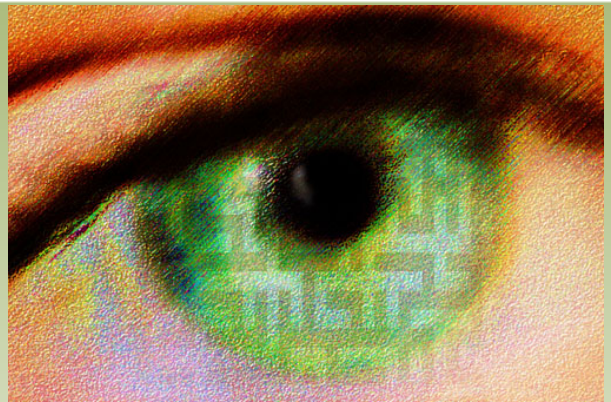
How Evolving Everyday Technology is Impacting Civil and Criminal Litigation

Hennepin County Law Library

September 15, 2023

John J. Carney, Esq.

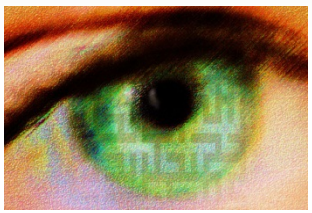
Carney Forensics



Integrated, Holistic Thinking

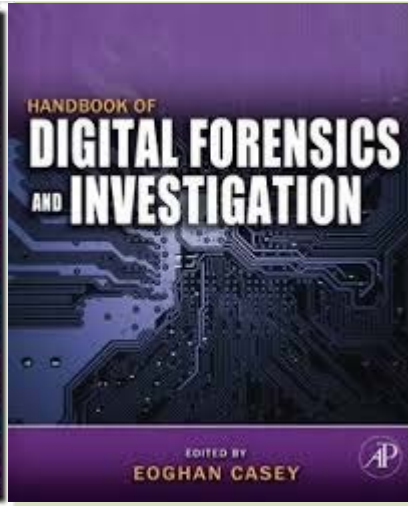
Buckminster Fuller

“Synergy is the only word in our language that means behavior of whole systems unpredicted by the separately observed behaviors of any of the system’s separate parts.”



Integrated, Holistic Approach

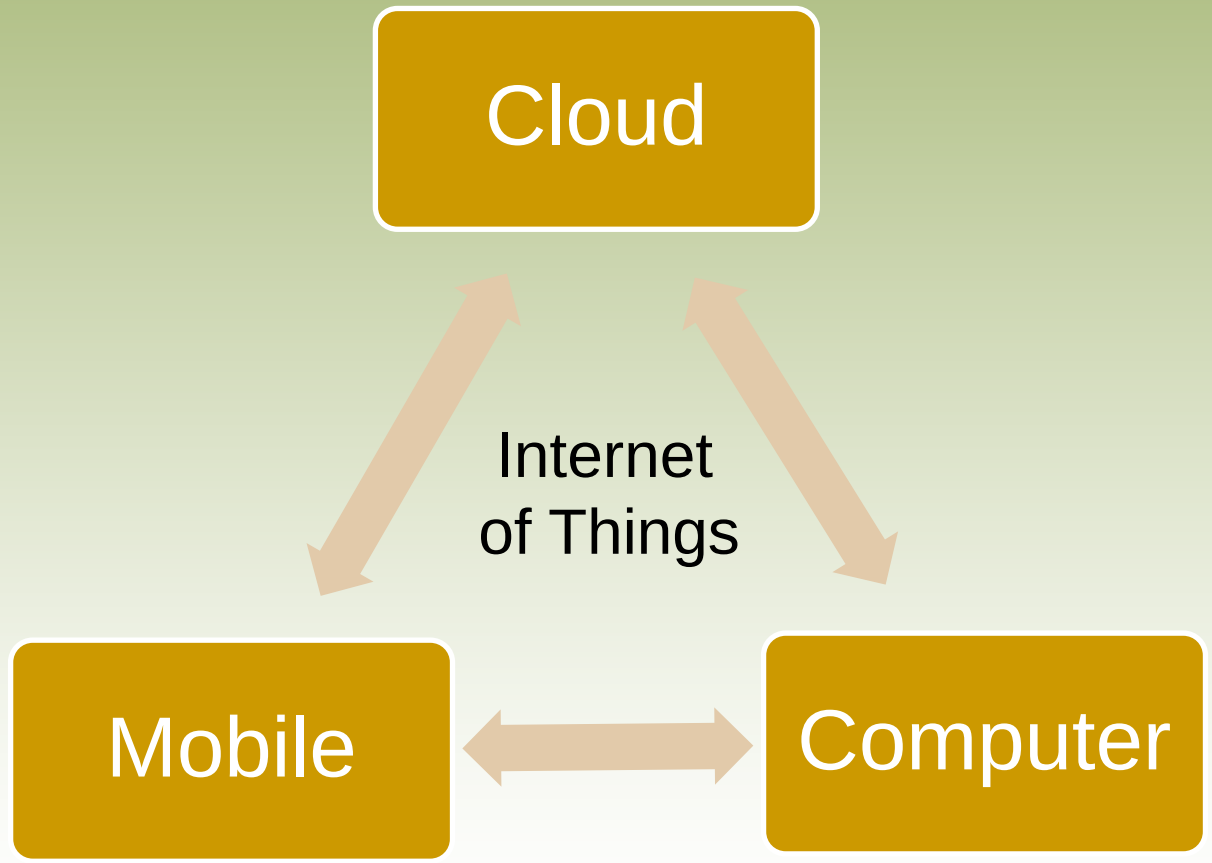
Mobile
Computer
Cloud
Nav Sat
Cellular
Vehicle
Appliance
Wearable
Speaker

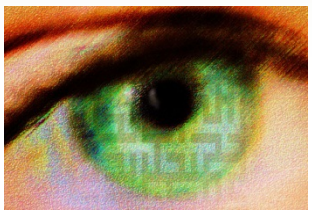


Chapter 20 – “Digital Evidence on Mobile Devices”
“Thinking Outside of the Device”

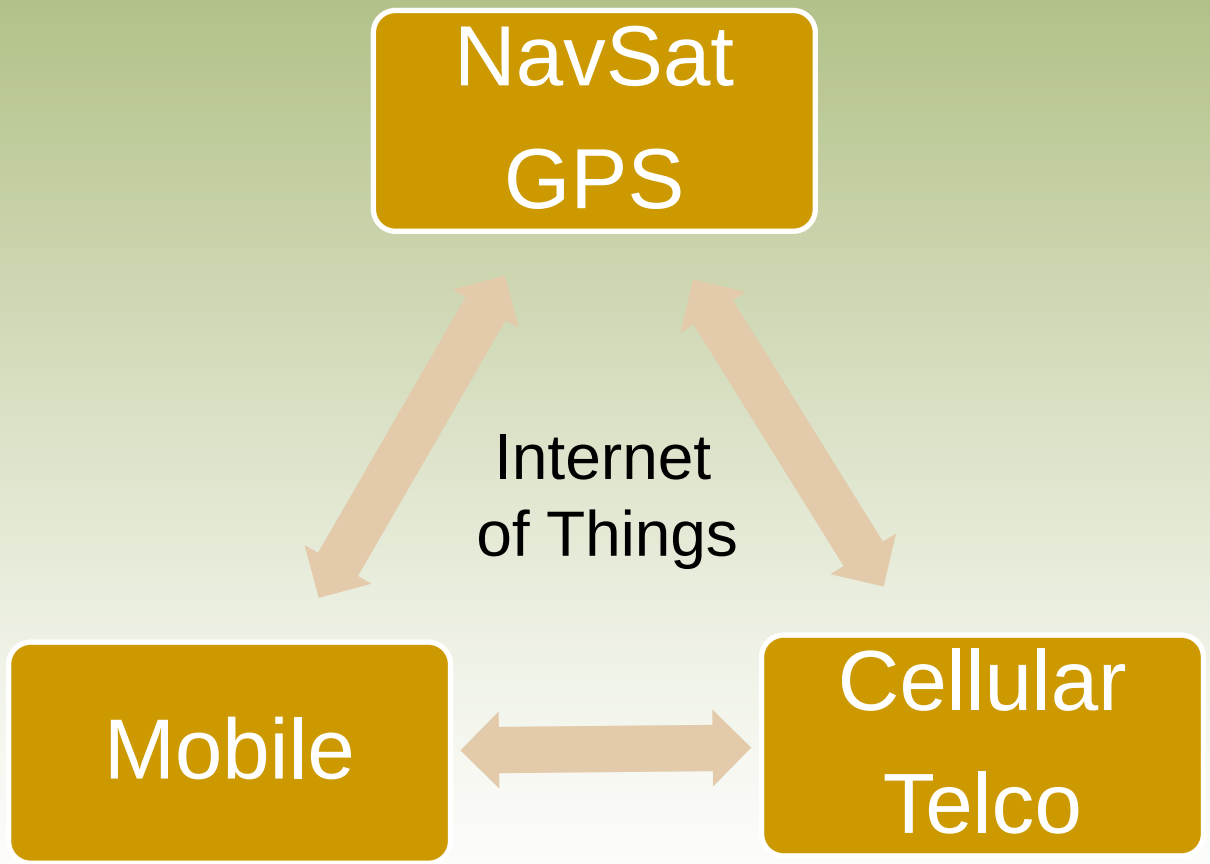
Criminal Cases
Civil Litigation
Investigations

