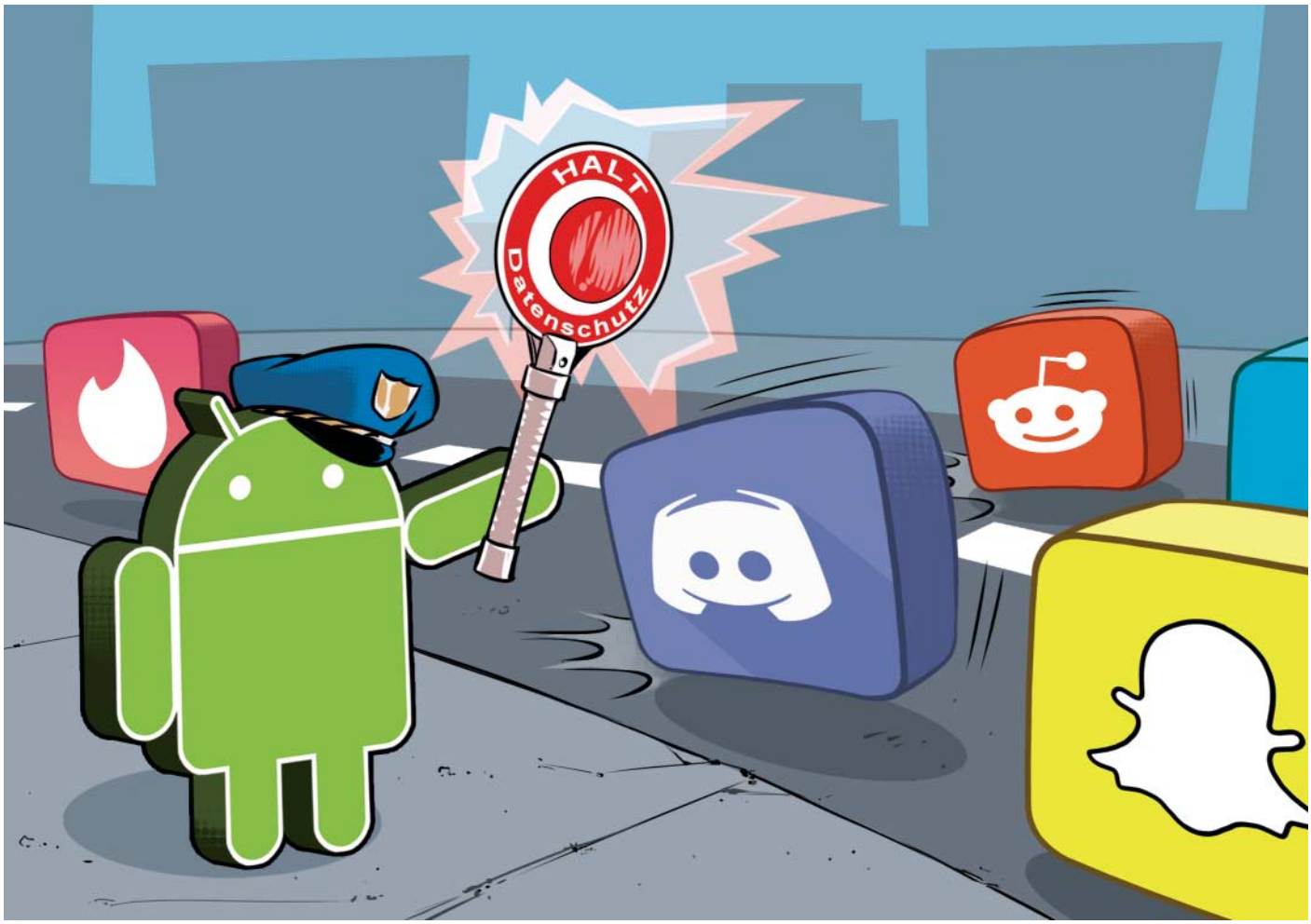



Bild: Albert Hulm

# Mobile Verkehrskontrolle

## Traffic-Analyse-Apps für Android

**Android und die installierten Apps sprechen gern und oft mit dem Internet. Doch welche Daten werden dabei übertragen? Und wohin? Mit den passenden Werkzeugen finden Sie das leicht heraus – ganz ohne Root-Zugriff.**

**Von Ronald Eikenberg**

Android-Apps genießen einen enormen Vertrauensvorschuss: Sie fordern Zugriff auf Kamera, Kontakte, Standort und vieles mehr, ohne jedoch transparent offenzulegen, was davon sie ins Internet schicken und wie diese Übertragung abgesichert ist. Wer wissen möchte, was hinter den Kulissen mit seinen Daten geschieht, muss einen Blick in den Netzwerkverkehr werfen. Mit den passenden Analyse-Apps ist das leichter denn je.

