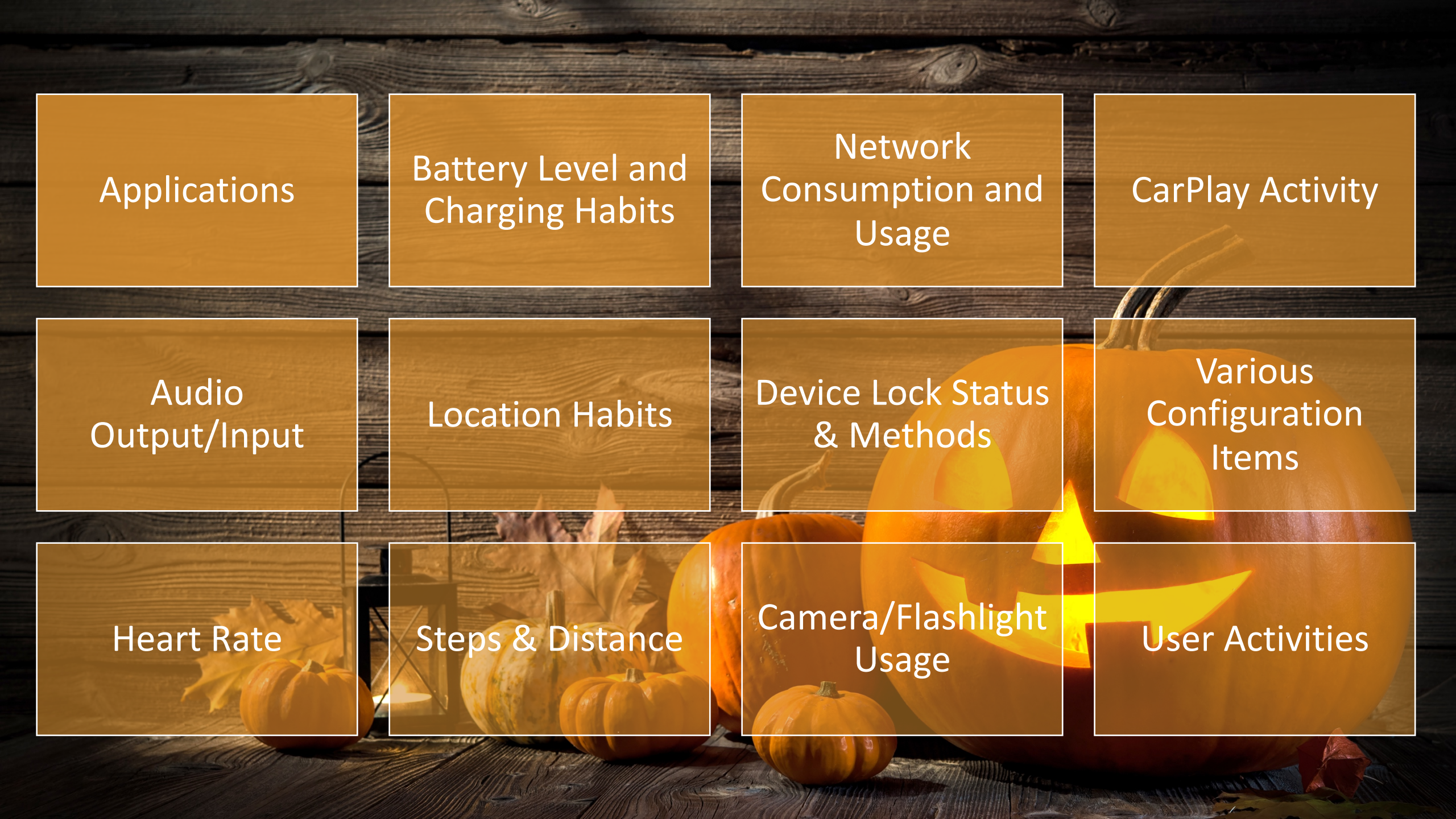
Getting Spooky with APOLLO

👻🚀🔎😳

Sarah Edwards | @iamevltwin

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!

