4th IAP NORTH AMERICAN AND CARIBBEAN REGIONAL CONFERENCE
Montego Bay, Jamaica W.I.
2 – 4 November 2016

“Digital Forensic Evidence - The New Frontier”

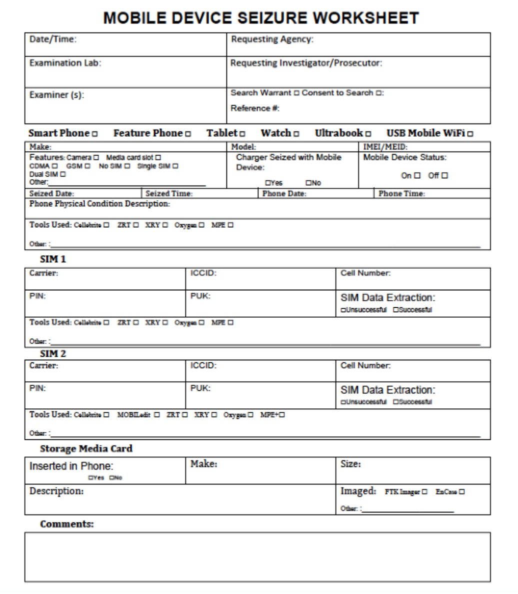
Steve Williams
Investigator/Analyst Expert Consultant
International Narcotics & Law Enforcement (INL) – US Antiterrorism Assistance (ATA) - Broward County Sheriff’s Office – Fort Lauderdale Police Department

Mobile Forensics Process

- Using proper seizure and processing techniques are critical to what can and cannot be recovered from a mobile device and avoiding digital data contamination.
- The Seizure & Collection Process:
  - Identification/Handling
  - Collection/Preservation
  - Acquisition/Image

Identification/Handling

- Identification:
  - Safety first – visually check the smartphone for external connections and physical evidence.
  - Ensure properly documentation or photograph has been obtained prior to moving the smartphone
  - Check battery life



MOBILE DEVICE SEIZURE WORKSHEET

Date/Time:	Requesting Agency:
Examination Lab:	Requesting Investigator/Prosecutor:
Examiner (s):	Search Warrant □ Consent to Search □: Reference #:

Smart Phone □ Feature Phone □ Tablet □ Watch □ Ultrabook □ USB Mobile WiFi □

Make:		Model:	IMEI/MEID:
Features: Camera □ Media card slot □ CDMA □ GSM □ No SIM □ Single SIM □ Dual SIM □ Other:____________________		Charger Seized with Mobile Device: □Yes □No	Mobile Device Status: On □ Off □
Seized Date:	Seized Time:	Phone Date:	Phone Time:

Phone Physical Condition Description:

Tools Used: Cellebrite □ ZRT □ XRY □ Oxygen □ MPE □

Other: :____

SIM 1

Carrier:	ICCID:	Cell Number:
PIN:	PUK:	SIM Data Extraction: □Unsuccessful □Successful

Tools Used: Cellebrite □ ZRT □ XRY □ Oxygen □ MPE □

Other: :____

SIM 2

Carrier:	ICCID:	Cell Number:
PIN:	PUK:	SIM Data Extraction: □Unsuccessful □Successful

Tools Used: Cellebrite □ MOBILedit □ ZRT □ XRY □ Oxygen □ MPE+□

Other: :____

Storage Media Card

Inserted in Phone: □Yes □No	Make:	Size:
Description:		Imaged: FTK Imager □ EnCase □ Other: :________________

Comments:

Collection/Preservation

- Preservation:
  - To avoid pressing buttons, handle the phone by the corners
  - Avoid unnecessary usage of the smartphone
    - Do not:
      - ➢ Make or receive calls
      - ➢ Check the call logs
      - ➢ Check messaging
      - ➢ Using 3rd-party Apps
      - ➢ Attempt to unlock/lock
      - ➢ Power the phone on or off

Collection/Preservation

- Preservation:
  - Check Bluetooth connections and history for external evidence:
    - Smart watch (places the phone to the suspect)
    - Connection with vehicle and/or GPS device
  - Place the phone in “airplane mode” to isolate the device from the network.
  - If the device is locked?
    - Use faraday packaging or heavy duty aluminum foil.