Das etablierte Standardverfahren zur Analyse von Smartphone-Traffic ist der Einsatz eines Analyseproxies wie mitmproxy oder Burp. Diese Vorgehensweise ist jedoch recht umständlich, es funktioniert nur im WLAN und zudem muss ein Rechner in Reichweite sein, auf dem der Proxy läuft. Viel komfortabler ist der Einsatz eines Analyse-Tools direkt auf dem Smartphone. Damit klappt die Traffic-Auswertung überall und jederzeit – sogar im Mobilfunknetz.

Die in diesem Artikel vorgestellten Apps nutzen einen Trick, um sich in den Traffic des Systems einzuklinken: Sie geben sich als VPN-Service aus, wodurch der gesamte Netzwerkverkehr durch sie hindurchgeschleust wird. Diese Schnittstelle nutzen auch VPN-Apps, um die Verbindung zu einem externen VPN-Anbieter herzustellen. Im Fall der Traffic-Analyse-Apps wird der Datenverkehr jedoch lokal ausgewertet und nicht zu einem VPN-Gateway außerhalb gelenkt.

### Netzwerkrekorder

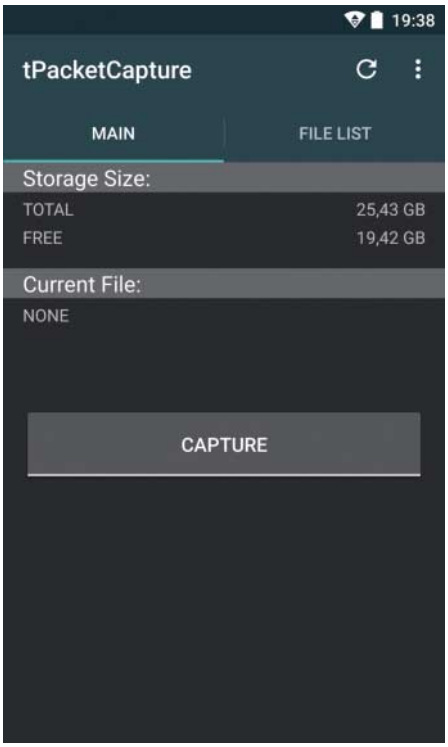
Eine der ersten Apps, die den VPN-Trick zur Traffic-Auswertung nutzten, ist tPacketCapture von Taosoftware (siehe ct.de/ynfx). Die Gratis-App beherrscht nur eine Funktion, diese aber mit Bravour: Vergleichbar mit dem unix-Tool tcpdump legt die App Traffic-Mitschnitte im PCAP-Format an, die man am besten am PC auswertet. tPacketCapture läuft unter allen Android-Versionen ab 4.0 und ist denkbar

simpel aufgebaut – es gibt nämlich nur einen Knopf namens „Capture“. Betätigen Sie ihn, um die Aufzeichnung zu starten. Danach meldet sich eine Sicherheitsabfrage des Android-Systems und erkundigt sich, ob Sie mit dem Aufbau der VPN-Verbindung durch die Analyse-App einverstanden sind. Diese Abfrage bestätigen Sie mit „OK“. Anschließend finden Sie unter „Current File“ den Dateinamen des laufenden Mitschnitts sowie die Dateigröße. Den Speicherort der Mitschnitte erfährt man auf der Unterseite „File List“. Die Dateien befinden sich im internen Speicher unter /Android/data/jp.co.taosoftware.android.packetcapture/files/. Um die Mitschnitte komfortabel auswerten zu können, übertragen Sie diese auf einen Rechner, zum Beispiel per USB-Kabel oder Mail. Zur Ansicht eignet sich das Analyse-Programm Wireshark (siehe ct.de/ynfx), das unter Windows, Linux und macOS läuft.

