

GETTING SPOOKY WITH APOLLO

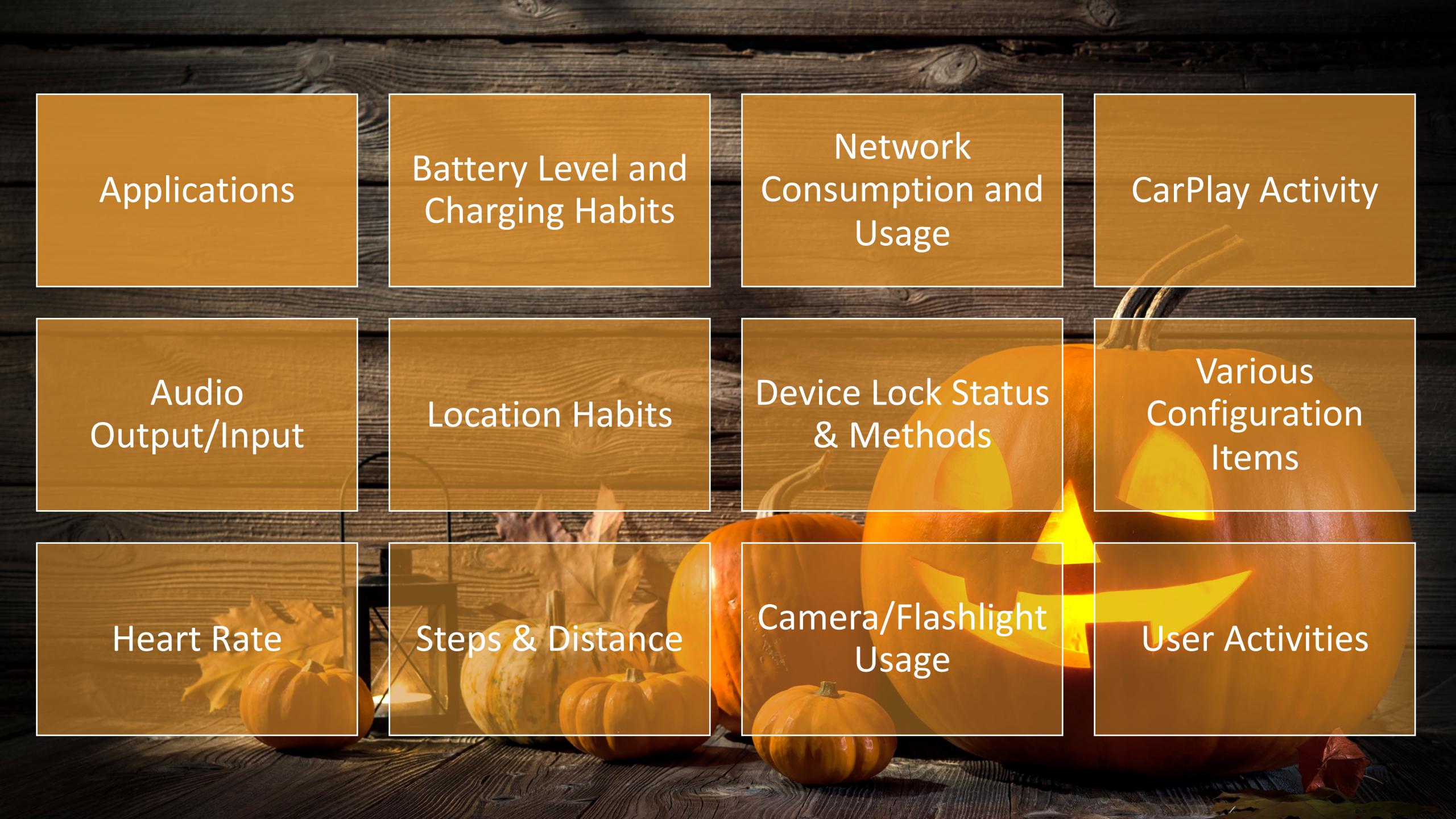


Sarah Edwards | @iamevl twin

mac4n6.com | for518.com

github.com/mac4n6/APOLLO





Applications

Battery Level and Charging Habits

Network Consumption and Usage

CarPlay Activity

Audio Output/Input

Location Habits

Device Lock Status & Methods

Various Configuration Items

Heart Rate

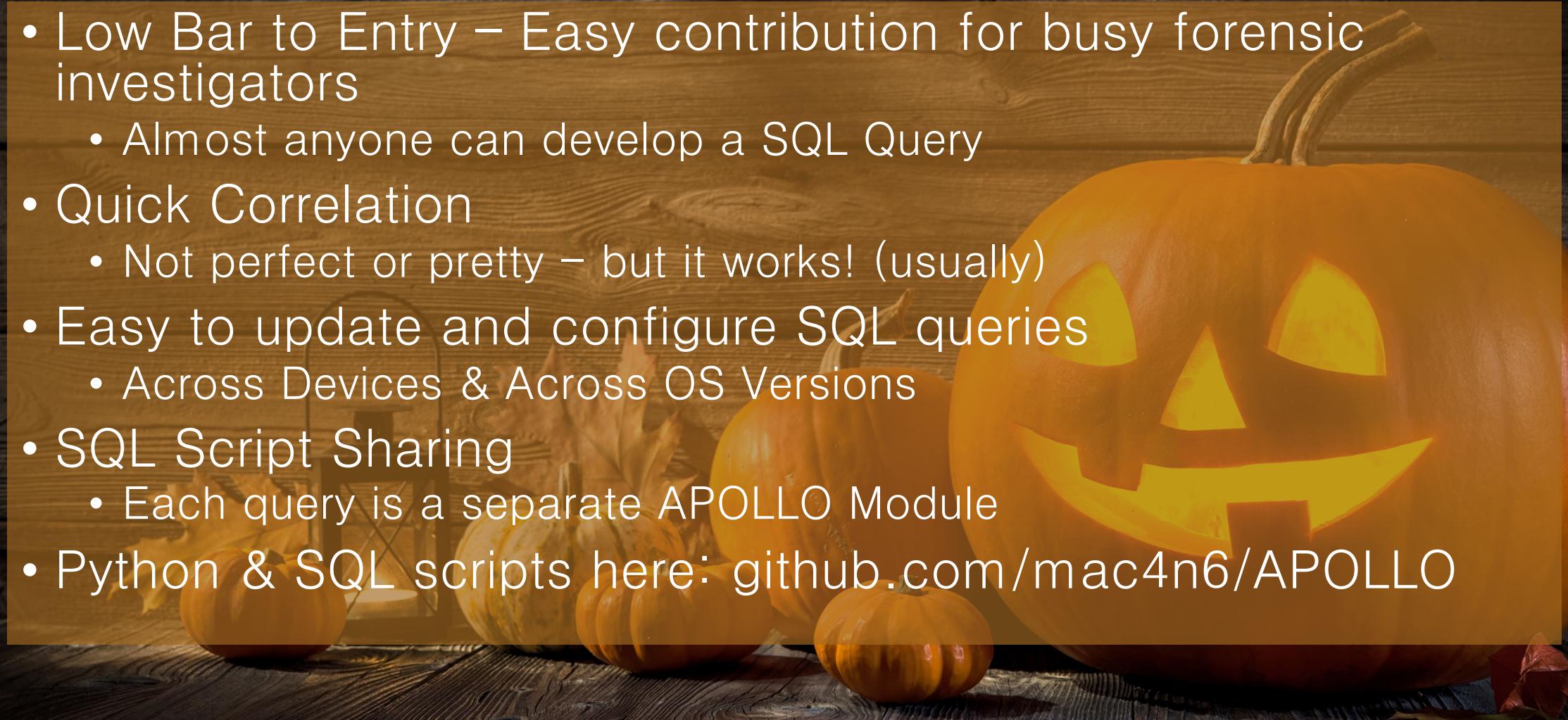
Steps & Distance

Camera/Flashlight Usage

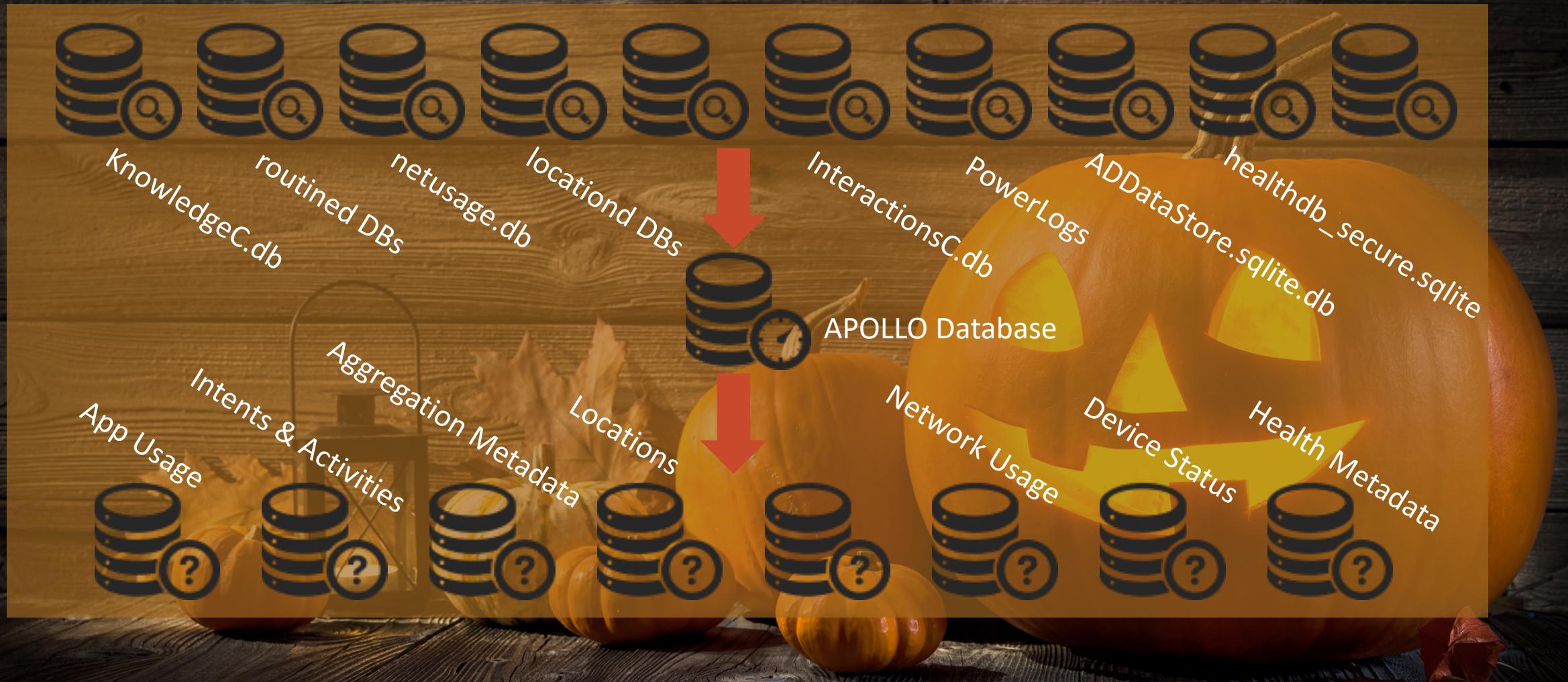
User Activities

APPLE PATTERN OF LIFE LAZY OUTPUT'ER

