UTILIZING DIGITAL FORENSICS IN MODERN INVESTIGATIONS

ST. CHARLES COUNTY CYBER CRIME TASK FORCE

Det. Bob O'Neal

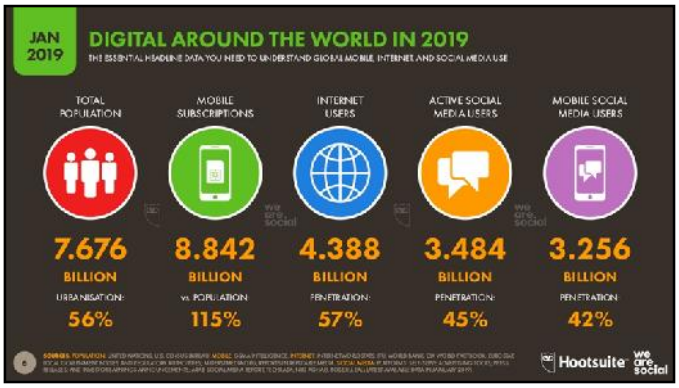
ICAC

DET. BOB O'NEAL

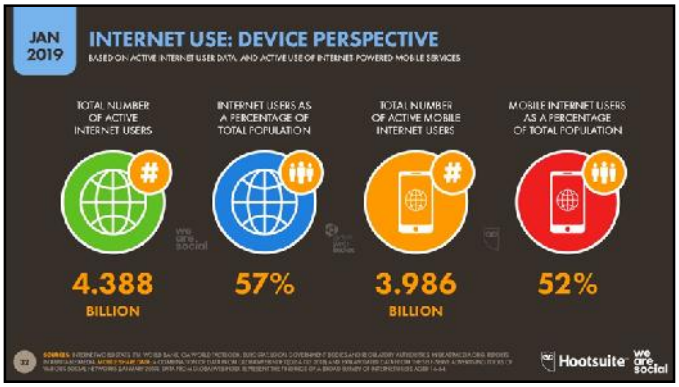
- LAW ENFORCEMENT OFFICER FOR 26 YEARS
- ASSIGNED TO THE CYBER CRIME UNIT FOR THE PAST 6 YEARS
- BACHELOR'S DEGREE FROM LINDENWOOD UNIVERSITY
- CERTIFIED COMPUTER FORENSIC EXAMINER (CFCE)
- TASK FORCE OFFICER WITH THE FBI CHILD EXPLOITATION TASK FORCE

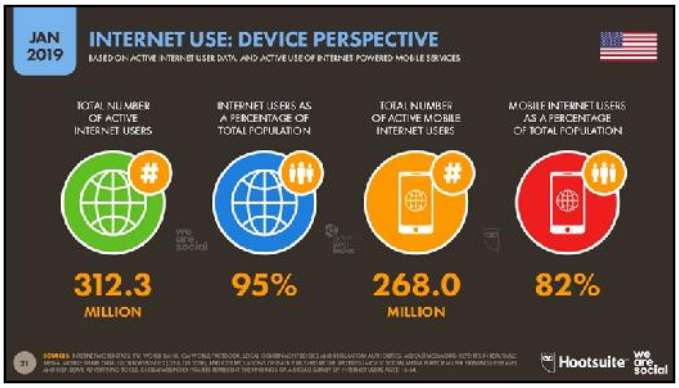
- DIGITAL STATISTICS

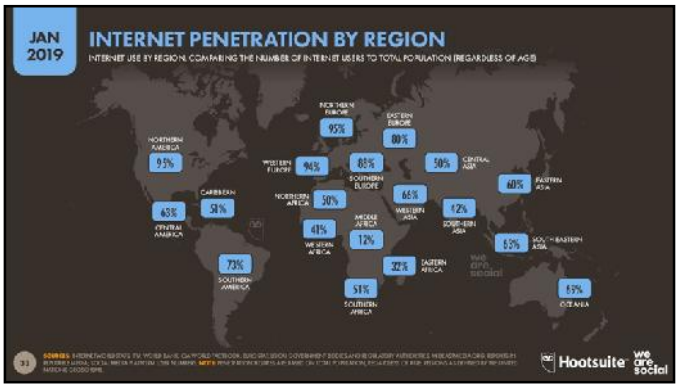
INTERNET OF THINGS (IoT)
INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

