Android Security Test

Home to Logging Test App

CarrierIQ

This information is written to the best of my knowledge using publicly available resources. No security was bypassed to obtain anything marked confidential, and Carrier IQ made no effort to protect said documents.

You can take the Carrier IQ training yourself here – https://dis1.water.carrieriq.com/dis/training.jsp

I have made a mirror of all materials referenced here for download for the sole purpose of allowing others to understand and verify my security research on Carrier IQ.

http://www.androidfilehost.com/main/.TrevE/CIQ/

mirror1 – http://www.multiupload.com/BAAKNNSM3J

What is Carrier IQ?

Written by Trevor Eckhart

Carrier IQ (CIQ) sells rootkit software included on many US handsets sold on Sprint, Verizon and more. Devices supported include android phones, Blackberries, Nokias, Tablet devices and more.

From carrieriq.com:

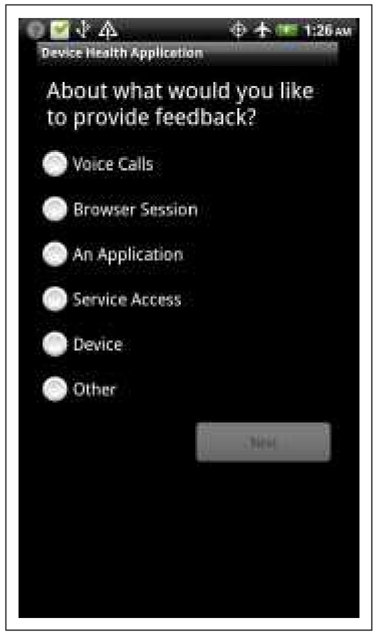
> *Carrier IQ is the market leader in Mobile Service Intelligence solutions that have revolutionized the way mobile operators and device vendors gather and manage information from end users.*
>
> *Recognizing the phone as an integral part of a mobile service delivery, and using the device to measure key parameters of service quality and usage, the Carrier IQ solution gives you the unique ability to analyze in detail usage scenarios and fault conditions by type, location, application and network performance while providing you with a detailed insight into the mobile experience as delivered at the handset rather than simply the state of the network components carrying it.*

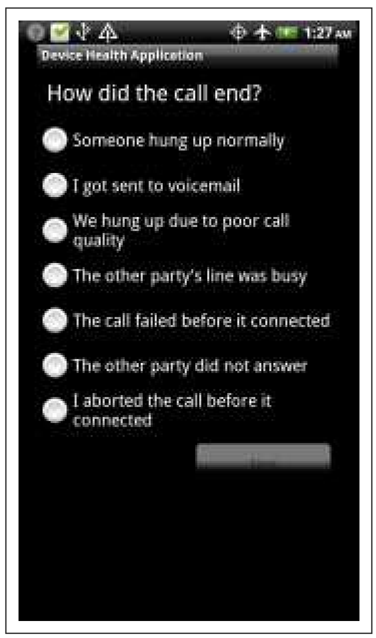
From http://www.bgr.com/2011/09/01/htc-sensation-and-evo-3d-revealed-to-be-spying-on-users/

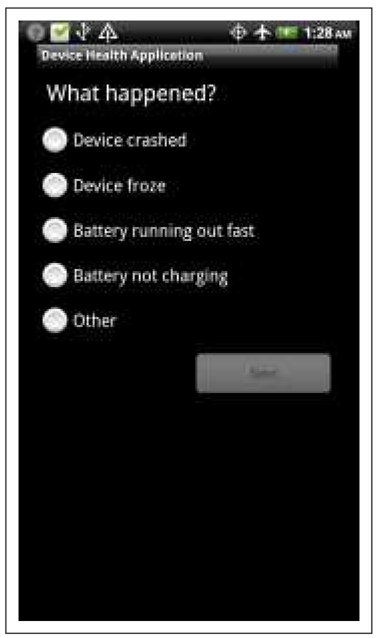
> *Carrier IQ is used to understand what problems customers are having with our network or devices so we can take action to improve service quality.*
>
> *It collects enough information to understand the customer experience with devices on our*

> *network and how to devise solutions to use and connection problems. We do not and cannot look at the contents of messages, photos, videos, etc., using this tool*

Great! Less dropped calls, better network experience. It sounds good on the surface. I was also able to obtain a stock copy of carrier IQ before it gets modified by third parties, and it has surveys users can fill out if they get a dropped call, browser ends unexpectedly, etc. It makes its presence known by putting a checkmark in the status bar. This could potentially be pretty useful information from a network administration standpoint, and is made clear to users its running. Unfortunately this is not always the real world case, it can be modified to be completely hidden.


