



# CYBER EVIDENCE



Cell Phone Analysis



Trooper Joel Gagne

Middlesex State Police Detective Unit

# Cell Phones Today



# Digital Evidence

**FINGER PRINTS WASH OFF  
DIGITAL PRINTS DON'T**



# Cell Phone Analysis

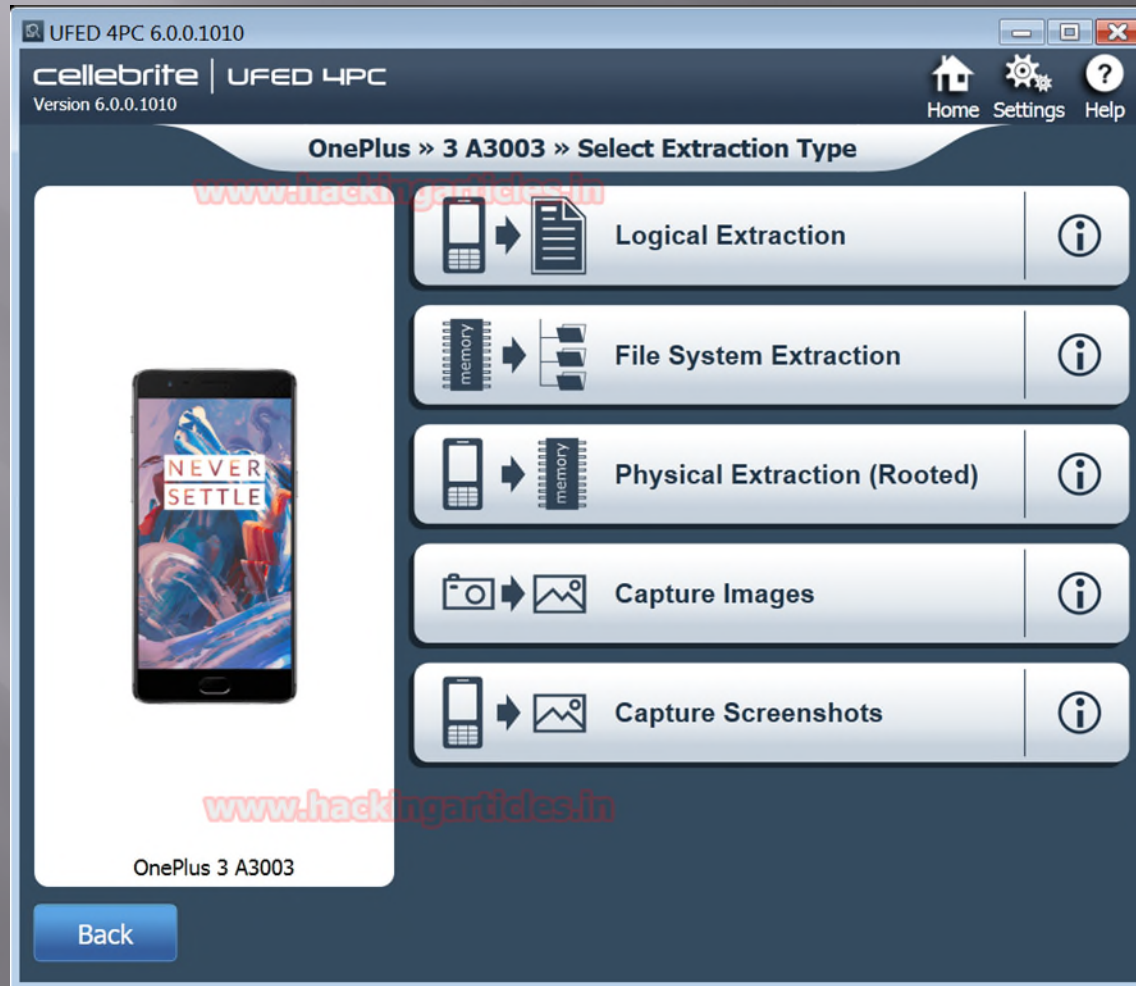
- Often referred to as a “cell phone dump”
- Comprehensive collection of data stored on the mobile device as well as sim card and sd card
- Several companies offer software for this process including Cellebrite, Oxygen and Mobile Forensics Central
- Data is then converted by the examiner into a report format

# Extraction Process



Cellebrite UFED  
(Universal Forensic Extraction Device)

# Extraction Types





















# Analysis Report

- Report can be generated in a variety of formats including PDF, HTML and EXCEL
- If you are receiving a report, it will be a comprehensive report, however, specific reports can be generated from the analysis by the examiner
  - Content between specific contacts
  - Limited to a certain time frame

# Report Information

## Contents

Type	Included in report	Total
 Calendar	164 (5 Deleted)	164 (5 Deleted)
 Call Log	127 (3 Deleted)	127 (3 Deleted)
 Chats	64 (1 Deleted)	64 (1 Deleted)
 Contacts	111 (1 Deleted)	111 (1 Deleted)
 Cookies	1061 (21 Deleted)	1061 (21 Deleted)
 Installed Applications	66	66
 Locations	1336	1336
 MMS Messages	455 (1 Deleted)	455 (1 Deleted)
 Notes	19 (7 Deleted)	19 (7 Deleted)
 SMS Messages	8425 (2 Deleted)	8425 (2 Deleted)
 Timeline	32931 (9 Deleted)	32931 (9 Deleted)
 User Accounts	1	1
 Voicemail	81	81
 Web Bookmarks	9	9
 Wireless Networks	20	20
 Data Files	4311	4311
• Audio	82	82
• Configurations	469	469
• Databases	90	90
• Images	3632	3632
• Text	10	10
• Videos	28	28
 Activity Analytics	222	222
 Analytics Phones	164	164

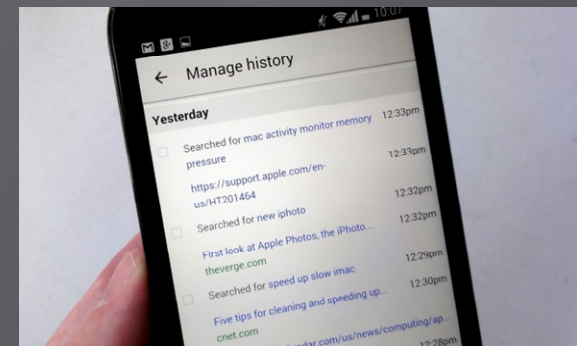


# Obvious vs the not so obvious

- Obvious
  - SMS
  - MMS
  - Calls
  - Chats
  - Contacts



- Things to consider
  - Search history
  - Location
  - Audio Files



# Examine your phones and READ YOUR REPORTS!

- Examiner may not be part of your case and is not searching the report for your information
- After the analysis is performed, take the opportunity to examine the mobile device
- Temporary files may fall into a different location than expected
  - Audio
  - Video

# Anticipate Limitations

- Constant development of new phones



- Daily Addition of new applications
  - Causing connection problems with software

# Adapting with technology

- Use of alternative messaging apps
  - Facebook messenger
  - Snapchat
  - Kik
  - Whatsap
- Taking the victims phone



# Passwords

