Mobile Device Isolation and Faraday Containers

Jason Filley

August 2018

Abstract: During the Isolation Phase of mobile phone forensics, diligence should be taken to prevent radio communications that can alter the state of the evidence. Faraday bags, and Faraday cages, are effective means of isolating the device's network connections. Following an indulgent sampling of historical examples of evidence isolation, the history and technical details of Faraday cages is provided, an overview of device radio capabilities and threats is given, and evidentiary steps listed.

Contents

The Physical Preservation of Knowledge

Throughout the history of the written word, people have taken steps to preserve those words. This is, indeed, the point of moving from an oral to a written record.

The longest-lasting records are written either in stone or metal – on cave walls, carved in rock, or cast in coins. Written words, on papyrus or vellum (plant and animal), were at increased risk for decomposition from sun, moisture, insects, and foragers. The routine method for preserving written material from external corruption was by placing them in sealed clay jars.

Preparing for the Apocalypse (Then)

The Prophet Jeremiah, in an ancient example of chain of custody and evidence preservation, provided an explicit record of his purchase of the field at Anathoth, along with deity-provided instructions for preserving that record:[1]

> "And I bought the field at Anathoth from my cousin Hanamel, and weighed out the money to him, seventeen shekels of silver. I signed the deed, sealed it, got witnesses, and weighed the money on scales. Then I took the sealed deed of purchase, containing the terms and conditions, and the open copy; and I gave the deed of purchase to Baruch son of Neriah son of Mahseiah, in the presence of my cousin Hanamel, in the presence of the witnesses who signed the deed of purchase, and in the presence of all the Judeans who were sitting in the court of the guard. In their presence I charged Baruch, saying, Thus says the Lord of hosts, the God of Israel: *'Take these deeds, both this sealed deed of purchase and this open deed, and put them in an earthenware jar, in order that they may last for a long time.'* " (Jeremiah 32:9–14)

The initial Dead Sea Scrolls cave was found in 1947 by Muhammad edh-Dhib, a Bedouin shepherd, in the Wadi Qumran, near Jericho. Protected by an arid climate, in caves blocking sunlight, and stored in clay jars, the scrolls made of biodegradable material survived.

> "[M]embers of an ancient Jewish religious community . . . hurried out one day and in secrecy climbed the nearby cliffs in order to hide away in eleven caves their precious scrolls. No one came back to retrieve them, and *there they remained undisturbed for almost 2,000 years*." [2]

Note that in 2017, a 12th cave was found, though it contained only a single piece of blank parchment and some ancillary artifacts. [3]

[1] The Bible (NRSV), 1989. New Revised Standard Version Bible, copyright 1989 the Division of Christian Education of the National Council of the Churches of Christ in the United States of America

Figure 1: Two Dead Sea Scrolls Jars at the Jordan Museum, Amman. *Photo: Osama S. M. Amin*

[2] Geza Vermes. *Complete Dead Sea Scrolls*. Penguin Books, 1998. ISBN 0140278079

[3] The Hebrew University of Jerusalem. Hebrew University Archaeologists Find 12th Dead Sea Scrolls Cave, 2017. URL `http://new.huji.ac.il/en/article/33424`

In 1945, on the banks of the Nile, near the Egyptian town of Nag Hammadi, two brothers digging for fertilizer stumbled upon a hidden Gnostic library.

> "Two brothers, Muhammad and Khalifah Ali of the al-Samman clan, hobbled their camels on the south side of the fallen boulder and came upon the jar as they were digging [for fertilizer] around its base. Muhammad Ali reports that at first he was afraid to break the jar, whose lid may have been sealed on with bitumen, for fear that a jinn might be closed up inside it; but, on reflecting that the jar might contain gold, he recovered his courage and smashed it with his mattock." [4] [pp 22–23]

In 1900, Sir Arthur Evans began excavation of the palace of Knossos in Crete, finding clay tablets in a then-unknown language, which he referred to as 'Linear B.' In a fortunate accident of history, the clay tablets had been tranformed from a read-write medium to a read-only one:

> "All these clay tablets had originally been allowed to dry in the sun, rather than being fired, so that they could be recycled simply by adding water. Over the centuries, rain should have dissolved the tablets, and they should have been lost for ever. However, it appeared that *the palace at Knossos had been destroyed by fire, baking the tablets and helping to preserve them for three thousand years*. Their condition was so good that it was still possible to discern the fingerprints of the scribes." [5]

[4] James M. Robinson. *The Nag Hammadi Library*. HarperOne, 1988. ISBN 0060669357

[5] Simon Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*. Doubleday, 1999. ISBN 0385495315

Preparing for the Apocalypse (Now)

Modern life is historical comparatively easy, in the United States, at least. People no longer toil for subsistence nutrition – food is so plentiful, and manual labor so declined, that obesity is now our number one health problem. Spare time, even among the fully-employed, is so great that we have crazes of searching for Pokemon, binge-watching Netflix, and playing fantasy sports (not even *playing* the sport – just pretending to manage imaginary sports teams).

Our thoughts, though, predictably fall back to the worst-case scenario. Could we survive without our highly-integrated infrastructure, for electricity, clean water, food, and transport? The post-apocalyptic genre never fails to solicit modern interest. "*The Walking Dead*" would have made no sense two hundred years ago, even in theory.

What knowledge would need to be preserved to not only survive, but to rebuild society?

In the novel "Lucifer's Hammer," the comet Hamner-Brown collides with Earth, and plunges us into a new ice age. Dan Forrester stuffed wrapped books into a septic tank to preserve the knowledge useful in rebuilding society.[6]

> "He whistled as he worked. Spray a book with insect spray, drop it in a bag, add some mothballs and seal it. Put it in another bag and seal it. Another. The packages piled up on the floor, each a book sealed in four plastic envelopes. . . . He'd packed books not to entertain, nor even to illustrate philosophies of life, but to rebuild civilization. . . . The territory was dotted with abandoned septic tanks. . . . The books went in in handfuls. He pushed them into the aged sewage with a plumber's helper, gently." [*Lucifer's Hammer*, pp 273–275]

[6] Larry Niven and Jerry Pournelle. *Lucifer's Hammer: A Novel*. Del Rey, 1985. ISBN 0449208133

Man-made disasters currently hold our mass attention. The majority of results for Internet search of "Faraday bag" or "Faraday cage" belongs to 'preppers,' survivalist-minded people providing information on protecting electronic equipment from an EMP (Electromagnetic Pulse) attack. A nuclear detonation 40–60km over Chicago would destroy much of the infrastructure of the Mid and Eastern United States .[7]

Following an EMP attack, we would quickly descend into chaos. William R. Forstchen's best-selling novel "One Second After," for example, is an approachable and entertaining read on how communities would react to an EMP attack. [8]. Survivalists recommend Faraday bags and cages to protect electronic equipment that would still be valuable with a broken infrastructure (eg., CB radios, walkie-talkies), with a noted interest in storage devices for computer and eReaders – load up an eReader with an ebook/PDF library of Army field manuals, and beet recipes, and any other knowledge one would think would bootstrap a new society. Printed material would survive

[7] Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2008. URL `http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf`

[8] William R. Forstchen. *One Second After*. Forge Books, 2011. ISBN 0765356864

an EMP attack, so it's a curiosity that such attention is given to electronic documentation preservation, which would be incredibly prone to failure of the reading devices.

