Bluetooth LE Packet-Capture auf Android

Die BLE-Kommunikation unter Android kann aus vielen Gründen schwierig sein, darunter Inkonsistenzen bei der Hardware wie Bluetooth-Adaptern (Funkgeräten), bei der Software wie der Firmware, mit der der Bluetooth-Adapter programmiert ist, und bei den Implementierungen des Android-Betriebssystems durch die Hersteller.

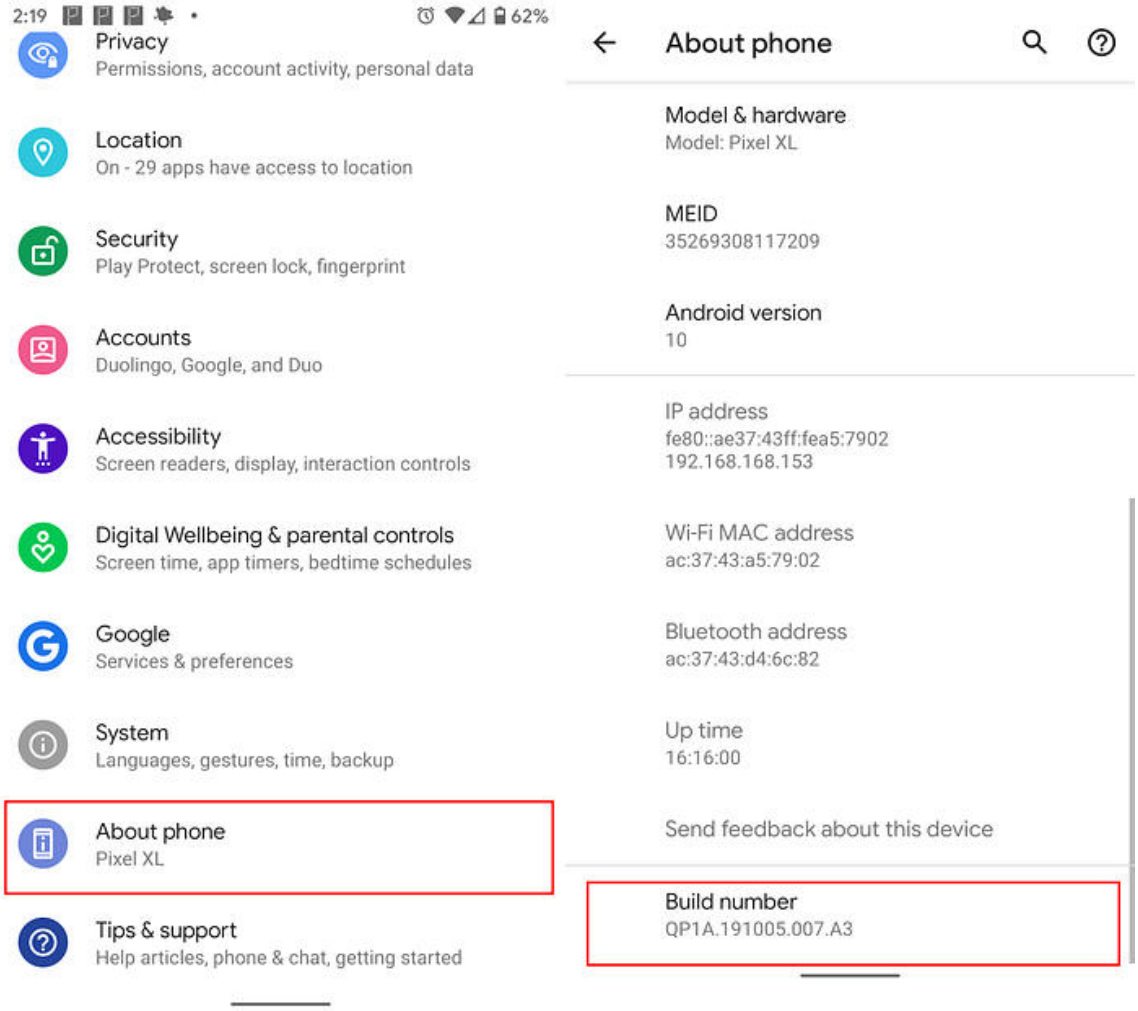
So funktioniert die Bluetooth-Paketerfassung unter Android

Benötigt werden:

- Ein Android-Gerät mit Android 4.4 (KitKat) oder höher, das als zentrales Gerät verwendet wird
- Ein BLE-Gerät, das als Peripheriegerät verwendet wird
- Eine Windows-, Linux- oder Mac-Workstation mit installierten Android SDK-Tools

Entwickleroptionen aktivieren

Die Entwickleroptionen müssen aktiviert sein, um Pakete beim Senden und Empfangen abzufangen und zu speichern. So werden die Entwickleroptionen aktiviert:

