Week 4 — Alexa Skill Traffic Capture Report

Environment: Android emulator routed through mitmproxy; certificate installed.

2025-08-11 02:53

Setup and Method

Traffic was captured by routing the mobile device through mitmproxy/mitmweb on the host machine. On the Android emulator, Wi-Fi proxy was set to the host (10.0.2.2) on port 8080, and the mitmproxy CA certificate was installed via http://mitm.it so HTTPS traffic could be inspected. For each skill we enabled/used it in the Alexa app, then captured the resulting flows, applied simple filters to surface interesting requests (OAuth, possible PII, media), and exported HAR files when applicable.

Filter expressions used in mitmweb

- ~u token|session|answer|choice|name|email|zip|postal|i

- ~u oauth|authorize|token|client_id|redirect_uri|code=|state=|signin|mfa|i

- ~d meethue|signify|hue|account.meethue|auth.meethue|amazon.com|i

- ~u \.m3u8|\.ts|\.mp3|\.(m4a|aac)

Sleep Sounds (Sleep Jar)

Ambient sound skill that streams looping audio (e.g., ocean). Traffic shows an HLS playlist (.m3u8) and segment (.ts) files fetched from a CDN.

How it was invoked

- Enabled skill in Alexa app; invoked: "open sleep sounds" / chose "ocean".

Key endpoints observed

- cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean.m3u8

- .../ocean0.ts, .../ocean1.ts, ... (segment fetch pattern)

Potentially sensitive parameters / notes

- No tokens or PII in requests. Streaming media only; safe to capture.

Screenshots

Path	Method	Status	Size	Time
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean.m3u8?src=alexa&src_request_id=amzn1.echo-api.request.c7bab921-76ec-48db-8e2b-0b0a01781530	GET	200	1.9kb	30ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean0.ts	GET	200	890.8kb	213ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean1.ts	GET	200	890.2kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean2.ts	GET	200	891.0kb	190ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean3.ts	GET	200	890.4kb	1 ↻
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean4.ts	GET	200	890.1kb	192ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean5.ts	GET	200	891.2kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean6.ts	GET	200	890.1kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean7.ts	GET	200	890.4kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean8.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean9.ts	GET	200	890.6kb	187ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean10.ts	GET	200	890.2kb	189ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean11.ts	GET	200	890.4kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean12.ts	GET	200	890.6kb	188ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean13.ts	GET	200	890.6kb	198ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean14.ts	GET	200	890.4kb	192ms

sleep_soundspic.png

Path	Method	Status	Size	Time
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean14.ts	GET	200	890.4kb	192ms
https://cdn.sleepjar.com/sleepsounds/v6/sd/3600/m3u8/ocean/ocean15.ts	GET	200	890.4kb	190ms

showhost | *:8080 | mitmproxy 12.1.

sleep_soundspic2.png

Question of the Day (Matchbox)

Trivia Q&A skill. We enabled it, opened the skill, asked to repeat the question, then answered.

How it was invoked

• "open question of the day"

• "repeat the question"

