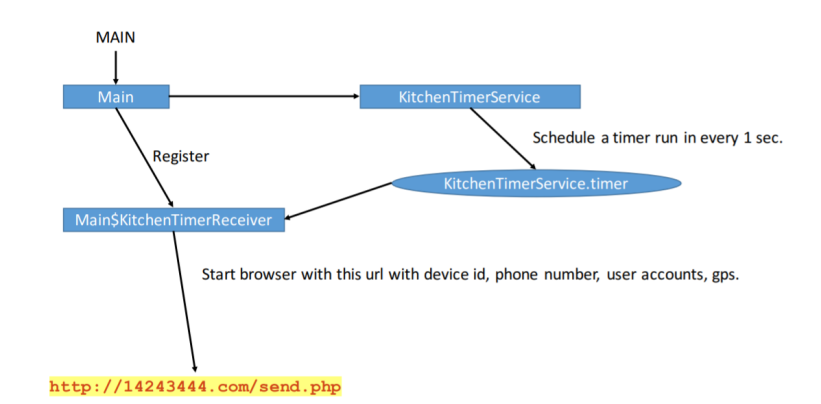
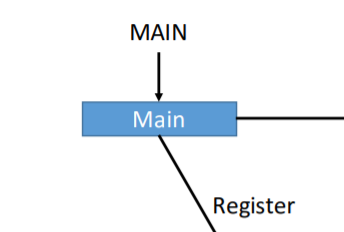
**Recognized Patterns：FakeTimer\_variety1**

**The name of the identified app：Fennec F-Droid**

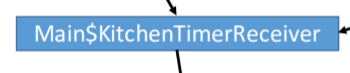
**Corresponding to the name of APP in sample：**



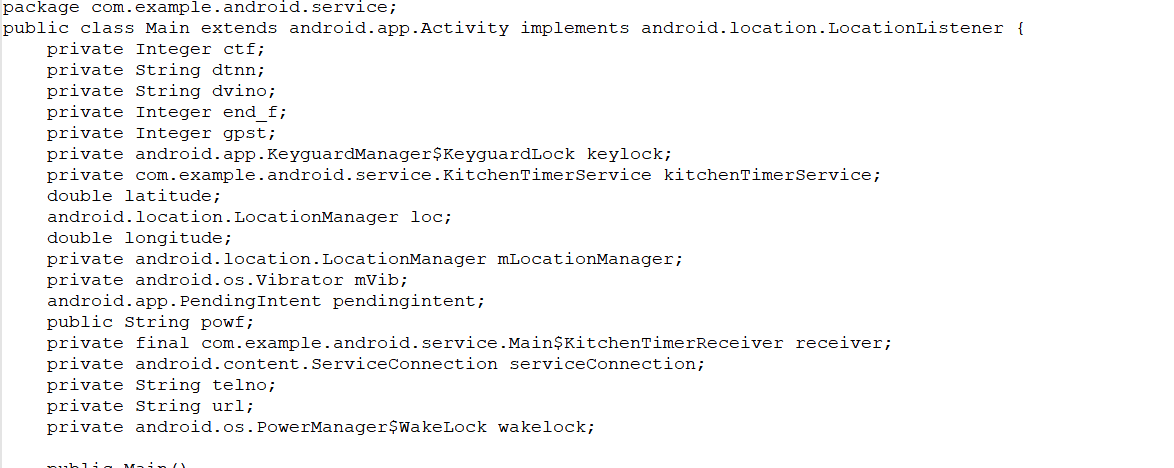
**For function**

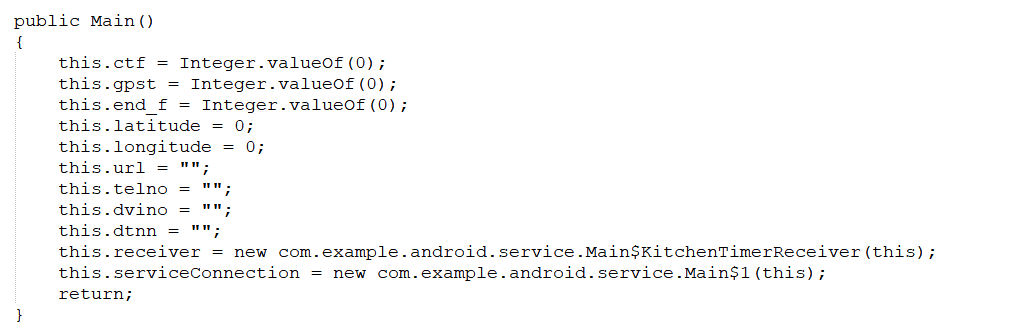


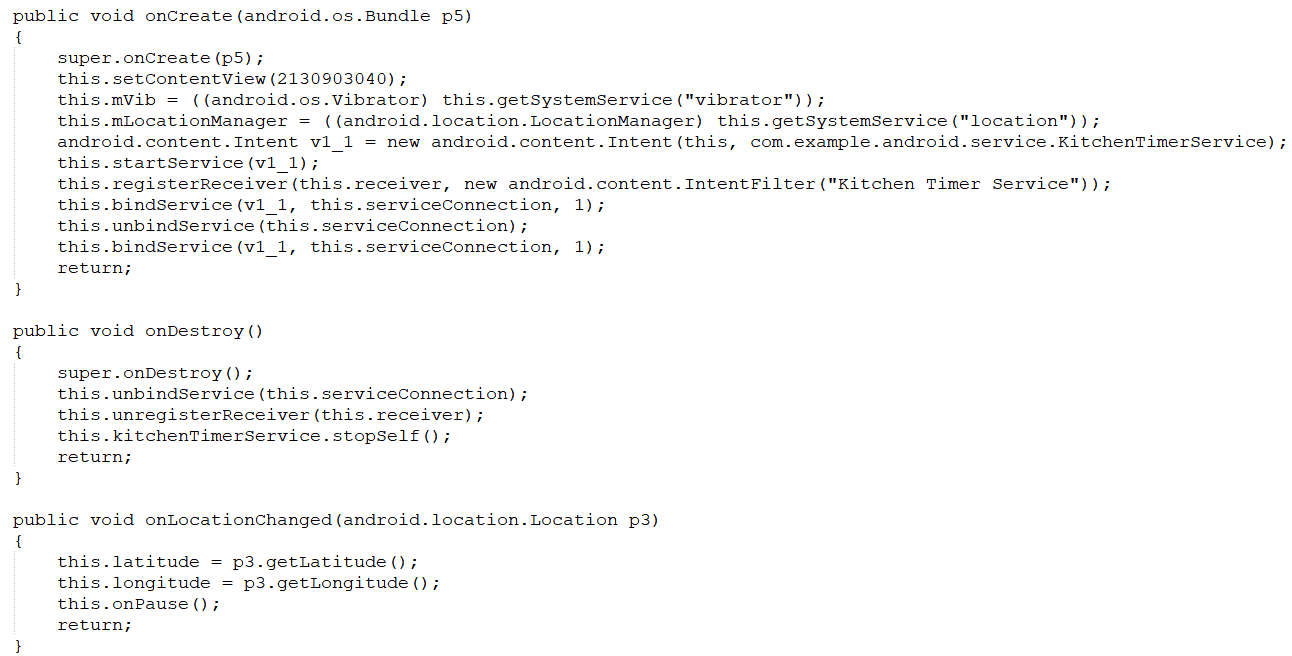
**Mainly used to obtain information about gps, as well as registration**

