Control, Yourself!

Hands-On Smartphone Security & Privacy for Audiologists

Josiah Dykstra, Ph.D.
Designer Security, LLC

Learning Outcomes

1. Attendees will be able to explain potential threats to business operations, reputation, patient privacy, and protected health information from insecure smartphones.

2. Attendees will be able to list the sensitive data stored on–and potentially recoverable from–a lost, stolen, or hacked smartphone.

3. Attendees will be able to demonstrate how to change settings to improve security and privacy of mobile devices.

Meet Dr. Josiah

Josiah Dykstra, Ph.D.

Designer Security

Financial Disclosures
Employee, U.S. Department of Defense
President, Designer Security, LLC
Author, O'Reilly Media, Inc.

Non-Financial Disclosures
Cyber Advisory Board, Bowie State University
Member, Association for Computing Machinery
Member/Program Committee, Human Factors and Ergonomics Society
Member/Conference Chair, Digital Forensics Research Workshop
Fellow, American Academy of Forensic Sciences
Member, American Association for the Advancement of Science

Roadmap

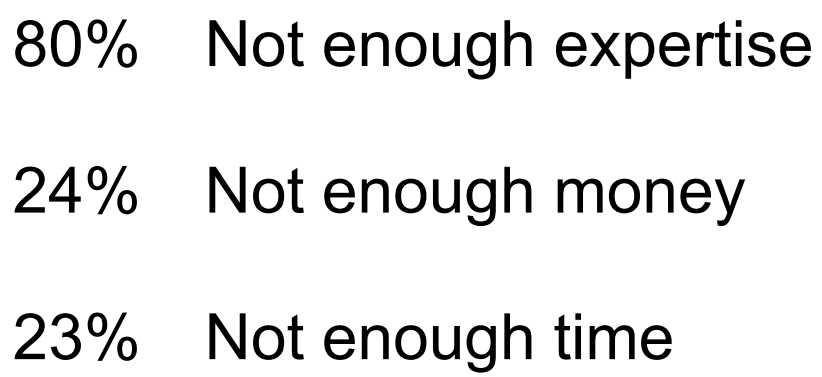
- Phones in the practice
- Real-world impact of phone theft, loss, and hacks
- Forensic recovery from an audiologist's mobile device
- 7 best-practices to securing mobile devices – *do them with me*
- Summary and further information

Slides, notes, and videos at
https://DesignerSecurity.com/ADA2020

Phones in the Practice

What limitations are preventing better protection? (Select all that apply)

104 responses



Dykstra, J., & Mathur, R. (2020). [Survey of cybersecurity in audiology]. Unpublished raw data.

https://img-s-msn-com.akamaized.net/tenant/amp/entityid/BBWig1y.img

Meet Dr. Anne and Dr. Ivan

What phone is most secure?

Market Share

Android: 86%

Apple: 14%

Software

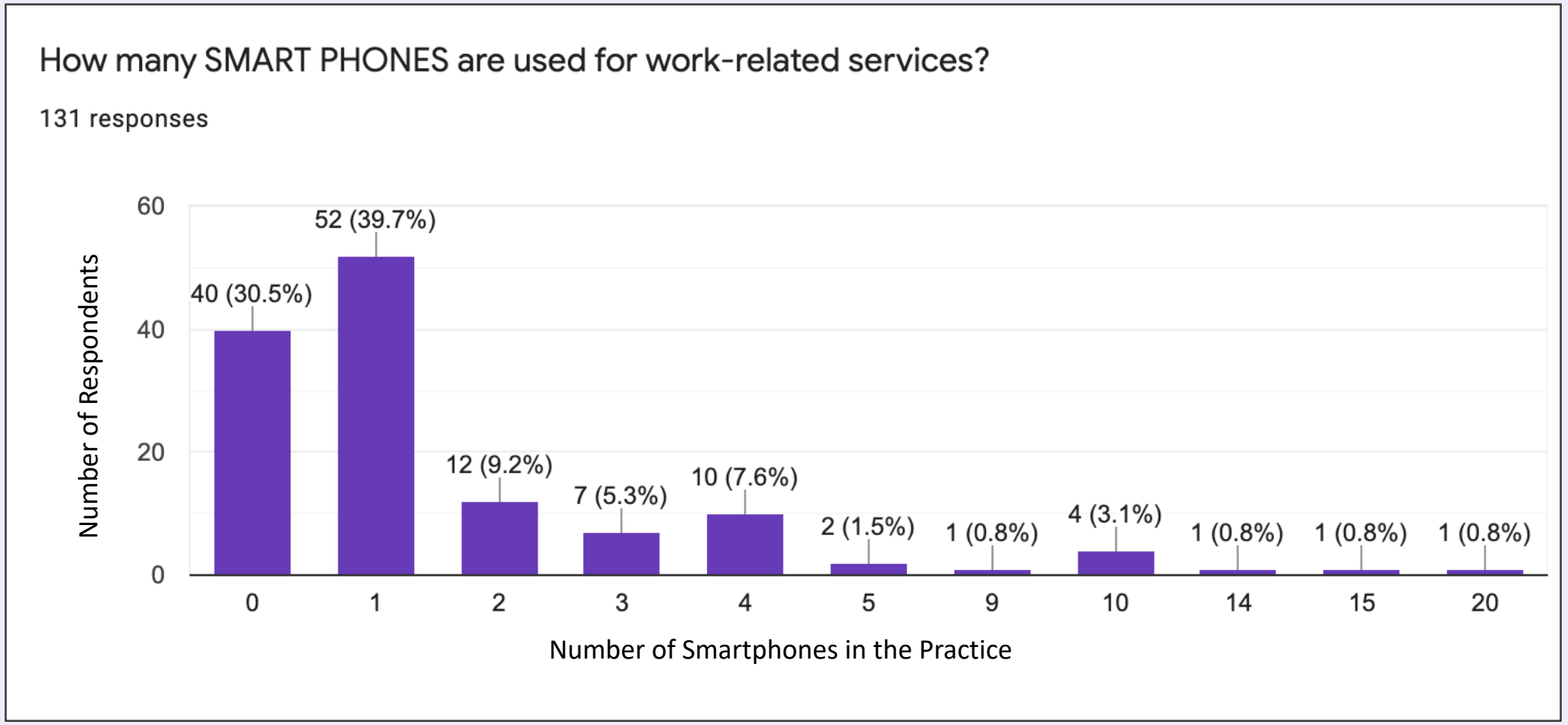
Android: Open

Apple: Closed

"Surveys have shown that around 80% of physicians use an iPhone, while most of the remainder opt for Android smartphones."

C. L. Ventola, "Mobile Devices and Apps for Health Care Professionals: Uses and Benefits," P T 39, no. 5 (2014)

Smartphones in Audiology



Dykstra, J., & Mathur, R. (2020). [Survey of cybersecurity in audiology]. Unpublished raw data.

A Day in the Life of Dr. Anne

A Day in the Life of Dr. Anne

A Day in the Life of Dr. Anne

A Day in the Life of Dr. Anne

A Day in the Life of Dr. Anne

A Day in the Life of Dr. Anne's Phone

6:00 Phone alarm
6:01 Check social media
6:05 Check work email
6:30 Check work calendar

6:59 Text staff "running late"
10:00 Scan insurance check to deposit into bank
3:00 Take fun staff photo
3:05 Post photo to Facebook

4:30 Text patient about dropping off batteries
4:50 Login to OMS to get patient address
4:55 Enter patient address into GPS

5:30 Connect to bar wifi at happy hour
6:00 Check social media
8:00 Check email

10:00 Check social media

Smartphones in the Practice

- Practice email
- Web access to EDR/OMS
- Calendar and patient schedule
- Texts to co-workers
- Calls/voicemails with patients
- Photos and videos
- Practice social media
- Bank deposits, payments
- Stored passwords
- …

Threats to Smartphones

Threats to Smartphones

Threats to Smartphones

Loss

Mostly at home

2x more likely than theft

Theft

1 in 10 owners
(68% unrecovered)

44% from public place

Pickpocket & Robbery

Mostly resold

Hacks

Social Engineering

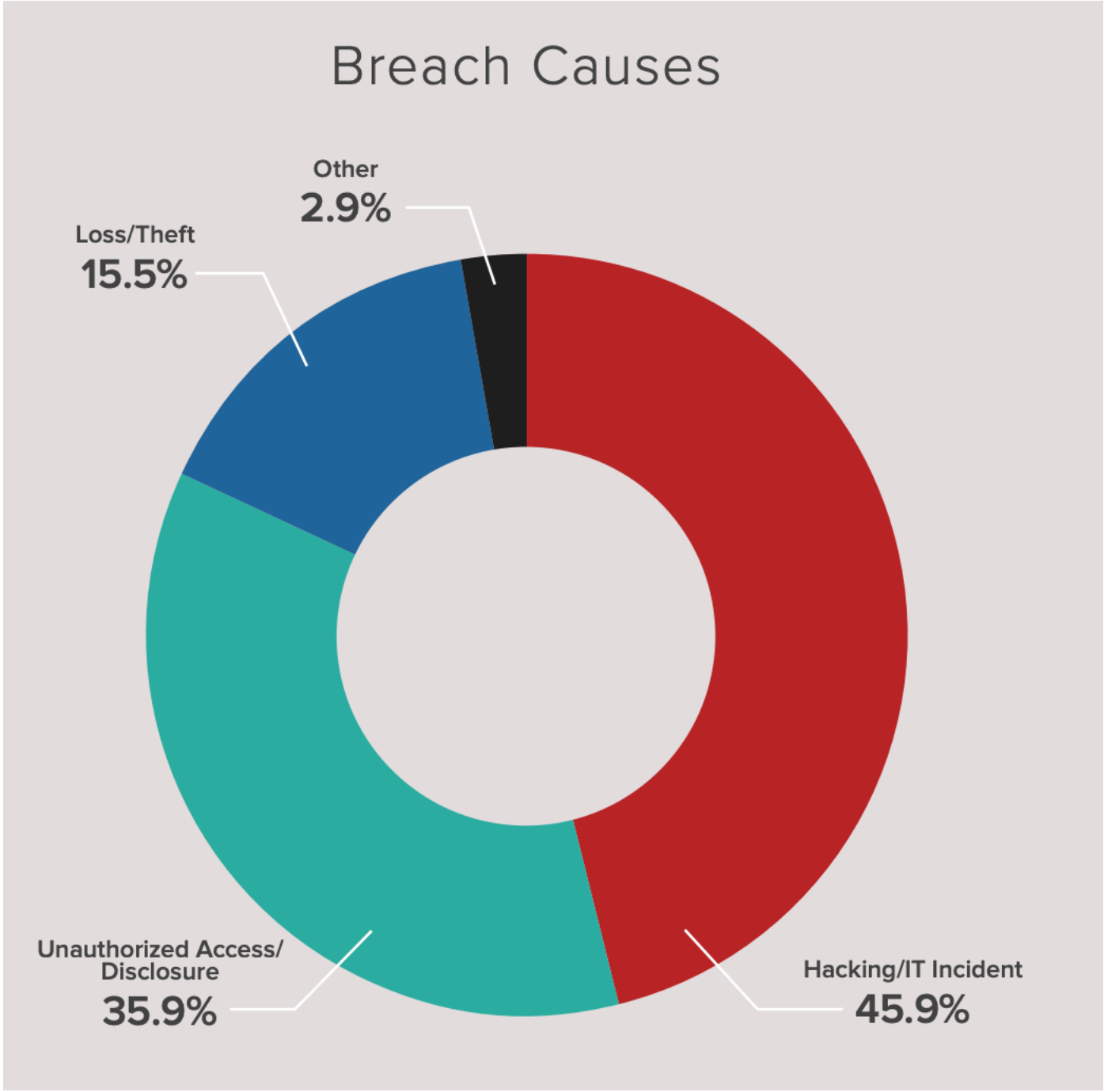
Software Bugs

Malicious Apps

Money, data, access

Insecure Passwords, Unencrypted Data

Hacking and IT Incidents was the top breach cause in healthcare in 2019.



