Captura de compartilhamento de dados pessoais

A infraestrutura necessária para capturar dados enviados a partir de um dispositivo, como telefone celular ou tablet, é composta por um servidor proxy e por certificado(s) implantado(s) no dispositivo, utilizando uma abordagem *Man-In-The-Middle*, na qual toda comunicação entre o dispositivo e a Internet passará pelo servidor proxy e, com o certificado do servidor implantado no dispositivo, poderemos capturar os pacotes de mensagens em *plain text*.

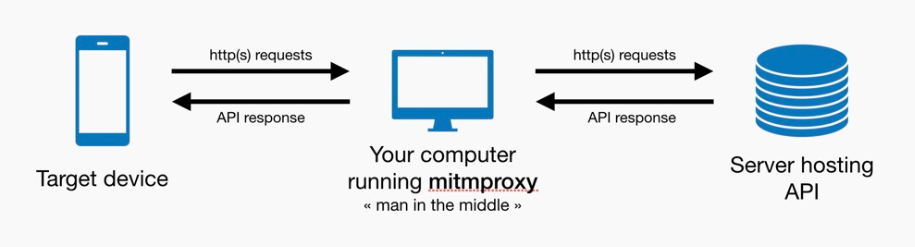
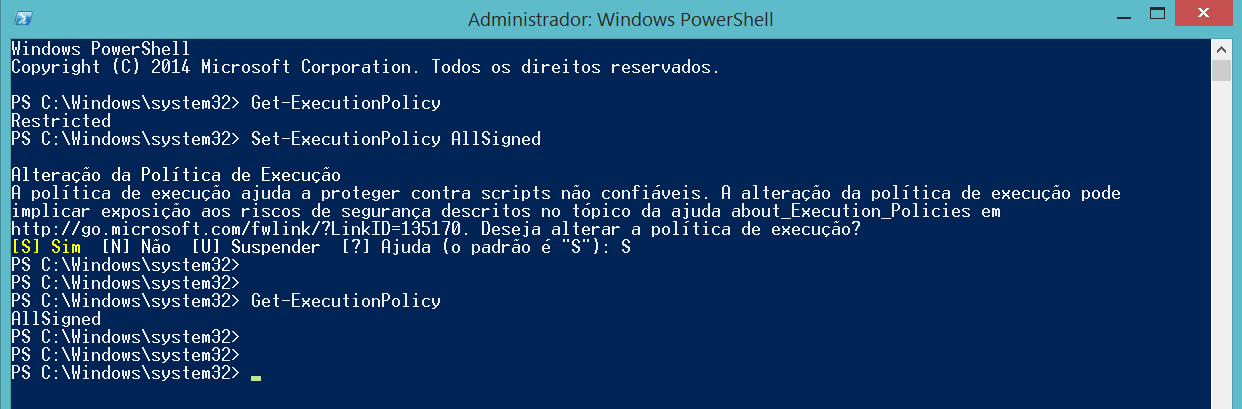


Figura 1 – Infraestrutura para captura de dados. Fonte: [2].

A instalação e configuração do servidor proxy e posterior configuração do dispositivo para utilizar esse servidor é mostrada a seguir. Neste estudo, utilizamos o software *mitmproxy*, disponível em <https://mitmproxy.org/>, instalado em um servidor Windows 8.1.

Durante a execução do instalador, é possível que a configuração da política de execução de scripts configurada impeça sua execução. Conforme [1], precisamos utilizar uma das políticas disponíveis no sistema operacional. O padrão é *restricted*. Para a execuçao dos scripts de *mitmproxy*, deve-se alterar a política para *unrestricted*. Altere a política usando os comandos mostrados abaixo.

Figura 2 – Alteração da política de execução de scripts. Fonte: Autor.

Na figura acima, o comando *Set-ExecutionPolicy* está configurando AllSigned, entretanto essa política não é suficiente para execução dos scripts de *mitmproxy*. Logo após a instalação, deve-se retornar a política para o padrão, *restricted*.

Após concluir a instalação do software, executamos o mitmweb, uma interface de navegador para visualizar o conteúdo capturado e, principalmente, construir filtros para essa captura.

