Preservation and Acquisition of a Locked iPhone Using Access Point Name Hijacking to Back up to iCloud

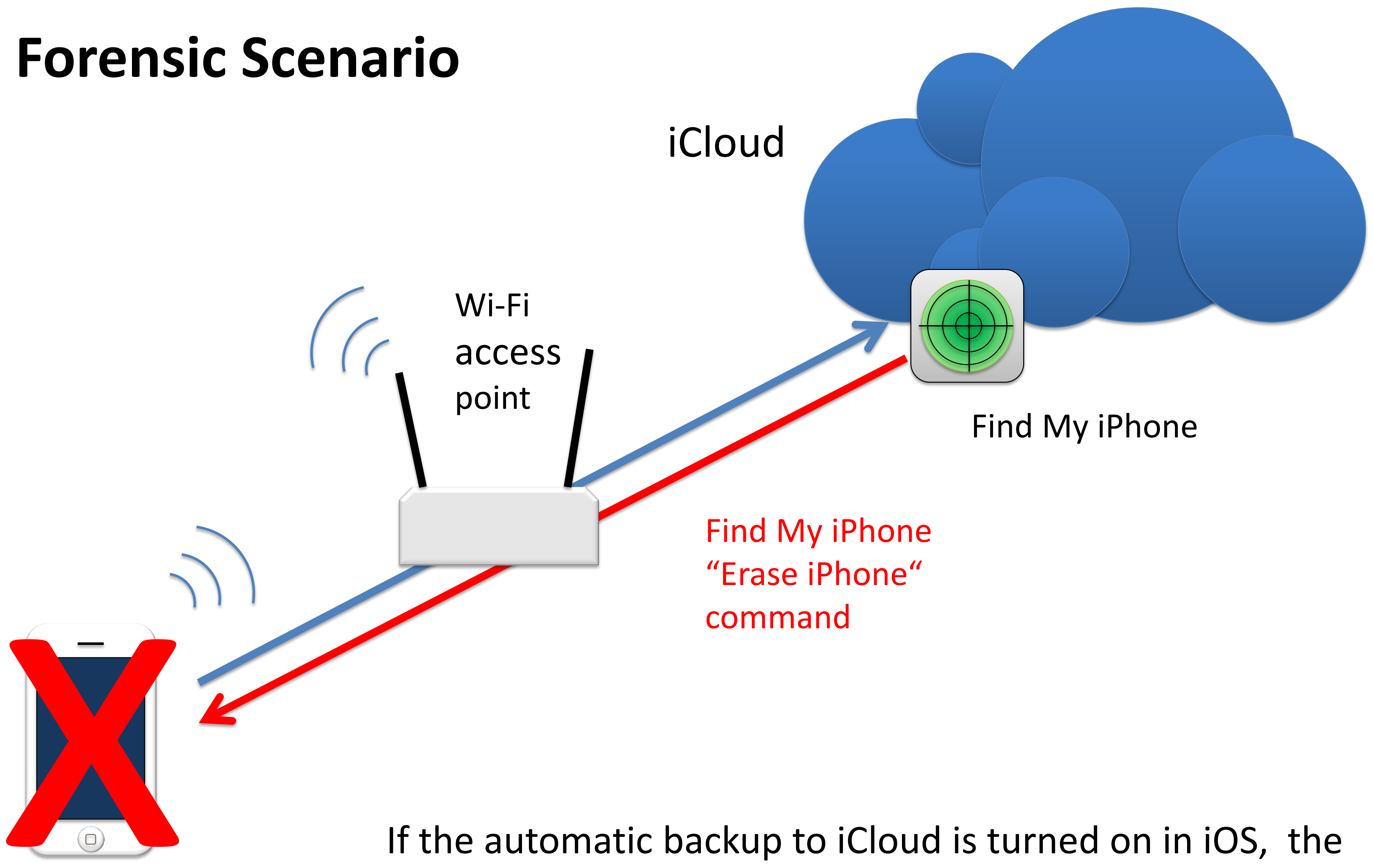
Christine Utz and Marcus Thompson
Purdue University

Significance

In recent years, mobile operating systems have introduced advanced security features such as full-disk encryption, two-factor authentication, or a limit to the maximum number of failed attempts to enter the device's passcode. This can hinder the work of law enforcement because these features also prevent the tools used by forensic examiners to access the device and retrieve data that might be potential evidence in a criminal investigation. In the aftermath of the San Bernardino shooting in early 2016, one penetrator's locked iPhone 5C caused a prolonged dispute between Apple and the FBI about Apple having to provide a means to enable the investigators to get access to the phone, which the company refused.

