



Version: 25/Apr/2007

User Manual

Decision Computer International Co., Ltd.



Copyright © 2007 Decision Computer International Co., Ltd

IMPORTANT NOTICE

This guide is delivered subject to the following conditions and restrictions:










Copyright Decision Computer Ltd. 2007. All rights reserved.

The copyright and all other intellectual property rights and trade secrets included in this guide are owned by Decision Ltd. The guide is provided to Decision customers for the sole purpose of obtaining information with respect to the installation and use of the E-Detective System, and may not be used for any other purpose.

The information contained in this guide is proprietary to Decision and must be kept in strict confidence.

It is strictly forbidden to copy, duplicate, reproduce or disclose this guide or any part thereof without the prior written consent of Decision.

Content

Chapter 1. Introduction	5
Chapter 2. E-Detective Function Description.....	7
A. Emails Recording	8
1. POP3 [inbound]	8
Ignore & Ignore and Delete:	9
Search:.....	10
Forward Email: 	10
Convertor: 	11
View Email content:	11
2. IMAP [inbound]	12
Search:.....	13
Forward Email: 	13
Convertor: 	13
View Email content:	14
3. SMTP [outbound].....	15
Ignore & Ignore and Delete:	16
Search:.....	17
Forward Email: 	17
Convertor: 	17
View Email content:	18
3. Webmail [inbound].....	19
Search:.....	20
Forward Email: 	20
View Email content:	20
4. Webmail (Send) [outbound]	21
Search:.....	22
Forward Email: 	22
Convertor: 	23
View Email content:	23
B. Instant Messengers (IM)	24
1. MSN.....	24
Search:.....	25
Display set:.....	25
MSN conversation:.....	26
2. ICQ / AOL	27
Search:.....	28

Display set:.....	28
ICQ conversation:.....	29
3. YAHOO	30
Search:.....	31
Display set:.....	31
YAHOO Conversation & Video Conference:	32
4. QQ	33
Search:.....	34
Display set:.....	34
Information- How to see the encrypted conversation:.....	35
Step 1 – Download the QQ cracker:	35
Step 2 – Install QQ cracker into computer.	35
Step 3 – Decrypt the conversation.	39
C. File Transfer.....	43
1. FTP	43
Search:.....	44
2. P2P	45
Search:.....	46
D. WEBSITE	47
1. HTTP	47
Search:.....	48
2. Web Page [URL Content]	49
Search:.....	50
Source code: []	50
E. Telnet	51
1. Telnet	51
View the browsing process:.....	52
Search:.....	52
F. SETTING	53
1. Network Set	53
Device Sets:	54
Mirror Mode:.....	55
Sniffer Mode:.....	58
Bridge Mode:.....	61
SENDER/ RECEIVER Mode:.....	64
DNS Set:.....	69
Shutdown/Reboot System & Time adjusting:	69
2. Storage	70

3. Services	71
FireWall:	73
4. Edit Password	74
5. Backup Data	75
Auto Backup:	75
Backup:	76
FTP Backup:	77
6. Domain	78
7. Network Rules	79
8. Setup Mail	82
Testing the Mail Server Adopted:	82
G. STATUS	83
1. Backup Record	83
2. Port number	84
3. Online IP	85
4. Login List	89
H. TOOL	90
1. Delete Data	90
In Time:	90
Schedule:	90
Record Count:	91
Delete All Data:	91
2. Group Set	92
Create New Group:	92
Rename the group:	92
3. Add Users	93
4. System Warning	94
HD Alarmer & Custom-Made Warning File.	94
Daily Report	95
5. Flow Warning	96
Show Monitored IP	96
Show All IP	96
Edit Admin Mail	96
Edit Monitored IP	97
Search IP	97
Interval Time (H)	97
I. REGISTER	99
J. Data Search	100

- 1. Data Mining 100
- 2. Search 103
 - Example 1 104
 - Example 2 105
 - Example 3 106
 - Example 4 108
 - Example 5 110
 - Example 6 112
 - Example 7 114
- K. Reporting 116
 - 1. Single functional report (Single Report) 116
 - 2. Group IP with Group Report (Group Report) 120
- Appendix A: Q&A 122

Chapter 1. Introduction

Internetworking becomes the most popular communications nowadays, escalation of frequent communications on internet becomes a challenge of monitoring and management. E-Detective is an Internet Surveillance System. It intercepts Email, instant messaging, web surfing, file transferring and telnet sessions. E-detective encourages efficiency, prevents network resource from abuses, keeps confidentiality from leaking, and monitors activities of employees.

