

SIGNAL ISOLATION

In mobile phone forensics as in traditional forensics there is an overarching requirement that seized items be protected so that the interaction of this evidence with the examiner during his or her investigation does not change the evidence. In “traditional” digital forensics we have seen specially formatted boot floppies, software write blocking and hardware write blocking devices that perform this function. But with wireless devices the examiner is faced with another challenge-preventing the mobile device from interacting with the wireless radio network.

This paper seeks to address the challenge of preventing the wireless device from interacting with the network and offer some explanation of some tools and techniques the examiner can use to perform an analysis while blocking the radio signal.

Signal Isolation-What is it?

As was stated in the introduction to this paper, the examiner of the mobile phone (and for that matter any wireless enabled device) must contend with the device seeking out and signing onto the network. This can cause a host of problems for the investigator from evidence overwriting to legal issues.

So what exactly do we mean by signal Isolation?

Despite the fact that a mobile phone resembles a traditional telephone in many ways-keypad, transceiver and receiver-it is in fact a radio. The cellular phone communicates back and forth with the public switched telephone network via radio signal. As long as a mobile phone is switched on the radio transmitter inside of it will seek the closest Cell Tower and attempt to gain service. If it can gain service data will be pushed out to the mobile-from calls, to text messages to even subtler information such as a location update-and thereby changing your original evidence.

Therefore when we talk about signal blocking we are referring to stopping the signal to the mobile phone so that it in effect is invisible to the network. This can also be referred to as RF Isolation.

RF Isolation is the protection of sensitive electrical equipment from external radiofrequency (RF) electromagnetic radiation by enclosing it in a conducting material. This type of Isolation is a refinement of the principle of the Faraday cage, which protects equipment from electric fields such as those from electrostatic discharges. The enclosure may be made of an unbroken conducting sheet, like the metal box surrounding a sensitive radio receiver, or a wire mesh, like that in the door of a microwave oven. Any holes in the box or mesh must be significantly smaller than the wavelength of the radiation that is being kept out, or the enclosure will not effectively approximate an unbroken conducting surface¹.

RF Isolation is itself a form of electromagnetic isolation. This type of isolation is done to limit the contact of electrical content with the outside environment (outside of the enclosure). In addition to the wiremesh referred to above, other conductive materials that can be used to create the shield barrier include sheet metal, metal mesh, ionized gas, plasma and aluminum foil. Sometimes inks mixed with suitable conductive metals such as copper are used to coat the insides of enclosures that house electronic components. This then forms the barrier against impedance.

FARADAY SHIELDING

The term Faraday Shielding is used interchangeably with RF isolation. The term comes about through the pioneering work of the British Physicist Michael Faraday. 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. This shielding effect is used in what is now known as a Faraday cage².

Faraday built a room coated with metal foil, and allowed high-voltage discharges from an electrostatic generator to strike the outside of the room. Using an electroscope he demonstrated there was no electric charge present on the inside of the room's walls.

This shielding effect is used to eliminate the effects of electric fields within a volume, for example to protect electronic equipment from lightning strikes and other electrostatic discharges (ESDs)².

A Faraday cage can be understood as an approximation to an ideal hollow conductor. Electric fields produce forces on the charge carriers (usually electrons) within the conductor. As soon as an electric field is applied to the surface of an ideal conductor, it generates a current that causes displacement of charge inside the conductor that cancels the applied field inside⁴.

Cellular Jammers

There are devices that are on the market that will cause interference with radio signals and effectively cause a “dead zone”. Known commonly as a cell phone jammer these devices emit signals in the same frequency range that mobile phones use, blocking their transmissions by creating strong interference. Someone using a cell phone within the range of a jammer will lose signal, but have no way of knowing a jammer was the reason. The phone will simply indicate poor reception strength⁵.

Cell phone jammers are manufactured in a number of different configurations from personal hand-held models that look like cell phones themselves, to units that resemble routers with multiple antennas, to even larger briefcase-style jammers. Personal jamming devices can create a “dead area” from approximately 30 — 100 feet (9 - 30 meters) depending on the model, while some of the more powerful devices can blanket areas of up to a mile (1.6 km) in radius.



Photos taken from <http://www.globalgadgetuk.com>

Personal cell phone jammers start at about \$250 (U.S.D.) and are widely available online despite their illegal status in most countries⁶. Manufacturers will claim to sell primarily to military and law enforcement but usually will sell the devices to anyone with the disclaimer that it is up to the buyer to make sure the device is legal in his or her country and that the buyer assumes all legal responsibility for buying, owning, or using the device.

LEGAL ISSUES WITH FARADAY SHIELDING

The examiner needs to be cognizant of two legal issues with the use of RF or faraday shielding.

