



Oxygen Forensic Suite 2012 Android rooting add-on principles



Due to UNIX nature of an Android smartphone file system almost all user files are under its protection. One needs to gain root access at least to /data/data subfolder where files created by preinstalled and 3rd party applications are located. The OS won't give such rights to anybody; thus the process known as "rooting" must be applied to "unlock" the file system.



There are two common types of rooting - temporary and permanent. Comparing Android smartphones with Apple devices where rooting is alike to "jail-breaking", temporary rooting is an analog of tethered jailbreak while permanent rooting is untethered one. Indeed, temporary rooting is gone once we reboot a rooted Android device. Permanent rooting involves significant changes in phone's firmware such as substitution of several system utilities and so on.



As far as we only need to extract all the files from the protected folders there is no need for a permanent rooting to perform forensic tasks. Oxygen Android exploit is designed to do as little as to only provide access to those files and not to modify phone's internals. The exploit is copied to the folder /data/local/tmp (which is common and standard folder for any application to be copied before installation). It is not an .apk app, though; it is a binary application which does not need to be installed. It simply starts and does its job. After it finishes, the application file (along with some temporary files which could have been created during the rooting process - see below) is erased. Now the files are exposed but have insufficient access rights. Oxygen Forensic Suite sets needed rights temporarily, reads all the files and sets the rights back when files are being read. The software leaves the phone rooted but after its reboot the device returns into the original state.





connected.

To perform all the tasks one must have an access to the phone's file system via adb. That means that adb daemon must be running inside the device and the phone must be in 'USB debugging' mode to be able to be



The exploit uses commonly known bugs in various Android OS versions. As far as these are bugs there is no guarantee the exploit will do its task with any Android smartphone as the exploited bug could be fixed in the firmware or the firmware could be initially modified and not have this bug from the very beginning. Bugs in older OS versions are fixed in newer releases; thus we use several different methods to root the phone - from simple ones for old versions to sophisticated for the latest. All these methods have one feature in common - they try to provide adb daemon with root access rights.



The methods for rooting Android phone with OS versions 1.6 - 2.2 are relatively simple and use holes in adb process memory protection. They do not try to write anything to the file system at all and don't deal with any other processes and their memory and data. All actions are done on adb process only so there is no worry about user data preservation. The majority of devices with 1.6 - 2.2 onboard are prone to be rooted with this method. Only highly customized firmwares are durable to it.



Smartphones with OS versions higher than 2.1 are better protected so more sophisticated procedures must to be used. Several variations are used to attack 2.* and 3.0.* firmwares. In such a case a flash card manager is involved. It is highly recommended to replace the original flash card with an empty one. Though one never experienced it, there is some theoretical chance the data on the flash card can be lost. Also, as a result the flash card can be unmounted after the rooting so there is no need to remount it in the device. During the process several temporary files can be created. They are deleted after the rooting procedure is finished.



There is a special case when the flash card is built-in. It's impossible to substitute it while all the warnings from the former paragraph concern this case. It's up to the forensic expert to decide whether to try to root the device or not. But unlimited access to all the files gives unmatched advantages for a forensic examination of an Android smartphone.