Bitglass *Healthcare Breach Report 2020*

FOR IMMEDIATE RELEASE
July 27, 2020

Contact: HHS Press Office
202-690-6343
media@hhs.gov

Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach

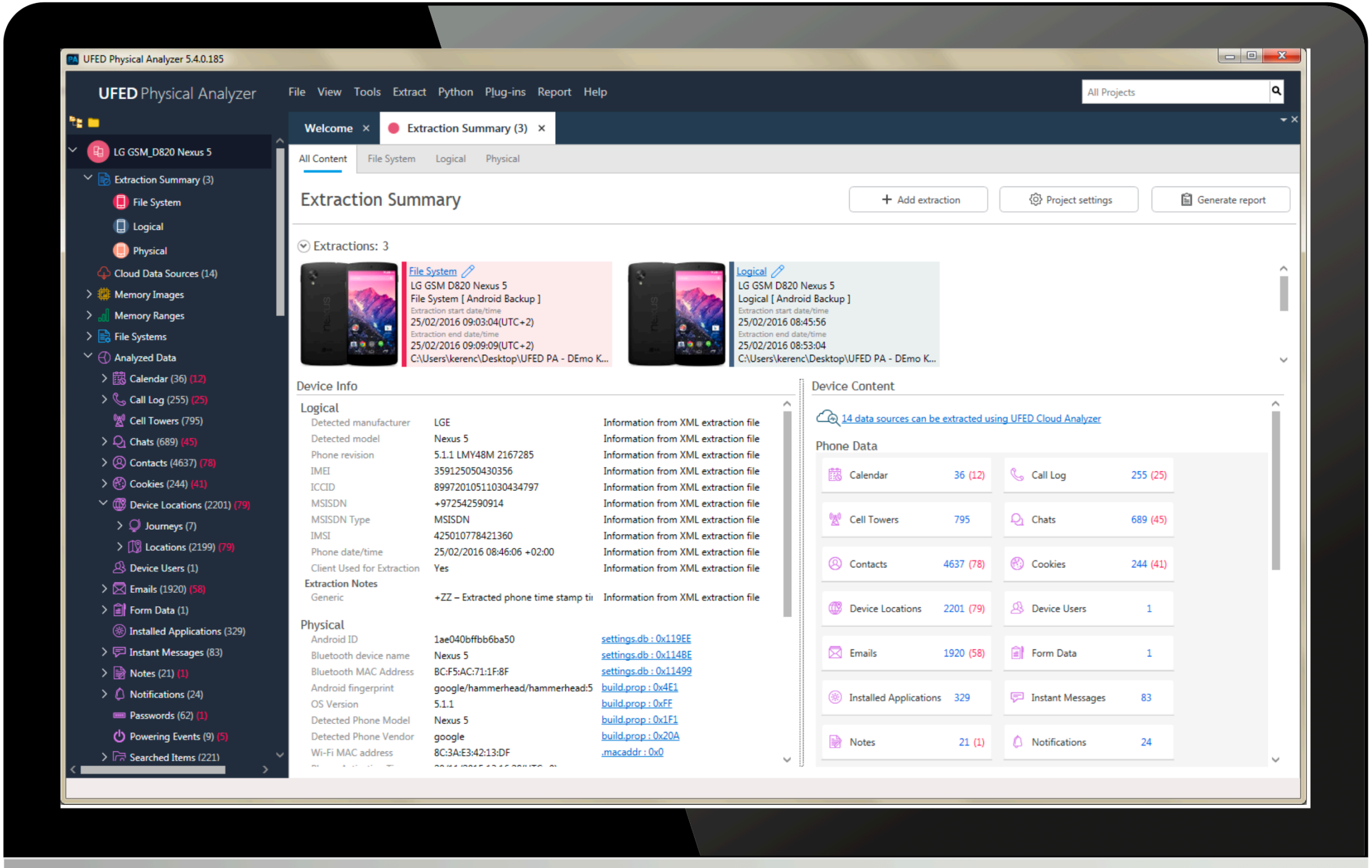
Lifespan Health System Affiliated Covered Entity (Lifespan ACE), a non-profit health system based in Rhode Island, has agreed to pay $1,040,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to implement a corrective action plan to settle potential violations of the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security Rules related to the theft of an unencrypted laptop. Lifespan ACE includes many healthcare provider affiliates in Rhode Island, and has designated itself as a HIPAA affiliated covered entity. [1]

On April 21, 2017, Lifespan Corporation, the parent company and business associate of Lifespan ACE, filed a breach report with OCR concerning the theft of an affiliated hospital employee's laptop containing electronic protected health information (ePHI) including: patients' names, medical record numbers, demographic information, and medication information. The breach affected 20,431 individuals.

https://www.hhs.gov/about/news/2020/07/27/lifespan-pays-1040000-ocr-settle-unencrypted-stolen-laptop-breach.html

Digital Forensics of Smartphones

- Installed applications
- Photos
- Text messages
- Email
- Web history
- Calendar
- Contacts
- Call history
- Voicemails
- Stored passwords
- WiFi networks
- Location data


UFED Physical Analyzer 5.4.0.185
UFED Physical Analyzer
File View Tools Extract Python Plug-ins Report Help
All Projects
Welcome
Extraction Summary (3)
All Content
File System
Logical
Physical
LG GSM_D820 Nexus 5
Extraction Summary (3)
File System
Logical
Physical
Cloud Data Sources (14)
Memory Images
Memory Ranges
File Systems
Analyzed Data
Calendar (36) (12)
Call Log (255) (25)
Cell Towers (795)
Chats (689) (45)
Contacts (4637) (78)
Cookies (244) (41)
Device Locations (2201) (79)
Journeys (7)
Locations (2199) (79)
Device Users (1)
Emails (1920) (58)
Form Data (1)
Installed Applications (329)
Instant Messages (83)
Notes (21) (1)
Notifications (24)
Passwords (62) (1)
Powering Events (9) (5)
Searched Items (221)
Extraction Summary
Add extraction
Project settings
Generate report
Extractions: 3
File System
LG GSM D820 Nexus 5
File System [Android Backup]
Extraction start date/time
25/02/2016 09:03:04(UTC+2)
Extraction end date/time
25/02/2016 09:09:09(UTC+2)
C:\Users\kerenc\Desktop\UFED PA - DEmo K...
Logical
LG GSM D820 Nexus 5
Logical [Android Backup]
Extraction start date/time
25/02/2016 08:45:56
Extraction end date/time
25/02/2016 08:53:04
C:\Users\kerenc\Desktop\UFED PA - DEmo K...
Device Info
Logical
Detected manufacturer LGE Information from XML extraction file
Detected model Nexus 5 Information from XML extraction file
Phone revision 5.1.1 LMY48M 2167285 Information from XML extraction file
IMEI 359125050430356 Information from XML extraction file
ICCID 89972010511030434797 Information from XML extraction file
MSISDN +972542590914 Information from XML extraction file
MSISDN Type MSISDN Information from XML extraction file
IMSI 425010778421360 Information from XML extraction file
Phone date/time 25/02/2016 08:46:06 +02:00 Information from XML extraction file
Client Used for Extraction Yes Information from XML extraction file
Extraction Notes
Generic +ZZ – Extracted phone time stamp ti Information from XML extraction file
Physical
Android ID 1ae040bffbb6ba50 settings.db : 0x119EE
Bluetooth device name Nexus 5 settings.db : 0x114BE
Bluetooth MAC Address BC:F5:AC:71:1F:8F settings.db : 0x11499
Android fingerprint google/hammerhead/hammerhead:5 build.prop : 0x4E1
OS Version 5.1.1 build.prop : 0xFF
Detected Phone Model Nexus 5 build.prop : 0x1F1
Detected Phone Vendor google build.prop : 0x20A
Wi-Fi MAC address 8C:3A:E3:42:13:DF .macaddr : 0x0
Device Content
14 data sources can be extracted using UFED Cloud Analyzer
Phone Data
Calendar 36 (12)
Call Log 255 (25)
Cell Towers 795
Chats 689 (45)
Contacts 4637 (78)
Cookies 244 (41)
Device Locations 2201 (79)
Device Users 1
Emails 1920 (58)
Form Data 1
Installed Applications 329
Instant Messages 83
Notes 21 (1)
Notifications 24

UFED Physical Analyzer 5.4.0.185

UFED Physical Analyzer

File View Tools Extract Python Plug-ins Report Help

All Projects

Welcome × Extraction Summary (3) × Images (22373) ×

- Instant Messages (83)
- Notes (21) (1)
- Notifications (24)
- Passwords (62) (1)
- Powering Events (9) (5)
- Searched Items (221)
- SMS Messages (243) (1)
- User Accounts (177)
- Web Bookmarks (99) (20)
- Web History (258) (13)
- Wireless Networks (1191) (1)
- Data Files
  - Applications (2564) (206)
  - Audio (204) (6)
  - Configurations (49) (3)
  - Databases (1779)
  - Documents (7) (3)
  - Images (22373) (171) (10630 non
  - Text (5063) (328)
  - Videos (135) (11)
  - Uncategorized (84865) (55206)
- Carving
  - Images
- Timeline (8875)
- Watch Lists
- Malware Scanner
- Project Analytics
  - Activity Analytics (3947)
- Hex Tags (0)
- Tags (0)

Images (22373)

Table View | Thumbnail View | Folder View

Export

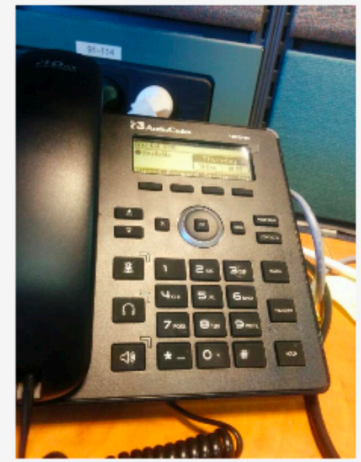
	#	Image	Name	Path
	3492		639b240e471c2c4b2bf4...	userdata (ExtX)/Root/media/0/Android/d
	3493		63a418349b59c550d88c...	userdata (ExtX)/Root/media/0/Android/d
	3494		63a667d101427331d891...	userdata (ExtX)/Root/media/0/Android/d
(2*)	3495		63a6ea94f5c1e120a48d7...	userdata (ExtX)/Root/media/0/Android/d
	3496		63a98c07bef71cd8_0_e...	userdata (ExtX)/Root/data/com.opera.brc
(2)	3497		63bb919e38a2f0b9_emb...	userdata (ExtX)/Root/media/0/UCDownlc
	3498		63cd16ec.clean	userdata (ExtX)/Root/data/com.instagram

Total: 19214 Deduplication: 8584 Items: 10630/12616 Selected: 10630 Non-system: 10630 Path: userdata (ExtX)/Root/data/com.gogii.textplus/cach

Images

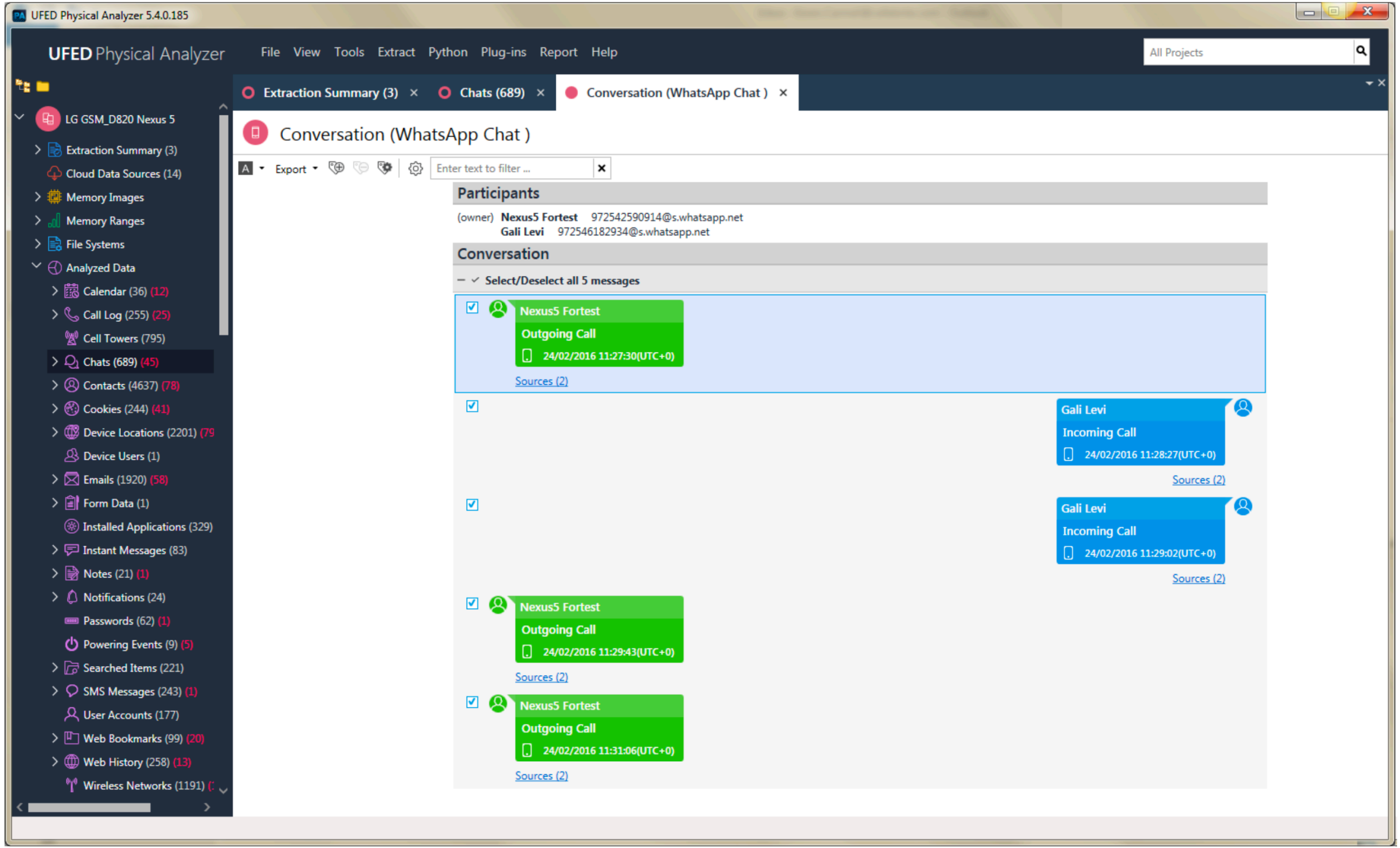
Go to

Details | Events (1)



