“Alexa, are you Skynet?”

Jessica Hyde
Director of Forensics – Magnet Forensics
Adjunct Professor – George Mason University

Brian Moran
Digital Strategy Consultant – BriMor Labs

Not sure I believe her….

A Brief List of Topics

- Introduction
- Amazon Echo Hardware
- Alexa
- kasa
- Security issues
- Scripts to parse data?
- Questions/comments/etc.?

Jessica's Introductory Introduction

- Hello, my name is Jessica Hyde
  - Hi Jessica!
- 6+ years Marines - Active Duty
  - 13ish years mobile exploitation/engineering/DFIR experience
- FUN FACT: I don't run often, but I do run for Data Gen


I RUN FOR
DATA GEN

Brian's Introductory Introduction

- Hello, my name is Brian Moran
  - Hi Brian!
- 13+ years Air Force Active Duty
  - 14ish years mobile exploitation/DFIR experience
- FUN FACT: Was unable to get smooth jazz by Davey C on my test Amazon account


THE VERY
BEST OF
DAVEY
C

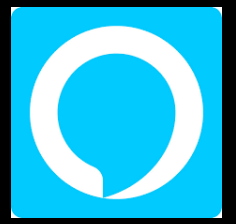
Devices Used For This Presentation

- Android phones
  - Galaxy S5
  - BLU R1 HD
- Amazon Echo devices
  - Echo Dot (Gen 1)
  - Echo Dots (Gen 2)
  - Echo (Gen 1)
  - Echo Show (Gen 1)

- Research on iOS phones & more Echo devices continues, because Amazon keeps making new ones!

App Versions Used For This Presentation

- Alexa (Android)
  - 1.24.2556.0



- Kasa (Android)
  - 1.9.1 Build 697

- REMEMBER: Data can slightly (or drastically!) change between app versions

How Did We Get Here?

- Adrian (@Cheeky4n6Monkey) tried very hard to win an Echo at SANS DFIRSummit in 2016 for chip off
  - Spurred some initial thoughts
- A smart bulb, controlled by Alexa, was the perfect fix for impending doom in my home
  - To turn off a lamp, had to stand on the couch, right in front of stairwell
- Wanted to generate data (and use) smart home devices for an extended period of time
  - Not just one week of test data

Obligatory Meme Capturing Research Mindset

Sources of Data

- Hardware
  - Amazon Echo
  - Amazon Echo Dot
  - Amazon Echo Show

Sources of Data

- Mobile Apps
  - Alexa
  - Kasa

Sources of Data

- Network
- Connected devices

Amazon Echo Devices

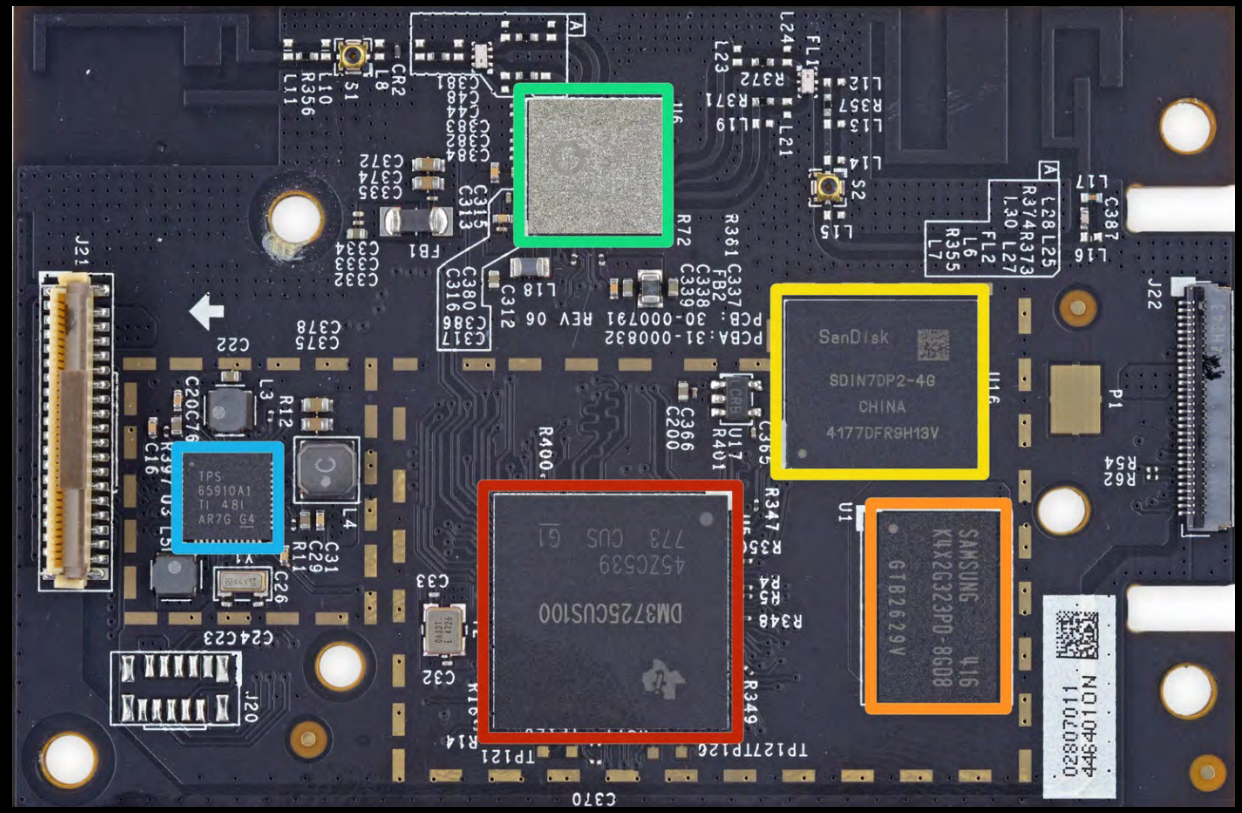
- How do you get to data on the device?
- Destructive vs. Non Destructive
- Ports
  - USB – root-able?
  - JTAG - no ports
  - ISP – eMMC – yes!
- What is the quickest way to see what is stored?
  - Chip-off followed by ISP

Amazon Echo

- Original Echo
- Disassembly
  - Well documented
- Device from WV
  - From an actual case
  - Compared to test device (from Teel Tech Canada)

Amazon Echo

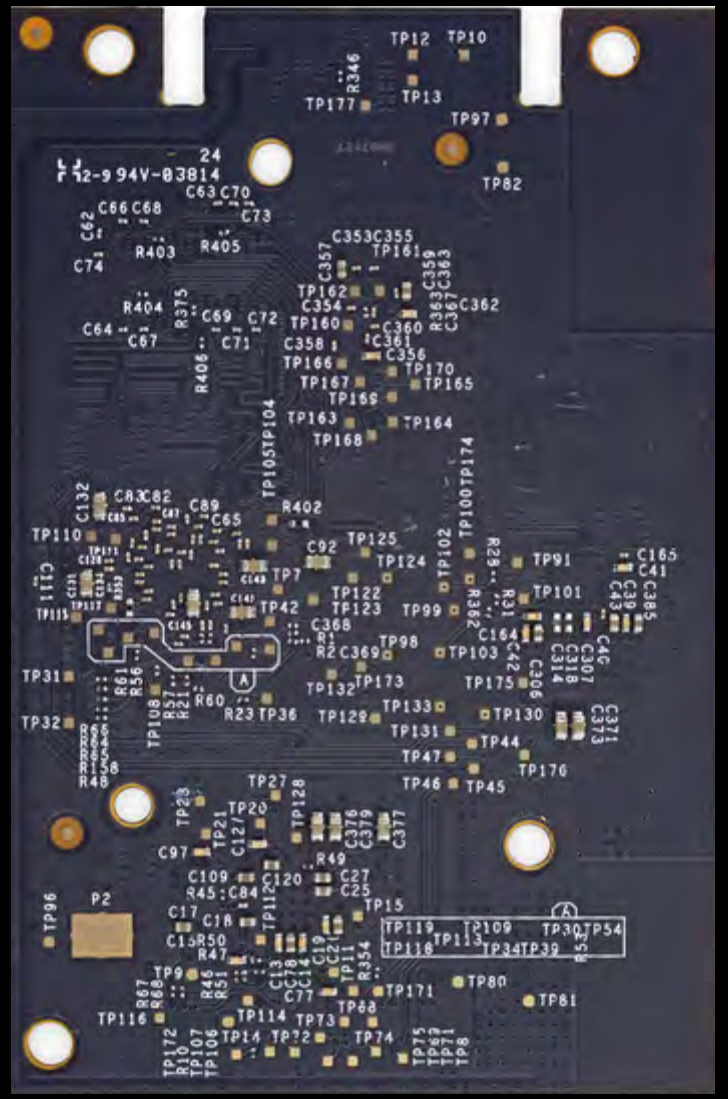
- Research
- Components
  - SanDisk SDIN7DP2-4G
    - 4GB iNAND Ultra Flash Memory
    - Documented



https://www.ifixit.com/Teardown/Amazon+Echo+Teardown/33953

Amazon Echo

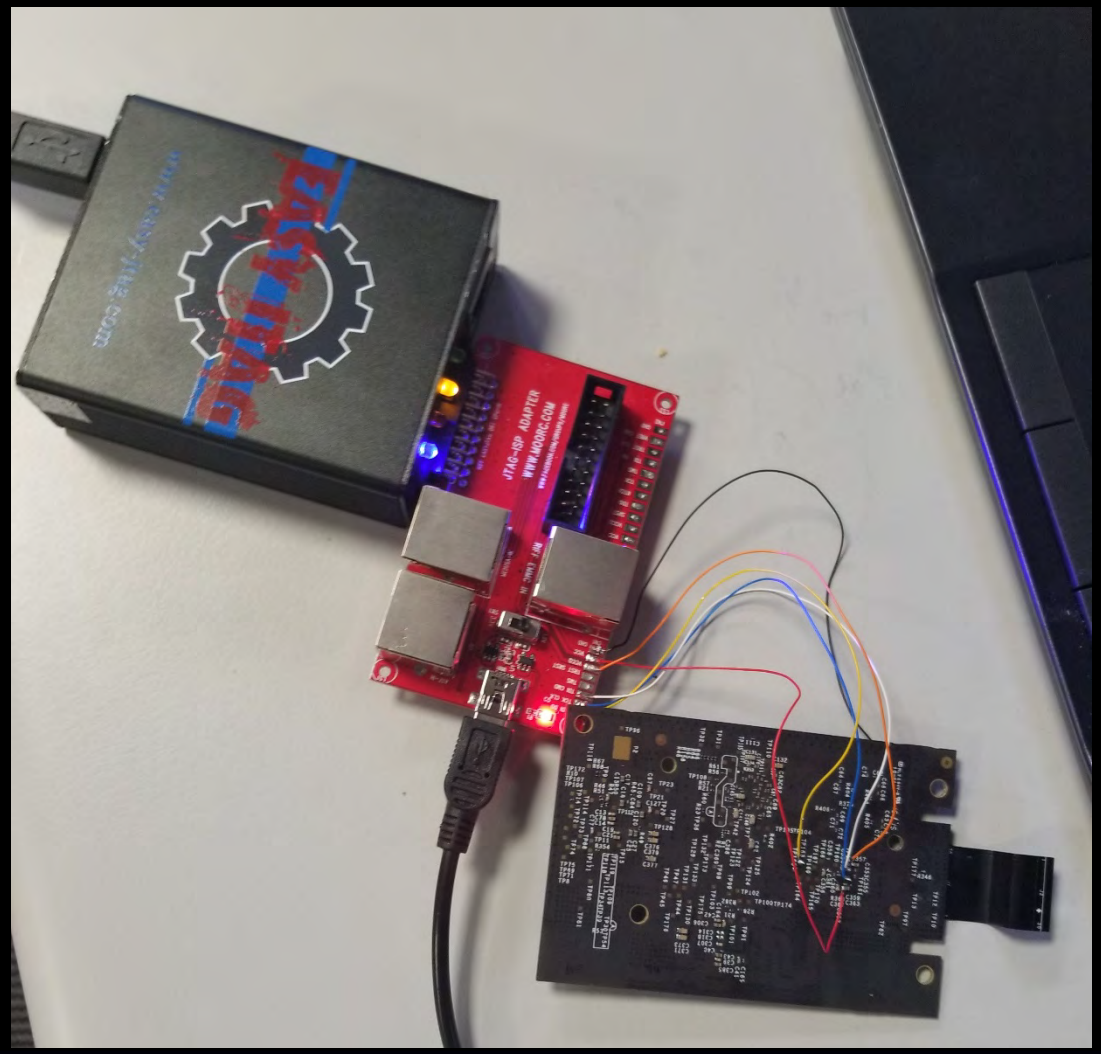
- ISP Pin out
  - VCC
  - VCCq
  - CMD
  - CLK
  - DAT0



Echo ISP Pinout

Amazon Echo

- Research pin out
- ISP using Z3X Easy JTAG Box

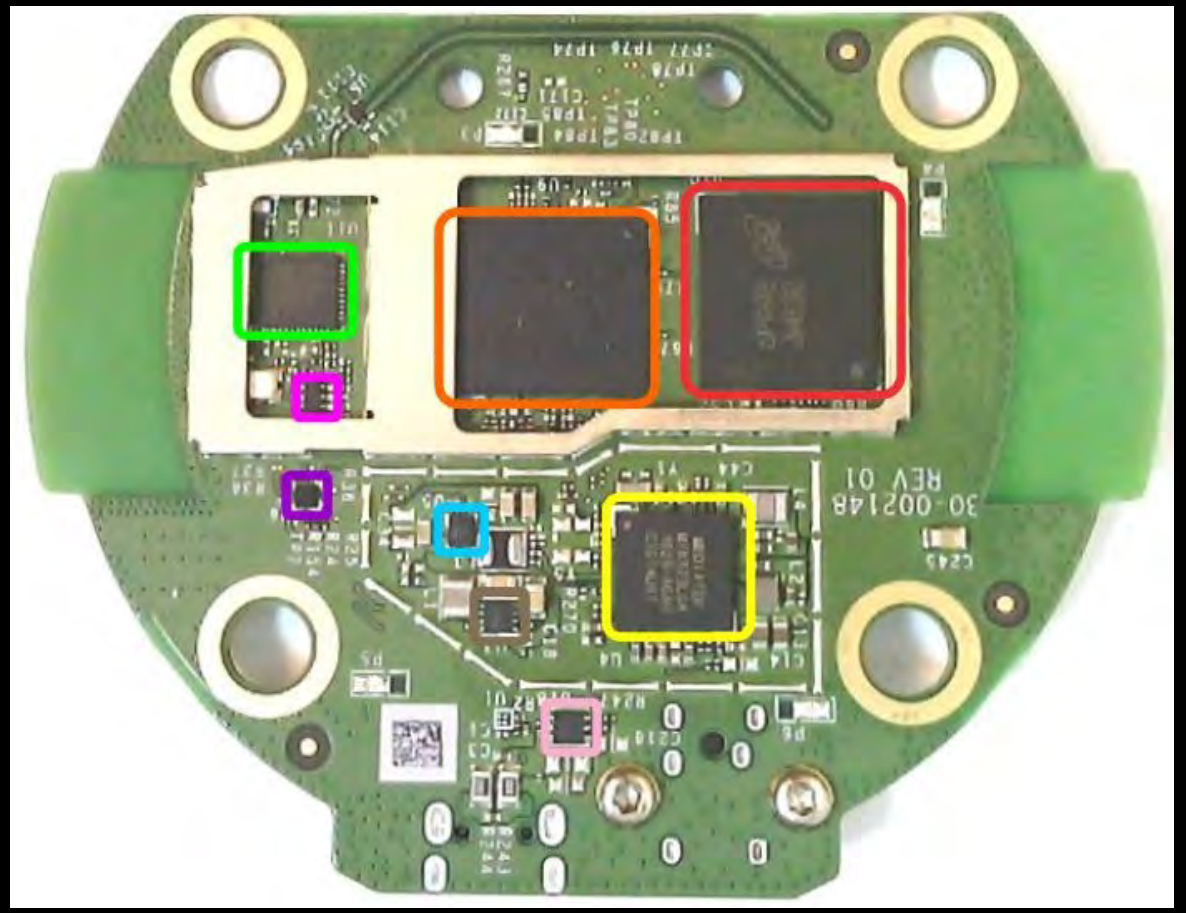


Amazon Echo Dot

- Echo Dot
- Disassembly
  - No Documentation
- Devices from Brian's smart home
  - One from test network
  - One from real use – 1 year
  - Compared to new OOB device