Network interception is an important approach to gather information of communications and digital evidence. Interception solutions capture all the traffic on the network and monitor the activities. It is capable of live intercepting, real time recording, category classifying, behaviour correcting, data mining, analysing and statistics.

E-Detective is optimised and based on Linux OS, It provides user friendly interface powered by Java plug-in, and well-tuned provisioning for easy installation and starting. E-Detective is capable of deep packet interception on high speed IP network, and able to target specific objective by using non-intrusive interception technology. E-Detective is a flexible policy based and non-intrusive network access behaviour monitoring solution. Alarm is triggered when violation of rules occurred.

The Benefits of E-Detective:

- Track down work effectiveness and prevent employees' laziness and boredom
- Prevent spam mails and invitation of virus
- Prevent cookies with "malicious intent" penetrating the network
- Prevent bandwidth wastage
- Prevent confidentiality disclosure
- Prevent company for being hacked
- Protect business right
- Traffic management and utilisation monitoring
- Managing network access behaviour
- Backup and reconstruction of information
- Help government and law enforcement agencies neutralize threats from terrorists and criminals

Main Features:

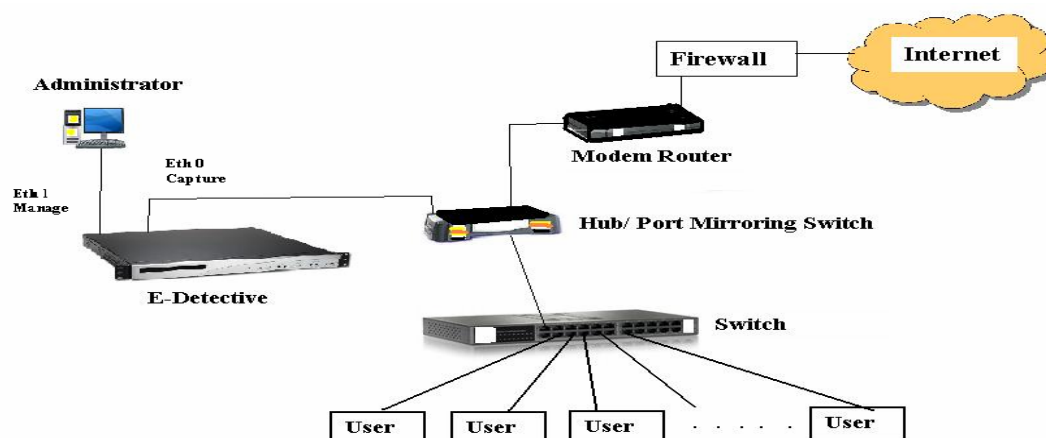
- Exclusive operating system
- Non-intrusion mode means it is undetectable
- Web-based management interface
- Monitor multiple internet and communications protocols
- Access control ensures only authorized use of resources
- Easy to define monitoring and alerting rules
- Centralized monitoring of local and remote stations
- Quick search function
- Useful management reports
- Data backup and recovery solution

3 Types of Companies that Need E-Detective:

- [1] Companies who want to monitor the daily activities of their staffs.
- [2] Financial, Banking and Investment companies who want to monitor and record daily transactions.
- [3] Companies like Marketing, Design and Architectural, Research & Development (R&D) and other corporate businesses which critically need the prevention of data and confidential information leakage.

E-Detective Basic Application Diagram

The diagram below is a Common E-Detective Application diagram which can be applied to any company networks. It uses the sniffer technology to sniff or capture network packets. It uses protocol converter to decode the information and displayed in original readable format. It also stores the recorded information.