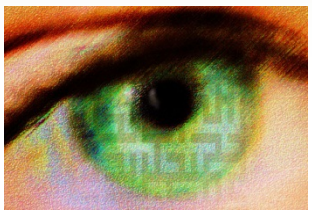
Forensics of Everything



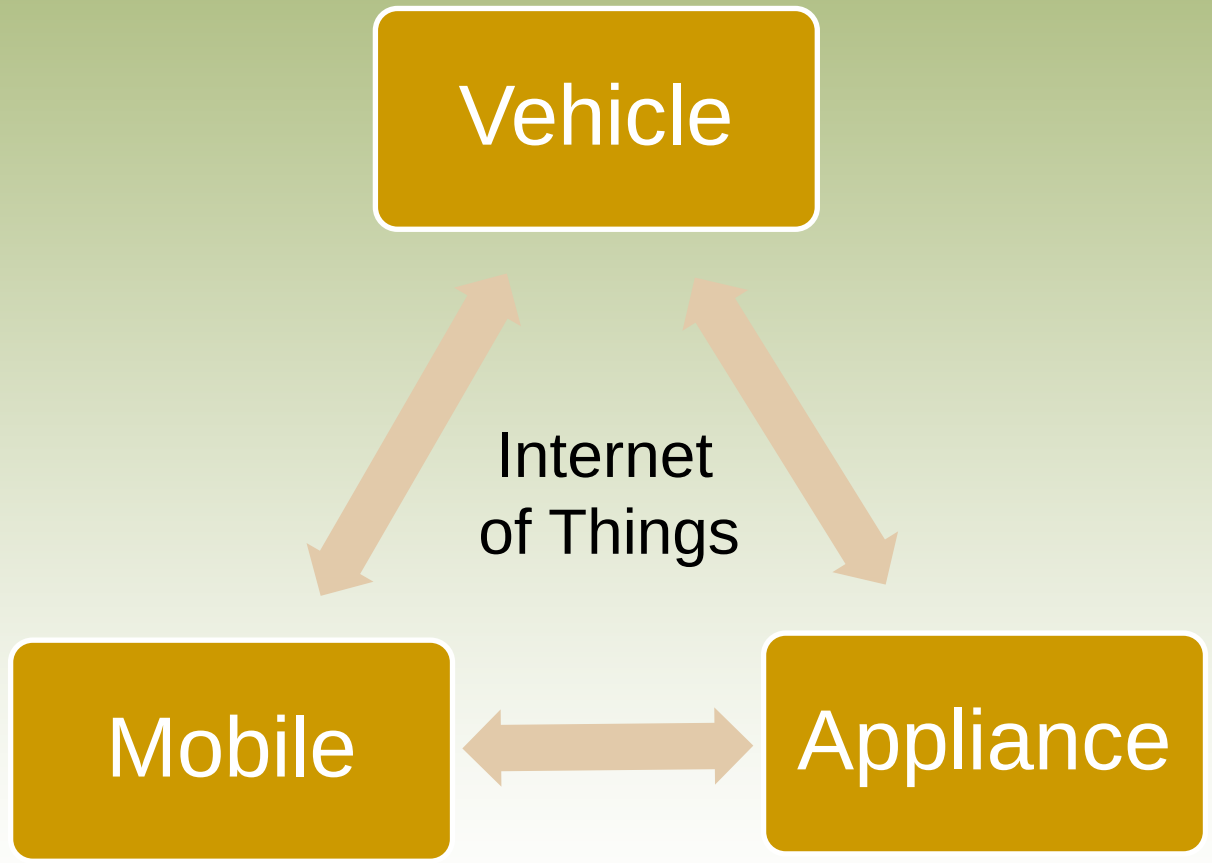


Forensics of Everything

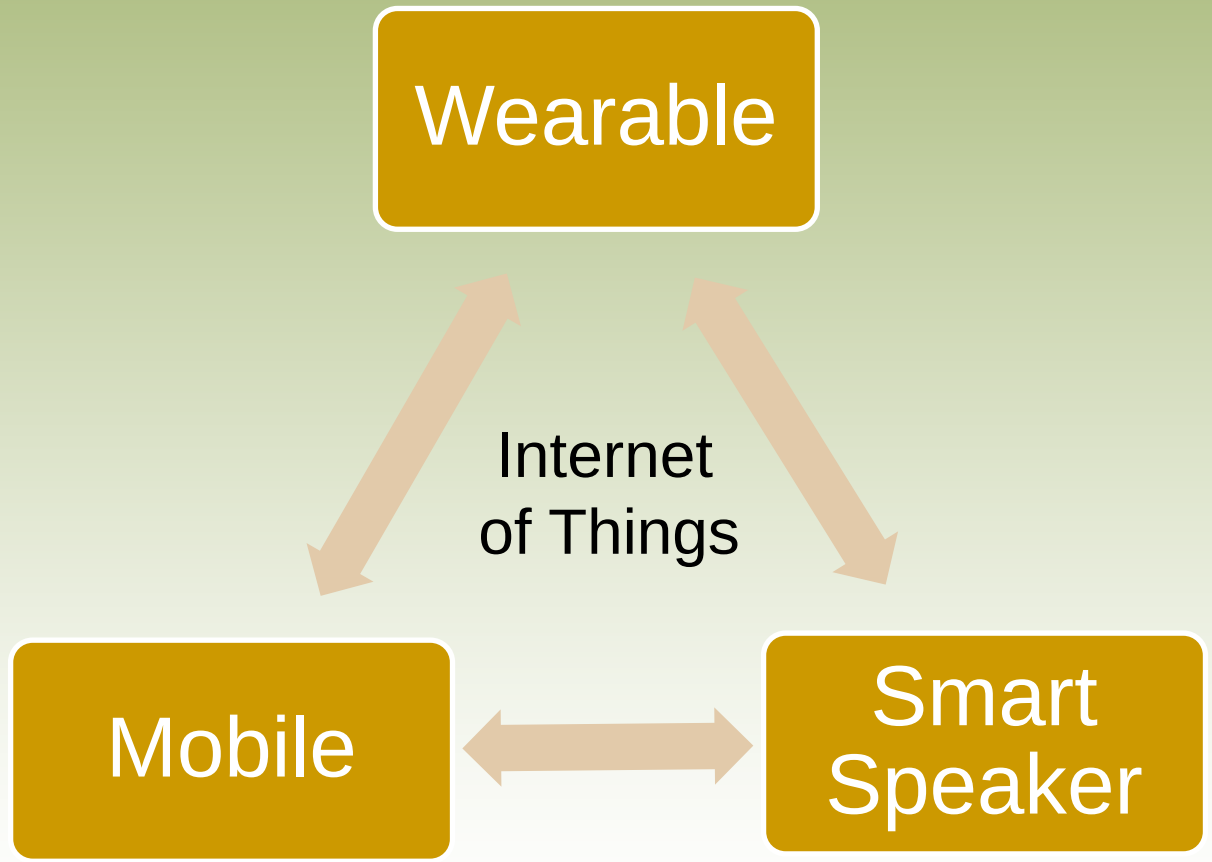




Forensics of Everything



Forensics of Everything



Why Mobile Evidence?

"My day starts and stops with my phone. I am not my phone, but my phone is a ***reflection of me***. It does a pretty good job of taking my life and folding it up into a nice little lightweight, pocket-sized summary. It's almost like I am holding a ***copy of my brain*** in my hands."

Derek Smith, Louisville Med-School Student (as reported by CNN)

Why Mobile Evidence?

"We must stop kidding ourselves that handhelds don't hold unique or discoverable information. Look up from your phones and tablets! *They are now the center of our digital lives.*"

Craig Ball, Esq.
Dem Phones, Dem Phones, Dem iPhones
Ball in Your Court

Why Mobile Evidence?

"Phones contain more probative evidence per byte of data than computer hard drives do."

Gary C. Kessler, Ph.D.
The Year Ahead for Mobile Forensics
Cellebrite's Panel Predictions for 2013

Everyday Technology 2023

- Apple iPhones
- Androids like Google Pixel, Samsung Galaxy
- Burner Phones
- Tablets like Apple iPad, Microsoft Surface, Amazon Fire

- Older GPS Units (Garmin, Magellan)

Everyday Technology 2023

- Laptops like Dell, Lenovo, Apple MacBook
- Desktops like Dell, Lenovo, Apple iMac
- Small Form Factors like Apple Mac Mini, Intel NUC
- Google Chromebooks (2022 Was the Year)
  - Low cost laptop replacement
  - Dominant @ K-12 and Colleges

Everyday Technology 2023

- Fitness Trackers (Fitbit)
- Digital Watches (Apple, Garmin, Samsung)
- Smart Speakers (Alexa, Siri, Google Asst.)
- Internet of Things (Nest Thermostats)
- Door Bells (Amazon Ring, Nest Door Cam)

- Vehicles (Infotainment, Telematics)

Speed of Technology Innovation

- Underlying Mobile Device Technology
  - Cell Phones
  - Fitness Trackers
  - Digital Watches
- Mobile Device Forensic Artifacts
  - Messaging
  - Activities
  - Device Locations
  - Photograph / Video
  - Browser / Search
  - Pattern of Life
- Artificial Intelligence / Machine Learning
  - Categorization of Messages and Photographs
  - Reverse Image Search

Probative Mobile Artifacts

- Messages and Chat go to communications
- Voice Calls and Mail go to communications
- Activity and Health go to motion, status, and proof of life
- Browsing & Search go to motive & intent
- Photos and Videos go to location and alibi
- Wi-Fi and Bluetooth go to location and alibi
- Device Locations go to alibi & vehicle path

“Pattern of Life” Mobile Artifacts

- Insights into digital behaviors and habits including normal routines in day to day life
  - Power On and Off, Battery Usage
  - Lock Screen and Device Orientation
  - Device Connections using Bluetooth and Wi-Fi to vehicles, watches, fitness trackers, etc.
  - Data Consumption from Wi-Fi and Cellular (4G LTE)
  - Screen Time and Digital Wellbeing Statistics

Probativeness A Must

- Most Probative Device Extraction / Image
- Key to Recovery of Deleted Evidence
- Key to Recovery of Fragments / Traces
- Key to Smoking Guns / Great Outcomes

One Tool is Never Enough

- Digital Forensic Tools are Diversified
- Strengths / Weaknesses / Killer Apps
- Cross Validate to Know What to Produce

Plan B for Critical Devices

- Smartphone Wiped, Traded @ Verizon Store
- Smartphone is Damaged, Destroyed
- Hard Drive is Replaced, Repurposed, Crashed, or Destroyed
- Fitness Tracker is Damaged

Apple iPhone Forensic Renaissance

- Examine new, probative, iOS full file system extractions
- Replace decades-old, limited iTunes backups
- Recover abundant, deleted evidence
- Recover new iPhone databases to expose “pattern of life” and other new evidence