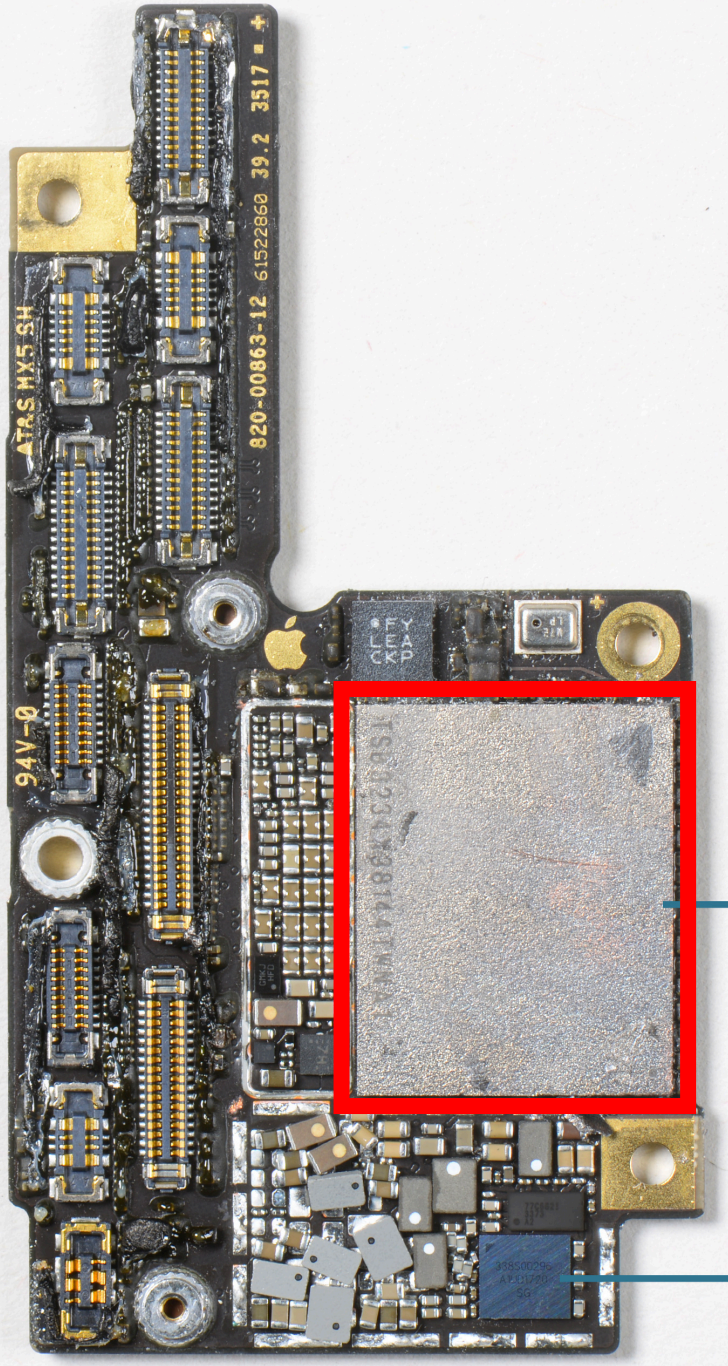
Name:
Type: Images
Size (bytes): 75480
Path: userdata (ExtX)/Root/data/com.gogii.textplus/cache/volley/-3877762851172687467/
Created: 22/12/2015 11:32:21(UTC+0)
Accessed:
Modified: 23/12/2015 11:32:17(UTC+0)
Deleted:
Extraction: Physical
MD5: e6363e52556fbad4923a0f0d77c3137f
Source file: -3877762851172687467 : 0x422

Map


UFED Physical Analyzer 5.4.0.185
UFED Physical Analyzer
File View Tools Extract Python Plug-ins Report Help
All Projects
Extraction Summary (3)
Chats (689)
Conversation (WhatsApp Chat)
LG GSM_D820 Nexus 5
Extraction Summary (3)
Cloud Data Sources (14)
Memory Images
Memory Ranges
File Systems
Analyzed Data
Calendar (36) (12)
Call Log (255) (25)
Cell Towers (795)
Chats (689) (45)
Contacts (4637) (78)
Cookies (244) (41)
Device Locations (2201) (79
Device Users (1)
Emails (1920) (58)
Form Data (1)
Installed Applications (329)
Instant Messages (83)
Notes (21) (1)
Notifications (24)
Passwords (62) (1)
Powering Events (9) (5)
Searched Items (221)
SMS Messages (243) (1)
User Accounts (177)
Web Bookmarks (99) (20)
Web History (258) (13)
Wireless Networks (1191)
Conversation (WhatsApp Chat)
Export
Enter text to filter ...
Participants
(owner) Nexus5 Fortest 972542590914@s.whatsapp.net
Gali Levi 972546182934@s.whatsapp.net
Conversation
Select/Deselect all 5 messages
Nexus5 Fortest
Outgoing Call
24/02/2016 11:27:30(UTC+0)
Sources (2)
Gali Levi
Incoming Call
24/02/2016 11:28:27(UTC+0)
Sources (2)
Gali Levi
Incoming Call
24/02/2016 11:29:02(UTC+0)
Sources (2)
Nexus5 Fortest
Outgoing Call
24/02/2016 11:29:43(UTC+0)
Sources (2)
Nexus5 Fortest
Outgoing Call
24/02/2016 11:31:06(UTC+0)
Sources (2)

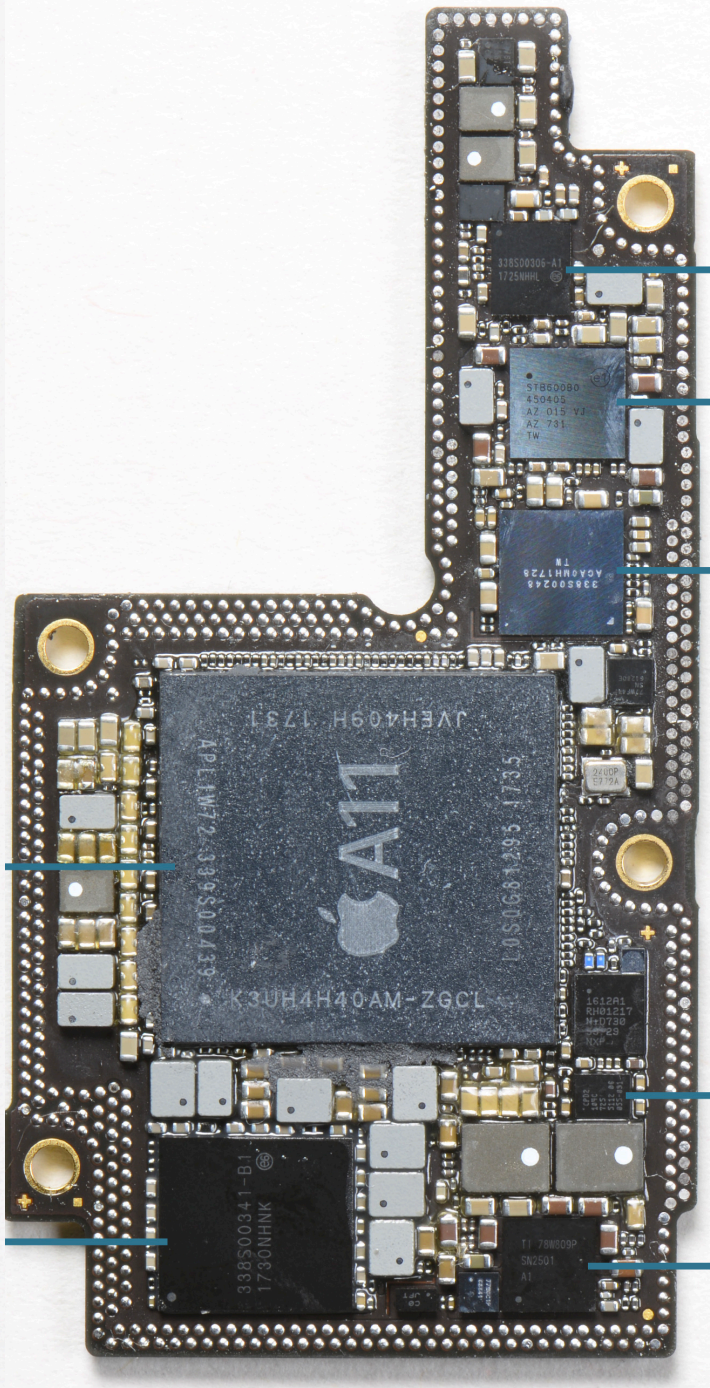

UFED Physical Analyzer
Device Locations (49394)
Location
Position
(31.902865, 34.813958)
(31.970292, 34.805567)
(32.160716, 34.809863)
Wireless Network

iPhone X Teardown



Toshiba TSB3234X38144
NAND Flash with 64-Layer
3D NAND die

338S00296 Audio Amp



338S00306 PMIC

STMicroelectronics
STB600B0 ASIC

338S00248 Audio Codec

Cypress CYPD2104
USB Type-C Controller

TI SN2501
Battery Charger

SIM Card

- Unique identification number
- Phone number
- May contain:
  - Contacts
  - Text messages

Seven Steps to Safer Smartphones

1. Install updates
2. Setup strong authentication
3. Set a lock screen
4. Install a password manager
5. Setup “find my phone” and remote wipe
6. Anonymize advertiser ID
7. Encrypt your device