Amazon Echo Dot

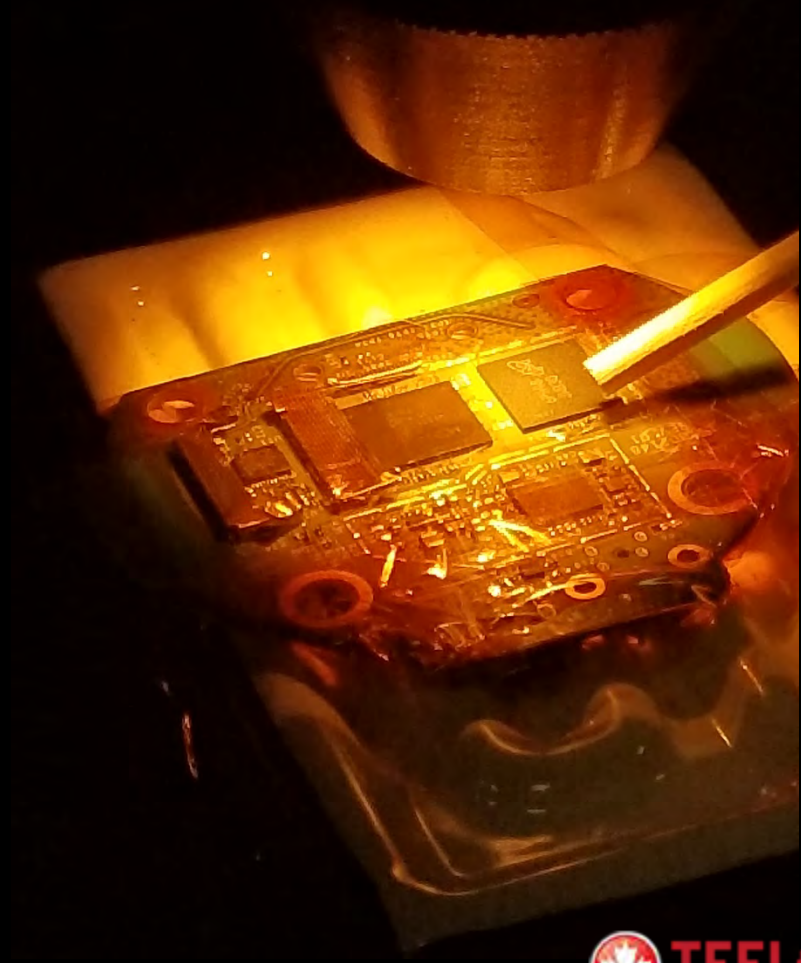
- Components
  - Different eMMC on each board
    - Micron 6PA98 JWB30
    - SEC 625
      B213
      KMF J2005A S4DCVA9VC
- Challenge
  - No Data Sheet
  - Assume eMMC



https://www.allaboutcircuits.com/news/teardown-tuesday-amazon-echo-dot-v2/

Amazon Echo Dot

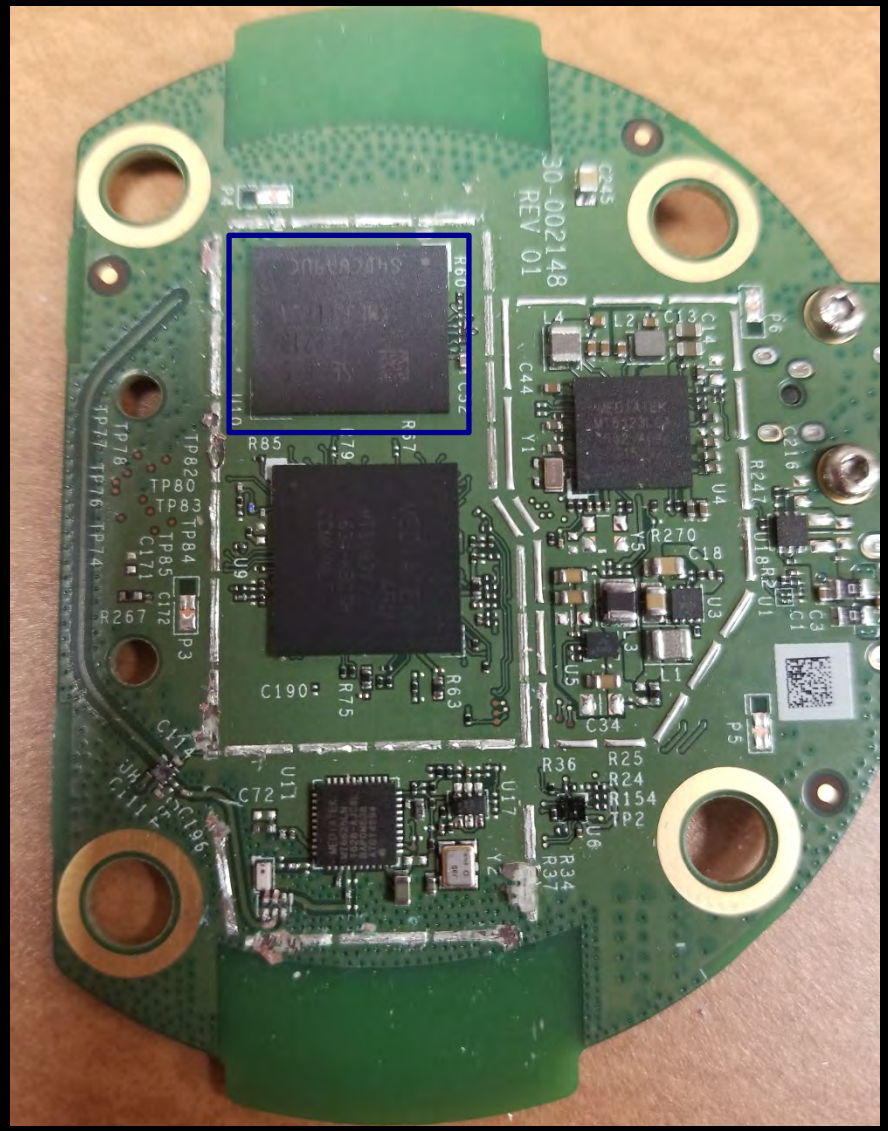
- Chip-off
  - New out-of-box
  - Used IR station
    - Thanks Teel Tech Canada
- Clean and Read chip
- Determine pinout by researching SD standard for BGA pattern



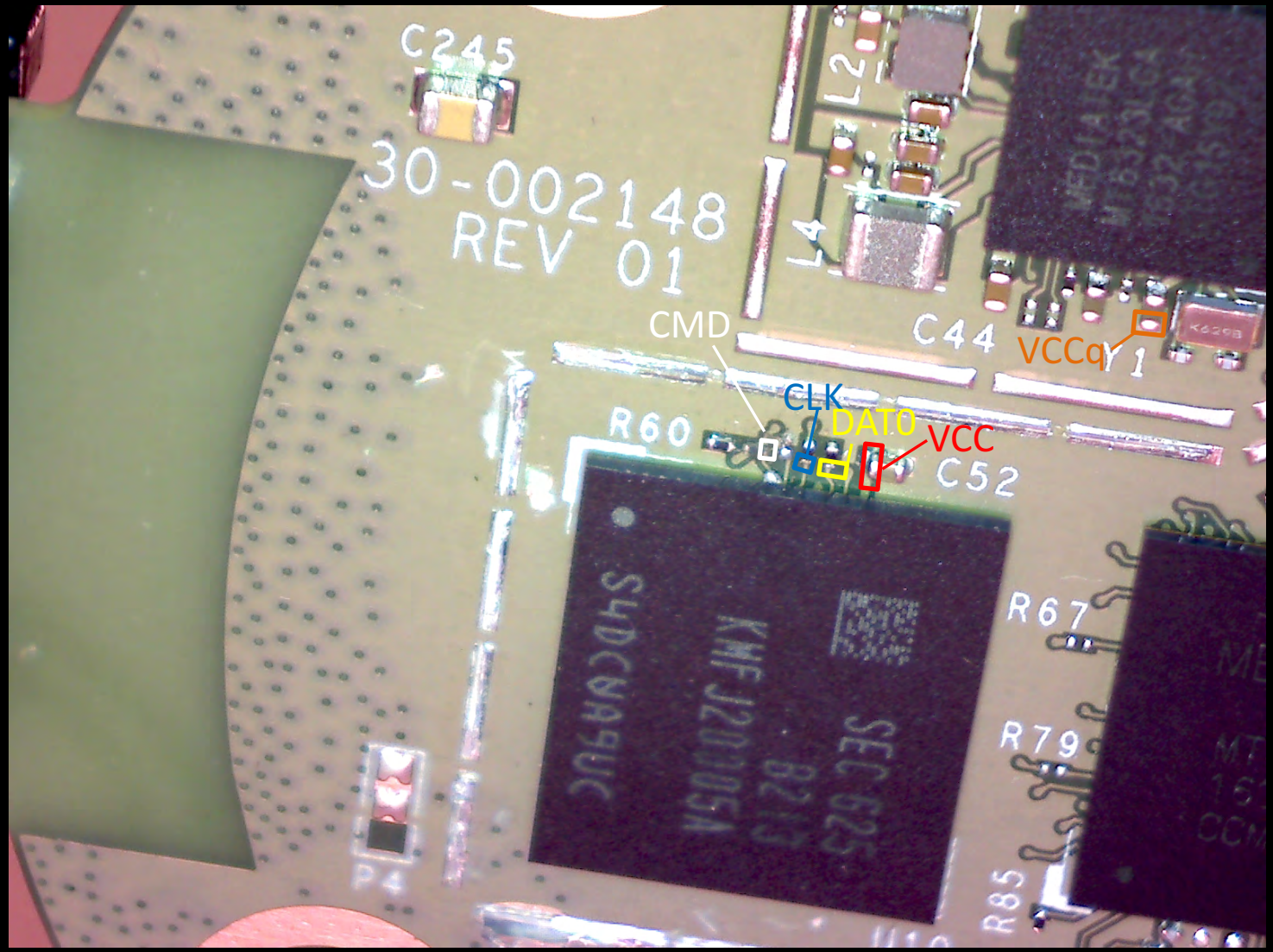
TEELtechnologies Canada

Amazon Echo

- ISP Pin out
  - VCC
  - VCCq
  - CMD
  - CLK
  - DAT0



Echo Dot ISP Pinout



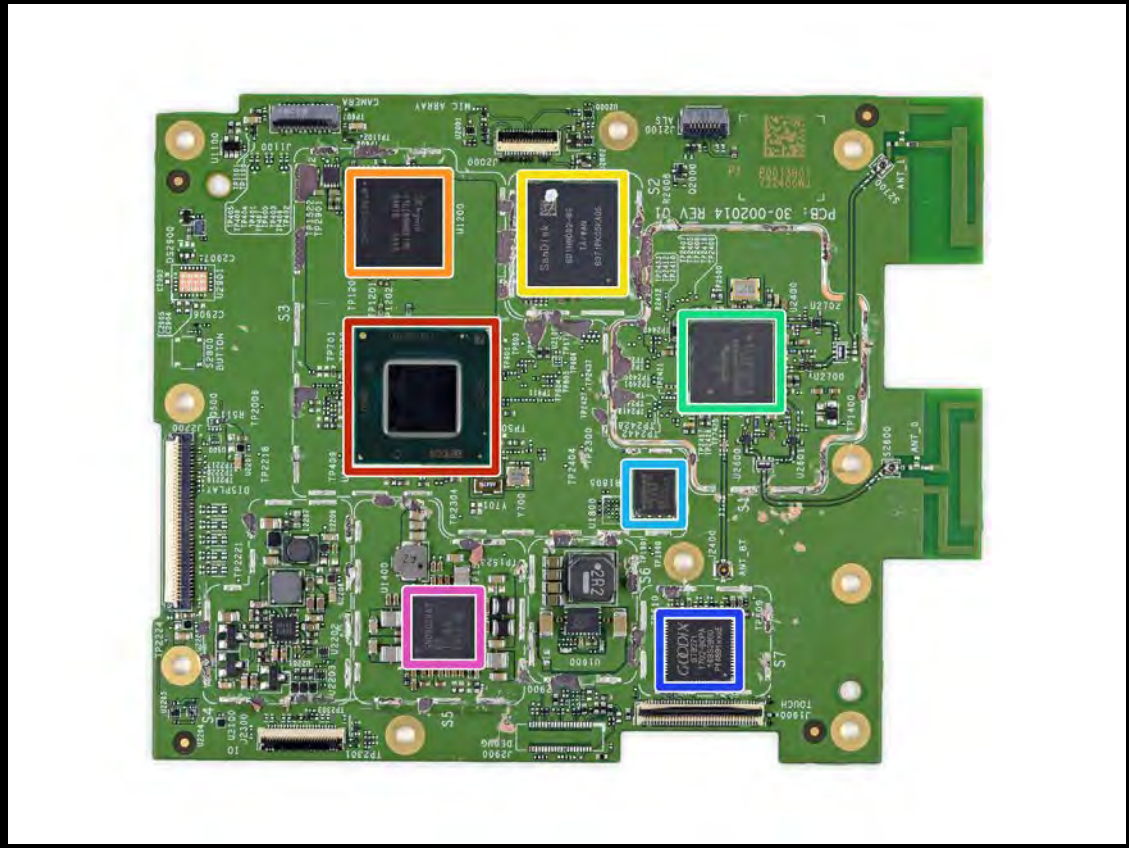
Amazon Echo Dot

- Image 4GB eMMC using RIFF2
- Huzzah – Non-destructive ISP method
- Apply ISP method to Brian's device (used 1 year)

https://www.riffbox.org/

Amazon Echo Show

- New June 2017
  - Thank you Amazon for the spare
- Disassembly
  - Well documented
  - 1 new in the box for pinout
  - 1 used for testing 3.5 months