Acquisition/Extract

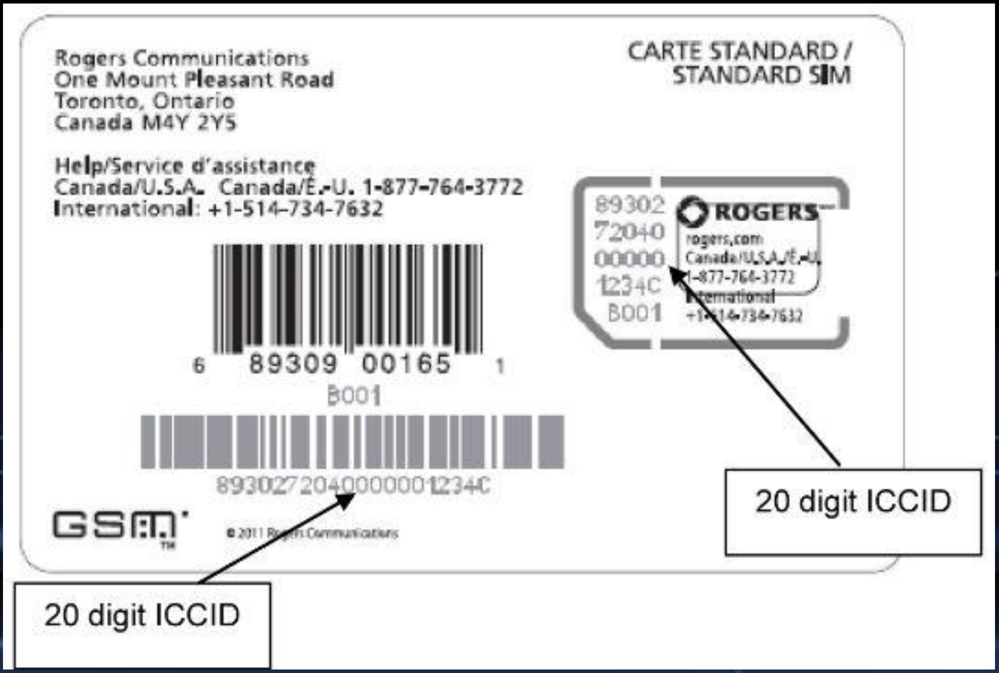
- Acquisition/Extract:
- Used validated forensics software to acquire/extract evidence:
  - Oxygen Forensic Detective
  - Cellebrite Mobile Forensics
  - MSAB XRY
  - MobilEdit

Acquisition/Extract

- Evidence from the mobile:
  - Evidence:
    - SMS
    - Call History
    - Phonebook
    - Email
    - Multimedia
    - Documents
    - GPS Data
    - 3rd-party Communication apps (Skype, Whatsapp, Instagram, Snapchat)
    - Social Media Apps (Facebook, Google+, Twitter)

Acquisition/Extract

- Evidence from the SIM Card:
  - ICCID – Integrated Circuit Card ID, which is the SIM card serial number and can be traced to the purchaser of the SIM card.
  - LAI – Local Area Identity, which is the last cell tower the SIM card connected to.