One idea briefly discussed in the Motion to Compel issued against Apple was to cause the locked device to back up its content to iCloud, from where it could later be retrieved after the account credentials have been obtained via search warrant. In the San Bernardino case, this idea could not be pursued further. The goal of this research is to find out whether it is possible to trigger the backup to iCloud on a locked iPhone. In case it is, this will provide forensic examiners with another point of access to locked iOS devices.

Forensic Scenario



Suspect's locked iOS device

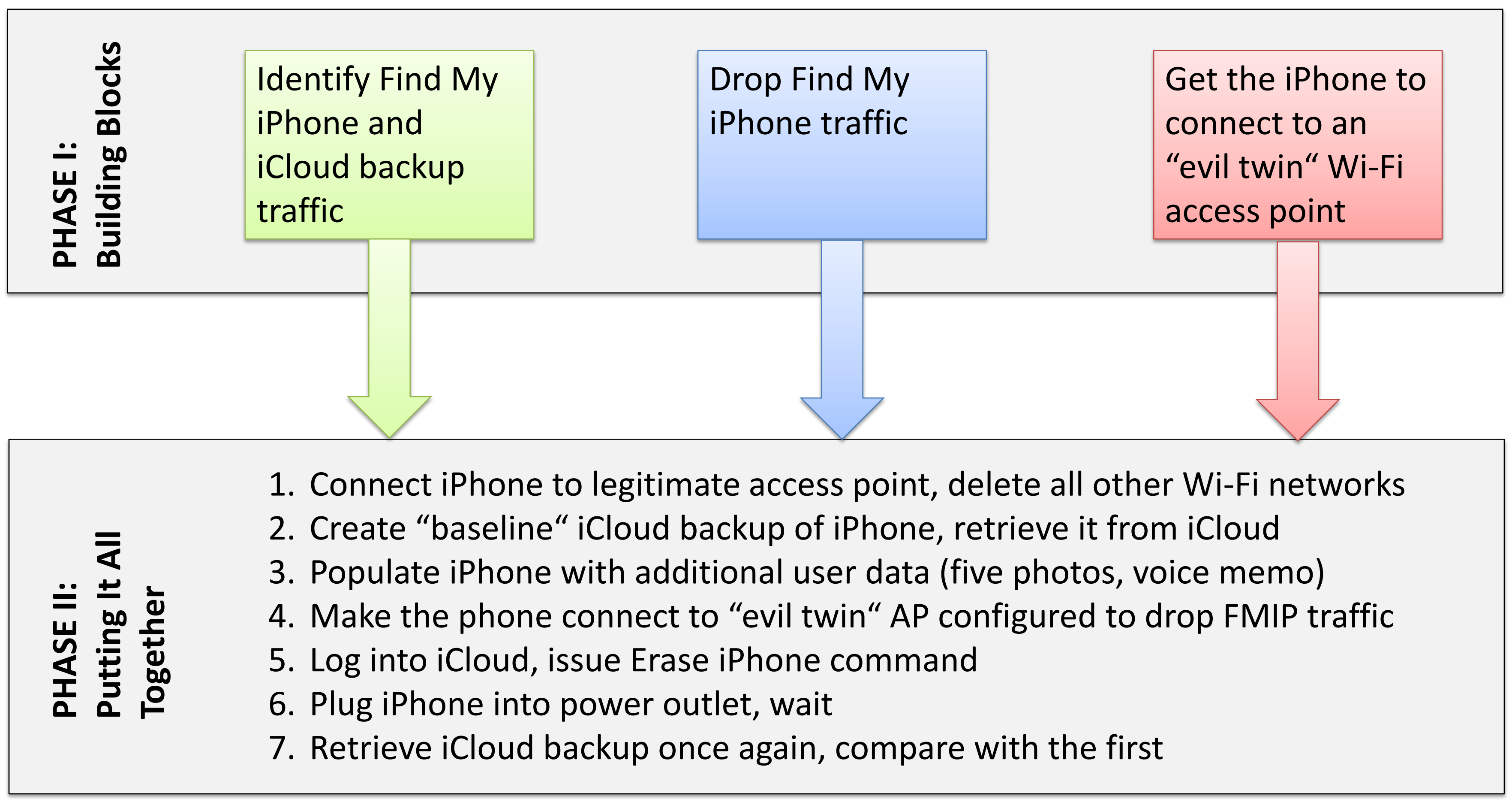
If the automatic backup to iCloud is turned on in iOS, the backup of the device is triggered when