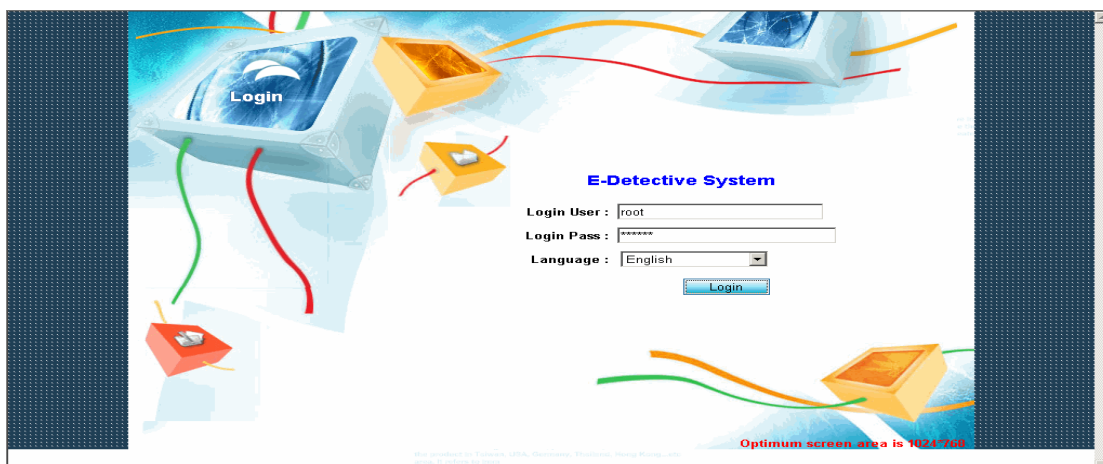
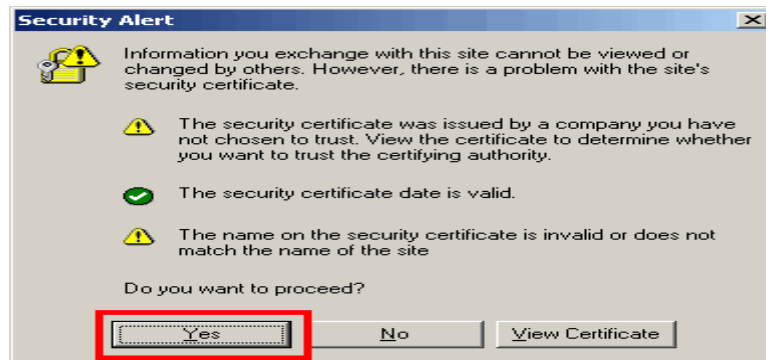


Support: <http://www.edecision4u.com>

Chapter 2. E-Detective Function Description

Remote Login

1. Use browser to access E-Detective server. E-Detective system uses 443 port, so please remember to type https://, e.g.https://192.168.1.60 (default)
2. User Name: root
Password: 000000
Choose you preferred language ([Traditional Chinese] · [English]) and press login button.



The navigation bar is on the top, and please follows chapters in this manual for details.



A. Emails Recording

E-Detective System records Emails and displays them in original message format.

Emails recording supports :

1. POP3 [inbound]
2. IMAP [inbound]
3. SMTP [outbound]
4. Webmail [inbound]
5. Webmail (send) [outbound]

1. POP3 [inbound]

Post Office Protocol 3 or POP3 [inbound] records information about the Email such as message arrival (received) time, sending time, sender, receiver, carbon copy, subject, size and attachment. The POP3 application sample is like Outlook Express, Microsoft Outlook/ Exchange and etc.



Features in this user interface (UI):

[1] : **POP3** : Refresh the page.

Delete : Delete the email that is checked.

Ignore : Ignore is to hide the email and put its information into a list if the email is checked and then click the ignore link. If there are any coming emails which are the same as the emails in the list, the system will hide these coming emails. User won't be able to see them. But system still stores these emails.


Ignore and Delete : This link is to skip any emails and put those email's information into a list when the emails are checked and click this link. ED system not only to hide the emails but also not


store them if there are any coming emails which are the same as the emails in the list.


Search : Users search the particular emails based on the specified conditions such as date, time, ip, receiver, sender...etc.


[2] : **Every Page**: It is to display how many records per page. Users input the number and press the confirm button to set up.

[3] : **Checkbox**: Records could be deleted or ignored by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.

[4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.

[5] :  : Place cursor on this icon to show recorded IP address.

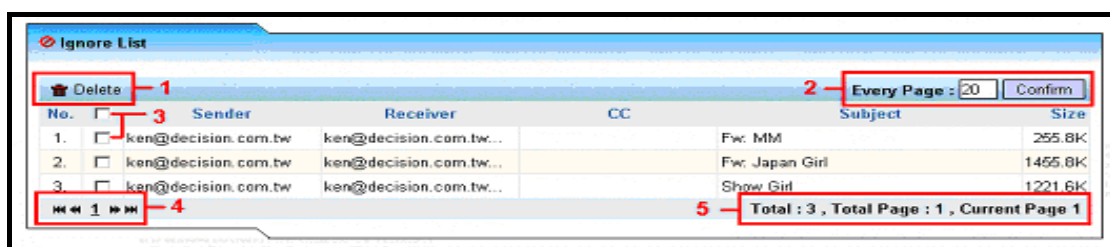
[6] :  Forward Email: To forward record to a specified email account.

