Wireless E-Detective Standard Specifications

Hardware Specification

IBM ThinkPad X61 Series base + External wireless PCMCIA network card (Atheros Chipset) that support 802.11a/b/g standard

Software Specification

Wireless E-Detective – Debian Linux OS

E-Detective Functions

A) Wireless Scanning and Packets Capturing Function:

- Wireless devices (Wi-Fi enabled device) working at 802.11 a/b/g standard wireless environment coverage ranging from 0-100 meter depending on environment factor.
- Capable of specific target AP/STA sniffing/capturing or by channel sniffing/capturing.

B) Wireless Decryption Function:

WEP key decryption (64, 128 and 256-bit) – Auto and Manual Decryption.

C) Decoding and Reconstruction Function:

Protocols that Wireless E-Detective system decoded and reconstructed can be displayed in real and exact format content with details.

1. **Emails (POP3, SMTP, IMAP, Web Mails Read and Sent)**

POP3: Record IP, Date/Time, From, To, CC, Subject, Account, Password, Content and Attachment of the email.
SMTP: Record IP, Date/Time, From, To, CC, BCC, Subject, Size, Content and Attachment of the email.
IMAP: Record IP, Date/Time, From, To, CC, Subject, Content and Attachment of the email.
Webmail (Read): This will record the date and time, subject and page content of inbound Web mail Read such as Hotmail/ Windows Live Mail and Yahoo Mail Standard and Beta, Gmail etc.
Webmail (Sent): Record the IP, date and time, subject and email content and attachment of emails (Web mails like Yahoo Mail Standard and Beta, Hotmail/ Windows Live Mail, Gmail new and older version etc.) sent by users on the network.
Other Types of Web Mails: *Hinet, PCHome, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com.*
Note: *A new tool developed by Decision Computer known as Webmail Token Analyzer which is capable to define different Webmail types is included in the system.*

2. **File Transfer Protocol (FTP)**

Record IP, Date/Time, Account, Password, Action (Upload/Download), FTP Server, File Name and the file content.

3. Instant Messengers (IM) Chat

- Real time IM message reconstruction

MSN: Record IP, Date/Time, Screen Name, Participants, Conversation, Counts and file transfer.

Note: *Tested and supported MSN version 8.5 beta and 8.1 and below. It is subjected to updates and changes.*

ICQ: Record IP, Date/Time, Screen Name, Participants, Conversation, Counts.

AOL: Record IP, Date/Time, Screen Name, Participants, Conversation, Counts.

QQ: Record IP, Date/Time, Screen Name, Participants, Conversation, Counts. (needs to decrypt manually by some settings).

YAHOO: Record IP, Date/Time, Screen Name, Participants, Conversation, Counts and file transfer.

Skype: Record sessions of VOIP chat. (Note: content cannot be reconstructed due to encrypted)

Note: *Tested and supported Yahoo version 7.5, 8.0, 8.1). It is subjected to updates and changes.*

4. HTTP (Link, Content, Reconstruct, Upload/Download)

HTTP Link: Record IP, Date/Time and URL links. When connected online, user/admin can click on the link to access on the page.

HTTP Content: Record IP, Date/Time, URL link with content at the moment the user accesses that URL.

HTTP Reconstruct: Record IP, Date/Time, URL Link and page content reconstructed for webpage viewed.

HTTP Upload/Download: Record IP, Date/Time, URL Link and file reconstruction of file upload/download through HTTP.

5. Telnet

Record IP, Date/Time, Account, Password, Server IP, File Name and Playback content.

6. VoIP and Webcam Sessions

Record VOIP and Webcam Sessions of MSN/Windows Live and Yahoo Messenger.

YAHOO VOIP: Support YAHOO version 7.5, 8.0, 8.1.

MSN Webcam: Support MSN version 8.1.

YAHOO Webcam: Support YAHOO version 7.5, 8.0, 8.1.

Note: *This function is subjected to version changes and updates by MSN and Yahoo Messenger.*

7. Peer to Peer (P2P) Communications

Record IP, Date/Time, Port used, Peer Port, Peer IP, Tool being used, Filename transferred, Action (Download/Upload) and Hash key. Records P2P Communications logs (*BitTorrent, BearShare, Foxy, Limewire, Ezpeer and Kazaa etc.*).