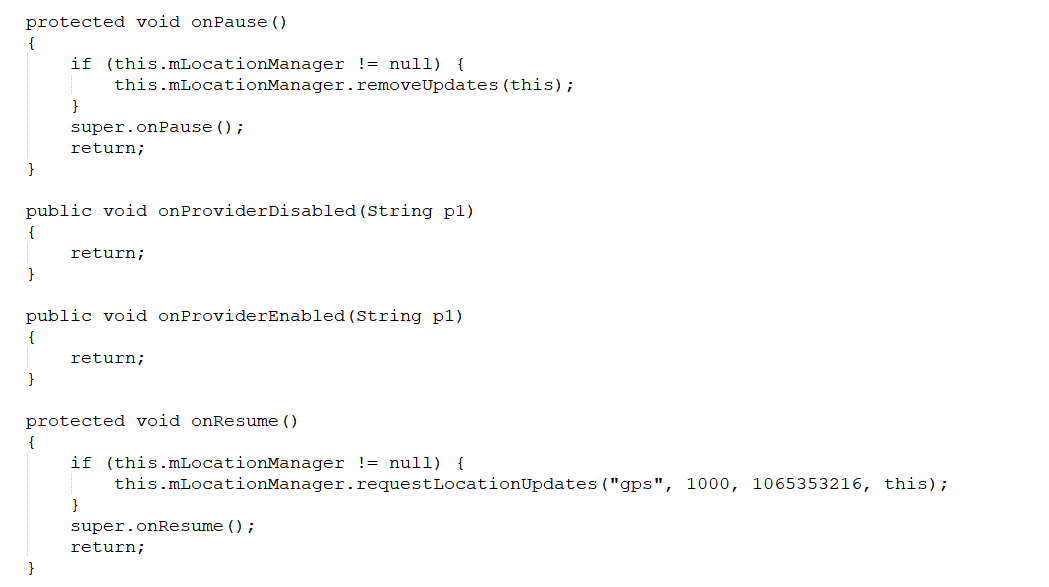


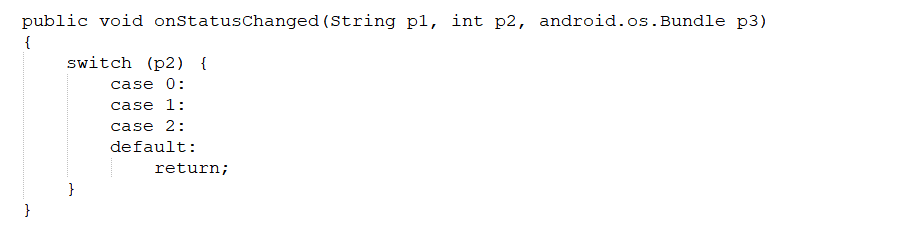
**Corresponding to the key code in sample：**