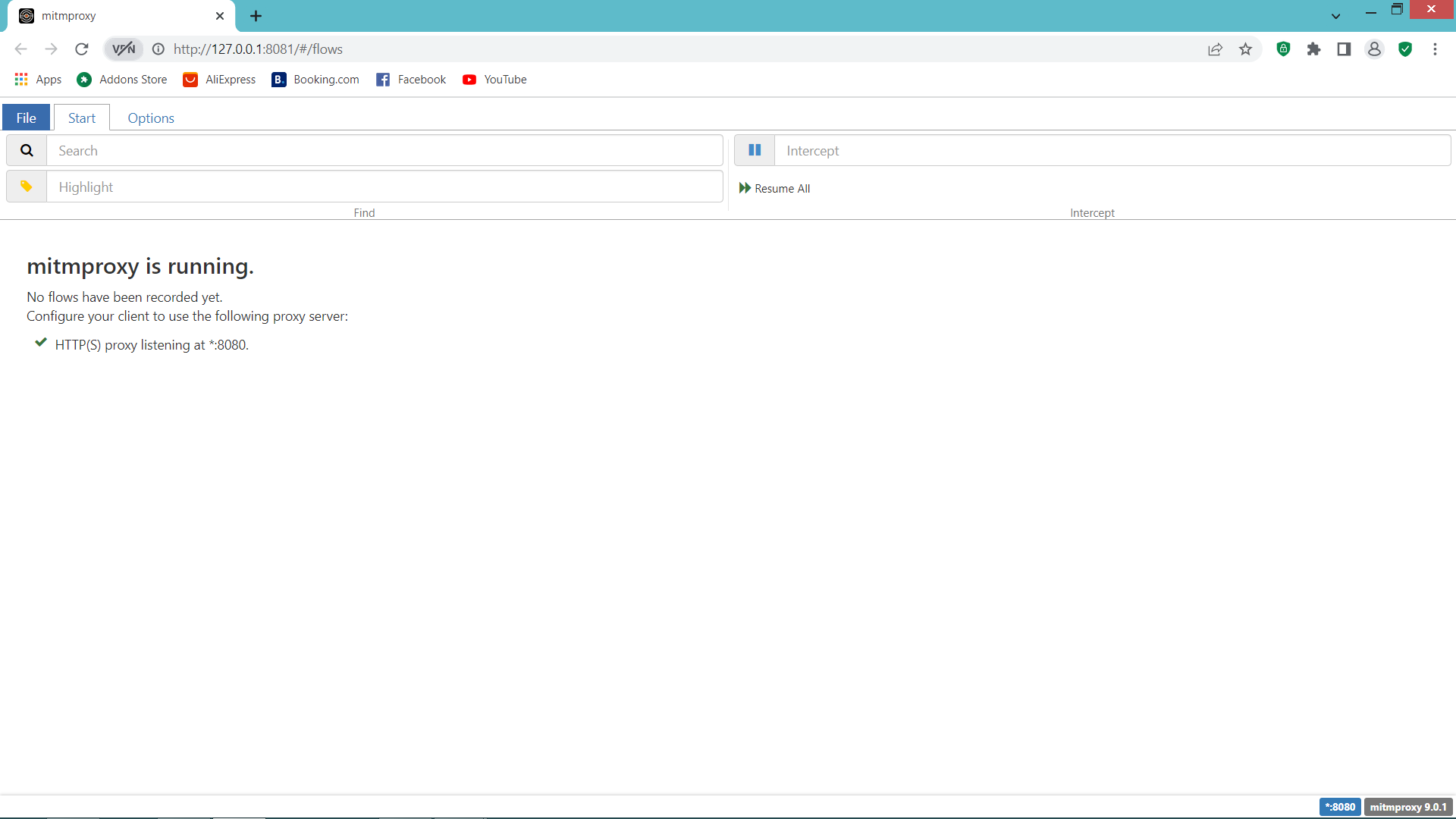


Figura 3 – mitmproxy em execução. Fonte: Autor.

O software embarca um servidor Web que roda na porta 8081 e o proxy roda na porta 8080, conforme mensagem mostrada. Para configurar o dispositivo para acessar a Web via mitmproxy, precisamos, além da porta, do endereço IP na rede local. Abaixo, o resultado da execução do ipconfig, que mostra o endereço IP local 192.168.0.12 e o gateway padrão 192.168.0.1, que é o roteador exposto na rede do provedor de Internet.

