White Paper for E-Detective System (Wireless)

An Introduction

Internet access have become more and more popular by the emergence of broadband services, and busy yet unregulated Internet traffic cause a challenge to administrator and management. E-Detective system can automatically sniff Internet activities of Email, Chat, URL and File Transfer (FTP), P2P, Telnet, Online Games etc. E-Detective can improve corporate efficiency, prevent network resources from misusing, block the loophole of leaking confidential information, monitor cyber-slacker and avoid accidental deleting and damage of email (recover from backup).

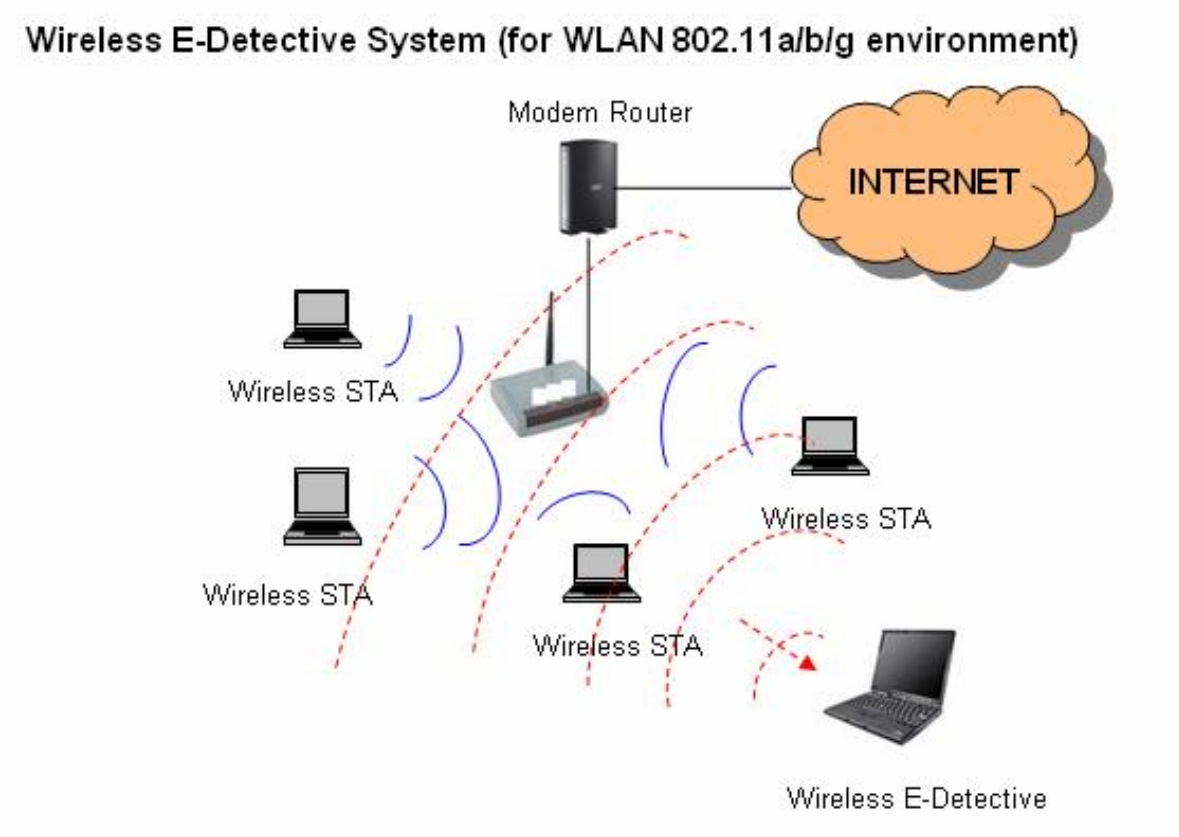
Network Sniffing is one of important way to preserve evidence. It will duplicate every activity and data transfer at the gateway of your network, and it also needs a powerful system to perform on-line sniffing, real-time recording, categorizing, correct misbehavior, search by parameters/keywords, statistics analysis, etc.

Wireless E-Detective adopts optimized Linux as the kernel and powerful Java Applet to provide a complete graphic interface, the user can install and use on the fly (Plug & Play). Wireless E-Detective's speedy wireless packet sniffing technology can sniff on specific target (by AP or STA) or scope (by channel) without interfering original network environment.

Since wireless access to Internet has been very popular at every where (Café, Restaurant, Airport, Shopping Malls, etc), Wireless E-Detective can be a perfect solutions for police, military, information investigation and forensic departments as a legal interception tool to crack and track down illegal internet activities such as illegal betting, transactions, access and activities that may lead to terrorism.

Wireless E-Detective System Application

Wireless E-Detective sniffs wireless packets (802.11a/b/g) from any available wireless network in its range of coverage. User can select specific wireless device (AP or STA) or network for data capturing. User can also capture date from specific wireless channel. For Open wireless network where no encryption is set, Wireless E-Detective system can capture the wireless packets and decode and display them immediately in original and readable format. For wireless network with encryption such as WEP key, Wireless E-Detective system can crack the WEP key automatically or manually.



Introduction to E-Detective 802.11 a/b/g Wireless LAN Forensics Appliance

First module E-Detective 802.11 a/b/g Wireless LAN Forensics Appliance provides front-end packet collection sub-module and back-end protocol restructured sub-module. This module can act as both wireless LAN detector and sniffer; and the sub-module is used to detect 802.11a/b/g Access Point (AP) and Wireless Station (STA) over the layer 2 network communication. The second module acts as a module of restoring and performing forensics, which categorizes the retrieved packet by its wireless nature and restores packet arrangement by sequence, then save the packet. At the same time, it will decipher the categorized packet by known protocol into plain text and store them into database for reference.