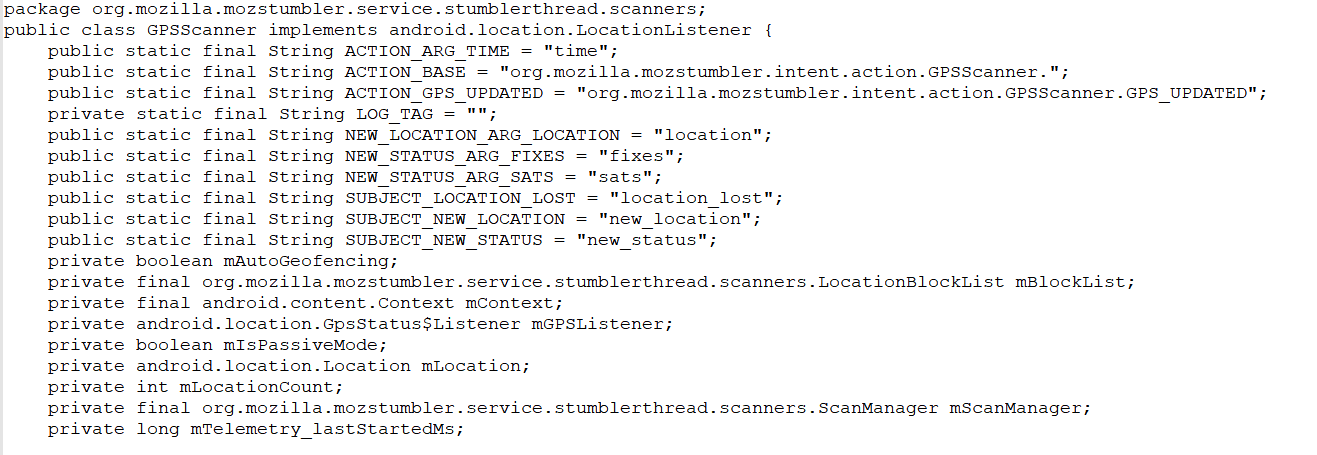


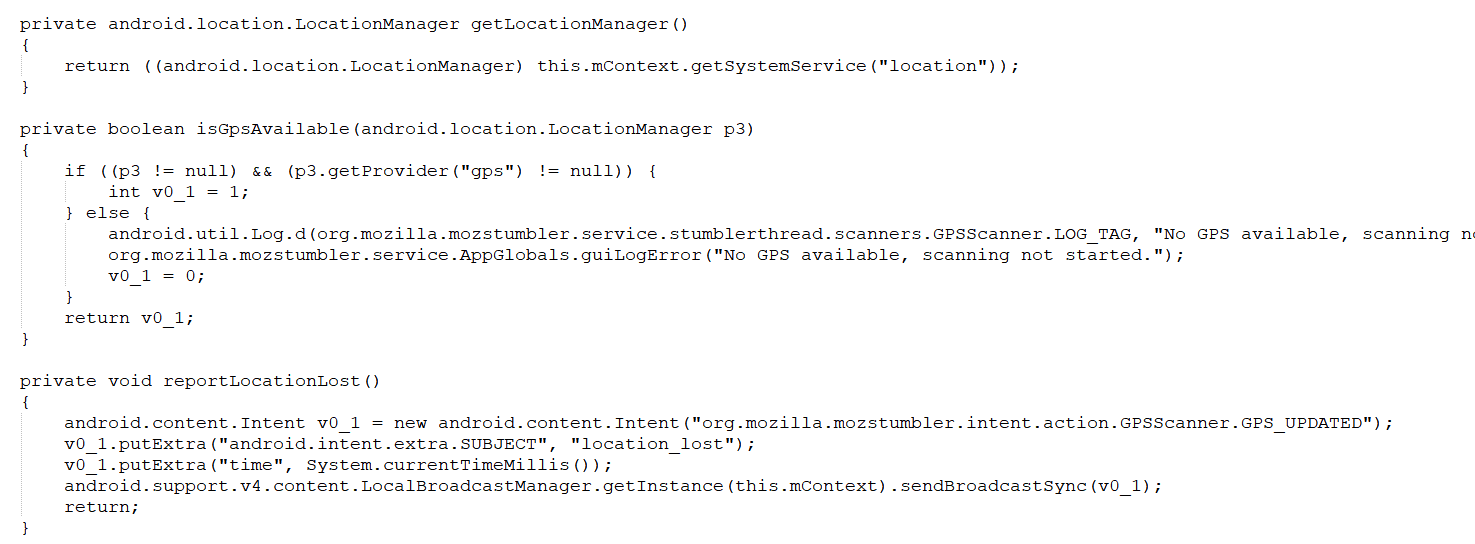


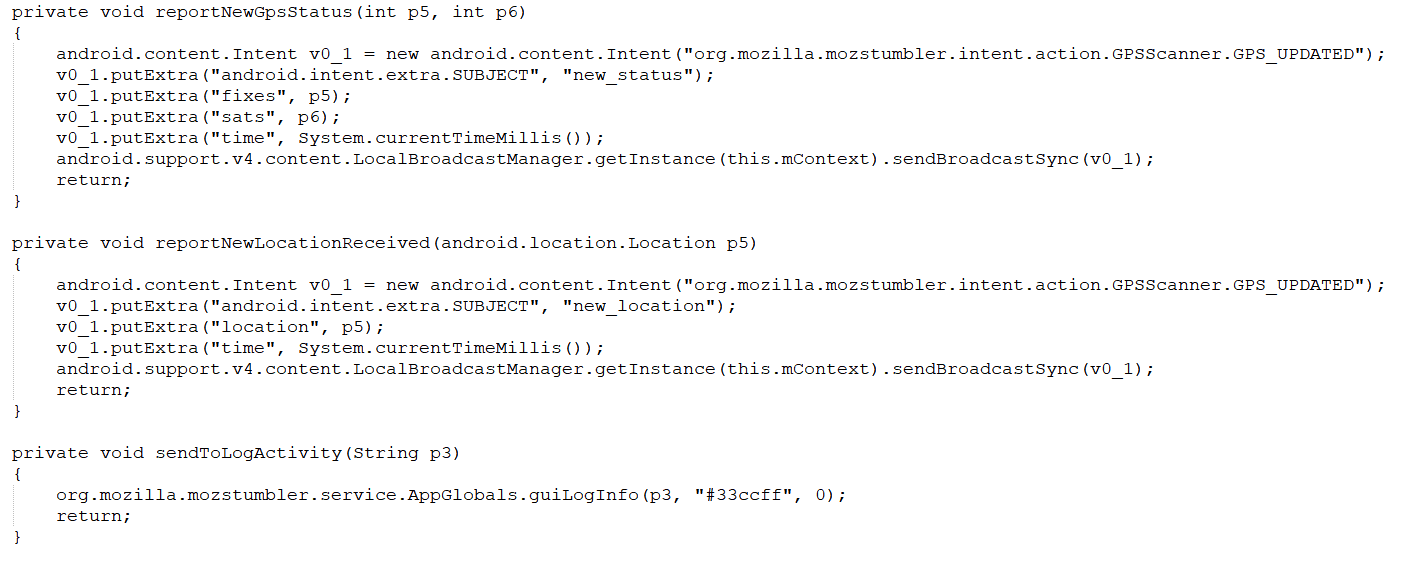