Android Smartphone Forensic Innovations

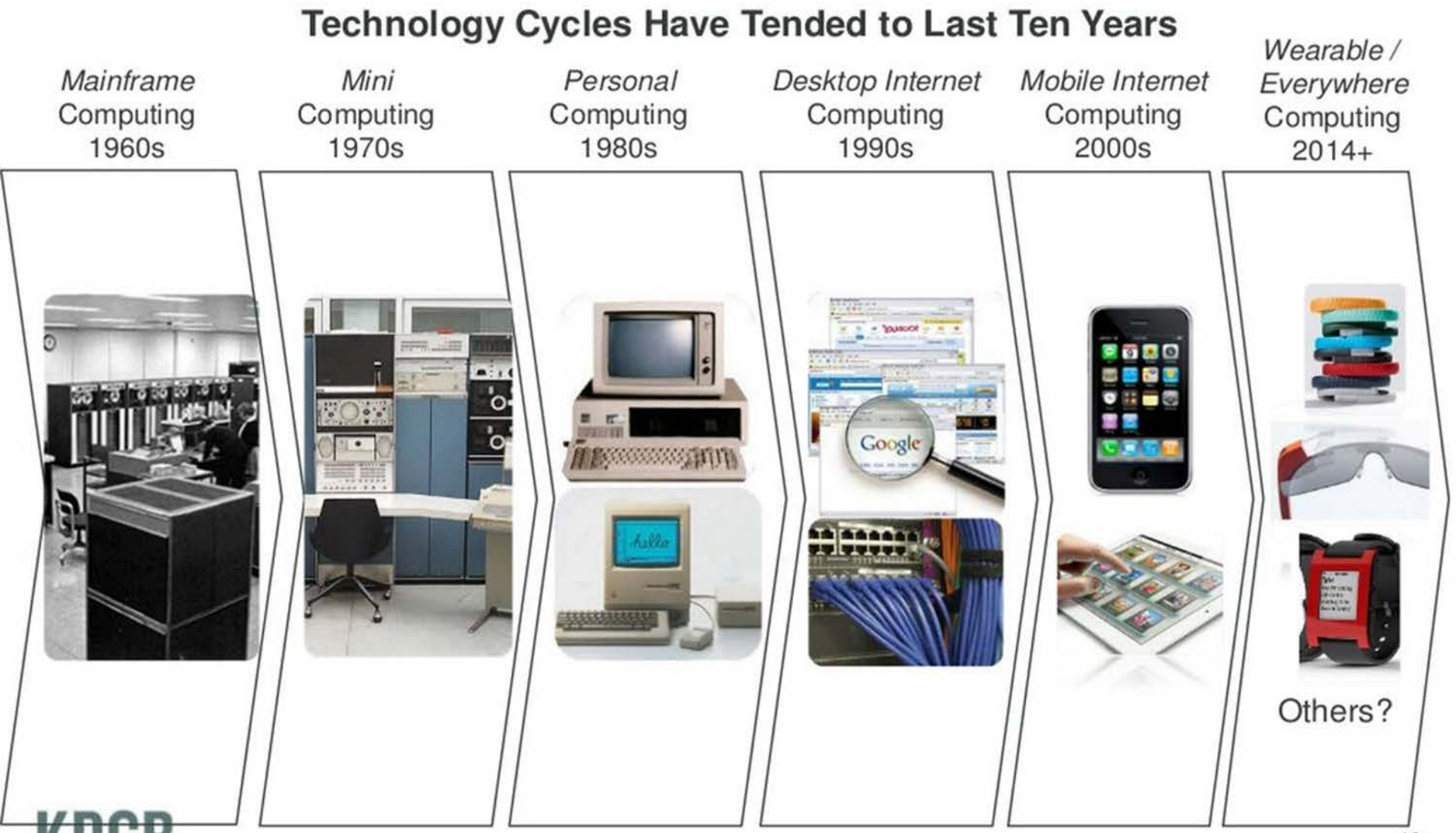
- Examine new, probative, physical and full file system extractions, instead of limited backups
- Recover, disable, or bypass Android passcodes
- Overcome encryption with new bootloaders
- Overcome security patch levels
- Analyze abundant, deleted evidence and new Android databases to expose new forms of evidence (pattern of life, digital wellbeing, etc.)

Low-Cost Android Burner Smartphones

- Unmarked, Android burners
- Mobile ID tools for make and model
- Or, call Verizon store, Metro PCS, etc.
- Supported phone lists for recovery capabilities
- Bypass or disable forgotten passcodes
- Obtain physical or full file system extractions

- Analyze live and deleted exculpatory evidence

Wearables



KPCB

Image Source: Computersciencelab.com, Wikipedia, IBM, Apple, Google, NTT docomo, Google, Jawbone, Pebble.

Wearable / Fitness Apps

endomondo

Health

fitbit

HEALTH SOLUTIONS

STRAVA™

Wearables – Digital Watches

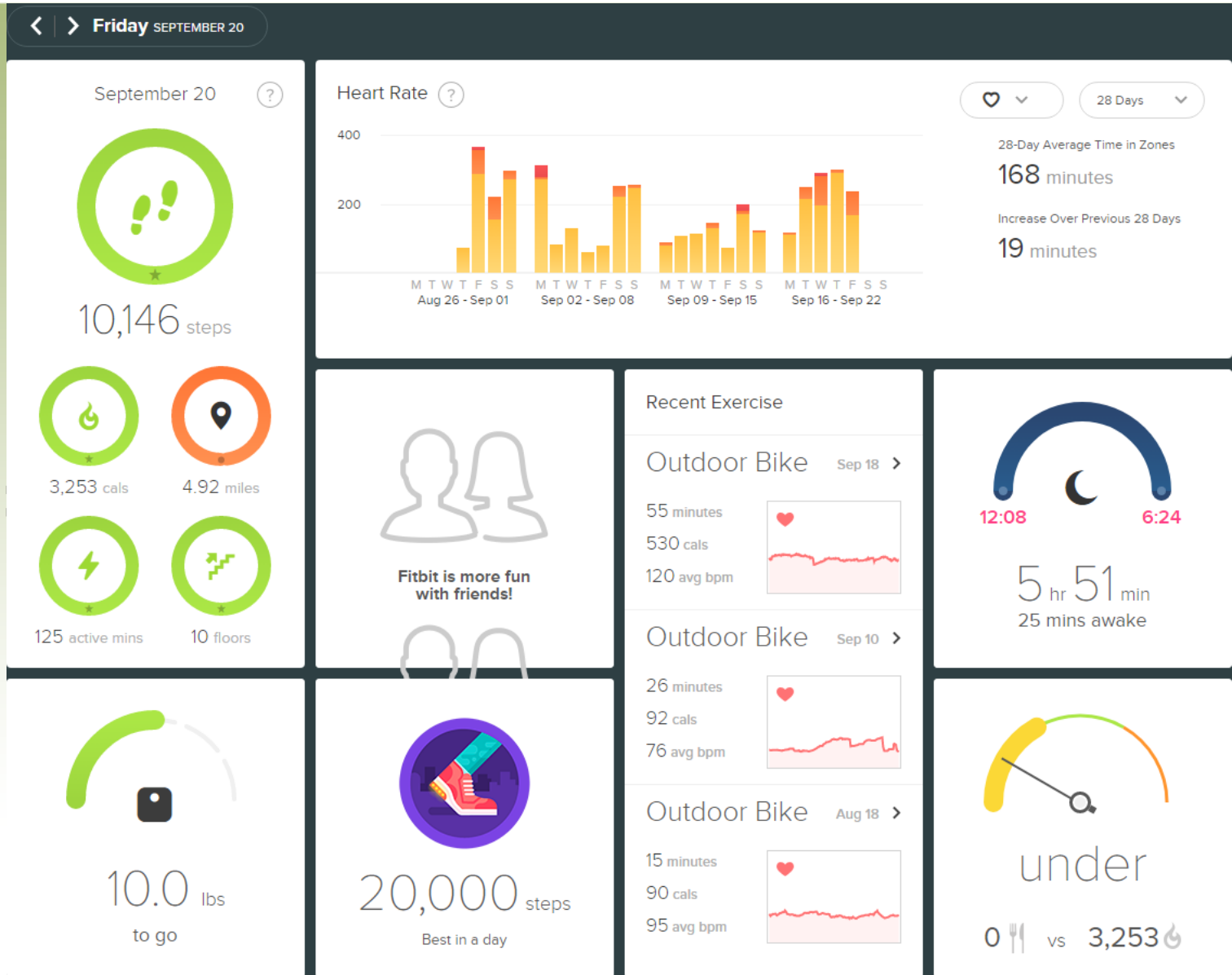
- Limited to no support for some models using mobile device forensic tools
- Access Apple watch evidence synced through to to paired iPhone
- Perform “live” extractions of watches
- Use digital watch vendor software tools like Garmin’s Basecamp to recover GPS and date/time stamp evidence

Wearables: Fitbit Forensics

- Activity Tracker over 10 Million Users
- Access Online with Forensic Collection or Examine Mobile App Paired to Tracker
- Personal Activity Metrics
  - Walk, Run, Swim, Sleep
  - Date & Time Stamps, Distance, Duration
  - Steps, Speed, Pace,
- Locations
  - Position
  - Journeys
  - Date & Time Stamps