- Low Bar to Entry – Easy contribution for busy forensic investigators
 - Almost anyone can develop a SQL Query
- Quick Correlation
 - Not perfect or pretty – but it works! (usually)
- Easy to update and configure SQL queries
 - Across Devices & Across OS Versions
- SQL Script Sharing
 - Each query is a separate APOLLO Module
- Python & SQL scripts here: github.com/mac4n6/APOLLO



HOW DOES IT WORK?



SPOOKY STORY TIME !

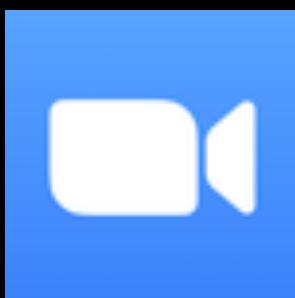
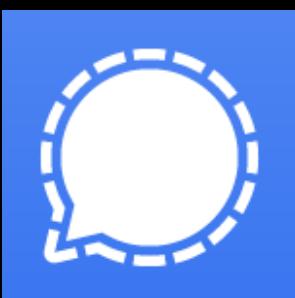
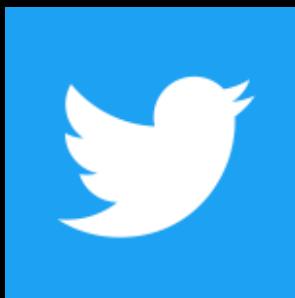




SO YOU'RE PLANNING A
HALLOWEEN PARTY...