Protecting electronic material from external influence is an intriguing thought experiment. What needs protected? And how?

The same thought given to protecting a Nook from a nuclear attack dovetails with our present concern – **how do we protect mobile phones and other devices from external electrical and radio interference that would destroy the value of their evidence**?

Faraday Cages Explained

History of the Faraday Cage

Michael Faraday (1791–1867) is one of the most influential scientists in history. He developed the first electrical generator, discovered electromagnetic induction, discovered benzene, developed the two Faraday laws concerning electrolysis, refrigeration by condensing and evaporating gases, and "laid the foundations of the classical field theory." [9] [10]

"In his work on static electricity, Faraday demonstrated that the charge only resided on the exterior of a charged conductor, and exterior charge had no influence on anything enclosed within a conductor. This is because the exterior charges redistribute such that the interior fields due to them cancel (the Faraday cage principle)." [*Ibid.*]

Simply put, a closed-conductor shield (eg., a wire mesh around a box), depending on mesh conductivity, thickness, and spacing, will prevent electric waves from penetrating the shield.

> "There is not much room to build a box the size of a garage in the Royal Institution's lecture theatre. Tiered seating surrounds the large central table and leaves little room for much else. It was the same in January 1836, but Michael Faraday had no choice. He left his cramped lab in the basement of the building in London's Mayfair and set to work. He put a wooden frame, 12ft square, on four glass supports and added paper walls and wire mesh. He then stepped inside and electrified it. Faraday all but lived in the box for two full days. In that time, with electrometers, candles, and a large brass ball on a white silk thread, he explored the nature of charge." [11]

Technical Details

Faraday shields are solid containers (see the Internet for videos of aluminum trashcan samples). [12]

> "Faraday cages are Faraday shields which have holes in them and are therefore more complex to analyze. Whereas continuous shields essentially attenuate all wavelengths shorter than the skin depth, the holes in a cage may permit shorter wavelengths to pass through or set up 'evanescent fields' (oscillating fields that do not propagate as EM waves) just beneath the surface. The shorter the wavelength, the better it passes through a mesh of given size. Thus to work well at short wavelengths (i.e., high frequencies), the holes in the cage must be smaller than the wavelength of the incident wave. Faraday cages may therefore be thought of as high pass filters." [13]

Faraday bags are lightweight, portable Faraday cages, with more flexible mesh, making them terribly convenient.

Figure 2: Portrait of Michael Faraday (1791-1867), Chemist and Physicist. *Photo: Smithsonian Institute*

[9] Julian Trubin. Michael Faraday Inventions and Discoveries, 2018. URL `https://www.juliantrubin.com/bigten/faradaycageexperiments.html`

[10] Famous Scientists. Michael Faraday, 2014. URL `https://www.famousscientists.org/michael-faraday/`

[11] Ian Sample. The Faraday cage: from Victorian experiment to Snowden-era paranoia , 2017. URL `https://www.theguardian.com/science/2017/may/22/michael-faraday-lost-better-call-saul-genius`

[12] Dr. Arthur Bradley. Testing Garbage Cans and EMP Bags, 2016. URL `https://www.youtube.com/watch?v=uYWhTMmv6bs`

[13] Wikipedia contributors. Faraday cage — Wikipedia, 2018. URL `https://en.wikipedia.org/wiki/Faraday_cage` Wikipedia has its occasional moments.

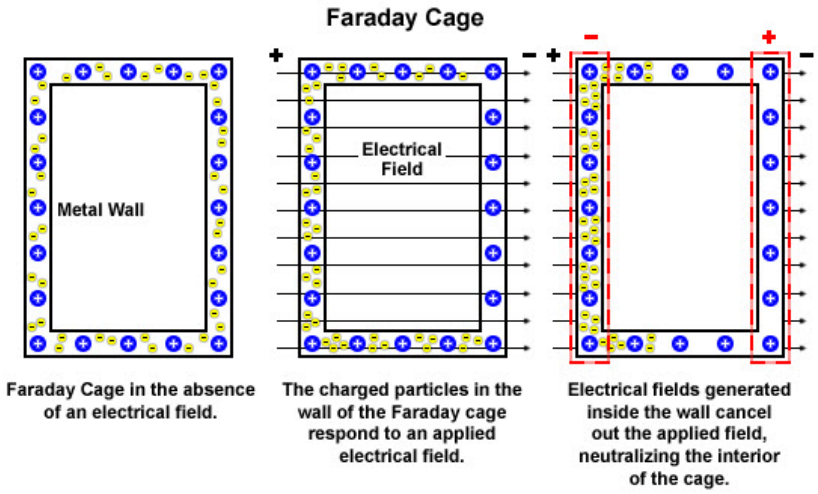

Figure 3: "Faraday cage diagram" *Diagram: National High Magnetic Field Labratory*

Examples of Faraday Cages

Some examples of everyday Faraday cages, and a sampling of uses of designed Faraday cages and bags:

Microwave ovens Microwave ovens excite water molecules by emitting radio waves. In addition to the microwave box, the mesh screen on the door attenuates the excess energy not absorbed by the food in the microwave. The microwaves cook the food, not the face of the cook watching.

Elevators Elevators attenuate a lot of cell phone signal, which is why you can't get into an elevator without hearing someone tell the other person on the end that they can't hear them. Wifi signal is greatly degraded, as well, and to provide coverage, an installer should use a can antenna at the roof of the elevator shaft, and point the signal straight down.

Cars near lightning strikes A car's frame protects the inhabitants by acting as a Faraday cage. The interior is protected from strong external electrical surges.

Shoplifters' "Booster bags" "Booster bags" are shopping bags with layers of aluminum foil lining the inside. This prevents RFID signals from being read, and the shoplifter merely walks out of the store with no worrisome alarms. [14]

MRI scan rooms are designed as Faraday cages, to prevent outside electrical interference, such as that produced by storms, to influence the readings inside.