Die Auswertungsmöglichkeiten mit Wireshark sind schier grenzenlos. Ein guter Anfang ist die Suche nach Daten, die ungeschützt im Klartext übertragen werden. Tippen Sie hierzu in die Filterzeile von Wireshark („Anzeigefilter anwenden …“) die Zeichenfolge `http` ein und aktivieren Sie den Filter mit Enter. Verschlüsselten Datenverkehr spüren Sie mit dem Filter `tls` auf. Aktivieren Sie unter „Ansicht/Namensauflösung“ die Option „Netzwerkadresse auflösen“, um zu erfahren, welche Server sich hinter den IP-Adressen befinden. Die Funktion „Statistiken/Verbindungen“ fasst zusammen, mit welchen Servern das Smartphone in welchem Umfang kommuniziert hat. Ein Klick auf „Namensauflösung“ zeigt auch hier wieder die zu den IP-Adressen passenden Hostnamen. Wer sich ausschließlich für den Datenverkehr einer bestimmten App interessiert und unnötigen Beifang vermeiden möchte, der kann zu der neun Euro teuren Pro-Version von tPacketCapture greifen. Diese kann bei Bedarf ausschließlich den Datenverkehr bestimmter Apps aufzeichnen.

## Verschlüsselung aufmachen

tPacketCapture erstellt einen passiven Mitschnitt und greift nicht in den Datenverkehr ein, was den Vorteil hat, dass man einen unverfälschten Eindruck vom Traffic bekommt. Der Nachteil dieser Methode ist, dass verschlüsselter Verkehr verschlüsselt bleibt – es besteht keine Möglichkeit, den Inhalt von Krypto-Paketen zu kontrollieren. Dazu benötigt man ein Analysewerkzeug, das aktiv eingreift und den Datenverkehr von Apps und System zunächst entschlüsselt und dann erneut verschlüsselt, ehe die Daten an das eigentliche Ziel weitergereicht werden. Dies ist einfacher, als es klingt. Sie benötigen dazu ein Smartphone oder Tablet, auf dem Android 6.0.x oder älter läuft. Alternativ tut es auch ein Emulator mit einer passenden Android-Version.



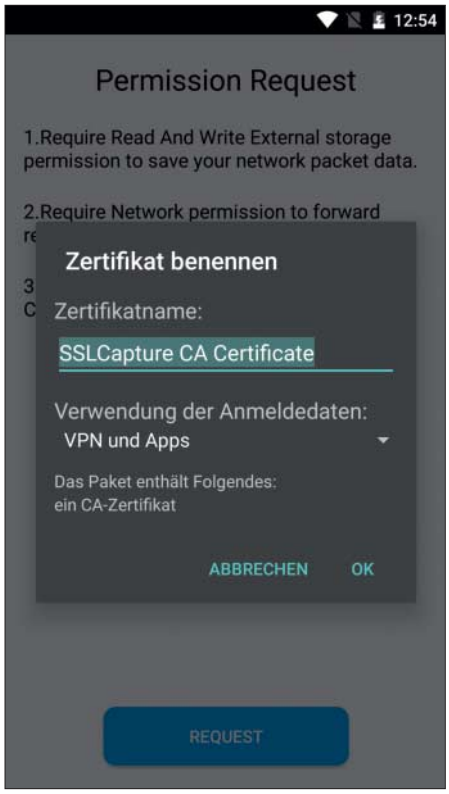

**tPacketCapture ist einfach aufgebaut. Der Capture-Button startet die Aufzeichnung in eine PCAP-Datei.**

Ab Android 7 führen verschärfte Sicherheitsbestimmungen dazu, dass die Analyse von TLS/SSL-Traffic bei vielen Apps nicht mehr ohne Weiteres möglich ist. Betroffen sind alle Apps, die mindestens für den API-Level 24 kompiliert wurden und unter Android 7 ausgeführt werden. In solchen Fällen ist entweder eine Modifikation des Systems (Root-Zugriff) oder der App nötig (siehe ct.de/ynfx). Beides ist recht umständlich – einfacher ist die Anschaffung eines günstigen Android-6-Smartphones zur App-Beobachtung. Auf einem solchen Gerät kann man Android-Apps erst mal gefahrlos ausprobieren und den Datenabfluss kontrollieren, ehe man sie auf das täglich genutzte Haupt-Smartphone und die darauf gespeicherten Datenschätze loslässt.

