on the same frequency and timeslot can communicate with each other.



Are these devices actually encountered in the wild?

- Survey conducted of Dutch Experts Exchange members
- Of the 47 respondents, 12 had encountered radio communication equipment in cases
  - Digital two-way radios: 7 cases
  - Analogue two-way radios: 6 cases
  - Smartphones with Push-to-Talk: 4 cases
  - VHF/UHF transceivers: 3 cases
  - Shortwave transceivers: 2 cases
  - Wifi two-way radios: 2 cases
  - Data communication modem connected to radio transceiver: 1 case
  - Software defined radio: 1 case

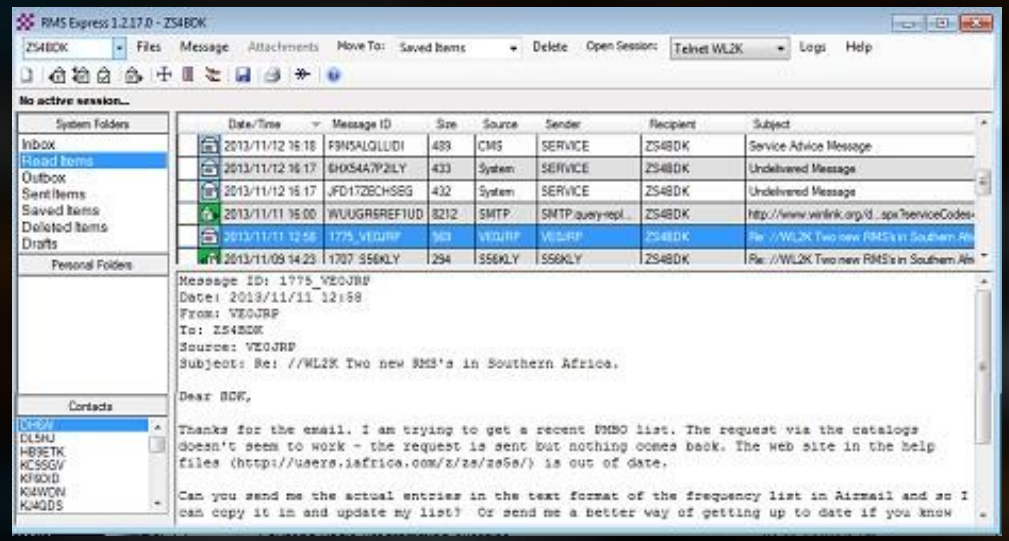
Motivation for this Work

- The digital two-way radio market is growing
  - The largest equipment manufacturer, Hytera, reported 100% YoY growth
  - The two-way radio market is expected to grow by $42b by 2022 (Acute Market Reports)
- These devices have been encountered in real-world cases
  - Communication between suspects
  - Communication between employees of a company under investigation
  - Secure out-of-band communication
- Cellebrite UFED, Magnet Acquire, MSAB XRY, and Blackbagtech's Blacklight are incompatible with two-way radios
- Little guidance for performing these investigations