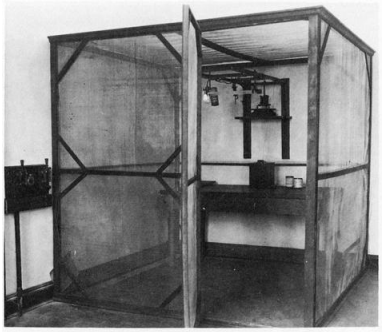

Figure 4: "Shielded cage room developed by the [National Bureau of Statistics] Radio Section in late 1917. This 'Faraday Cage,' as it was called, reduced the very strong signals from across the Potomac river from the Navy's strong signals broadcast at Arlington." *Photo: NBS/NIST*

[14] Shopguard Limited. Booster bagging — new era of organised crime with tinfoil lined tools, 2018. URL `http://shopguard.com/frequently-asked-questions/what-is-a-booster-bag/`

Coax cable is shielded with a flexible mesh, to keep electrical interference from disrupting network communications.

An English Pub Steve Tyler, owner of the Gin Tub pub in East Sussex, England, turned his entire bar into a Faraday cage, to keep patrons from yapping on the phone the entire time, and ruining the experience for themselves and others. One can sympathize. [15]

Potato chip bag A Perth, Australia, electrician was recently fired from his job for being absent 140 times to play golf. When playing hooky, he placed his GPS-enabled PDA (a tracker) inside an aluminum "Twisties" potato chip bag, preventing the reception of GPS signals. [16]

Faraday bags for car keyfobs Explicit Faraday bags are being marketed for keyfobs, to prevent amplification attacks, wherein a car-thief expands the listening area for a car determining if the keyfob is within starting distance. Keyfobs and cars are designed to only recognize each other within a limited space (10ft). Thieves can increase the distance of the signal, and the keyfob might be on a bedside table, but the car recognizes it, and the thief just opens the door and drives away. The devices to do this currently run about $30. [17] [18]

Electronic Toll Collectors As another use case for an explicit Faraday bag, ETC transponders' locations are routinely tracked at locations that *aren't* toll booths. In addition to protecting a commuter's privacy, guarding the transponder when not in use helps prevent cloning and theft. [19]

Electronic Monitoring Devices In a most amusing example of an explicit Faraday bag, is the recent case where an accomplice (Conn) provided a bag to hide the signal of a tracking device, to aid the escape of a friend (Wyatt) to Mexico. "Wyatt further admitted that on the day prior to Conn's escape, he provided Conn with a Faraday bag for the purpose of suppressing the signal emitted from Conn's electronic monitoring device. . . . " [20]

Particularly amusing is the evidence from the accomplice Conn's phone of the downloading of an application to test the efficacy of the Faraday bag.

> e. CONN ordered from an online retailer a Faraday bag for the purpose of concealing, blocking, and suppressing the electronic signals sent to or received by CONN's Monitoring Device, which shipped on or about May 10, 2017, to WYATT's address in Raccoon, Kentucky;

[15] BBC Online. Hove bar uses Faraday cage to block mobile phone signals, 2016. URL https://www.bbc.com/news/uk-england-sussex-36943686

[16] Emma Wynne. Faraday cage: How a humble chip packet helped an electrician hide his absence from work, 2017. URL http://www.abc.net.au/news/2017-11-27/employee-sacked-over-chip-packet-deception-faraday-cage/9196732

[17] Patrick J. Kiger. How To Protect Your Car From Keyless-Entry Hacking, 2016. URL https://www.edmunds.com/car-news/technology/how-to-protect-your-car-from-keyless-entry-hacking.html

[18] MOS Equipment. Mission Darkness Faraday Bag for Keyfobs, 2018a. URL https://mosequipment.com/products/mission-darkness-faraday-bag-for-keyfobs

[19] MOS Equipment. Electronic Toll Collection Transponders - Friend or Foe?, 2018b. URL https://mosequipment.com/blogs/news/electronic-toll-collection-transponders-friend-or-foe

[20] Office of the Inspector General. Kentucky Man Pleads Guilty to Assisting Former Social Security Disability Attorney Escape from Federal Custody, 2018. URL https://oig.ssa.gov/audits-and-investigations/investigations/march30-wyatt-guilty-plea

f. On or about May 17, 2017, WYATT downloaded an application to his cellular telephone to test the effectiveness of the Faraday bag; ...

j. On or about June 1, 2017, in Lexington, Kentucky, WYATT delivered to CONN, at CONN's direction, the Faraday bag mentioned above; ...

m. On or about June 2, 2017, in Lexington, Kentucky, CONN, without permission from the United States District Court or the USPO, severed the Monitoring Device from his ankle, and discarded it on the side of a highway in Faraday-bag-like material; [21]

[21] EASTERN DISTRICT OF KENTUCKY UNITED STATES DISTRICT COURT. UNITED STATES OF AMERICA CLERK U.S. DISTRICT COURT V. ERIC CHRISTOPHER CONN and CURTIS LEE WYATT, 2017. URL https://www.justice.gov/opa/press-release/file/1005031/download

Mobile Devices and Faraday Containers

Having seen historical (non-digital) examples of evidence preservation, and having seen the history, details, and example uses of Faraday cages, we turn our attention to the core of our subject.

When a mobile device is seized, what forensic steps should be taken to maintain the integrity of the evidence? Specifically, how should the device be protected from outside interference? This is the "Isolation Phase" of mobile forensics.

> "Isolation of the phone prevents the addition of new data to the phone through incoming calls and text messages as well as the potential destruction of data through remote access or remote wiping via a 'kill signal' as well as the possibility of accidental overwriting of existing data as new calls and text messages come in." [22]

[22] Det. Cynthia A. Murphy. Developing process for mobile device forensics, 2014. URL `https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf`

Mobile Device Radio Types and Characteristics

Smart phones have a number of radios, to provide different types of connectivity.

The NIST "Assessing Threats to Mobile Devices and Infrastructure" draft document [23] [sec 2.2] lists common network types:

[23] NIST. Assessing Threats to Mobile Devices and Infrastructure (NISTIR 8144)[DRAFT]), 2016. URL `https://csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf`

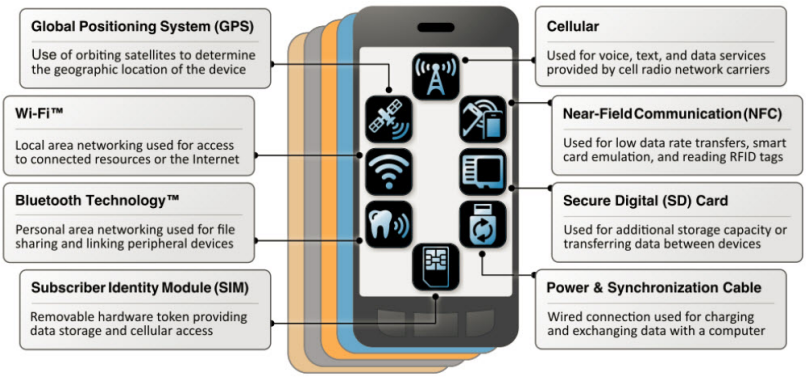

Figure 5: "NIST Overview of Mobile Device Communication Methods"

Cellular radios (CDMA, GSM, etc) allow communication to a cell provider's network. The most prominent fear of the forensic examiner is a remote wipe, wherein all personal data on the phone is erased. If a phone is seized, and the suspect, a conspirator, or a logic bomb triggers a remote wipe, all evidence disappears. It's of paramount importance to disconnect the device from cellular networks. It seems excessively optimistic to expect that a device is in, or can immediately be placed in, "Airplane Mode" and to trust that no cell connections will actually exist.