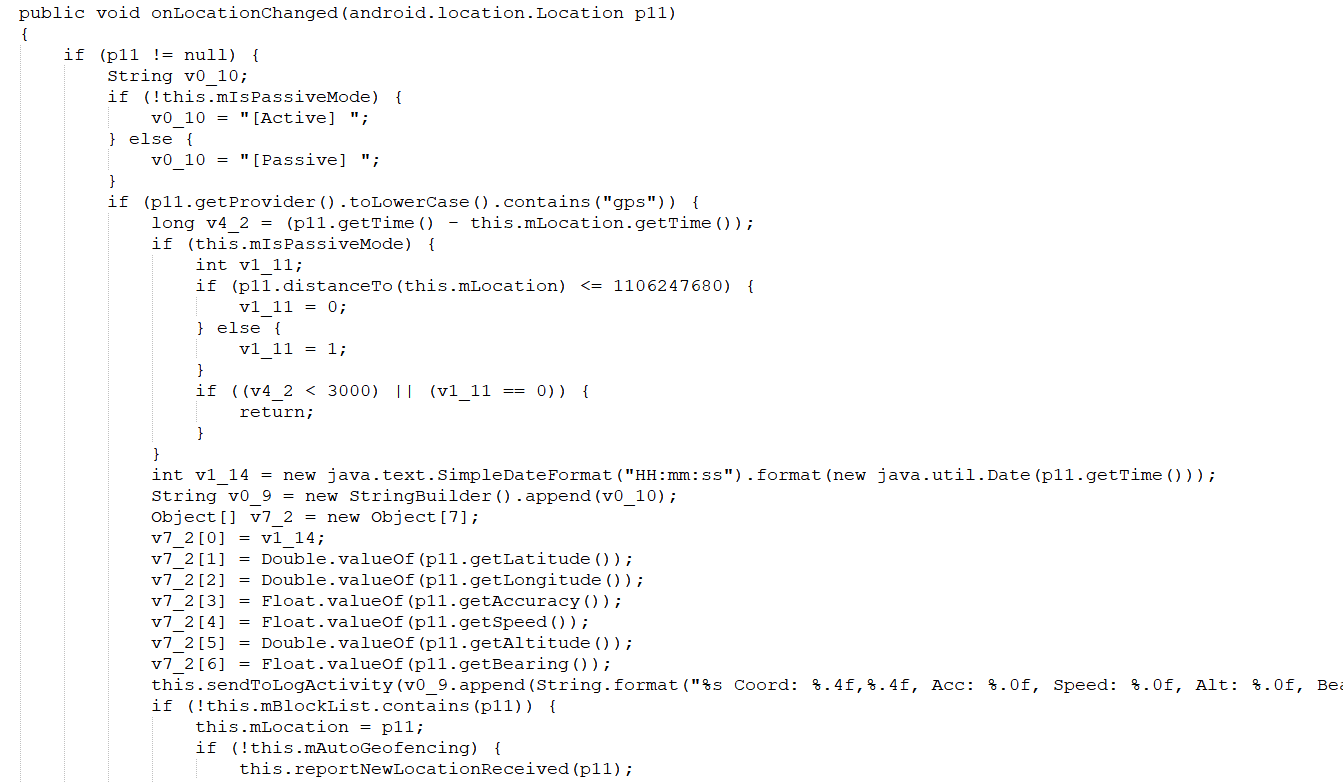


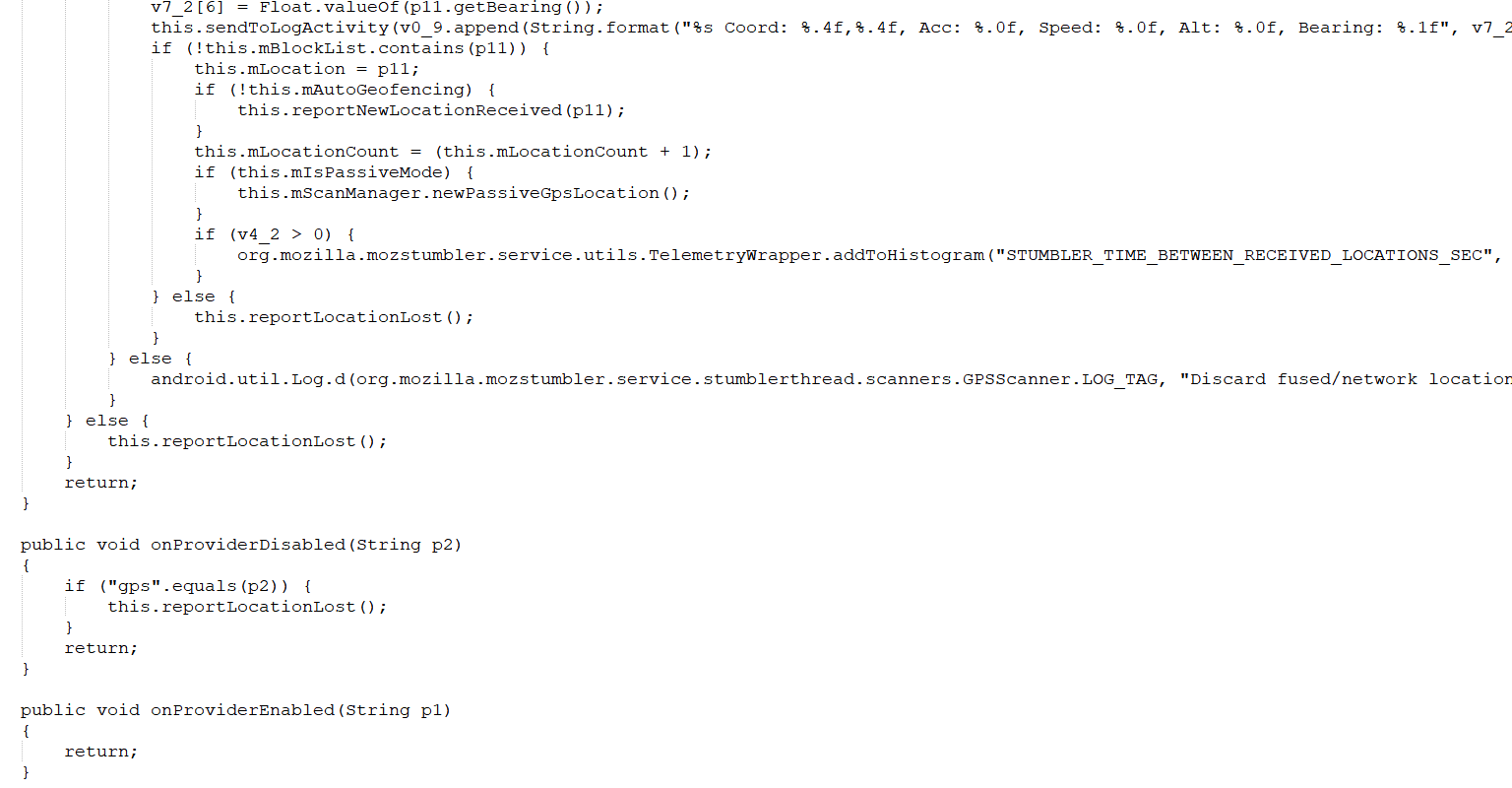
**Corresponding to the key code in this app：**