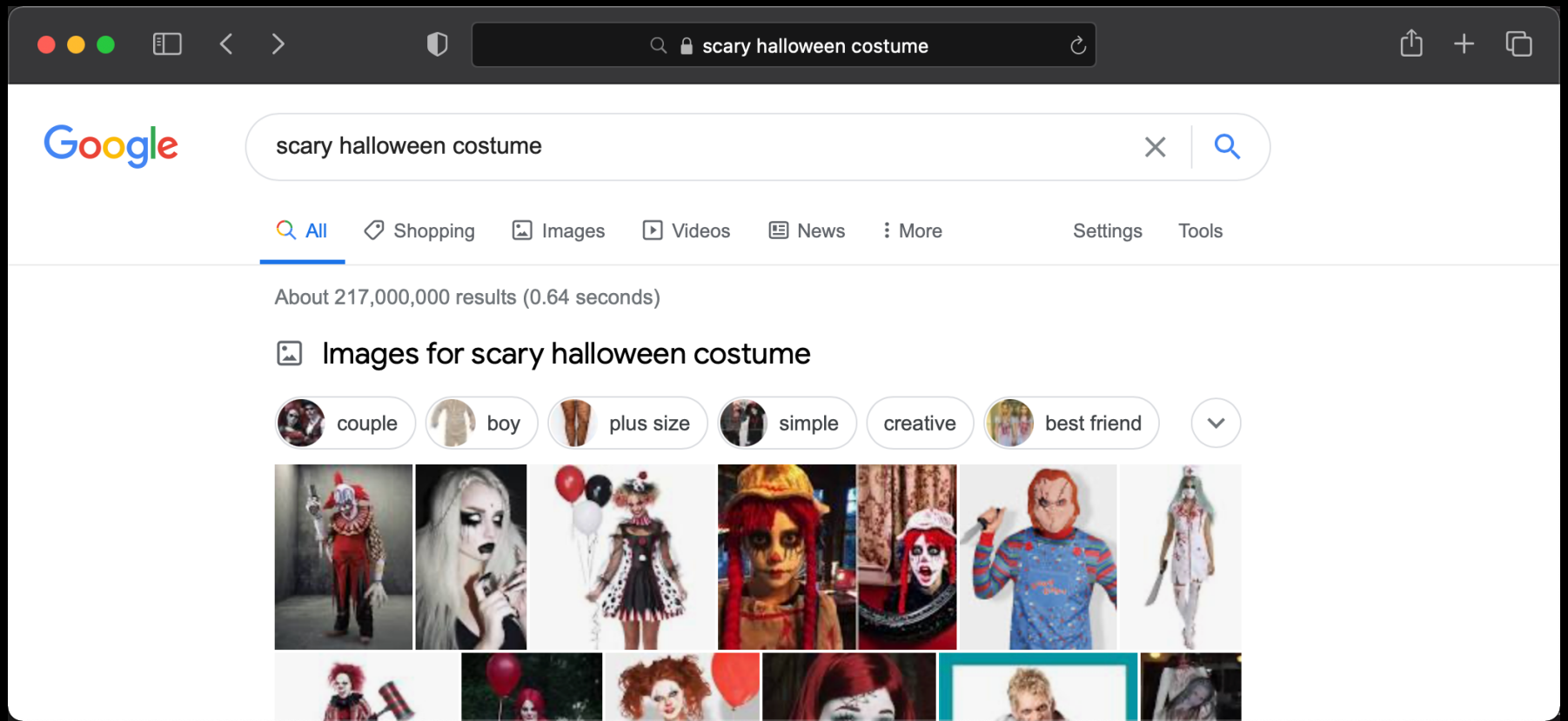

So You're Planning a
Halloween Party...

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.storedata
- sms.db - iMessage, SMS, FaceTime