- the device is locked,
- connected to a Wi-Fi network,
- and to a power outlet.

Due to the high connectivity of mobile devices, connecting them to the Internet comes at the cost of communication protocols starting to execute, which can alter the device state and render the data inadmissible in court. This especially holds true for the iCloud-based Find My iPhone service, designed to help iOS users protect their user data in case the device is stolen or lost. It also allows the device owner to prevent a forensic examination of the device by logging into iCloud and executing a remote "Erase iPhone" command. The next time the phone has access to the internet, all of its data is wiped irrevocably.

Methodology

This research consists of two distinct phases. Phase I investigates the feasibility of the individual building blocks required for the final setup. Phase II emulates the forensic scenario described to the left and tries to find out if an automatic backup to iCloud can be triggered or not.



PHASE I: Building Blocks

- Identify Find My iPhone and iCloud backup traffic
- Drop Find My iPhone traffic
- Get the iPhone to connect to an "evil twin" Wi-Fi access point

PHASE II: Putting It All Together

1. Connect iPhone to legitimate access point, delete all other Wi-Fi networks
2. Create "baseline" iCloud backup of iPhone, retrieve it from iCloud
3. Populate iPhone with additional user data (five photos, voice memo)
4. Make the phone connect to "evil twin" AP configured to drop FMIP traffic
5. Log into iCloud, issue Erase iPhone command
6. Plug iPhone into power outlet, wait
7. Retrieve iCloud backup once again, compare with the first

Results

- Find My iPhone traffic uses HTTP and HTTPS. Routing the iPhone's traffic through a web proxy revealed that all Find My iPhone traffic originates from a host with a specific, device and Apple ID dependent hostname. The iCloud backup involves HTTP(S) requests and responses to a variety of hosts, but does not communicate with FMIP servers.
- Blocking FMIP traffic based on the server URL works very well if the iPhone is configured to route its web traffic through a web proxy that decrypts the HTTPS traffic. This cannot be done when the phone is locked. URL-based filtering on the Wi-Fi access point does not work when the traffic is encrypted. Filtering by IP address does not help because the FMIP servers are part of iCloud and their IP addresses change constantly.
- Getting the phones to automatically connect to the rogue Wi-Fi access point masked as a legitimate one is difficult. Unlocked phones connect to an "evil twin" Wi-Fi access point if the SSIDs and WPA2 passwords of the two access points match. When locked, the iPhone 4 and 4S would connect to the rogue access point if they were connected to the legitimate access point prior to being locked and then brought close to the rogue AP, whose signal then was stronger than the legitimate one's.

Conclusion

Additional research is necessary to find out if there are other ways to cause an iOS device to connect to a Wi-Fi network while being in a locked state.
A reliable way to prevent at least Find My iPhone traffic from reaching the phone must be found. An ideal solution would be to completely block all communication to and from the device and only let the backup to iCloud pass. Achieving this appears difficult due to the complexity of the protocol and the high number of different hosts involved.