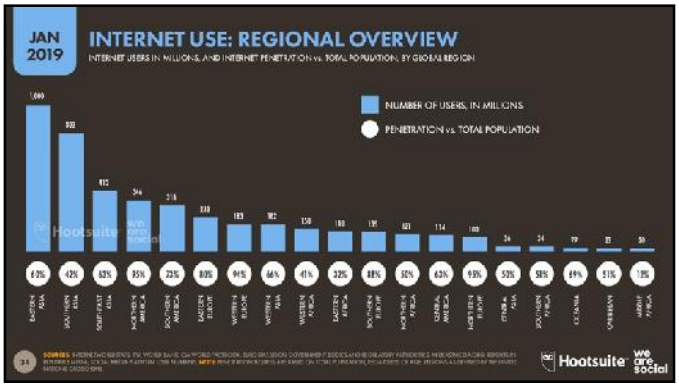

JAN 2019
DIGITAL AROUND THE WORLD IN 2019
THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND GLOBAL MOBILE, INTERNET, AND SOCIAL MEDIA USE
TOTAL POPULATION
MOBILE SUBSCRIPTIONS
INTERNET USERS
ACTIVE SOCIAL MEDIA USERS
MOBILE SOCIAL MEDIA USERS
7.676 BILLION
URBANISATION: 56%
8.842 BILLION
vs. POPULATION 115%
4.388 BILLION
PENETRATION: 57%
3.484 BILLION
PENETRATION: 45%
3.256 BILLION
PENETRATION: 42%
Hootsuite
we are social


JAN 2019
THE UNITED STATES OF AMERICA
THE ESSENTIAL HEADLINE DATA YOU NEED TO UNDERSTAND MOBILE, INTERNET, AND SOCIAL MEDIA USE
TOTAL POPULATION
MOBILE SUBSCRIPTIONS
INTERNET USERS
ACTIVE SOCIAL MEDIA USERS
MOBILE SOCIAL MEDIA USERS
327.9 MILLION
URBANISATION: 82%
347.4 MILLION
vs. POPULATION 106%
312.3 MILLION
PENETRATION: 95%
230.0 MILLION
PENETRATION: 70%
200.0 MILLION
PENETRATION: 61%
Hootsuite
we are social

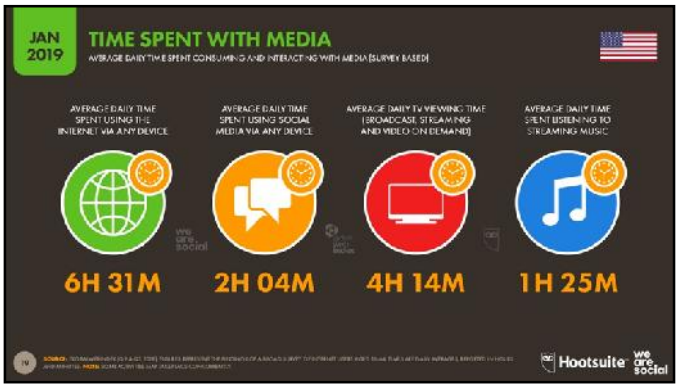

JAN 2019
INTERNET USE: DEVICE PERSPECTIVE
BASED ON ACTIVE INTERNET USER DATA, AND ACTIVE USE OF INTERNET-POWERED MOBILE SERVICES
TOTAL NUMBER OF ACTIVE INTERNET USERS
INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION
TOTAL NUMBER OF ACTIVE MOBILE INTERNET USERS
MOBILE INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION
4.388 BILLION
57%
3.986 BILLION
52%
Hootsuite
we are social

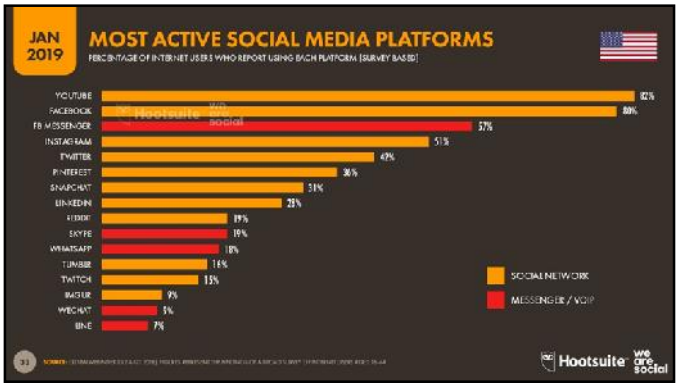

JAN 2019
INTERNET USE: DEVICE PERSPECTIVE
BASED ON ACTIVE INTERNET USER DATA, AND ACTIVE USE OF INTERNET POWERED MOBILE SERVICES
TOTAL NUMBER OF ACTIVE INTERNET USERS
INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION
TOTAL NUMBER OF ACTIVE MOBILE INTERNET USERS
MOBILE INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION
312.3 MILLION
95%
268.0 MILLION
82%
Hootsuite
we are social