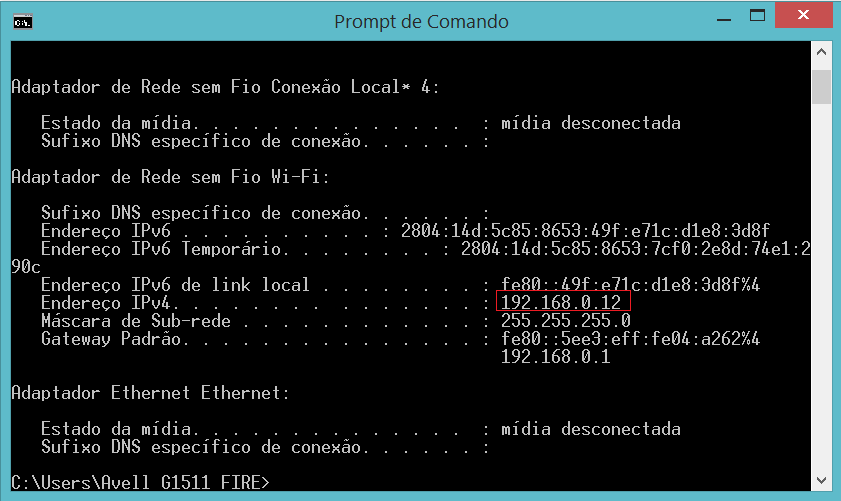


Figura 4 – Endereço local. Fonte: Autor.

Os dispositivos utilizados para os testes devem também estar conectados a esse roteador para que seja possível configurar, no telefone celular por exemplo, um proxy manual apontando para o endereço do *mitmproxy*. Portanto, o próximo passo é configurar o servidor proxy no dispositivo de teste. Em um Android 10+, procure pelas configurações da rede à qual está conectado e altere proxy para “Manual” e indique o endereço do servidor proxy; no exemplo, 192.168.0.12.

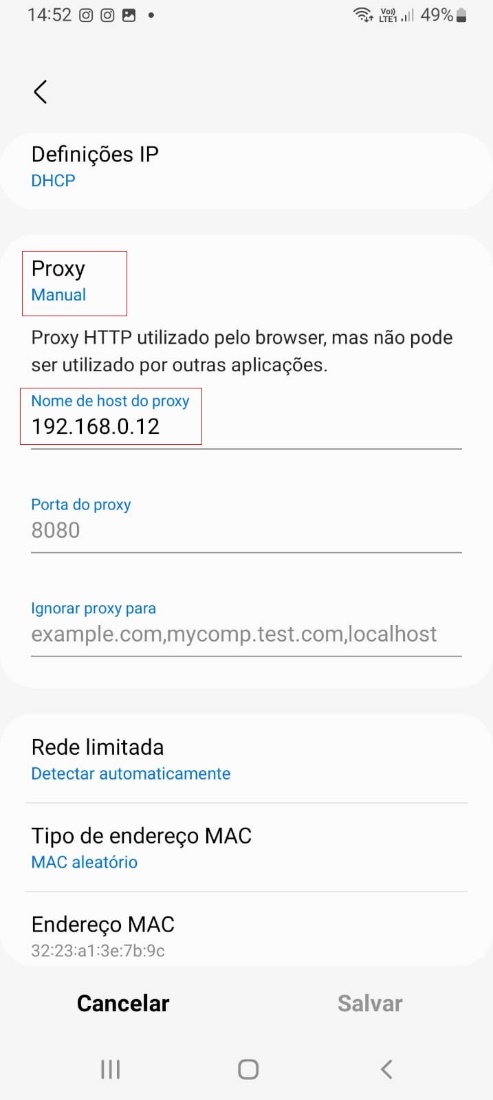


Figura 5 – Configuração do Proxy. Fonte: Autor.

Com essa configfuração realiza, o mitmweb já comneça a mostrar todas as mensagens HTTP enviadas a partir do dispositivo para a Internet.