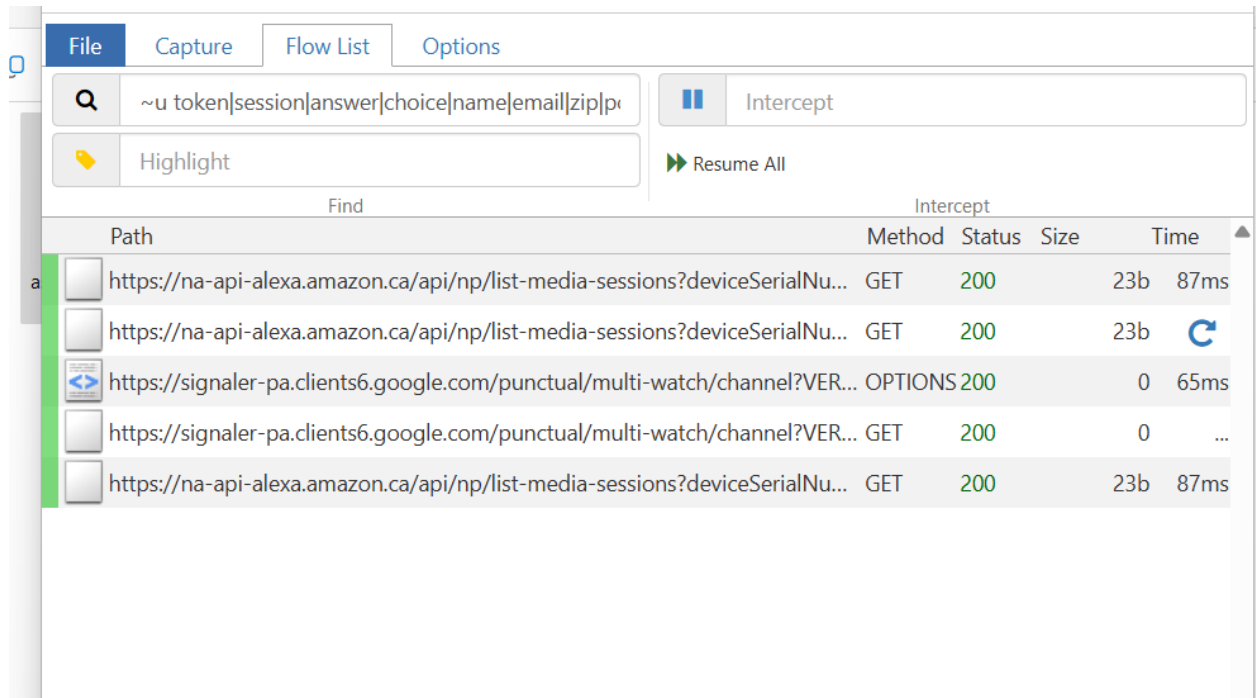• "the answer is A"

• "stop"

Key endpoints observed

• na-api-alexa.amazon.ca/api/np/list-media-sessions (Alexa app background polling)

• signaler-pa.clients6.google.com/punctual/multi-watch/channel

Potentially sensitive parameters / notes

• No observable PII; normal app polling and signaling traffic. Media endpoints may vary by region.

Screenshots

qotd.png

Cat Facts

Simple fact skill; responses are spoken by Alexa. Capture indicates standard Alexa endpoints; no external OAuth or vendor API calls visible from the app during invocation.

How it was invoked

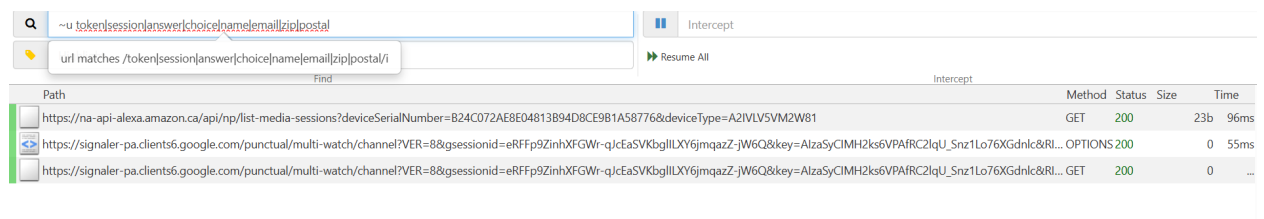• "open cat facts"

• listened to a few facts; then "stop"

Key endpoints observed

• na-api-alexa.amazon.ca/api/np/list-media-sessions

• signaler-pa.clients6.google.com/punctual/multi-watch/channel

Potentially sensitive parameters / notes

• No tokens nor personal data observed in URLs.

Screenshots

cat_facts.png

Ask My Buddy (Account Linking)

This skill requires account linking (OAuth). The Alexa app opens a webview to the vendor's site to sign in/authorize, then redirects back to Amazon to complete linking.

How it was invoked

• Enabled "Ask My Buddy" → proceeded to link account inside the Alexa app.

