

cellebrite

delivering mobile expertise

UFED series

UFED Touch/4PC Nokia Lumia Windows Phone Extractions

March 2015

<https://t.me/learningnets>

Introduction

This document describes the Nokia Lumia Windows Phone 8.0 password bypassing physical extraction solution.

Supported devices

Most Nokia Lumia devices that were initially released with Windows Phone 8.0 (as opposed to Windows Phone 8.1).

Workflow

This solution depends on the charge level of the battery, therefore most of the workflow is related to charging and discharging the battery.

- ◆ The device needs to be connected to UFED (UFED Touch or UFED 4PC), and it must be **powered off**. UFED will detect whether the extraction is possible with the current charge level of the battery (for most devices, between 12 – 20%, but for some devices it may be up to 95%).
- ◆ If the battery is over the required charge level, you will be asked to drain the battery by leaving the device powered on. This can take several hours. Ideally the battery should be discharged until it reaches about 10%.
- ◆ Connect the device to UFED again. UFED will start charging the device until it reaches the correct charge level. The device will reset several times during this process.
- ◆ Hold the device's Volume Up button for a few seconds, after which the extraction will begin, with no further interaction is required.

Additional information

During the extraction process, a small file is written and then deleted from one of the system partitions on the device. This has no effect on the user data, and does not change the information saved on the device.

Troubleshooting

During the initialization of the extraction process (and as described under "Additional information"), a small file will be written to the device. In the very unlikely event in which this file is corrupted (or if the device behaves differently than expected), the device may enter a "bootloop", in which it will not charge and will not power on.

Solution: A special removal utility will be supplied. To use this utility, the device must have enough battery power to boot without an external power source. The following two cases are possible:

- A.** The device's battery is strong enough, so that the utility will succeed in removing the problematic file.
- B.** The device's battery is too weak. In this case, physically remove the battery from the device, and charge it with an external charger (~15 minutes). Then connect the device to UFED and retry the removal utility.

Notes:

- i. Case **B** above needs to be avoided if possible, because the battery is not always removable and an external charger may not be available.
 - ii. It is crucial to react to the "bootloop" scenario immediately, because while the device is stuck in this loop, the battery will drain until the device can no longer start without an external power source.
-

Copyright © 2015 Cellebrite Mobile Synchronization Ltd. All rights reserved.

This document is delivered subject to the following conditions and restrictions:

- ◆ This document contains proprietary information belonging to Cellebrite Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED.
- ◆ No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- ◆ The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- ◆ Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are Fictitious unless otherwise noted.