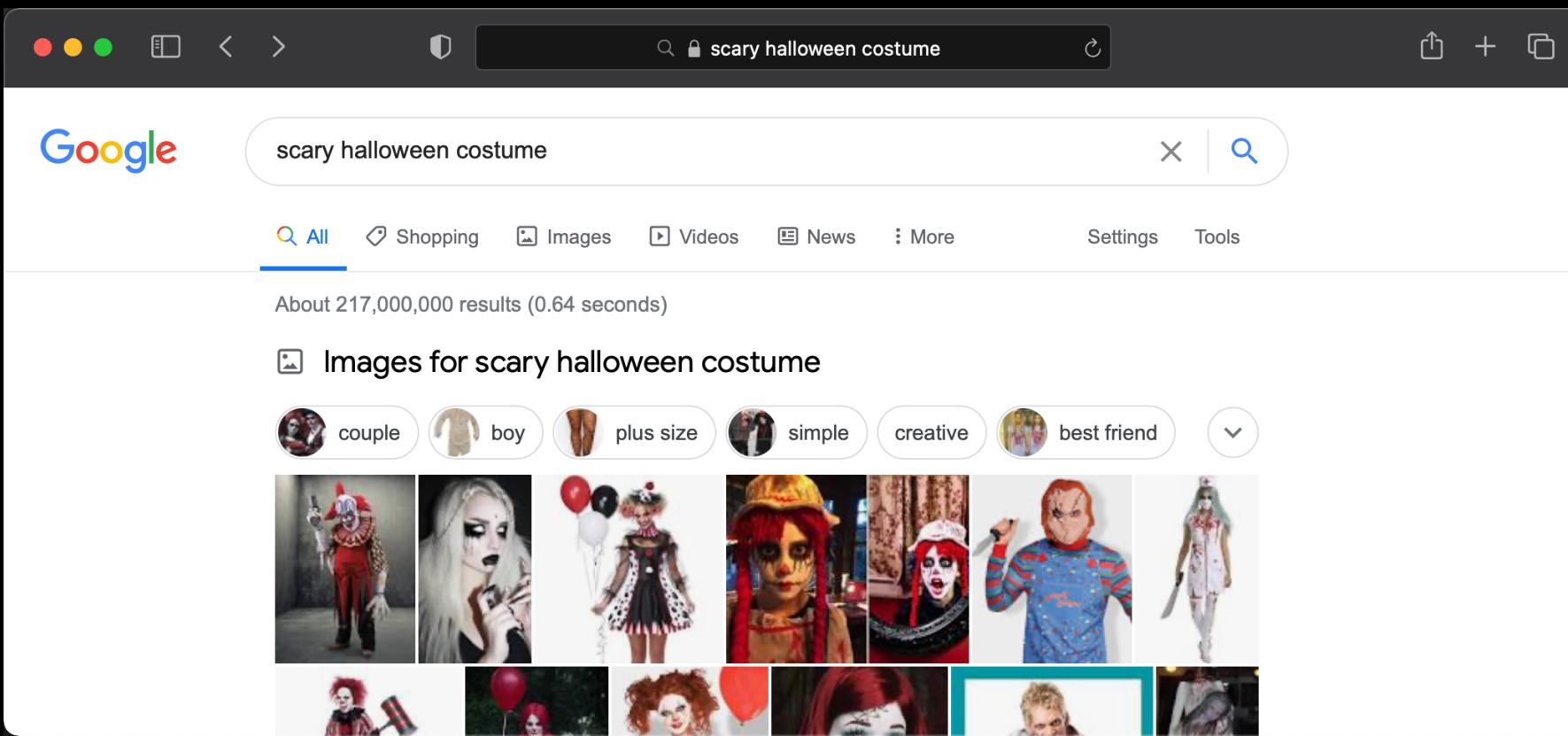
INVITE YOUR FRIENDS

- knowledgeC.db
 - App In Focus/App Usage (Synced)
 - App Activity
 - Access Email Mailbox
 - View Phone Contact Card
 - Twitter Browsing
 - App Intents
 - Phone Calls
 - Created Calendar Entry
 - Messages Sent
 - Twitter DM's
 - WhatsApp Message & Call
 - App Web Usage (I see you doom scrolling!)
 - Also synced!
- Power Log
 - App Frontmost (macOS)
 - App Usage
- InteractionC.db
 - Contact Interactions via Phone, Email, Messages
- CallHistory.storeddata
- sms.db - iMessage, SMS, FaceTime



FIND A COSTUME

- History.db – Synced (but which device?)
- knowledgeC.db – App Activity (Safari), App Web Usage (Synced, with HW UUID), Safari Browsing



GET SOME PARTY FIXINS'



- Passes23.sqlite – Purchases made at Grocery Store, Home Depot, Liquor Store, Farmers Market using Apple Wallet and/or Apple Pay
- knowledgeC.db
 - App Intents
 - Add item in “Super Fun Halloween Party” List in Reminders
 - App Activity
 - Safari Queries
 - Credit Cards Used
 - App Web Usage