JAN 2019
INTERNET PENETRATION BY REGION
INTERNET USE BY REGION, COMPARING THE NUMBER OF INTERNET USERS TO TOTAL POPULATION (REGARDLESS OF AGE)
NORTHERN EUROPE 95%
EASTERN EUROPE 80%
NORTHERN AMERICA 95%
WESTERN EUROPE 96%
SOUTHERN EUROPE 88%
CENTRAL ASIA 50%
EASTERN ASIA 60%
CARIBBEAN 54%
NORTHERN AFRICA 30%
WESTERN ASIA 65%
SOUTH-EASTERN ASIA 42%
CENTRAL AMERICA 65%
MIDDLE AFRICA 41%
WESTERN AFRICA 12%
SOUTH-EASTERN ASIA 69%
SOUTHERN AMERICA 73%
EASTERN AFRICA 32%
SOUTHERN AFRICA 51%
OCEANIA 69%
Hootsuite
we are social

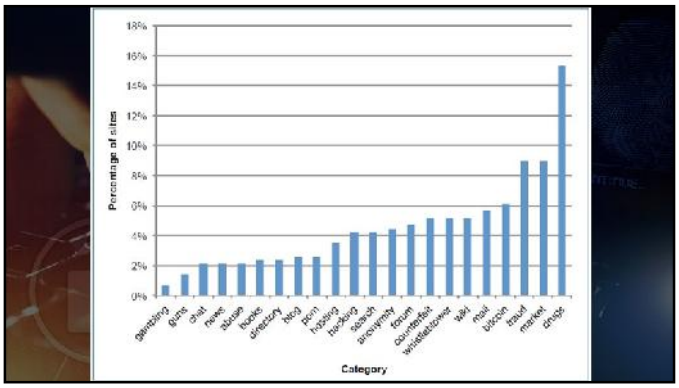

JAN 2019
INTERNET USE: REGIONAL OVERVIEW
INTERNET USERS IN MILLIONS, AND INTERNET PENETRATION vs. TOTAL POPULATION, BY GLOBAL REGION
NUMBER OF USERS, IN MILLIONS
PENETRATION vs. TOTAL POPULATION
Hootsuite
we are social

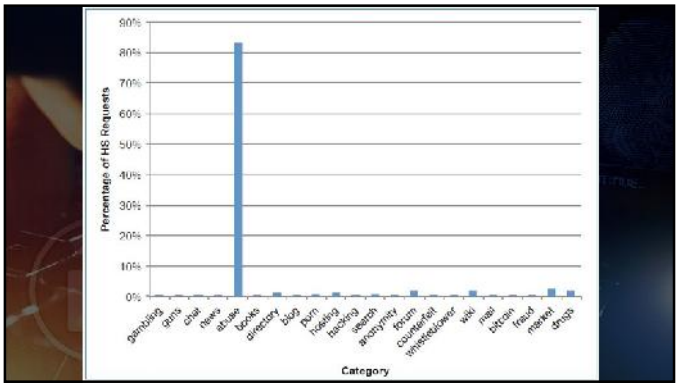

JAN 2019
ALEXA'S TOP WEBSITES
RANKING OF WEBSITES BY THE NUMBER OF VISITORS AND TOTAL PAGE VIEWS
WEBSITE TIME / DAY PAGES / VISIT
01 GOOGLE.COM 07M 42S 9.54
02 YOUTUBE.COM 08M 47S 5.02
03 AMAZON.COM 08M 09S 8.26
04 FACEBOOK.COM 09M 43S 4.00
05 REDDIT.COM 11M 40S 7.54
06 WIKIPEDIA.ORG 04M 13S 3.15
07 YAHOO.COM 04M 08S 3.60
08 TWITTER.COM 06M 23S 3.21
09 NETFLIX.COM 02M 06S 1.79
10 EBAY.COM 09M 08S 5.76
WEBSITE TIME / DAY PAGES / VISIT
11 INSTAGRAM.COM 06M 47S 3.85
12 LINKEDIN.COM 08M 19S 4.52
13 TWITCH.TV 08M 36S 2.78
14 PORNHUB.COM 08M 43S 3.35
15 MICROSOFTONLINE.COM 00M 56S 1.87
16 LIVE.COM 03M 53S 3.76
17 ESPN.COM 05M 42S 4.08
18 IMGUR.COM 03M 10S 2.57
19 PAYPAL.COM 03M 57S 4.61
20 CRAIGSLIST.ORG 09M 20S 8.45
Hootsuite
we are social


JAN 2019
TIME SPENT WITH MEDIA
AVERAGE DAILY TIME SPENT CONSUMING AND INTERACTING WITH MEDIA (SURVEY BASED)
AVERAGE DAILY TIME SPENT USING THE INTERNET VIA ANY DEVICE
6H 31M
AVERAGE DAILY TIME SPENT USING SOCIAL MEDIA VIA ANY DEVICE
2H 04M
AVERAGE DAILY TV VIEWING TIME (BROADCAST, STREAMING AND VIDEO ON DEMAND)
4H 14M
AVERAGE DAILY TIME SPENT LISTENING TO STREAMING MUSIC
1H 25M
Hootsuite
we are social