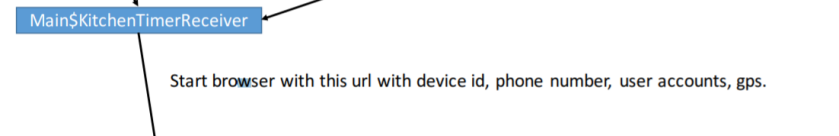


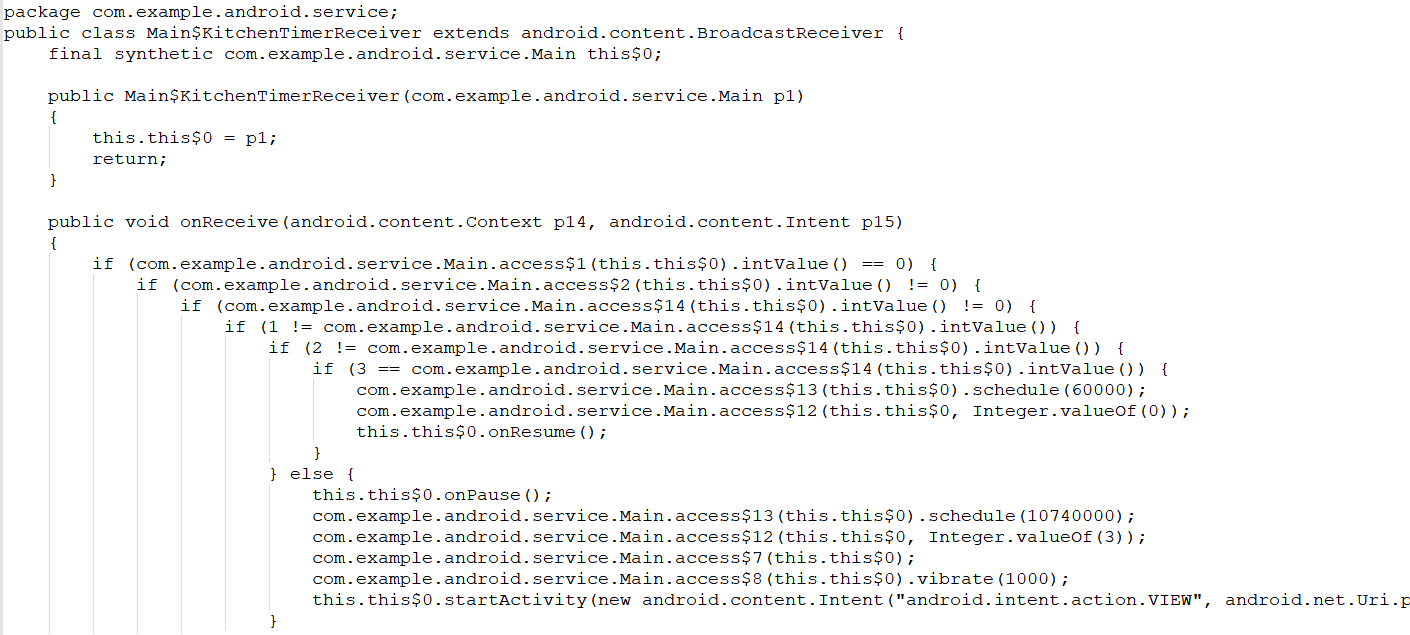


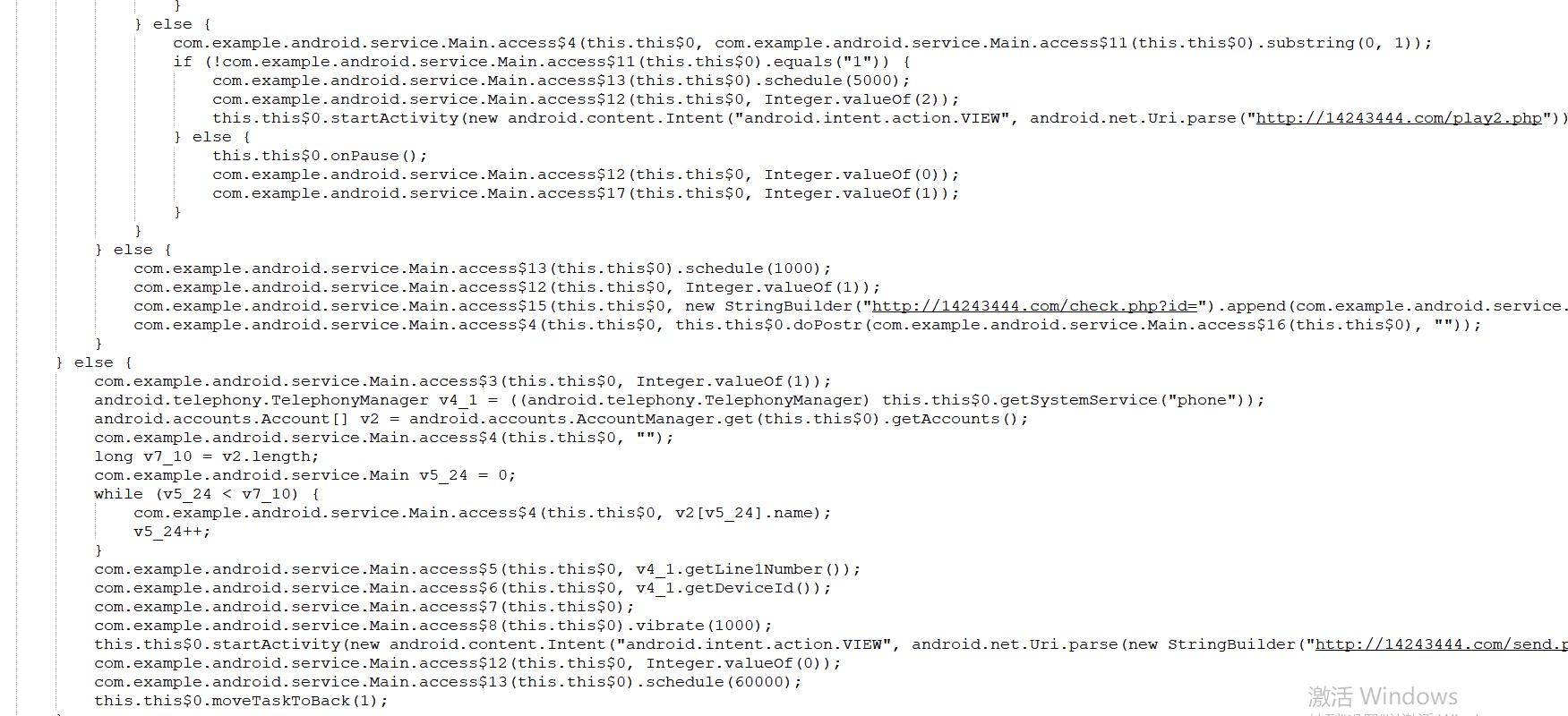




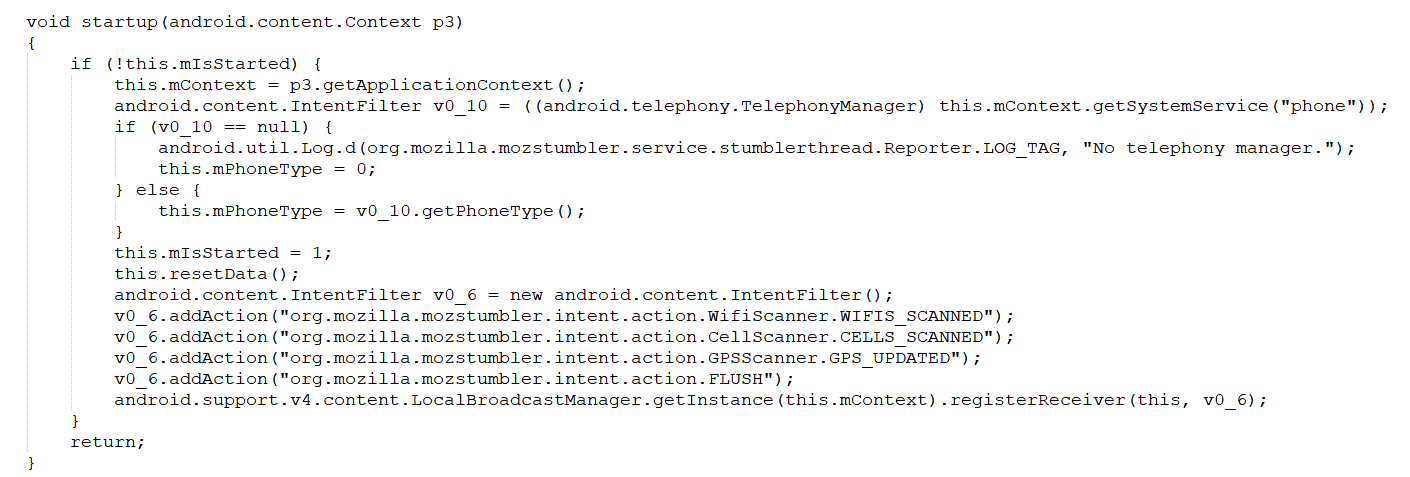
**For functions:：**

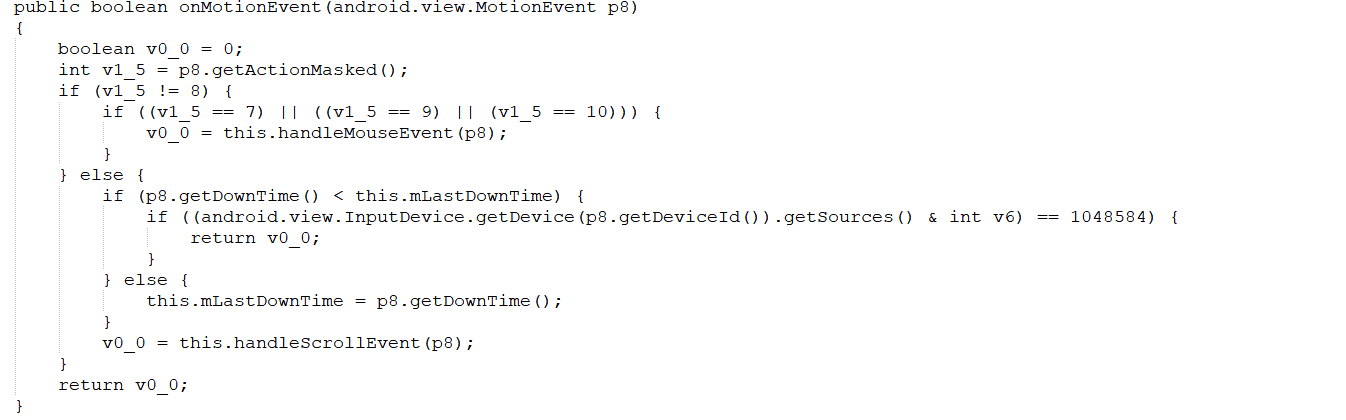