8. Online Games

Record IP, Date/Time, MAC address, Port used, Game server IP, Game server Port and Game name. The Online Games that can be logged are like 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.

D) Management Function:

1. **Search by Parameters and Search by Keywords**

Search by Parameters: Allow General search by Date/Time, IP, MAC address etc. Allow specific application search.
Search by Keywords: Allow keywords search.

2. **Notification/Alert (by condition, hard disk capacity full etc.)**

Administrator can set different condition based on different online application for notification and alert. If any of the condition meets, administrator will be informed through email alert.

3. **Import, Export and Backup Data (Burn to CD or Export to External Hard drive)**

Import: Wireless raw data file in tcpdump (pcap) format can be imported into the system for decoding and reconstructing purpose.
Export: Captured raw data or decoded data can be exported out for backup into external storage or burn into CD/DVD.

4. **Authority Setup**

Administrator can setup authorized user to access the system.

5. **System Setup (Network Setup)**

Administrator can setup IP and network information for the system.

6. **Delete Data**

Captured data can be deleted by specific application or delete all data.

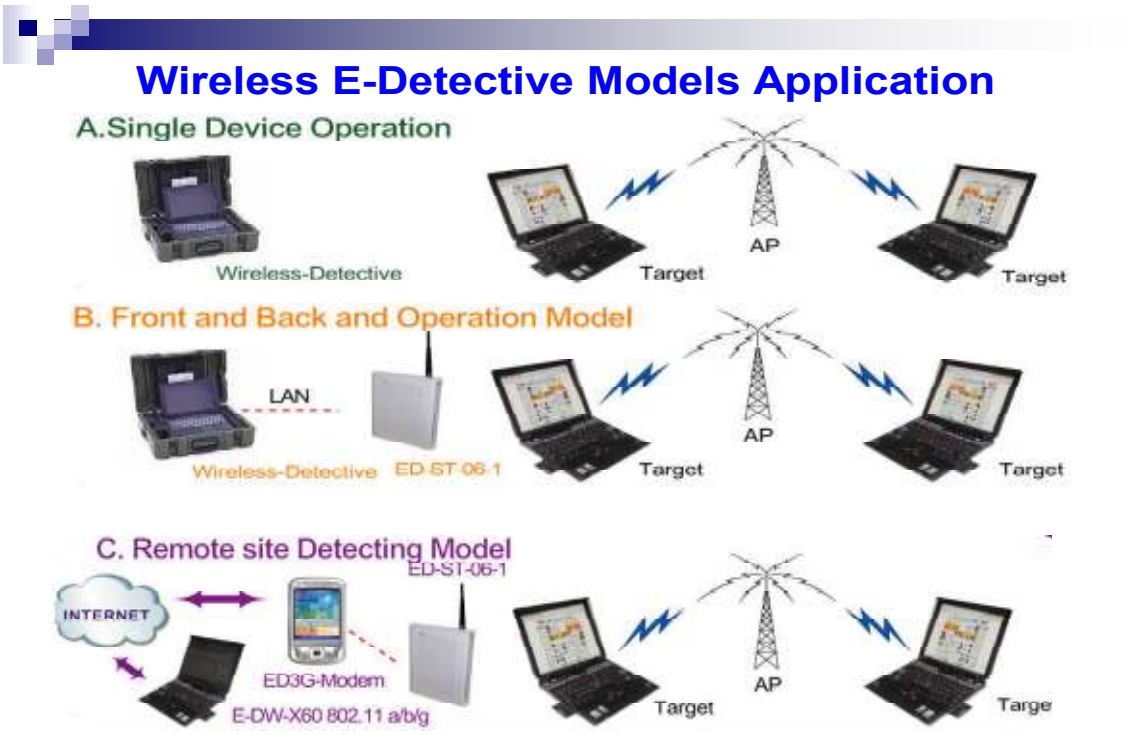
E)Other Function:

1. **GPS Orientation**

Longitude and Latitude of the system relative to the signal strength of targeted AP/STA.

Note: *All functions and features are subjected to updates and changes by Decision Computer International Co., Ltd.*

Models:



Note: *Model A is the most common model used by all forensic, intelligence and legal intercept agencies. Model C is not released yet.*