Wireless-DETECTIVE®

Forensics & Investigation Tool

Ranging 50 to 100 meters, and even farther.
Wiretap Computer 802.11 a/b/g Wireless LAN or Network Transmission

Decrypt ···E-mail, Hotmail, Webmail, MSN/ICQ/AOL/Yahoo, FTP, VOIP, ORL Browsing...etc.

Wireless-Detective   Target   AP   Target

Different with normal Sniffer, it can record session then decode and recombine packets to reproduce the original file. If there's common WEP key encrypted wireless transmission, Wireless-Detective can offer WEP decryption function for you. Wireless-Detective can decrypt the WEP key of the length of 64, 128, 256 bits or the special defined WEP key and can also decrypt part of WPA encryption.

A Special Device for Detective and Investigator

The Most Advanced, Smallest System in the World

802.11a/b/g Computer Wireless Network Forensic System

《We are designer and Manufacturer, welcome Project Design, OEM, and ODM》

Functions and Operation Modes

Wireless-Detective 802.11 a/b/g Wireless LAN Detector & Sniffer Module

The primary feature of this module is to detect all 802.11 Wireless LAN communications within the area that this detector can work, and detect any Access Point and station (STA) within its covering area. Furthermore, this detector can combine with Global Positioning System (GPS) and locate the approximate geographic location of detected APs or STAs through electronic map. For more accurate position of STA or AP, the user may connect three E-Detective Wireless detectors with networking connection, high-sensitivity antenna and signal amplifier to calculate the location of the sniffed object through triangulation, and the accuracy can be improved into less 10 meters. The effective area of remote sniffing depends on the weather, terrain and interference. The farthest distance of sniffing can be reached into 2 to 4 kilometers, even 5 kilometer. But the utmost distance couldn't be over 10 kilometers because of the curvature of earth.
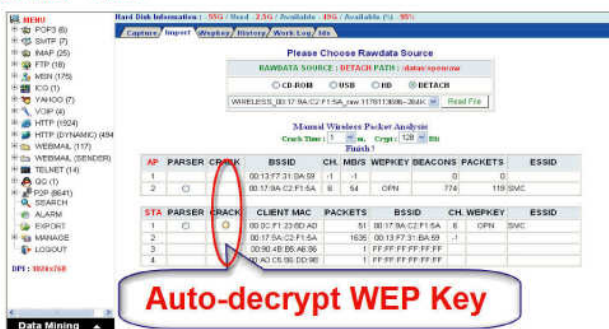
For the completion of sniffing, the sniffer can be configured into the following configurations and functions:

### The information of detectable Wireless LAN AP includes:

1. BBSID of AP (MAC address)
2. Channel
3. The number of STAs
4. The number of encrypted packet
5. The number of data packet
6. Additional information of AP (the manufacturer of AP, the manufacturer of AP IC component has to be authenticated through international registration)
7. Noise level and signal level
8. SSID or ESSID
9. Type of Wireless LAN: Probe, Ad-hoc or Infra
10. WEP (wired equivalent privacy protocol) status
11. The amount of transferring Wireless LAN packet

The information of detectable Station (STA) includes:

1. The number of encrypted packet through this STA
2. The number of packet through this STA
3. IP Address of STA
4. MAC Address of STA
5. The manufacturer of STA (the one has been authenticated)
6. The highest transferring rate of STA
7. Noise level and signal level of STA
8. Type of STA (Established, To-DS or From-DS)

Wireless-Detective Systemized Functions :

A.WEP KEY

Auto-decrypt WEP Key

B.BSSID & Client information

Scanned Access points' Info.

Scanned Stations' Info.
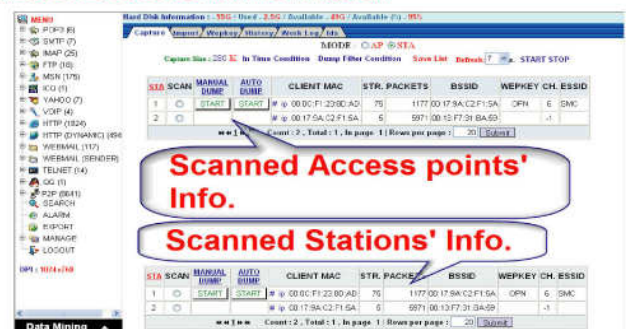
C.GPS Positioning Information

capture 1
capture 3
capture 2

GPS Orientation
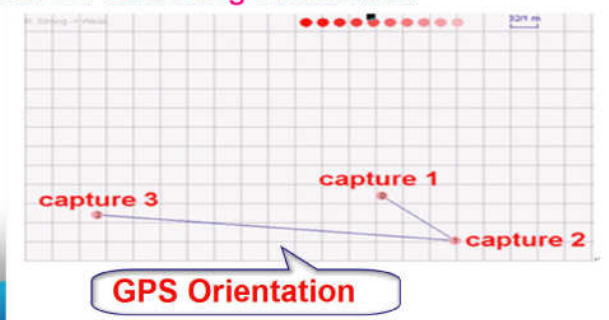
D.Sniff Specific Target

Sniff Specific Targets

In different with normal sniffer, it can decode and recombine packets of session then reproduce the orignal file of every protacal, Wireless-Detective reveal the contents of network transmisson like e-mail, IM, Web browsing, FTP upload and download, Telnet, P2P, On-Line Game...etc.