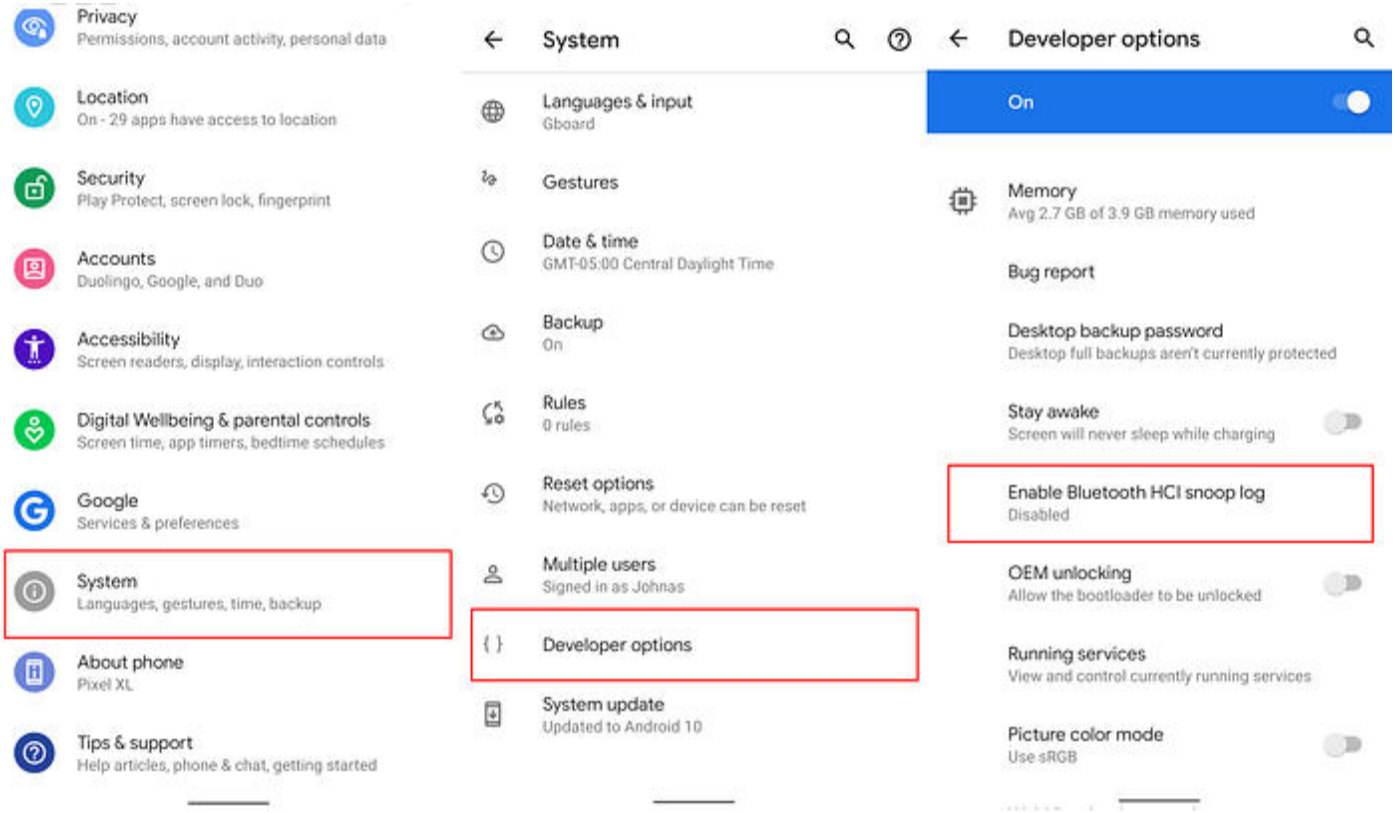


1. Öffnen Sie auf einem Standard-Android-Gerät „Einstellungen“ > „Über das Telefon“ > „Build-Nummer“.
2. Tippen Sie sieben Mal auf „Build-Nummer“. Nach den ersten paar Malen sollten Sie eine Countdown-Anzeige sehen, bis die Entwickleroptionen freigeschaltet sind. Nach der Aktivierung erscheint die Meldung „Sie sind jetzt Entwickler!“.
3. Gehen Sie zurück zu Einstellungen > System > Erweitert, wo Sie nun den Eintrag Entwickleroptionen finden, oder suchen Sie mit der Suchfunktion nach „Entwickleroptionen“.

Beachte: es ist nicht empfehlenswert, die Entwickleroptionen länger als nötig aktiviert zu lassen, da dies die Sicherheit des Geräts beeinträchtigt. Schließlich werden Daten erfasst und gespeichert, die zwischen dem zentralen und den peripheren Geräten übertragen werden sollen, was ein gewisses Risiko birgt.