1:26 AM
Device Health Application
About what would you like to provide feedback?
Voice Calls
Browser Session
An Application
Service Access
Device
Other


1:27 AM
Device Health Application
How did the call end?
Someone hung up normally
I got sent to voicemail
We hung up due to poor call quality
The other party's line was busy
The call failed before it connected
The other party did not answer
I aborted the call before it connected



What does CarrierIQ do?

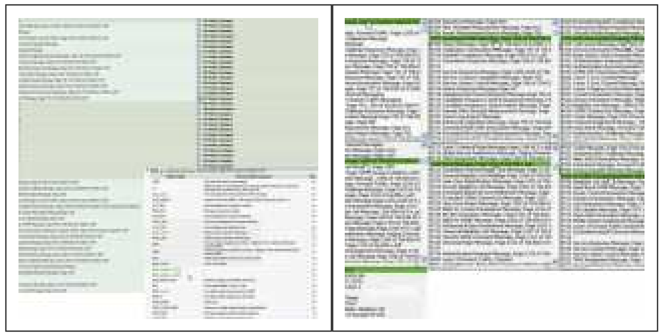
Carrier IQ is able to query any metric from a device. A metric can be a dropped call because of lack of service. The scope of the word metric is very broad though, including device type, such as manufacturer and model, available memory and battery life, the type of applications resident on the device, the geographical location of the device, the end user's pressing of keys on the device, usage history of the device, including those that characterize a user's interaction with a device. (From http://www.faqs.org/patents/app/20110106942)

Carrier IQ software, which consists of embedded software on mobile devices and server-side analytics applications, enables mobile operators and device OEMs to understand in detail a wide range of performance and usage characteristics of mobile services and devices. These include both network-facing services such as core voice and data offerings, as well as non-network-facing capabilities such as music players, cameras and other side loaded media, in order to assist with product and service development and roll-out. (From http://www.carrieriq.com/company/PR.CIQ-SeriesC.2009-01-27.pdf)

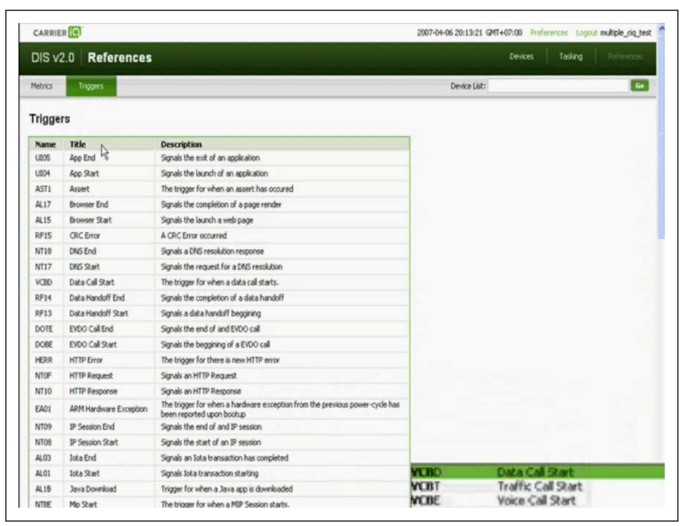
When is information logged?

Gathering information from the training videos, we see everything is broken down into two categories – Metrics and Triggers.

Metrics appears to be what data to log/send when a trigger is encountered. From the functions we have found already on our devices we knew the list was big, but even the below list only begins to scratch the surface.



Triggers appear to be when to collect metrics. For example when a user installs or opens an app any given metric can be called getting information. When a user browses a webpage HTTP header information can be grabbed along with detailed information on the page, or CarrierIQ can log keypresses made on what webpage. When location is changed the phone can report in. When a call is placed or data is started any metrics can be queried. There is alot more, these are just what was shown in public documents. These triggers seem to be menu items shown in the hidden Carrier IQ Test UI.



Known triggers found on HTC Phones:

Key in HTCDialer Pressed or Keyboard Keys

pressed:
Intent – com.htc.android.iqagent.action.ui01

App Opened –
Intent – com.htc.android.iqagent.action.ui15

Sms Received –
Intent – com.htc.android.iqagent.
action.smsnotify

Screen Off/On –
Intent – com.htc.android.iqagent.action.ui02

Call Received –
Intent – com.htc.android.iqagent.action.ui15

Media Statistics –
Intent – com.htc.android.iqagent.action.mp03

Location Statistics –
Intent – com.htc.android.iqagent.action.lc30

Known Samsung triggers provided by XDA member k0nane :

UI01: screen tapped in any location, or InputMethod (any soft keyboard) key pressed.
NT10: HTTP request read.
NT0F: HTTP request send.
UI11: unknown, located in the View class, which has its own IQClientThreadRunnable subclass.
AL34: loading started in a browser frame – URL.
AL35: loading started in a browser frame – data receive begin and end, page render begin and end.
AL36: data length.
(The above two are also found in LoadListener and WebViewCore classes. Web metrics are