[7] :  Convertor: A Convertor to convert the subject's name if the subject's name is unreadable.

[8] : Subject: Click on Email's subject to see the content or download mail record.

Ignore & Ignore and Delete:

The following UI called ignore list will be popped up if users click either the [Ignore] link or the [Ignore and delete] link because both of these two functions have the exactly same figure of UI.



Features in this Ignore list:

[1] : Delete : Delete the records that are checked.

[2] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.

[3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.

[4] : First, Previous, Next and Last Page.

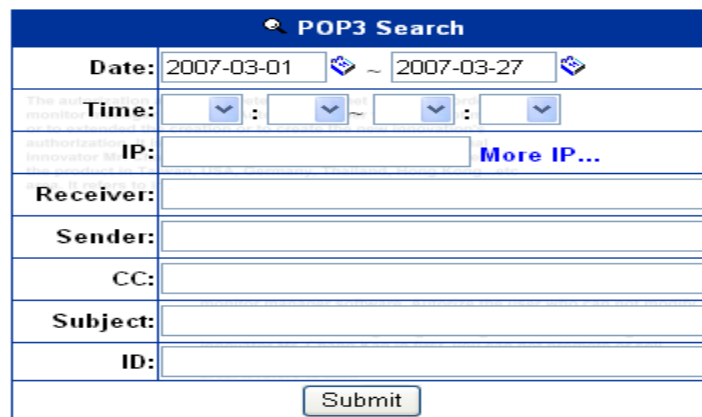
[5] : Current page's information.

In terms of [Ignore] function, its list records the Email's information such as sender, receiver, cc, subject and size that the user are not interested in seeing. If there are any comings Emails which are the same as the records from this list, these coming Emails will be hidden but still be stored.

In terms of [Ignore and Delete] function, its list records the Email's information such as the sender, receiver, cc, subject and size that the users do not want to store them into the system. If there are any comings Emails which are the same as the records from this list, these coming Emails will be auto-deleted.


Search:

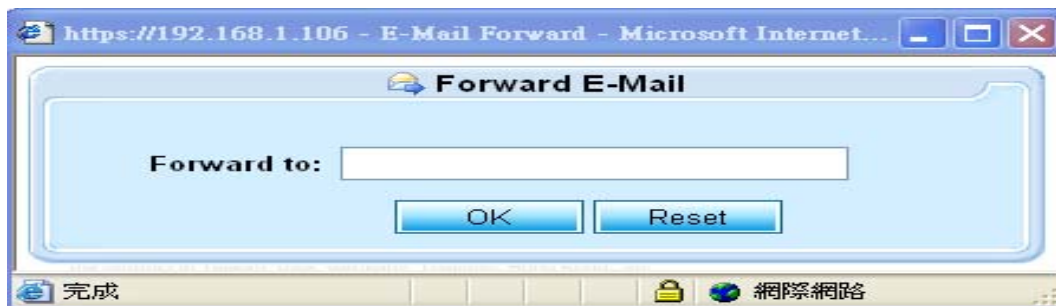
Users click on [Search] link to popup the following UI and search the particular Emails according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.



The screenshot shows a web form titled "POP3 Search". It contains several input fields: "Date" with a range from "2007-03-01" to "2007-03-27"; "Time" with dropdown menus for hour, minute, and second; "IP" with a text input field and a "More IP..." link; "Receiver:", "Sender:", "CC:", "Subject:", and "ID:" each with a text input field. A "Submit" button is located at the bottom of the form.


Forward Email: 

The following UI will be popped up when click the icon . In the blank field users type the email account at where the email is forwarded.



The screenshot shows a dialog box titled "Forward E-Mail" with a "Forward to:" label and a text input field. Below the input field are "OK" and "Reset" buttons. The dialog box is displayed in a browser window with the address bar showing "https://192.168.1.106 - E-Mail Forward - Microsoft Internet...". The browser's status bar at the bottom shows "完成" (Complete) and "網際網路" (Internet).