JAN 2019
MOST ACTIVE SOCIAL MEDIA PLATFORMS
PERCENTAGE OF INTERNET USERS WHO REPORT USING EACH PLATFORM (SURVEY BASED)
YOUTUBE 82%
FACEBOOK 80%
FB MESSENGER 57%
INSTAGRAM 51%
TWITTER 49%
PINTEREST 36%
SNAPCHAT 31%
LINKEDIN 28%
REDDIT 19%
SKYPE 19%
WHATSAPP 18%
TUMBLR 16%
TWITCH 15%
IMGUR 9%
WECHAT 8%
LINE 7%
SOCIAL NETWORK
MESSENGER / VOIP
Hootsuite
we are social

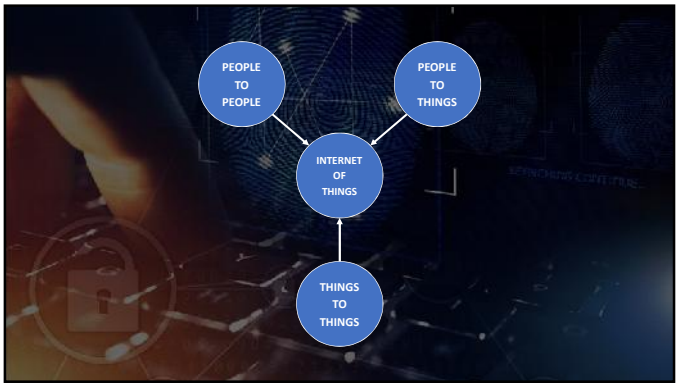

Surface Web
Yahoo!
Google
reddit
CNN.com
bing
Deep Web
Academic databases
Medical records
Financial records
Legal documents
Some scientific reports
Some government reports
Subscription only information
Some organization specific repositories
96%
of content on the Web (estimated)
Dark Web
TOR
Political pages
Drug trafficking
and other illegal activities

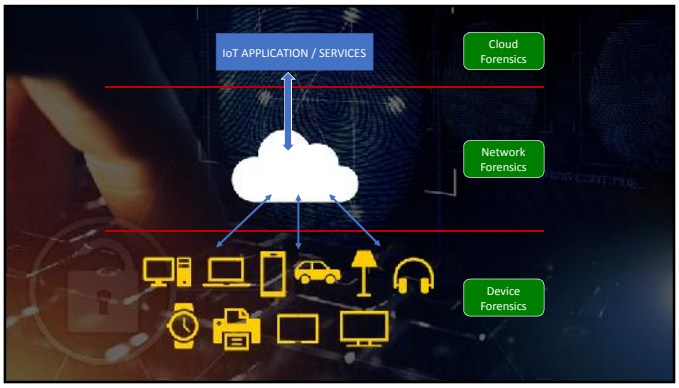

Percentage of sites
18%
16%
14%
12%
10%
8%
6%
4%
2%
0%
gambling
guns
chat
news
abuse
books
directory
blog
porn
hosting
hacking
search
anonymity
forum
counterfeit
whistleblower
wiki
mail
bitcoin
fraud
market
drugs
Category

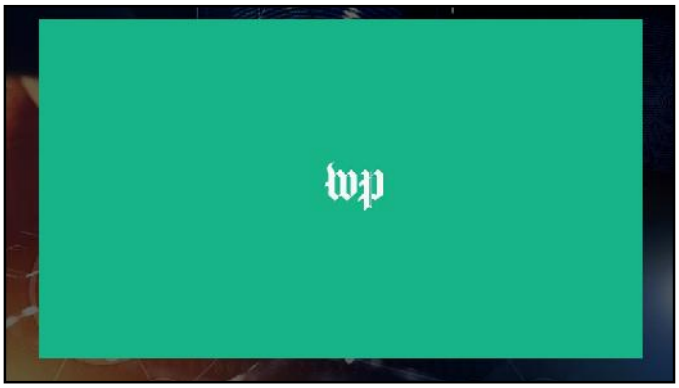

Percentage of HS Requests
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
gambling
guns
chat
news
abuse
books
directory
blog
porn
hosting
hacking
search
anonymity
forum
counterfeit
whistleblower
wiki
mail
bitcoin
fraud
market
drugs
Category

DIGITAL STATISTICS
- INTERNET OF THINGS (IoT)

INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES







IDENTIFICATION

- Understand the case.
- Assess the minimum set of the IoT evidence needed.
- Estimate the cost in manpower, time, and money.
- Start with what is/was available.
- Consult with a legal team as often as possible.

PRESERVATION

- Seek support from manufacturers, vendors, and customer service.
- Only collect the evidence that is collectable; avoid destroying evidence.
- Save the data in a commonly acceptable format if possible.
- Take pictures of IoT devices if necessary.

ANALYSIS

- Seek professional opinions of the IoT evidence experts.
- Study the interaction and relationship between IoT devices and local or remote devices.
- Know the lifecycle of the IoT devices.
- Understand the IoT reactions to its environment.