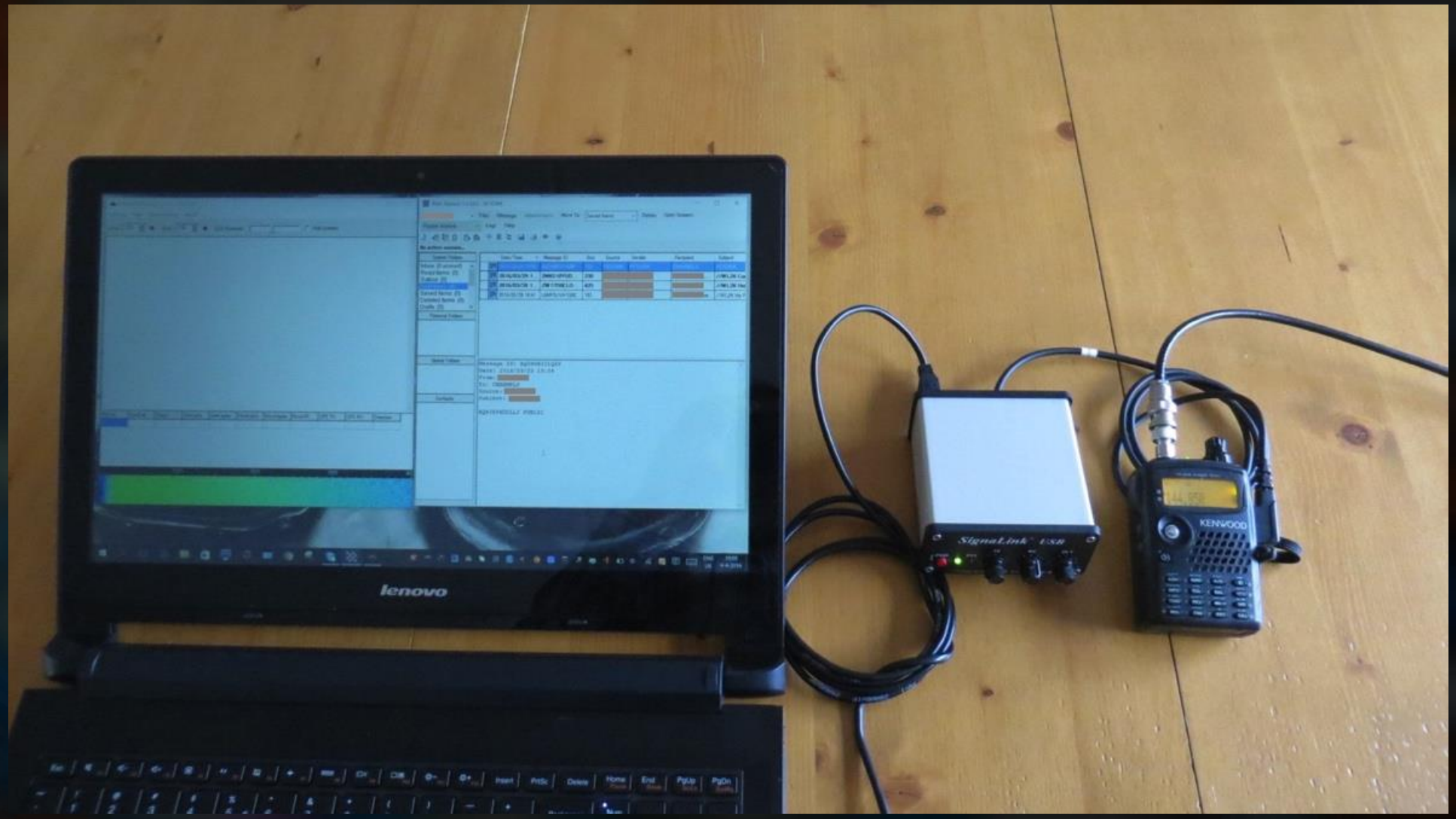
Case Study 1:
Winlink Radio Email

Experimental Setup

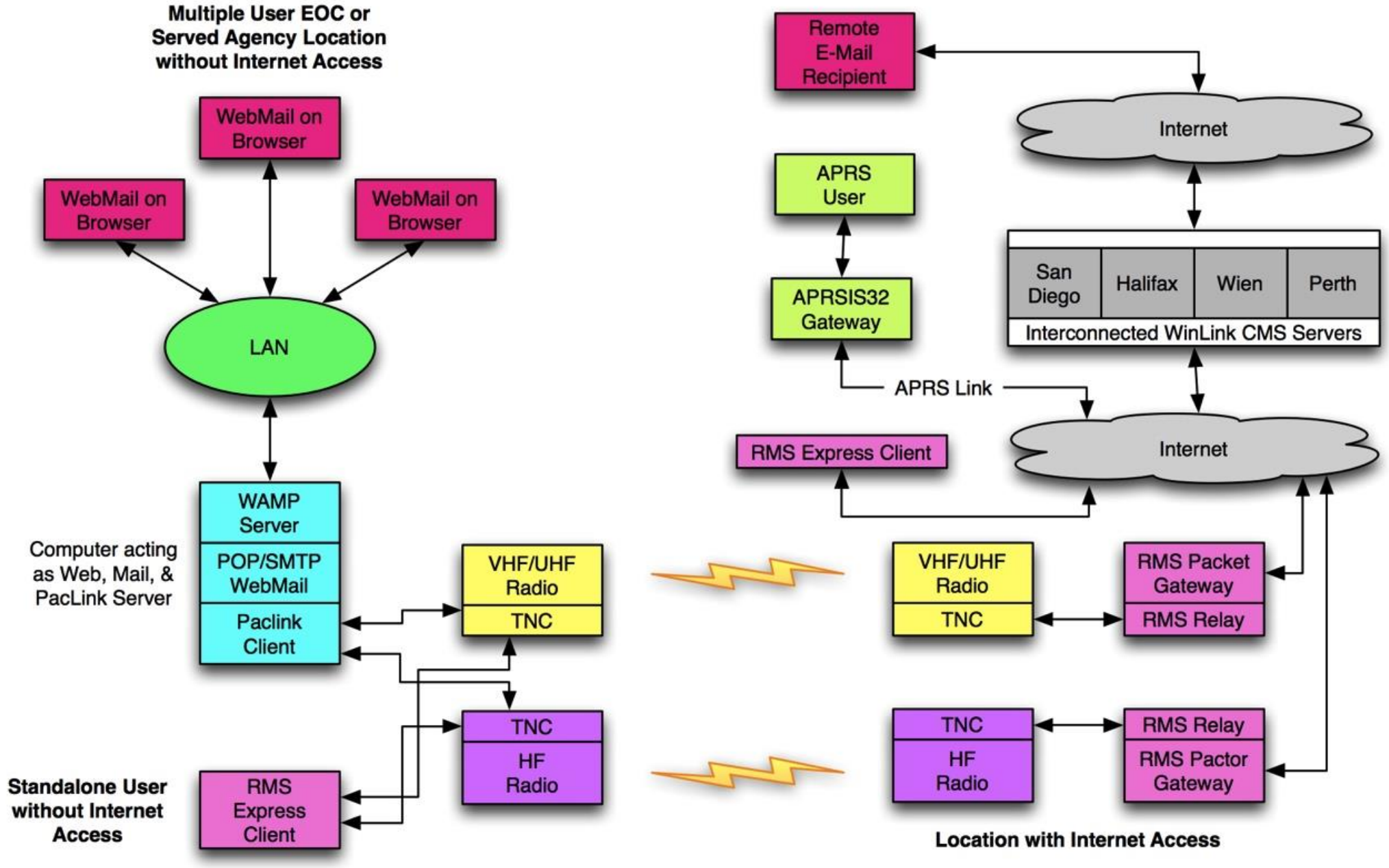
- A Kenwood TH-F7E VHF/UHF portable transceiver.
- A Diamond X-30 antenna.
- A Tigertronics Signalink-USB Soundlink modem.
- A Windows 8 PC with RMS Express installed and sound modem application