Ignoring the logic bomb problem, the simplest way to prevent cellular communication is to power off the device and remove the

It makes *far* more sense for a logic bomb to run locally and trigger a local wipe, but only the rarest of criminals would prepare for that, and radio isolation isn't going to help in that case.

battery. However, newer phones don't allow easy removal of the battery – you have to send them in to Apple and friends for near-factory service. Additionally, complete removal of power alters the state of the evidence, most notably by losing the contents of RAM.

A next-best alternative to complete power removal, is, of course, to place the phone in a Faraday bag.

Wifi connections have the same challenges as cellular networks. Data can still be received and alter the state of the evidence. Remote wipes are also a concern, so the problems and remediations of cellular radios are the same – place the phone in a Faraday bag.

GPS signals are constantly being received, which can possibly overwrite existing data. Also, logic bombs are a possibility ("if the phone is within one block of an RCFL facility, remote-wipe"). Place the phone in a Faraday bag.

Logic bombs and time-constraints deserve their own guidelines. There's more time to analyze the phone of a generic meth dealer than there is for that of a knowledgeable and determined terrorist. In what cases would isolating a phone actually hurt?

Bluetooth [24] and NFC [25] are limited to closer ranges, but likewise should be isolated. And most smart phones have FM receivers, even if the vendor doesn't enable them. [26]

Placing a mobile device in a validated Faraday bag is an acceptable means to isolate it and still retain current state.

As an asid, air-gapped and Faraday cages susceptible to leakage by magnetic interference, though exploitation requires relatively close proximity, and malware already planted on the device [27] [28].

[24] RF Wireless World. Bluetooth Tutorial, 2018. URL http://www.rfwireless-world.com/Tutorials/Bluetooth_tutorial.html

[25] Ian Poole. NFC Near Field Communication Tutorial, 2018. URL https://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php

[26] April Glaser. Your Phone Has an FM Chip. So Why Can't You Listen to the Radio?, 2016. URL https://www.wired.com/2016/07/phones-fm-chips-radio-smartphone/

[27] Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *CoRR*, abs/1802.02700, 2018b. URL http://arxiv.org/abs/1802.02700

[28] Mordechai Guri, Andrey Daidakulov, and Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. *CoRR*, abs/1802.02317, 2018a. URL http://arxiv.org/abs/1802.02317

Off-the-Shelf Experiments

To test very-low-priced off-the-shelf consumer Faraday bags, I purchased:

Wisdompro — Faraday Bag, Wisdompro RFID Signal Blocking Bag Shielding Pouch Wallet Case for Cell Phone Privacy Protection and Car Key FOB ($8.99) `https://www.amazon.com/gp/product/B01HETGX00/`

Mission Darkness — Non-Window Faraday Bag for Phones ($22.99) `https://www.amazon.com/gp/product/B01A7MACL2/`

The Wisdompro is a cell-phone sized Faraday bag, while the Mission Darkness bag fits a Kindle Fire or Nook comfortably.

Both bags reliably blocked cell signal enough that incoming calls were not received. Likewise, all Wifi connectivity was lost.

Screenshots taken from the Mission Darkness phone app are in the Appendix and show:

Wisdompro All cell and wifi signals blocked.

Mission Darkness All cell and wifi signals blocked.

Wisdompro inside Mission Darkness All signals blocked. No appreciable difference in reported strength and shielding levels.

Mission Darkness with USB cable Cell and wireless signal were received. Since the USB connection is ungrounded, the cable actually works as an antenna.

See screenshots of the app in the Appendix.

Forensic Guidelines for Mobile Device Radio Isolation

In 2014, the US Supreme Court, in the unanimous decision of *Riley v California*, ruled that police are not allowed to search devices seized incident to arrest, without a warrant. The bulk of evidence collection workflows and diagrams available were written prior to this decision, which seems to limit options to just two: get permission, or get a warrant.

"Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple – get a warrant." *[Ibid.]*

The availability of Faraday bags to provide isolation and negate law-enforcement arguments about evidence destruction was explicitly addressed by the Court:

> "In any event, as to remote wiping, law enforcement is not without specific means to address the threat. Remote wiping can be fully prevented by disconnecting a phone from the network. There are at least two simple ways to do this: First, law enforcement officers can turn the phone off or remove its battery. Second, if they are concerned about encryption or other potential problems, they can leave a phone powered on and place it in an enclosure that isolates the phone from radio waves. . . . Such devices are commonly called 'Faraday bags,' after the English scientist Michael Faraday. They are essentially sandwich bags made of aluminum foil: cheap, lightweight, and easy to use. . . . They may not be a complete answer to the problem, . . . but at least for now they provide a reasonable response. In fact, a number of law enforcement agencies around the country already encourage the use of Faraday bags." [29]

[29] US Supreme Court. Riley v. California, 573 US (2014), 2014. URL `https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf`

The RCFL (Regional Computer Forensics Laboratory) was established by the FBI in 2002, and has a number of regional offices (`https://www.rcfl.gov/about`). The RCFL assists smaller jurisdictions with computer and phone forensics in more serious cases. Smaller towns and counties can't be expected to maintain permanent qualified staff for mobile forensics, so the most efficient course of action is to provide guidelines for the smaller jurisdictions to aid in submissions.

The RCFL's "Best Practices for the Collection / Seizure of Mobile Devices for Investigators" [30] is undated, but as of 8/25/2018 shows the PDF metadata was last updated 12/19/2016, which is post-*Riley-v-California*.

[30] RCFL. Best Practices for the Collection / Seizure of Mobile Devices for Investigators, 2016. URL `https://www.rcfl.gov/heart-of-america/documents-forms/preserving-mobile-devices-brochure`

I recently talked to a police officer in a city of about ten thousand people. In a rare case where it's easier to get permission than forgiveness, an officer's easiest recourse to viewing a phone is to simply ask. In the common case where the suspect says, "No," the officer replies, "Well, I'm going to have to seize your phone then, and put it into evidence and send it off. It'll probably take a couple months until you get it back." This sometimes works, but only on the less intelligent suspect with comparatively little to lose.