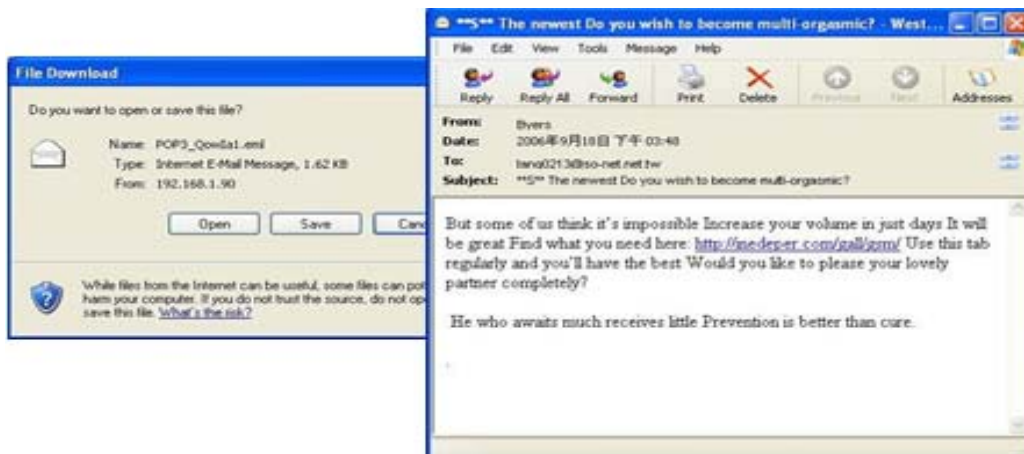
Convertor: 

The following UI will be given if the icon  is clicked. Users use convertor to change the characters if the subject is unreadable. This convertor transfers the character in different formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).



View Email content:

Click on Email subject, the following two UIs will be given. Users choose open button to see mail's content or save it into computer.







2. IMAP [inbound]

Internet Message Protocol (IMAP) records information about the Email such as message arrival (received) time, sending time, sender, receiver, carbon copy, subject, size and attachment.

No.	<input type="checkbox"/>	Date-Time	Sender	Receiver	CC	Subject	Size
1.	<input type="checkbox"/>	2007-03-26 09:42:27	sunny@decision.com.tw	taipeidecision@aol.com		Fw: F*~@j@k/YX	54.2K
2.	<input type="checkbox"/>	2007-03-26 09:42:27				No Subject	0B
3.	<input type="checkbox"/>	2007-03-24 11:20:44	root@decision.com	taipeidecision@aol.com		Bandwidth Monitor Alert	2K

Callouts in the image:
1: IMAP, Delete, Search buttons
2: Every page input field and Confirm button
3: Checkbox for row 1
4: Date-Time column header
5: IP address icon for row 1
6: Forward icon for row 1
7: Convert icon for row 2
8: Subject text for row 1
9: Total 14, Total Page 5, Current Page 1
10: Page navigation buttons (1, 2, 3, 4, 5)

Features in this user interface (UI):


- [1] : IMAP : Refresh the page.
Delete : Delete the email that is checked.
Search : Users search the particular emails based on the specified conditions such as date, time, ip, receiver, sender... etc.
- [2] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] :  : Place cursor on this icon to show recorded IP address.
- [6] :  Forward Email: To forward record to a specified email account.
- [7] :  Converter: A Converter to convert the subject's name if the subject's name is unreadable.
- [8] : Subject: Click on Email's subject to see the content or download mail record.
- [9] : Current page's information.
- [10] : First, Previous, Next and Last Page.

Search:

Users click on [Search] link to popup the following UI and search the particular Emails according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.


The screenshot shows a web browser window titled "https://192.168.1.90 - IMAP Search - Microsoft Inter...". The main content area is titled "IMAP Search" and contains several search criteria fields: "Date:" with a range from "2007-03-01" to "2007-03-27"; "Time:" with dropdown menus for hour, minute, and second; "IP:" with a text input field and a "More IP..." link; "Receiver:"; "Sender:"; "CC:"; "Subject:"; and "ID:". A "Submit" button is located at the bottom of the form.

Forward Email: 

The following UI will be popped up when click the icon . In the blank field users type the email account at where the email is forwarded.

The screenshot shows a web browser window titled "https://192.168.1.106 - E-Mail Forward - Microsoft Internet...". The main content area is titled "Forward E-Mail" and features a large text input field labeled "Forward to:". Below the field are two buttons: "OK" and "Reset".