The information of detectable AP includes:

- BSSID of AP (MAC address)
- Channel
- The number of STAs
- The number of encrypted packet
- The number data bytes
- Additional information of AP (the manufacturer of AP IC component has to be authenticated through international registration)

- Noise level and signal level
- SSID or ESSID
- WEP (wired equivalent privacy protocol) status
- Others

The information of detectable Station (STA) includes:

- The number of packets transferring to and from this STA
- IP Address of STA
- MAC Address of STA
- The manufacturer of STA (the one has been authenticated)
- The highest transferring rate of STA
- Noise level and signal level of STA
- Others

Content Monitoring Functions:

1. Email (POP3, SMTP, IMAP, Webmail)

Wireless E-Detective system reconstructs Email content which includes sender and receiver's Email address, CC, BCC and mail content with attached files. Emails that use SMTP (Outbound) and POP3 (Inbound) protocols running with Email Client like Microsoft Outlook Express, Microsoft Office Outlook etc can be reconstructed. Besides, Common Web Mail (Read and Sent) such as Yahoo mail, Hotmail, Hinet, PCHome, URL, Giga, Yam, Sina and etc. can be reconstructed and displayed as well.

2. Instant Message (YAHOO, MSN, ICQ, AOL, QQ)

Wireless E-Detective reconstructs the content of instant messages such as MSN, Yahoo Messenger, AOL, ICQ and QQ which includes IP, date/time, user handle, participant, message content and file transfer through MSN and YAHOO.

3. Website (HTTP Link, HTTP Content)

Wireless E-Detective reconstructs Website content which includes IP, date/time, URL (HTTP Link), HTTP content etc.

4. File Transfer Protocol (FTP)

Wireless E-Detective reconstructs FTP content which includes IP, login ID, password, server IP, file name and content, action (upload or download) etc.

5. Peer to Peer Communication Protocol (P2P)

Wireless E-Detective captures and displays P2P information which includes date/time, local IP, local port, peer IP, peer port, file name, hash key etc.

5. Telnet

Wireless E-Detective reconstructs Telnet session. It also provides "playback" function.

6. VOIP and Webcam for MSN and YAHOO Messenger (Forensics version)

Wireless E-Detective reconstructs VOIP and Webcam sessions. VOIP and Webcam sessions using Yahoo Messenger and MSN Messenger can be reconstructed. The reconstructed VOIP and Webcam session can be playback.

7. Online Game

Wireless E-Detective captures and displays online games information such as date/time, local IP, local port, server IP, server port, game name etc. Example of online games are Maplestory, ZT, FairyLand, Kinf of king, Katrider, BnB, Mabinogi, Hotdance, Gatamped, Pangya, Heatproject, DTG, Superrich, O2jam, Seal, COCOCAN, Nage, Gersang, Laghaim, Hot, 3P, SF, Noritel, Elysium, Stoneage, A3, HE, ZU, Cabala, JY1, JY2, Wonderland, SAN, TS, LoveBox, SANGO, Dekaron, Cabal, Rohan, GVO, CG, DOMO, BO, SWDOL, DOMOFREE, RICHOL, RO, Mir3, JX, JX2, TTH, RF Online, SOL, Nobol, FDO, GHOSTSOUL, AL, CPW, 1003b, 9D, EverQuestII,.

Silkroad2, Metin, MS, SUN, Hero, HB, WE5, FongShen, FongShen2, Q3baby, SHE and Megaten.

Management Functions:

1. System Control

Wireless E-Detective allows browser-based modification to networking setup, DNS setup, correspondent IP, communication port and shut down control. It also displays the information of hard disk drive usage, which includes HDD size, used space, available space, percentage of usage, and warning at the used space reaching 80%.

2. User list

Wireless E-Detective allows editing of user's IP and Domain Name. It as well displays the status of current users

3. User account management

Wireless E-Detective allows setting up of username, password, group and authorization.

4. Security management

Wireless E-Detective has built-in firewall and group limitations. It provides system data confidentiality and best security.

5. Data backup and exporting

Wireless E-Detective provides importing and exporting abilities to CD-ROM and data backup for evidential data storing and processing.

6. Importing of raw data

Wireless packets (raw data) can be imported into the system for parser and content reconstruction.

7. Search by Parameters and Search by Keywords

General search by date/time, IP, MAC etc. Specific search by different applications. Search by keyword.

The Benefits of Wireless E-Detective

- Prevent confidentiality disclosure
- Prevent company for being hacked
- Protect business right (such as intellectual property etc)
- Wireless traffic management and utilization monitoring
- Managing wireless network access behavior
- Backup and reconstruction of information
- Help government and law enforcement agencies such as Police and Military force to neutralize threats from terrorists and criminals
- Mobility and portability
- Legal interception system

Main Features of E-Detective

- Exclusive operating system (Linux OS)
- Non-intrusion mode means it is undetectable
- Web-based management interface
- Decrypt encryption (WEP, WPA) of wireless network
- Monitor multiple internet and communications protocols
- GPS for locating wireless device
- Access control ensures only authorized use of resources

- Easy to define monitoring and alerting rules
- Quick search function
- Data backup and recovery solution

Who needs Wireless E-Detective?

- Business Enterprises (finance and banking) sector
- Government ministry
- Police sector
- Military sector
- Forensics and Information Investigation
- Lawful department

Note: Wireless E-Detective System functions and features are subjected to updates and changes from Decision Computer.

