Getting logs

When some component misbehaves or stops working on Replicant, it is recommended to:

1. Get logs showing the issue
2. Open a ticket on our tracker to report the issue (**New issue** tab) or submit the logs to an existing issue that already describes the same misbehavior (**Update** at the bottom of the issue)

Buffers

The Android logging subsystem uses different log buffers: events, main, radio and system.
Generally speaking, when the issue you encountered concerned telephony, including data (3G), the buffer you want is radio. In any other case, that's the main buffer you want.

In some cases, the information provided by the Android log buffers is not sufficient and the message buffer of the Linux kernel is additionally required for investigating the issue.

There are various ways to obtain the logs:

Using ADB

First you need to had adb installed.

If you don't you can follow the ToolsInstallation page to install it.

Retrieving a buffer from the Android logging subsystem

Display a buffer from the Android logging subsystem:

```
adb logcat -b BUFFER
```

To prepare a new issue report, you need to save the output to a file:

```
adb logcat -b BUFFER -d > path/to/file
```

Retrieving the kernel message buffer

Display the kernel message buffer:

```
adb shell dmesg
```

To prepare a new issue report, you need to save the output to a file:

```
adb shell dmesg > path/to/file
```

Using aLogcat

aLogcat is a (free) Android app that will collect logs and save them to a file, either regularly or when you press the **Save** button from the app menu.
You can set the desired buffer from the Preferences.

After saving the log, you can get it from a file stored in the alogcat folder on the root of storage.

Submitting the logs

You can simply attach the log file to the issue report.

Encrypting radio logs

Logs from the radio buffer can contain privacy-sensitive information. If you don't want to have this information publicly available on

the issue tracker, you can encrypt the radio log, so only Replicant developers can view it.

Encrypting logs has the disadvantage that very likely no other contributors besides the main Replicant developers will be able to help in order to solve the issue.

First, you need to retrieve the GPG keys of the active Replicant developers. They are listed on the People page. It is recommended to retrieve them using

```
gpg --recv-keys KEY_ID
```

and replacing KEY_ID with the listed key IDs. If you have issues retrieving a key of a developer, you can still continue and encrypt the log for the other developers.

Then, you can encrypt the log file:

```
gpg --recipient KEY_ID_1 --recipient KEY_ID_2 ... --encrypt LOG_FILE
```

Replace KEY_ID_1 and KEY_ID_2 with the key IDs of the developers and add more --recipient options replacing ... until the key IDs of all active developers are listed. Replace LOG_FILE with the path to the log file you want to encrypt. The command should produce a file with the same name as your log file, but with the file ending gpg. This is the encrypted log file. Attach this file to the issue report.

Replicant developers will not share publicly entire unencrypted logs, but they might include unencrypted snippets of the logs in the issue discussion if it helps to fix the issue. The developers will make sure that these snippets do not contain privacy-sensitive information or that all privacy-sensitive information was removed.