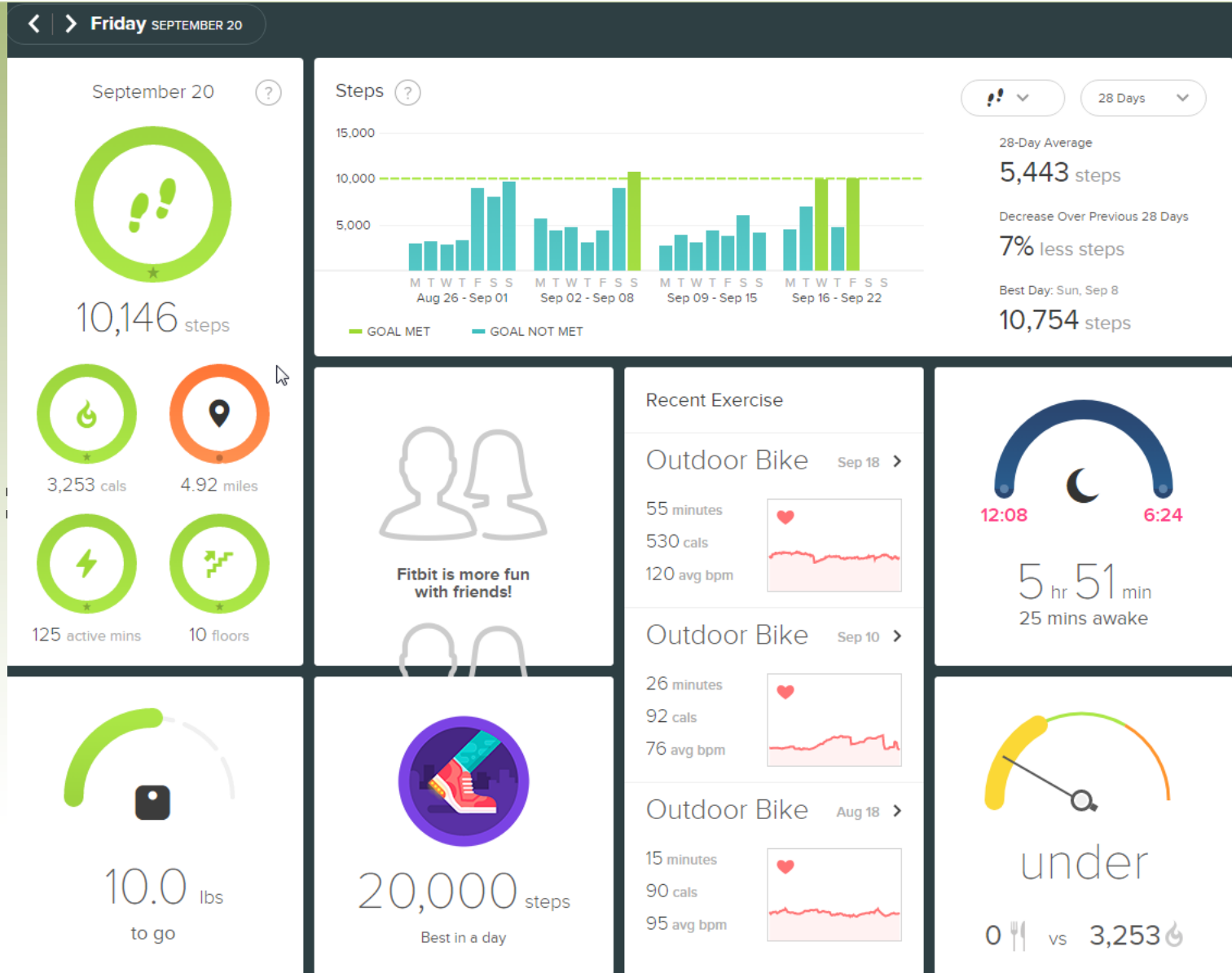
Wearables: Fitbit Forensics

Fitbit Dashboard Heart Rate



Wearables: Fitbit Forensics

Fitbit Dashboard: Steps



Wearables: Fitbit Forensics

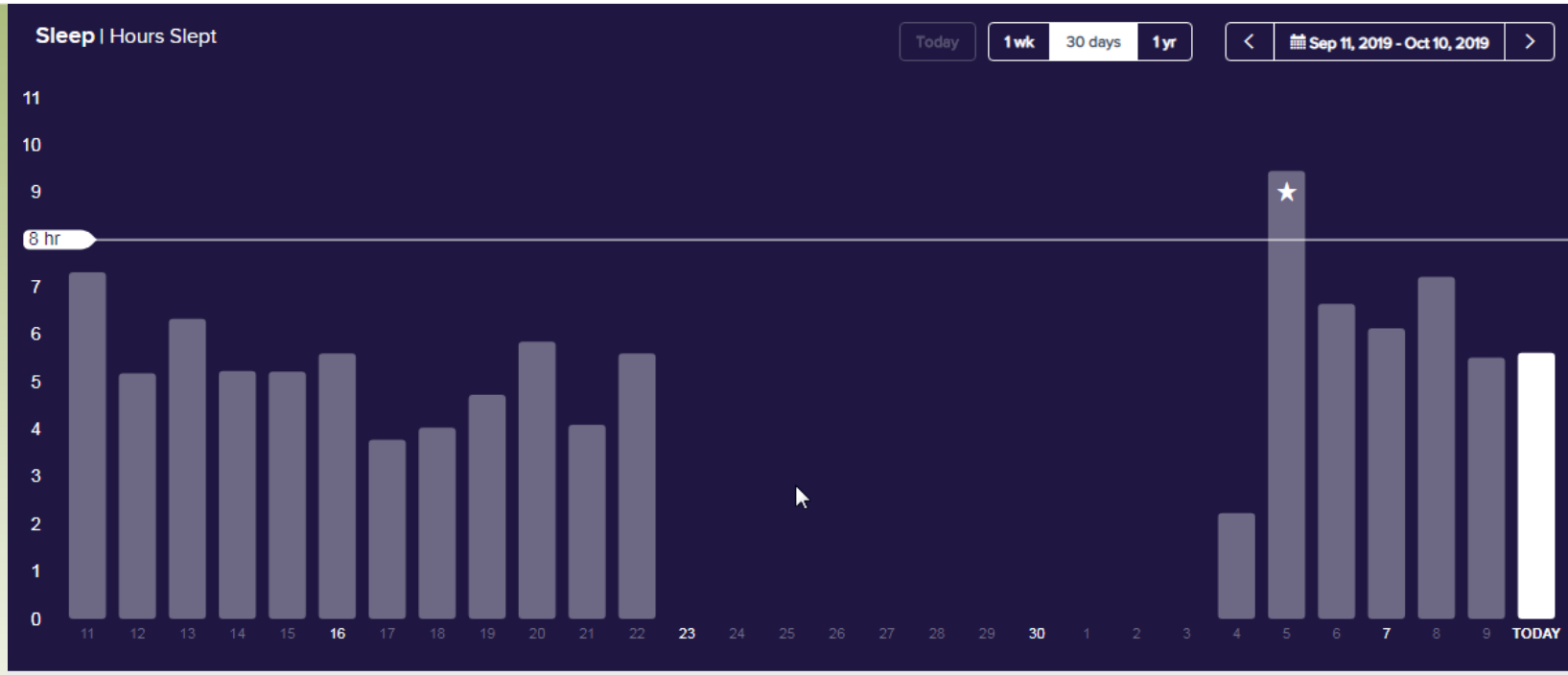
Fitbit Activity Log

Activity History

Date	Activity	Steps	Distance	Duration	Calories	
Oct 8, 5:54PM	Outdoor Bike	N/A	N/A	26:27	240 cals	View Details
Sep 22, 10:58AM	Walk	1,631	N/A	17:04	136 cals	View Details
Sep 18, 6:18PM	Outdoor Bike	N/A	N/A	54:37	530 cals	View Details
Sep 10, 10:02PM	Outdoor Bike	N/A	N/A	26:27	92 cals	View Details
Aug 18, 4:13PM	Outdoor Bike	N/A	N/A	15:22	90 cals	View Details
Aug 18, 3:35PM	Outdoor Bike	N/A	N/A	18:46	102 cals	View Details
Aug 17, 8:33AM	Walk	2,063	N/A	30:43	259 cals	View Details
Jul 29, 6:42PM	Sport	2,039	N/A	43:31	416 cals	View Details
Jul 27, 10:24AM	Sport	1,386	N/A	24:45	239 cals	View Details

Wearables: Fitbit Forensics

Fitbit Sleep Log



This Week		6 hrs 7 mins avg
Today	Thu 12 am - Thu 6 am	5 hrs 37 mins
Wed	Wed 12 am - Wed 6 am	5 hrs 31 mins
Tue	Mon 11 pm - Tue 7 am	7 hrs 13 mins
Mon	Sun 11 pm - Mon 5 am	6 hrs 8 mins
Week of Sep 30th		**6 hrs 7 mins avg**
10/06/2019	Sun 3 am - Sun 6 am	3 hrs 14 mins
10/06/2019	Sat 10 pm - Sun 1 am	3 hrs 25 mins
10/05/2019	Fri 11 pm - Sat 9 am	9 hrs 27 mins ★

Log Sleep

SLEEP START

11:00 PM

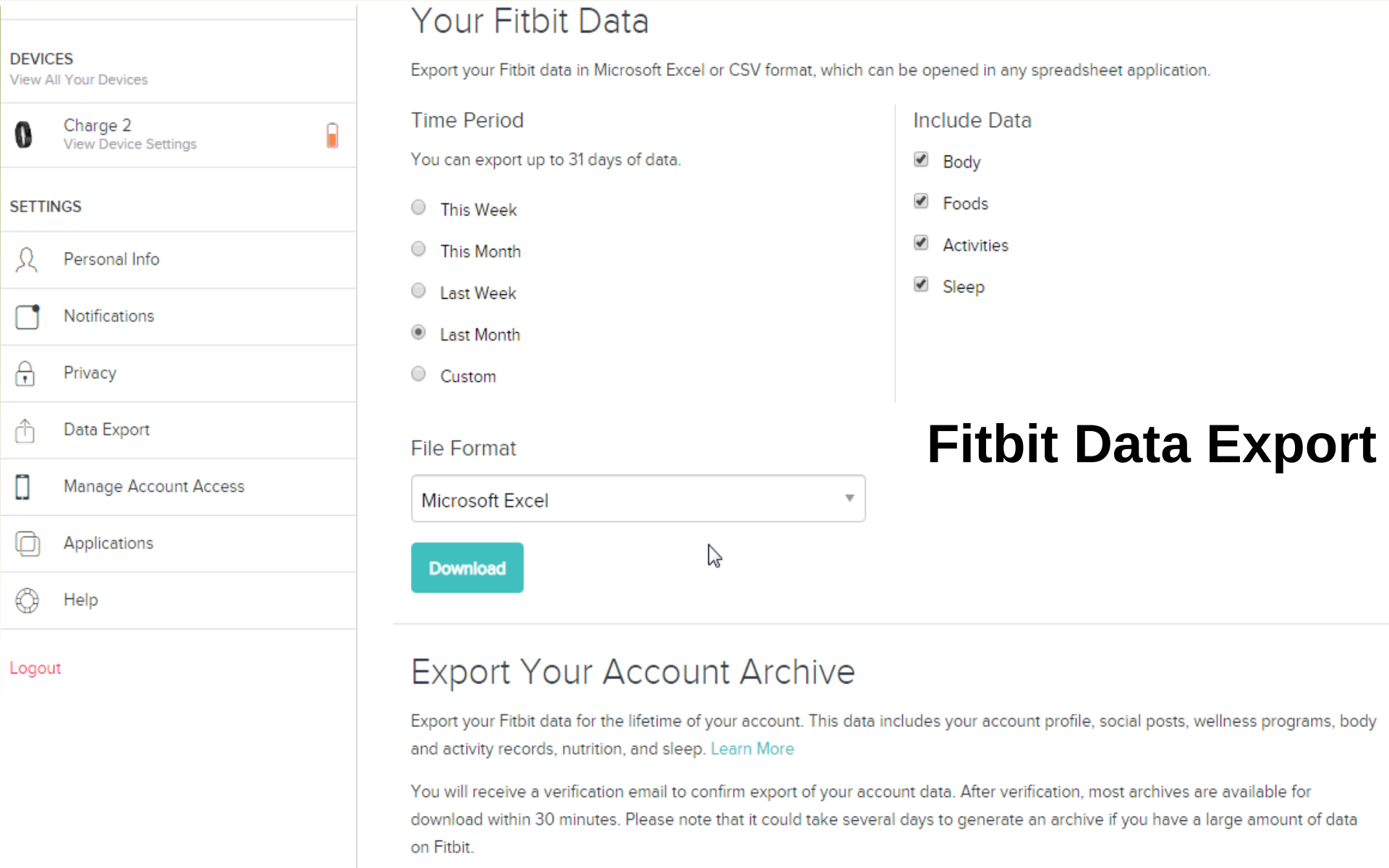
2019-10-09

SLEEP END

07:00 AM

2019-10-10

Wearables: Fitbit Forensics



Fitbit Data Export

The Cloud

Dropbox

box

EVERNOTE

iCloud

OneDrive

Google Cloud

The Cloud

- Photographs / Videos
- Contacts
- Email / Documents
- Messages
- Activity / Health
- GPS Locations
- Phone Backups