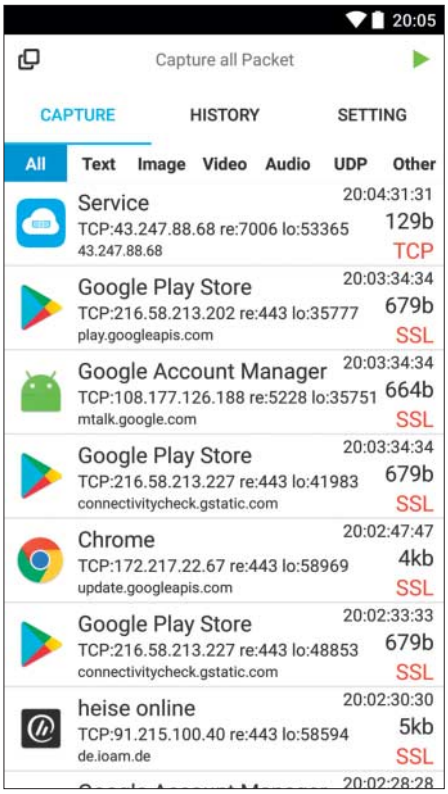
Jetzt fallen die letzten Hüllen. Um den Inhalt verschlüsselter Verbindungen einzusehen, können Sie zum Beispiel die kostenlose App NetCapture einsetzen (siehe ct.de/ynfx). Sie agiert ebenfalls als VPN-Service, greift aber – anders als tPacketCapture – aktiv in die Verbindung ein, um den TLS/SSL-Traffic zu entschlüsseln. Beim ersten Start leitet Sie die App durch die Einrichtung. Zunächst müssen Sie der App die Berechtigung einräumen, auf den lokalen Speicher zuzugreifen. Diese benötigt sie zum Speichern der Mitschnitte. Anschließend installiert NetCapture ein SSL-Zertifikat in den Zertifikatsspeicher des Betriebssystems. Dieser Schritt ist notwendig, damit System und Apps dem Analyse-Tool das zum Aufbau der verschlüsselten Verbindungen nötige Vertrauen entgegenbringen. Bestätigen Sie die Installation des Zertifikats. Falls Sie Ihr System noch nicht mit einem Passcode geschützt haben, wird Sie Android nun auffordern, dies nachzuholen. Anschließend öffnet sich der Hauptbildschirm von NetCapture.

Drücken Sie auf den grünen Pfeil oben rechts, um die Aufzeichnung zu starten. Daraufhin erkundigt sich das Tool, ob Sie die „Floating View Function“ aktivieren möchten. Es handelt sich dabei um ein schwebendes Minifenster, über das Sie jederzeit den Traffic-Fluss beobachten können – ganz gleich, welche App sich gerade im Vordergrund befindet. Diese Funktion ist durchaus nützlich, klicken Sie also ruhig auf „Enable“. Im folgenden Dialog schalten Sie für diese Funktion die Berechtigung „Einblenden über anderen Apps zulassen“ scharf. Danach müssen Sie nur noch die Verbindungsabfrage für die lokale VPN-Verbindung zulassen.

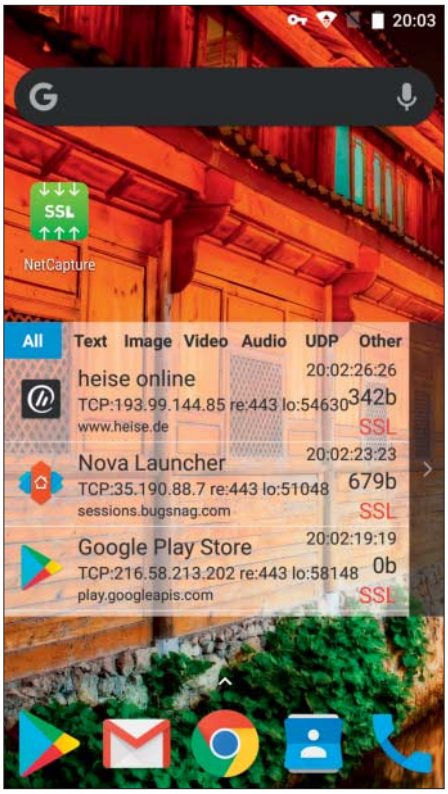
Jetzt ist es geschafft: Das Hauptfenster von NetCapture füllt sich nun nach und nach mit den TCP-Verbindungen der installierten Apps und des Systems. Sie erkennen auf den ersten Blick, von welcher App eine Verbindung ausging und welcher Server auf welchem Port kontaktiert wurde. Zudem erfahren Sie den Zeitpunkt der Anfrage, die Größe der übertragenen Pakete, das Protokoll sowie die angefragte URL. Den Inhalt der Pakete sehen Sie, indem Sie auf eine der Verbindungen tippen. In der Detailansicht steht oben in Rot die ausgehende Anfrage, darunter befindet sich in Blau die Antwort des Servers. Wurden Bilder oder Videodateien übertragen, können Sie diese direkt anzeigen lassen. Auch abgefischte Audiodateien spielt NetCapture auf Wunsch im Analysefenster ab. Ein Klick auf „Share“ öffnet das Teilen-Menü von Android, über das Sie den