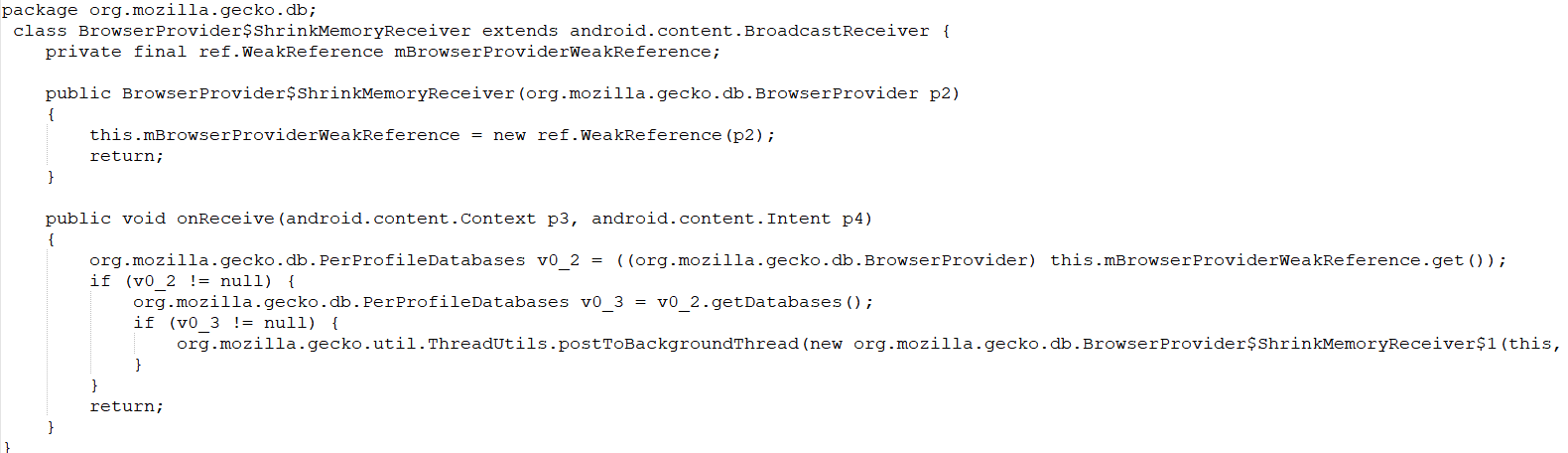


**Corresponds to the key code in this App: (for this part of the function app, only the key token matches, but not the function matches completely)**