Google Cloud

iPhone Personal Navigation Apps

- Apple Maps
- Google Maps
- Waze – Social GPS
- Garmin USA
- Magellan RoadMate
- Navigon North America
- TomTom
- CoPilot Live
- MotionX GPS Drive
- MapQuest
- Scout by TeleNav
- Bing Maps

Android Personal Navigation Apps

- Google Maps
- Waze – Social GPS Maps
- Wisepilot
- Navigon North America
- CoPilot Live
- MapQuest
- Scout by TeleNav
- GPS Navigation by Sygic
- iGO My Way
- BackCountry Navigator
- MapFactor
- OsmAnd+ Maps & Navigation

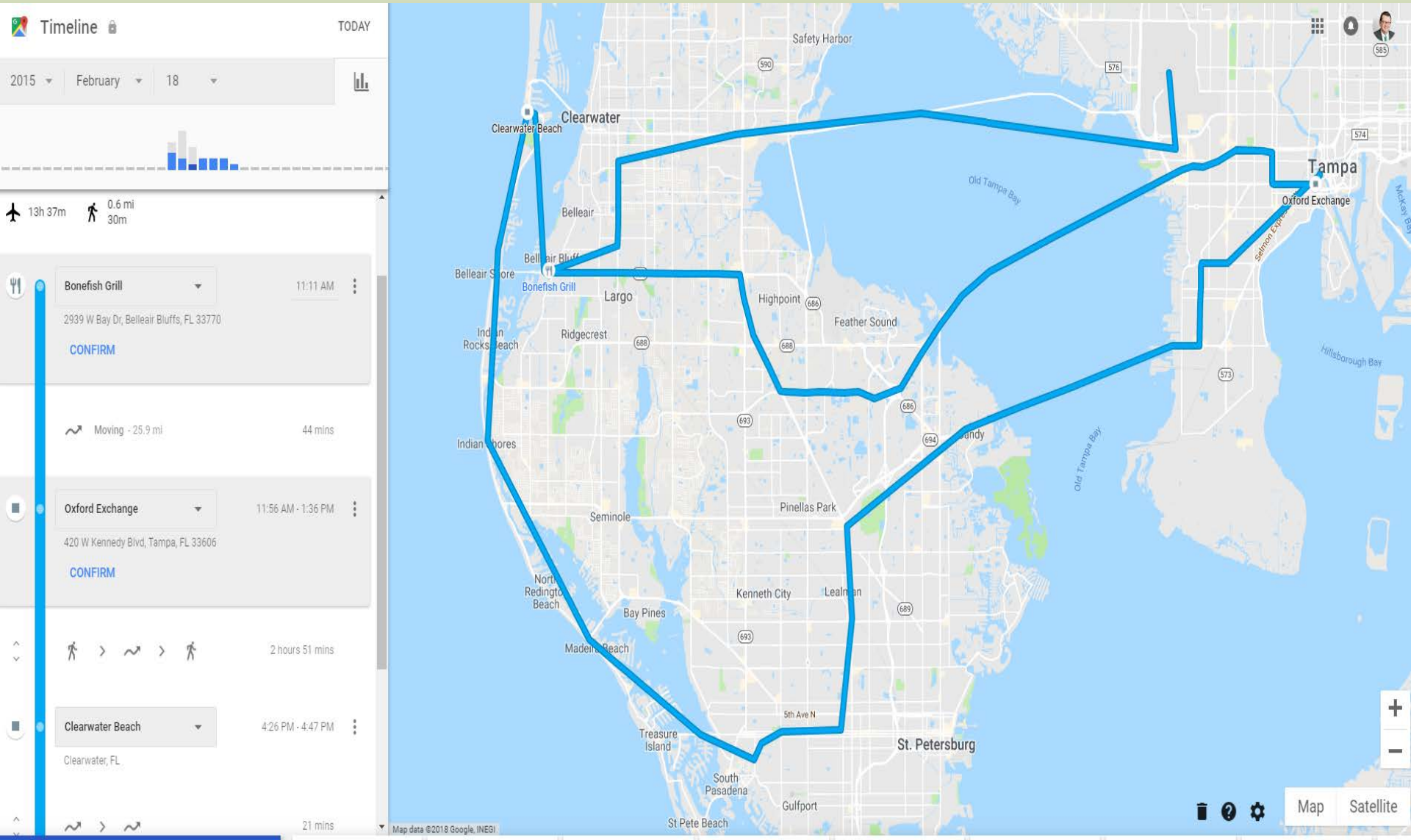
Waze

- 48MM Users, +2x Y/Y
- 1B+ Miles Driven per Month w/ Waze Open

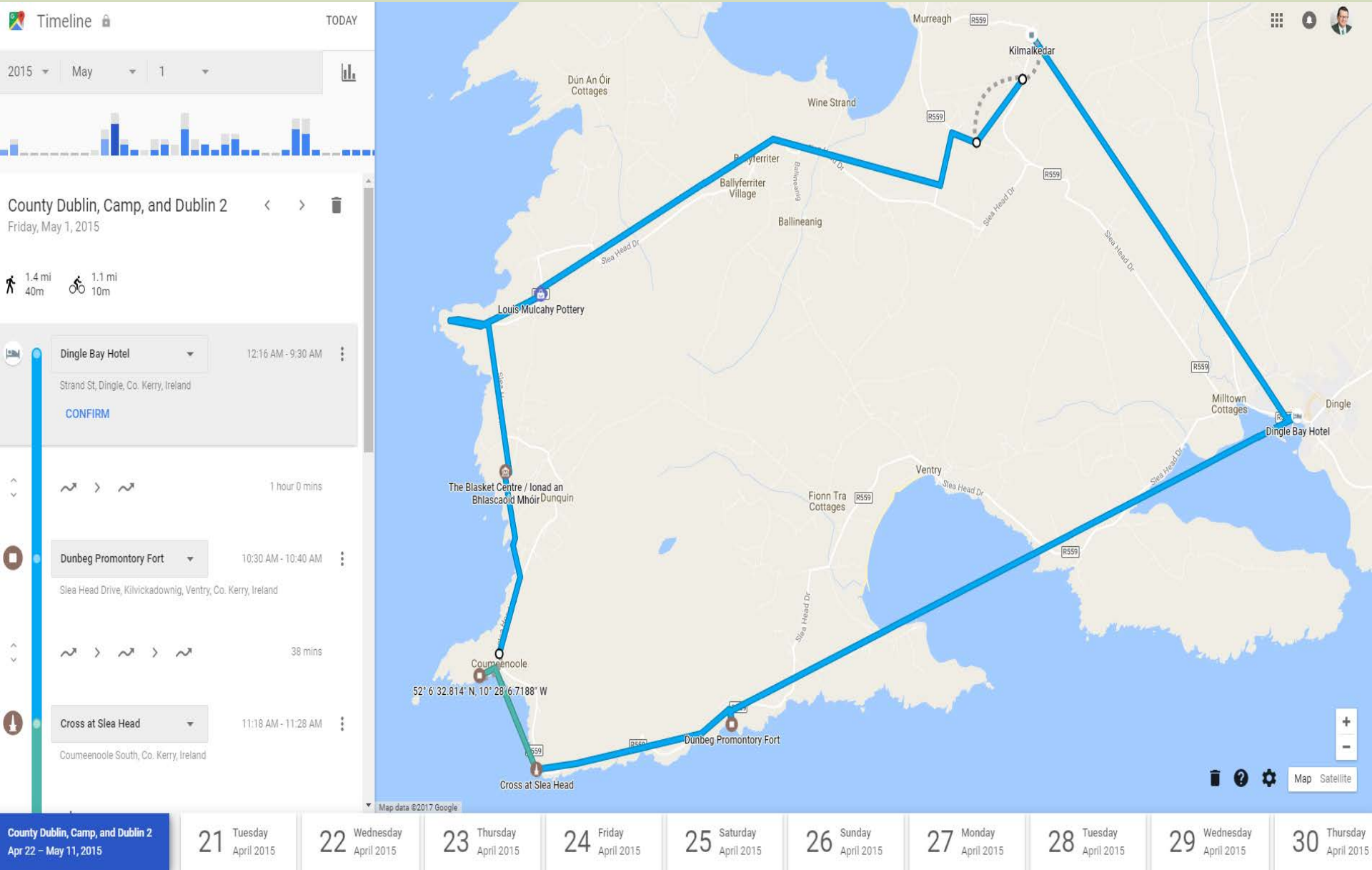
Examine Cloud for GPS Locations

- Apple iCloud Photos and Photo Stream
  - GPS locations in photo EXIF data
- Google Timeline Tracked from Mobile Device (aka Google Location History)
  - Passive GPS locations tracked every few minutes for years
  - More GPS locations are sampled when moving
  - GPS location time stamps are precise to second
  - Google shows compelling GPS location maps