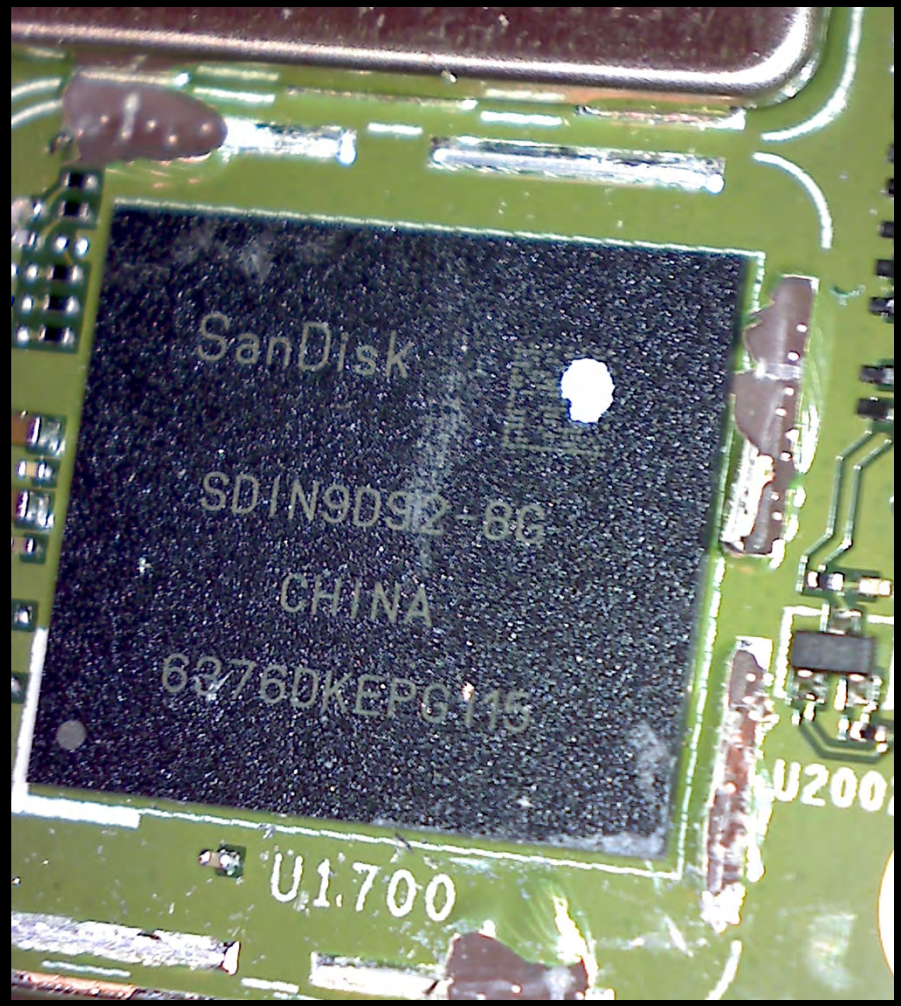


https://www.ifixit.com/Teardown/Amazon+Echo+Show+Teardown/94625

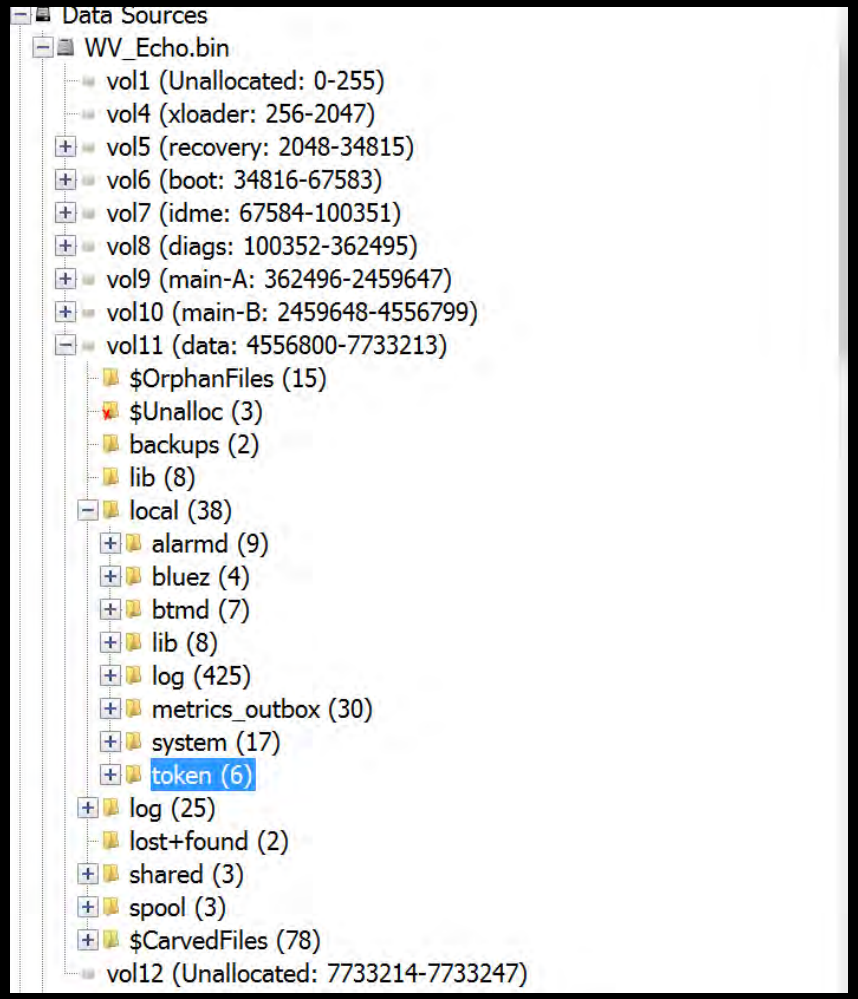
Amazon Echo Show

- Components
  - 8GB NAND Embedded Flash Drive

    Sandisk SDIN9D92-8G
- Challenge
  - No Data Sheet
  - Future Pinout



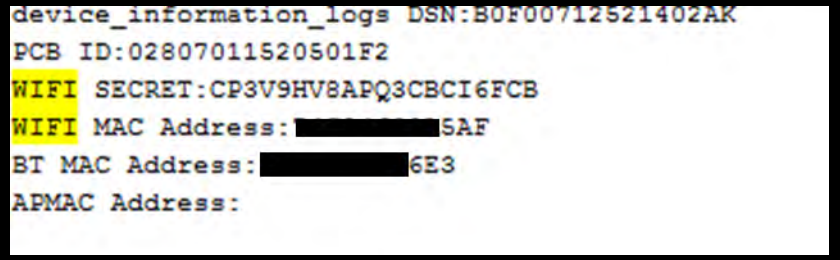
Amazon Echo Flash Dump



Amazon Echo Flash Memory

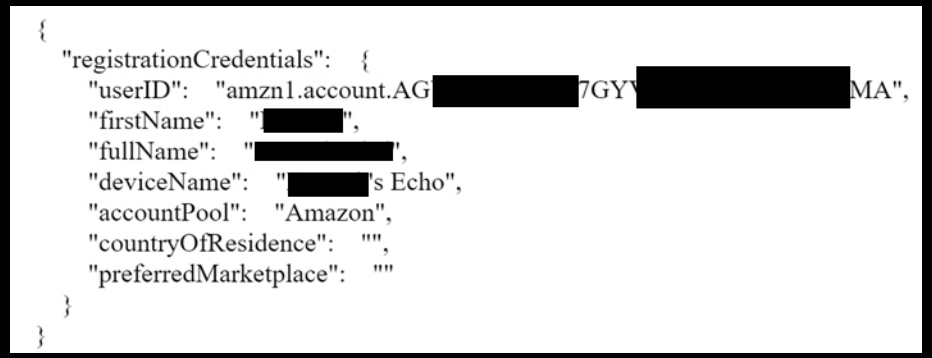
- What data can we find?
  - WiFi Connections

    device_information_logs



  - Registration Information

    data\local\token\registrationinfo.txt

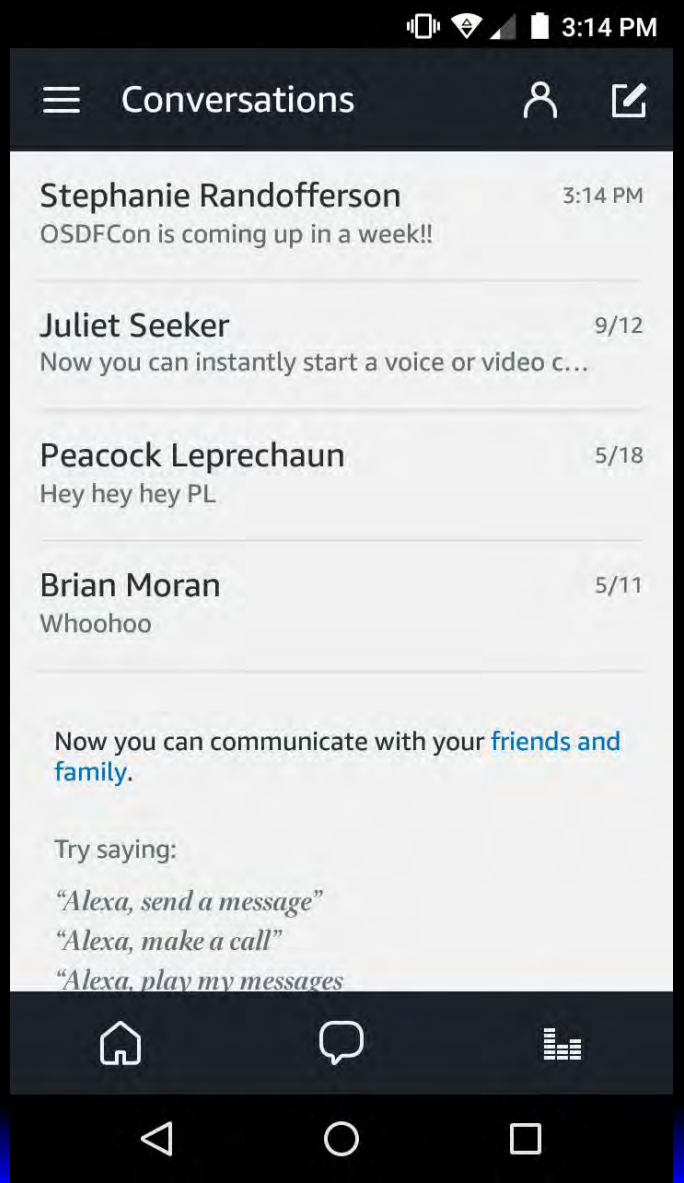


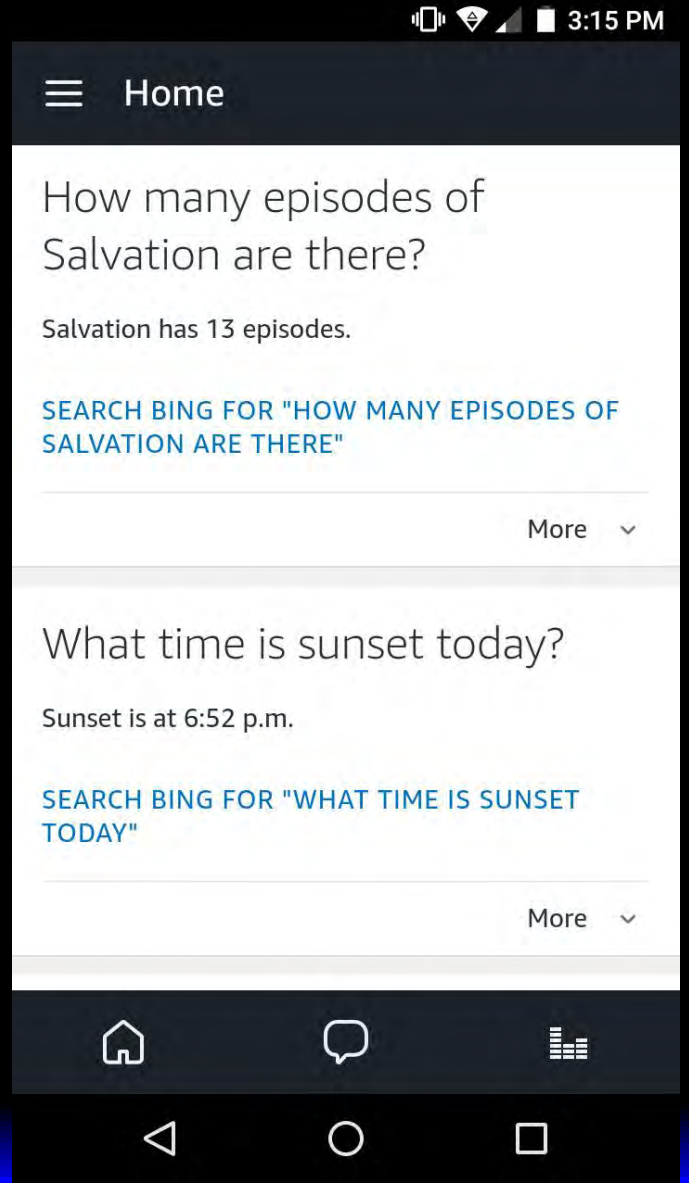
Alexa mobile application

- View your Echo devices (Dot, Echo Tap, Echo Show, etc)
- Control what's playing on an Echo device

- Message and call other Amazon Alexa application users
  - And Echo device owners

Alexa mobile application





Alexa mobile application

- Very little information is stored within the application itself, there have been numerous posts on the data that is stored, so we won't go over that
- Most of the data is pulled from URLs (more on that soon!)

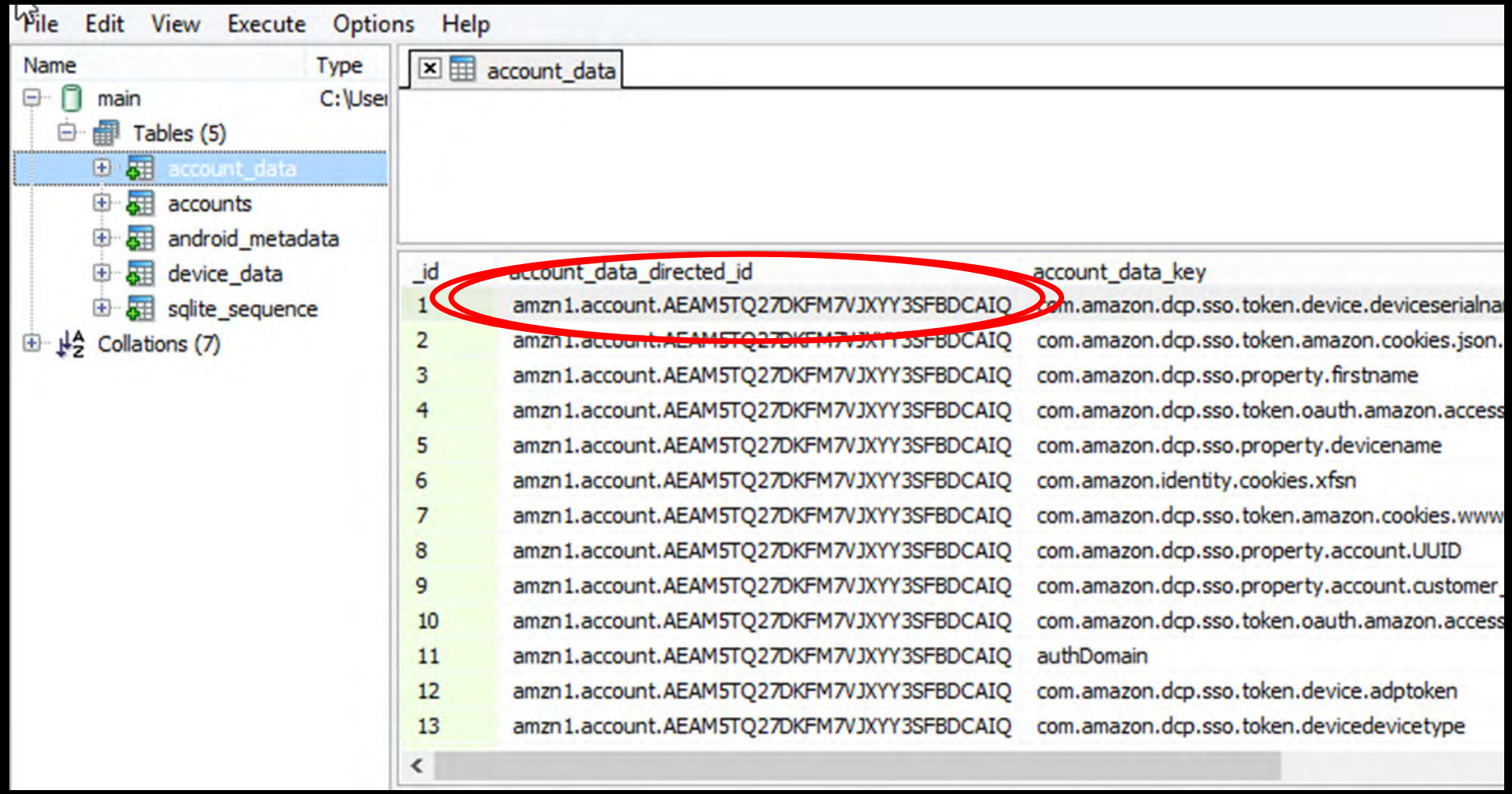
Alexa mobile application

- There is a file named “comms.db” stored in the Alexa application folder under the path
  - “data\com.amazon.dee.app\databases”
- One could wager this contains messages/messaging information
  - The data is encrypted, have not figured out the encryption/decryption yet
- Kudos to Amazon! (But we did find a work around!!)

