

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

 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

[show host](#) [*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”

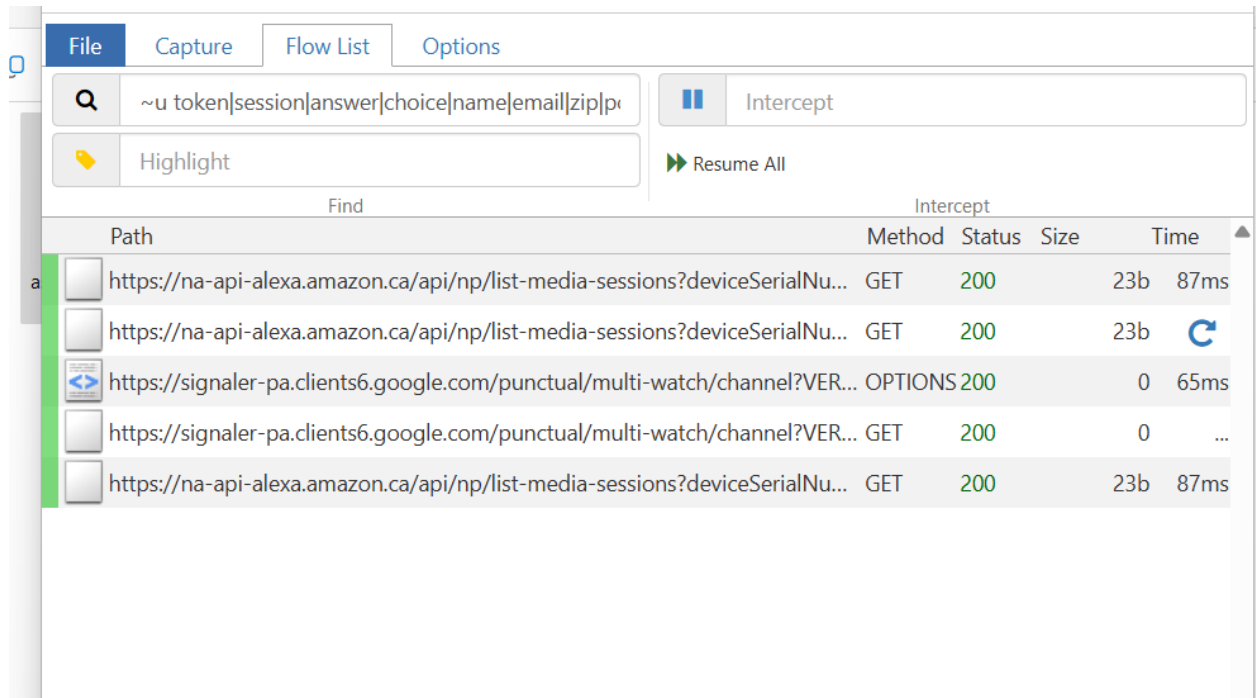
Key endpoints observed

- 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”

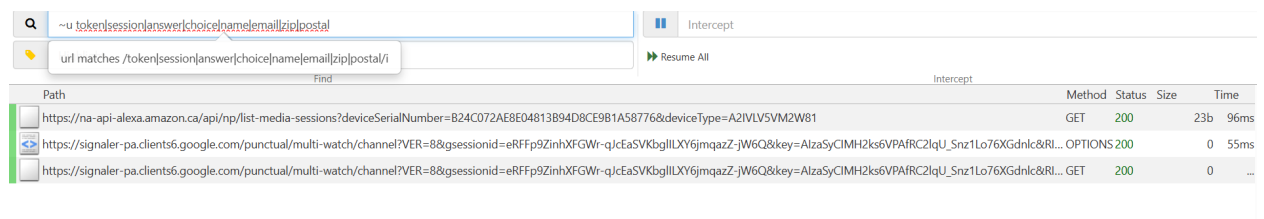
Key endpoints observed

- na-api-alex.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

	https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPU...	POST	200	2.3kb	151ms
	https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fwww.askmybuddy.net%252...	GET	302	2b	130ms
	https://www.askmybuddy.net/loginSystem/loginNew_Boee.php?client_id=amzn1.application-oa2-client.b198fa73acff4d6...	GET	200	17.3kb	81ms
	https://www.google-analytics.com/j/collect?v=1&_v=j102&a=268351649&t=pageview&_s=1&dl=https%3A%2F%2Fwww...POST	POST	200	15b	60ms
	https://www.google-analytics.com/q/collect?v=2&tid=G-SHVCDKQ9XP&qtm=45je5861v9136065518za200& p=1754878...POST	POST	204	0	48ms

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.