 - How long were you contemplating the giant skeleton purchase?

The screenshot shows a product page from homedepot.com. The URL in the address bar is homedepot.com. The page title is "12 ft. Giant-Sized Skeleton with LifeEyes". The product is described as a "Best Seller" by Home Accents Holiday. It has a rating of 4.5 stars from 313 reviews. The price is \$299.00, with suggested payments of \$50.00 per month for 6 months. The product is an animated skeleton with glowing blue eyes. There are several smaller images and video thumbnails on the left side of the main product image.

Internet #312513260 Model #5124738 Store SKU #1005309103

12 ft. Giant-Sized Skeleton with LifeEyes
by Home Accents Holiday > Shop the Collection >

★★★★★ (313) Write a Review Questions & Answers (171)

Makes a spine-tingling centerpiece for Halloween
Animated LCD eyes create a creepy effect
Designed for indoor or outdoor use
See More Details

\$299⁰⁰

OR

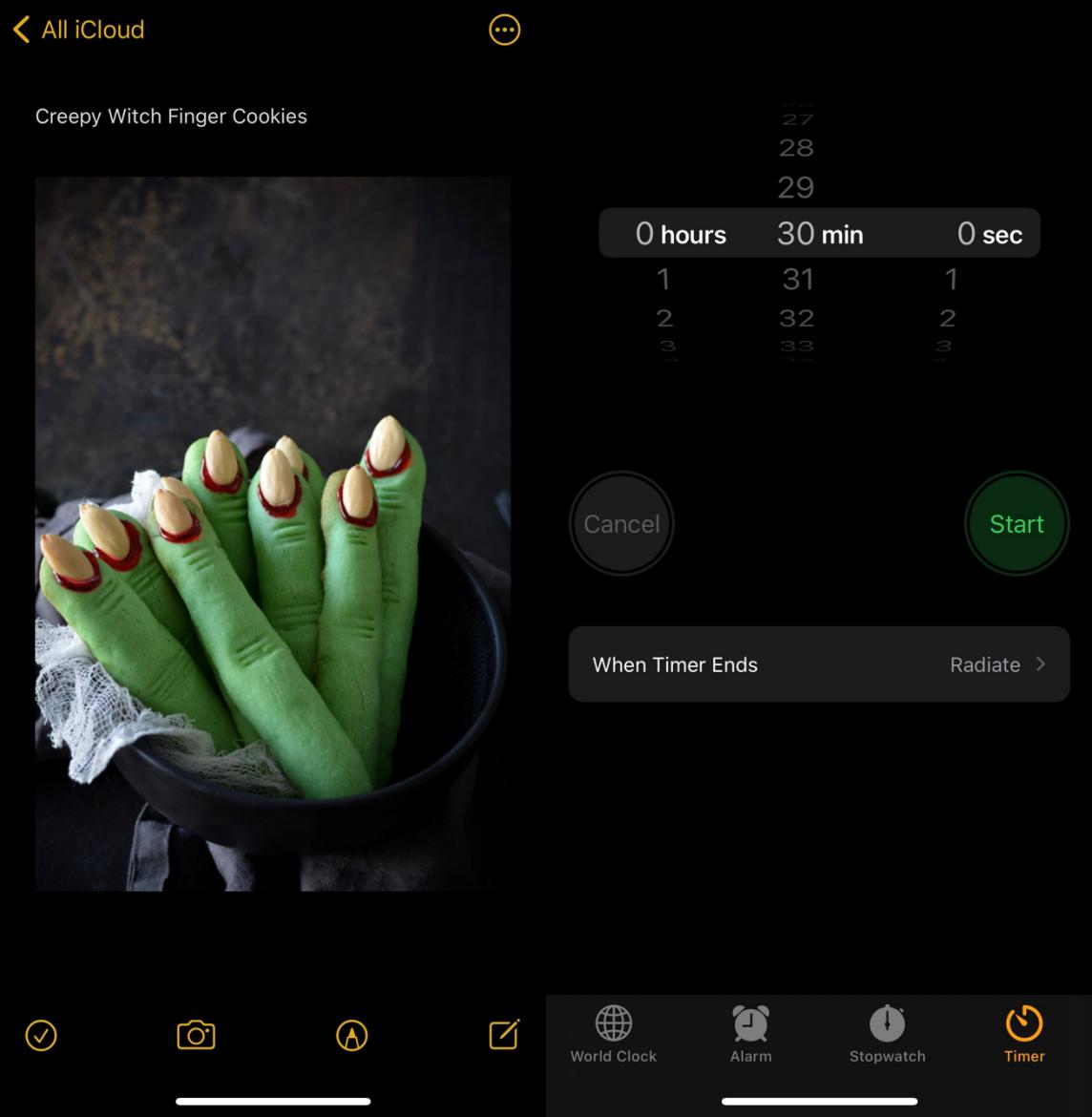
\$50⁰⁰ per month* suggested payments with 6 months* financing on this \$299 purchase* i