Alexa mobile application

- One database file worth noting for later use is “map_data_storage_v2.db”, stored under the path “data\com.amazon.dee.app\databases”
- It was possible, in previous versions, to pull out authentication data & use that to access information. This is no longer the case as the data is now encrypted
  - This is why it is important to stay on top of new releases!
- The main thing we want from here is the Amazon account ID string

Alexa mobile application



Alexa mobile application

- But what if you only have a logical acquisition?
- Good news!! You can navigate to the path

“com.amazon.avod.thirdpartyclient\db\map_data_storage.db”

- Search for the “amzn1.account” string to find the customer ID

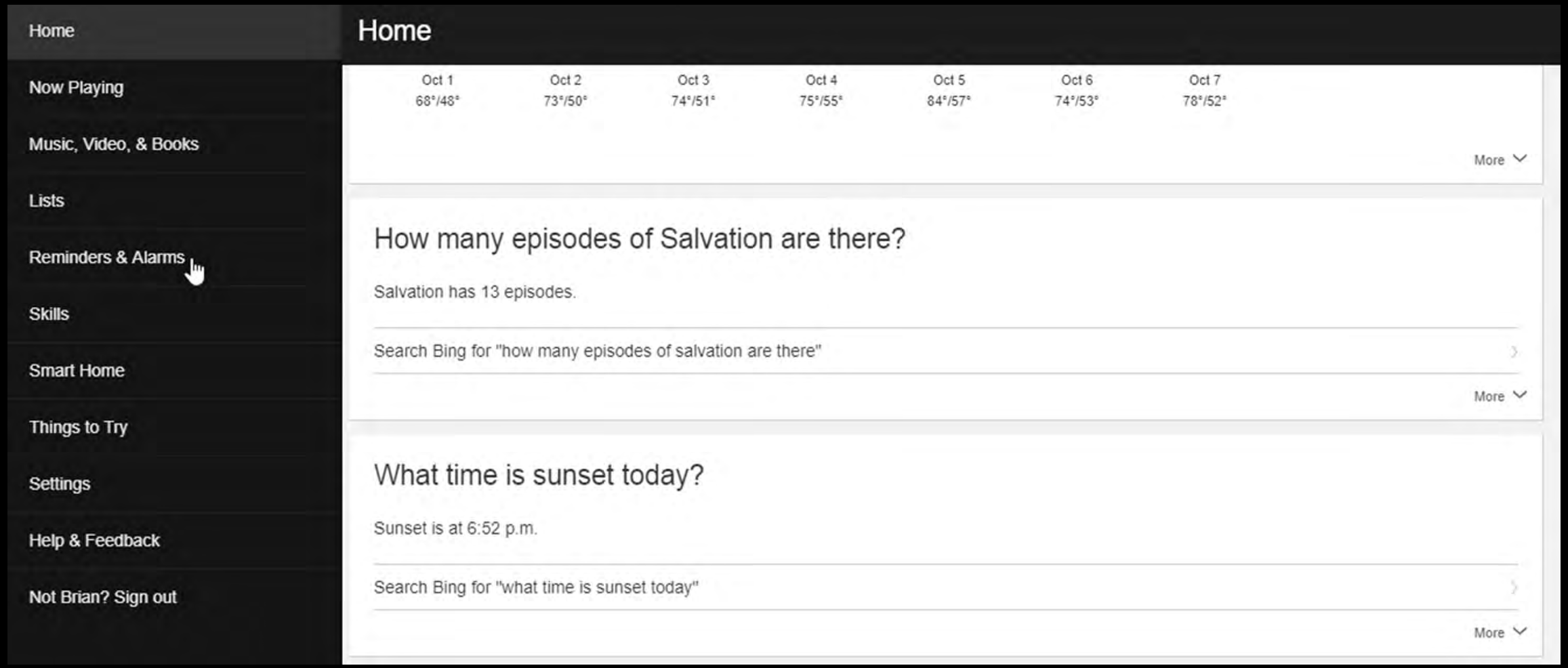
Alexa mobile application

- We be using this string shortly
  - “amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ”

Alexa web application

- Browse to the URL “http://alexa.amazon.com/”
  - Should be required to sign in to your Amazon account
- Even more options than the mobile app
  - But no messaging!

Alexa (viewed in browser)



Alexa applications (behind the GUI)

- Remember we said most of the data is pulled from URLs
  - One we will use a LOT is variations of “https://pitangui.amazon.com/api”
- In fact, if your investigation involves Amazon Echo/Alexa, most of your good information will come from here
  - HINT: One keyword should be “pitangui.amazon.com/api”
- You will need the email address & password for the Amazon account in question

Alexa Calling & Messaging

- Remember the string from before?
  - amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ
- We will add it to the URL “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~”

https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ

Alexa Calling & Messaging

- To view the Alexa Contacts, use this full URL
  - “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ/contacts”

Alexa Calling & Messaging


```
[{"name":{"firstName":"Peacock","lastName":"Leprechaun"},"numbers":
[{"number":"+[redacted]","type":"Mobile"}],"number":"+[redacted]","id":"34dd5e82-830e-4e05-953b-
e889468b410c","deviceContactId":null,"serverContactId":"34dd5e82-830e-4e05-953b-
e889468b410c","alexaEnabled":true,"isHomeGroup":false,"isBulkImport":false,"sourceDeviceId":null,"sourceDeviceName":null,"commsId":
["amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ"],"commsIds":
[{"aor":"sips:id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ@amcs-
tachyon.com","id":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ"}],"homeGroupId":null,"commsIdsPreferences"
:{"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ":{"preferenceGrantedToContactByUser":
{},"preferenceGrantedToUserByContact":{}}}},{"name":{"firstName":"Brian","lastName":"Moran"},"numbers":
[{"number":"+[redacted]","type":"Mobile"},{"number":"+[redacted]","type":"Work"}],"number":"+[redacted]","id":"a64805d7-8c3d-4632-
863c-ba630174f19b","deviceContactId":"1","serverContactId":"a64805d7-8c3d-4632-863c-
ba630174f19b","alexaEnabled":true,"isHomeGroup":false,"isBulkImport":true,"sourceDeviceId":"7937eab431ccce9ba1f6a2e0ddee8598","source
DeviceName":"Peacock's 12th Android Device","commsId":
["amzn1.comms.id.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A"],"commsIds":
[{"aor":"sips:id.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A@amcs-
tachyon.com","id":"amzn1.comms.id.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A"}],"homeGroupId":null,"commsIdsPreferences"
:{"amzn1.comms.id.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A":{"preferenceGrantedToContactByUser":
{},"preferenceGrantedToUserByContact":{}}}},{"name":{"firstName":"Home","lastName":null},"numbers":[],"number":null,"id":"61e06f26-
ae86-407d-81d4-92f9df0d82c2","deviceContactId":null,"serverContactId":"61e06f26-ae86-407d-81d4-
92f9df0d82c2","alexaEnabled":true,"isHomeGroup":true,"isBulkImport":false,"sourceDeviceId":null,"sourceDeviceName":null,"commsId":
["amzn1.comms.id.hg.amzn1~HH1RDEMIITRVOO7"],"commsIds":[],"homeGroupId":{"aor":"sips:id.hg.amzn1~HH1RDEMIITRVOO7@amcs-
tachyon.com","id":"amzn1.comms.id.hg.amzn1~HH1RDEMIITRVOO7"},"commsIdsPreferences":{"amzn1.comms.id.hg.amzn1~HH1RDEMIITRVOO7":
{"preferenceGrantedToContactByUser":{},"preferenceGrantedToUserByContact":{}}}},{"name":
```

Alexa Calling & Messaging

- To view the Alexa Conversations, use this full URL
  - “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ/conversations”

Alexa Calling & Messaging


```
{"lastPage":true,"conversations":
[{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","participants":
["amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ"],"firstVisibleMes
sageId":1,"lastMessageId":3,"lastSequenceId":3,"lastMessage":
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","messageId":3,"sequenceId":3,"time":"2017-05-
19T03:59:32.315Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3S
FBDCAIQ","type":"message/text","payload":{"text":"Hi"}},"lastModified":"2017-05-
19T04:03:13.084Z","readStatus":
{"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ":3},"unreadMessage
s":0,"unreadNotifications":0,"sendAsCommsId":"amzn1.comms.id.person.amzn1~amzn1.account.AEA
M5TQ27DKFM7VJXYY3SFBDCAIQ","viewAsCommsId":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5
TQ27DKFM7VJXYY3SFBDCAIQ"},
{"conversationId":"amzn1.comms.messaging.id.conversation~4ByDCyq_fJSzZcsjq_iBNm9vhnQ","part
icipants":
["amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ","amzn1.comms.id.p
erson.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A"],"firstVisibleMessageId":1,"lastMes
sageId":23,"lastSequenceId":23,"lastMessage":
{"conversationId":"amzn1.comms.messaging.id.conversation~4ByDCyq_fJSzZcsjq_iBNm9vhnQ","mess
ageId":23,"sequenceId":23,"time":"2017-05-
19T03:44:43.504Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEV
YHQAL3A","type":"message/text","payload":{"text":"Hey hey hey PL"}},"lastModified":"2017-
05-19T03:45:17.043Z","readStatus":
{"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ":23,"amzn1.comms.i
d.person.amzn1~amzn1.account.AG3YF7QO2BRDC56R5IXEVYHQAL3A":20},"unreadMessages":0,"unreadNo
tifications":0,"sendAsCommsId":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJX
YY3SFBDCAIQ","viewAsCommsId":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY
3SFBDCAIQ"},
{"conversationId":"amzn1.comms.messaging.id.conversation~hGhpq7GF25b950niuHRHXZ1XKHE","part
icipants":
```

Alexa Calling & Messaging

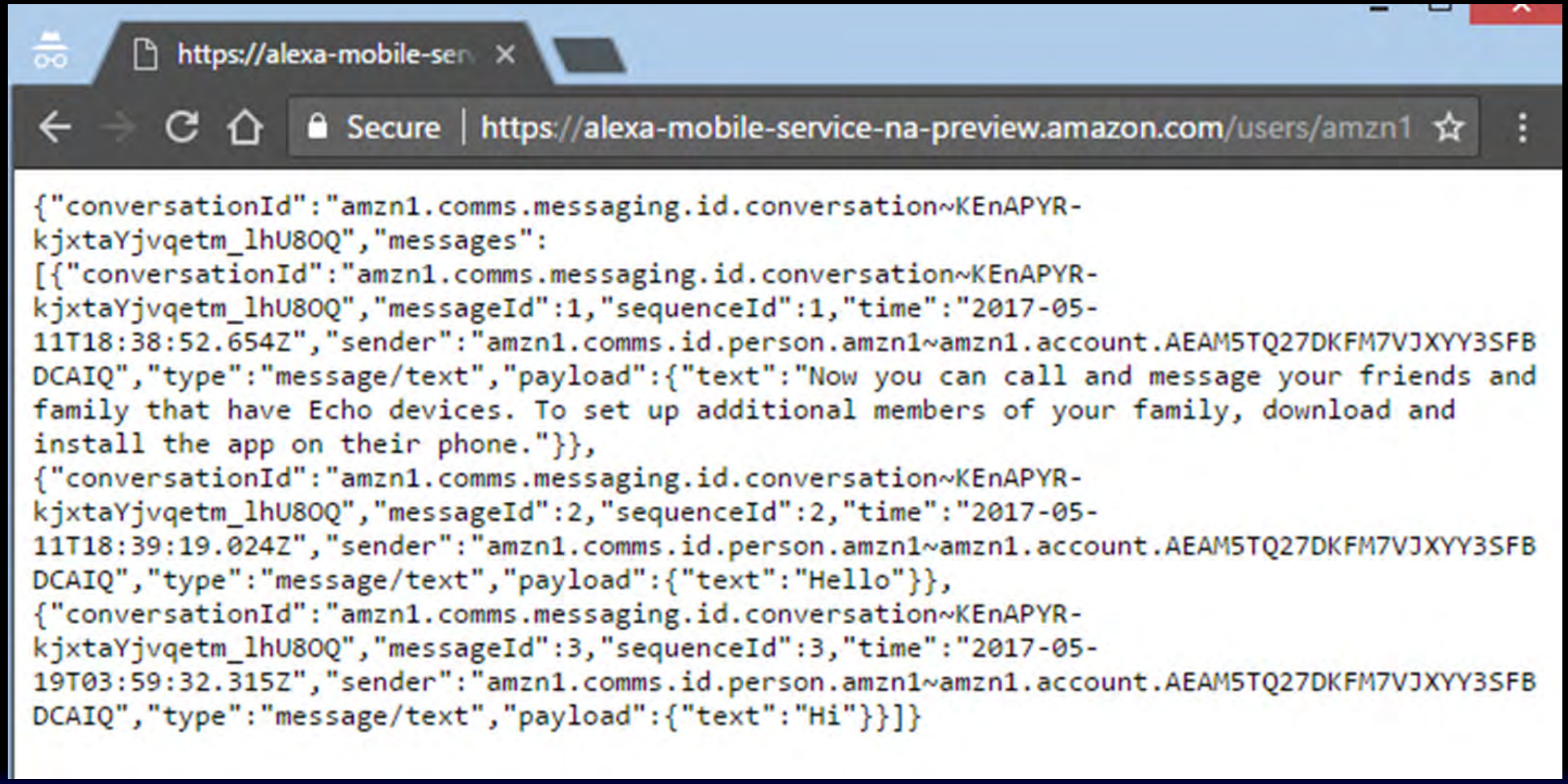
- We will need the conversation ID to get the messages for each conversation
  - “amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ”

- We will add that to the URL “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ/conversations/”
- And append “messages?count=100&sort=asc” to the end of the URL

Alexa Calling & Messaging

- So to view the messages, this is our URL:
  - “https://alexa-mobile-service-na-preview.amazon.com/users/amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFBDCAIQ/conversations/amzn1.comms.messaging.id.conversation~KEnAPYR-kjxtaYjvqetm_lhU8OQ/messages?count=100&sort=asc”

Alexa Calling & Messaging




```
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","messages":
[{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","messageId":1,"sequenceId":1,"time":"2017-05-
11T18:38:52.654Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB
DCAIQ","type":"message/text","payload":{"text":"Now you can call and message your friends and
family that have Echo devices. To set up additional members of your family, download and
install the app on their phone."}},
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","messageId":2,"sequenceId":2,"time":"2017-05-
11T18:39:19.024Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB
DCAIQ","type":"message/text","payload":{"text":"Hello"}},
{"conversationId":"amzn1.comms.messaging.id.conversation~KEnAPYR-
kjxtaYjvqetm_lhU8OQ","messageId":3,"sequenceId":3,"time":"2017-05-
19T03:59:32.315Z","sender":"amzn1.comms.id.person.amzn1~amzn1.account.AEAM5TQ27DKFM7VJXYY3SFB
DCAIQ","type":"message/text","payload":{"text":"Hi"}}]}
```