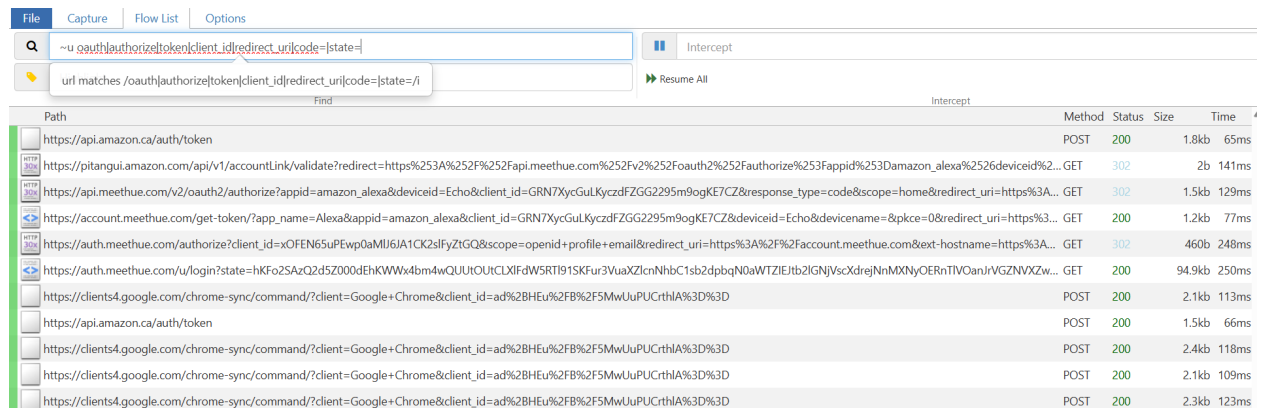
Key endpoints observed

- `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



Path	Method	Status	Size	Time
https://api.amazon.ca/auth/token	POST	200	1.8kb	65ms
https://pitanguia.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fapi.meethue.com%252Fv2%252Foauth2%252Fauthorize%253Fappid%253Damazon_alexa%2526deviceid%2...	GET	302	2b	141ms
https://api.meethue.com/v2/oauth2/authorize?appid=amazon_alexa&deviceid=Echo&client_id=GRN7XycGuLkyczdfZGG2295m9ogKE7CZ8&response_type=code&scope=home&redirect_uri=https%3A...	GET	302	1.5kb	129ms
https://account.meethue.com/get-token/?app_name=Alexa&appid=amazon_alexa&client_id=GRN7XycGuLkyczdfZGG2295m9ogKE7CZ8&deviceid=Echo&devicename=8pkce=08&redirect_uri=https%3A...	GET	200	1.2kb	77ms
https://auth.meethue.com/authorize?client_id=xOFEN65uPEwp0aMIU6IA1CK2sIFyZtGQ&scope=openid+profile+email&redirect_uri=https%3A%2F%2Faccount.meethue.com&text-hostname=https%3A...	GET	302	460b	248ms
https://auth.meethue.com/u/login?state=hKFo25AzQ2d5200dEhKWWx4bm4wQUiOUtCLXIFdW5RTl91SKFur3VuaXZlcnNhbc1sb2dpbqN0aWTZlEtbt2lGNjVscXdrejNnMXNyOERnTlVOanRlVGZNVXZw...	GET	200	94.9kb	250ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthIA%3D%3D	POST	200	2.1kb	113ms
https://api.amazon.ca/auth/token	POST	200	1.5kb	66ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthIA%3D%3D	POST	200	2.4kb	118ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthIA%3D%3D	POST	200	2.1kb	109ms
https://clients4.google.com/chrome-sync/command/?client=Google+Chrome&client_id=ad%2BHEu%2FB%2F5MwUuPUCrthIA%3D%3D	POST	200	2.3kb	123ms