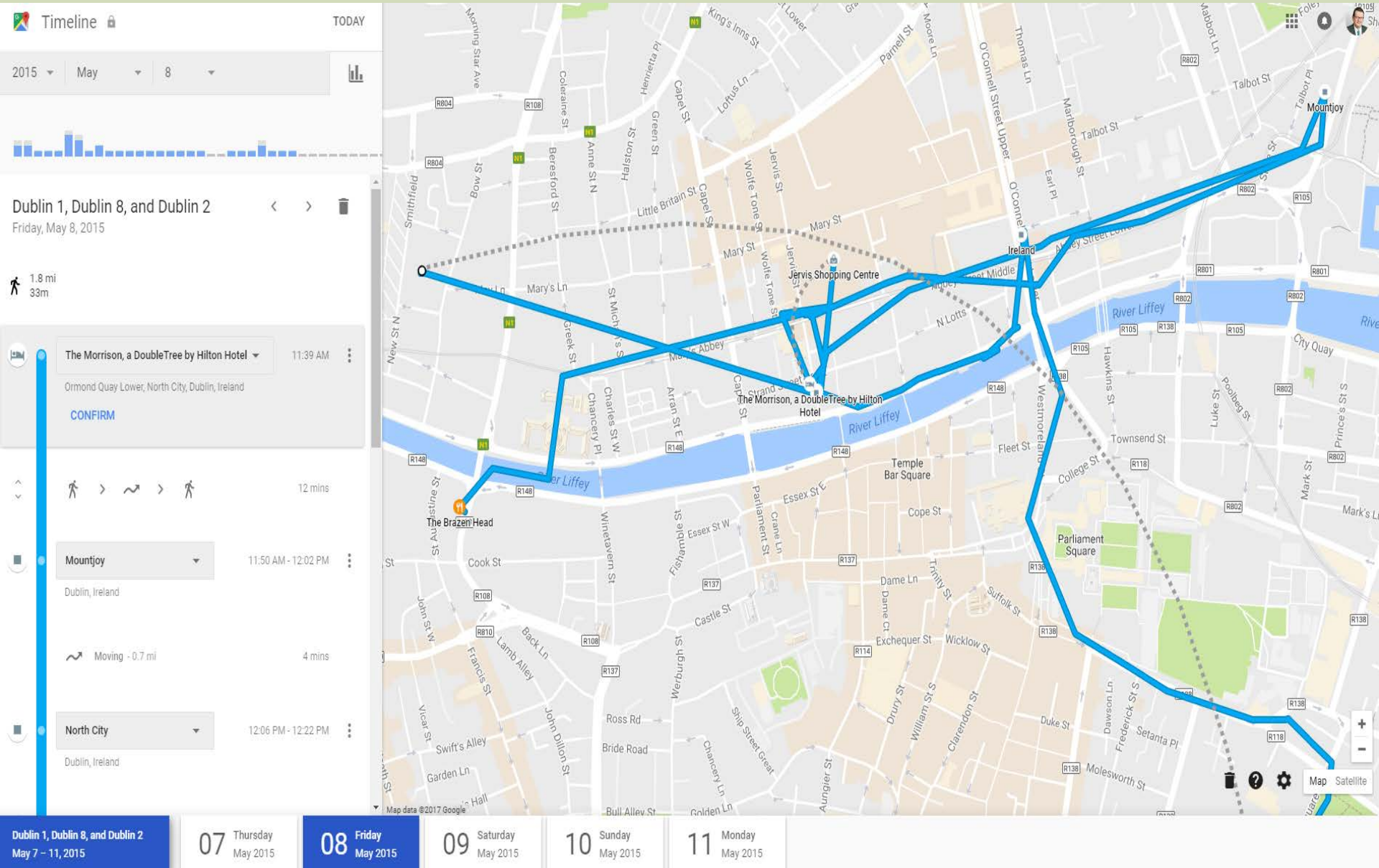
Google Timeline: Tampa Bay 2015



Google Location History: Ireland 2015



Google Location History: Ireland 2015



Beyond the Black Box

Beyond the Black Box

- Infotainment System
  - Advanced technology in vehicle for user interaction
  - Seamlessly & safely integrates access to digital life
  - Facilitates voice & data communications while we travel

- Telematics System
  - Embedded in vehicle
  - Integration of telecommunications and information
  - Connects infotainment system to
    - Vehicle's infrastructure (v2i)
    - Sensors that detect other vehicles on the road (v2v)

Recoverable Device Evidence

- Mobile Devices Connected to Vehicle
  - Smart Phones
  - Media Players
  - USB Drives
  - SD Cards
  - Wireless Access Points

- Bluetooth Connections – when and where
- Wi-Fi Connections – " " "
- USB Connections – " " "
- SD Card Connections – " " "

Vehicle System Forensics

- Recoverable User Evidence
  - Contact Lists (Phone Books)
  - Text Messages
  - Call Logs
  - E-mails
  - Photographs
  - Movies / Videos
  - Music / Audio
  - Games
  - Social Media Feeds
  - Installed Apps

Recoverable Navigation Evidence

- Track Logs or Navigation History
- Track Points or GPS Locations
- Recent Destinations
- Favorite Locations or Waypoints
- Favorite Routes

“Your Car is Spying on You”

[redacted] “We had a Ford Explorer … we pulled the system out, and we recovered 70 phones that had been connected to it. All of their call logs, their contacts and their SMS.”

Berla iVe Founder and CEO, The Forensic Lunch podcast, 2015

[redacted] The kit can discover “when and where a vehicle’s lights are turned on, and which doors are opened and closed at specific locations.”

Sam Biddle, The Intercept_, May 3, 2021

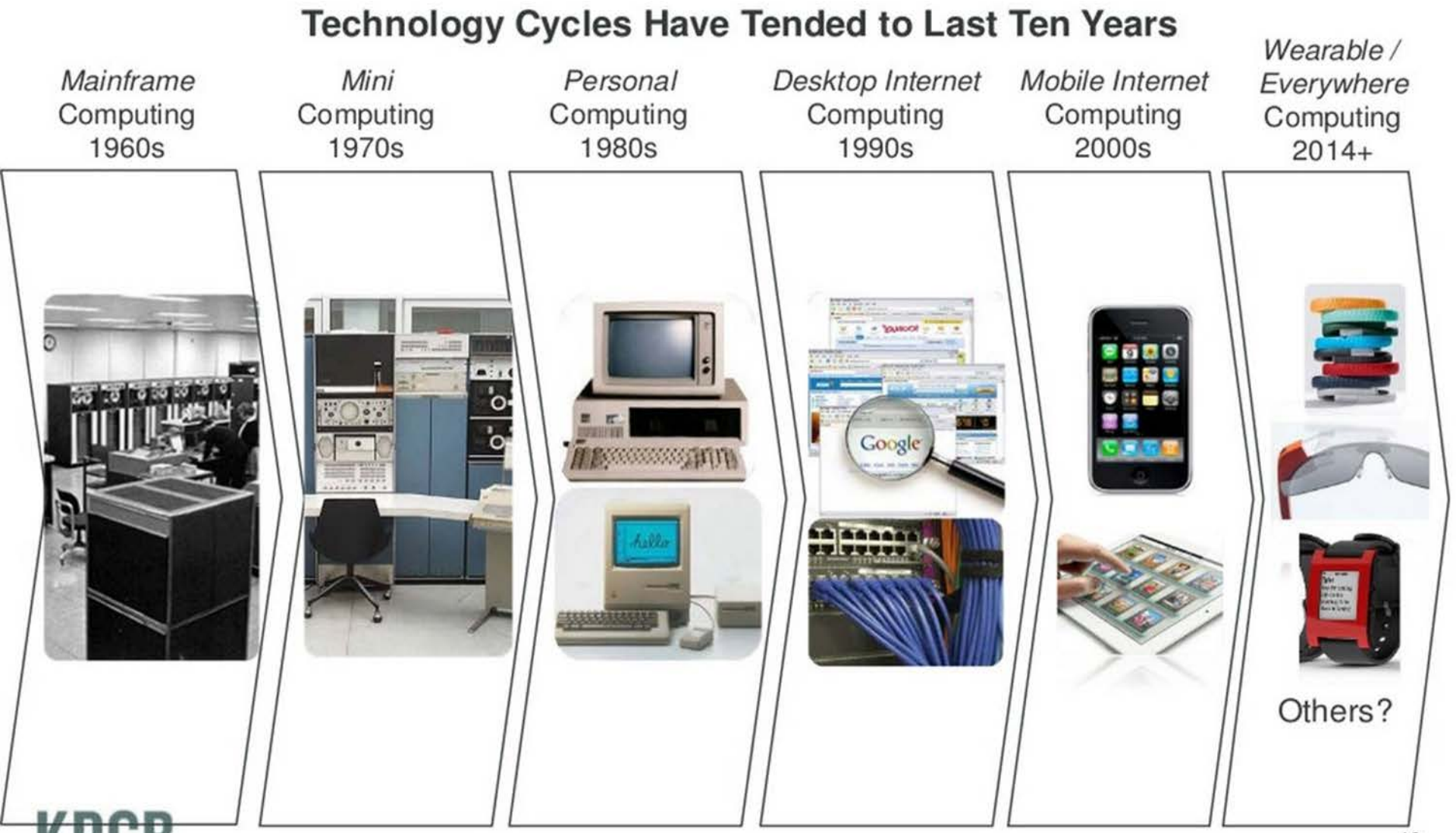
Vehicle System Forensics

- Recoverable Vehicle Evidence
  - Serial Number
  - Original VIN Number
- Recoverable Vehicle Event Evidence
  - Headlights On and Off
  - Doors Identified for Open and Close
  - Gear Changes for Park and Drive
  - Odometer Readings
  - Velocity Logs
  - GPS Time Synchs
  - System Reboots

Automotive Vehicle Support

- Over 5,200 Models Back to 2008
- Non-destructive Acquisition
- Acquire Evidence via Logical and Physical Extractions
- Recover Deleted Data Using Three VSF Tools
- Map Geo-coded Data
- Search and Filter Data
- Revealing Reports for Digital Forensic Investigations