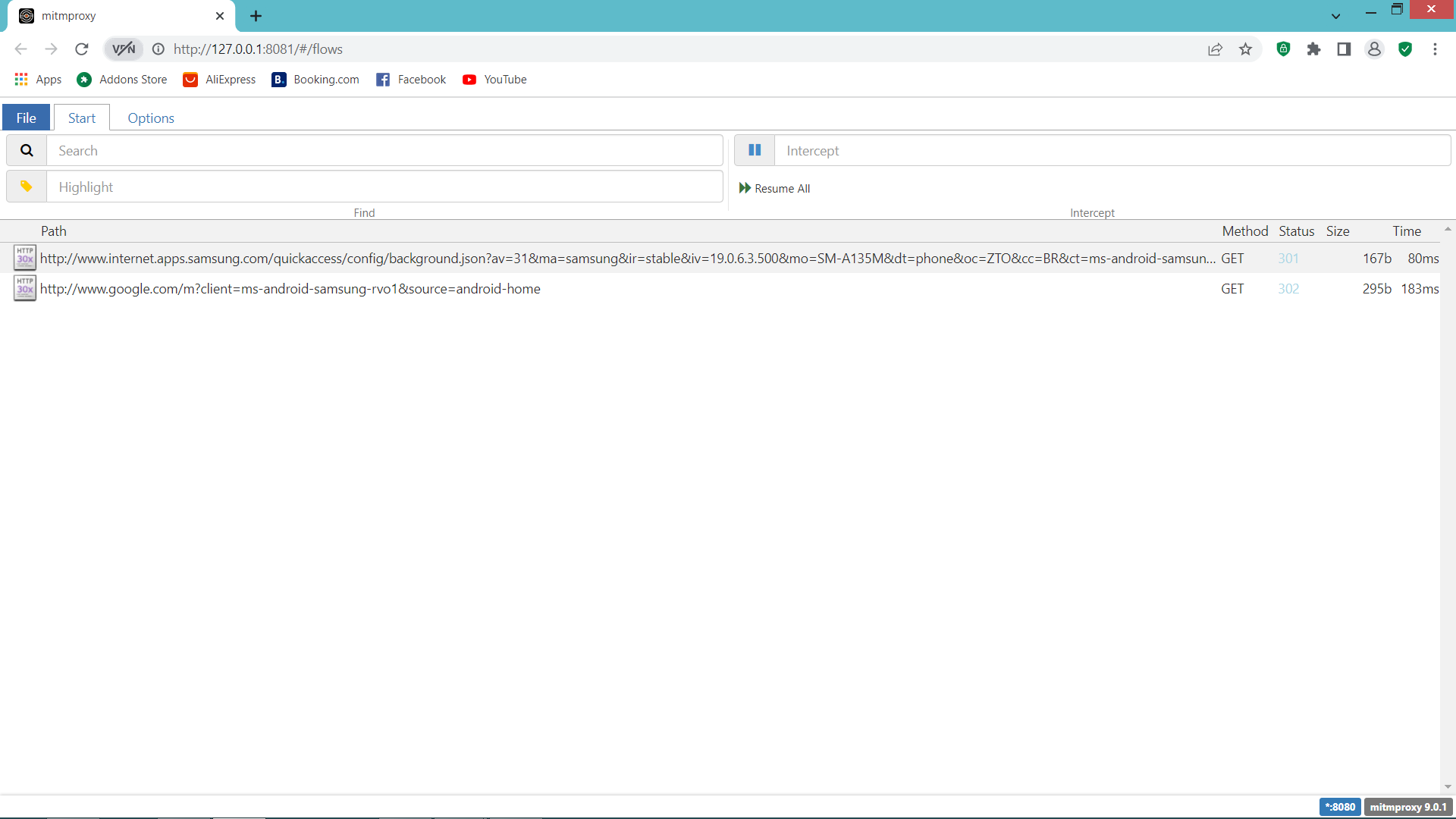
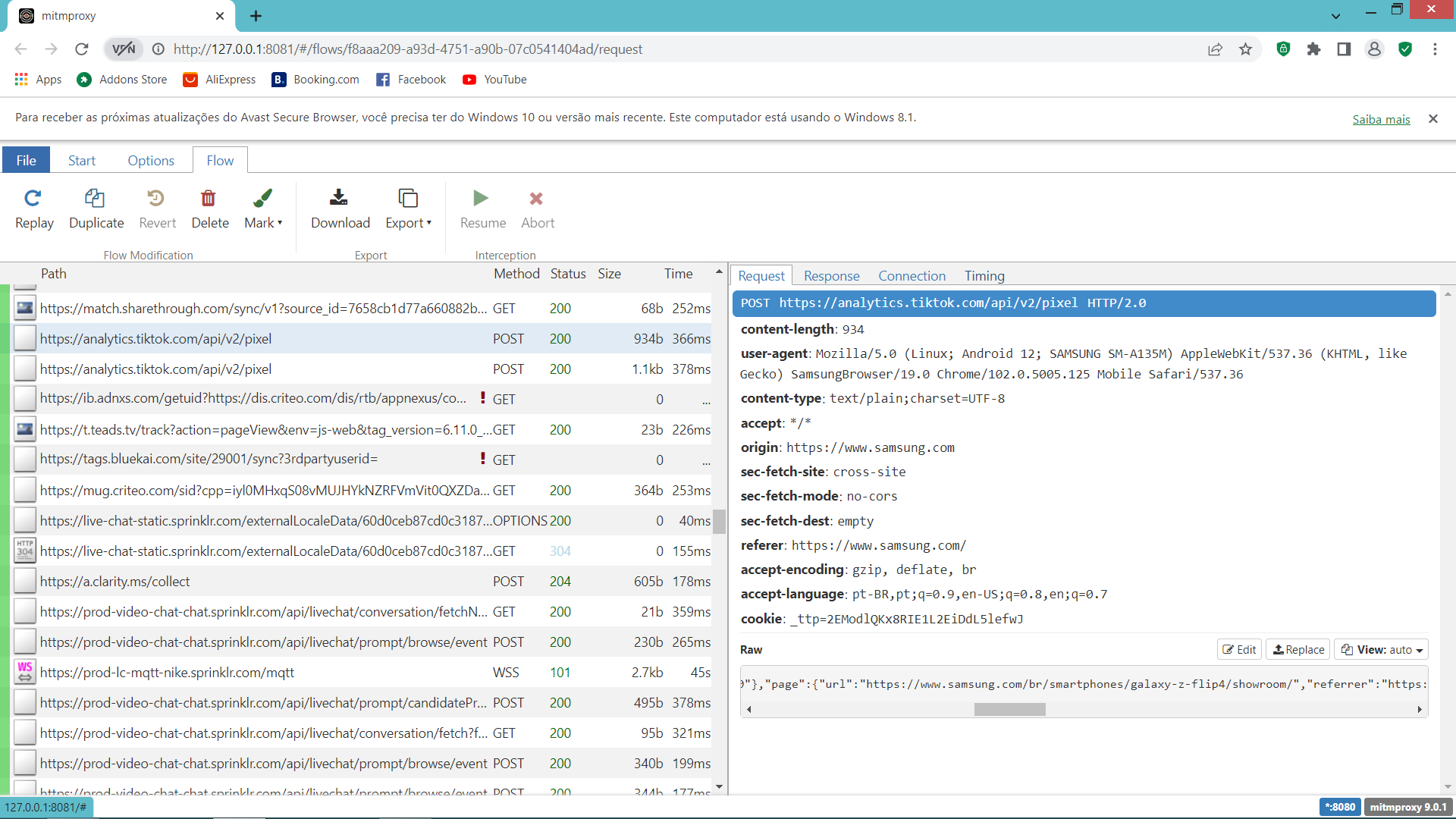