philips_hue1.png

File Capture Flow List Options									
~d meethue:signifyhue:account:meethue:amazon.com:lap:/oai					Intercept				
domain matches /meethue:signifyhue:account:meethue:amazon.com:lap:/oai/					Resume All				
Path	Method	Status	Size	Time					
https://pitangui.amazon.com/api/v1/accountLink/validate?redirect=https%253A%252F%252Fapi.meethue.com%252Fv2%252Foauth2%252Fauthorize%253Fappid%253Damazon_alexa%2526deviceid%2...	GET	302	2b	141ms					
https://api.meethue.com/v2/oauth2/authorize?appid=amazon_alexa&deviceid=Echo&client_id=GRN7XycGuLkyczdFZGG2295m9ogKE7CZ&response_type=code&scope=home&redirect_uri=https%3A...	GET	302	1.5kb	129ms					
https://account.meethue.com/get-token/?app_name=Alexa&appid=amazon_alexa&client_id=GRN7XycGuLkyczdFZGG2295m9ogKE7CZ&deviceid=Echo&devicename=&pkce=0&redirect_uri=https%3...	GET	200	1.2kb	77ms					
https://account.meethue.com/manifest.json	GET	200	383b	33ms					
https://account.meethue.com/assets/index-ee134c6f.js	GET	200	299.7kb	193ms					
https://account.meethue.com/assets/vendor-45091bae.js	GET	200	412.3kb	245ms					
https://account.meethue.com/assets/style-c719184f.css	GET	200	10.0kb	36ms					
https://auth.meethue.com/authorize?client_id=xOFEN65uPEwp0aMIJ6A1CK2slFyZiGQ&scope=openid+profile+email&redirect_uri=https%3A%2F%2Faccount.meethue.com&ext-hostname=https%3A...	GET	302	460b	248ms					
https://auth.meethue.com/u/login?state=hKfo2SAzQ2d5Z000dEhKWWx4bm4wQUiH0UitCLXiFdw5RTI91SKFur3VuaXZlcnNhbc1sb2dpbqN0aWTZIEJtb2lGNjVscXdirejNnM0NyoERnTIV0anJrVGZNVXZw...	GET	200	94.9kb	250ms					
https://account.meethue.com/dd/api/v2/rum?ddsource=browser&ddtags=sdk_version%3A5.35.1%2Capip%3Abeacon%2Cenv%3Aprod%2Cservice%3Aheimdall-client%2Cversion%3A8.0.16767-g98873e...	POST	202	2.3kb	173ms					
https://www.philips-hue.com/content/experience-fragments/hue/nl/nl/navigation/header/master/_jcr_content/root/navigation_component/desktop.signifyimg.82.200.png/1608020231951.png	GET	302	0	440ms					
https://account.meethue.com/auth0/fonts/soehne-buch.woff2	GET	200	32.3kb	40ms					
https://account.meethue.com/auth0/hue-ambient-background.webp	GET	200	35.2kb	46ms					
https://www.philips-hue.com/	GET	302	0	132ms					
https://www.philips-hue.com/en-ca	GET	200	23.4kb	67ms					
https://avs-alexa-12-na.amazon.com/v20160207/ping	GET	404	45b	40ms					

philips_hue_oauth2.png

https://www.philips-hue.com/	GET	302	0	132ms
https://www.philips-hue.com/en-ca	GET	200	23.4kb	67ms
https://avs-alexa-12-na.amazon.com/v20160207/ping	GET	404	45b	40ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	42ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	2.0kb	41ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	48ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	2.0kb	48ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	74ms
https://fls-na.amazon.com/1/batch/1/OE/	POST	204	1.1kb	80ms

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.