PRESENTATION

- Expert testimony may need to be provided by a team of experts.
- Use as many pictures as possible if they are sufficient to explain the situation to the jurors.
- A simple experiment on how an IoT device reacts to its environment can be equivalent to hundreds of pictures.
- Only discuss the IoT devices from which you can collect evidence.

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
•VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

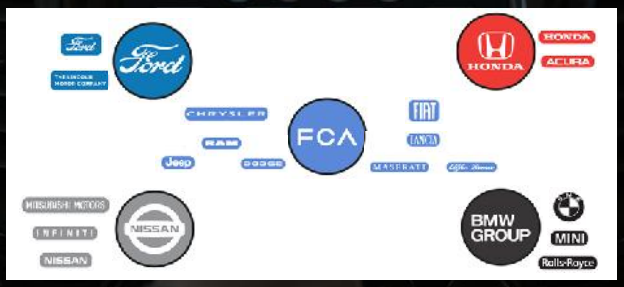
WHAT DATA CAN YOU GET?

- Vehicle / System Information
  - Serial Number • Part Number • VIN • Build Number
- Installed Application Data
  - Weather • Traffic • Facebook • Twitter
- Connected Devices
  - Phones • Media Players • USB Drives • SD Cards • Wireless Access Points
- Navigation Data
  - Tracklogs • Saved Locations • Previous Destinations • Routes

WHAT INFO DO YOU NEED?

- Year
- Make
- Model
- Trim Package
- VIN
- Photograph of radio head unit

SUPPORTED MODELS



SUPPORTED MODELS

PROPER EVIDENCE PRESERVATION

- Turn off the vehicle
- Pop the hood release
- Exit the vehicle with all key fobs
- Close all doors and wait [approx. 2 minutes]
- Disconnect vehicle power (e.g. disconnect battery or place the vehicle into transport mode)
- Tow vehicle to secure area
- Obtain a search warrant for the removal and examination of system

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
•COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

COMPUTERS / LAPTOPS

- If the computer is off – leave it off!
- If the computer is on – please consult with a computer examiner when possible.
- Photograph the screen to show what processes are running.
- Note any connections to cloud storage.
- Photograph everything connected to the device.
- Evaluate the impact of pulling the plug vs. shutting the computer down.

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
•MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