#1 Install Updates

Risk management (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

45 C.F.R. § 164.308(a)(1)(ii)(B)

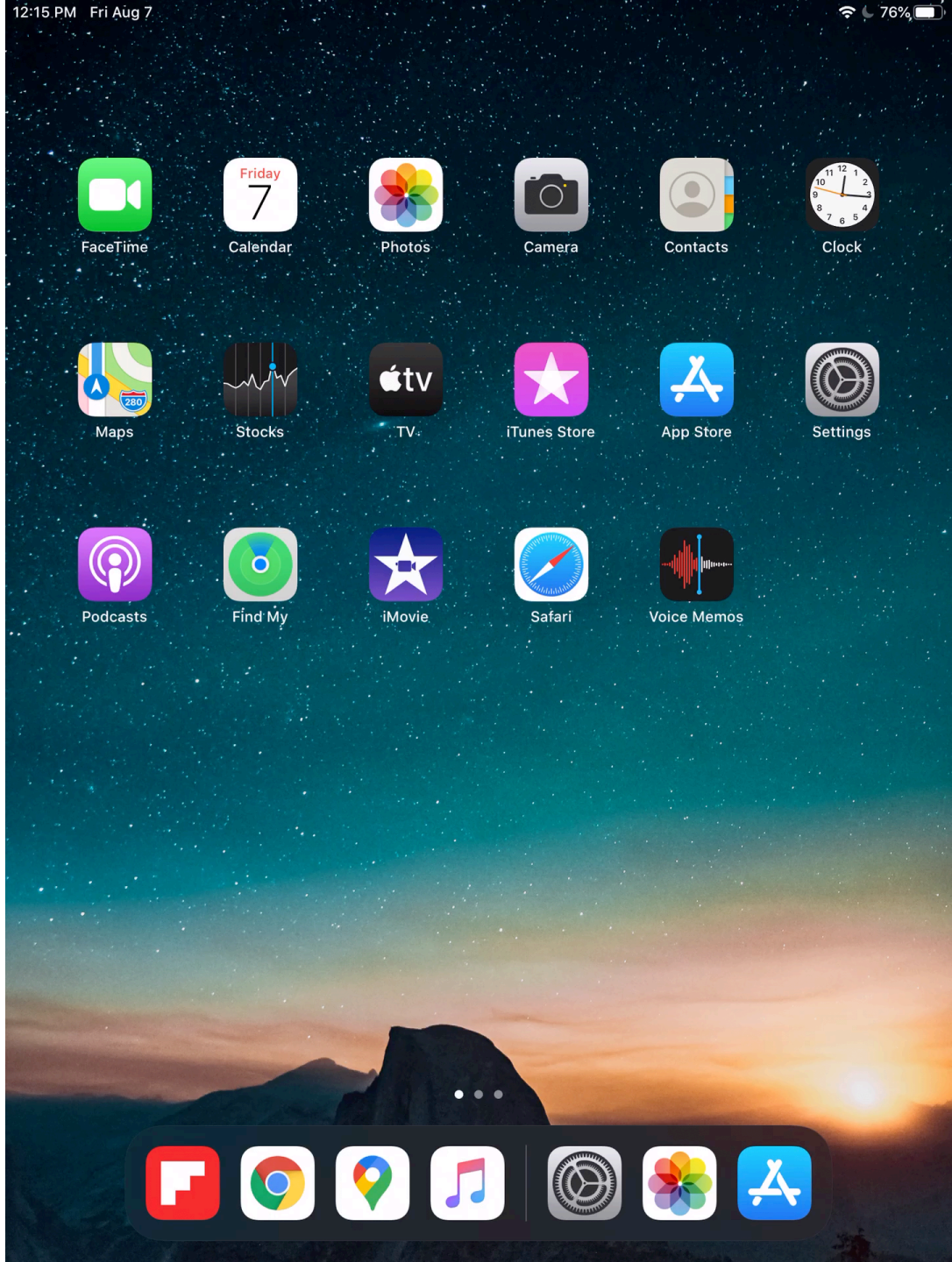
#1 for iPhone

Operating System

1. Open Settings
2. General > Software Update

Apps

1. Open App Store
2. Click Profile Icon (upper right)
3. Scroll and click Update All



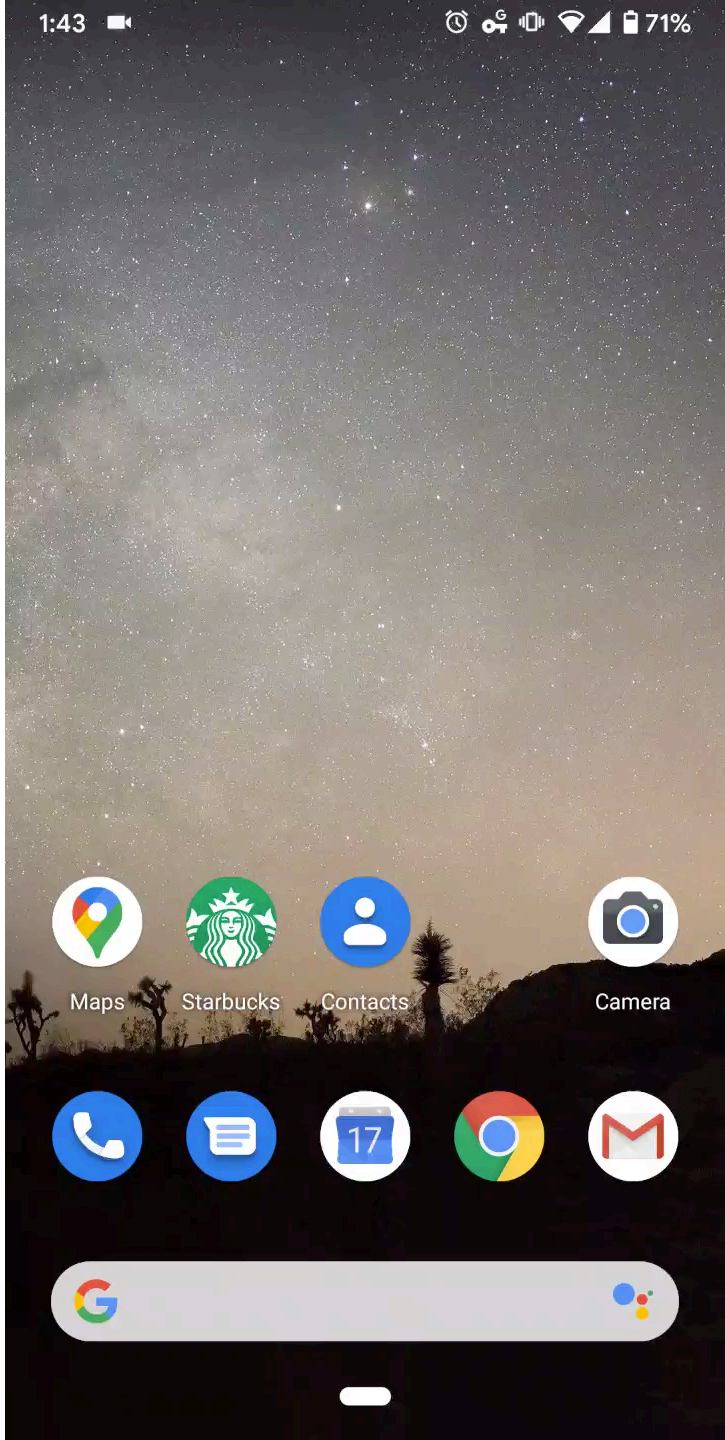
#1 for Android

Operating System

1. Open Settings
2. System > Advanced > System Update

Apps

1. Open Play Store
2. Click My Apps & Games
3. Click Update All



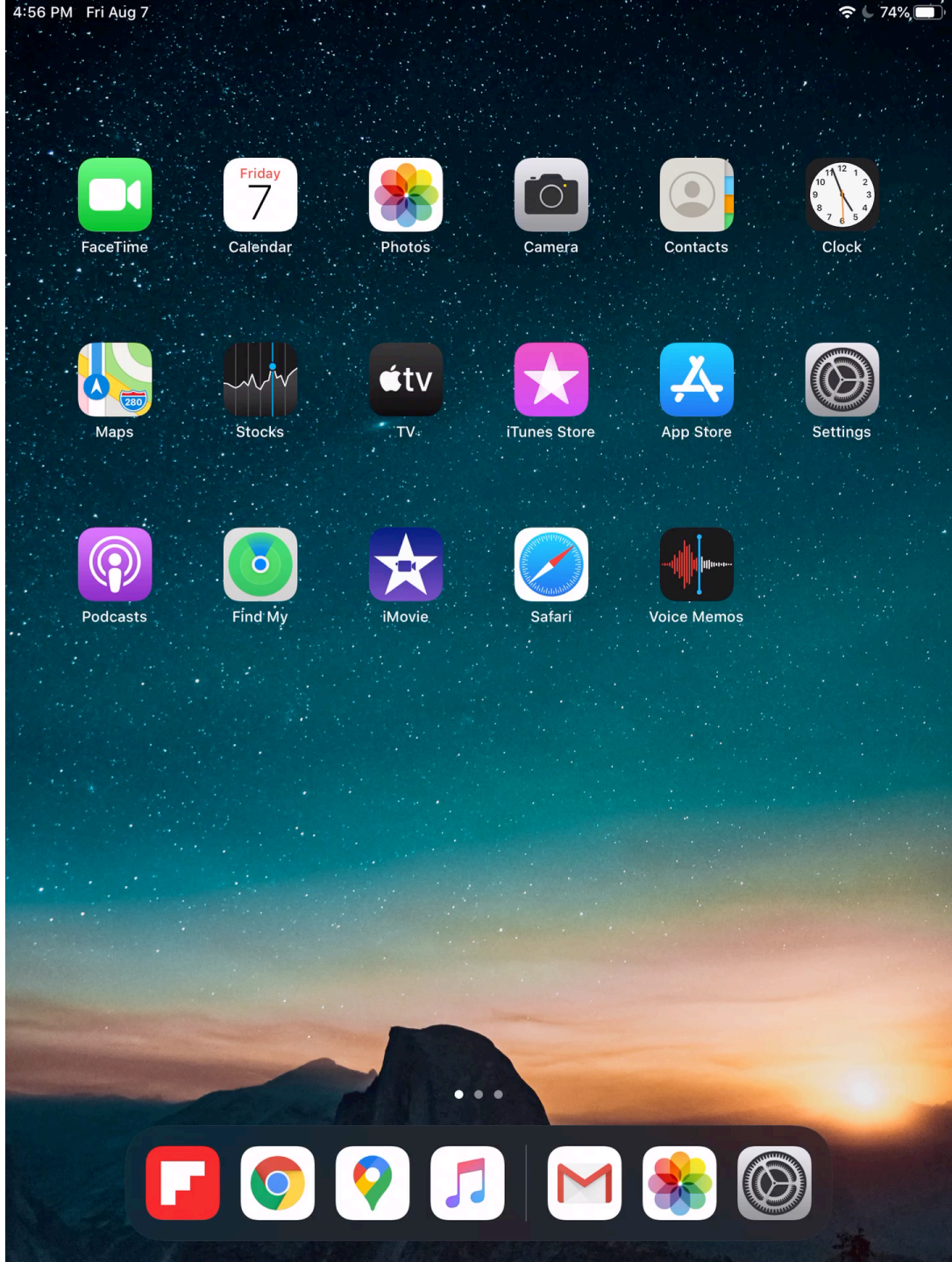
#2 Setup strong authentication

Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

45 C.F.R. § 164.312(a)(2)(i)

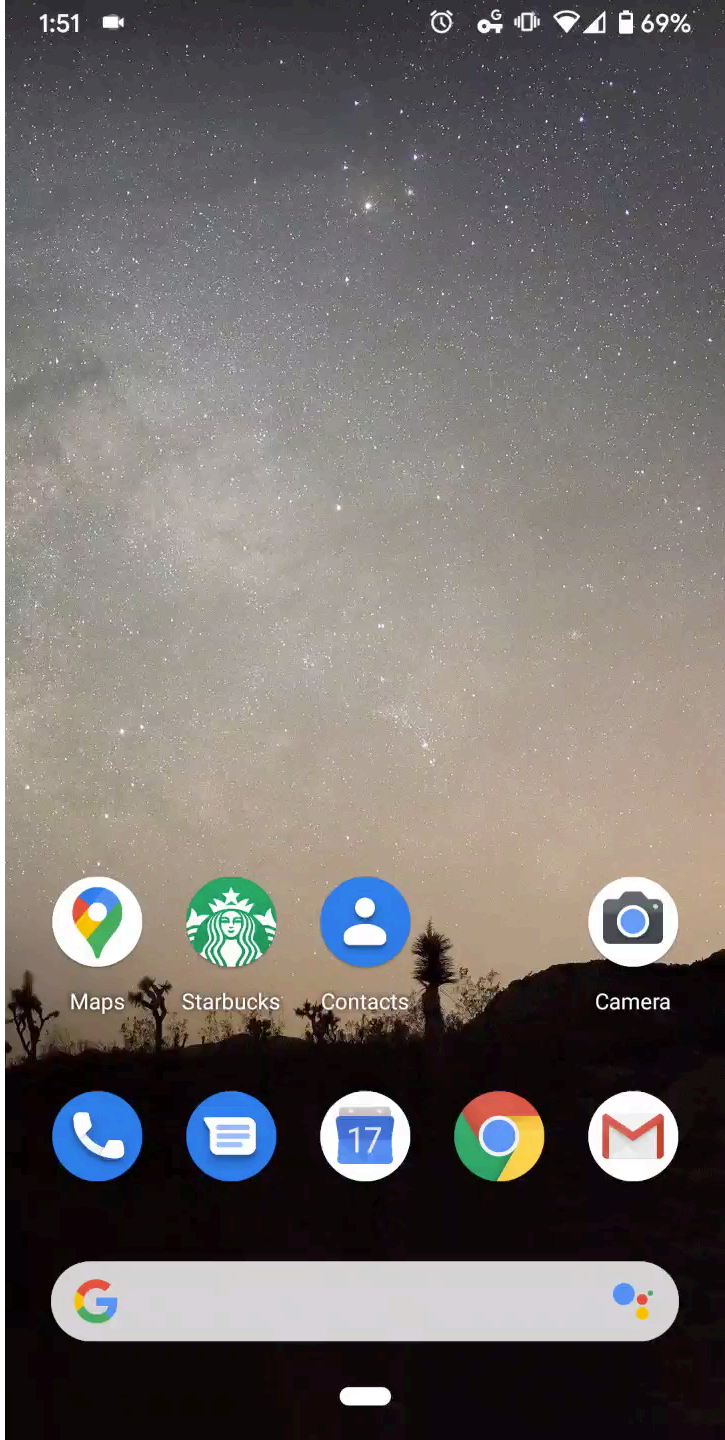
#2 for iPhone

1. Open Settings
2. Touch ID & Passcode
3. Setup fingerprint, passcode, and/or face ID



#2 for Android

1. Open Settings
2. Security
3. Under Device Security
    1. Configure Screen Lock with
        - Swipe
        - Pattern
        - PIN, or
        - Password
    2. Configure fingerprints