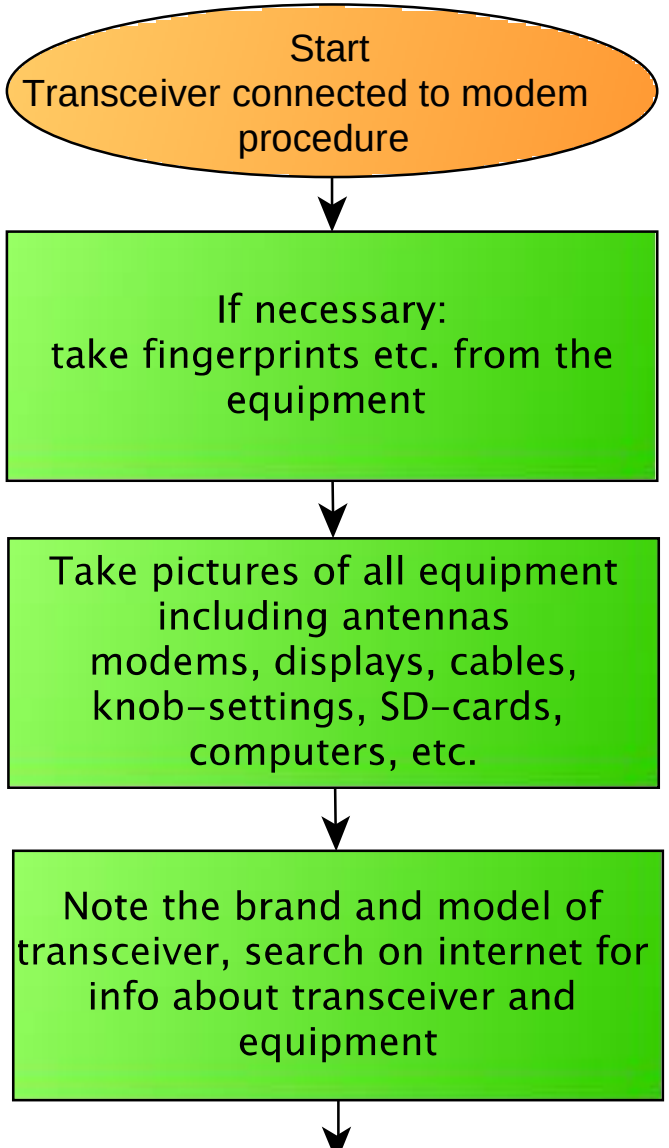
Experimental Setup

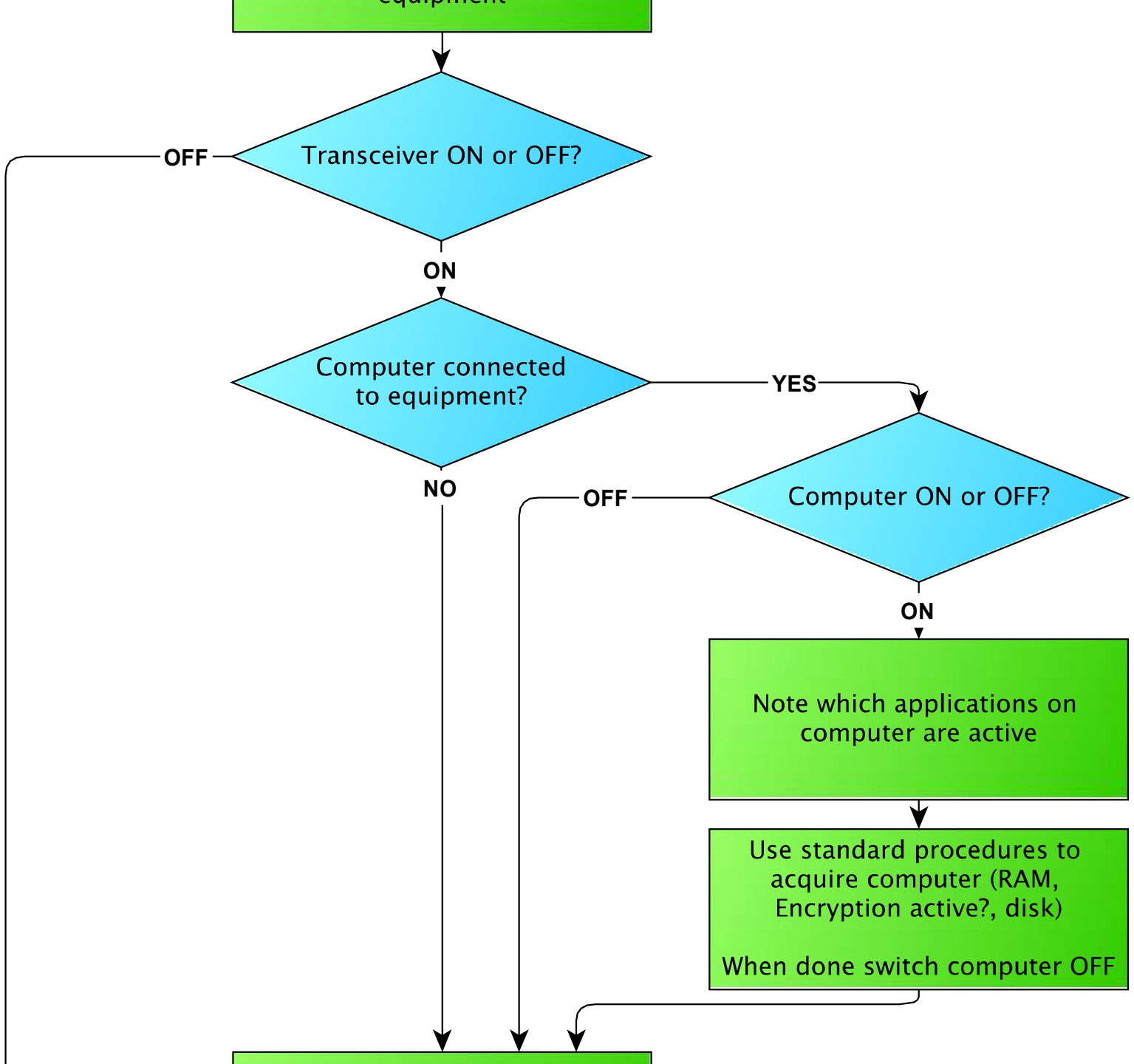


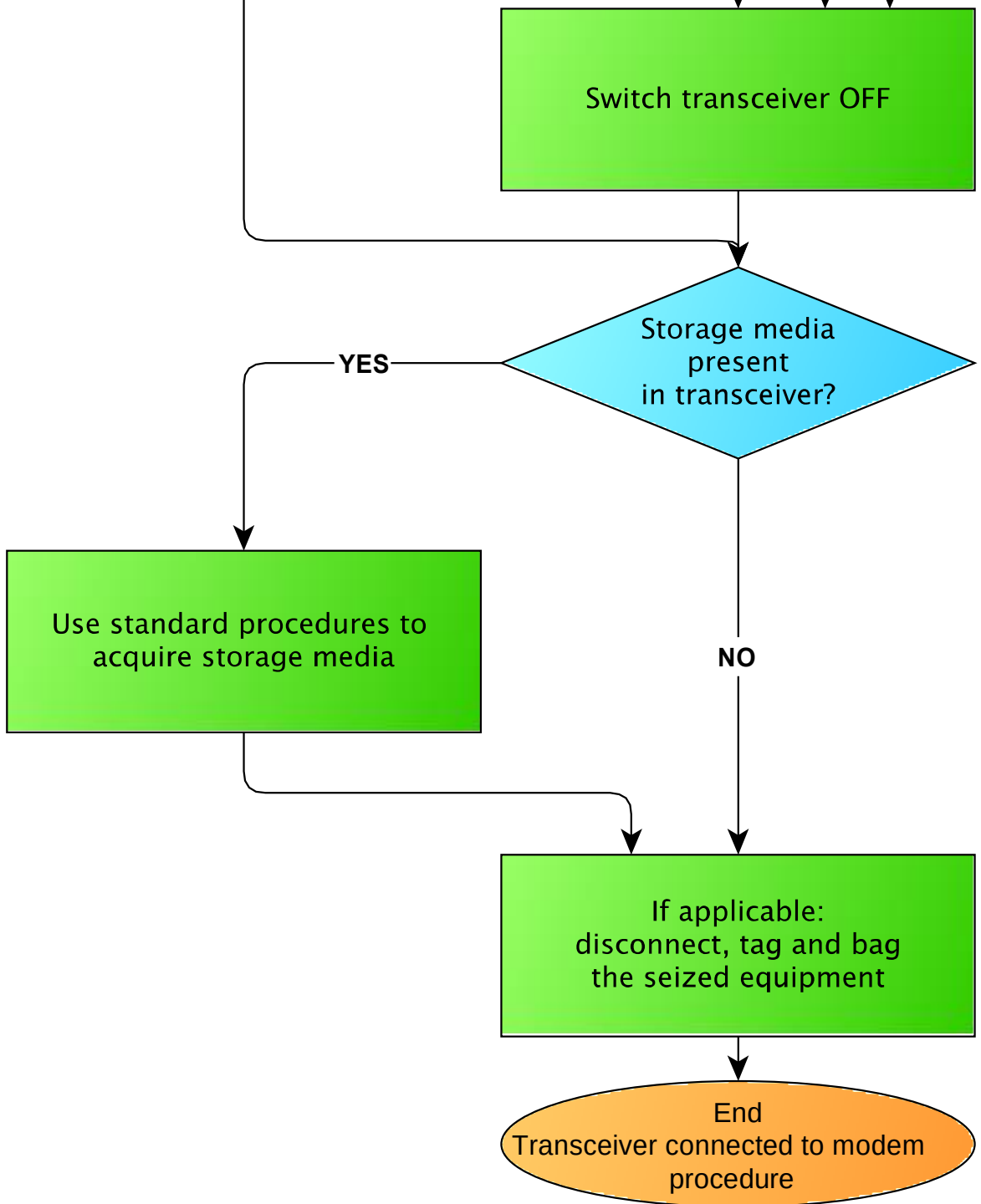
WinLink Topology



Investigative Workflow




Transceiver ON or OFF?
OFF
ON
Computer connected to equipment?
YES
NO
Computer ON or OFF?
OFF
ON
Note which applications on computer are active
Use standard procedures to acquire computer (RAM, Encryption active?, disk)
When done switch computer OFF


Switch transceiver OFF
Storage media present in transceiver?
YES
NO
Use standard procedures to acquire storage media
If applicable: disconnect, tag and bag the seized equipment
End
Transceiver connected to modem procedure