Bluetooth-HCI-Snoop-Protokoll aktivieren

Nachdem die Entwickleroptionen aktiviert wurden, kann nun das Bluetooth-HCI-Snoop-Protokoll aktiviert werden. Wenn das Bluetooth-HCI-Snoop-Protokoll aktiviert ist, erfasst das Android-Framework die zwischen zentralen und peripheren Geräten gesendeten und empfangenen Bluetooth-Pakete und speichert sie als Teil eines Fehlerberichts. So wird das Bluetooth-HCI-Snoop-Protokoll aktiviert:



1. Auf einem Standard-Android-Gerät öffnen Sie Einstellungen > System > Erweitert > Entwickleroptionen.
2. Tippen Sie auf Bluetooth-HCI-Snoop-Protokoll aktivieren.
3. Tippen Sie im angezeigten Dialogfeld auf die Option Aktivieren.

Nachdem das Bluetooth-HCI-Snoop-Protokoll aktiviert wurde, muss der Bluetooth-Adapter der Smartphones neu gestartet. Dazu: Bluetooth auf dem Gerät aus- und wieder einschalten. Alle vom Bluetooth-Adapter gesendeten und empfangenen Bluetooth-Pakete werden nun im Bluetooth-HCI-Snoop-Protokoll gespeichert.

BLE-Kommunikation initiieren

Nachdem nun das Gerät für die Erfassung des übertragenen Bluetooth-Datenverkehrs konfiguriert wurde, kann die Kommunikation zwischen dem zentralen und den peripheren Geräten durchgeführt werden.

Extrahieren des Bluetooth-HCI-Snoop-Protokolls

Um das Bluetooth-HCI-Snoop-Protokoll aus dem Android-Gerät zu extrahieren, muss das Android-Gerät an den PC angeschlossen werden und mit dem Befehl „adb“ ein Fehlerbericht (bug report) erstellt werden. Der Befehl sollte in dem (Arbeits-) Verzeichnis ausgeführt werden, in dem der Fehlerbericht erstellt werden soll.

adb bugreport bugreport

Dadurch wird der Fehlerbericht in eine ZIP-Datei namens bugreport.zip auf den Arbeitsplatzrechner extrahiert. Entpacken des Fehlerberichts:

unzip bugreport.zip

In den extrahierten Dateien muss die Datei mit dem Namen „btsnoop_hci.log“ gesucht werden. Diese Datei enthält die Paketerfassung. (Hinweis: Ordner *FS\data\misc\bluetooth\logs*)

Bluetooth-HCI-Snoop-Protokoll deaktivieren

Nachdem der gewünschte Datenverkehr erfasst wurde, kann das Bluetooth-HCI-Snoop-Protokoll deaktiviert werden. Das Bluetooth-HCI-Snoop-Protokoll kann auf die gleiche Weise deaktiviert werden, wie es aktiviert wurde:

1. Öffnen Sie unter Android „Einstellungen“ > „System“ > „Erweitert“ > „Entwickleroptionen“.
2. Tippen Sie auf „Bluetooth-HCI-Snoop-Protokoll aktivieren“.
3. Tippen Sie im angezeigten Dialogfeld auf die Option „Deaktivieren“.

Auch hier müssen die Bluetooth-Dienste umgeschaltet werden, um den Bluetooth-Adapter neu zu starten. Außerdem ist jetzt möglicherweise ein guter Zeitpunkt, um die Entwickler-optionen zu deaktivieren

Analyse des Bluetooth-HCI-Snoop-Protokolls

Ein beliebter und bekannter Netzwerkprotokollanalysator ist Wireshark. Wenn die MAC-Adresse des Peripheriegeräts bekannt ist, ist der folgende Anzeigefilter hilfreich:

> ***bthci_evt.bd_addr == xx:xx:xx:xx:xx:xx || bthci_cmd.bd_addr == xx:xx:xx:xx:xx:xx || bluetooth.addr == xx:xx:xx:xx:xx:xx***

xx:xx:xx:xx:xx:xx: muss durch die MAC-Adresse des verbundenen Geräts ersetz werden.

MAC-Adresse des verbundenen Geräts

Dazu wird der Bluetooth-Adapter auf dem Handy geöffnet (Schaltfläche Bluetooth ein-ausschalten). Es wird eine Liste der gekoppelten Geräte angezeigt. Wird das gesuchte Gerät dort nicht angezeigt, muss es zunächst gekoppelt werden. Neben dem gekoppelten Gerät wird ein Symbol angezeigt, mit dem man weitere Informationen zu dem Gerät (u.a. die MAC-Adresse) abrufen kann.