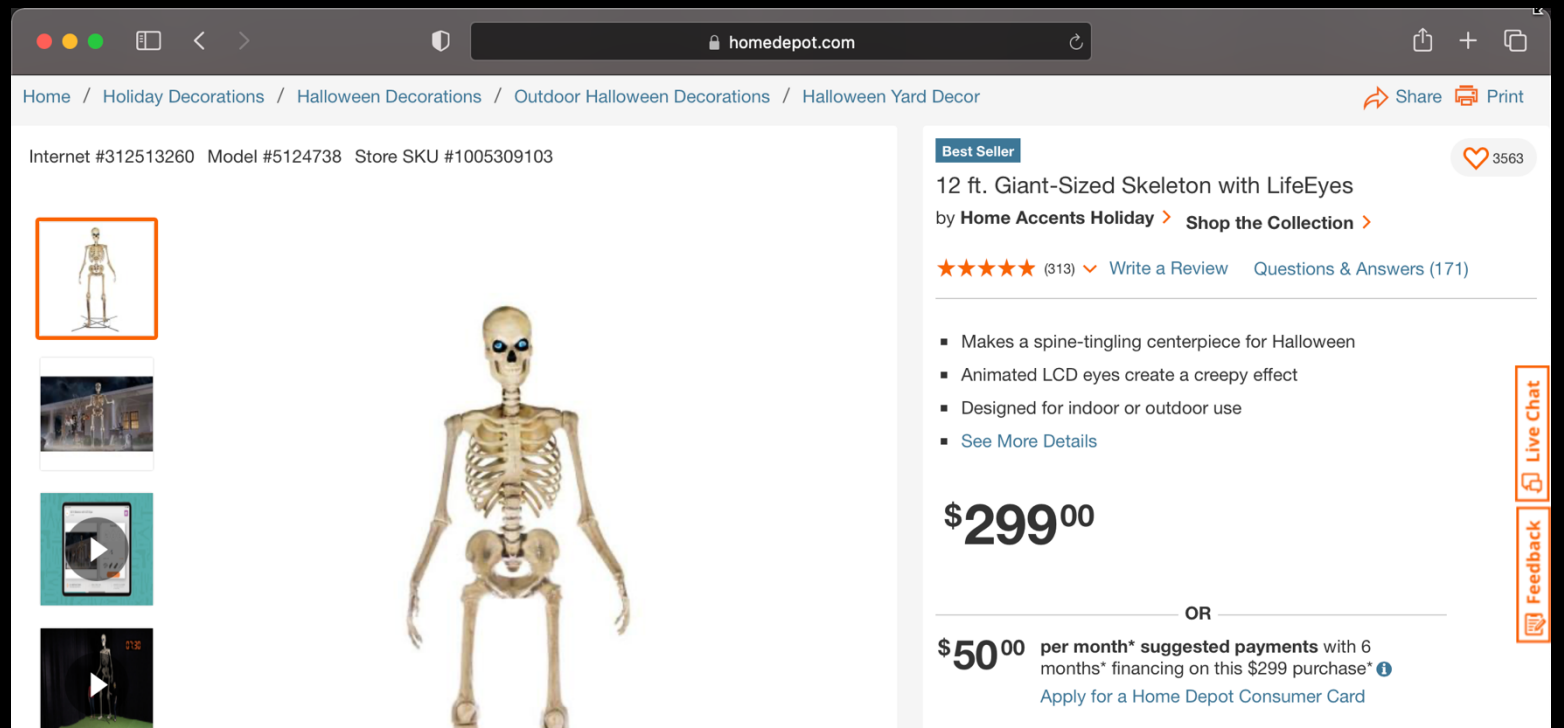
Find a Costume

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

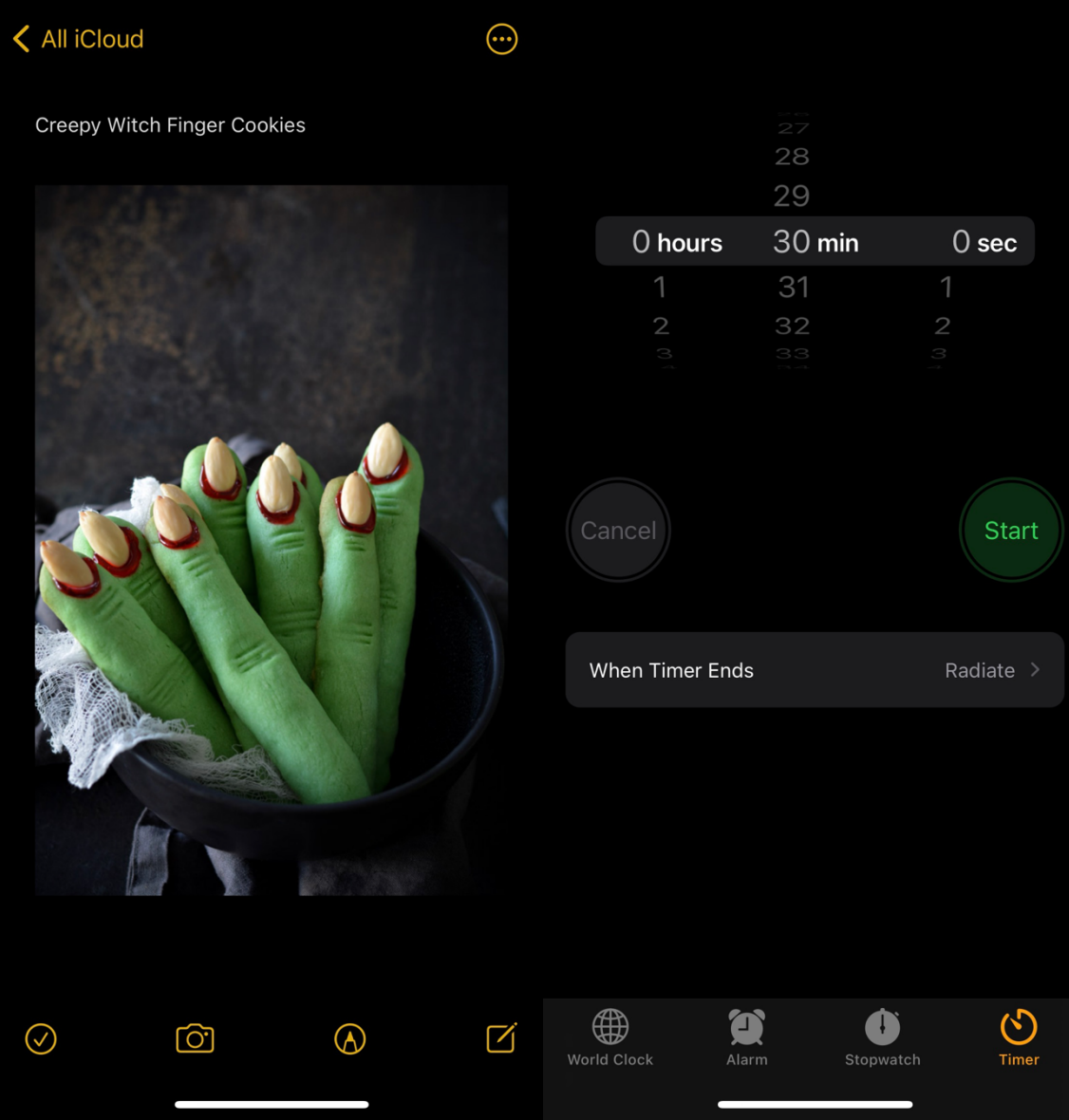


Get Some Party Fixins'

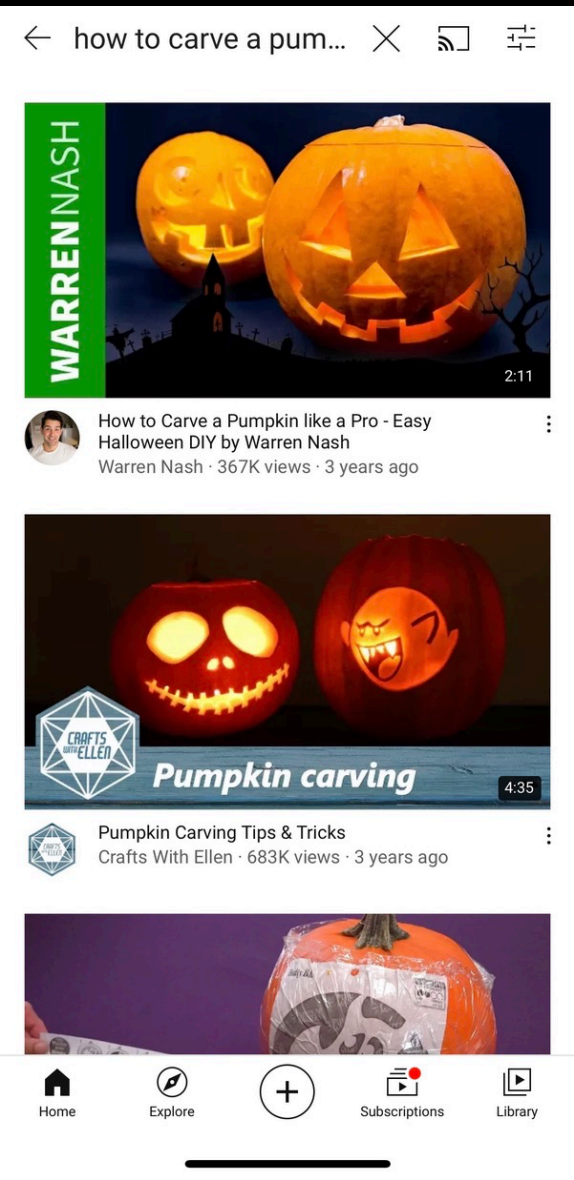
- Passes23.sqlite – Purchases made at Grocery Store, Home Depot, Liquor Store, Farmers Market using Apple Wallet and/or Apple Pay
- knowledgeC.db
  - App Intents
    - Add item in "Super Fun Halloween Party" List in Reminders
  - App Activity
    - Safari Queries
    - Credit Cards Used
  - App Web Usage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



Bake Cookies & Carve Pumpkins!