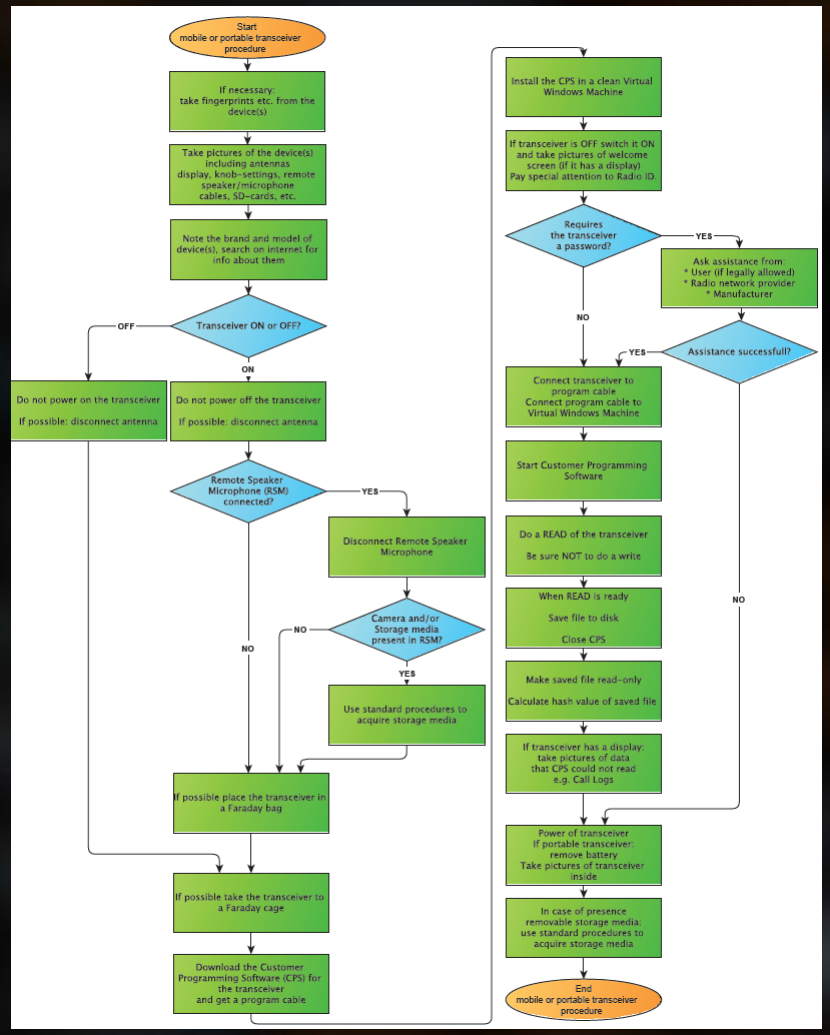
Recoverable Evidence

- No history on radio device
- Traditional Windows machine forensics was conducted
- Device IDs recoverable for connected equipment
- RMS Express Application log files
  - Date/Time stamps with connection information to Radio Message Server, Central Message Server and message IDs
  - Sent and received messages recoverable with filenames corresponding to message IDs

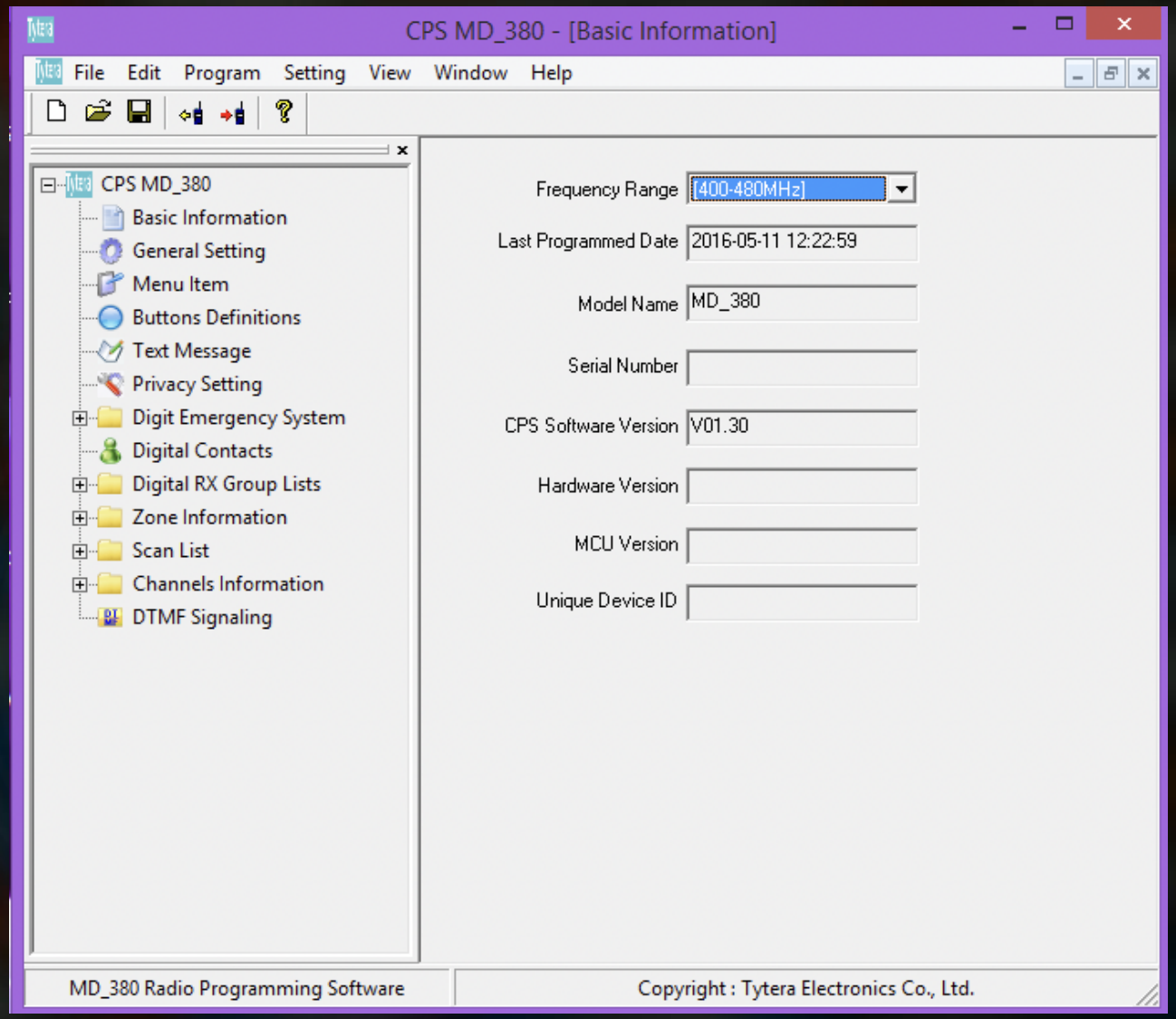
Case Study 2: Hytera PD-785G Portable Two-Way Radio