In the more common case, where no permission is granted and it is determined that it's likely that the phone contains vital evidence, the phone is seized, the battery removed, and the phone is wrapped in foil and then placed in a plastic evidence bag. The Detective submits a warrant application to the Prosecuting Attorney, who then submits it to the Judge. If the warrant is approved, the phone is then transferred to the RCFL office in Kansas City. They have perhaps six cases a year that get escalated to the RCFL.

First, it's surprising that the RCFL guidelines mention wrapping a device in foil. Faraday bags like the Mission Darkness model I bought are individually serial-numbered, with a plastic pouch for placing evidence tags. They work better than aluminum foil – what gauge, and how many wraps? – and are very cost-effective.

Second, the RCFL guideline, in **all** cases – iOS and Android – where the device is already powered on, is: **"Do Not Turn Off - Keep Charged"** [see full diagram in the PDF]. How can you keep a device wrapped in foil fully charged? It would require what should be done with Faraday bags: place a compact charger inside. This is much easier with a dedicated Faraday bag than aluminum foil.

Third, the only recommended case where a battery is to be removed is where the device is 1) off, 2) damaged, 3) discovered in liquid, and 4) the battery is removable.

Fourth, in **no** case where the recommendation is to enable Airplane Mode, would it harm to also place the device in a Faraday bag. On/off is a binary decision, and I suspect there are scheduling apps that can automatically disable this, and it also seems like a very weak link. Enable airplane mode and place it in a Faraday bag with a charger.

The only open question here is when the warrant application and approval and transport take longer than the leftover charge and whatever an additional charger can provide. You can't reopen the bag as is and swap chargers. Some Faraday bag vendors sell kits with grounded external USB ports, so the device can be charged and accessed via external connection without breaking the seal of the Faraday shield.

Conclusion

For millennia, man has protected knowledge and evidence with physical enclosures, from religious sects placing their sacred library in sealed earthenware pottery, to paranoid (?) preppers loading up their Nooks for the Apocalypse.

The same principles and methods apply to isolating mobile devices to preserve their state.

The RCFL guidelines seem to be current practice, though I believe it's safer – while still cost-effective – to never use foil, and always place mobile devices in Faraday bags with an ample power supply – enough to cover the full time until the device would arrive at a forensic facility. In the cases serious enough to require data extraction, a nominal cost to insure the data integrity is warranted. Who couldn't justify $150 on a rape, or murder, or human trafficking case?

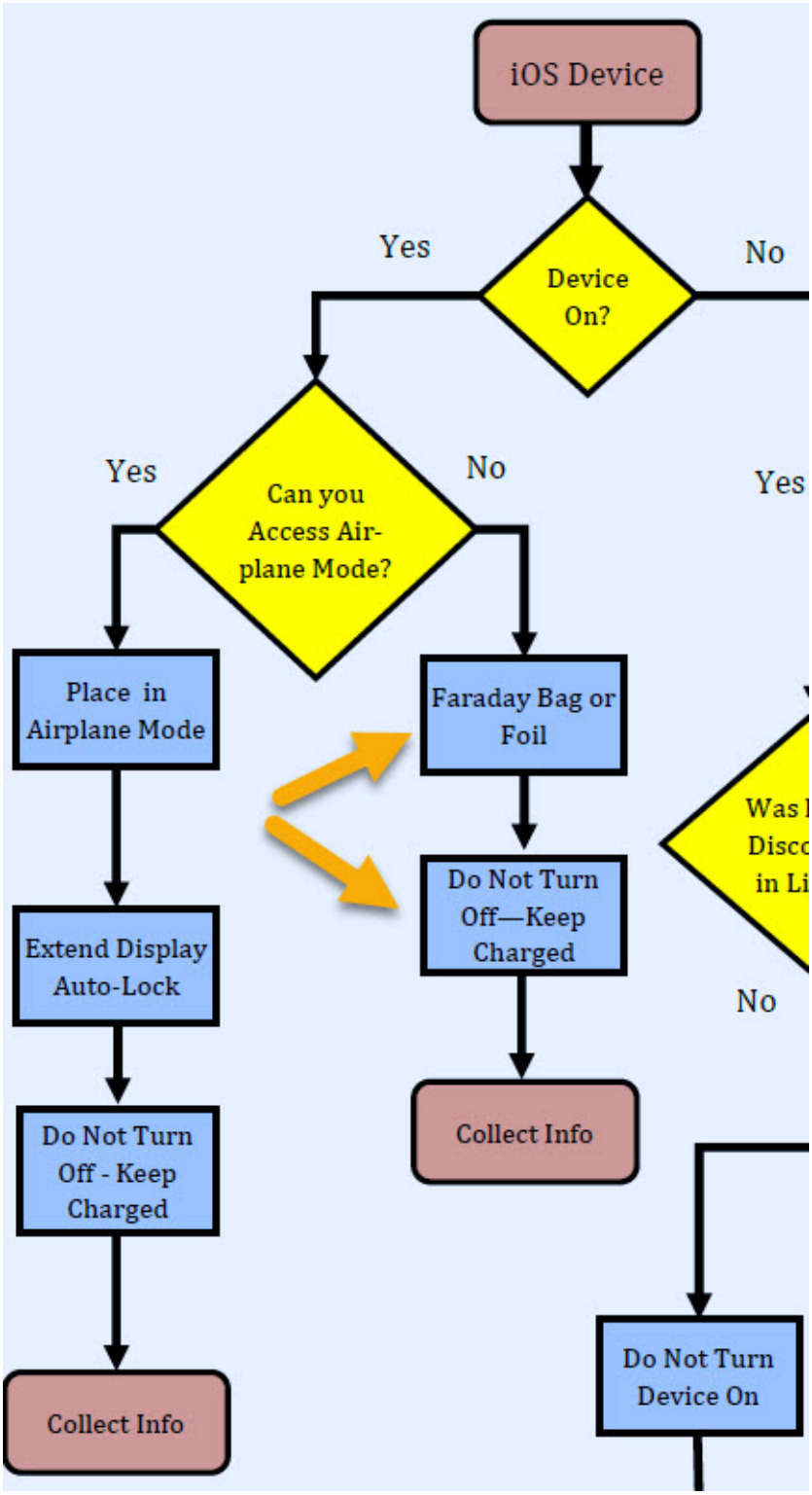

Figure 6: "RCFL Guidelines for iOS Isolation"