Smart Speakers



KPCB

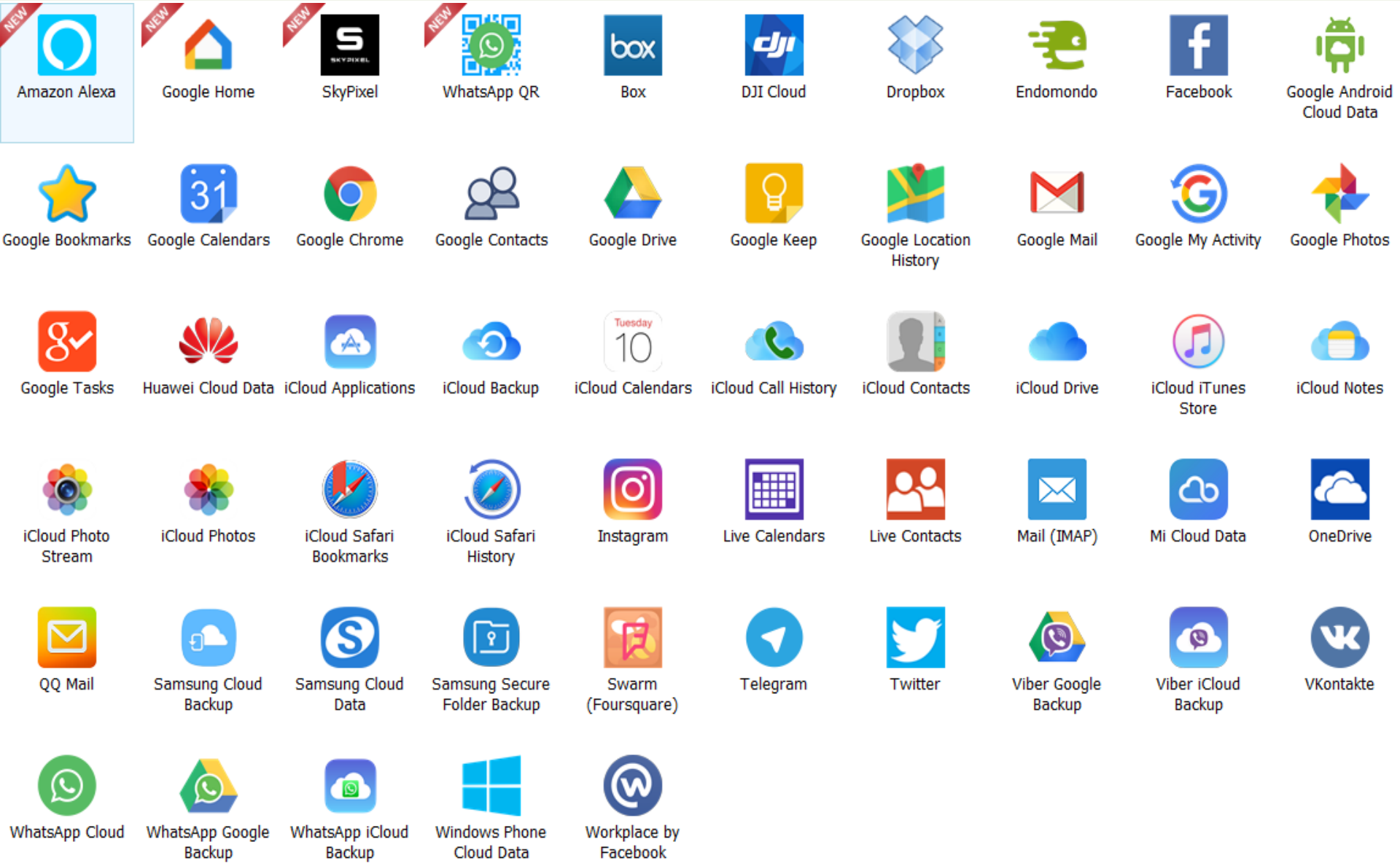
Image Source: Computersciencelab.com, Wikipedia, IBM, Apple, Google, NTT docomo, Google, Jawbone, Pebble.

Smart Speaker Apps

Smart Speaker: Amazon Alexa

- Tens of Millions of Echo Devices Sold
- Alexa Works w/ 20,000 Smart Home Devices
- Over 50,000 “Skills” Available for Integration
  - Thermostat, Fitbit, Pandora, TED Talks
  - Sleep Sounds, NY Times, Famous Quotes, UPS
- Alexa Data Stored in Primarily in Cloud
  - Echo Dot has only Wi-Fi Connections
  - Mobile Apps have Limited Data
  - What Evidence is Recoverable?

Smart Speaker: Amazon Alexa



Smart Speaker: Amazon Alexa

Categories

- Activity
- Contacts
- Messages
- Voice records
- Player history
- Reminders and alarms
- Skills
- Lists
- Other

Date range

1/ 1/2000

10/22/2018

Apply for all services

Smart Speaker: Amazon Alexa

Extraction finished!

Data is successfully extracted from the Cloud

Extraction ID: 0F6F7FB310FA4FEEBE816332A383DCF0
Account owner: John Carney

Cloud services

Amazon Alexa -

Extraction summary

- Activity - 749
- Contacts - 472
- Messages - 1
- Voice records - 748
- Player history - 0
- Reminders and alarms - 0
- Skills - 13
- Lists - 2
- Other - 74

Exhibit – Facebook Messenger

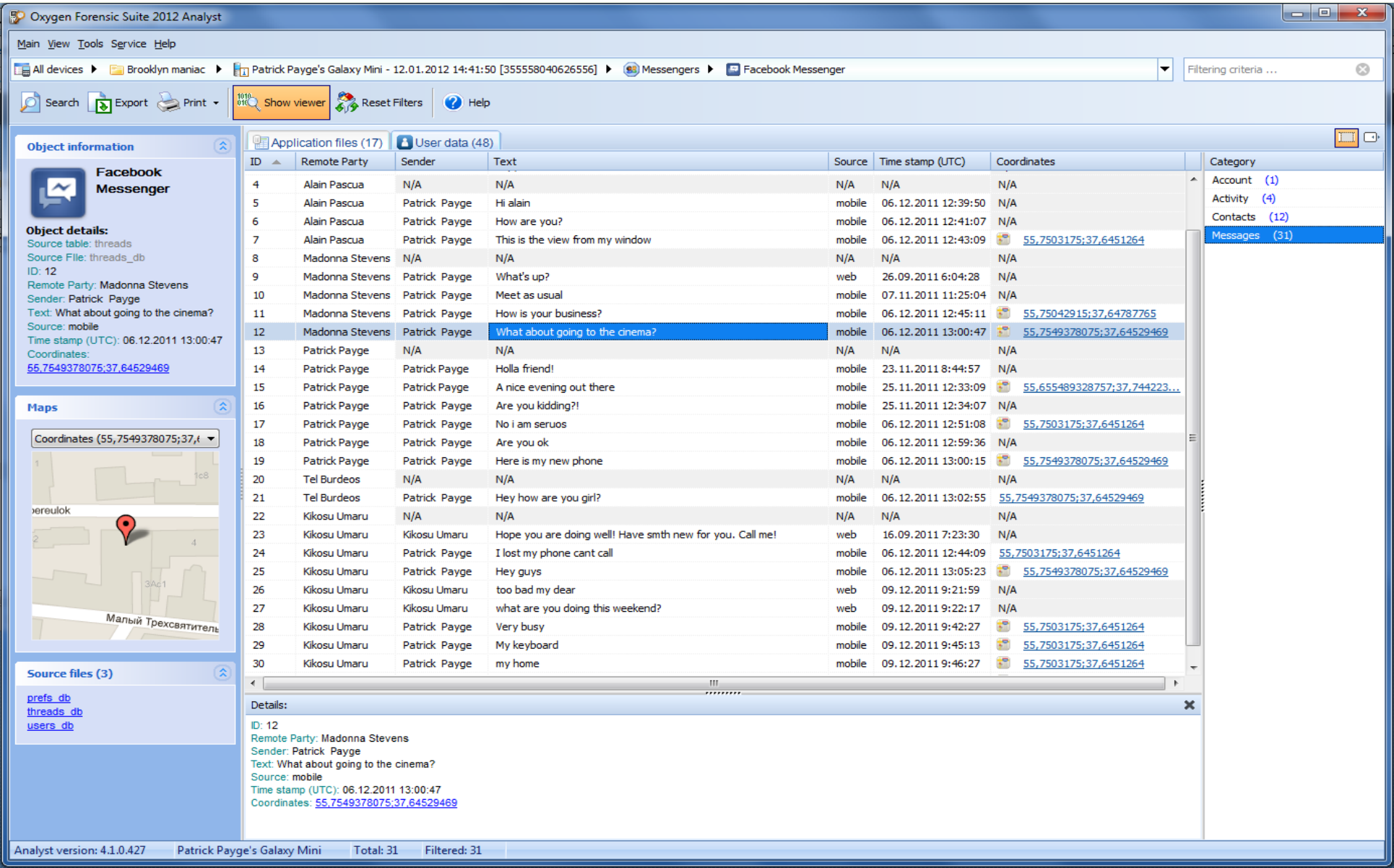
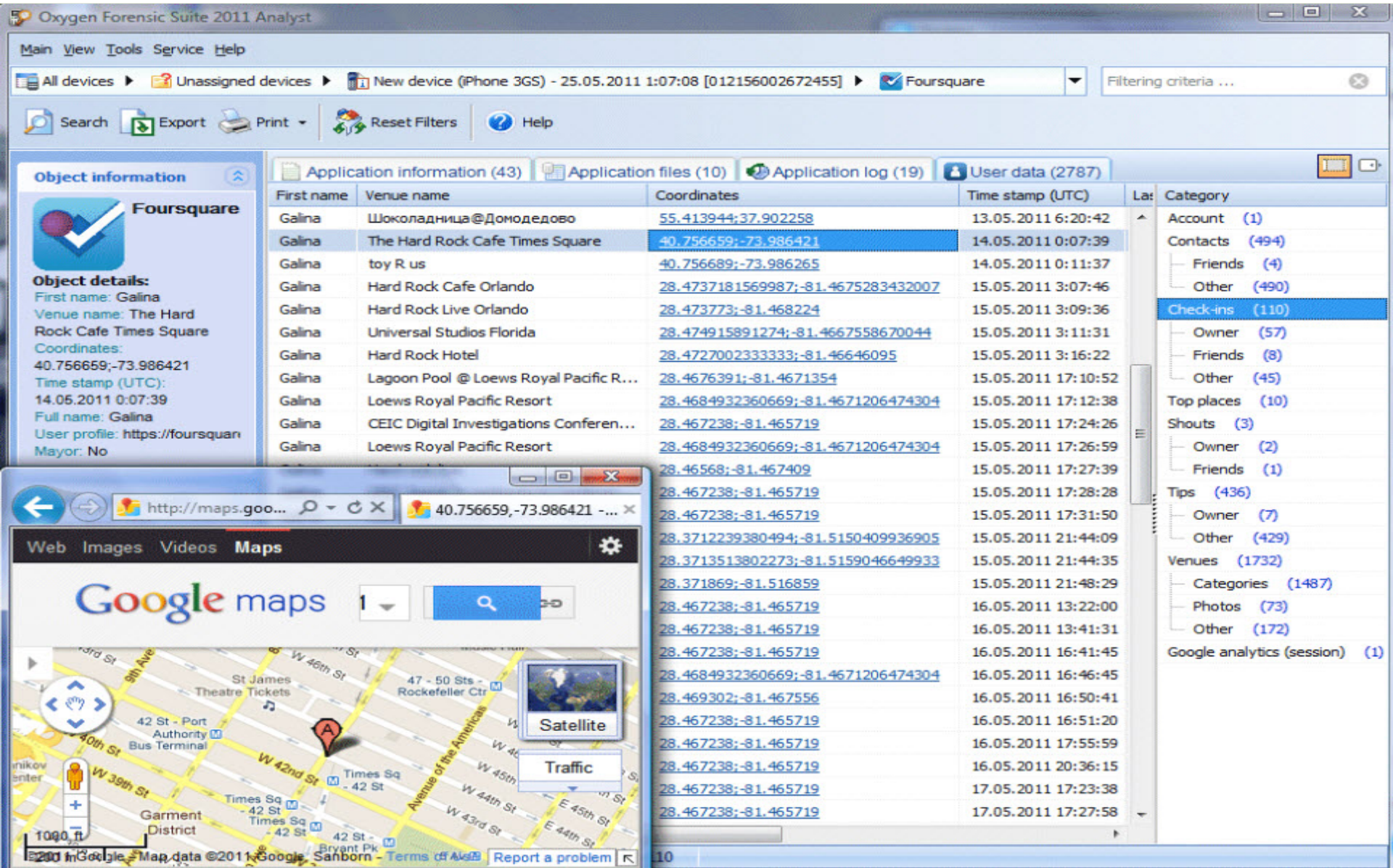