Device Investigative Workflow

1. Disconnect antenna and any remote peripherals
2. Use faraday cage to eliminate remote wipe
3. Use radio manufacturer configuration software
4. Read the configuration and settings from device
5. Ensure step-by-step photographic evidence of the process is documented
6. Perform Investigation of Storage Media

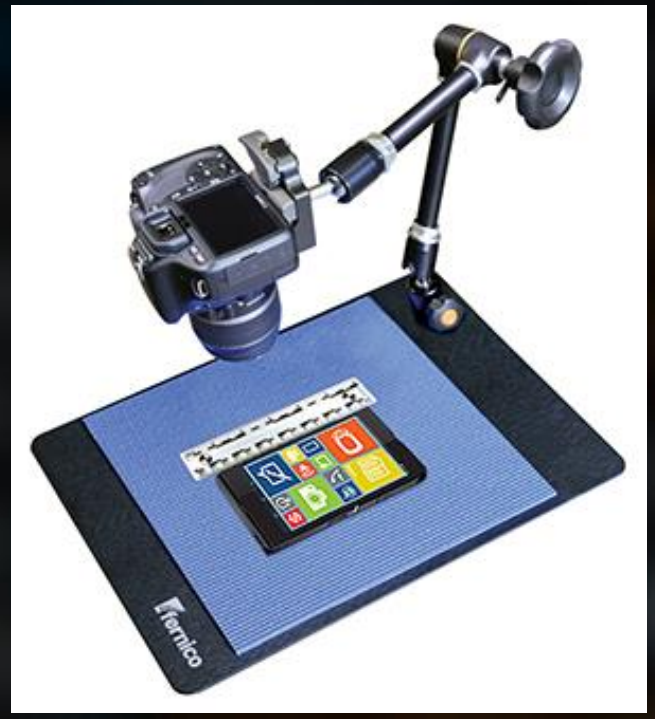


Customer Programming Software (CPS)



Not all data is recoverable using CPS

- Recoverable data:
  - Serial Number
  - Model
  - Frequency Range
  - Radio Alias
  - Radio-ID
- Any non-configuration data is not recoverable, e.g.,
  - Call Logs
  - Short Messages
- Therefore, a manual read was conducted using a Fernico ZRT3