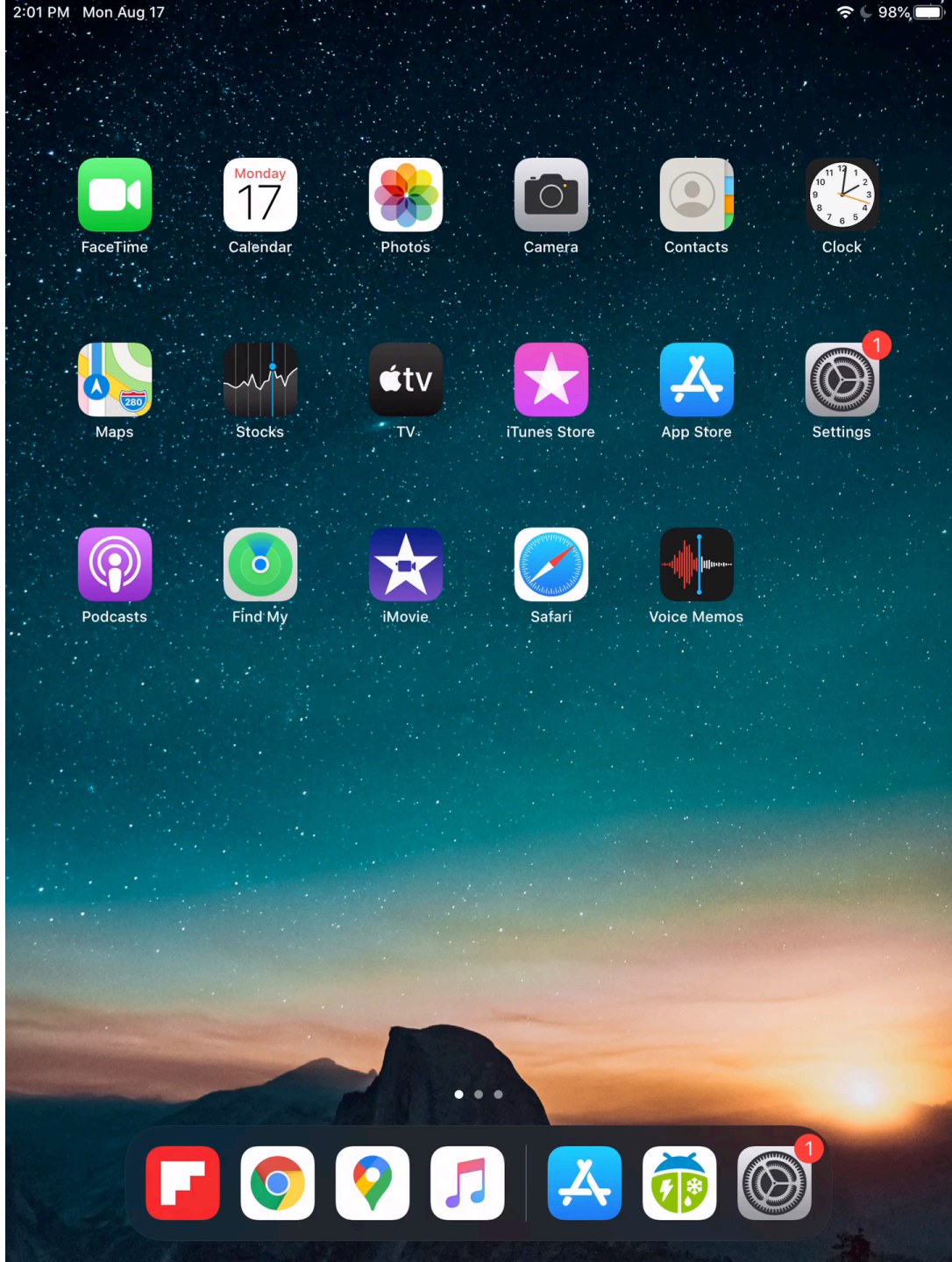
#3 Set a Lock Screen

Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

45 C.F.R. § 164.312(a)(2)(iii)

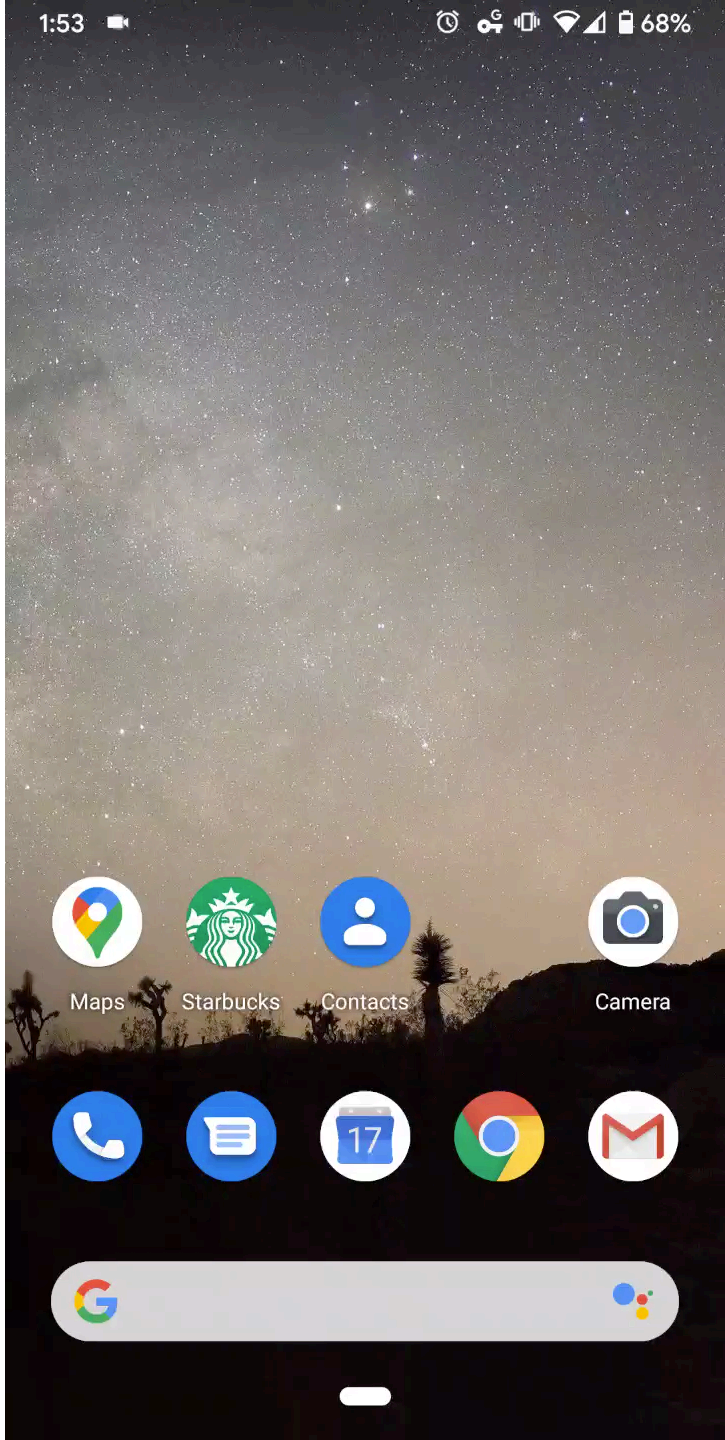
#3 for iPhone

1. Open Settings
2. Select Display & Brightness
3. Select Auto-Lock
4. Select the desired option (e.g., 30 seconds)

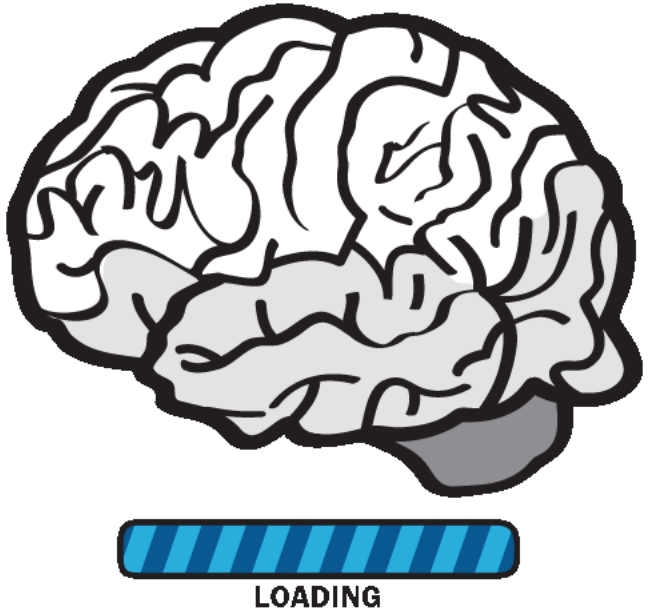


#3 for Android

1. Open Settings
2. Security
3. Under Device Security, select the gear icon next to Screen lock
4. Select “Lock after screen timeout”
5. Select the desired option (e.g., 30 seconds)