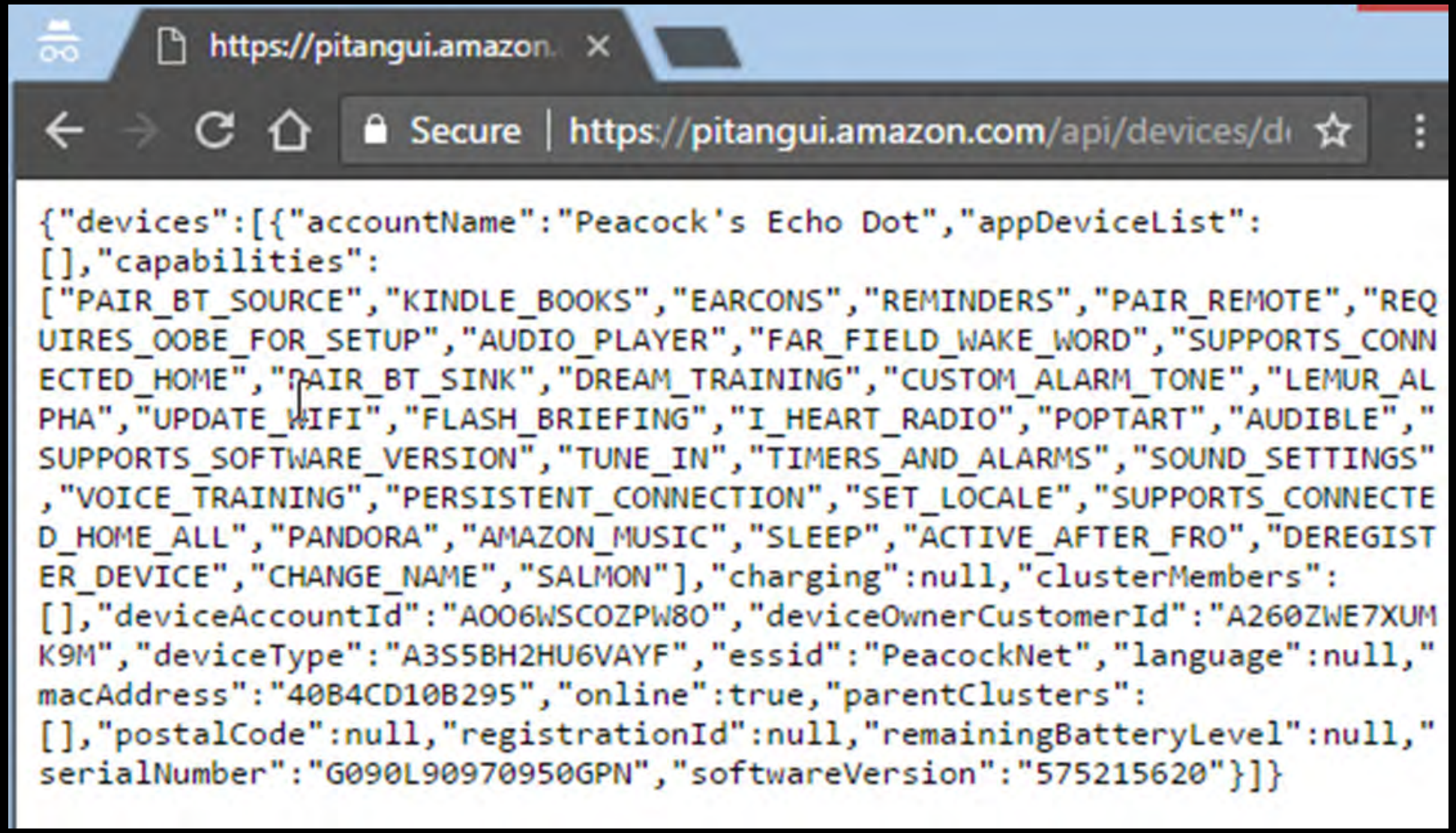
Alexa Calling & Messaging

- Important things to note:
  - The URL query only allows for 100 messages
  - You must be signed in as the user (username and password)
  - This may change in the future. Or by the time we give this presentation!

Alexa Devices

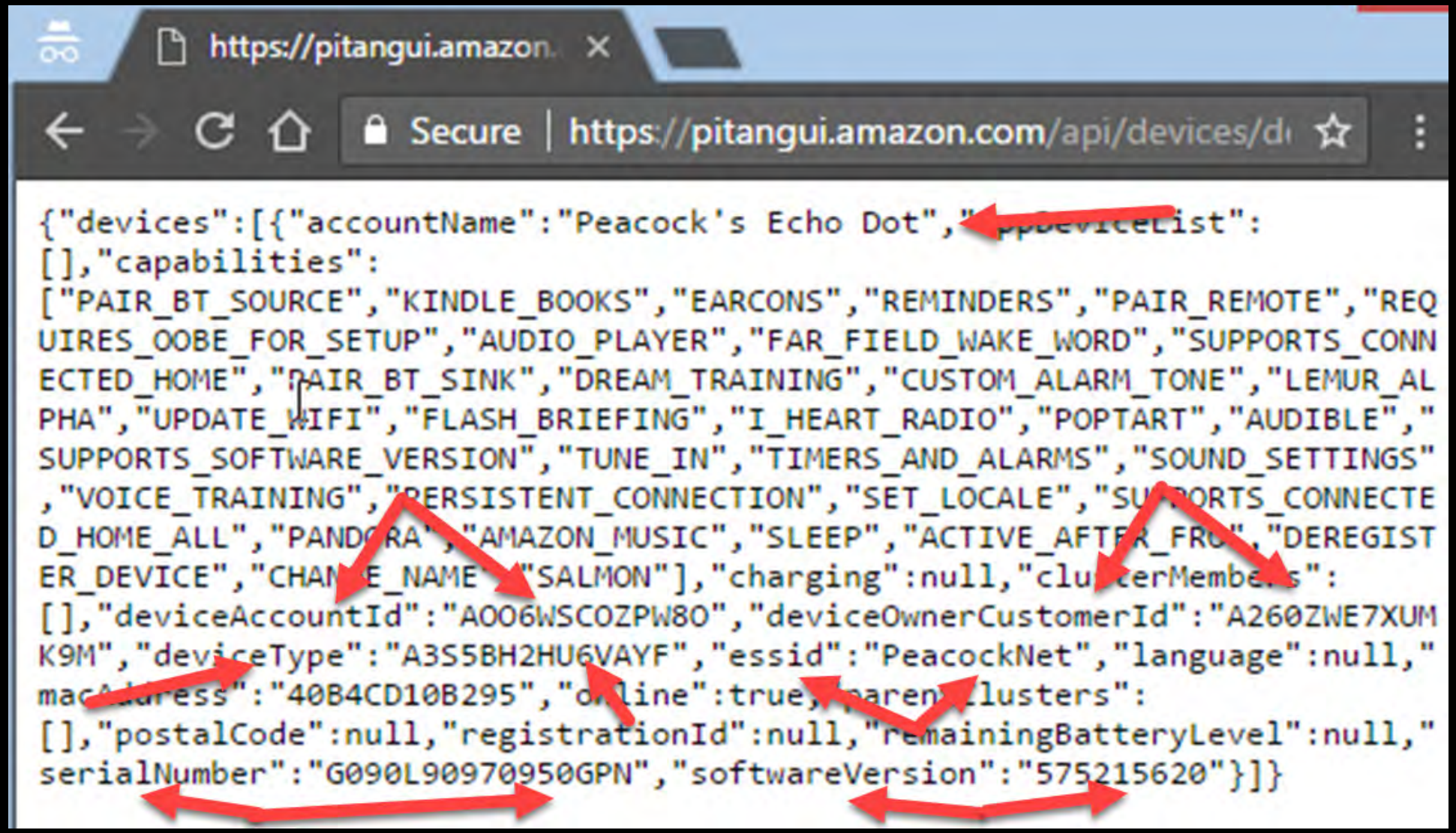
- Browse to https://pitangui.amazon.com/api/devices/device?
- This lists all the Alexa enabled devices associated with the account (in JSON format)

Alexa Devices




```
{"devices":[{"accountName":"Peacock's Echo Dot","appDeviceList":
[],"capabilities":
["PAIR_BT_SOURCE","KINDLE_BOOKS","EARCONS","REMINDERS","PAIR_REMOTE","REQ
UIRES_OOBE_FOR_SETUP","AUDIO_PLAYER","FAR_FIELD_WAKE_WORD","SUPPORTS_CONN
ECTED_HOME","PAIR_BT_SINK","DREAM_TRAINING","CUSTOM_ALARM_TONE","LEMUR_AL
PHA","UPDATE_WIFI","FLASH_BRIEFING","I_HEART_RADIO","POPTART","AUDIBLE","
SUPPORTS_SOFTWARE_VERSION","TUNE_IN","TIMERS_AND_ALARMS","SOUND_SETTINGS"
,"VOICE_TRAINING","PERSISTENT_CONNECTION","SET_LOCALE","SUPPORTS_CONNECTE
D_HOME_ALL","PANDORA","AMAZON_MUSIC","SLEEP","ACTIVE_AFTER_FRO","DEREGIST
ER_DEVICE","CHANGE_NAME","SALMON"],"charging":null,"clusterMembers":
[],"deviceAccountId":"AOO6WSCOZPW8O","deviceOwnerCustomerId":"A260ZWE7XUM
K9M","deviceType":"A3S5BH2HU6VAYF","essid":"PeacockNet","language":null,"
macAddress":"40B4CD10B295","online":true,"parentClusters":
[],"postalCode":null,"registrationId":null,"remainingBatteryLevel":null,"
serialNumber":"G090L90970950GPN","softwareVersion":"575215620"}]}
```

Alexa Devices



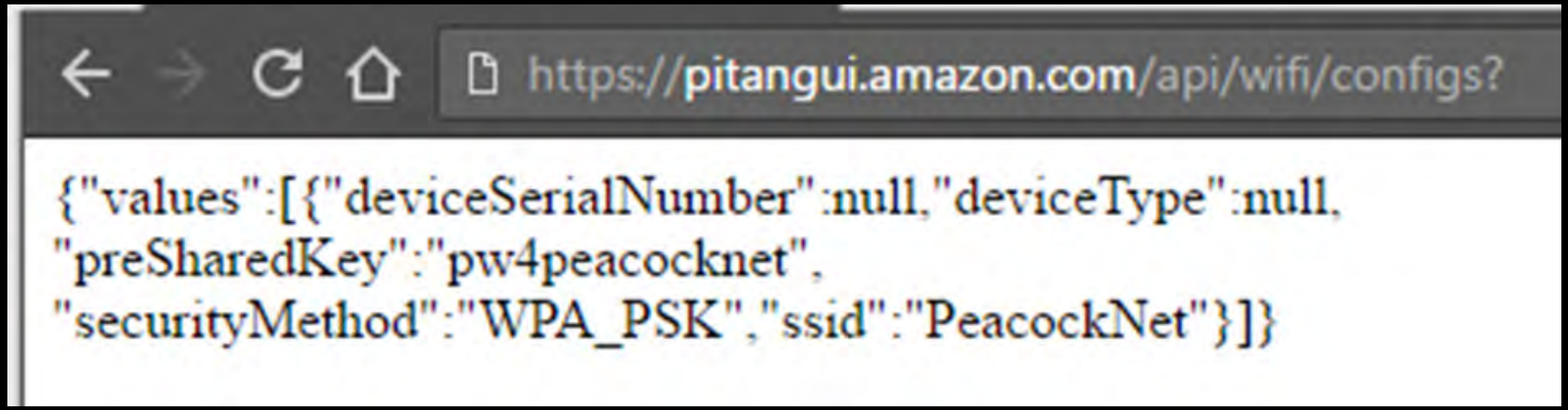
Alexa Devices

- We now have the following items:
  - A3S5BH2HU6VAYF
    - Model type of Echo Dot
  - G090L90970950GPN
    - Serial Number of Echo Dot
  - A260ZWE7XUMK9M
    - Customer ID
  - 575215620
    - Software version
  - AOO6WSCOZPW80
    - Device Account ID
- Searching for these may lead to more URLs to pull data from!

Alexa Wifi

- Browse to “https://pitangui.amazon.com/api/wifi/configs?”
- This lists wireless network information that the user chooses to save to the Amazon cloud (on by default)
  - Including SSID & plain-text password

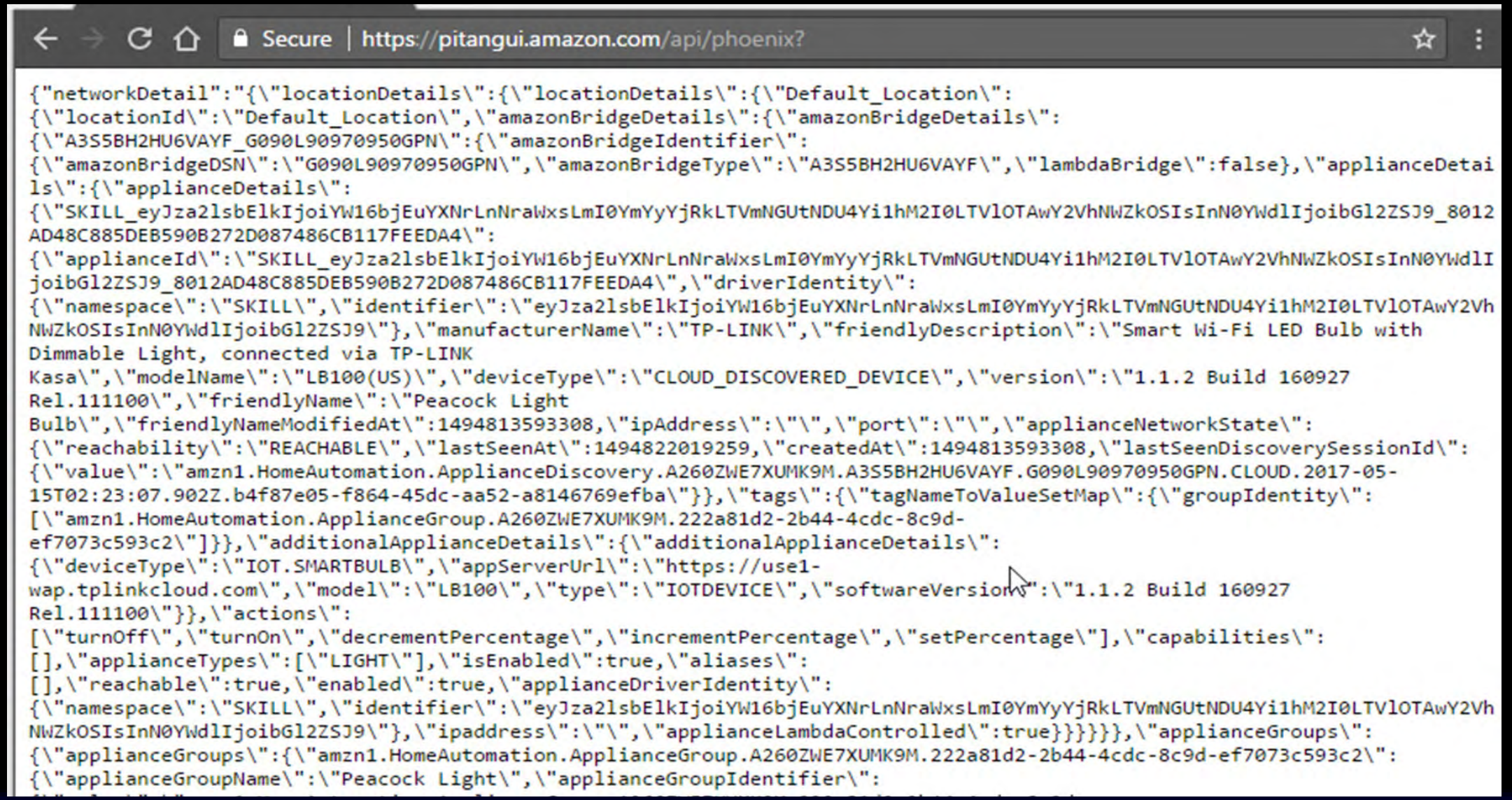
Alexa Wifi


https://pitangui.amazon.com/api/wifi/configs?
{"values":[{"deviceSerialNumber":null,"deviceType":null,
"preSharedKey":"pw4peacocknet",
"securityMethod":"WPA_PSK","ssid":"PeacockNet"}]}