Um verschlüsselten Datenverkehr mitzulesen, muss man das Zertifikat der Analyse-App installieren.




NetCapture ordnet den Datenverkehr einzelnen Apps zu und kann den Inhalt verschlüsselter Pakete anzeigen.




Durch das schwebende Mini-Fenster von NetCapture hat man den Traffic jederzeit im Blick.

Mitschnitt als Textdatei etwa per Mail weitergeben können. Das PCAP-Format beherrscht NetCapture nicht. Wenn Sie im Hauptfenster auf die rote Stopptaste oben rechts drücken, wird die Aufzeichnung beendet und automatisch gespeichert. Alle aufgezeichneten Mitschnitte finden Sie unter „History“. Um sie extern zu archivieren oder auf einem großen Bildschirm zu betrachten, können Sie diese aus dem Verzeichnis VpnCapture des internen Speichers auf einen Rechner kopieren.

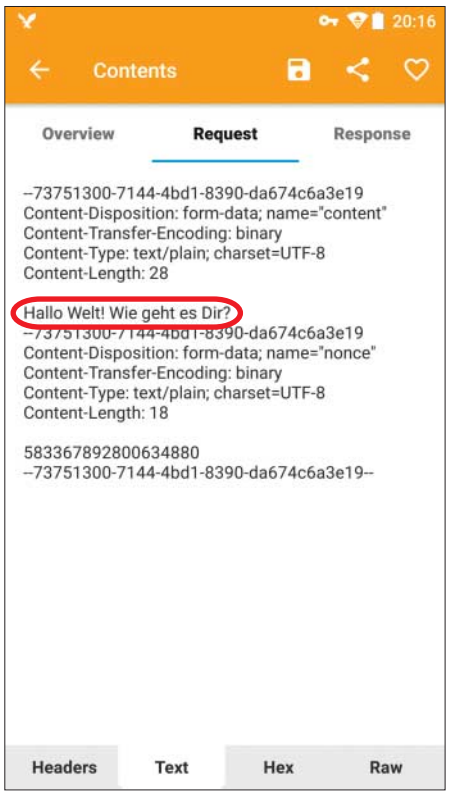
Unter „Setting“ hält NetCapture einige interessante Optionen bereit. „Auto Capture“ etwa startet die Aufzeichnung automatisch, sobald Sie das Tool öffnen. Aktivieren Sie „Save UDP“, um auch UDP-Pakete analysieren zu können. So können Sie zum Beispiel DNS-Anfragen nachvollziehen und überprüfen, ob diese noch unverschlüsselt auf Port 53 rausgehen oder ob schon ein verschlüsseltes Verfahren wie DNS-over-TLS (Port 853) oder DNS-oder-HTTPS (443) im Einsatz ist. Eine weitere nützliche Funktion verbirgt sich hinter dem Knopf oben links (zwei Kästchen): Hier können Sie den Datenverkehr filtern. Wählen Sie unter „Selected App“ eine installierte App aus, um nur deren Traffic anzeigen zu lassen. Zudem können Sie Verbindungen zu bestimmten IP-Adressen und Hosts herausfiltern.

NetCapture ist kostenlos und werbefinanziert. Wer sich an dem Werbebanner stört, kann für fünf Euro die werbefreie Ausgabe erwerben. Diese heißt NetKeeper und bietet gegenüber der Gratis-Version auch noch eine Suchfunktion. Falls NetCapture respektive NetKeeper nicht wie erwartet funktioniert, lohnt sich ein Blick auf Packet Capture, das wir in c’t 13/2017 ausführlich vorgestellt haben (siehe ct.de/ynfx). Es hat weniger Funktionen, erledigt die Grundaufgaben aber ebenso zuverlässig.