Apply for a Home Depot Consumer Card

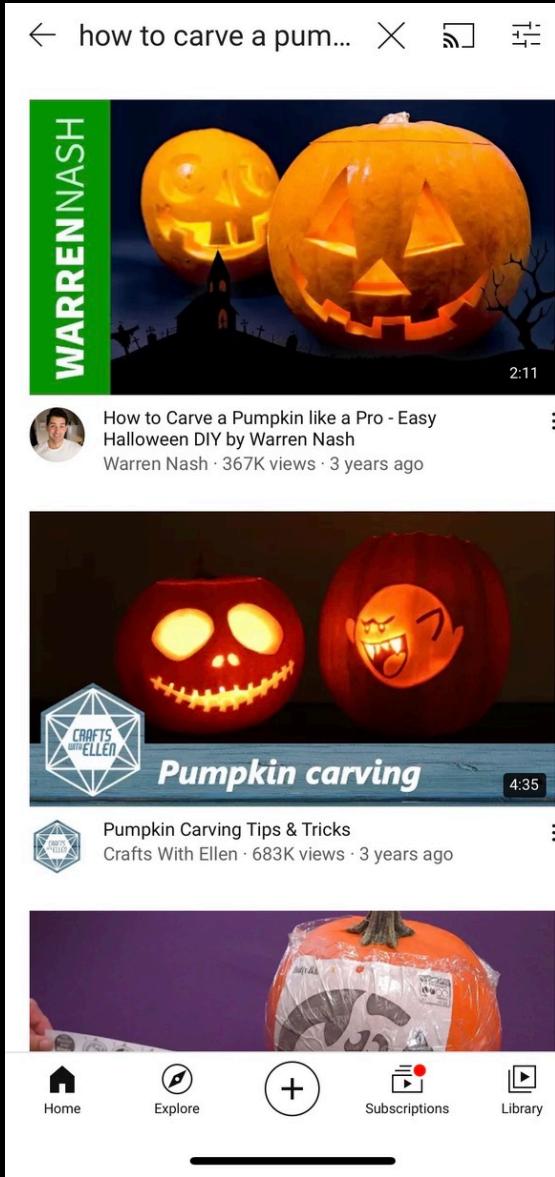
Live Chat

Feedback

BAKE COOKIES & CARVE PUMPKINS!

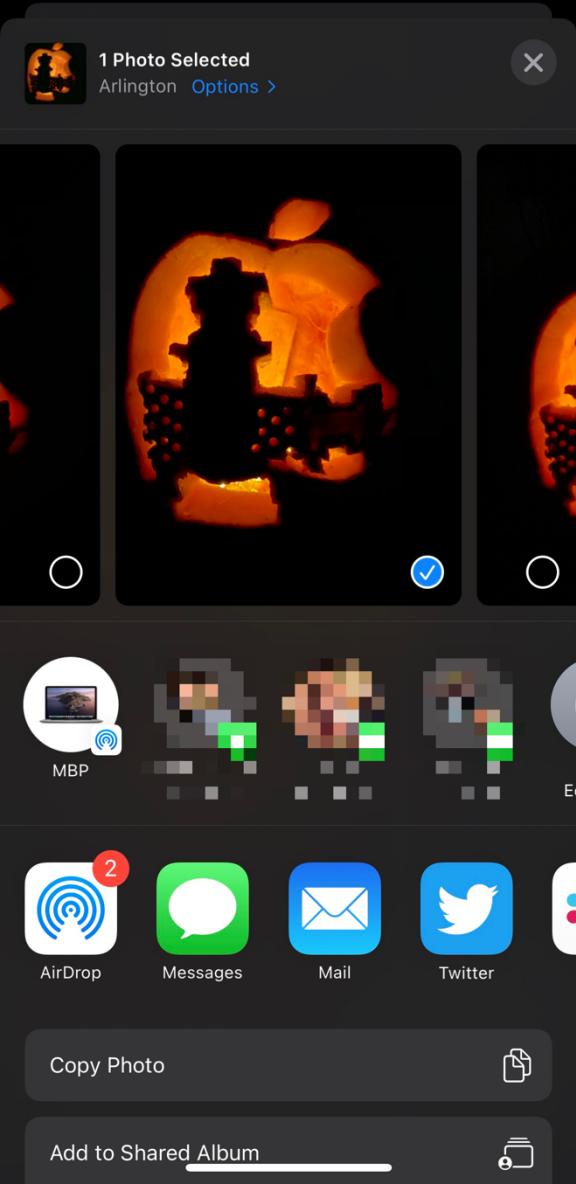


- knowledgeC.db
 - App Activity
 - Safari
 - “Creepy Witch Finger Cookies”
 - Edit recipe in Notes
 - YouTube Search
 - “How to carve...”
 - Viewing photos of last year’s party and the pics you just took of your pumpkins.
 - App Intent
 - Set Timer for cookies