Alexa Smart Home Devices

- Browse to “https://pitangui.amazon.com/api/phoenix?”
- This lists all the Smart Home devices, and groups, that the user has associated with the Alexa account

Alexa Smart Home Devices

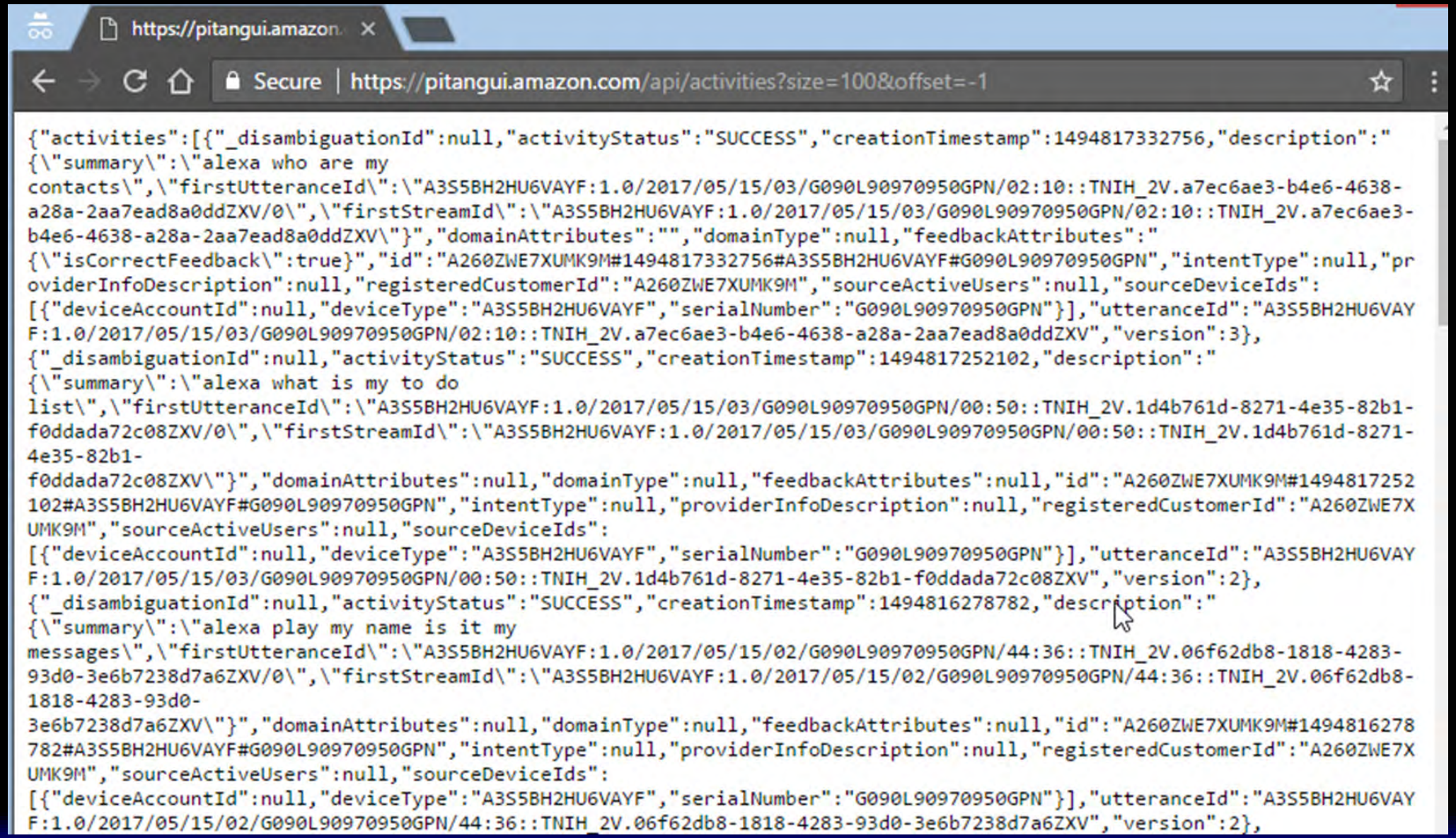



```
{"networkDetail":"{\"locationDetails\":{\"locationDetails\":{\"Default_Location\":
{\"locationId\":\"Default_Location\",\"amazonBridgeDetails\":{\"amazonBridgeDetails\":
{\"A3S5BH2HU6VAYF_G090L90970950GPN\":{\"amazonBridgeIdentifier\":
{\"amazonBridgeDSN\":\"G090L90970950GPN\",\"amazonBridgeType\":\"A3S5BH2HU6VAYF\",\"lambdaBridge\":false},\"applianceDetai
ls\":{\"applianceDetails\":
{\"SKILL_eyJza2lsbElkIjoiYW16bjEuYXNrLnNraWxsLmI0YmYyYjRkLTVmNGUtNDU4Yi1hM2I0LTVlOTAwY2VhNWZkOSIsInN0YWdlIjoibGl2ZSJ9_8012
AD48C885DEB590B272D087486CB117FEEDA4\":
{\"applianceId\":\"SKILL_eyJza2lsbElkIjoiYW16bjEuYXNrLnNraWxsLmI0YmYyYjRkLTVmNGUtNDU4Yi1hM2I0LTVlOTAwY2VhNWZkOSIsInN0YWdlI
joibGl2ZSJ9_8012AD48C885DEB590B272D087486CB117FEEDA4\",\"driverIdentity\":
{\"namespace\":\"SKILL\",\"identifier\":\"eyJza2lsbElkIjoiYW16bjEuYXNrLnNraWxsLmI0YmYyYjRkLTVmNGUtNDU4Yi1hM2I0LTVlOTAwY2Vh
NWZkOSIsInN0YWdlIjoibGl2ZSJ9\"},\"manufacturerName\":\"TP-LINK\",\"friendlyDescription\":\"Smart Wi-Fi LED Bulb with
Dimmable Light, connected via TP-LINK
Kasa\",\"modelName\":\"LB100(US)\",\"deviceType\":\"CLOUD_DISCOVERED_DEVICE\",\"version\":\"1.1.2 Build 160927
Rel.111100\",\"friendlyName\":\"Peacock Light
Bulb\",\"friendlyNameModifiedAt\":1494813593308,\"ipAddress\":\"\",\"port\":\"\",\"applianceNetworkState\":
{\"reachability\":\"REACHABLE\",\"lastSeenAt\":1494822019259,\"createdAt\":1494813593308,\"lastSeenDiscoverySessionId\":
{\"value\":\"amzn1.HomeAutomation.ApplianceDiscovery.A260ZWE7XUMK9M.A3S5BH2HU6VAYF.G090L90970950GPN.CLOUD.2017-05-
15T02:23:07.902Z.b4f87e05-f864-45dc-aa52-a8146769efba\"}},\"tags\":{\"tagNameToValueSetMap\":{\"groupIdentity\":
[\"amzn1.HomeAutomation.ApplianceGroup.A260ZWE7XUMK9M.222a81d2-2b44-4cdc-8c9d-
ef7073c593c2\"]}},\"additionalApplianceDetails\":{\"additionalApplianceDetails\":
{\"deviceType\":\"IOT.SMARTBULB\",\"appServerUrl\":\"https://use1-
wap.tplinkcloud.com\",\"model\":\"LB100\",\"type\":\"IOTDEVICE\",\"softwareVersion\":\"1.1.2 Build 160927
Rel.111100\"}},\"actions\":
[\"turnOff\",\"turnOn\",\"decrementPercentage\",\"incrementPercentage\",\"setPercentage\"],\"capabilities\":
[],\"applianceTypes\":[\"LIGHT\"],\"isEnabled\":true,\"aliases\":
[],\"reachable\":true,\"enabled\":true,\"applianceDriverIdentity\":
{\"namespace\":\"SKILL\",\"identifier\":\"eyJza2lsbElkIjoiYW16bjEuYXNrLnNraWxsLmI0YmYyYjRkLTVmNGUtNDU4Yi1hM2I0LTVlOTAwY2Vh
NWZkOSIsInN0YWdlIjoibGl2ZSJ9\"},\"ipaddress\":\"\",\"applianceLambdaControlled\":true}}}}}},\"applianceGroups\":
{\"applianceGroups\":{\"amzn1.HomeAutomation.ApplianceGroup.A260ZWE7XUMK9M.222a81d2-2b44-4cdc-8c9d-ef7073c593c2\":
{\"applianceGroupName\":\"Peacock Light\",\"applianceGroupIdentifier\":
```

Alexa Activities

- Browse to “https://pitangui.amazon.com/api/activities?size=100&offset=-1”
- This the last 50 activities that was performed by Alexa
  - Regardless of device that it originated from
    - Currently last 50 are returned, but URL lists size as 100 just in case Amazon changes that amount!

Alexa Activities




```
{"activities":[{"_disambiguationId":null,"activityStatus":"SUCCESS","creationTimestamp":1494817332756,"description":"
{\"summary\":\"alexa who are my
contacts\",\"firstUtteranceId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/03/G090L90970950GPN/02:10::TNIH_2V.a7ec6ae3-b4e6-4638-
a28a-2aa7ead8a0ddZXV/0\",\"firstStreamId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/03/G090L90970950GPN/02:10::TNIH_2V.a7ec6ae3-
b4e6-4638-a28a-2aa7ead8a0ddZXV\"}","domainAttributes":"","domainType":null,"feedbackAttributes":"
{\"isCorrectFeedback\":true}","id":"A260ZWE7XUMK9M#1494817332756#A3S5BH2HU6VAYF#G090L90970950GPN","intentType":null,"pr
oviderInfoDescription":null,"registeredCustomerId":"A260ZWE7XUMK9M","sourceActiveUsers":null,"sourceDeviceIds":
[{"deviceAccountId":null,"deviceType":"A3S5BH2HU6VAYF","serialNumber":"G090L90970950GPN"}],"utteranceId":"A3S5BH2HU6VAY
F:1.0/2017/05/15/03/G090L90970950GPN/02:10::TNIH_2V.a7ec6ae3-b4e6-4638-a28a-2aa7ead8a0ddZXV","version":3},
{"_disambiguationId":null,"activityStatus":"SUCCESS","creationTimestamp":1494817252102,"description":"
{\"summary\":\"alexa what is my to do
list\",\"firstUtteranceId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/03/G090L90970950GPN/00:50::TNIH_2V.1d4b761d-8271-4e35-82b1-
f0ddada72c08ZXV/0\",\"firstStreamId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/03/G090L90970950GPN/00:50::TNIH_2V.1d4b761d-8271-
4e35-82b1-
f0ddada72c08ZXV\"}","domainAttributes":null,"domainType":null,"feedbackAttributes":null,"id":"A260ZWE7XUMK9M#1494817252
102#A3S5BH2HU6VAYF#G090L90970950GPN","intentType":null,"providerInfoDescription":null,"registeredCustomerId":"A260ZWE7X
UMK9M","sourceActiveUsers":null,"sourceDeviceIds":
[{"deviceAccountId":null,"deviceType":"A3S5BH2HU6VAYF","serialNumber":"G090L90970950GPN"}],"utteranceId":"A3S5BH2HU6VAY
F:1.0/2017/05/15/03/G090L90970950GPN/00:50::TNIH_2V.1d4b761d-8271-4e35-82b1-f0ddada72c08ZXV","version":2},
{"_disambiguationId":null,"activityStatus":"SUCCESS","creationTimestamp":1494816278782,"description":"
{\"summary\":\"alexa play my name is it my
messages\",\"firstUtteranceId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/02/G090L90970950GPN/44:36::TNIH_2V.06f62db8-1818-4283-
93d0-3e6b7238d7a6ZXV/0\",\"firstStreamId\":\"A3S5BH2HU6VAYF:1.0/2017/05/15/02/G090L90970950GPN/44:36::TNIH_2V.06f62db8-
1818-4283-93d0-
3e6b7238d7a6ZXV\"}","domainAttributes":null,"domainType":null,"feedbackAttributes":null,"id":"A260ZWE7XUMK9M#1494816278
782#A3S5BH2HU6VAYF#G090L90970950GPN","intentType":null,"providerInfoDescription":null,"registeredCustomerId":"A260ZWE7X
UMK9M","sourceActiveUsers":null,"sourceDeviceIds":
[{"deviceAccountId":null,"deviceType":"A3S5BH2HU6VAYF","serialNumber":"G090L90970950GPN"}],"utteranceId":"A3S5BH2HU6VAY
F:1.0/2017/05/15/02/G090L90970950GPN/44:36::TNIH_2V.06f62db8-1818-4283-93d0-3e6b7238d7a6ZXV","version":2},
```

Alexa URLs

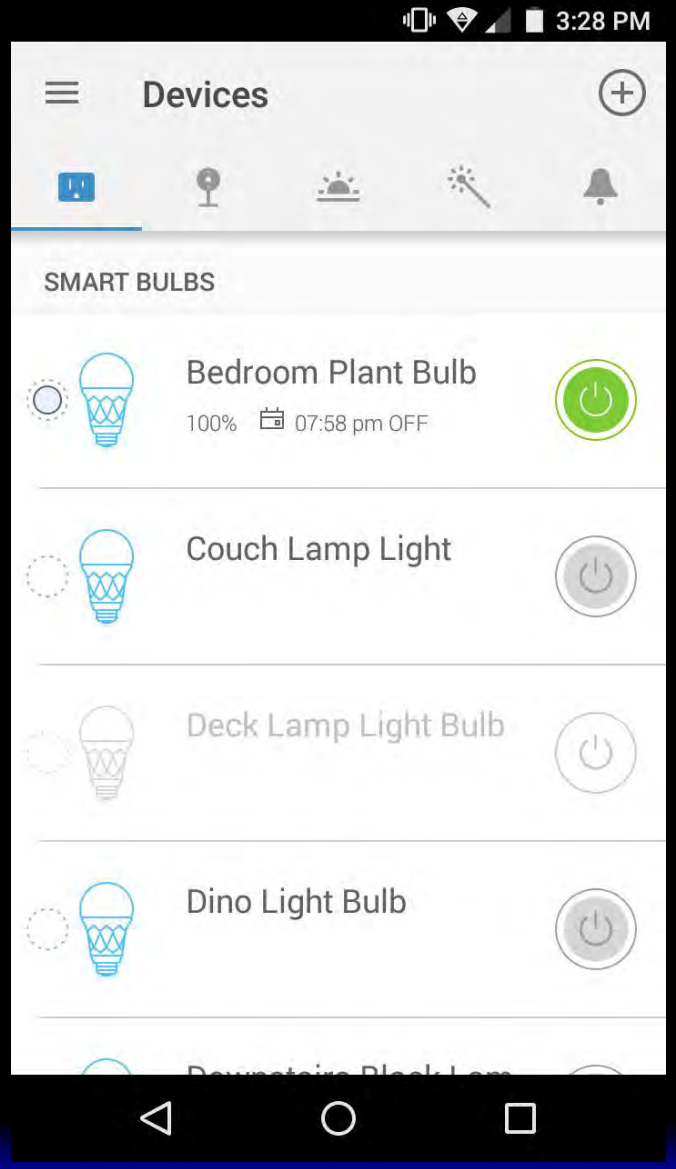
- There are many more known (and probably unknown) URLS to pull data from as well