FIRST HANDHELD MOBILE PHONE - 1983

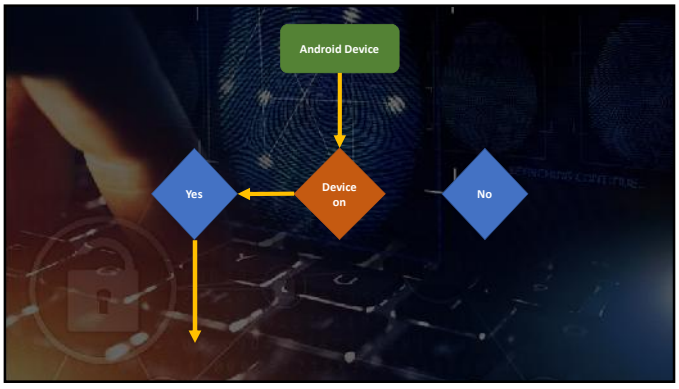
MOBILE PHONES - 2019

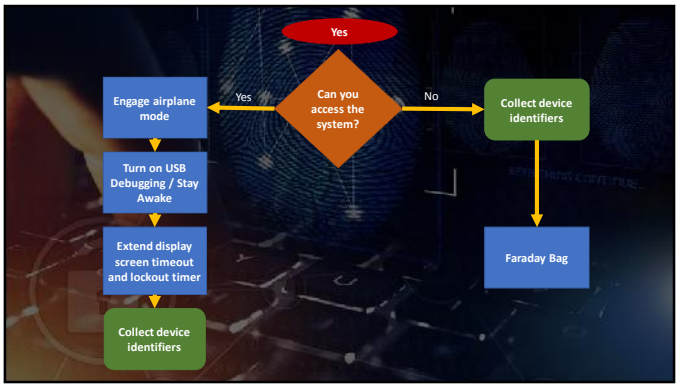
ANDROID

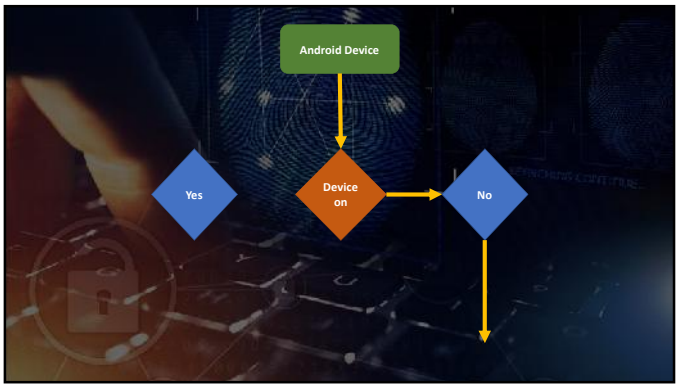

iPHONE

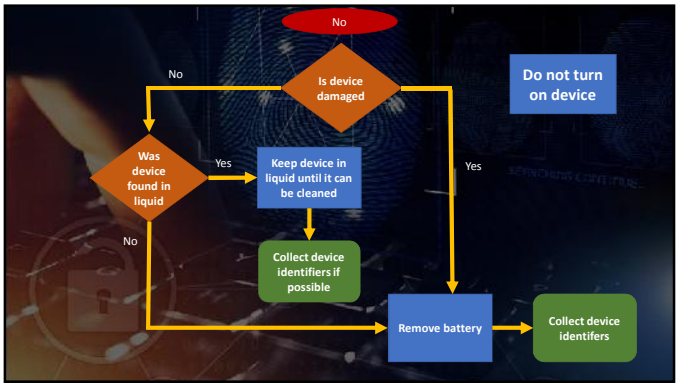
ANDROID SECURITY

- After 24 hours since last unlock, biometrics are disabled.
- May randomly require a passcode prior to 24 hours since last unlock.
- When phone is restarted, biometrics are disabled and passcode is required.
- If device is found unlocked – remove passcode in settings or repeatedly interact with screen to prevent locking until it can be examined.
- Turn on Airplane mode and USB Debugging (if possible).
- Connect to power source
- If device is found off – leave off!



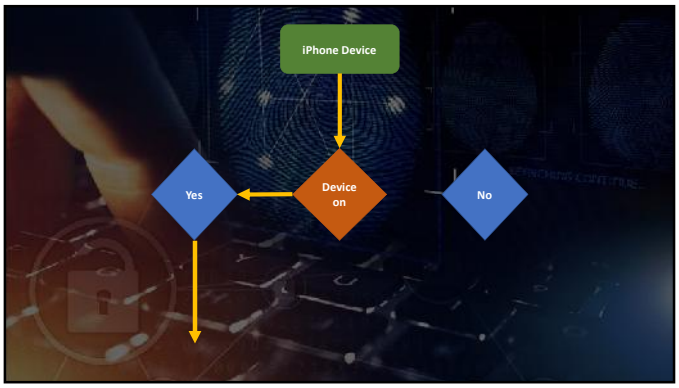

Yes
Can you access the system?
Yes
No
Engage airplane mode
Collect device identifiers
Turn on USB Debugging / Stay Awake
Extend display screen timeout and lockout timer
Faraday Bag
Collect device identifiers

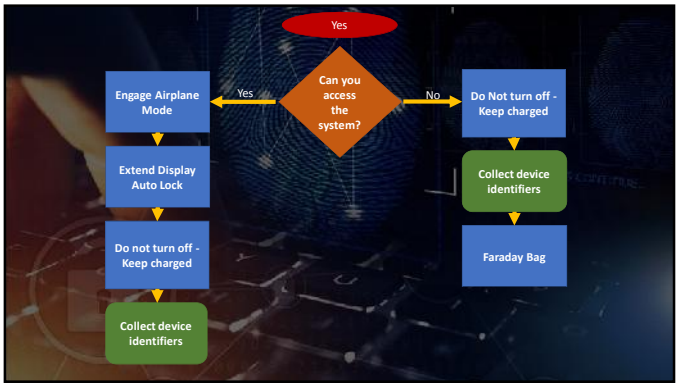

Android Device
Yes
Device on
No

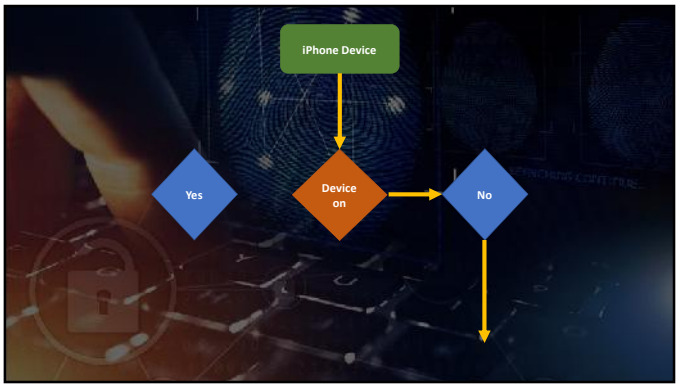

No
Is device damaged
No
Do not turn on device
Was device found in liquid
Yes
Keep device in liquid until it can be cleaned
Yes
No
Collect device identifiers if possible
Remove battery
Collect device identifers