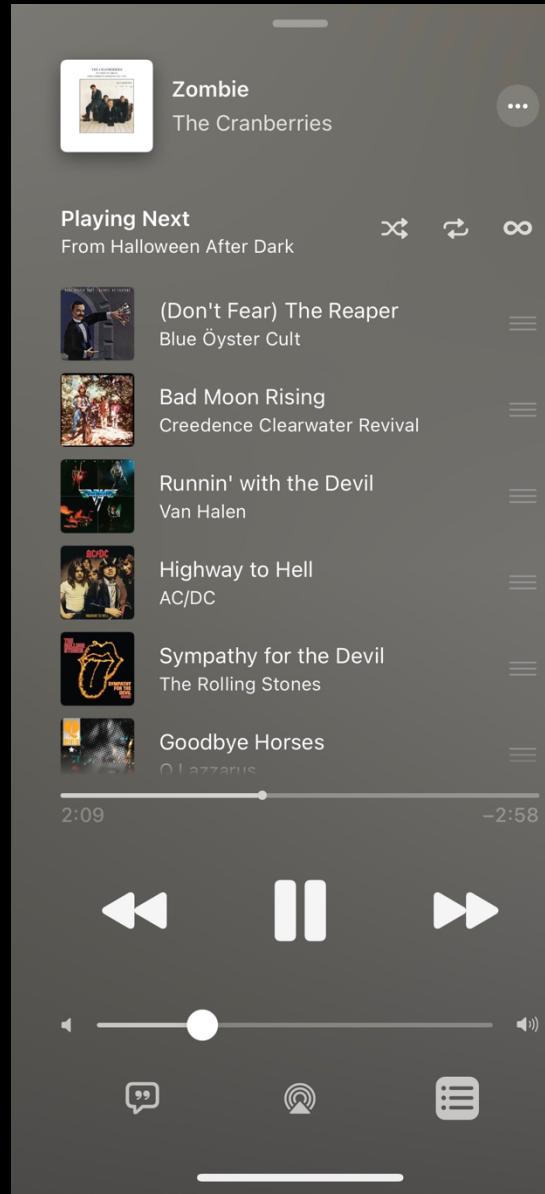


CHILLIN' AT THE PARTY

GOT A KILLER PLAYLIST & HANGIN' WITH FRIENDS



- knowledgeC.db
 - App Intent – Start Halloween Playlist in Music
 - App in Focus – Taking photos
 - Lock screen camera scroll and/or Camera app
 - App In Focus – Airdrop photos
 - Audio Bluetooth Connected – Bluetooth Speaker
 - Audio Output Route – Bluetooth, Speaker
 - Audio Media Now Playing – App & Media Metadata
 - Did you skip a song?
- Power Log
 - Airdrop – Which app did the Airdropping
 - App Audio – App, Output Device, Start/Stop>Status
 - App Now Playing – App, On/Off
 - Camera State – On/Off, Front/Back



LET'S DO THE TIME WARP!

- healthdb_secure.sqlite
 - Dance Workout
 - Location
 - Weather
 - Calories
 - Elevated Heart Rate
- knowledgeC.db
 - App Activity Health – Checked your step count