Exhibit – Foursquare App



GPS Evidence

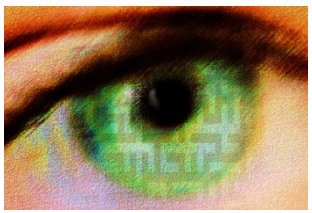
Verizon Wireless Text Message Log

Network Element Nam	Switch	MDN	Msg Send Date	Msg Deliver Date	Message	Originating Adc	Destination Address	Message Direction	
GoldenValley_MR85	M	612	8/30/2014 11:41:11 AM	8/30/2014 11:41:20 AM	1	612	612		3
GoldenValley_MR85	M	612	8/30/2014 11:54:49 AM	8/30/2014 11:54:49 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:54:49 AM	8/30/2014 11:54:55 AM	1	612	612		3
GoldenValley_MR85	M	612	8/30/2014 11:55:12 AM	8/30/2014 11:55:13 AM	1	612	612		4
GoldenValley_MR85	M	612	8/30/2014 11:55:12 AM	8/30/2014 11:55:13 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:57:39 AM	8/30/2014 11:57:39 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:57:39 AM	8/30/2014 11:57:40 AM	1	612	612	Sent	4
GoldenValley_MR85	M	612	8/30/2014 11:57:54 AM	8/30/2014 11:57:54 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:57:54 AM	8/30/2014 11:57:58 AM	1	612	612	Received	3
GoldenValley_MR85	M	612	8/30/2014 11:54:18 AM	8/30/2014 11:54:19 AM	1	612	612		4
GoldenValley_MR85	M	612	8/30/2014 11:54:18 AM	8/30/2014 11:54:19 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:56:41 AM	8/30/2014 11:56:47 AM	1	612	612		3
GoldenValley_MR85	M	612	8/30/2014 11:56:41 AM	8/30/2014 11:56:41 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:54:03 AM	8/30/2014 11:54:03 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 11:54:03 AM	8/30/2014 11:54:08 AM	1	612	612		3
GoldenValley_MR85	M	612	8/30/2014 11:57:11 AM	8/30/2014 11:57:12 AM	1	612	612	Sent	4
GoldenValley_MR85	M	612	8/30/2014 11:57:11 AM	8/30/2014 11:57:12 AM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 12:00:21 PM	8/30/2014 12:00:22 PM	16	612	90008		4
GoldenValley_MR85	M	612	8/30/2014 12:08:05 PM	8/30/2014 12:08:06 PM	1	612	612		3
GoldenValley_MR85	M	612	8/30/2014 12:08:05 PM	8/30/2014 12:08:05 PM	16	612	90008		4

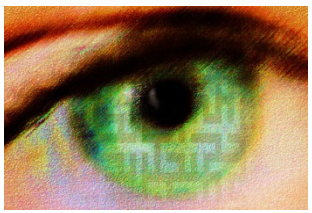
#1

#2

#3



GPS Evidence



UFED Physical Analyzer 4.2.1.7

File View Tools Extract Python Plug-ins Report Help

Welcome × Extraction Summary ×

- Garmin_Nuvi 1300
  - Extraction Summary
  - Device Info
  - Images
  - Memory Ranges
  - File Systems
  - Analyzed Data
    - Device Locations (49130)
      - Journeys (318)
      - Locations (1223)
        - Favorites (16)
        - Orphaned Fixes (1207)
  - Data Files
    - Applications
    - Audio
    - Configurations
    - Databases (4)
    - Documents
    - Images (12)
    - Text (15)
    - Videos
    - Uncategorized
  - Carving
    - Images
  - Tags
  - Timeline (49114)
  - Watch Lists
  - Malware Scanner
  - Project Analytics
  - Hex Bookmarks
  - Entity Bookmarks
  - Reports

Extraction Summary

Extraction Info

Garmin_Nuvi 1300 Garmin

Extraction start date/time	3/24/2015 6:05:50 PM
Extraction end date/time	3/24/2015 6:11:50 PM
Unit Version	4.1.2.8 PSP 1
Selected Manufacturer	Garmin
Selected Device Name	Nuvi 1300
Connection Type	Cable No. 80
Is encrypted	False
Extraction Type	File system
Extraction ID	B9B68BB4-69C8-45BD-8740-F8A0C79CEA43

Image Hash Information

Hashes have been calculated for this project, but no reference data is available.

Device Info

Detected model: nüvi 1300

Device Content

Phone Data

Device Locations: 49130 (1207)

Data Files

Databases: 4 (0)

Images: 12 (0)

Text: 15 (0)

Garmin GPS unit contained 318 journeys with 49,130 device locations.

Correlated Message & GPS Evidence

Locations (43)

#	Name	Time	Latitude	Longitude
1		8/30/2014 11:57:12 AM(UTC-5)	46.673725	-96.420178
2		AM(UTC-5)	46.67396	-96.420363
3		AM(UTC-5)	46.673959	-96.420332
4		AM(UTC-5)	46.673956	-96.42018
5		AM(UTC-5)	46.673897	-96.420179
6		8/30/2014 11:57:19 AM(UTC-5)	46.673937	-96.420179
7		8/30/2014 11:57:20 AM(UTC-5)	46.673956	-96.42018
8		8/30/2014 11:57:21 AM(UTC-5)	46.673956	-96.42018
9		8/30/2014 11:57:22 AM(UTC-5)	46.673956	-96.42018
10		8/30/2014 11:57:23 AM(UTC-5)	46.673956	-96.42018
11		8/30/2014 11:57:24 AM(UTC-5)	46.673956	-96.42018
12		AM(UTC-5)	46.675805	-96.42018
13		AM(UTC-5)	46.676166	-96.42018
14		AM(UTC-5)	46.67626	-96.42018
15		AM(UTC-5)	46.67634	-96.42018
16		8/30/2014 11:57:39 AM(UTC-5)	46.676407	-96.42018
17		8/30/2014 11:57:40 AM(UTC-5)	46.676534	-96.419905
18		8/30/2014 11:57:41 AM(UTC-5)	46.676561	-96.419755
19		8/30/2014 11:57:49 AM(UTC-5)	46.676838	-96.418179
20		8/30/2014 11:57:54 AM(UTC-5)	46.676896	-96.417581
21		8/30/2014 11:58:00 AM(UTC-5)	46.676956	-96.416806
22		AM(UTC-5)	46.676815	-96.415275
23		AM(UTC-5)	46.676531	-96.413828
24		AM(UTC-5)	46.676531	-96.413828
25		AM(UTC-5)	46.676531	-96.413828
26		8/30/2014 11:58:19 AM(UTC-5)	46.676347	-96.413053
27		8/30/2014 11:58:20 AM(UTC-5)	46.676341	-96.413029
28		8/30/2014 11:58:29 AM(UTC-5)	46.676625	-96.413054
29		8/30/2014 11:58:30 AM(UTC-5)	46.67664	-96.413113
30		8/30/2014 11:58:31 AM(UTC-5)	46.676658	-96.413184
31		8/30/2014 11:58:32 AM(UTC-5)	46.67668	-96.413271
32		8/30/2014 11:58:49 AM(UTC-5)	46.678126	-96.417461
33		8/30/2014 11:58:50 AM(UTC-5)	46.678268	-96.417713
34		8/30/2014 11:58:51 AM(UTC-5)	46.678434	-96.417967
35		8/30/2014 11:58:59 AM(UTC-5)	46.679626	-96.419388
36		8/30/2014 11:59:06 AM(UTC-5)	46.679879	-96.420222
37		8/30/2014 11:59:12 AM(UTC-5)	46.679871	-96.420278
38		8/30/2014 11:59:13 AM(UTC-5)	46.679936	-96.420222
39		8/30/2014 11:59:14 AM(UTC-5)	46.67989	-96.420222
40		8/30/2014 11:59:15 AM(UTC-5)	46.679856	-96.420222
41		8/30/2014 11:59:16 AM(UTC-5)	46.679834	-96.420222
42		8/30/2014 11:59:17 AM(UTC-5)	46.679834	-96.420222
43		8/30/2014 11:59:28 AM(UTC-5)	46.67971	-96.420222

Text message sent @ 11:57:11AM

Text message sent @ 11:57:39AM

Text message received @ 11:57:58AM

Visualizing Message & GPS Evidence

Visualizing Message & GPS Evidence

Visualizing Message & GPS Evidence

Questions & Answers

Carney Forensics

"Digital Evidence is Everywhere"

Cell Phones / Smart Phones

Smart Tablets

Computer Forensics

GPS Devices

Social Media / Web Mail

Sign up for our Newsletter!!

www.carneyforensics.com