http://www.oxygen-forensic.com
+1 (877) 9-OXYGEN
+1 (877) 969-9436
+44 1296 621121

Oxygen Forensic Suite
Android rooting add-on principles

Due to the UNIX nature of the file system used in Android smartphones, most user files are under protection. One needs to gain root access for /data/data subfolder (at least). This folder contains files created by preinstalled and third-party applications. The OS won't give these access rights easily; thus the process known as "rooting" must be applied to "unlock" the file system.

There are two common types of rooting: temporary and permanent. Making an analogy with Apple devices where rooting is called "jailbreaking", temporary rooting is similar to tethered jailbreak while permanent rooting is similar to untethered one. Indeed, a temporary rooting is gone once a rooted Android device is rebooted. Permanent rooting involves significant changes in the phone's firmware such as replacing several system files.

All we need is extracting files from protected folders. There is no need for a permanent rooting to perform forensic tasks. Oxygen Android exploit is designed to do as little as possible to only provide access to those files, and not to modify the phone's internals. The exploit is copied to /data/local/tmp (which is a standard folder for applications to be placed to before installation). It is not an .apk app, though; it is just a binary application that does not need to be installed. It simply starts and does its job. After it finishes, the application file is erased along with any temporary files that could be created during the rooting process (see below). At this time, the files are accessible but still have insufficient access rights. Oxygen Forensic Suite sets access rights temporarily, reads all the files and sets the rights back to their original state after it’s done. The software leaves the phone rooted, but after a reboot the device returns to its original non-rooted state.

In order to perform the task, one must have access to the phone's file system via adb, meaning that adb daemon must be running in the device. The phone itself must be in 'USB debugging' mode to be able to be connected.

The exploit uses certain vulnerabilities in various versions of the Android OS. Technically, these are bugs that may be fixed in later releases, so there is no guarantee the exploit will work with all current and future models. The vulnerability could be fixed, or the phone can be shipped with modified firmware out of the box. It's a common practice for manufacturers to fix bugs found in older systems in newer releases. We are using several different methods to root the phone, from simple ones for the old versions to very sophisticated for latest releases. These methods are attempting to grant root access rights to adb daemon.

Methods used to root Android phones running OS versions 1.6 through 2.2 are relatively simple, and are using vulnerabilities in memory protection of the adb process. These methods do not write to the file system and do not deal with any other processes, their memory and stored data. Only the adb process is affected, so there is no worry about preserving user data in its original state. Most Android devices with OS 1.6 to 2.2 onboard can be rooted with this method, with very few exceptions of highly customized firmware.

Android smartphones running OS versions higher than 2.1 are better protected, and more sophisticated procedures must be used. Several variations are used to attack firmware versions 2.*, 3.0.* and 4.0.* These cases involve the use of flash card manager. It is highly recommended to replace the original memory card with an empty one as there can be a theoretical chance or losing data stored on the flash memory card. In addition, the flash card can be dismounted after rooting, so there is no need to re-mount it in the device. Several temporary files are created during the process. They are deleted after the rooting procedure is finished.

There is a special case if flash memory is built-in. Investigators will be unable to substitute it with another card. It's up to a forensic expert to decide whether to attempt rooting the device or not. However, unlimited access to all files gives unmatched advantages for forensic examinations of Android smartphones.