

**NAME**

androiddump – Provide interfaces to capture from Android devices

**SYNOPSIS**

```
androiddump [ --help ] [ --version ] [ --extcap-version ] [ --debug ] [ --extcap-interfaces ]
[ --extcap-dlts ] [ --extcap-interface=<interface> ] [ --extcap-config ] [ --capture ]
[ --fifo=<path to file or pipe> ] [ --adb-server-ip=<IP address> ]
[ --adb-server-tcp-port=<TCP port> ] [ --logcat-text=<TRUE or FALSE> ]
[ --bt-server-tcp-port=<TCP port> ] [ --bt-forward-socket=<TRUE or FALSE> ]
[ --bt-local-ip=<IP address> ] [ --bt-local-tcp-port=<TCP port> ]
```

```
androiddump --extcap-interfaces [ --adb-server-ip=<IP address> ]
[ --adb-server-tcp-port=<TCP port> ]
```

```
androiddump --extcap-interface=<interface> [ --extcap-dlts ]
```

```
androiddump --extcap-interface=<interface> [ --extcap-config ]
```

```
androiddump --extcap-interface=<interface> --fifo=<path to file or pipe> --capture
```

**DESCRIPTION**

**Androiddump** is a extcap tool that provide interfaces to capture from Android device. There is only two requirements:

1. You must have Android SDK and add it PATH environment variable. PATH should contain directory with tools like "adb" and "android". Android SDK for various platform are available on: <https://developer.android.com/sdk/index.html#Other>
2. You must have permission to Android devices. Some Android devices requires on-screen authentication.

Supported interfaces:

1. Logcat Main (binary [<=Jelly Bean] or text)
2. Logcat System (binary [<=Jelly Bean] or text)
3. Logcat Events (binary [<=Jelly Bean] or text)
4. Logcat Radio (binary [<=Jelly Bean] or text)
5. Logcat Crash (text; from Lollipop)
6. Bluetooth Hcidump [<=Jelly Bean]
7. Bluetooth BlueDroid External Parser [Kitkat]
8. Bluetooth BtsnoopNet [>=Lollipop]
9. WiFi tcpdump [need tcpdump on phone]

Please note that it will work also for FirefoxOS or other Android-based stuffs.

**OPTIONS**

--help

Print program arguments.

--version

Print program version.

--extcap-version

Print extcapized version.

—debug

Print additional messages.

—extcap—interfaces

List available interfaces.

—extcap—interface=<interface>

Use specified interfaces.

—extcap—dlts

List DLTs of specified interface.

—extcap—config

List configuration options of specified interface.

—capture

Start capturing from specified interface save saved it in place specified by —fifo.

—fifo=<path to file or pipe>

Save captured packet to file or send it through pipe.

—adb—server—ip=<IP address>

Use other then default (127.0.0.1) ADB daemon's IP address.

—adb—server—tcp—port=<TCP port>

Use other then default (5037) ADB daemon's TCP port.

—logcat—text=<TRUE or FALSE>

If TRUE then use text logcat rather then binary. This option has effect only on Logcat interfaces. This have no effect from Lollipop where is no binary Logcat available.

Defaults to FALSE.

—bt—server—tcp—port=<TCP port>

Use other then default Bluetooth server TCP port on Android side. On Lollipop defaults is 8872, earlier 4330.

—bt—forward—socket=<TRUE or FALSE>

If TRUE then socket from Android side is forwarded to host side.

Defaults to FALSE.

`--bt-local-ip=<IP address>`

Use other than default (127.0.0.1) IP address on host side for forwarded socket.

`--bt-local-tcp-port=<TCP port>`

Specify port to be used on host side for forwarded socket.

## EXAMPLES

To see program arguments:

```
androiddump --help
```

To see program version:

```
androiddump --version
```

To see interfaces:

```
androiddump --extcap-interfaces
```

### Example output

```
interface {display=Android Logcat Main unknown MSM7627A}{value=android-logcat-main}
interface {display=Android Logcat System unknown MSM7627A}{value=android-logcat-system}
interface {display=Android Logcat Radio unknown MSM7627A}{value=android-logcat-radio}
interface {display=Android Logcat Events unknown MSM7627A}{value=android-logcat-events}
interface {display=Android Bluetooth Hcidump unknown MSM7627A}{value=android-bluetooth-hcidump}
```

Human-readable display name of interfaces contains interface type, one of:

```
android-logcat-main (Android Logcat Main)
android-logcat-system (Android Logcat System)
android-logcat-radio (Android Logcat Radio)
android-logcat-events (Android Logcat Events)
android-logcat-text-main (Android Logcat Main)
android-logcat-text-system (Android Logcat System)
android-logcat-text-radio (Android Logcat Radio)
android-logcat-text-events (Android Logcat Events)
android-logcat-text-crash (Android Logcat Crash)
android-bluetooth-hcidump (Android Bluetooth Hcidump)
android-bluetooth-external-parser (Android Bluetooth External Parser)
android-bluetooth-btsnoop-net (Android Bluetooth Btsnoop Net)
android-wifi-tcpdump (Android WiFi)
```

Then Android Device's name if available, otherwise "unknown".

Last part of it is DeviceID - the identifier of the device provided by Android

For example:

```
"Android Logcat Main unknown MSM7627A"
```

"Android Logcat Main" - user-friendly type of interface

"unknown" - name of Android Device

"MSM7627A" - device ID

To see interface DLTs:

```
androiddump --extcap-interface=android-bluetooth-hcidump-MSM7627A --extcap-dlts
```

#### Example output

```
dlt {number=99}{name=BluetoothH4}{display=Bluetooth HCI UART transport layer plus
```

To see interface configuration options:

```
androiddump --extcap-interface=android-bluetooth-hcidump-MSM7627A --extcap-config
```

#### Example output

```
arg {number=0}{call=--adb-server-ip}{display=ADB Server IP Address}{type=string}{
arg {number=1}{call=--adb-server-tcp-port}{display=ADB Server TCP Port}{type=inte
```

To capture:

```
androiddump --extcap-interface=android-bluetooth-hcidump-MSM7627A --fifo=/tmp/blu
```

#### Note

To stop capturing CTRL+C/kill/terminate application.

## SEE ALSO

wireshark(1), tshark(1), dumpcap(1), extcap(4)

## NOTES

**Androiddump** is part of the **Wireshark** distribution. The latest version of **Wireshark** can be found at <https://www.wireshark.org>.

HTML versions of the Wireshark project man pages are available at <https://www.wireshark.org/docs/man-pages>.

## AUTHORS

### Original Author

Michal Labedzki <michal.labedzki[AT]tieto.com>

### Contributors

Roland Knall <rknall[AT]gmail.com>