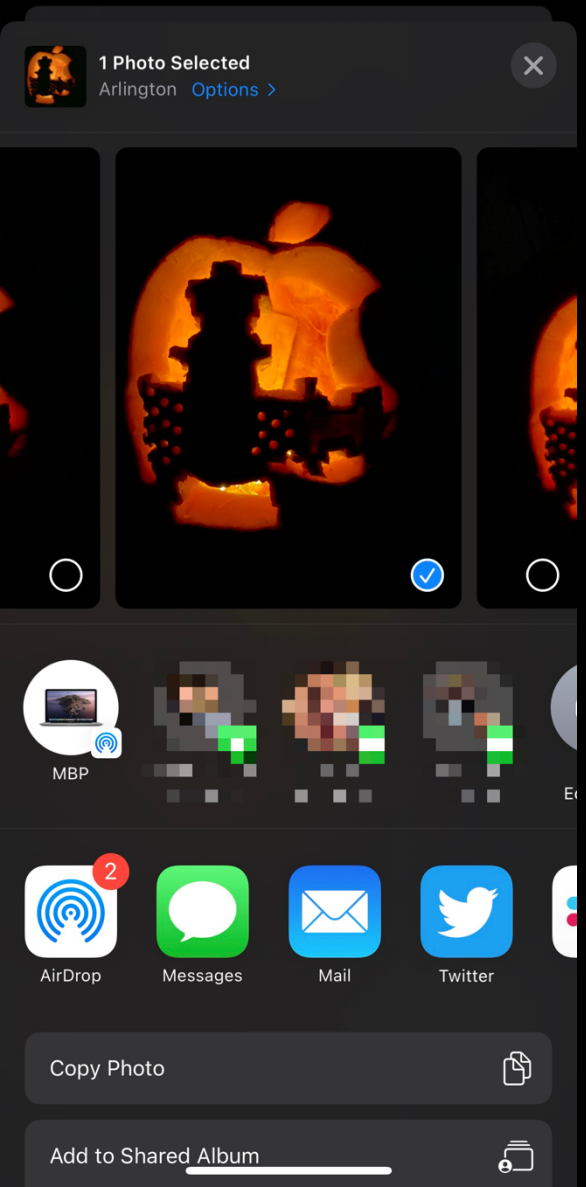


- knowledgeC.db
  - App Activity
    - Safari
      - “Creepy Witch Finger Cookies”
    - Edit recipe in Notes
    - YouTube Search
      - “How to carve…”
    - Viewing photos of last year’s party and the pics you just took of your pumpkins.
  - App Intent
    - Set Timer for cookies

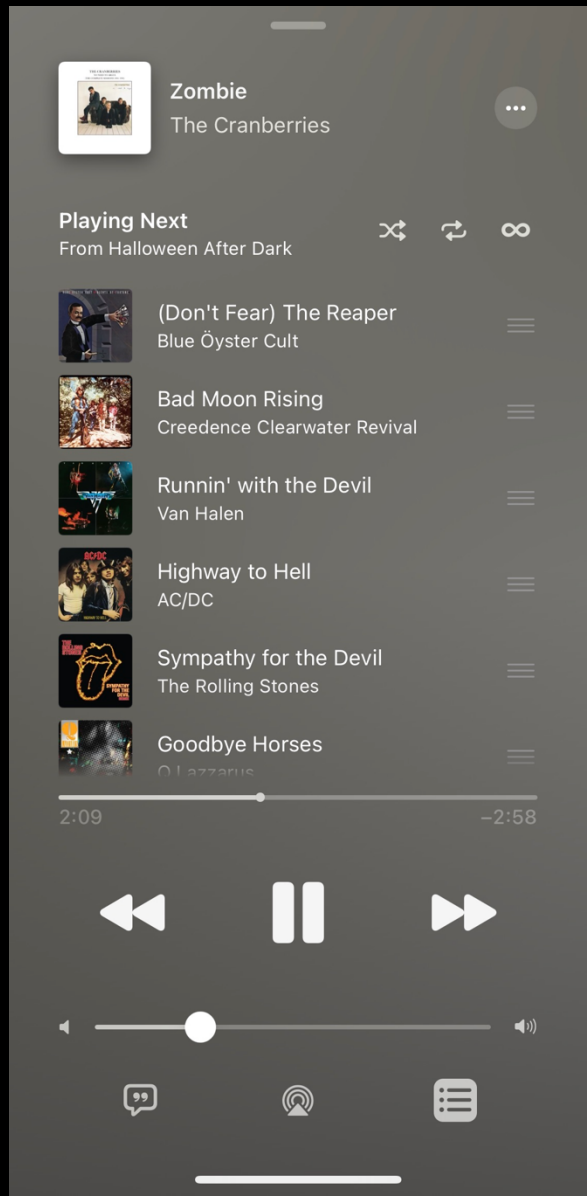


Chillin' At the Party

Got a Killer Playlist & Hangin' with Friends

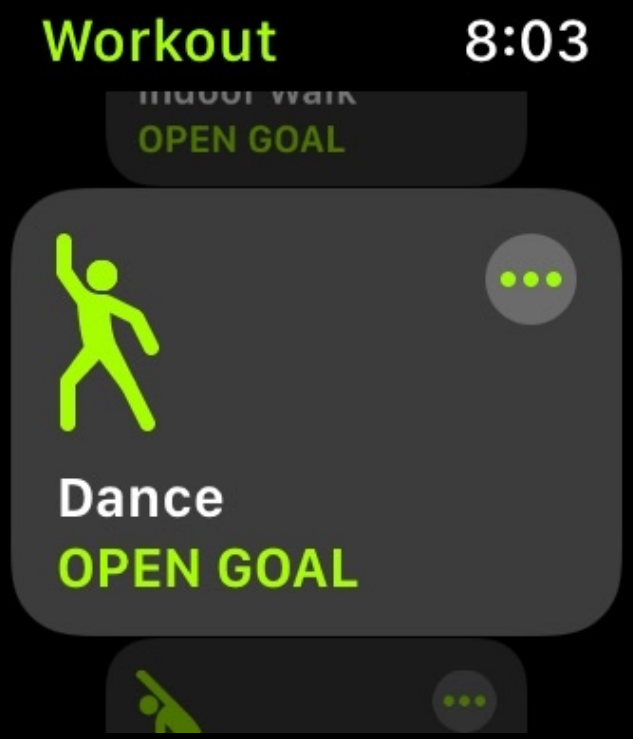


- knowledgeC.db
  - App Intent – Start Halloween Playlist in Music
  - App in Focus – Taking photos
    - Lock screen camera scroll and/or Camera app
  - App In Focus – Airdrop photos
  - Audio Bluetooth Connected – Bluetooth Speaker
  - Audio Output Route – Bluetooth, Speaker
  - Audio Media Now Playing – 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!