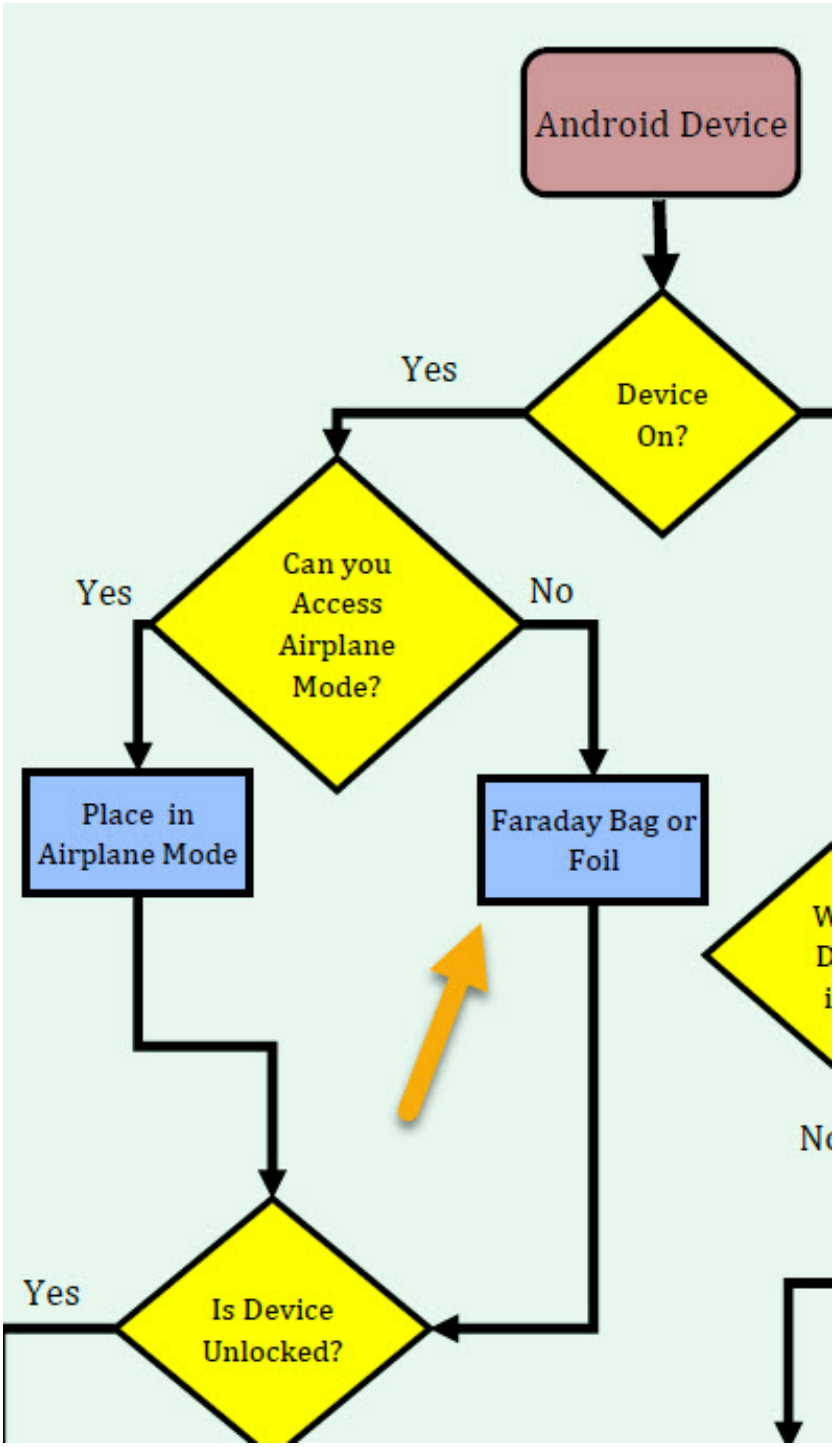

Figure 7: "RCFL Guidelines for Android Isolation"

Bibliography

References

The Bible (NRSV), 1989. New Revised Standard Version Bible, copyright 1989 the Division of Christian Education of the National Council of the Churches of Christ in the United States of America.

Dr. Arthur Bradley. Testing Garbage Cans and EMP Bags, 2016. URL https://www.youtube.com/watch?v=uYWhTMmv6bs.

US Supreme Court. Riley v. California, 573 US (2014), 2014. URL https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

MOS Equipment. Mission Darkness Faraday Bag for Keyfobs, 2018a. URL https://mosequipment.com/products/mission-darkness-faraday-bag-for-keyfobs.

MOS Equipment. Electronic Toll Collection Transponders - Friend or Foe?, 2018b. URL https://mosequipment.com/blogs/news/electronic-toll-collection-transponders-friend-or-foe.

William R. Forstchen. *One Second After*. Forge Books, 2011. ISBN 0765356864.

Osama Shukir Muhammed Amin FRCP(Glasg). Two Dead Sea Scrolls Jars at the Jordan Museum, Amman, 2018. URL https://commons.wikimedia.org/wiki/File:Two_Dead_Sea_Scrolls_Jars_at_the_Jordan_Museum,_Amman.jpg.

April Glaser. Your Phone Has an FM Chip. So Why Can't You Listen to the Radio?, 2016. URL https://www.wired.com/2016/07/phones-fm-chips-radio-smartphone/.

Mordechai Guri, Andrey Daidakulov, and Yuval Elovici. MAGNETO: Covert Channel between Air-Gapped Systems and Nearby Smartphones via CPU-Generated Magnetic Fields. *CoRR*, abs/1802.02317, 2018a. URL http://arxiv.org/abs/1802.02317.

Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. ODINI : Escaping Sensitive Data from Faraday-Caged, Air-Gapped Computers via Magnetic Fields. *CoRR*, abs/1802.02700, 2018b. URL http://arxiv.org/abs/1802.02700.

Smithsonian Institute. Portrait of Michael Faraday (1791–1867), Chemist and Physicist., 2008. URL https://www.flickr.com/photos/smithsonian/2550779733/in/photostream/.

Patrick J. Kiger. How To Protect Your Car From Keyless-Entry Hacking, 2016. URL https://www.edmunds.com/car-news/technology/how-to-protect-your-car-from-keyless-entry-hacking.html.

National High Magnetic Field Labratory. Faraday Cage diagram, 2016. URL https://nationalmaglab.org/about/around-the-lab/what-the/faraday-cage.

Shopguard Limited. Booster bagging — new era of organised crime with tinfoil lined tools, 2018. URL http://shopguard.com/frequently-asked-questions/what-is-a-booster-bag/.