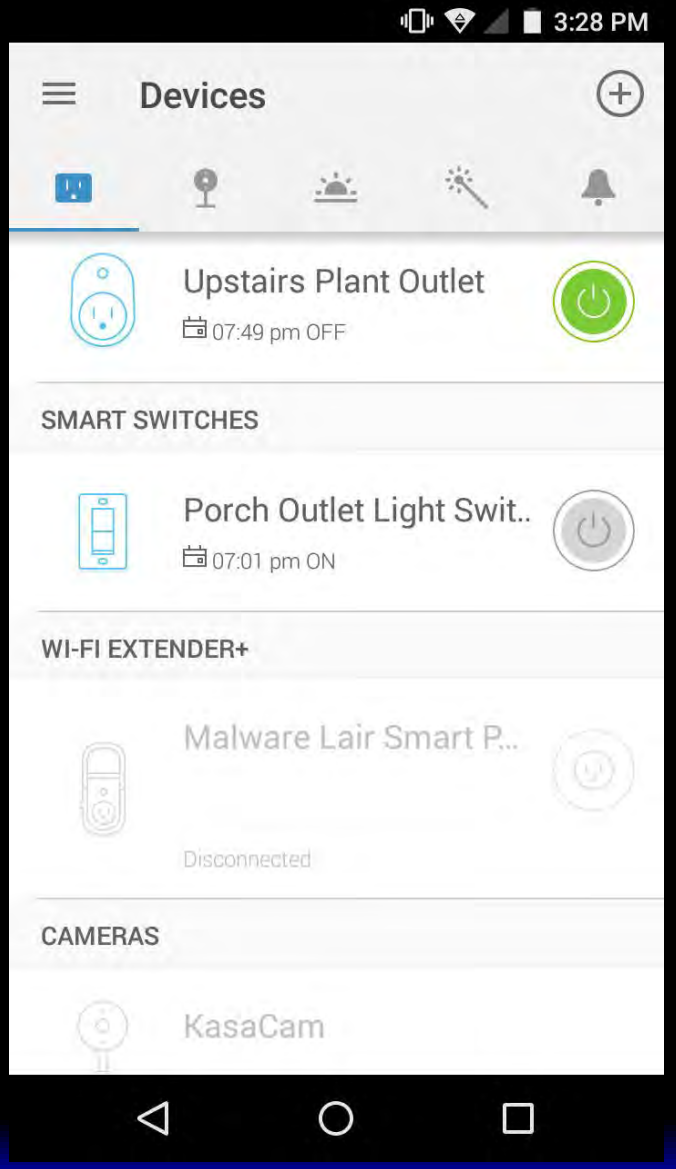
- Smart keyword searching is DEFINITELY your friend

kasa mobile application

- “kasa” is the mobile application for TP-Link smart devices
  - Smart Plug (HS100/110)
  - Smart Plug Mini (HS105)
  - Smart Switch (HS200)
  - Smart Bulbs (LB100/110/120/130)
- Just like Amazon, new devices keep coming

kasa mobile application (cont.)

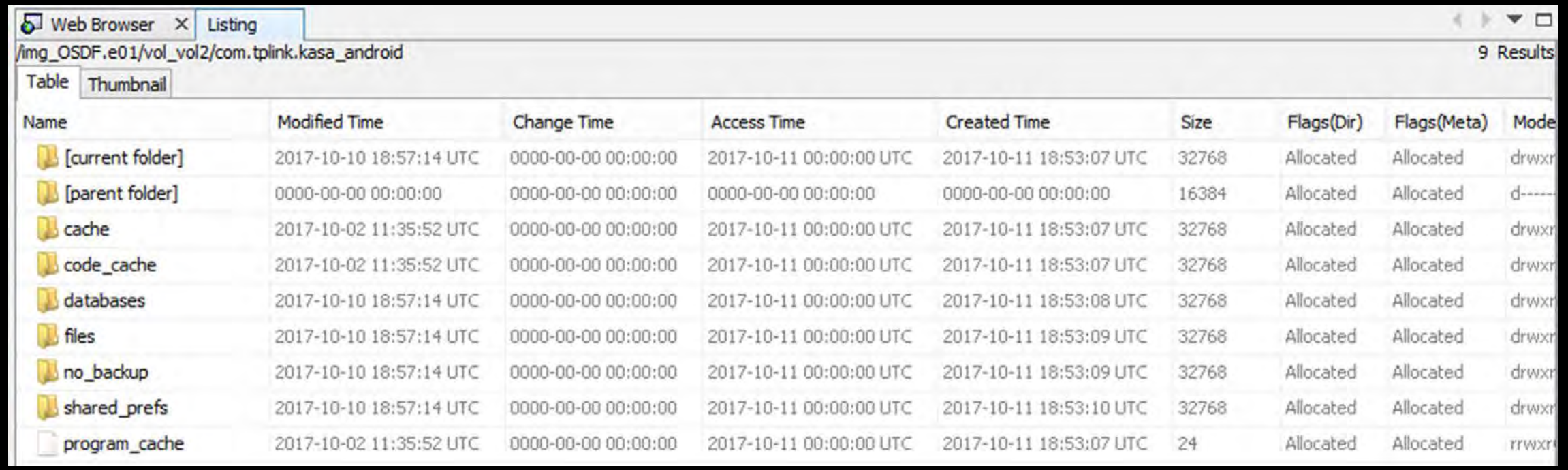




kasa mobile application (cont.)

- “\data\com.tplink.kasa_android” is the path to kasa folder on device
- Folder of primary interest is “databases”
- This folder contains (surprise) SQLite databases

kasa mobile application (cont.)



Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Mode
[current folder]	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:07 UTC	32768	Allocated	Allocated	drwxr
[parent folder]	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	16384	Allocated	Allocated	d-----
cache	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:07 UTC	32768	Allocated	Allocated	drwxr
code_cache	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:07 UTC	32768	Allocated	Allocated	drwxr
databases	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	32768	Allocated	Allocated	drwxr
files	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:09 UTC	32768	Allocated	Allocated	drwxr
no_backup	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:09 UTC	32768	Allocated	Allocated	drwxr
shared_prefs	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:10 UTC	32768	Allocated	Allocated	drwxr
program_cache	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:07 UTC	24	Allocated	Allocated	rrwxr

Data viewed in Autopsy 4.4.1

kasa mobile application (cont.)

Well that is a convenient name!

/img_OSDF.e01/vol_vol2/com.tplink.kasa_android/databases — 8 Results

Table | Thumbnail

Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(D
[current folder]	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	32768	Allocat
[parent folder]	2017-10-10 18:57:14 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:07 UTC	32768	Allocat
google_analytics_v4.db	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	28672	Allocat
google_analytics_v4.db-journal	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	8720	Allocat
google_app_measurement_local.db	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	16384	Allocat
google_app_measurement_local.db-journal	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:08 UTC	8720	Allocat
iot.1.db	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:09 UTC	184320	Allocat
iot.1.db-journal	2017-10-02 11:35:52 UTC	0000-00-00 00:00:00	2017-10-11 00:00:00 UTC	2017-10-11 18:53:09 UTC	66176	Allocat

Data viewed in Autopsy 4.4.1

iot.1.db

- Contains at least 8 tables, with straight-forward naming conventions
- For example, “accounts” contains account information

– Notice anything particularly useful?

iot.1.db – “accounts”

accounts

createdOn	email	firstN...	id	lastN...	password	refre...	token
1503575310415	peacockleprechau...		911D43A56B9CD0494975A0B03D0CF7D90834ED590494...		TPLG9ND9ZDT2msdfeZmtGX0KbvJMFbBDb8cvu/r56PUJBj...		ChrzrdSqrtlBlbsrtt1T/iaDBCvrk5ufShbltj

Data viewed in SQLiteSpy 1.9.6

iot.1.db – “devices”

- Following that line of thinking, I bet “devices” contains a list of all the TP-Link devices associated with the account!

iot.1.db – “devices”

addr...	appServerUrl	cate...	cloud...	createdOn	deviceAddress	deviceAlias	devic...	devic...	deviceId	deviceM...	deviceName
	https://use1-wap.tplinkcloud.com			1494271325826	50:C7:BF:	Upstairs Plant Outlet	switch		800679A[redacted]142D	HS100(US)	Wi-Fi Smart Plug
	https://use1-wap.tplinkcloud.com			1494271325781	50:C7:BF:	Downstairs Couch Light	switch		8006801[redacted]30D	HS100(US)	Wi-Fi Smart Plug
	https://use1-wap.tplinkcloud.com			1494271325801	50:C7:BF:	Downstairs Fireplace Plant Light	switch		800695C[redacted]2B16	HS100(US)	Wi-Fi Smart Plug
	https://use1-wap.tplinkcloud.com			1494271325761	50:C7:BF:	Living Room Green Lamp Light	lightBulb		8012F6F[redacted]306B	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
	https://use1-wap.tplinkcloud.com			1494271325734	50:C7:BF:	Kitchen Sink One	lightBulb		8012345[redacted]FFD0	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing
	https://use1-wap.tplinkcloud.com			1494271325707	50:C7:BF:	Kichen Sink Two	lightBulb		8012ABB[redacted]B0E	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing
	https://use1-wap.tplinkcloud.com			1494271325684	50:C7:BF:	[redacted]Panda Lamp Light	lightBulb		8012198A[redacted]0B71	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light
	https://use1-wap.tplinkcloud.com			1494271325607	50:C7:BF:	Couch Lamp Light	lightBulb		8012610[redacted]12AF	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
	https://use1-wap.tplinkcloud.com			1494271325634	50:C7:BF:	Dino Light Bulb	lightBulb		8012D66[redacted]1A02	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
	https://use1-wap.tplinkcloud.com			1494271325662	50:C7:BF:	Downstairs Black Lamp Light	lightBulb		8012A07[redacted]0998	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
	https://use1-wap.tplinkcloud.com			1494271325562	50:C7:BF:	Bedroom Plant Bulb	lightBulb		8012EDE[redacted]5974	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light

devic...	devic...	deviceId	deviceM...	deviceName
switch		800679A[redacted]142D	HS100(US)	Wi-Fi Smart Plug
switch		8006801[redacted]30D	HS100(US)	Wi-Fi Smart Plug
switch		800695C[redacted]2B16	HS100(US)	Wi-Fi Smart Plug
lightBulb		8012F6F[redacted]306B	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
lightBulb		8012345[redacted]FFD0	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing
lightBulb		8012ABB[redacted]B0E	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing
lightBulb		8012198A[redacted]0B71	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light
lightBulb		8012610[redacted]12AF	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
lightBulb		8012D66[redacted]1A02	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
lightBulb		8012A07[redacted]0998	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light
lightBulb		8012EDE[redacted]5974	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light

Data viewed in SQLiteSpy 1.9.6

iot.1.db – “devices”

- Created date, device MAC address, user created alias, device type, unique device ID, model, given name, current device state, hardware ID, IP address, cloud bound (remotely controllable), signal strength, etc.

- SOO MANY DETAILS!!

iot.1.db – “locations_v2”

- Contains account ID, created time, last sync time, and geographic coordinates of where the user account is

iot.1.db – “locations_v2”

- A quick Google map search shows the location to be pretty accurate
  - Not 100% accurate, but pretty darn close!

iot.1.db – “locations”

Addressing kasa Security Concerns

- TP-Link was responsive and had an application update out by June 23rd (DFIRSummit presentation date)
  - No longer storing credentials in plain-text
  - Must now sign in to kasa to control devices (both locally and remotely)
    - This means Timmy at the family reunion can no longer control the smart home just because he downloaded kasa app
      - Sorry Timmy!

Addressing kasa Security Concerns (cont.)

- TP-Link has (will have been) outstanding in working with us to ensure these issues are fixed
- TP-Link has continually stressed that they are actively working on identifying any/all issues and balancing the fine line between user security & usability
- Honestly wish that more companies took such an active approach to working with researchers to identify, mitigate, and implement solutions to security concerns
  - Many, many thanks to TP-Link!!

Alexa Security Concerns

- Initially, we found almost nothing with security issues of Alexa
- Alexa Calling & Messaging changed all of that
- Thanks to Twitter, we were able to get in directly touch with security folks at Amazon in about an hour

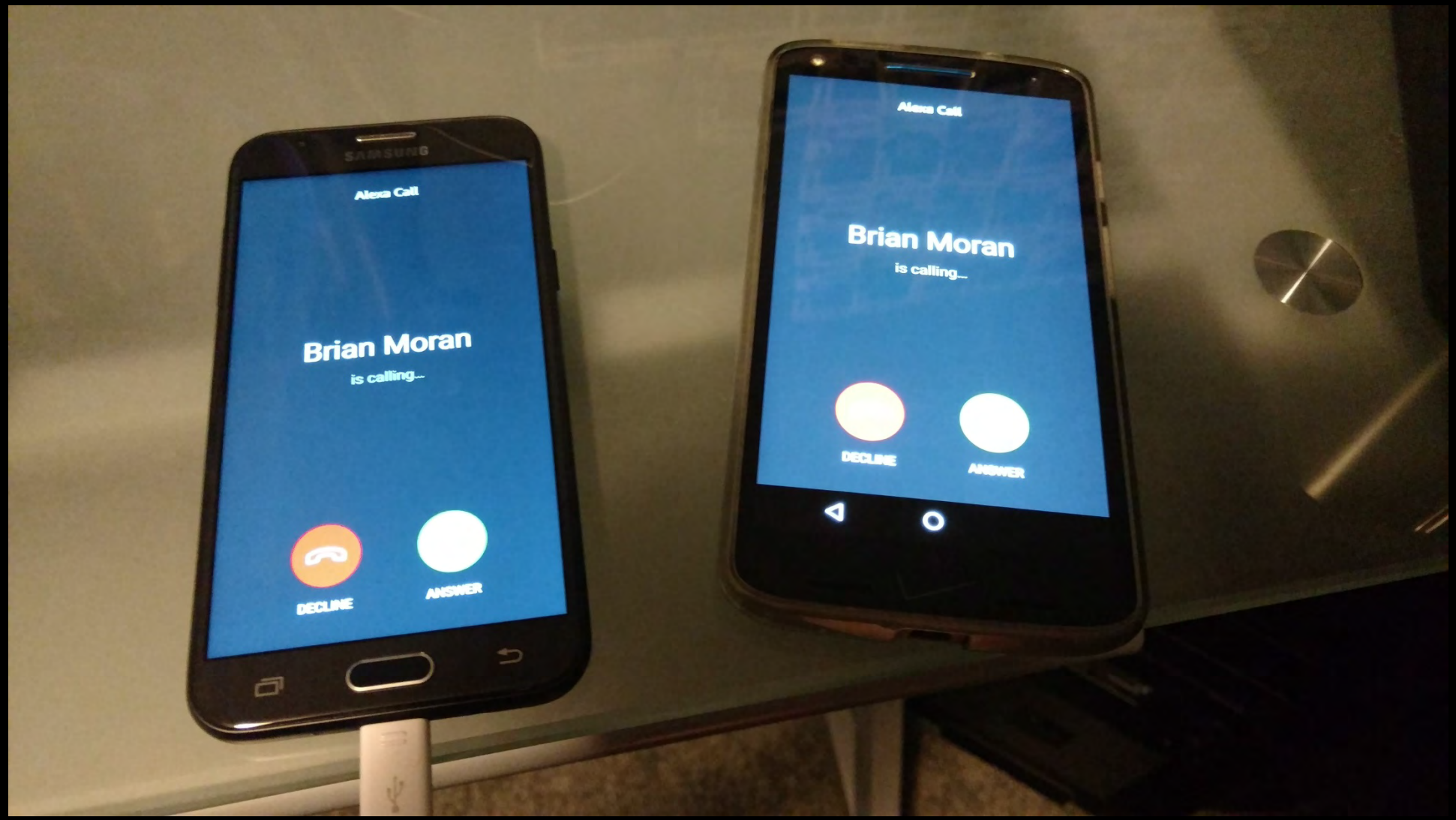
Alexa Security Concerns (cont.)