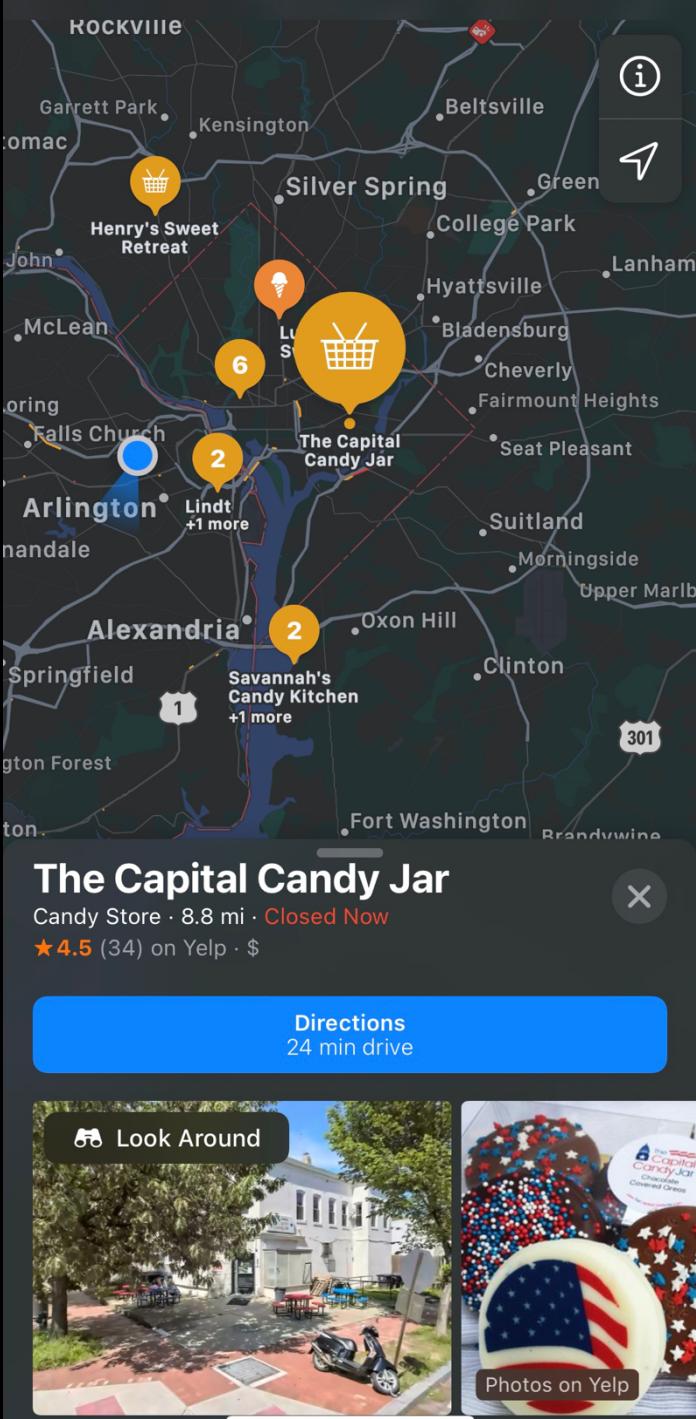


MOVIE TIME!

- knowledgeC.db – Also on Apple TV!
 - App In Focus (Netflix, TV, HBO, Disney+)
 - Now Playing – The Nightmare Before Christmas



OH NO!
YOU RAN OUT OF CANDY CORN!



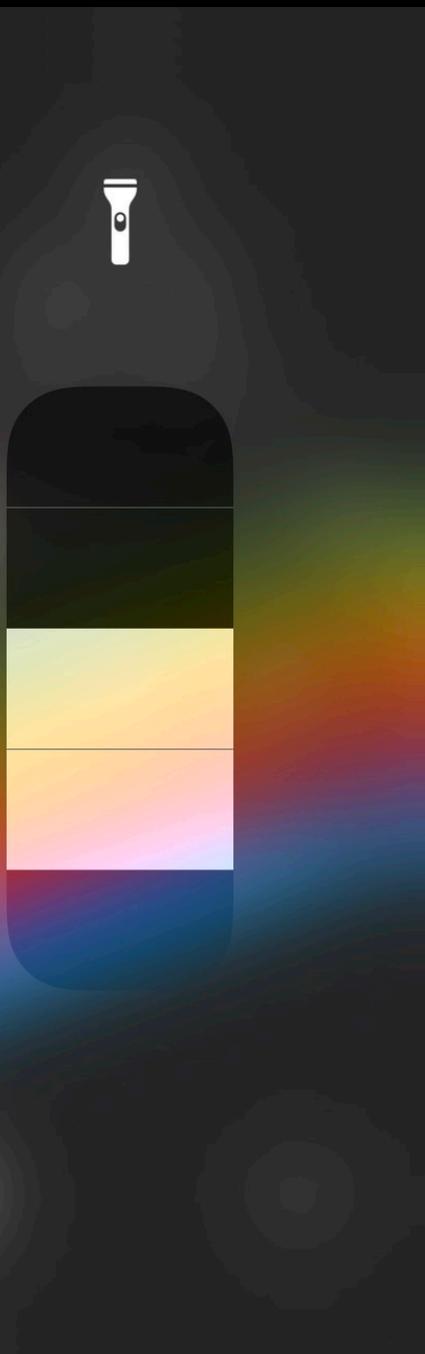
HOP IN THE CAR & FIND DIRECTIONS TO THE CANDY STORE

- knowledgeC.db
 - App Activity – Maps “Candy Store”
 - App Intents – Used Siri for Navigation Search
 - Device Plugged In
 - Device CarPlay Connected
 - Audio Input Route – CarPlay
- cache_encryptedC.db (locationd)
 - Motion State History – In/Out of Vehicle, Moving/Non-moving
- Power Log - App Usage (CarPlay)

KILLER PLAYLIST BACK ON

- KnowledgeC.db
 - Audio Media Now Playing – App & Media Metadata
 - Audio Output Route – Speaker, CarPlay
- Power Log
 - App Now Playing
 - Audio Routing (Phone, Speaker, Siri, etc)
 - Audio Volume - Volume
 - Device Volume or Volume Level – Volume, Muted or Not
- Routined
 - Cache.db (ZRTCLLocationMo) – Granular location, Speed, Course, Accuracy





YOU GET LOST & POP A TIRE

- Routined
 - Cache ZRTCLLocationMo – Granular location, Speed, Course, Accuracy
- cache_encryptedC.db (locationd)
 - Motion State History – In/Out of Vehicle, Moving/Non-moving
- Power Log
 - Torch State
- knowledgeC.db
 - App Usage
 - App Activity – Safari “how to change a tire”
 - App Web Usage
 - Safari Browsing

AA Q how to change a tire ⌂

Google

how to change a tire

ALL VIDEOS IMAGES SHOPPING NEWS

on a car on a truck on a travel trailer on a S

THESE ITEMS SHOULD HAVE COME WITH YOUR VEHICLE
CAR OWNER'S MANUAL
WHEEL CHOCKS
JACK
JACK STANDS
SPARE TIRE
TIRE PRESSURE GAUGE

