Samsung Galaxy S4 (and probably other Android devices) are being BIG BROTHER using the device camera

Yaniv Miron aka Lament lament [AT] ilhack [DOT] org @lament1337

Responsible Disclosure: I don't want to have a responsible disclosure here and give Samsung the opportunity to reply as they never revealed that they are watching us.

Goal: During a security audit that I've made to Samsung Galaxy S4 I found that the back camera is keeping photos even though I did not clicked on the capture button and/or on the screen and/or intended to keep/capture/save them. This is a major privecy issues as the device camera is acting as a BIG BROTHER keeping images without the owner permission.

This is just one variant out of many other possible variants that could happen as if the device camera is keeping images without the owner permission in this case there is no guarantee that it does not save images on other cases.

Saving images without the owners permission is a major privacy issue.

Attack steps:

All of the steps below are relevant for:

Device: Samsung Galaxy S4

Model: GT-I9500

Android Version: 4.3

Kernel Version: 3.4.x

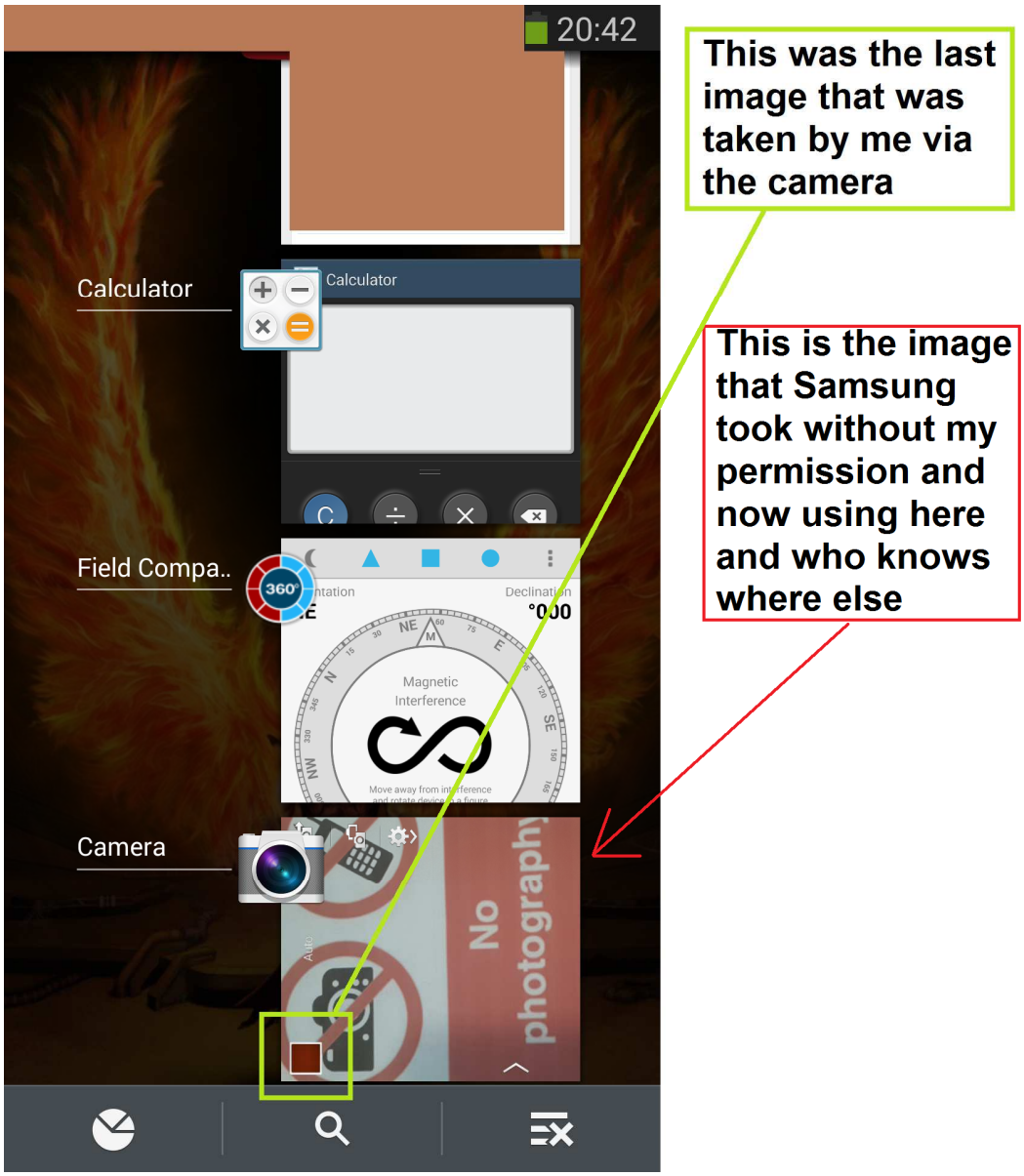
Step 1: Open the Camera built in application.

Step 2: Hold the back camera toward an item you **DO NOT** want to take photo of.

Step 3: Press the main button for 3 seconds (the physical button on the bottom of the phone).

Step 4: You will now enter to the task manager that will show you small images of the last running applications. The image near the Camera application is the image you have directed your back camera towards. As you can see the Samsung device decided to keep the image, just in case.

Step 5: Know that Samsung keeps images that you do not intend to take.



Final notes: BIG BROTHER is watching you over your cellphone and Samsung (and maybe others) are helping him. I did not had the time to research more and see where does Samsung stores the image and grab it from there, that could be an interesting thing to do.

Timeline: xx xxx 2014 - Issue Found.

08 Oct 2014 - Publishing this document after waiting a while.

 # e [0] f #