Alexa Security Concerns (cont.)

- This means that you could
  - Make Alexa Calls as another person
  - Receive Alexa Calls being sent to another person
  - Send Alexa Messages as another person
  - Receive Alexa Messages being sent to another person
  - Have Alexa contacts synced to your device

- All without the original user ever knowing!

Alexa Security Concerns (cont.)



Alexa Security Concerns (cont.)

- All of my contacts replicated across the Peacock Leprechaun account, regardless of what device it was signed in on

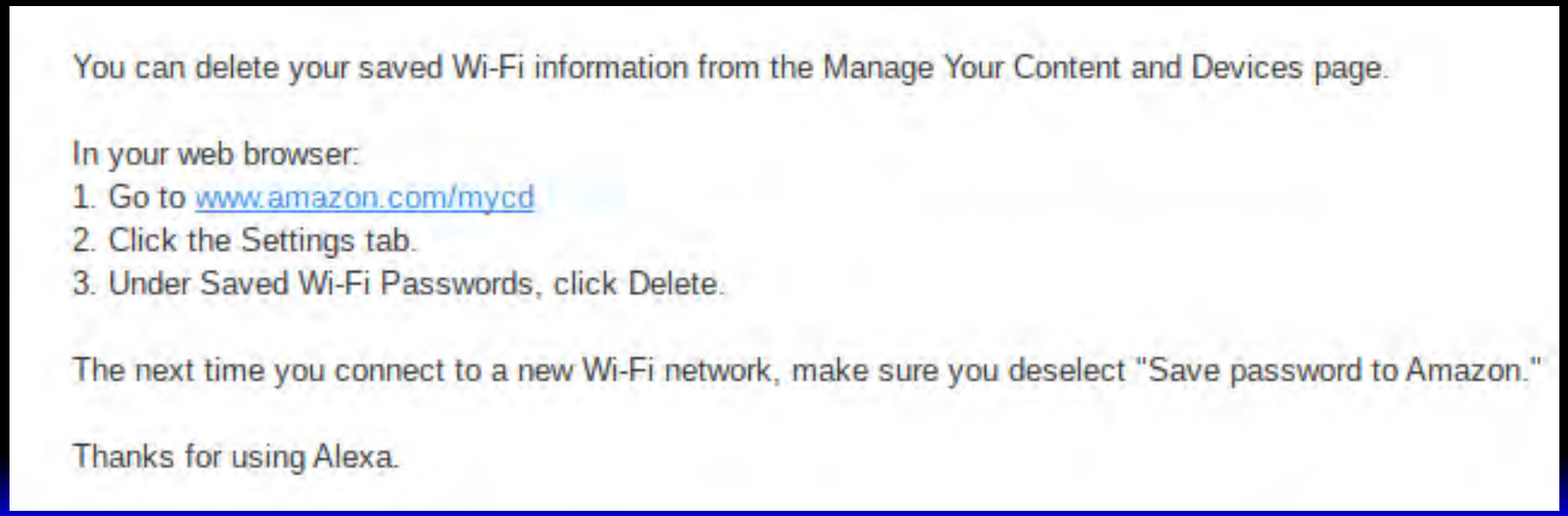
- Even enabling two factor authentication did not change that, once the user logged in on the device, they were in the account

Alexa Security Concerns (cont.)

- The wifi/configs? URL query could also give someone who has your Amazon account credentials the SSID & plain-text password for your wireless network(s)
  - As long as they are saved to Amazon (on by default)

Addressing Alexa Security Concerns

- You can call Amazon to remove Wi-Fi profiles from your account
  - Watch your Echo while you do this. Blinking lights!
- Or you can do it through the browser…



You can delete your saved Wi-Fi information from the Manage Your Content and Devices page.

In your web browser:
1. Go to www.amazon.com/mycd
2. Click the Settings tab.
3. Under Saved Wi-Fi Passwords, click Delete.

The next time you connect to a new Wi-Fi network, make sure you deselect "Save password to Amazon."

Thanks for using Alexa.

Addressing Alexa Security Concerns (cont.)

- Amazon security team working on fixes
  - Hard to fix something when, it works the way that it should, but can also be used for malicious purposes
- Amazon was very happy that we identified issues & shared this with them
- The Amazon security team has been fantastic to work with!

Plugins. For Autopsy. To Parse Data

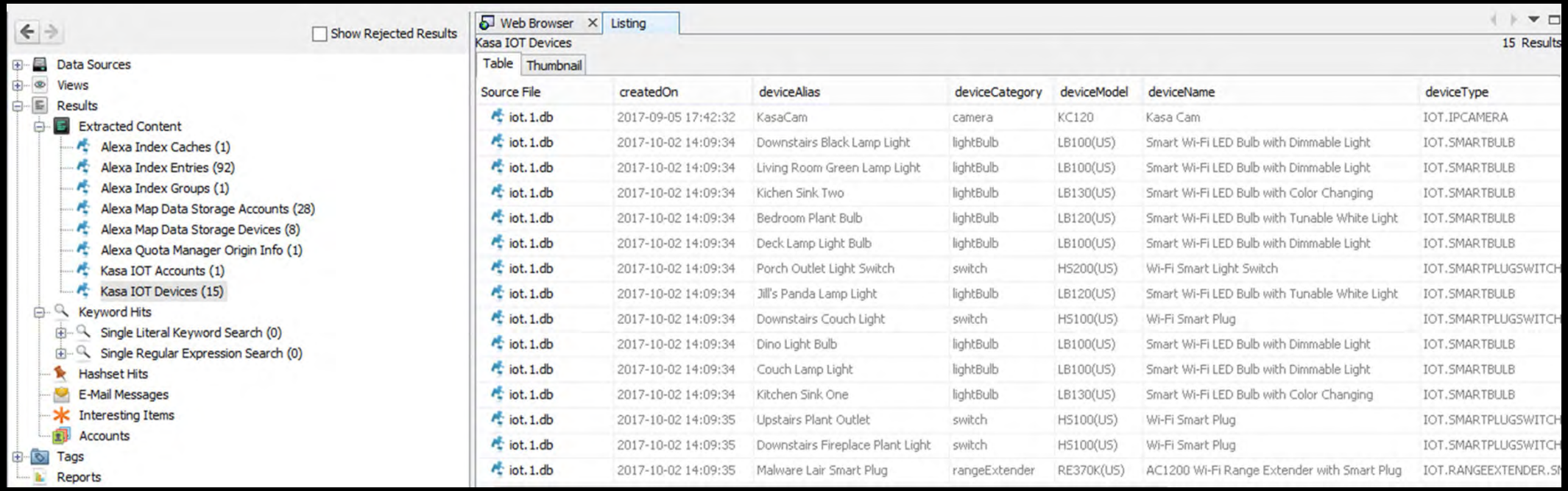
Because this is OSDFCon after all!!

- Thanks to the hard work of Mark McKinnon, we were able to make a plugin called “Amazon Echosystem Parser” available for Autopsy.

- Download from: https://github.com/markmckinnon/Autopsy-Plugins/tree/master/Amazon_Echosystem_Parser

Plugins. For Autopsy. To Parse Data (cont.)

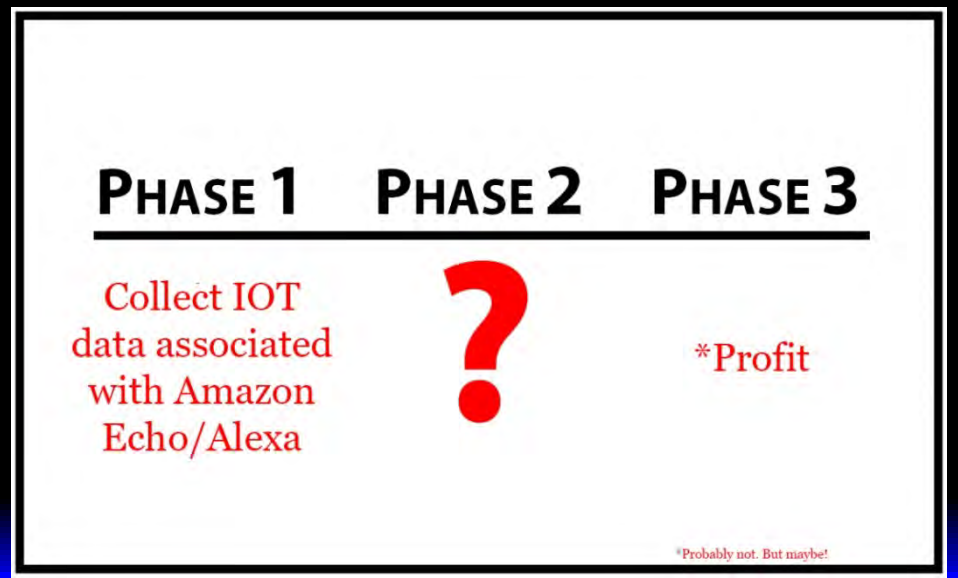
- Currently parses Alexa and Kasa related databases
  - Presents data under “Extracted Content”



Source File	createdOn	deviceAlias	deviceCategory	deviceModel	deviceName	deviceType
iot.1.db	2017-09-05 17:42:32	KasaCam	camera	KC120	Kasa Cam	IOT.IPCAMERA
iot.1.db	2017-10-02 14:09:34	Downstairs Black Lamp Light	lightBulb	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Living Room Green Lamp Light	lightBulb	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Kichen Sink Two	lightBulb	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Bedroom Plant Bulb	lightBulb	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Deck Lamp Light Bulb	lightBulb	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Porch Outlet Light Switch	switch	HS200(US)	Wi-Fi Smart Light Switch	IOT.SMARTPLUGSWITCH
iot.1.db	2017-10-02 14:09:34	Jill's Panda Lamp Light	lightBulb	LB120(US)	Smart Wi-Fi LED Bulb with Tunable White Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Downstairs Couch Light	switch	HS100(US)	Wi-Fi Smart Plug	IOT.SMARTPLUGSWITCH
iot.1.db	2017-10-02 14:09:34	Dino Light Bulb	lightBulb	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Couch Lamp Light	lightBulb	LB100(US)	Smart Wi-Fi LED Bulb with Dimmable Light	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:34	Kitchen Sink One	lightBulb	LB130(US)	Smart Wi-Fi LED Bulb with Color Changing	IOT.SMARTBULB
iot.1.db	2017-10-02 14:09:35	Upstairs Plant Outlet	switch	HS100(US)	Wi-Fi Smart Plug	IOT.SMARTPLUGSWITCH
iot.1.db	2017-10-02 14:09:35	Downstairs Fireplace Plant Light	switch	HS100(US)	Wi-Fi Smart Plug	IOT.SMARTPLUGSWITCH
iot.1.db	2017-10-02 14:09:35	Malware Lair Smart Plug	rangeExtender	RE370K(US)	AC1200 Wi-Fi Range Extender with Smart Plug	IOT.RANGEEXTENDER.SM

The Road Ahead

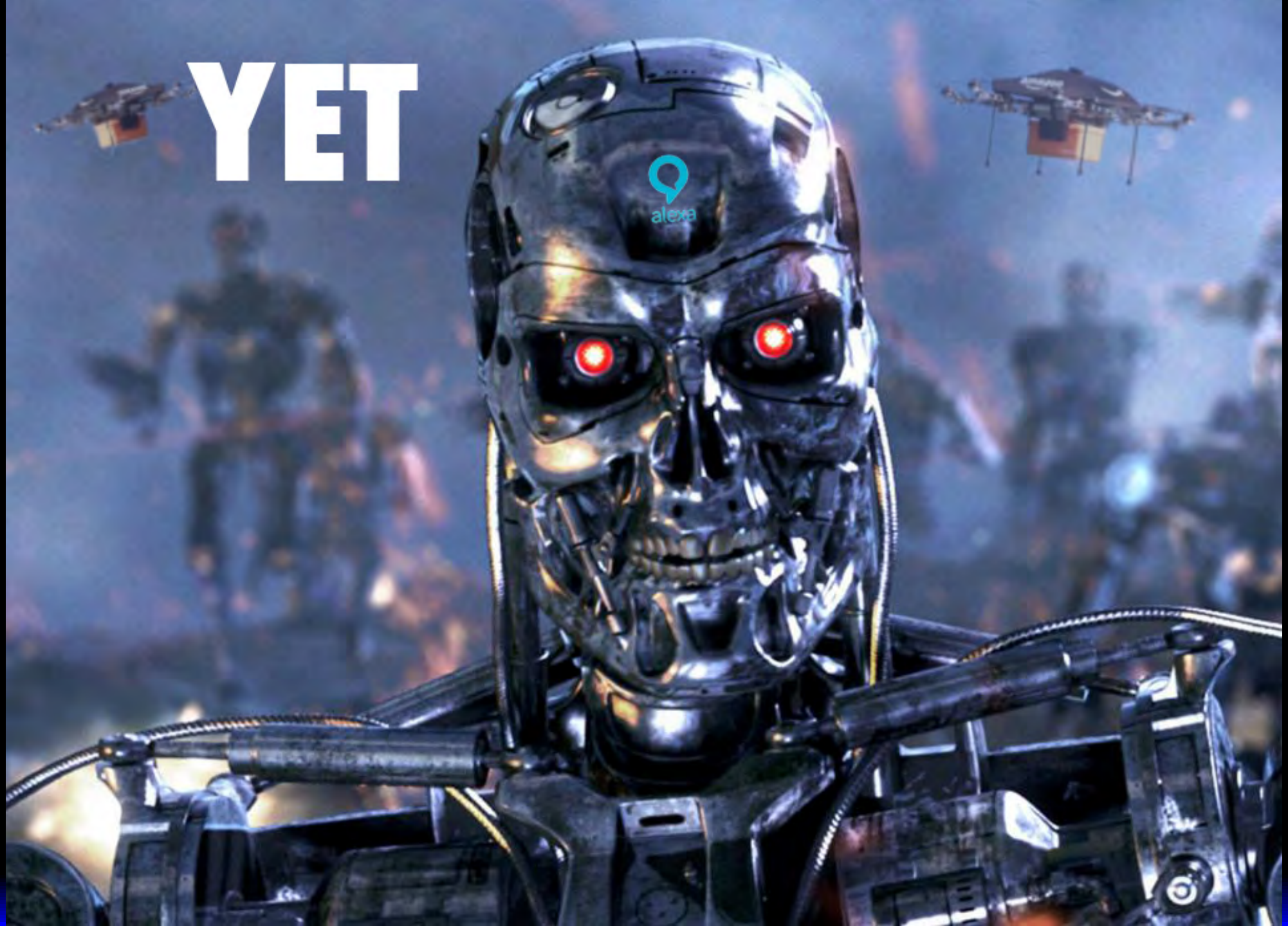
- Add iOS device testing
- Enhance scripts, plugins, and applications to parse the SQLite and JSON data
- Continue to help ensure applications are working in as secure a manner as possible



Summary

- Alexa data is stored primarily in the cloud
  - Very little is available offline
- The kasa/TP-Link application stores a ton of useful data in plain-text
  - But not as much thanks to our research!
- Account credentials are all that is needed to control smart home devices from anywhere
- Connected applications (Alexa's "skills") however likely contain a good amount of data
- Amazon's security team is really on top of things!
- TP-Link also takes smart home security very seriously!

- Alexa is not quite Skynet …


YET
alexa

Questions?

Contact Us!

Jessica Hyde
Twitter: *@B1N2H3X*
Email: Jessica.hyde@magnetforensics.com

Brian Moran
Twitter: *@brianjmoran*
Email: *brian@brimorlabs.com*