Det. Cynthia A. Murphy. Developing process for mobile device forensics, 2014. URL https://digital-forensics.sans.org/media/mobile-device-forensic-process-v3.pdf.

NIST. Assessing Threats to Mobile Devices and Infrastructure (NISTIR 8144)[DRAFT]), 2016. URL https://csrc.nist.gov/csrc/media/publications/nistir/8144/draft/documents/nistir8144_draft.pdf.

NIST. The story of an old timer: Shielding techniques, 2017. URL https://www.nist.gov/pml/story-old-timer-shielding-techniques.

Larry Niven and Jerry Pournelle. *Lucifer's Hammer: A Novel*. Del Rey, 1985. ISBN 0449208133.

The Hebrew University of Jerusalem. Hebrew University Archaeologists Find 12th Dead Sea Scrolls Cave, 2017. URL http://new.huji.ac.il/en/article/33424.

Office of the Inspector General. Kentucky Man Pleads Guilty to Assisting Former Social Security Disability Attorney Escape from Federal Custody, 2018. URL https://oig.ssa.gov/audits-and-investigations/investigations/march30-wyatt-guilty-plea.

BBC Online. Hove bar uses Faraday cage to block mobile phone signals, 2016. URL https://www.bbc.com/news/uk-england-sussex-36943686.

Ian Poole. NFC Near Field Communication Tutorial, 2018. URL https://www.radio-electronics.com/info/wireless/nfc/near-field-communications-tutorial.php.

RCFL. Best Practices for the Collection / Seizure of Mobile Devices for Investigators, 2016. URL https://www.rcfl.gov/heart-of-america/documents-forms/preserving-mobile-devices-brochure.

James M. Robinson. *The Nag Hammadi Library*. HarperOne, 1988. ISBN 0060669357.

Ian Sample. The Faraday cage: from Victorian experiment to Snowden-era paranoia , 2017. URL https://www.theguardian.com/science/2017/may/22/michael-faraday-lost-better-call-saul-genius.

Famous Scientists. Michael Faraday, 2014. URL https://www.famousscientists.org/michael-faraday/.

Simon Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography*. Doubleday, 1999. ISBN 0385495315.

Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack. Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2008. URL http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf.

Julian Trubin. Michael Faraday Inventions and Discoveries, 2018. URL https://www.juliantrubin.com/bigten/faradaycageexperiments.html.

EASTERN DISTRICT OF KENTUCKY UNITED STATES DISTRICT COURT. UNITED STATES OF AMERICA CLERK U.S. DISTRICT COURT V. ERIC CHRISTOPHER CONN and CURTIS LEE WYATT, 2017. URL https://www.justice.gov/opa/press-release/file/1005031/download.

Geza Vermes. *Complete Dead Sea Scrolls*. Penguin Books, 1998. ISBN 0140278079.

Wikipedia contributors. Faraday cage — Wikipedia, 2018. URL https://en.wikipedia.org/wiki/Faraday_cage.

RF Wireless World. Bluetooth Tutorial, 2018. URL http://www.rfwireless-world.com/Tutorials/Bluetooth_tutorial.html.

Emma Wynne. Faraday cage: How a humble chip packet helped an electrician hide his absence from work, 2017. URL http://www.abc.net.au/news/2017-11-27/employee-sacked-over-chip-packet-deception-faraday-cage/9196732.

"The chips put into a dog can't be read from more than a couple inches away. If the government wants to track you they'll do it through your phone, not your dog."

Appendix

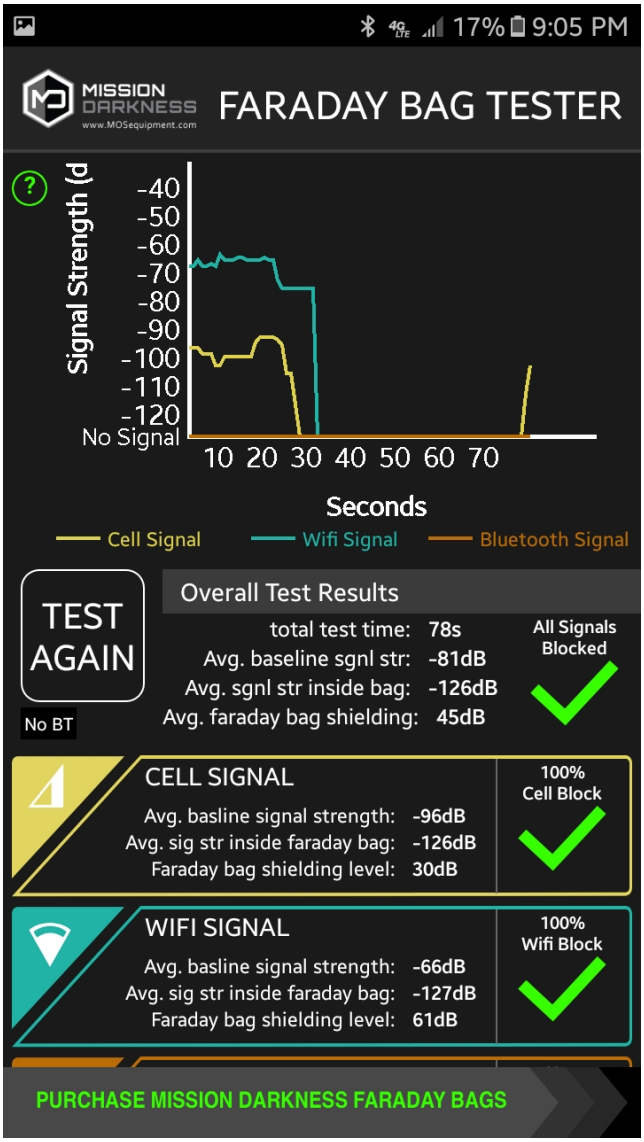

Figure 8: Loss of cell and wifi signal while in $8.99 Wisdompro Faraday bag.