> *not found on the Skyrocket, but are on the Epic 4G and Epic 4G Touch.)*
> *HW03: battery status changed. (Also not found on Skyrocket.)*

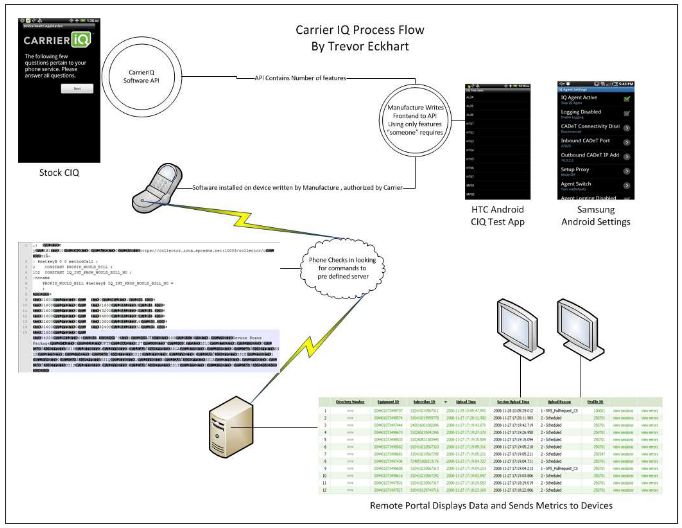
How does Carrier IQ work?

As mentioned before, Carrier IQ is rootkit software. It listens on the phones for commands contained in "tasking profiles" sent a number of ways and returns whatever "metric" was asked for.

> *Profile transmission can occur in a variety of ways, including "pushing" the data collection profile to the target device, sending a message, such as an SMS, to the target device prompting it to retrieve the data collection profile, and preparing the data collection profile for download the next time the target device contacts SQP 201 such as when it uploads a metrics package. Such profile transmission to the SQC 402 residing on the target device(s) may be achieved using any of a variety of transport mechanisms and standards including Short Message Service ("SMS"), Hypertext Transport Protocol ("HTTP"), Hypertext Transport Protocol Secure ("HTTPS"), Wireless Application Protocol ("WAP") Push, IP-based Over-the-Air (IOTA) protocol, OMA/DM, or other protocols that are known in the art or that may be developed in the future. From (http://www.patents.com/us-7609650.html)*
>
> *IQ Insight Experience Manager uses data directly from the mobile device to give a precise view of how the services and the applications are being used, even if the phone is not communicating with the network.*

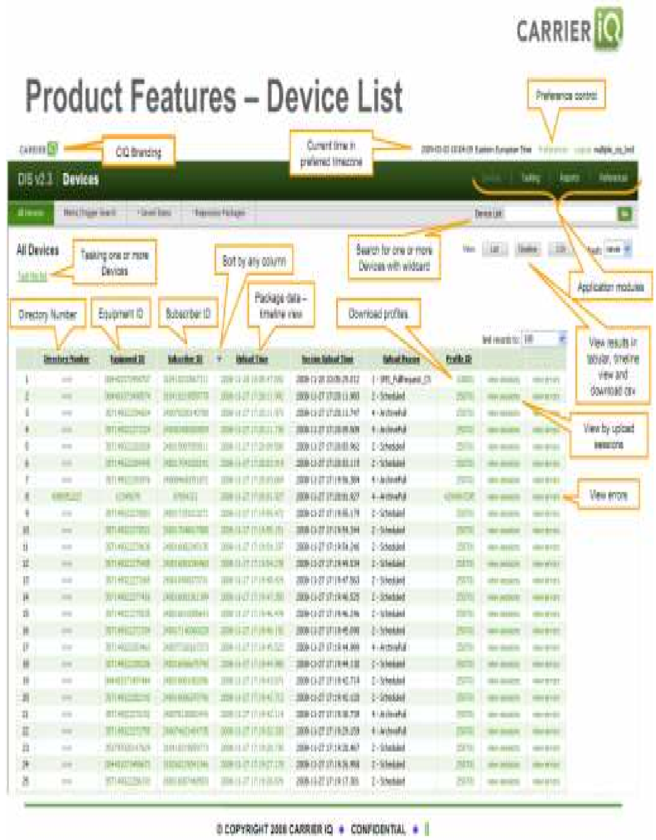
(From http://www.carrieriq.com/company/PR.Experience_Manager.CTIA-09.090325.pdf)