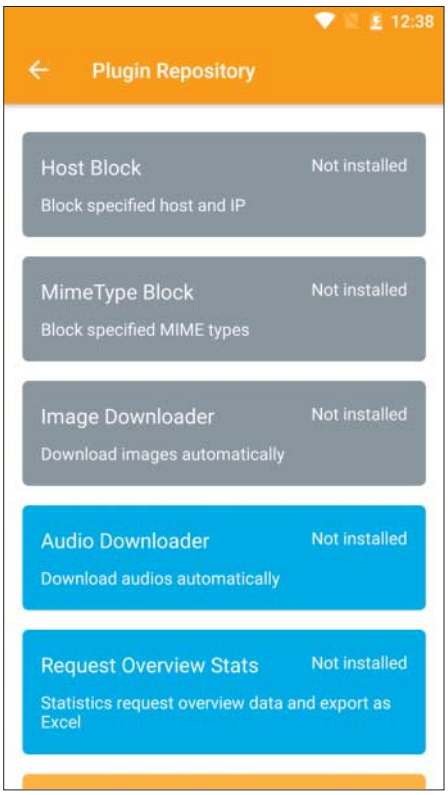
## Dazwischenfunken

In manchen Situationen möchte man die Position des stillen Beobachters verlassen und selbst in das Geschehen eingreifen. Dann ist die App HttpCanary nützlich, die den Datenverkehr nicht nur umfassend auswertet und entschlüsselt, sondern auch beliebig manipulieren kann. Wer möchte, bekommt damit Kontrolle über jedes einzelne Datenpaket. Auf diese Weise kann man beim Testen einer App zum Beispiel sensible Informationen aus den ausgehenden Datenpaketen entfernen oder den Server mit unerwarteten Werten konfrontieren – Letzteres ist etwa im Rahmen eines Sicherheitstests ein gängiges Vorgehen. Entdeckt ein Security-Forscher, dass eine App die Datei https://example.com/daten/rechnung/kunde-23546.pdf abruft, dann wird er auch probieren, ob der Server die Datei kunde-23547.pdf herausrückt.

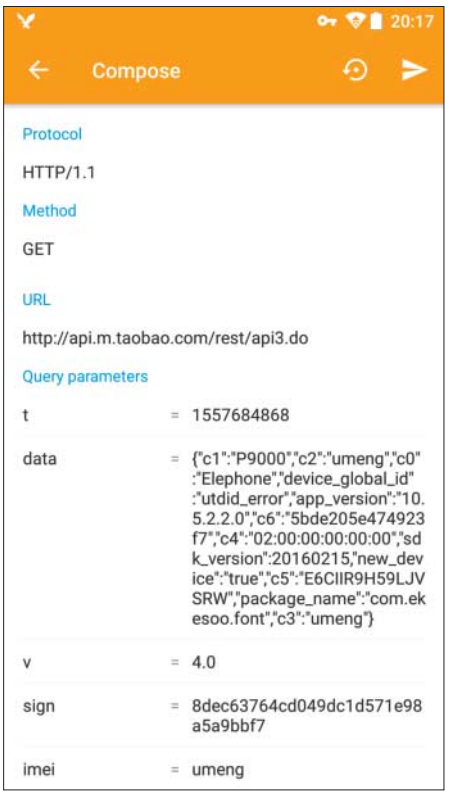
Da auch HttpCanary verschlüsselten Datenverkehr auswerten kann, müssen Sie bei dessen Einrichtung ebenfalls ein Zertifikat installieren. Tippen Sie auf das blaue Symbol unten rechts, um die Aufnahme zu starten. Anschließend tauchen die ausgehenden Datenpakete und die Antworten der Server im Hauptfenster auf. Anders als die bisher erwähnten Tools hat sich HttpCanary ausschließlich auf HTTP(S)-Traffic und WebSocket spezialisiert, andere Protokolle sind also außen vor. Wenn man auf eines der Datenpakete tippt, wird schnell klar, dass die Formulierung „spezialisiert“ hier durchaus angebracht ist: Es öffnet sich zunächst eine Übersicht, welche die Daten der Verbindung aufbereitet. Dort zeigt die App nicht nur die angesprochene URL und die IP-Adresse des Servers an, sondern auch Informationen aus dem Header wie das eingesetzte Protokoll, den HTTP-Statuscode und etwaige Cookies.




