



Intelligraphics Bloodhound Product Suite 802.11 a/b/g/n Wi-Fi Packet Sniffer/Injector Solutions

Copyright © 2013, Intelligraphics Inc. ALL RIGHTS RESERVED.

Any usage of this file without the prior written permission of Intelligraphics is strictly prohibited. For more details about Copyrights contact Intelligraphics Inc.

**Intelligraphics, Inc
One University Place,
1651 N Collins Blvd
Richardson, TX 75080**

Table of Contents

1. Introduction.....	3
2. Purpose of 802.11 a/b/g/n Sniffer/Injector Solutions.....	3
3. Intelligraphics Bloodhound Features.....	3
4. Off-the-Shelf Solutions.....	6

1. Introduction

Intelligraphics is proud to partner with Texas Instruments to deliver optimized experiences on the OMAP platform. From smartphones to tablets, and e-readers to enterprise and industrial applications, TI's smart multicore OMAP processors provide a scalable, high-performance ultra-low power platform that absolutely delivers the experience users expect, while unleashing the unexpected. If it's mobile, it's made best with OMAP technology and Intelligraphics engineering expertise.

Intelligraphics has developed a mobile Wi-Fi sniffer solution – the Intelligraphics Bloodhound, utilizes the TI WiLink 6.0, WiLink 7.0 and WiLink 8.0 series mobile Wi-Fi chipsets (TI WL127x / WL128x/WL18xx) to create a truly portable Mobile Hardware Sniffer. It features a single Wi-Fi driver that can either act as a Wi-Fi sniffer, or as a regular Wi-Fi driver.

This document offers complete information on the features and off-the-shelf supported platforms for Intelligraphics Bloodhound series of Wi-Fi packet sniffer/injector solutions.

2. Purpose of 802.11 a/b/g/n Sniffer/Injector solutions

From the introduction of IEEE 802.11 standards for Wireless (MAC & PHY), more and more devices have become Wireless – be it for domestic purposes or for industrial automation/ control applications. IEEE 802.11 groups have shaped the original standard with additional security, throughput upgrade and reliability improvements through specific amendments. These advantages coupled with mobility and improved user experience has made Wi-Fi as the de facto communication mode in homes, public areas, offices and in industrial sites.

To obtain highest performance of any Wi-Fi installment, precise control of the wireless network with provisions for debugging, access control and continuous monitoring for security has become more relevant. Debugging and monitoring Wi-Fi networks comes with a requirement of stable, reliable, technically advanced solutions – the Wi-Fi packet monitors (sniffers) and packet probe tool (injector).

A Wi-Fi Sniffer is a device which will passively “listen” and “record” information exchanged in the particular Wi-Fi channel. A Wi-Fi Injector device on the other hand is an active device which can be used to transmit data in a Wi-Fi channel and record/analyze the response for it's action. Both together form the “Swiss Army Knife” toolkit for any Wi-Fi development or maintenance or surveillance teams.

3. Intelligraphics Bloodhound Features

Intelligraphics Bloodhound series of 802.11 a/b/g/n Sniffer/Injector solutions are based on Texas Instruments WiLink series of Wi-Fi chipsets. WiLink 6, WiLink 7 and WiLink 8 (WL126x, WL127x and WL18xx respectively) are the chipsets supported in this product suite.

Intelligraphics Bloodhound series products consist of modifications in TI WiLink driver/firmware/both for sniffer/injector functionality. Majority of the Intelligraphics Bloodhound products have both driver and firmware changes, whereas few have only firmware change (to run on platforms with no support for driver modification).