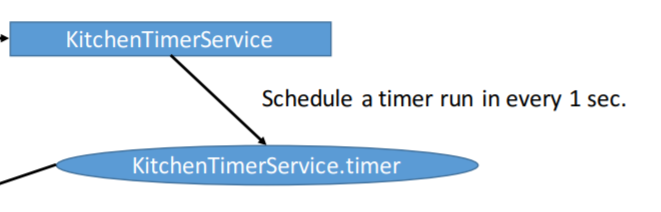




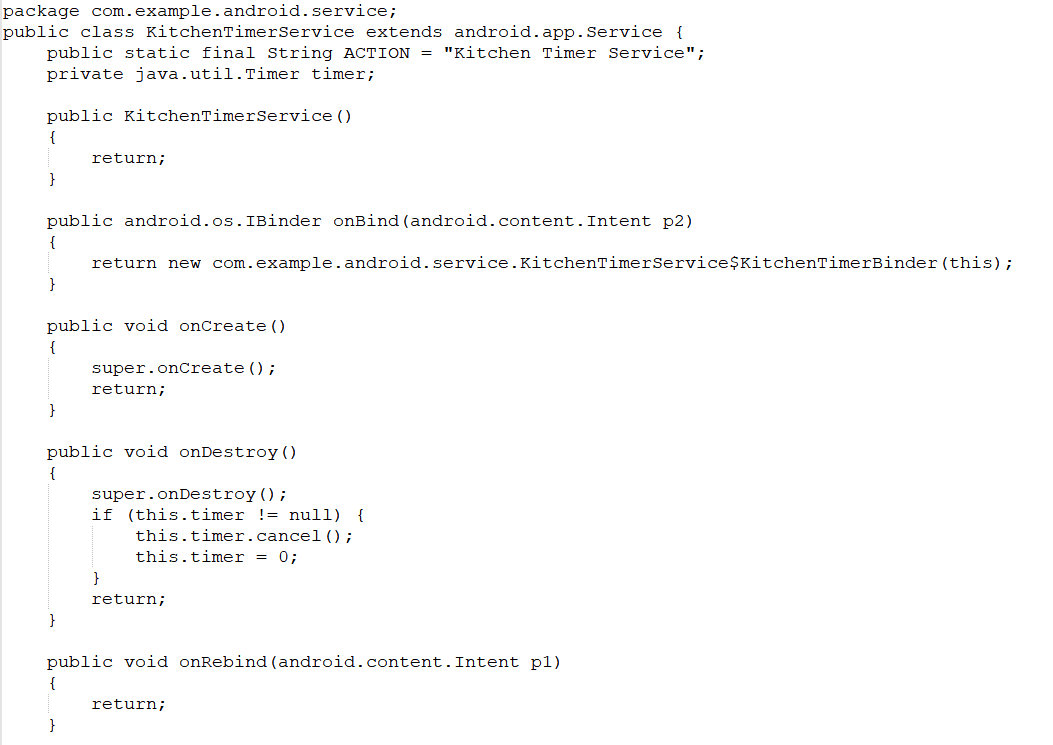


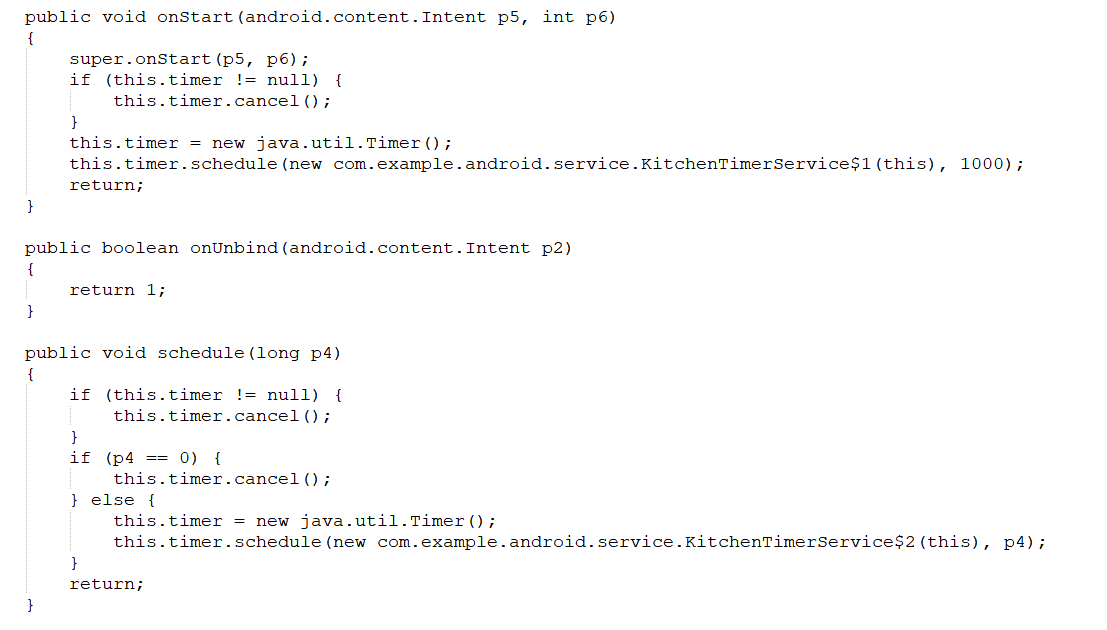


**For functions：**

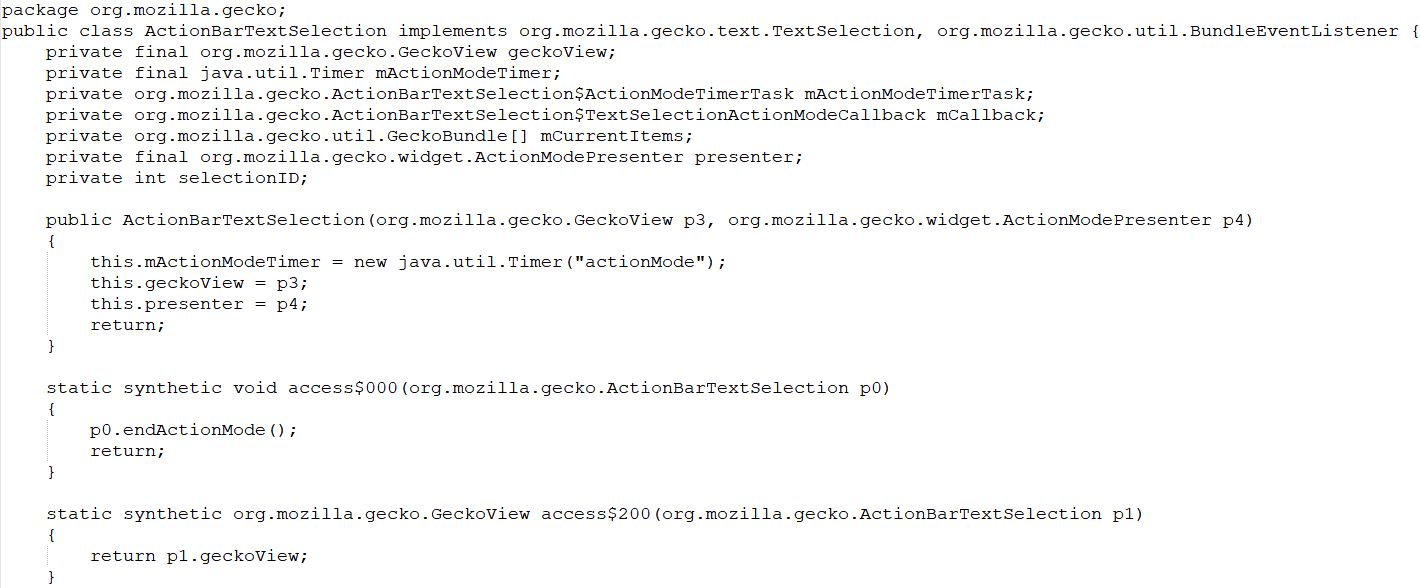


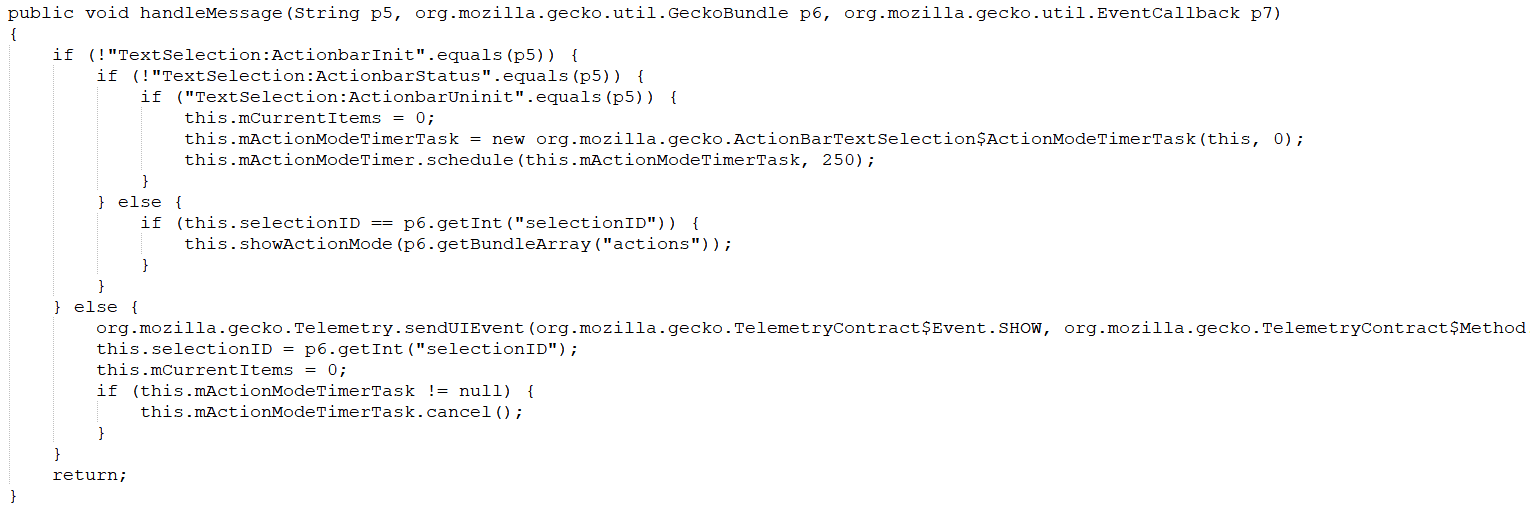
**The key code in sample is:**



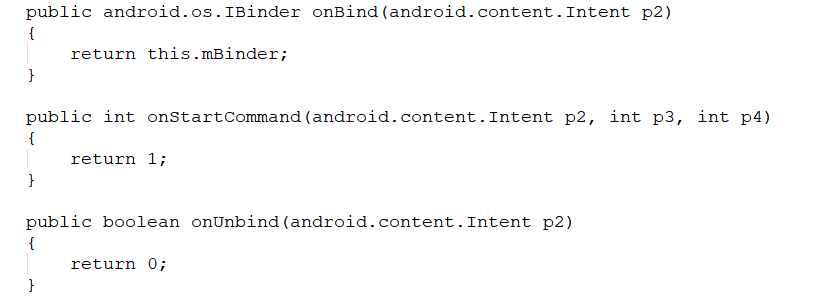


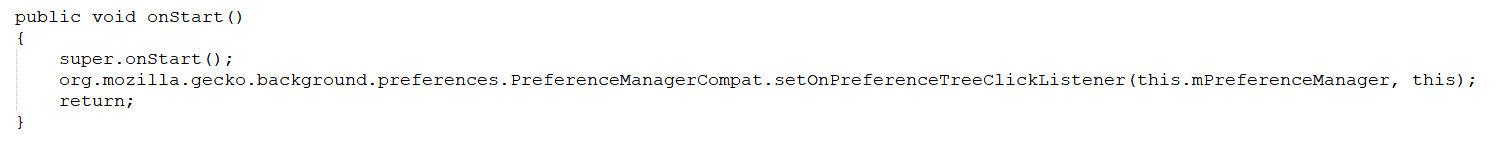
**Corresponding to the key code in this app：**

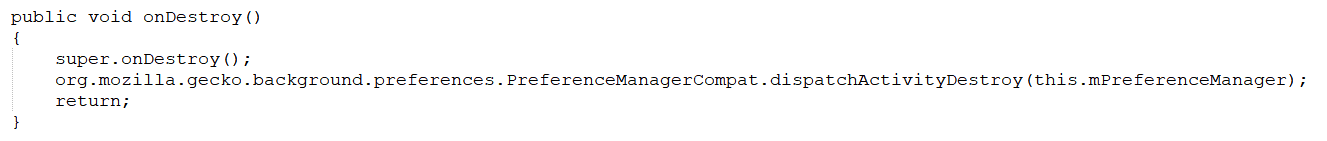




**Corresponding to the callback function in sample:**







**Error Cause Analysis:**

**Because the GPS and personal information acquired in sample are sent to a fixed URL address through the network, while the GPS information and device information acquired in app are not used to send to a fixed URL address. Although the hierarchical and non-hierarchical token are matched, the ultimate purpose is different and there is no malicious behavior, so the recognition fails.**