Figura 6 – Captura de mensagens HTTP. Fonte: Autor.

Fato é que as comunicações HTTPS não podem ser capturadas porque o dispositivo não possui o certificado do servidor instalado. Assim, após baixar o certificado em <http://mitm.it>, abrir o arquivo CER baixado, nomear e configurar *credential use* com “VPN and apps”. Assim, quando uma conexão do smartphone para o Google é estabelecido via TLS, mitmproxy encaminha a solicitação ao Google, mas, ao invés do certificado do Google, retorna o seu certificado autoassinado para o smartphone. Isso permite a mitmproxy capturar os dados em *plain text*. O proxy se comporta em de forma transparente e os servidores do Google não conseguem distinguir entre a comunicação com o smartphone e com o proxy.

Algumas distribuições Android requerem que os certificados sejam instalados via Settings >> Security >> Advanced >> Encryption e Credentials >> Install a certificate >> CA certificate. Ademais, aplicações que utilizam a API Android nível 24 (disponibilizada em 2016) ou superior somente aceitam certificados da *System Trusted Store* (#2054). Certificados adicionados pelo usuário não são aceitos a menos que a aplicação possa ser configurada para isso. Exceto para navegadores, aplicações devem ser configuradas em *Android Network Security Config*.

Uma vez que o certificado esteja instalado no dispositivo, as mensagens enviadas com protocolo HTTPS serão capturadas pelo mitmproxy.



Na mensagem acima, podemos ver claramente um serviço em *tiktok.com* recebendo uma mensagem enviada do celular contendo a URL *samsung.com* acessada pelo usuário. De fato, durante a sessão capturada, todas as URLs acessadas foram “informadas” ao *tiktok.com* através do mesmo serviço.

Bem, o que queremos a partir daqui? Queremos provar que dados pessoais são “informados” a serviços hospedados na Web. Mas, o que são dados pessoais?

**Referências**

[1] MITMPROXY. <https://mitmproxy.org/>

[2] MITMPROXY Documentation. <https://docs.mitmproxy.org/stable/>

[3] <https://lucaslegname.github.io/mitmproxy/2020/04/10/mitmproxy.html>