Key endpoints observed

• pitangui.amazon.com/api/v1/accountLink/validate?... (Amazon linking endpoint)

• askmybuddy.net/loginSystem/loginNew_Boe... (vendor login)

• Google Analytics beacons from the embedded webview

Potentially sensitive parameters / notes

• Observed OAuth redirection chain (302s) between Amazon and askmybuddy.net.

• Parameters included client_id, redirect_uri, and state (expected for OAuth). No raw credentials captured.

Screenshots

askbuddy skill.png

Philips Hue

Requires account linking to Hue. The Alexa app opens the Hue sign-in page and the flow completes via OAuth2 (PKCE), with redirects between Amazon and meethue domains.

How it was invoked

• Enabled "Philips Hue" → started account linking and followed prompts in the webview.
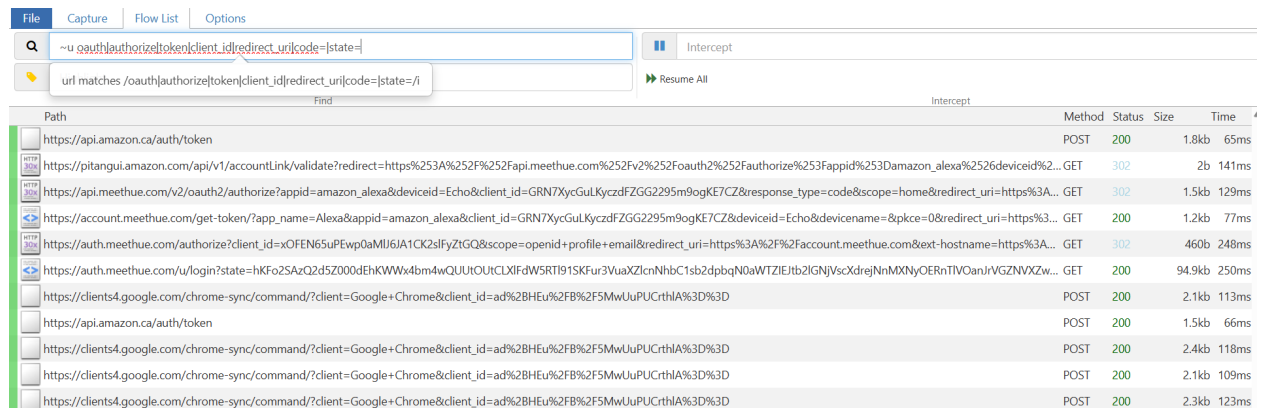
Key endpoints observed

• api.meethue.com/v2/oauth2/authorize?...response_type=code&...

• account.meethue.com/get-token?app_name=Alexa&appid=amazon_alexa

• auth.meethue.com/authorize?...client_id=...&redirect_uri=...

• na-api-alexa.amazon.com/... (linking callback)

Potentially sensitive parameters / notes

• OAuth parameters observed: client_id, redirect_uri, code, state; PKCE values are transient.

• No password values appear in URL; login forms are POSTed over TLS inside the webview.

Screenshots

philips_hue1.png

philips_hue_oauth2.png

philips_hue_oauth3.png

Artifacts saved

• sleep_sounds.har (available locally from capture session)

• qotd.har (available locally from capture session)

• cat_facts.har (available locally from capture session)

• ask_buddy_oauth.har (available locally from capture session)

Findings Summary

All five skills were exercised successfully through the proxied emulator with the mitmproxy certificate installed. For content skills (Sleep Sounds, Cat Facts, Question of the Day), traffic is primarily to Amazon Alexa APIs and CDNs (for audio playlists/segments); no personal data was found in request URLs. For account-linking skills (Ask My Buddy and Philips Hue), standard OAuth flows were observed. We saw expected parameters like client_id,

redirect_uri, state, and (post-authorization) short-lived authorization codes. No user passwords or tokens were visible in URLs; those are submitted via HTTPS forms. Overall, captures look consistent with normal operation and do not expose PII in URL query strings.