

---

# Wireless Detective Extreme System

---

*Advanced Technology of  
Distributed Wireless Network  
Interception from Decision  
Group*

---

Product Marketing Division,  
Decision Group

---



March 2011

# **Advanced technology of Distributed Wireless Network Interception from Decision Group**

## **Wireless Detective Extreme System**

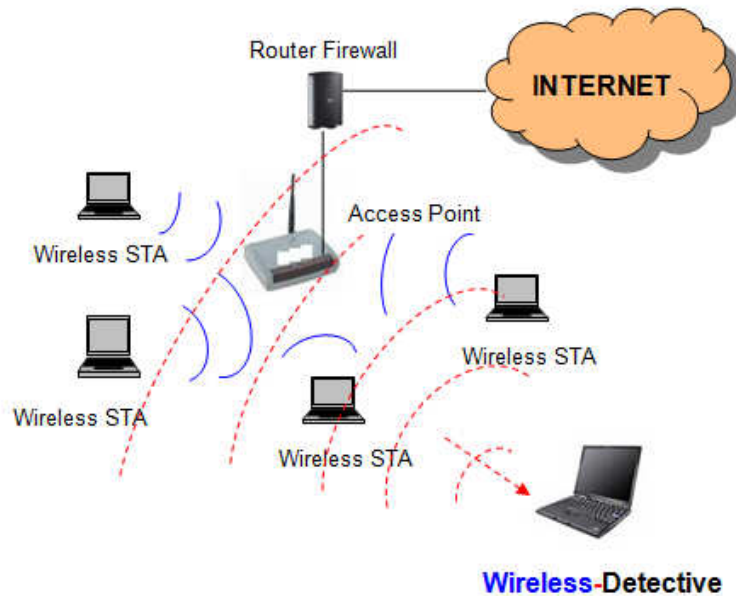
Application and service in cyber space become more and more popular because broadband communication is built up everywhere through wired or wireless infrastructure provided by governments or ISPs. Popular but untamed online activities have also caused challenge and potential risk to public and major concern of the management team in enterprises and government. Decision Group **Wireless-Detective** system can sniff/capture, decrypt WEP key, decode and reconstruct Internet activities through Wireless LAN (WLAN) by the protocols of *Email (POP3, SMTP, IMAP, Web Mail – Gmail, Yahoo Mail, Windows Live Hotmail etc.), Instant Messages/Chat (Yahoo, MSN, ICQ, AOL, QQ, UT Chat Room, IRC, Google Talk TW, Skype VOIP Call log), HTTP (Link/URL, Content, Reconstruct, Upload/Download, Video Stream), File Transfer (FTP, P2P), Telnet, Facebook, twitter, plurk, Online Games, VOIP and Webcam (MSN and Yahoo) etc.*

Wireless-Detective system adopts optimized Linux as the kernel and powerful Java Applet to provide a comprehensive and user friendly graphical interface (GUI). User can implement the system easily and use it immediately. With speedy packet sniffing and reconstruction technology Wireless-Detective system can reconnoiter a specific target (AP or STA) or specific channel (all Wireless LAN devices on the same channel) without interference into the existing network environment.

Wireless-Detective system is an important tool used by forensic and intelligence agencies like police and military to intercept the Wi-Fi online activities of the targeted suspect and preserve the content which is able to bring the suspect to court in case it involves legal issues. Besides, Wireless-Detective system can track down suspect or terrorist, who intends to commit fraud or create chaos to society, and impacts National Security. Prevention work can be done in order to safeguard the nation.

Since there are lot of public hotspots of Wi-Fi access to Internet everywhere in most large cities in the world, Wireless-Detective system can be used by police, military,

information investigation and forensic departments to track down all illegal and unauthorized online activities such as illegal drug dealing, gambling, fraud transactions, child porno, spill-over wireless access and others.



***Diagram: Standalone Architecture – Wireless-Detective System Implementation***

**Wireless-Detective Extreme system** is specially designed to enhance the capturing, decoding and reconstruction capability by utilizing more than one Wireless-Detective systems and a Wireless-Detective Centralized Management Centre to sniff data packets from a target Wireless Channel, AP, or STA.