#4 Install a Password Manager



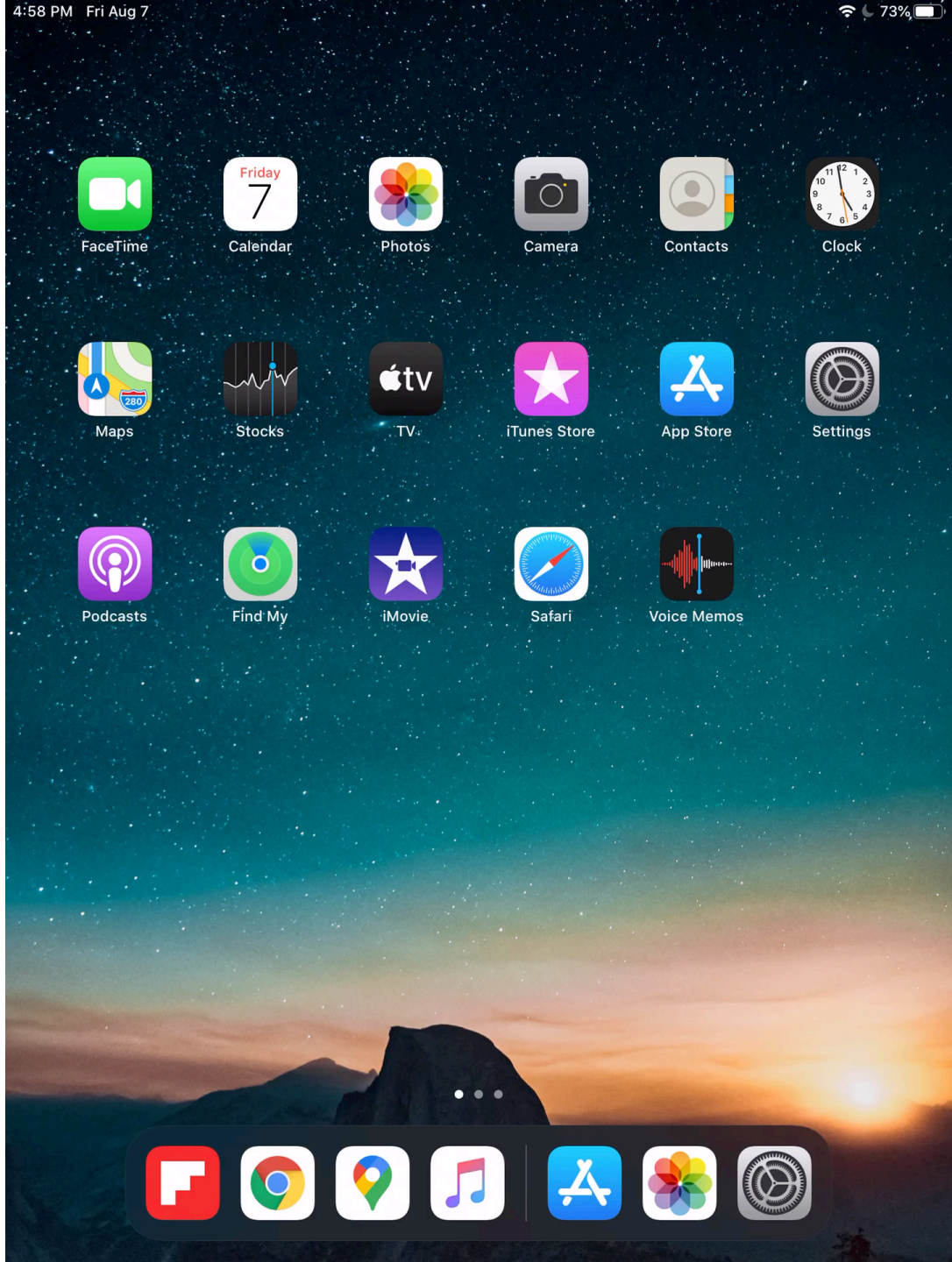
Password management (Addressable). Procedures for creating, changing, and safeguarding passwords.

45 C.F.R. § 164.308(a)(5)(ii)(D)

NIST Special Publication 800-63B (June 2017)

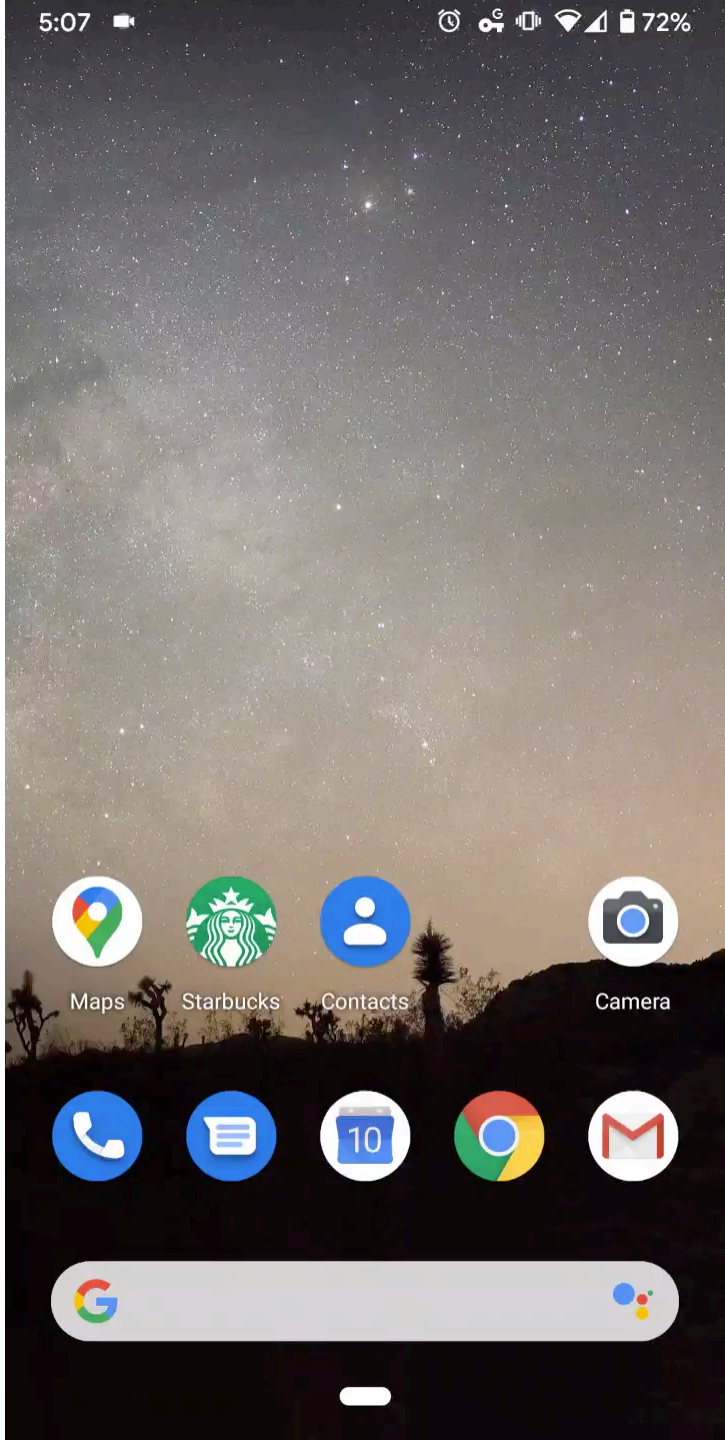
#4 for iPhone

1. Open App Store
2. Search for LastPass
3. Install and configure



#4 for Android

1. Open Play Store
2. Search for LastPass
3. Install and configure



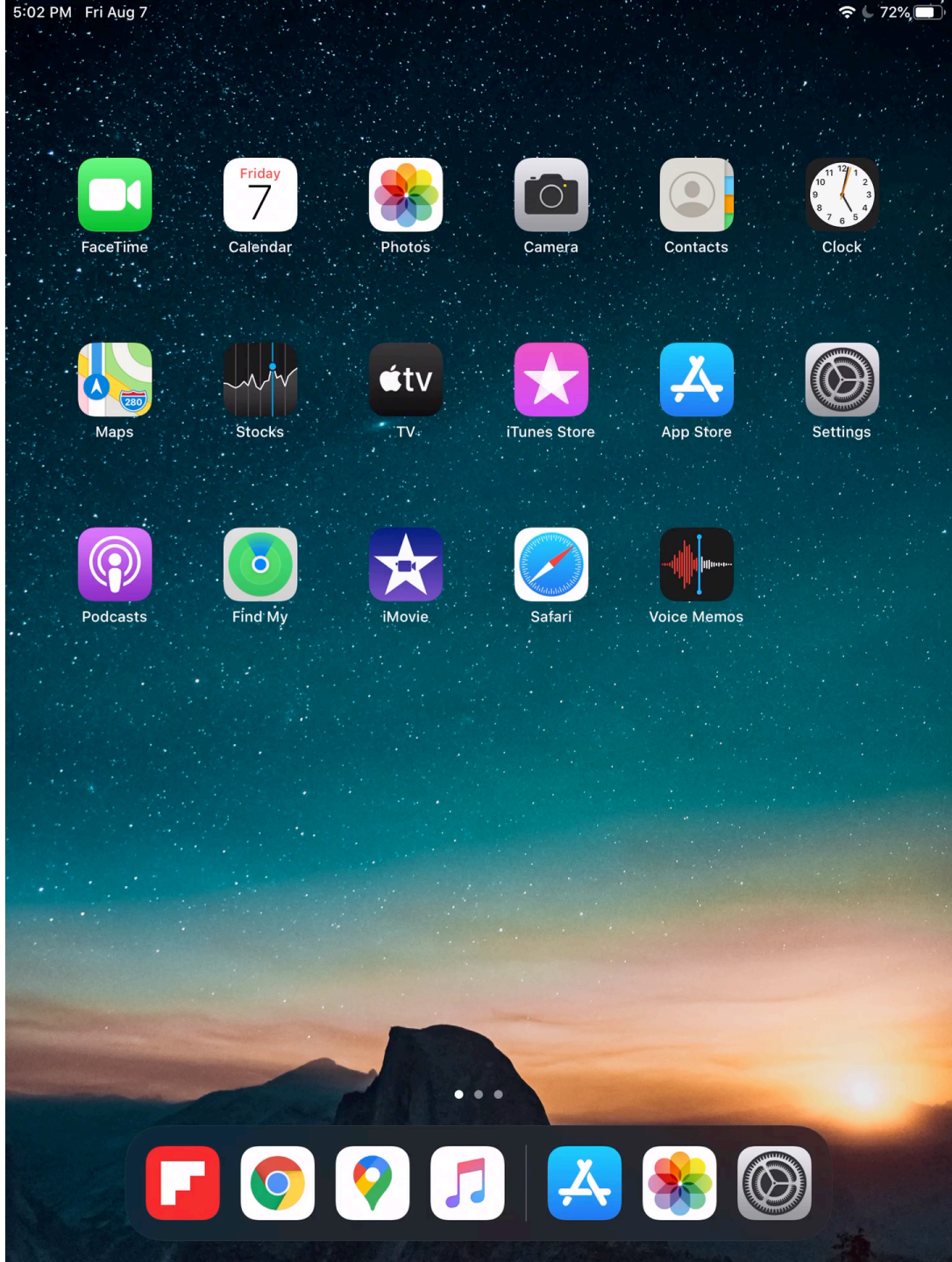
#5 Setup “Find My Phone” + Remote Wipe

A breach will be presumed to have occurred unless the party considered responsible can demonstrate that protected health information was not compromised. Remote wipe can virtually eliminated the risk of a financial penalty.

