

Wired E-Detective System (Standard Version) System Specification



Hardware Specification:

Please refer to our website at www.ed-system.sg.

Note: These specifications may change due to upgrade and updates of our systems.

Software Specification:

Wired E-Detective system captures Ethernet packets from LAN network (10/100/1000 Mbps), decodes and reconstructs the raw data into original and exact information or message.

Protocols captured and decoded by E-Detective:

1. Emails (POP3, SMTP, IMAP, Webmails)

POP3: Record Date/Time, Sender, Receiver, CC, Subject, Size, Content and Attachment of the email.

SMTP: Record Date/Time, Sender, Receiver, CC, BCC, Subject, Size, Content and Attachment of the email.

IMAP: Record Date/Time Sender, Receiver, CC, Subject, Content and Attachment of the email.

Webmail (Read): Record Date/Time, IP, URL/Page Content of Webmail Read such as Hotmail (Standard version).

Webmail (Sent): Record Date/Time, Sender, Receiver, CC, BCC, Subject, Webmail Type and email content and attachment of email sent by users on the network.

Types of Webmail pre-defined and supported: **Hotmail/ Windows Live, Yahoo Standard Mail and Yahoo Beta Mail (2.0), Gmail (Older and Newer Version), PCHome, Hinet, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com.**

Note:

User may use Webmail Token Analyzer to define those unknown/undefined Webmail Types.

2. File Transfer Protocol (FTP)

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

3. Instant Messengers (IM) – Real Time Decoding/ Reconstruction

MSN/ Windows Live Messenger: Record Date/Time, IP, User Handle, Participants, Conversation, Counts. It also records and reconstructs the Webcam session (allow playback).

ICQ: Record Date/Time, IP, User Handle, Participants, Conversation, Counts.

AOL: Record Date/Time, IP, User Handle, Participants, Conversation, Counts.

QQ: Record Date/Time, IP, User Handle, Participants, Conversation, Counts. (need to decrypt manually by some settings).

YAHOO: Record Date/Time, IP, User Handle, Participants, Conversation, Counts. (It also includes reconstruction of VOIP and Webcam sessions playback)

UT Chat room: Record Date/Time, IP, User Handle, Participants, Conversation, Counts.

Skype: Records the Date/Time, User and Participant IPs, Conversation Period, Counts.

Note:

The supported features, VOIP and Webcam reconstruction of MSN/Windows Live Messenger and YAHOO may change due to update by both Windows Live Messenger and YAHOO. We will provide the update patch once available.



4. Peer to Peer File Transfer (P2P)

Record Date/Time, IP, Port used, Peer Port, Peer IP, Tool being used, Filename transferred, Action (Download/Upload). P2P supported are like *BitTorrent*, *BearShare*, *Foxy*, *Limewire*, *Ezpeer* and *Kazaa* etc.

5. Telnet

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

6. Online Games

Record Date/Time, IP, Port used, Game Server IP, Game Server Port and Game Name. The Online Games that can be logged are like Maplestory, ZT, FairyLand, King of King, Katrider, BnB, Mabinogi, Hotdance, Gatampad, 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.

7. HTTP (LINK)

Record Date/Time, IP and URL links. When admin's PC is connected online, admin can click on the link to access to the website.

8. HTTP (CONTENT)

Record Date/Time, IP, URL Link with Content captured at that moment the user accessed that URL.

9. HTTP (RECONSTRUCT)

Record Date/Time, IP, URL Link with reconstructed web page of websites that are accessed by the users.

10. HTTP (UPLOAD/DOWNLOAD)

Record Date/Time, IP, URL Link, File Name with Content, File Size.

Management functions of E-Detective system:

1. System Setting

Set system IP/ network and Domain configurations, filter configuration, check hard disk size and memory status, define storage policy (disk space control), protocols/ services and system time setup, edit system password, port number configuration etc.

2. Backup (Auto/Manual/FTP Backup)

Backup data into image format (ISO file). Manual backup data into image (ISO file) format at any time convenient to administrator. Auto backup data by selecting date/time and specify the applications/categories. Backup file can be burned into CD/DVD. FTP backup data by connecting to an FTP server. Backup ISO file can be read by using Application Server software provided by Decision Computer.

3. Network Users and Authority Setup

Check on Online List, Network Users, Configure IP to match PC Name, Skip and Ignore IP, Add groups and users etc.

4. System Update

The E-Detective system, ED 2.0 can be updated easily by uploading the update patches through the web management interface.



5. Delete Data

Delete data by specific application/category and delete all data in the system.

6. Station Management

Station list, NetBios PC list and Active Directive Account list.

7. Registration

Registration of system through box.

8. Search by Parameters and Search by Keywords

General search by date/time, IP, MAC etc. Specific search by different applications. Search by keyword. Similar contents search is also available.

9. Alert with Content

Alert can be created base on alert parameters set such as alert by key words, file extension etc. Administrator can be informed or alerted through email if any of these parameters meet the condition. Throughput alert can also be set to alert the administrator regarding specific user has reach the bandwidth limit allowed.





10. Reports

Single, Group and Comprehensive Statistical reports can be created.

Note:

Features and functions are due to update and change by Decision Computer International Co., Ltd.

E-Detective Models & Spec

Model Number	PIC	Client Supported	HDD SIZE	DUD	External Storage Support	Infrastructure
ED-FX 6		10-49	80G	-	-	Single
ED-FX30		50-200	160G	✓	-	Single
ED-FX100		201-999	120G-300G Max.	✓	Support	Double
ED-FX120		above1000	120G-300G Max.	✓	Support	Double