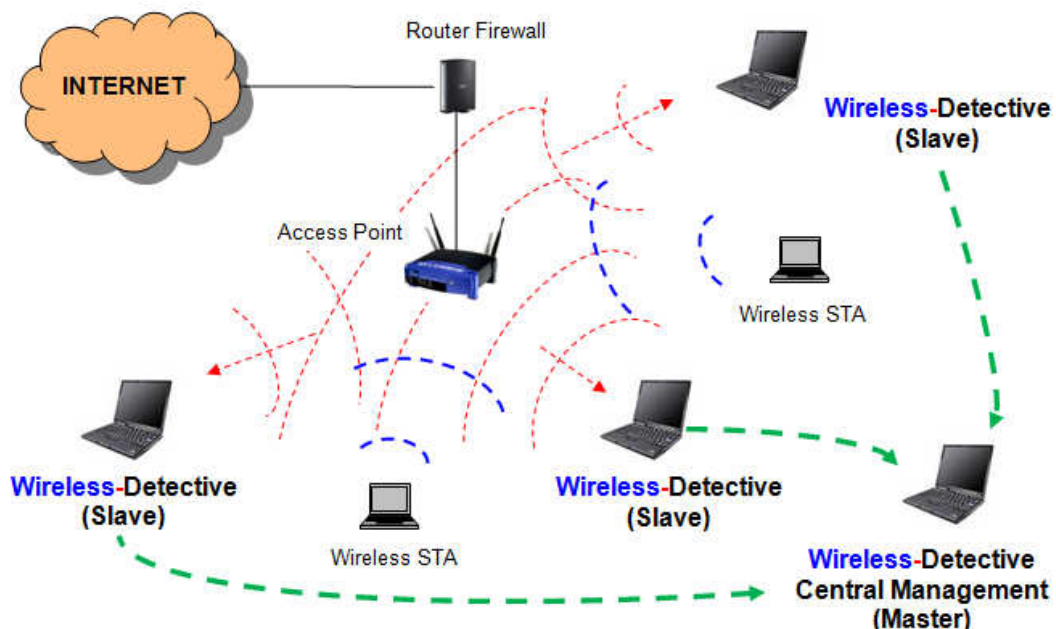
Wireless-Detective system uses sniffer technology to intercept Wireless Local Area Network (WLAN) or Wi-Fi packets ranging from 0 – 100 meters distance depending on the background and the high/low gain antenna used. For indoor environment with walls, furniture blockage, the coverage range would be less (estimated 0 – 25 meters). For outdoor with few blockage and possibility line of sight, the coverage range can be broader. Higher gain omni or directional antenna can be used to extend the coverage range of sniffing WLAN packets.

Based on the physical nature of radio wave, the capture rate of Wi-Fi packets will be enhanced by low down the white noisy of background and magnifying the meaningful signal. Some of the mechanism must be embedded inside the device

driver of wireless network card as well as network function module in the OS kernel. Decision Group spent 2 years to develop such mechanism in Wireless-Detective Extreme system (WDXS), and also passed the benchmark test in SBIR of Department of Industrial technology, Ministry of Economic Affairs, Taiwan in 2010.

The deployment of this WDXS is to utilize more than one Wireless-Detective (WD – Slave) systems managed by a Wireless-Detective Centralized Management (WDCM – Master) system to capture Wireless traffic within the coverage distance of Wi-Fi network. With a group of WD (Slave) systems and WDCM (Master) system performing simultaneous data capturing, the packet loss will be effectively minimized. Hence, it will improve the completeness and integrity of data reconstruction. Data captured by all WD (Slave) systems will be sent to the WDCM (Master) system through **ad-hoc** Wireless communication network among the systems. WDCM (Master) will then re-assemble all the packets captured (from all WD – Slave systems and itself), decode and reconstruct the raw data back to its original content format. If the targeted network is WEP encrypted, each WD system is able to decrypt the WEP key.

### Wireless-Detective Extreme System Implementation



*Diagram: Distributed Architecture - Wireless-Detective Extreme System (consist of 1 Wireless-Detective Central Management (Master) and N x Wireless-Detective Standard Systems (Slave) Sample Implementation*

From internal system setup MENU of each workstation, you can specify one as the Wireless-Detective Central Management system (Master) with several frontend wireless Detective workstations (Slave). Once initiating interception against public WiFi network simultaneously with all workstations, you can get lots of raw data from all Slave workstations into backend Master system. With the high performance reconstruction capability, Master system will provide the most complete reconstruction information for your task.

In some case with lawful enforcement agents, intelligence agents...etc, information from public hot-spot space is quite valuable, because suspect thinks that it is safer to transmit message in such public place with anonymity. With WDXS, those agents can collect all information content, MAC address, IP address, account name, receiver information and associated IP, even password (optional module)...etc. It is a powerful tool for information collection in the field, and also provides utility for data backup for later analysis on link, relationship, text mining...etc with standard ISO format.

The application of wireless network interception device is quite rare in the world, because there is obstacle of physical nature of radio wave: i.e. high data packet loss rate. Decision Group has developed wireless interception tool – Wireless Detective appliance since 2004, and gains lots of practical experience from customers in the field. With such experience, we keep on improving the feature and capability of our product. Wireless Detective Extreme System is our newest product with enhanced capability on high data packet capture rate. We will continue our effort to offer the best in line solution to our customers, and try to make it as industry standard.

*Email: [decision@decision.com.tw](mailto:decision@decision.com.tw)*  
*URL: <http://www.edecision4u.com>*  
*Phone: +886 2 27665753*  
*FAX: +886 2 27665702*