The first is, the blocking of radio signals might, in fact, be illegal (and it is the position of the FCC that jammers most certainly are though no one has yet to be taken to task on the issue). The Act that is referred to on this account is the Communications Act of 1934, specifically sections 303 and 333.

SEC. 302. [47 U.S.C. 302] DEVICES WHICH INTERFERE WITH RADIO RECEPTION.

(a) The Commission may, consistent with the public interest, convenience, and necessity, make reasonable regulations (1) governing the interference potential of devices which in their operation are capable of emitting radio frequency energy by radiation, conduction, or other means in sufficient degree to cause harmful interference to radio communications; and (2) establishing minimum performance standards for home electronic equipment and systems to reduce their susceptibility to interference from radio frequency energy. Such regulations shall be applicable to the manufacture, import, sale, offer for sale, or shipment of such devices and home electronic equipment and systems, and to the use of such devices.

(b) No person shall manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section.

(c) The provisions of this section shall not be applicable to carriers transporting such devices or home electronic equipment and systems without trading in them, to devices or home electronic equipment and systems manufactured solely for export, to the equipment manufacturer, assembly, or installation of devices or home electronic and systems for its own use by a public utility engaged in providing electric service, or to devices or home electronic equipment and systems for use by the Government of the United States or any agency thereof. Devices and home electronic equipment and systems for use by the Government of the United States or any agency thereof shall be developed, procured, or otherwise acquired, including offshore procurement, under United States Government criteria, standards, or specifications designed to achieve the objectives of reducing interference to radio reception and to home electronic equipment and systems, taking into account the unique needs of national defense and security.

(d)(1) Within 180 days after the date of enactment of this subsection, the Commission shall prescribe and make effective regulations denying equipment authorization (under part 15 of title 47, Code of Federal Regulations, or any other part of that title) for any scanning receiver that is capable of--

(A) receiving transmissions in the frequencies allocated to the domestic cellular radio telecommunications service,

(B) readily being altered by the user to receive transmissions in such frequencies, or

(C) being equipped with decoders that convert digital cellular transmissions to analog voice audio.

(2) Beginning 1 year after the effective date of the regulations adopted pursuant to paragraph (1), no receiver having the capabilities described in subparagraph (A), (B), or (C) of paragraph (1), as such capabilities are defined in such regulations, shall be manufactured in the United States or imported for use in the United States.

(e) The Commission may--

(1) authorize the use of private organizations for testing and certifying the compliance of devices or home electronic equipment and systems with regulations promulgated under this section;

(2) accept as prima facie evidence of such compliance the certification by any such organization; and

(3) establish such qualifications and standards as it deems appropriate for such private organizations, testing, and certification.

SEC. 333. [47 U.C.S. 333] WILLFUL OR MALICIOUS INTERFERENCE.

No person shall willfully or maliciously interfere with or cause interference to any radio communications of any station licensed or authorized by or under this Act or operated by the United States Government⁷.

The second legal issue is that the examiner may indeed have to employ some sort of signal blocking to insure that evidence is not inappropriately received or overwritten.

EXAMPLES OF FARADAY SHIELDING

There are several commercial products on the market that claim to do Faraday shielding for mobile phones. A wily and inventive examiner though may be able to build his or her own faraday shield. For instance it has been remarked that it is possible to build a faraday enclosure using a unlined "Arson" paint can available at most hardware stores and suitable wire mesh-such as tightly woven copper. Wireless signal blocking paint is also available for sale on the Internet-<http://www.forcefieldwireless.com/>. This author has also used aluminum foil to wrap mobile phones and effectively block the RF signal. However it should be noted for do-it-yourself inclined examiners that extreme caution should be used when using "home-brew" faraday enclosures. Testing and validation should always be the norm. Signal impedance could be affected by the phone, the brand of foil (or wire) or any number of factors (though in fact this same caveat emptor should be used for any tool hardware or software).

Some commercial products that are for sale include faraday bags and tents (on scene acquisition!) for mobile phones from Network Security Services, LLC (www.network-securityservices.com).



Photos courtesy of www.network-securitysolutions.com

Paraben Forensics (www.paraben-forensics.com) also sells a Faraday Bag and tent called Stronghold.



There are a number of other companies that manufacture RF-shielding or provide a service. The below list is not all inclusive

Ramsey Electronics- <http://www.ramseyelectronics.com/te/default.asp>

Hemford Communications- <http://www.hemford.com/>

Envisage Systems- <http://www.phonebase.info/>

Forensic Telecommunications Services- <http://www.forensicts.co.uk/fts-packaging.asp>

This paper has sought to explain in general terms the principals of RF-signal blocking and the legal and forensic ramifications of performing such shielding. The individual examiner is encouraged to follow-up with the listed citations and references to further his or her understanding of this concept.

CITATIONS

1. http://en.wikipedia.org/wiki/RF_shielding
2. http://en.wikipedia.org/wiki/Michael_Faraday