45 CFR § 164.402

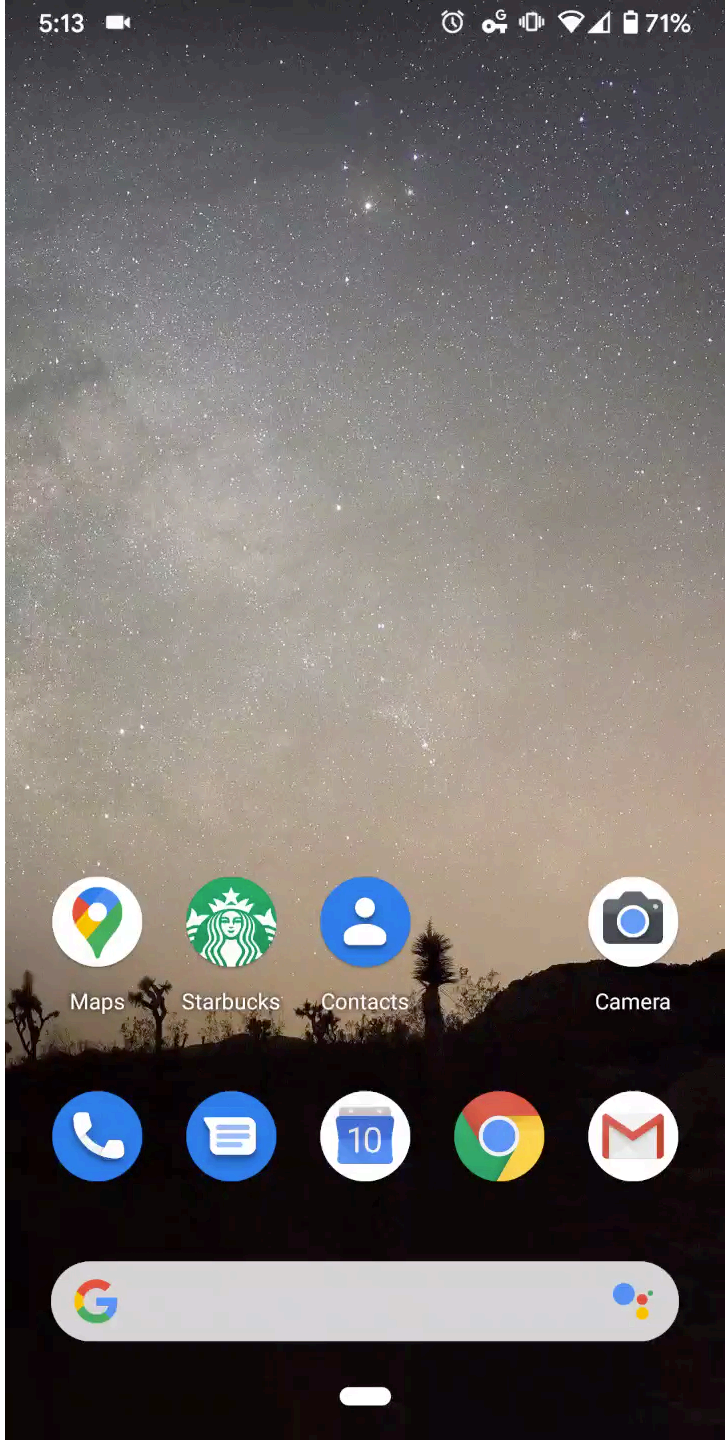
#5 for iPhone

1. Open Settings
2. Click your profile name
3. Click “Find My iPhone”
4. Click to Enable

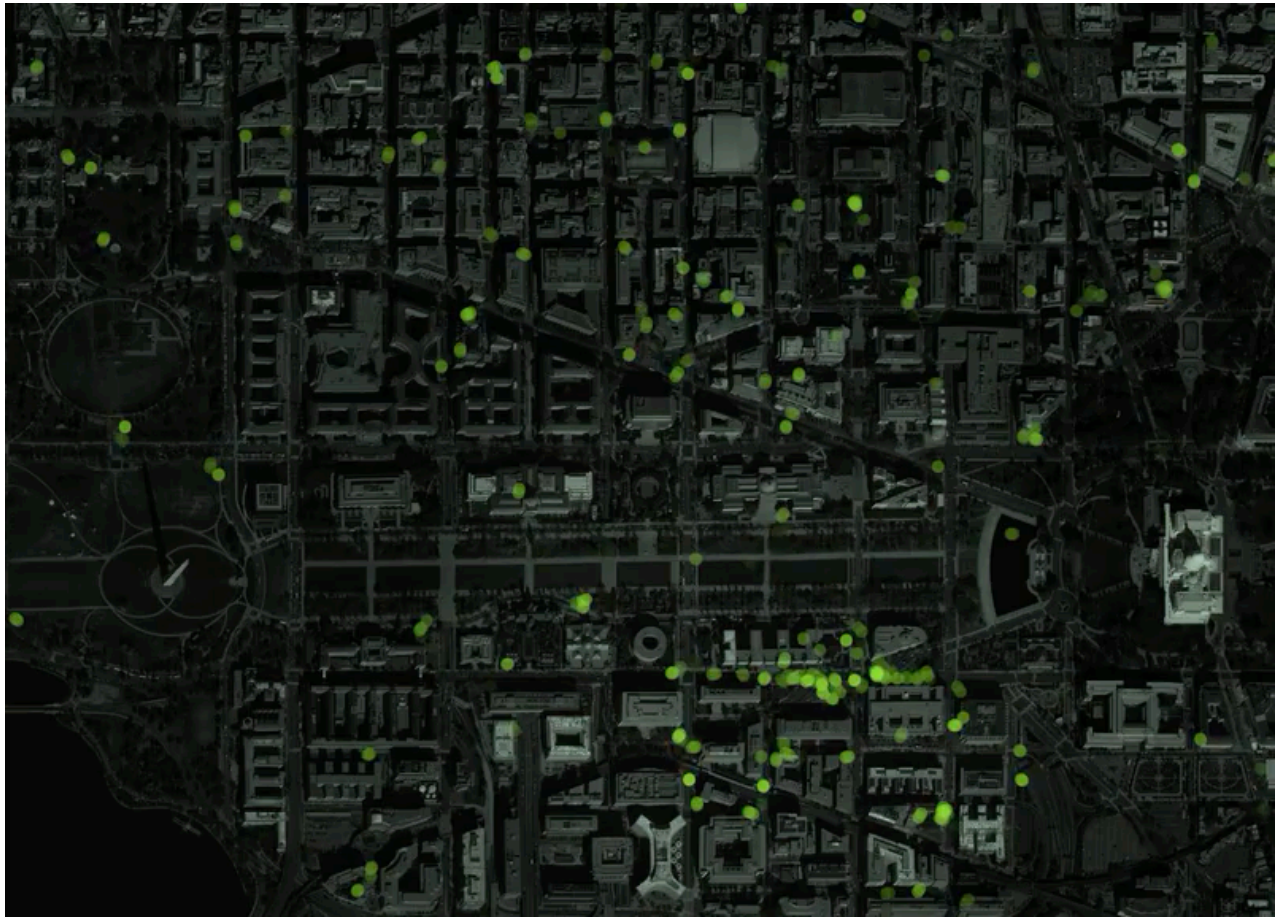


#5 for Android

1. Open Settings
2. Click Security
3. Click “Find My Device”
4. Click to Enable
5. You may need to install an app from the Play Store



#6 Anonymize advertiser ID



https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html

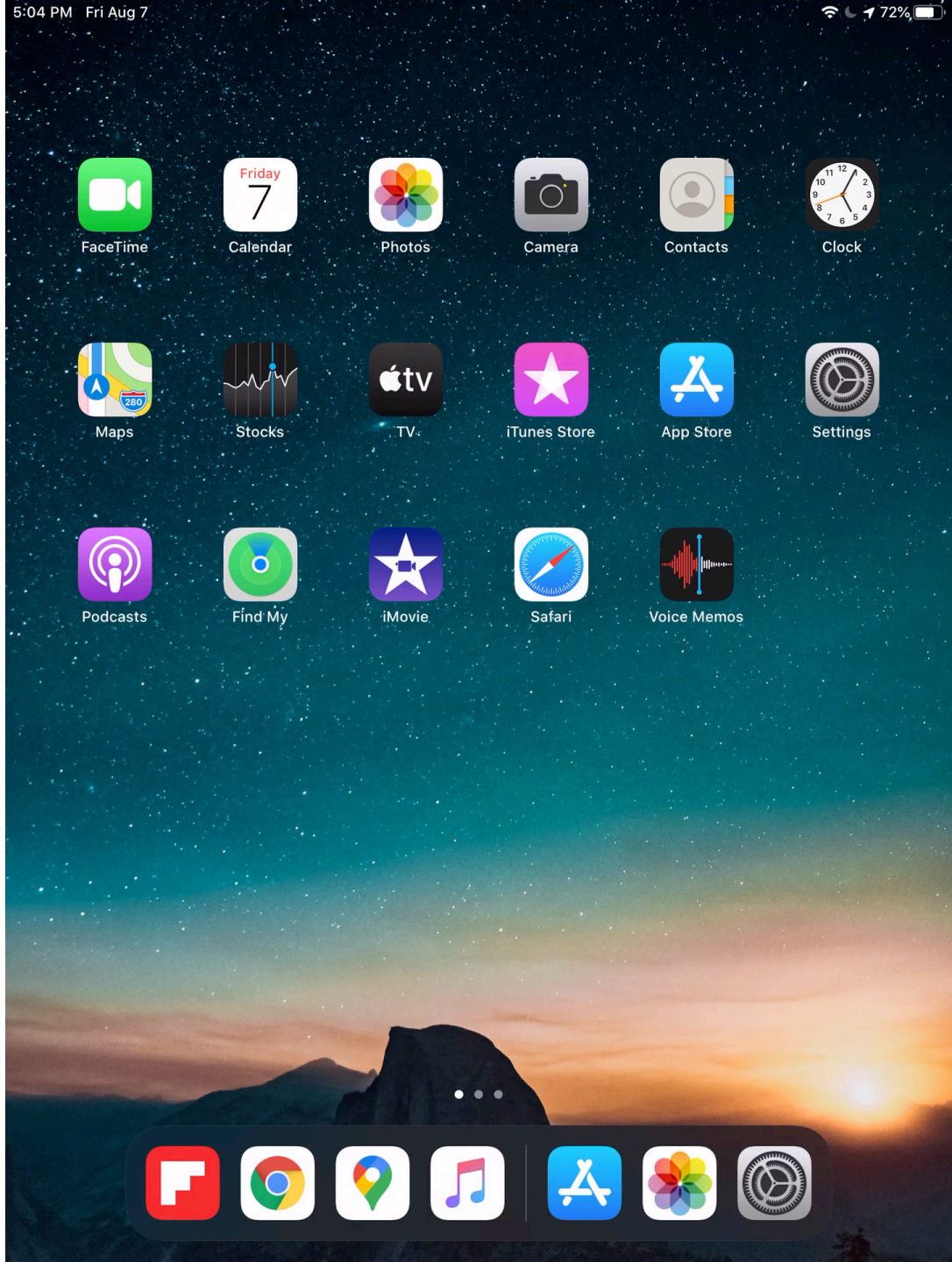
#6 for iPhone

Limit ad tracking

1. Open Settings
2. Click Privacy
3. Click Advertising
4. Ensure “Limit Ad Tracking” is enabled

Turn off location-based ads

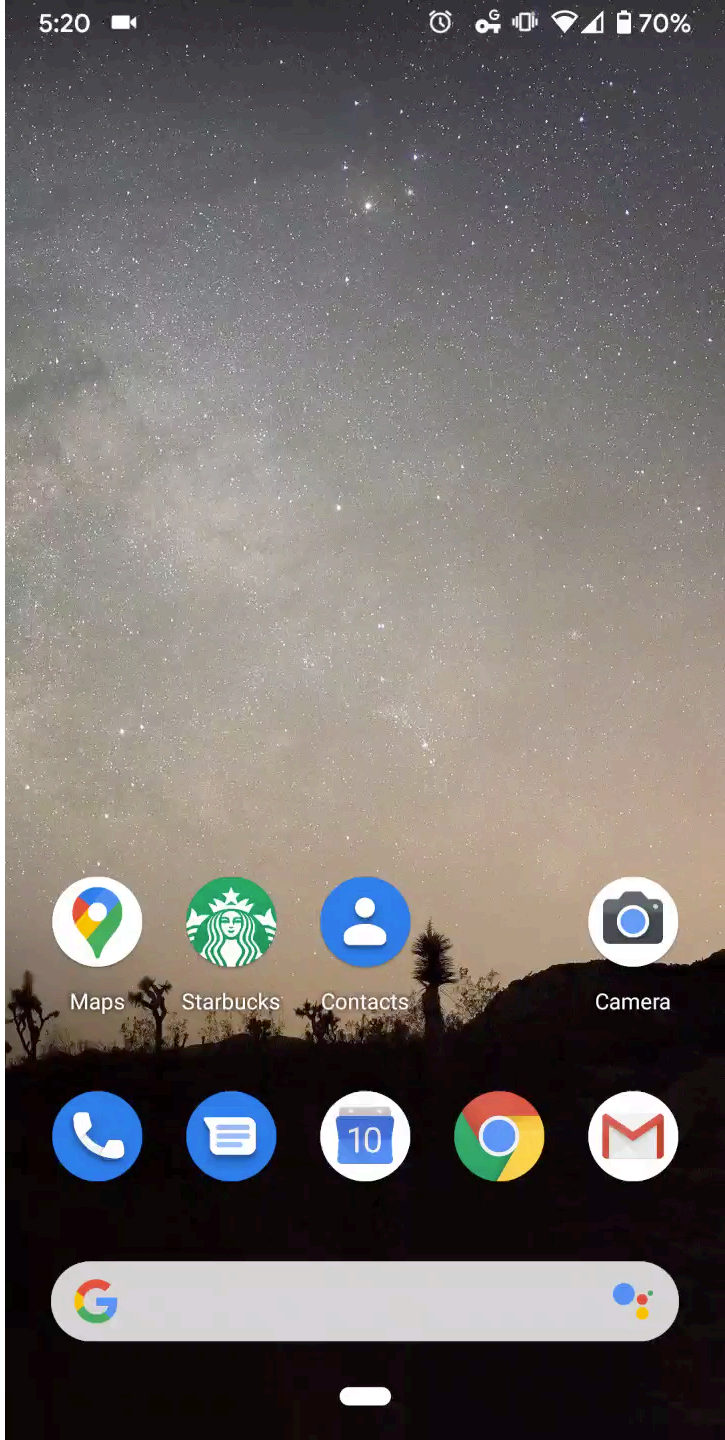
1. Go to Settings > Privacy > Location Services > System Services
2. Turn off Location-Based Apple Ads