See the below process flow

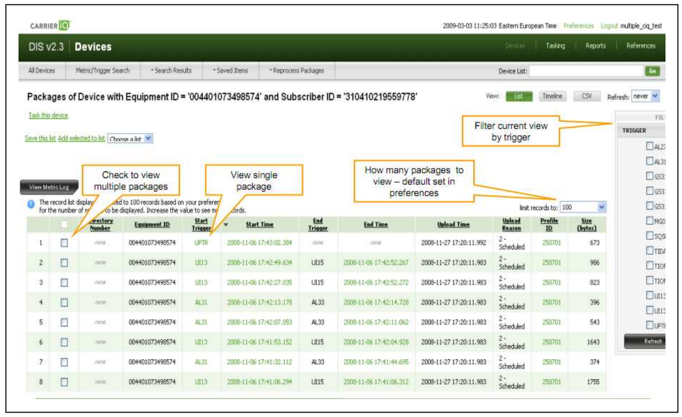


So theres a remote portal?

From training documents found we get an insight to the Carrier IQ Portal. Devices are displayed to the portal operator by individual phone Equipment ID and Subscriber IDs. The "portal administrator" can put devices into categories and see devices in California that have dropped calls at 5pm.



The down side to all of this is the "portal administrator" is also able to "task" a single phone with a profile containing any combinations of metric and trigger. From leaked training documents we can see that portal operators can view and task metrics by equipment ID, subscriber ID, and more. So instead of seeing dropped calls in California, they now know "Joe Anyone's" location at any given time, what he is running on his device, keys being pressed, applications being used.



Why do you keep calling CarrierIQ a rootkit?

The definition of rootkit from wikipedia is exactly what CarrierIQ is.

> *A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the software components that implement the tool)*

CarrierIQ as seen in real world usage (HTC Devices especially) is nothing like the stock copies shown on the first page. All menus have been stripped, hiding it from users presence without advanced knowledge. The service also runs as user Root in ramdisk. It checks in to a server (or receives commands through other various access) with commands to allow someone undetected access.

Who is using this data?

Verizon has publicly came forward with a statement regarding their usage on Carrier IQ statistics and give users a way to stop them from selling the information outside of Verizon

https://email.vzwshop.com/servlet/website/ResponseForm?OSPECC_9_0_9hg_eLnHs_uhmpJLE

Verizon Wireless will use the following categories of information:

Mobile Usage Information:

- Addresses of websites you visit when using our wireless service. These data strings (or URLs) may include search terms you have used
- Location of your device ("Location Information")
- App and device feature usage

Consumer Information:

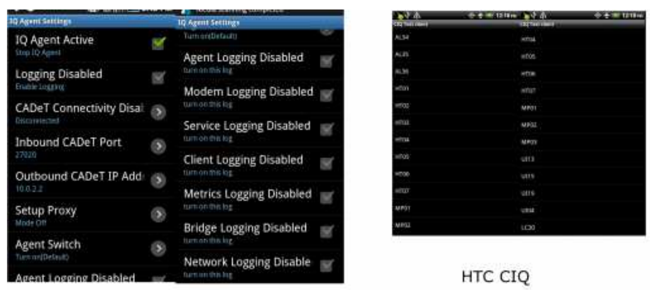
- Information about your use of Verizon products and services (such as data and calling features, device type, and amount of use)
- Demographic and interest categories provided to us by other companies, such as gender, age range, sports fan, frequent diner, or pet owner ("Demographics")

Sprint is known to collect carrier IQ data because users have the application running reporting to them, but have no privacy policy, retention policy, or public information on what they use the data for.

Do we have to Opt-In to this collection? Can it be stopped?

Devices are automatically entered into using Carrier IQ. Samsung android devices have an on off switch, but it is not easily accessible or made known to users that it’s even there. HTC android devices have no such off switch. Even if you purchase a phone on eBay completely off of sprint, use it on wifi only, Sprint will still be enabled to task your device with metrics because of no available off switch and Carrier IQs aggressive reporting nature across multiple protocols.

It also should be noted all the surveys and user facing dialogs have been stripped besides the below screenshots which require advanced skills to access.



Samsung CIQ

HTC CIQ

Samsung screenshots thanks to k0nane on XDA See the full post where he removed carrier IQ here

Detection / Removal:

There are a few advanced methods that can be used to detect Carrier IQ. Logging Test App scanner will detect it in the kernel (use Check Props Feature), as well files used in the regular Loggers scan. This will detect Carrier IQ regardless if you are rooted or not. You can also use this app to bring out hidden menus for known versions of CIQ clients.

The only way to remove Carrier IQ is with advanced skills. If you choose to void your warranty and unlock your bootloader you can (mostly) remove Carrier IQ.

Logging Test App can identify files used in logging and you can manually patch or use Pro version to automatically remove.