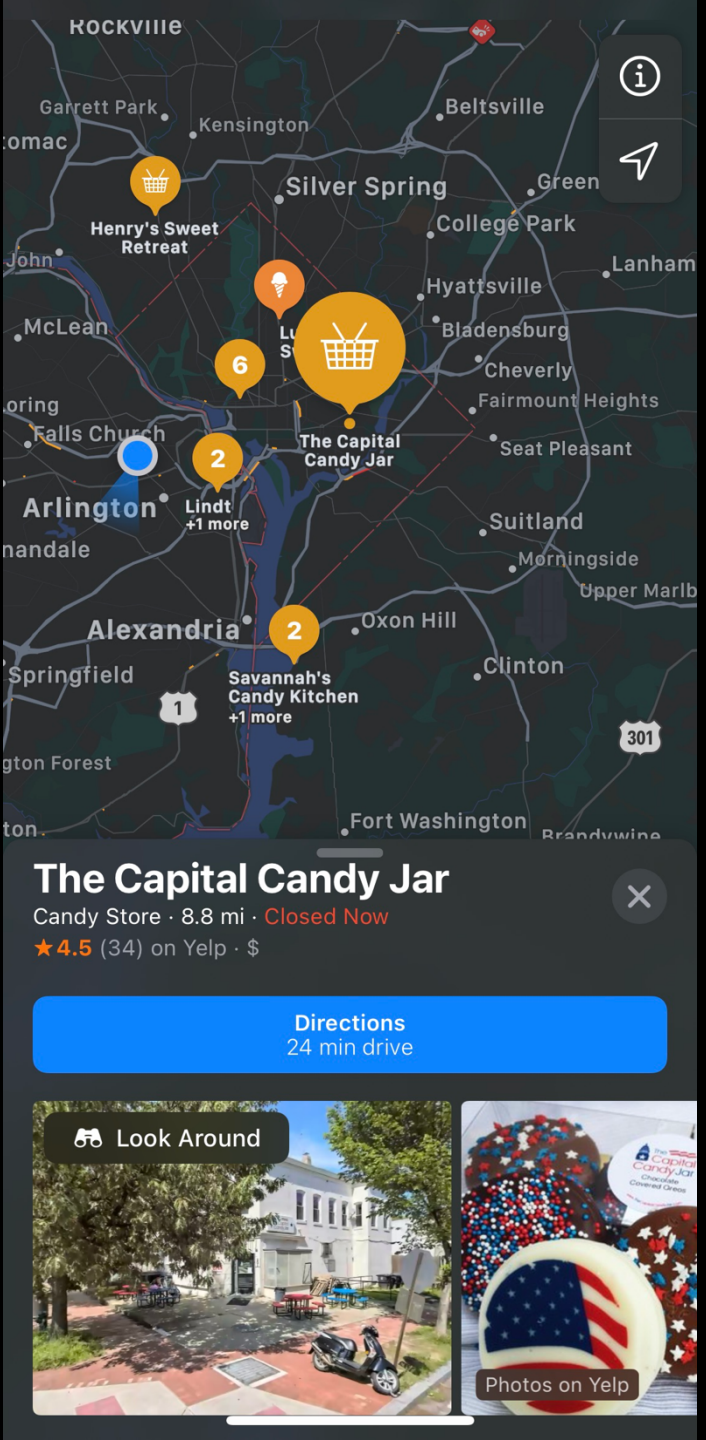
- healthdb_secure.sqlite
  - Dance Workout
    - Location
    - Weather
    - Calories
  - Elevated Heart Rate
- knowledgeC.db
  - App Activity Health – Checked your step count



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!