#6 for Android

1. Open Settings
2. Click Privacy
3. Click Advanced
4. Click Ads
5. Enable “Opt out of Ads Personalization”

Note: Each Google Account and Service has its own ad settings
https://support.google.com/ads/answer/2662856



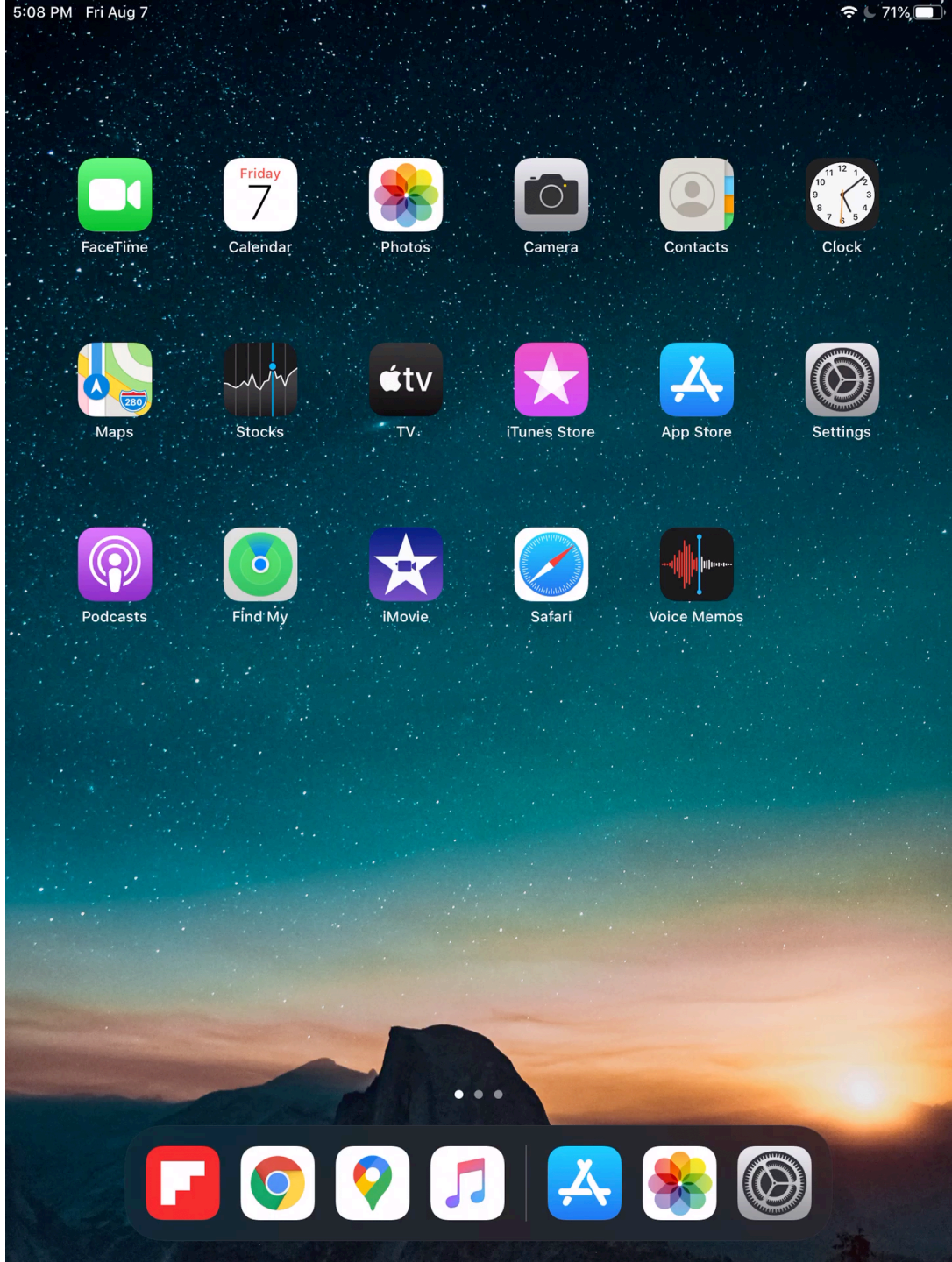
#7 Encrypt Your Device

Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

45 C.F.R. § 164.312(a)(2)(iv)

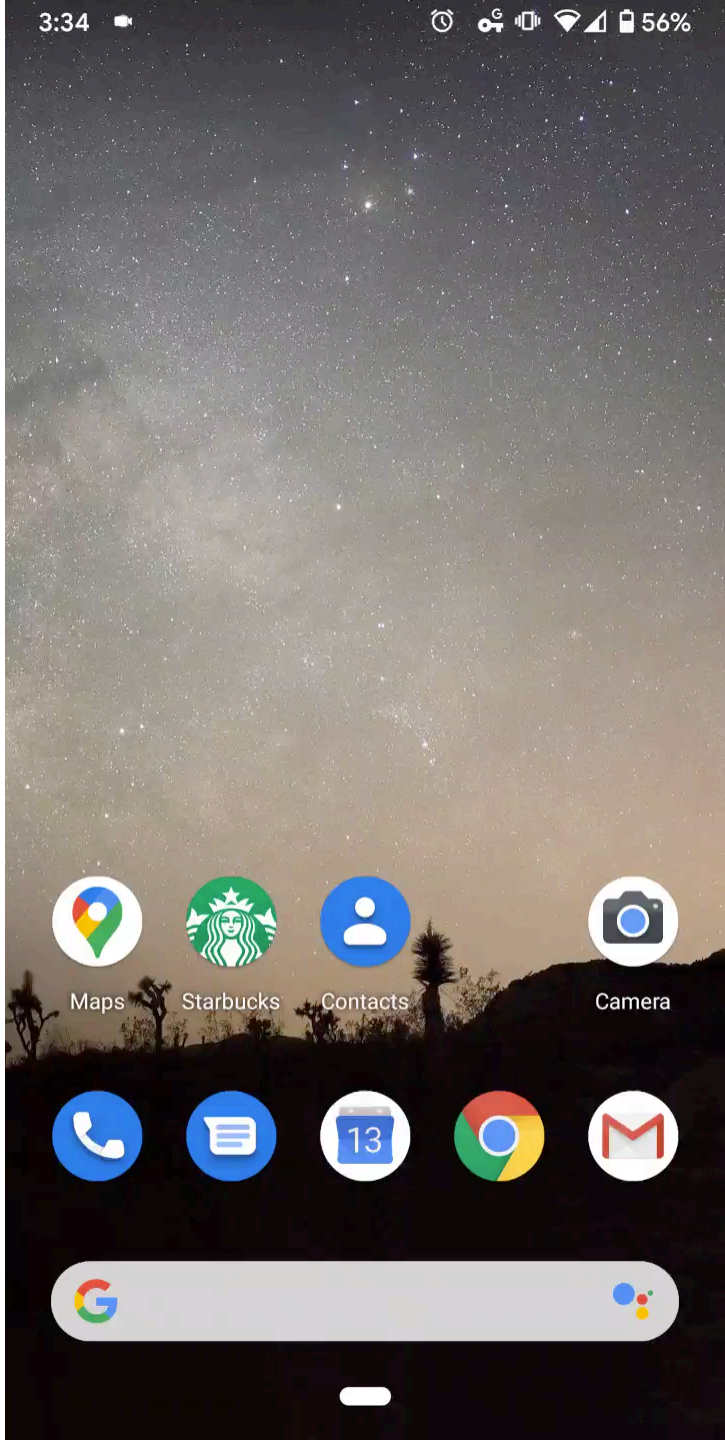
#7 for iPhone

1. Go to Settings > Touch ID & Passcode
2. Press “Turn Passcode On” if not enabled already
3. Confirm your device is encrypted by scrolling to the bottom of the screen and looking for “Data protection is enabled”



#7 for Android

1. Open Settings
2. Click Security
3. Click Encryption & Credentials
4. Enable ”Encrypt phone”



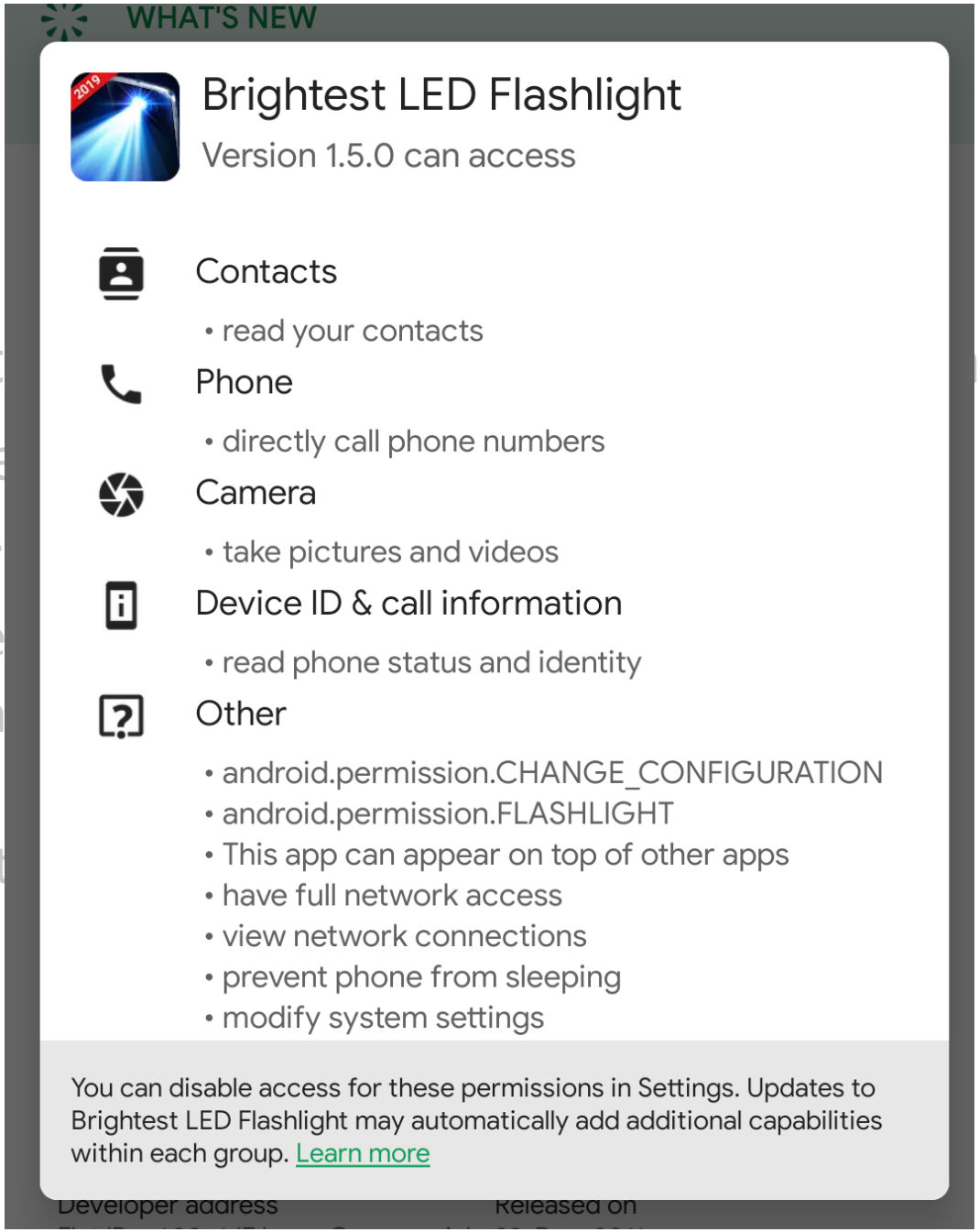
You Did It!

Summary

- Lower risk to patients' info and your business with a secure phone
- Where else is there risk in your practice?
- Ready to do more?
  - Beware apps permissions
  - Two-factor authentication (2FA)
  - VPN
  - Risk assessment

Summary

- Lower risk to pat … secure phone
- Where else is the
- Ready to do mor
  - Beware apps pe
  - Two-factor auth
  - VPN
  - Risk assessment



Summary

- Lower risk to patients' info and your business with phone security
- Where else is there risk in your practice?
- Ready to do more?
  - Beware apps permissions
  - Two-factor authentication (2FA)
  - VPN
  - Secure wipe when EOL

Slides, notes, and videos at
https://DesignerSecurity.com/ADA2020

Questions

Josiah Dykstra, Ph.D.
Josiah@DesignerSecurity.com
https://DesignerSecurity.com/ADA2020