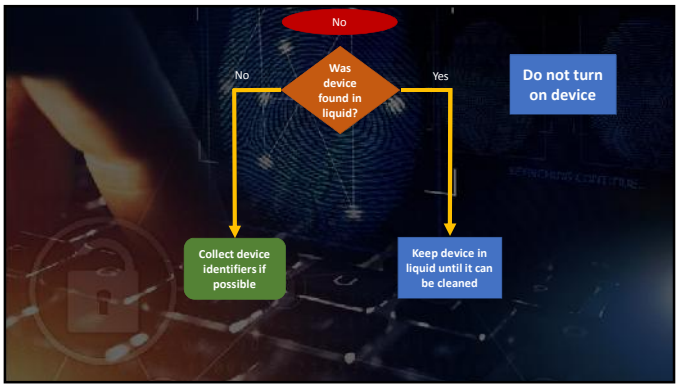
iOS SECURITY

- After 48 hours since last unlock, biometrics are disabled.
- After 1 hour since last unlock, charging port blocks data transfer.
- When phone is restarted, biometrics are disabled and passcode is required.
- If device is found unlocked – remove passcode in settings or repeatedly interact with screen to prevent locking until it can be examined.
- Turn on Airplane mode
- Connect to power source
- If device is found off – leave off!



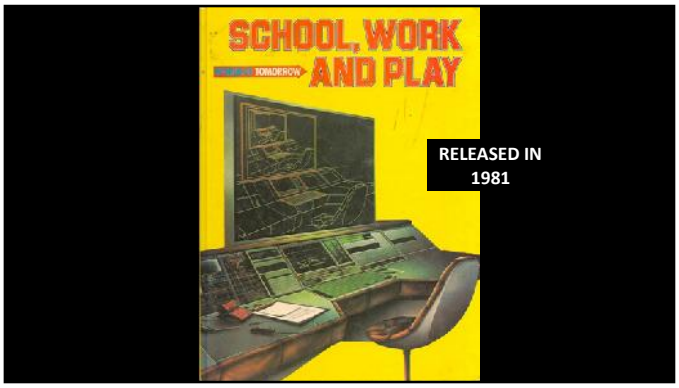




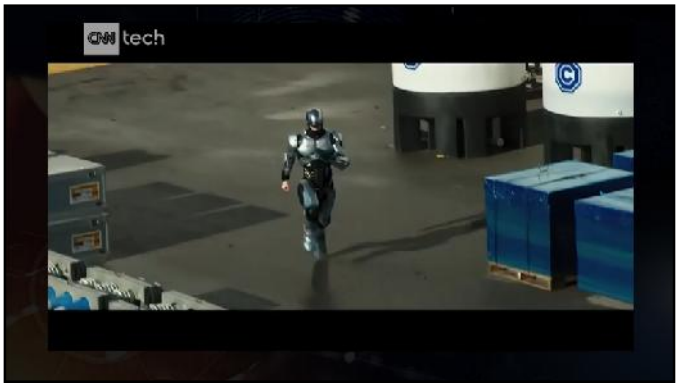


RECOMMENDATIONS FOR INVESTIGATORS

- Use social engineering to identify possible passcodes.
  - People are creatures of habit.
  - Where do you hide passcodes?
- When legally permissible, take all devices linked to a suspect.
- Focus interviews and confessions around providing passcodes.
- Be creative!
  - Use ruses or surveillance to surreptitiously, but legally, obtain a suspect's passcode.
- Consider going to the cloud.


SCHOOL, WORK
AND PLAY
TOMORROW
RELEASED IN
1981


Computer criminals
'Computers will make the world of tomorrow a much safer place. They will do away with cash so that you no longer fear being attacked for your money.'
'Nevertheless, a computer criminal may succeed now and then and the detectives of the future will have to be highly skilled computer operators.'


CNN tech

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
• DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

MYTH 1

Forensic analysis involves a digital investigative analyst looking at every file on the digital device.

MYTH 2

Once a forensic analysis is conducted, every item of significance to a case has been identified.

MYTH 3

There should never be a second analysis conducted because of the potential for conflicting forensics reports.

MYTH 4

Cell phone extraction tools accurately get and show everything on a phone.

MYTH 5

Digital forensic examiners are able to have all available forensic tools on-site to conduct all types of digital forensic analysis.

MYTH 6

All data viewable on a digital device is stored locally on that digital device.

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
•CASE STUDY
SEARCH WARRANT CHALLENGES
RESOURCES

INITIAL FACTS

- Law Enforcement investigating two individuals believed to be involved in extortion.
- The suspects allegedly used Facebook Messenger to communicate with a victim in which they threatened to distribute an embarrassing video of him if he did not pay them. A search warrant was applied for the suspects' residence.
- Magistrate Judge Westmore found that there were sufficient facts to support a finding of probable cause to conduct a search of the Subject Premises.
- The warrant included the ability to compel all individuals found in the residence to provide biometric access into the phones to complete a search of the data.