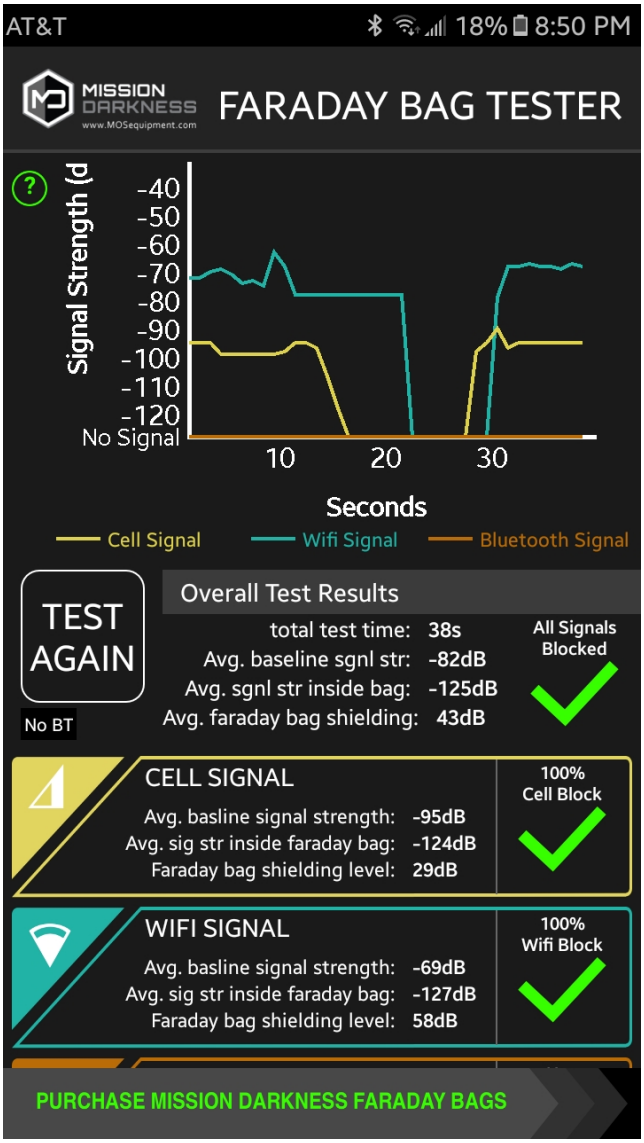

Figure 9: Loss of cell and wifi signal while in $22.99 Mission Darkness Faraday bag.

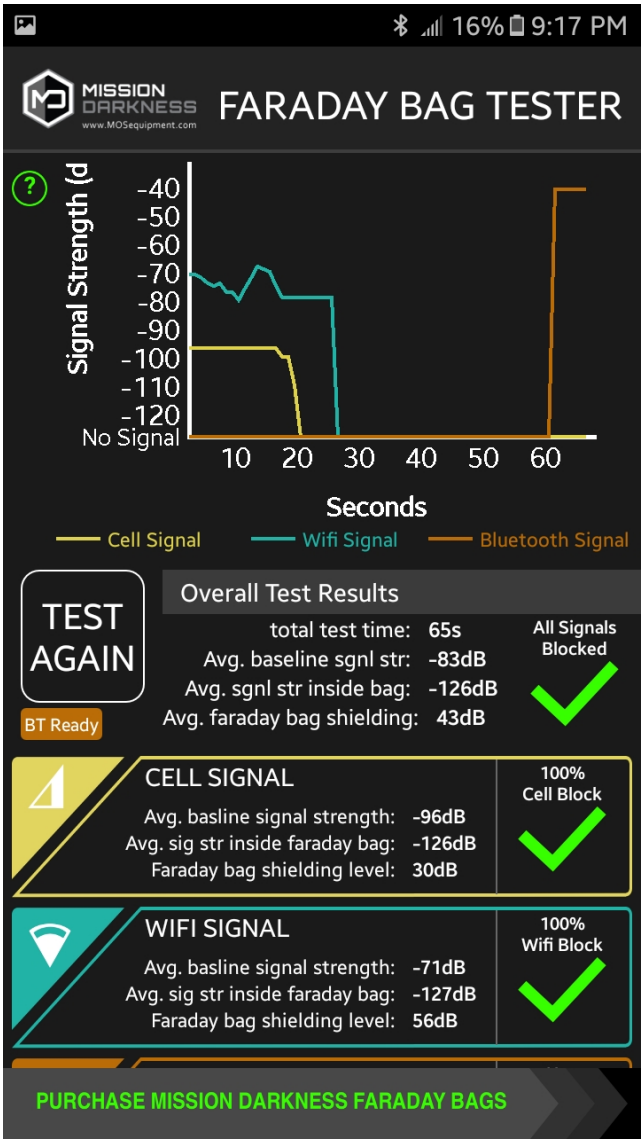

Figure 10: Loss of cell and wifi signal while in Wisdompro bag inside Mission Darkness bag

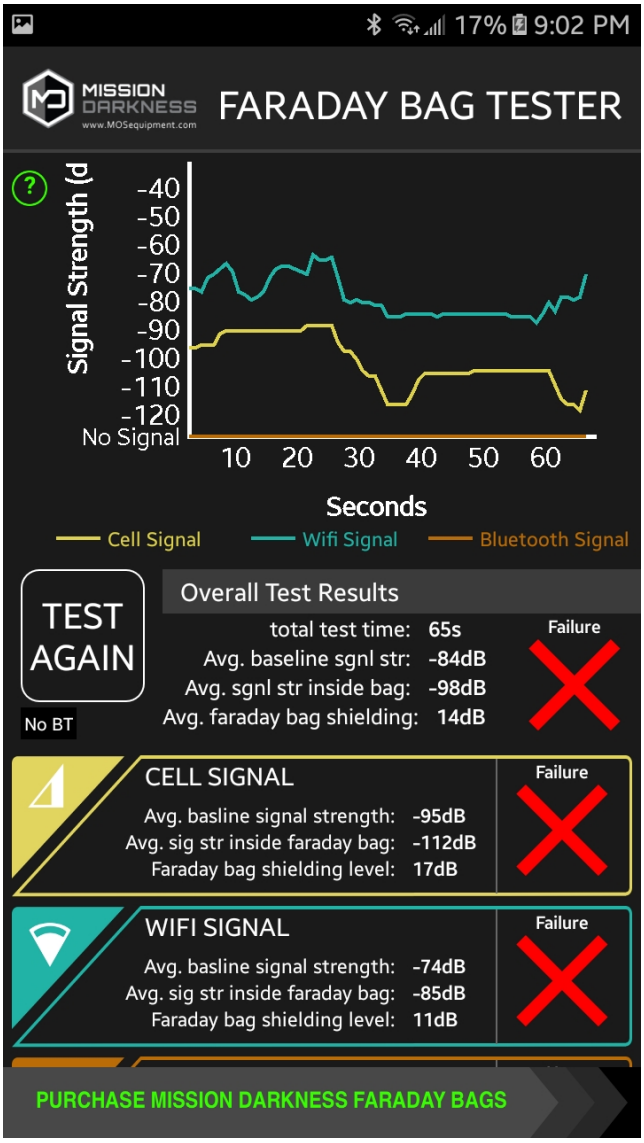

Figure 11: Inside Mission Darkness bag, with USB charging cable attached. An unshielded USB/charging cable not only breaks the seal of the Faraday bag, it acts as an antenna.

Figure 12: Inside Mission Darkness bag, with USB charging cable attached.