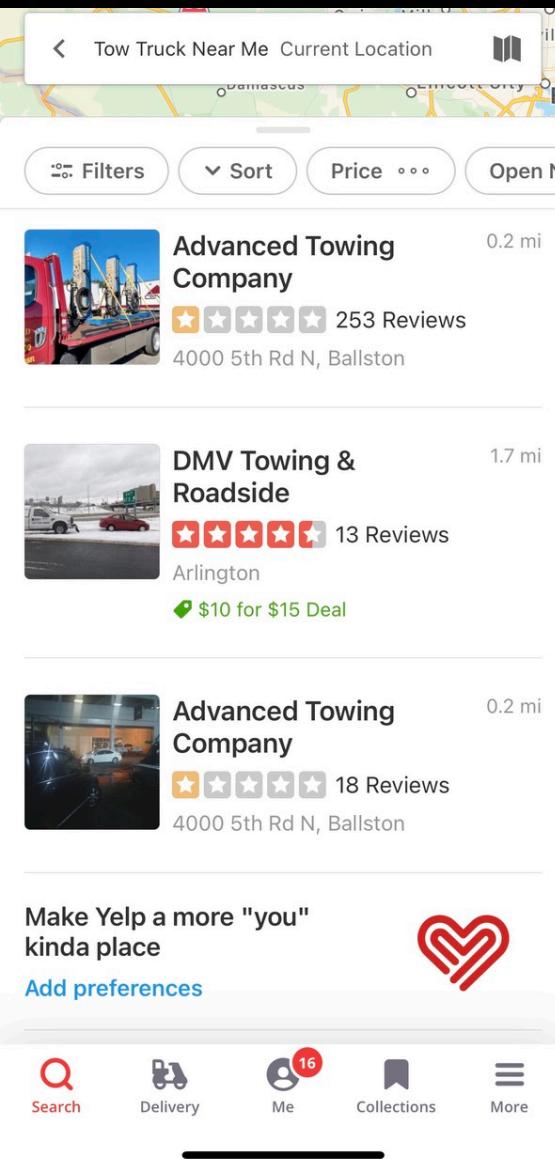


Below, I've broken down how to change a tire in 10 simple steps.

1. Find a Safe Place to Pull Over. ...
2. Use Your Hazard Lights and Parking Brake. ...
3. Check for Materials. ...
4. Loosen the Lug Nuts. ...
5. Lift Your Vehicle Off the Ground. ...
6. Remove the Lug Nuts and the Tire. ...

< > ⌂ ⌚ ⌚

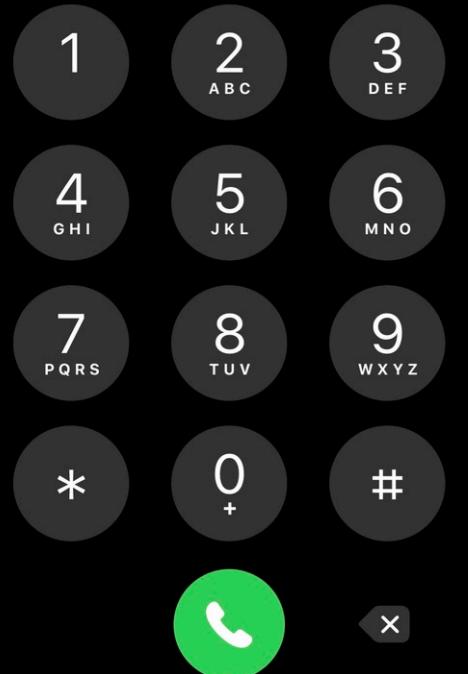
GIVE UP, CALL FOR A TOW TRUCK



1 (800) 555-1337

[Add Number](#)

- CallHistory.storedData
 - Can't make a call, attempts but no service!
- Power Log
 - Device Telephony Activity – Call Status (Ringing, etc.), Signal Bars, Airplane Mode
 - Device Telephony Registration – Network (AT&T, GoogleFi, etc.)
 - In Call Service – App (Phone, FaceTime, 3rd Party), Call Status (Background, Foreground, Start/Stop), Video On/Off



VISIT CREEPY HOUSE AT THE TOP OF A HILL

- healthdb_secure.sqlite
 - Flights of Stairs
 - Elevated Heart Rate
- cache_encryptedC.db (locationd)
 - Step Count History – Floors Ascended/Descended
- Routined
 - Cache ZRTCLLocationMo – Granular location, Speed, Course, Accuracy



KNOCK ON THE DOOR, SCARY CLOWNS! RUN AWAY!

- cache_encryptedC.db (locationd)
 - Step Count History – Floors Ascended/Descended
- healthdb_secure.sqlite
 - Heart Rate
 - Steps & Distance
- Routined
 - Cache ZRTCLLocationMo – Granular location, Speed, Course, Accuracy
 - Running? How fast are you!?



BACK ON THE HIGHWAY...YOU CHOOSE TO HITCHHIKE

- 
- healthdb_secure.sqlite
 - Heart Rate – Calm yet?
 - Routined
 - Cache ZRTCLLocationMo
 - Granular location, Speed, Course, Accuracy
 - cache_encryptedC.db (locationd)
 - Motion State History – In/Out of Vehicle, Moving/Non-moving

DEAD BATTERY 😱

- knowledgeC.db
 - Device Battery Level
 - Device Plugged In
- Power Log
 - Battery Level
 - Battery Level UI
 - Lightning Connector Status – Plugged In or Not
- healthdb_secure.sqlite
 - Heart Rate – You Dead?
 - (When powered back up and synced from Apple Watch)





WAKE UP! IT WAS JUST A NIGHTMARE.

HOWEVER...YOU'RE STILL IN A NIGHTMARE

SHAMELESS SELF PROMOTION

- APOLLO – github.com/mac4n6/APOLLO
- FOR518 - SANS Mac and iOS Forensics and Incident Response
 - for518.com
- mac4n6.com
- [@iamevtwin](https://twitter.com/@iamevtwin)
- sarah@blackbagtech.com