The following section summarizes Intelligraphics Bloodhound product series features :

- Clear API interface to configure and control the Sniffer/Injector operations
 - Intuitive API interface and clear documentation helps in reducing Application layer development time
 - Complete control of all Wi-Fi parameters
 - Channel, Band (2.4GHz and 5GHz), Bandwidth (HT20/HT40+/HT40-) support
 - Out-of-band operation support
- Support for Infrastructure specific metadata on per-packet basis
 - Custom metadata added to each captured frame
 - Channel/Frequency Information
 - Length of the MAC frame
 - RSSI
 - SNR
 - Received timestamp
 - MAC timestamp
 - PHY timestamp
 - Received Data rate
 - FCS (4 bytes)
 - Metadata header can be tailored to requested format/order
- Support for packet filters at hardware/software layers
 - Packet filters at the hardware reduces power consumption and increases capacity of the sniffer solution
 - Software packet filters can be used for discarding particular packets after certain stage of processing
- Support for packet filters for all 802.11 Wi-Fi Type and Sub-types
 - All 802.11 frame types (Management, Data and Control) supported
 - All 802.11 frame sub-type supported
 - APIs for Set/Reset packet filter from Application
- Recording captured packets with standard RadioTap header support (in .pcap format)

- Packet capture (.pcap) file type is useful in analysis of the capture using standard applications (for eg. Wireshark)
- Capturing unprocessed frames with MAC/PHY errors
 - API support to accept or reject error frames during capture
- Agile design architecture for additional buffering support
 - Additional buffer driver can be added to reduce the pressure on Kernel stack. Recording the captured packets will be through Intelligraphics APIs.
 - Architecture allows to bypass the buffer driver and provide the captured packets to stack directly. Recording the captured packets will be through standard tools (for eg. tcpdump)
- Support for decoding encrypted frames
 - Ability to decode 802.11 frames with inputs from User for encryption type, keys and session variables
- Full-featured 802.11 Wi-Fi packet Injection support
 - All the 802.11 MAC header information injected as per User information
 - Length, Data rate, Type/Sub-type, Sequence Number
 - PHY preamble type control
 - 802.11 Wi-Fi ACK frame behavior control
 - Injection operation with “no wait for ACK” (fire and forget)
 - Injection operation with “wait for ACK” (retry and succeed)
 - Complete feedback on the injected frame can be provided to the Application
 - Helpful for error tracking, flow control algorithm etc.
- BT coexistence
 - No hindrance in BT operation (scan/pairing/file transfer) before/during/after 802.11 Wi-Fi Sniffer/Injector operation
 - A reliable way to control Sniffer/Injector operation and transfer capture contents to other high-performance devices for analysis
- Zero-backoff Injector feature
 - Complete channel black-out with continuous injector operation
 - API to enable/disable zero-backoff during operation
- Combo designs for different requirements

- Firmware only solution available for platforms with no support to change driver
- Driver-Firmware solution for most of the platforms
- A driver-firmware can support combinations of different modes
 - Sniffer-Injector only
 - Sniffer-Injector and Wi-Fi

4. Off-the-Shelf Solutions

The following table provides a complete overview about “Off-the-Shelf” solutions available with Intelligraphics Bloodhound product suite :

Board/Product Name	TI WiLink chipset	Host Processor	OS/Distribution	Implementation	Notes
Motorola DROID Razr MAXX Smart phone	WL128x	TI OMAP 4	Android/Ice Cream Sandwich	Firmware only solution for Sniffer-Injector.	
LG Thrill - 3D Smart phone	WL127x	TI OMAP 4	Android/Ginger bread	Sniffer-Injector with buffering driver	
LogicPD Torpedo DM3730 reference design	WL128x	TI DM3730	Linux/OpenWrt	Sniffer-Injector solution with option for enabling/disabling buffer driver	
LogicPD Torpedo DM3730 (SOM-LV)	WL127x	TI DM3730	Linux/OpenWrt	Sniffer-Injector solution with buffering driver	
Pandaboard OMAP 4 reference design	WL127x	TI OMAP4430	Android/Ice Cream Sandwich and Linux	Sniffer-Injector with buffering driver	
Blaze OMAP 4 reference design	WL128x	TI OMAP4430	Android/Ginger Bread, Android/Ice Cream Sandwich and Linux	Firmware only solution and Sniffer-Injector with buffering driver	
Beagle Bone Black with	WL18xx	TI AM335x	Linux/Angstrom	Sniffer-Injector with no	tcpdump application is

WL8 RF cape				buffering driver.	used to display/record captured packets
Amazon Kindle Fire	WL127x	TI OMAP 4430	Android/Customized	Sniffer-Injector with buffering driver.	