EN_Wireless Detective_02

Decode and Recover Packets of Different Modes

1.POP3/SMTP/Web/Mail

Detailed Record:
1. Sender/Receiver
2. Account, Pass
3. Attached Files
4. Email Content,..etc.

2.URL Browsing

Browsed Website Content, IP,...etc.

3.IM-MSN, ICQ, YAHOO, QQ

Date/Time, IP, Account, Messages Transferred Files,...etc.

4.Telnet

Date/Time, Account, Pass, IP, Browsed Process,...etc.

5.FTP

Date/Time, IP, Port, Transfer Tool, Transferred File Name,...etc.

6.P2P

Date/Time, IP, Port, Transfer Tool, Transferred File Name,...etc.

7.On-Line Game

Date/Time, IP, Port, Game Name, ...etc.

8.VOIP & Webcam

Click to hear/view records.

Omnibearing content recovering and forensic function, make information reveal completely.

Solidified Technics Helps Tackle Your WLAN Communications

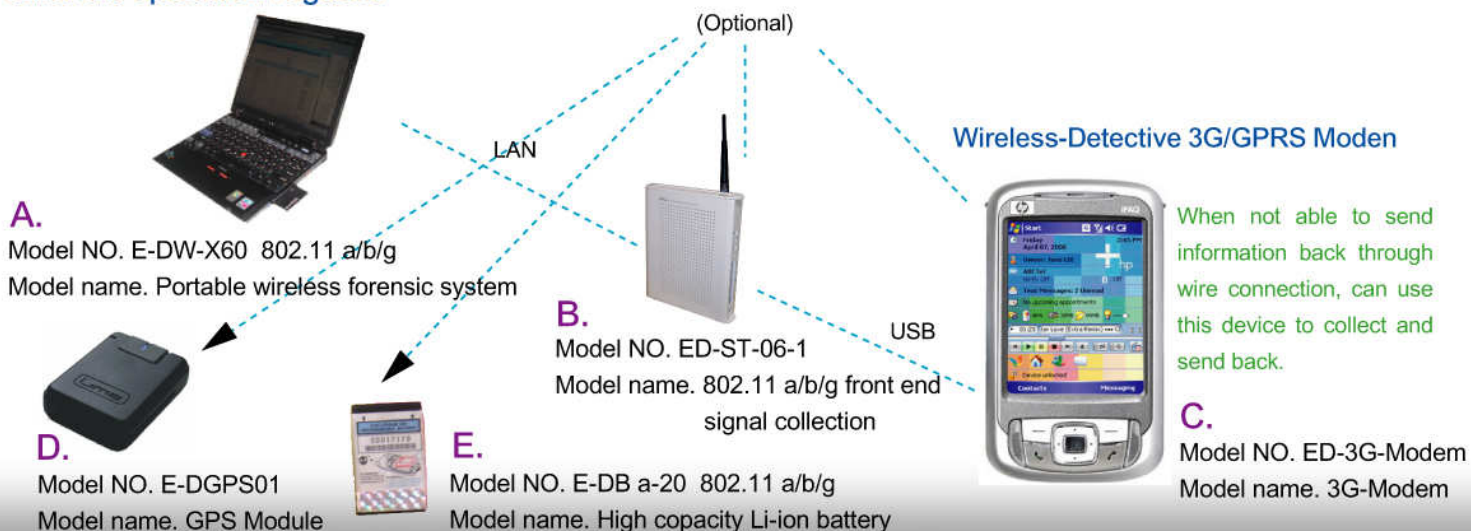## Wireless-Detective Network Forensic Operation Models

A. Single Device Operation

Wireless-Detective

Target

AP

Target

B. Front and Back and Operation Model

Wireless-Detective   ED-ST-06-1

LAN

Target

AP

Target

C. Remote site Detecting Model

ED-ST-06-1

INTERNET

ED3G-Modem

E-DW-X60 802.11 a/b/g

Target

AP

Target

Wireless-Detective network forensic devices offen various models and options for customer base on different operation reguest

(Optional)

LAN

Wireless-Detective 3G/GPRS Moden

A.
Model NO. E-DW-X60 802.11 a/b/g
Model name. Portable wireless forensic system

B.
Model NO. ED-ST-06-1
Model name. 802.11 a/b/g front end signal collection

USB

When not able to send information back through wire connection, can use this device to collect and send back.

D.
Model NO. E-DGPS01
Model name. GPS Module

E.
Model NO. E-DB a-20 802.11 a/b/g
Model name. High copacity Li-ion battery

C.
Model NO. ED-3G-Modem
Model name. 3G-Modem

Wireless-Detective Leading Technologies Make Everything Under Your Control.
Decision's R&D Team Create Innovative Technologies For You

EN_Wireless Detective_04