**Hallo Welt: Eine Analyse mit HttpCanary zeigt, dass der Messenger Discord keine Ende-zu-Ende-Verschlüsselung nutzt.**




**Mit Plug-ins bringt man HttpCanary neue Tricks bei. So schaltet man etwa einen Host-Filter scharf.**




**Mit HttpCanary kann man nicht nur mitlesen, sondern den HTTP(S)-Verkehr sogar beliebig verändern.**

Ganz unten finden Sie noch die Verbindungsdauer und die exakte Größe von Anfrage und Antwort. Das ist nützlich, wenn man etwa als Entwickler der Netzwerk-Performance seiner App auf den Zahn fühlen möchte. Auf den Registerreitern Request und Response können Sie alle Details zu Anfrage und Serverantwort abrufen. Zunächst präsentiert HttpCanary die Header, klickt man unten auf „Text“, sieht man den Inhalt des HTTP(S)-Pakets in Textform. Zudem kann man eine Hex-Ansicht aufrufen („Hex“) und unter „Preview“ einige Inhaltstypen wie Mediendateien oder JSON-Daten direkt anzeigen lassen. Für Entwickler interessant ist die ansprechende Darstellung von WebSocket-Paketen: HttpCanary zeigt den Austausch wie eine Chat-Konversation zwischen Client und Server an.

Zurück im Hauptfenster führt ein Klick auf die Lupe zu den umfangreichen Suchfiltern. Darüber können Sie gezielt nach Inhaltstypen wie Mediendateien suchen, aber auch nach Anfragen, die vom Server mit einem Fehlercode beantwortet wurden, um schnell herauszufinden, wo es hakt. Um aktiv in den Datenverkehr einzugreifen, hält man während der Aufzeichnung den Finger auf eines der Datenpakete, um das Kontextmenü zu öffnen. Darüber hat man die Qual der Wahl: „Repeat“ wiederholt das selektierte Paket schlicht, „Repeat Advanced“ wiederholt es beliebig oft mit zeitlichem Versatz. Mit „Compose“ erstellt man ein neues Datenpaket auf Grundlage der ausgewählten Anfrage. Diese lässt sich vor dem Abschicken beliebig verändern. Über „Static Injection“ legt man eine Regel an, anhand derer aus- oder eingehende Datenpakete automatisch modifiziert werden, ehe sie ihr Ziel erreichen. So kann man beispielsweise den User-Agent ändern und vorgeben, dass die Datenpakete von einem anderen Betriebssystem verschickt wurden. Last, but not least gibt es die „Dynamic Injection“. In diesem Modus hält die Analyse-App eine Anfrage an und öffnet sie in einem Editor. Man kann sie beliebig modifizieren, ehe man sie ins Internet rausschickt.

Weitere spannende Funktionen verbergen sich in den „Settings“ – etwa das gezielte Mitschneiden des Datenverkehrs einzelner Apps oder der Plug-in-Manager, über den man weitere Features wie eine einfache Firewall einschalten kann (Host Block). Wie auch NetCapture ist HttpCanary kostenlos und zeigt ein Werbebanner an. Die Funktionen zur Manipulation des Traffics sind sieben Tage nach Installation nutzbar, danach kann man sich den Datenverkehr nur noch anschauen. Für 4,50 Euro kann man alle Funktionen zeitlich unbegrenzt freischalten und wird zudem die Werbung los – angesichts des enormen Funktionsumfang ist das ein faires Geschäft.

## Die passende App

Die vorgestellten Apps nutzen allesamt die VPN-Schnittstelle von Android, um Netzwerkverkehr anwenderfreundlich mitzuschneiden. In ihrem Funktionsumfang unterscheiden sie sich jedoch enorm. Wer lediglich mit minimalem Aufwand einen Traffic-Mitschnitt im PCAP-Format erstellen und diesen später am Rechner auswerten möchte, greift am besten zu tPacketCapture. Will man einer Android-App live über die Schulter schauen und auch verschlüsselten Datenverkehr einsehen, dann ist NetCapture eine gute Wahl. Netzwerkprofis, Entwickler und Hacker werden an HttpCanary ihre Freude haben – die Analyse-App zeigt den Traffic nicht nur an, sondern verändert ihn auch nach Gusto des Nutzers. *(rei@ct.de)* c't

***Analyse-Apps:* ct.de/ynfx**