ZRT Example Report

Officer ak

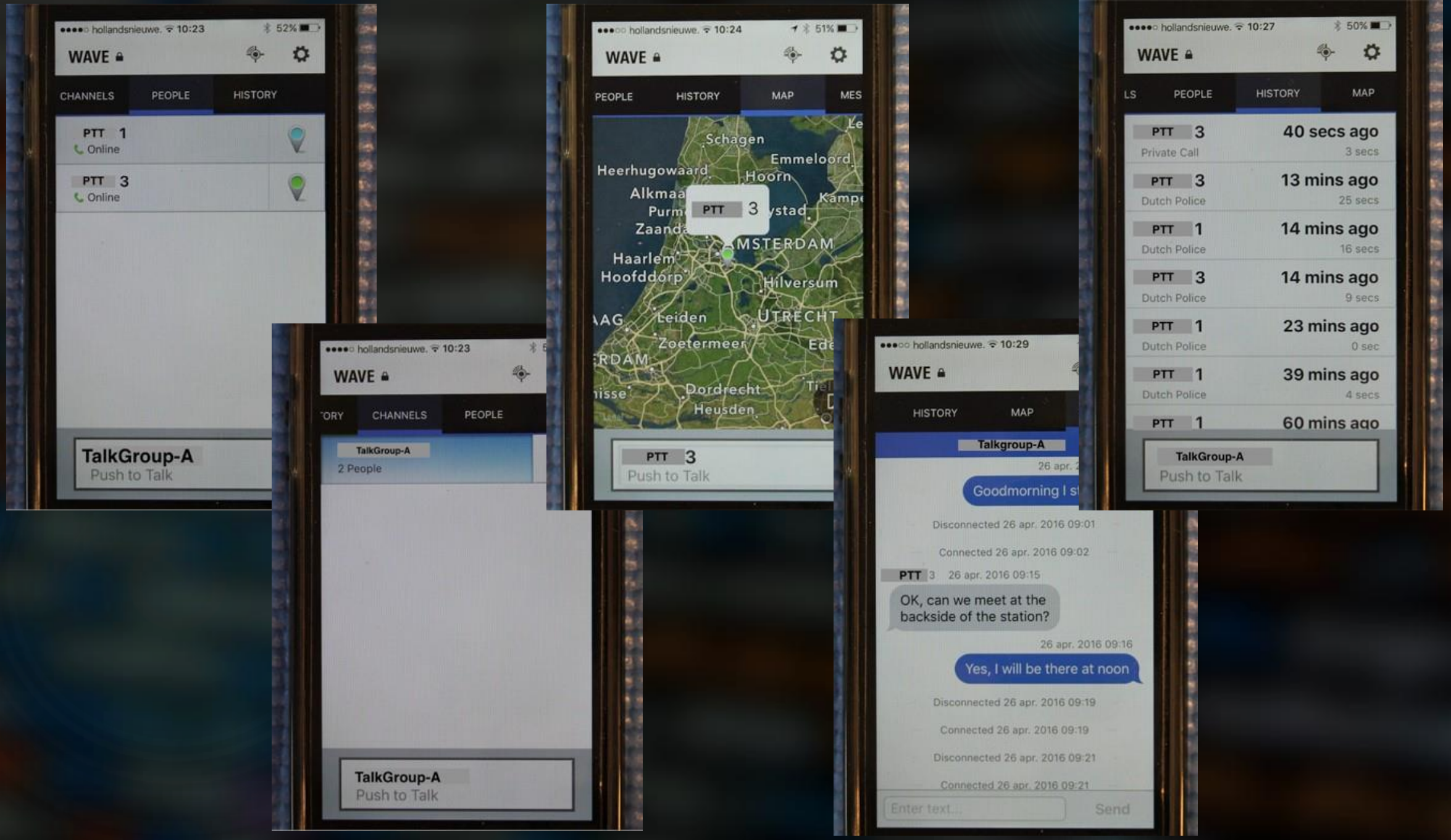
Case Number Hytera_PD785G

Settings 1 - Page 3

MD5	2-5-2016 11:32:29 4A15CB7AC6477A1A697857AA3555843F	SHA1	2-5-2016 11:32:29 26B195D57ACF3F878455CFC956B3785732B9F4B

Description

Case Study 3:
Motorola WAVE
Push-to-Talk Smartphone App


hollandsnieuwe. 10:23 52%
WAVE
CHANNELS PEOPLE HISTORY
PTT 1
Online
PTT 3
Online
TalkGroup-A
Push to Talk
hollandsnieuwe. 10:24 51%
WAVE
PEOPLE HISTORY MAP MES
Schagen
Emmeloord
Heerhugowaard
Hoorn
Alkmaar
PTT 3
Zaandam
AMSTERDAM
Haarlem
Hoofddorp
Hilversum
Leiden
UTRECHT
Zoetermeer
Dordrecht
Heusden
PTT 3
Push to Talk
hollandsnieuwe. 10:27 50%
WAVE
LS PEOPLE HISTORY MAP
PTT 3 40 secs ago
Private Call 3 secs
PTT 3 13 mins ago
Dutch Police 25 secs
PTT 1 14 mins ago
Dutch Police 16 secs
PTT 3 14 mins ago
Dutch Police 9 secs
PTT 1 23 mins ago
Dutch Police 0 sec
PTT 1 39 mins ago
Dutch Police 4 secs
PTT 1 60 mins ago
TalkGroup-A
Push to Talk
hollandsnieuwe. 10:23
WAVE
ORY CHANNELS PEOPLE
TalkGroup-A
2 People
TalkGroup-A
Push to Talk
hollandsnieuwe. 10:29
WAVE
HISTORY MAP
Talkgroup-A
Goodmorning I s
Disconnected 26 apr. 2016 09:01
Connected 26 apr. 2016 09:02
PTT 3 26 apr. 2016 09:15
OK, can we meet at the backside of the station?
26 apr. 2016 09:16
Yes, I will be there at noon
Disconnected 26 apr. 2016 09:19
Connected 26 apr. 2016 09:19
Disconnected 26 apr. 2016 09:21
Connected 26 apr. 2016 09:21
Enter text...
Send

Conclusion

- If you haven't encountered two-way radios yet on a case, it's increasingly likely you will in the near future
- Currently, it's not possible to acquire information from digital radios using standard forensic tools
- As a result, there is little choice available for the investigation besides performing a manual step-by-step acquisition
- Two procedural workflows have been outlined for conducting these investigations

Future Work

- Exploration of two-way radio JTAG and chip-off forensics, akin to mobile phone forensics
- Exploration of software defined radio (SDR) forensics, e.g., HackRF and GNU radio

MARK.SCANLON@UCD.IE

WWW.FORENSICSANDSECURITY.COM

@MRKSCN / @FORSECRESEARCH

UCD Forensics and
Security Research Group