FOURTH AMENDMENT VIOLATION

- Magistrate Judge Westmore held that the request to search the subject premises was proper, but the request to search any and all electronic devices found during the search and to use the phones' biometric features to retrieve data from the phones was overbroad.
- The request was not limited to a particular person or a particular device.
- There was not sufficient probable cause to compel **everyone** at the premises at the time of the search to provide biometric access into their phones.
- It would also violate the Fourth Amendment reasonableness requirement.

FIFTH AMENDMENT VIOLATION

- Magistrate Judge Westmore believed it would violate the Fifth Amendment right against self-incrimination by providing biometric access.
- Users have had the ability to lock their electronic devices by using an alpha-numeric code for decades and courts have determined that a passcode cannot be compelled under the Fifth Amendment because the act of communicating the passcode is testimonial.
- The Judge makes a distinction between compelling DNA or fingerprints and providing a passcode whether verbally or through biometrics.
- This ruling still allowed seizure of those digital devices that were reasonably believed to be owned and/or possessed by the two suspects named.

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
•SEARCH WARRANT CHALLENGES
RESOURCES

SEARCHING HOMES VS. DIGITAL DEVICES

- Data is not necessarily stored contiguously in one location, nor in an easily read or understood format.
- Valuable descriptive information such as date and time values (known as metadata), is often not co-located with the actual information of relevance.
- There is no common layout to how each device stores its data.
- The only way to provide specific data from a device is to download the entire contents.

TECHNICALLY IMPOSSIBLE LIMITATIONS

- Only active information can be seized; deleted data must be excluded.
- Digital acquisitions are restricted to data falling within a specified timeframe.
- Only files located with a specific user's "profile" can be copied.
- Only certain data can be imaged from digital media.

EXPLAINING THE PROCESS

- A more realistic solution would be narrowing down the requested data during post-acquisition.
  - Taint teams
  - Privilege reviews
  - Special masters
- Request a trained forensic examiner to assist with writing the search warrant affidavit for description of what needs to be searched.

DIGITAL STATISTICS
INTERNET OF THINGS (IoT)
VEHICLE INFOTAINMENT SYSTEMS
COMPUTER EVIDENCE COLLECTION
MOBILE DEVICE EVIDENCE COLLECTION
DIGITAL EVIDENCE MYTHS
CASE STUDY
SEARCH WARRANT CHALLENGES
•RESOURCES

Contact Name: Oath Inc
Online Service: Oath, Inc.
Online Service Address: 22000 AOL Way
Dulles, VA 20166
USA

Phone Number: 703-265-1933

E-mail Address: LawEnforcement@teamaol.com

Note(s): When Verizon acquired Yahoo, Inc in April 2017, it merged Yahoo and AOL into the new name Oath, Inc.

AOL Inc. now accepts criminal legal process from domestic law enforcement agencies by email. Please direct criminal legal process to:
LawEnforcement@teamaol.com

Emergencies - business hours: 703-265-1933

Emergencies - After Hours: 703-265-2677

In the event you issue legal process to AOL, be sure to issue it to AOL or AOL Inc. -- NOT to American Online or AOL LLC

Quick Access ISP Information

Use our handy form below to request one or more of these documents, offered by ISPs as a service to law enforcement investigators.

- Apple Law Enforcement Guide
- Bitmex Law Enforcement Guide
- Chatstep Law Enforcement Guide
- Comcast Cable/Xfinity Law Enforcement Handbook
- Discord Law Enforcement Guide
- Dropbox Law Enforcement Guide
- Ebay Responding to Law Enforcement Record Requests
- Experience Project Law Enforcement Guidelines
- Formspring Law Enforcement Guide
- Formspring Legal Process Policies
- hi5 Official Law Enforcement Guide
- KIK - LED_Guide Feb 2019
- MeetMe Law Enforcement Compliance Guide
- Megaupz Compliance Process
- MocoSpace Law Enforcement Guide
- myYearbook Law Enforcement Guidelines
- Omegle Law Enforcement Guide
- Orkut Law Enforcement Guide
- Pinger LE Contact Info
- Skype International Guidelines for LEA
- Snapchat Law Enforcement Guide
- Sonic.net Legal Process Policy
- Sony (PlayStation) - Sony Interactive Entertainment LLC
- Stickam Law Enforcement Guide
- Tagged Official Law Enforcement Guide
- TeenSpot.com Law Enforcement Handbook
- TextNow LE Guide - U.S.A.
- Tiktok Law Enforcement Guide
- TracFone Wireless, Inc
- Tumblr Law Enforcement Guide
- Uber US Law Enforcement Guide and Primer
- Verizon Law Enforcement Legal Compliance Guide
- Wickr Law Enforcement Guide
- Yahoo! Compliance Guide for Law Enforcement

Contact Information

Det. Bob O'Neal

- St. Charles Police Department
- St. Charles County Cyber Crime Task Force
- P: (636) 949-3000 x4402
- C: (314) 713-6063
- Boneal@sccmo.org