Rogers Communications
One Mount Pleasant Road
Toronto, Ontario
Canada M4Y 2Y5

CARTE STANDARD /
STANDARD SIM

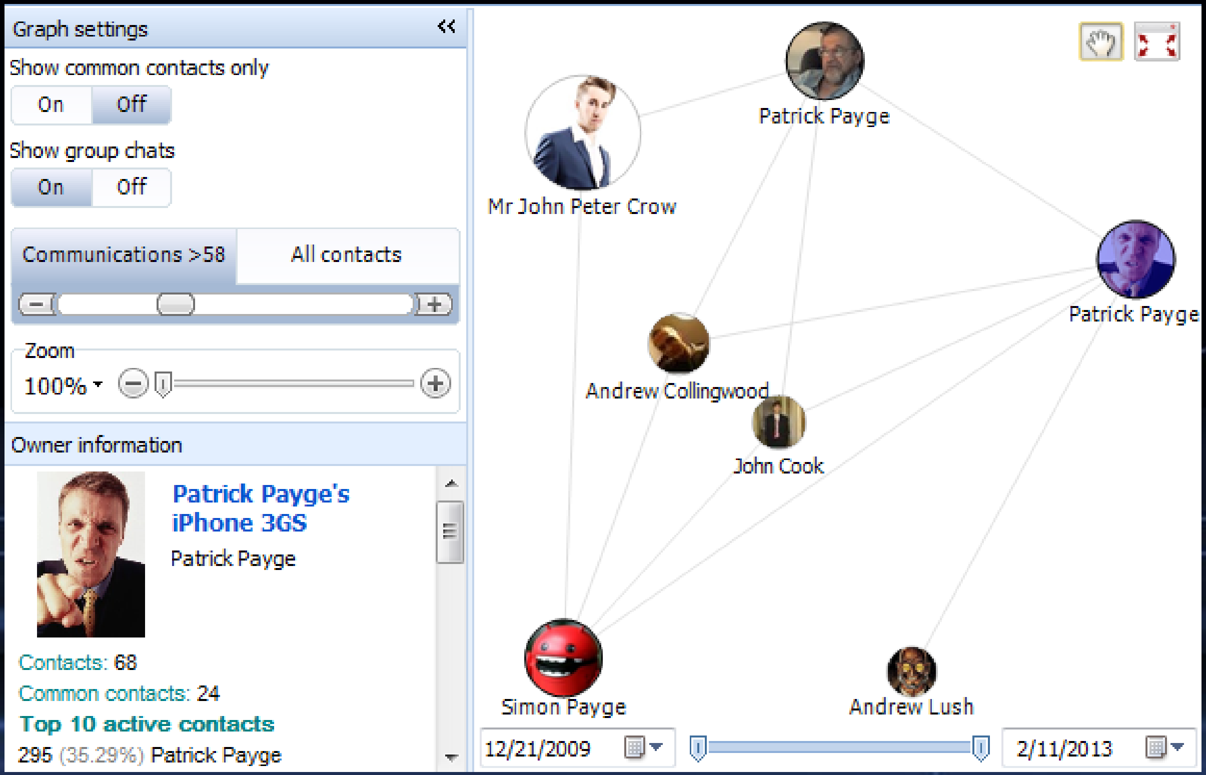
Help/Service d'assistance
Canada/U.S.A. Canada/É.-U. 1-877-764-3772
International: +1-514-734-7632

Acquisition/Extract

- Evidence from the microSD card:
  - Pictures (transferred to the phone) and Photos (taken by the phone)
  - Audio and video files
  - Documents
  - The mobile device database, which is transferred to the phone
  - Mobile device application databases

Acquisition/Extract

- Connecting the Suspects:
  - Once mobile evidence, 3rd-party communication apps and social networking applications extracted, suspects communications are analyzed and linked.



Graph settings

Show common contacts only: On | Off

Show group chats: On | Off

Communications >58 | All contacts

Zoom: 100%

Owner information

Patrick Payge's iPhone 3GS
Patrick Payge

Contacts: 68
Common contacts: 24
Top 10 active contacts
295 (35.29%) Patrick Payge

12/21/2009 – 2/11/2013

Questions

Pictures
Video
Audio
Mobile
Pictures
Audio
Pictures
Mobile Calls
Text Messages
Video
Mobile Calls
Audio
Text Messages
Video
Mobile Calls
Audio
Video
Text Messages