

Mobile Phone Seizure and Examination Guide

SEIZURE

- Identify the item. Is it actually a telephone? Is it a dummy phone?
- Note if it is switched on or off.
- Note what is displayed on the screen - pay particular attention to icons displayed as Envelopes, or messages informing of new unread text messages.
- Protect the phone with RF-Isolation
- Do not dismantle the phone - Do not take the back off the phone, or remove the SIM card as this can cause important data to be lost from the phone. time/date etc.
- ASK the owner, or appropriate person for any passwords or PIN numbers that may lock out the examiner during the examination of the phone or SIM - This can save lots of time should these PIN numbers or password be required, as the Service Provider will not have to be contacted.
- Check for handset boxes, SIM card holders, phone bills, etc. - These can hold very important information, such as PIN numbers, PUK numbers, account details, account holder details, telephone numbers, etc.
- Search for Phone chargers - These are as important as the handset itself, certainly from an examiner's point of view. Telephones ideally should be fully charged during an examination, and what better charger than the phone's own charger?
- Place the telephone in a sealed evidence bag, and preferably in a box where the buttons cannot be pressed on the phone once sealed. – this prevents “helpful” interaction with the phone and in any case prevents the telephone being turned on accidentally.
- Are there any other forensic Issues such as protecting the phone for DNA / Fingerprints? If so the phone will need to be submitted to the appropriate unit prior to a mobile forensic examination.

PREPARATION FOR EXAMINATION

- Photograph evidence inside the seizure enclosure.
- Document seizure labels.
- Open seizure enclosure.
- Photograph and details any marks or peculiarities of note
 - Caveat if the evidence is on and within a RF-Isolation enclosure you may not want to perform this step until an acquisition has taken place unless it is absolutely necessary to determine the make and model of phone
- Determine specifications of phone and what software is appropriate to download information from handset.

EXAMINATION

- Connect phone with appropriate cables or method, I.e. Infra-red or Bluetooth
- Acquire with software
 - Bookmark items of note
- If the phone is a GSM phone note IMEI number on screen (by typing *#06#) and employ other manufacturer-specific handset codes to obtain handset information.
- Remove handset from RF-Isolation and turn power cycle the unit. Photograph any startup screens or messages
- Note time and date on handset.
- Power off handset, and remove casing
- Photograph battery, and label behind it once battery removed (usually shows IMEI)
- If the phone is a Nextel or GSM remove SIM and photograph both sides.
- Acquire SIM with software
 - Bookmark items of note
- Perform of memory cards if present.
- Reassemble handset.
- Reseal and return evidence to property locker
- Create reports and burn onto CD/DVD