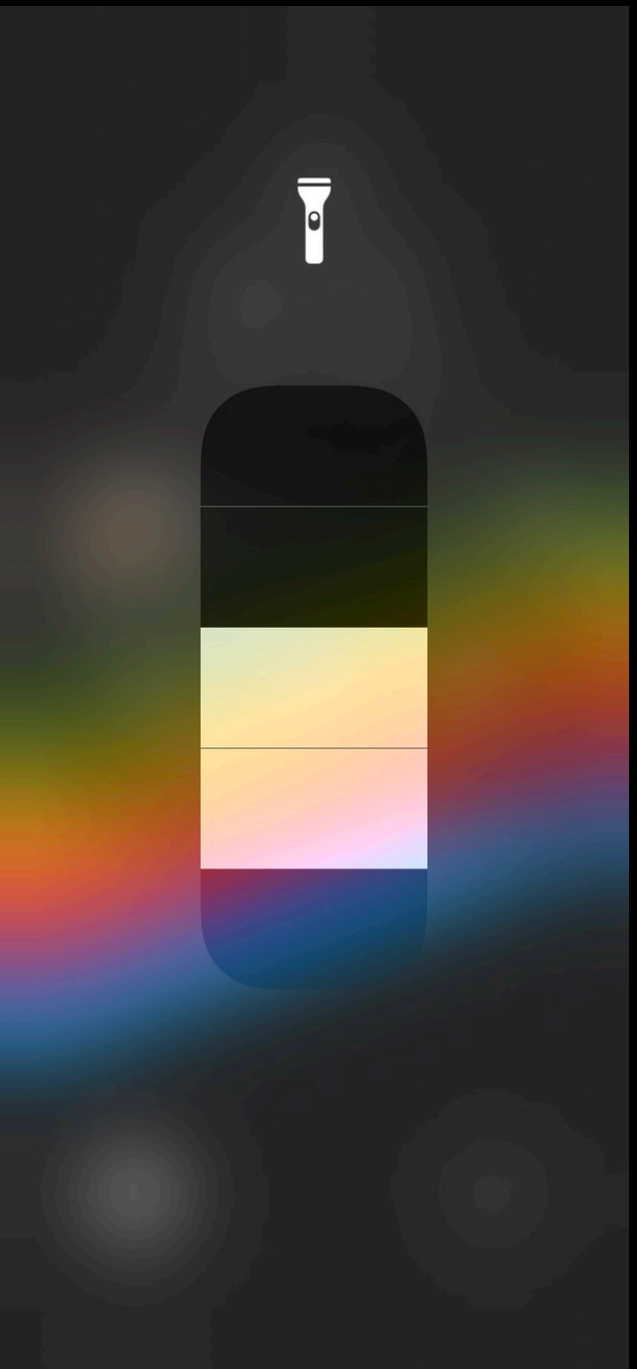


Hop in the Car & Find Directions to the Candy Store

- 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)

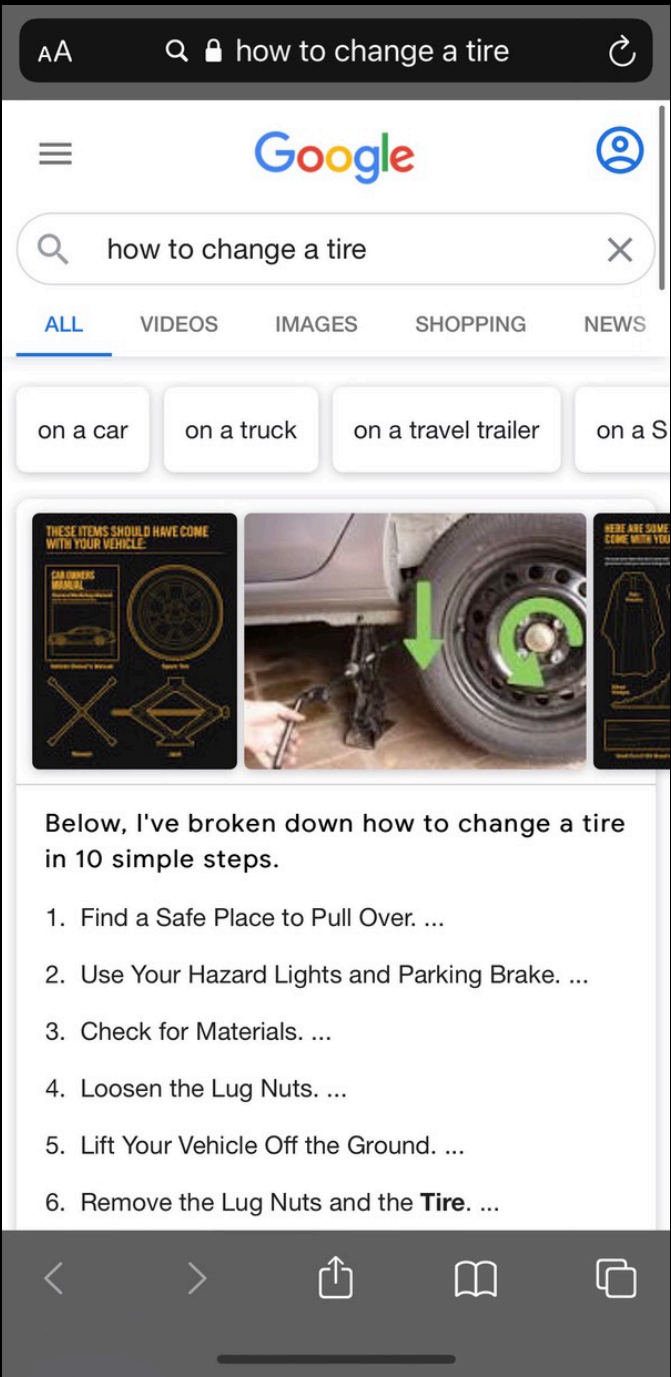
Killer Playlist Back On

- 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

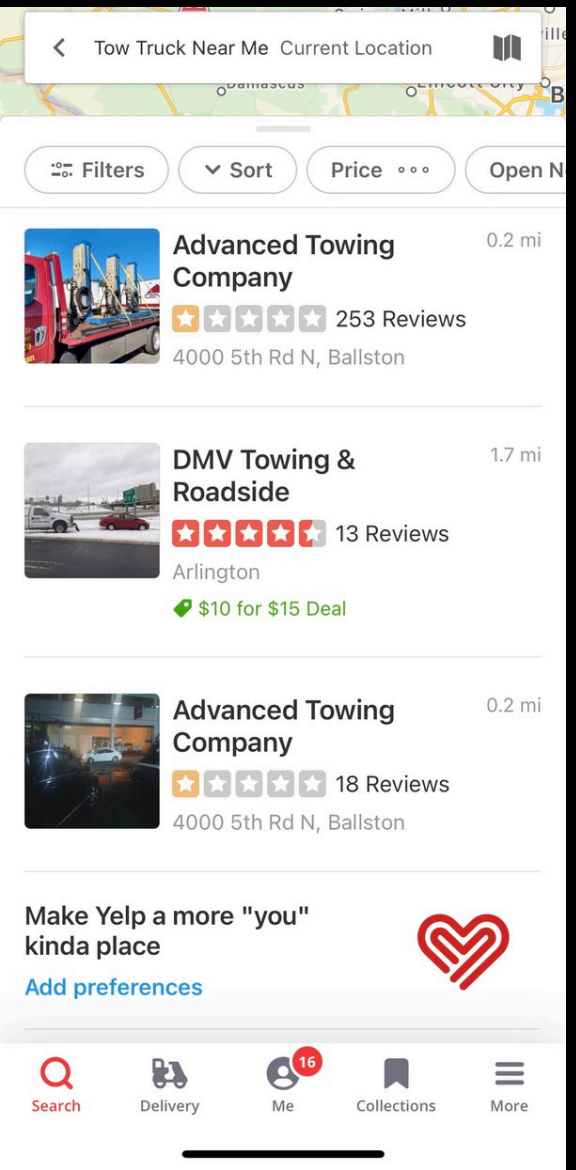


You Get Lost & Pop a Tire

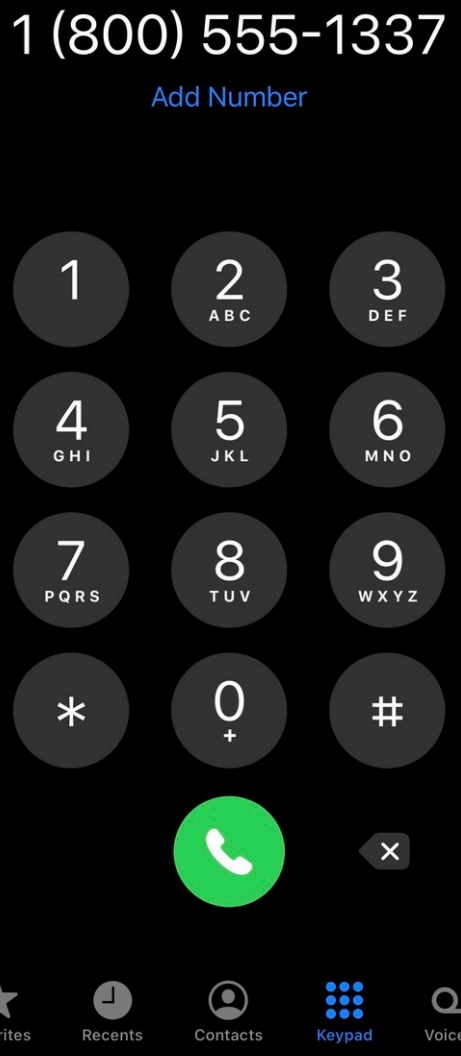
- Routined
  - Cache ZRTCLLocationMo – Granular location, Speed, Course, Accuracy
- cache_encryptedC.db (locationd)
  - Motion State History – In/Out of Vehicle, Moving/Non-moving
- Power Log
  - Torch State
- knowledgeC.db
  - App Usage
  - App Activity – Safari “how to change a tire”
  - App Web Usage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



Give Up, Call for a Tow Truck



- CallHistory.storedata
  - 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
- @iamevltwin
- sarah@blackbagtech.com