Convertor: 

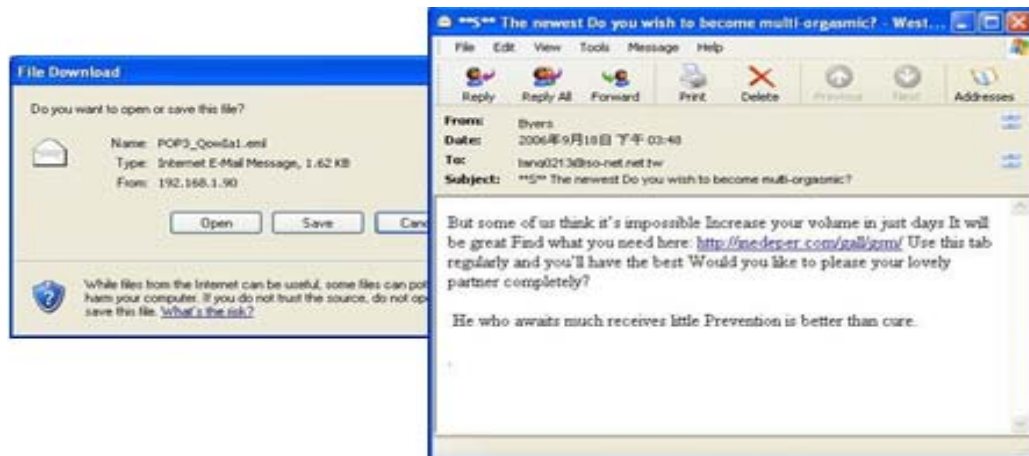
The following UI will be given if the icon  is clicked. Users use convertor to change the characters if the subject is unreadable. This convertor transfers the character in different formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).

The screenshot shows a web browser window titled "https://192.168.1.106/mail/sub_con.php?TYPE=POP3&_CHARSET=BI...". The main content area is titled "Converse Subject" and contains a "Charsets:" dropdown menu currently set to "zh-tw". Below it, the "Original" and "View" fields both display the subject line: "安全學習地墊★喜寶嬰兒食品\買1組送1罐★". A "Submit" button is located at the bottom of the form.

Copyright © 2007 Decision Computer International Co., Ltd

View Email content:

Click on Email subject, the following two UIs will be given. Users choose open button to see mail's content or save it into computer.






3. SMTP [outbound]


Simple Mail Transfer Protocol or SMTP [outbound] records the information about the Email such as the message arrival (received) time, sending time, sender, receiver, carbon copy, subject, size and attachment.

The screenshot shows an SMTP interface with a table of email records. The interface includes a toolbar at the top with buttons for SMTP, Delete, Ignore, Ignore and Delete, and Search. The table has columns for No., Date/Time, Sender, Receiver, CC, BCC, Subject, and Size. The first three rows of the table are highlighted in blue, green, and blue respectively. The bottom of the interface shows a pagination bar with page numbers 1-9 and a summary of 94 records, 32 pages, and current page 1.

No.	Date/Time	Sender	Receiver	CC	BCC	Subject	Size
1.	2007-03-27 15:29:42	lrex@decision.com.tw	chang_kan@decision.c...			Project report	16.1K
2.	2007-03-27 15:06:11	ja824@pchome.com.tw	sunny@decision.com.t...			Test Subject	307B
3.	2007-03-27 15:01:14	ja824@pchome.com.tw	sunny@decision.com.t...			Test Subject	307B

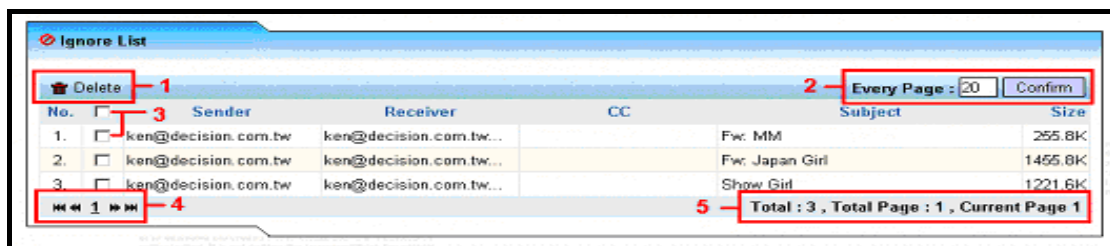
Features in this UI:

- [1] : SMTP : Refresh the page.
Delete : Delete the email that is checked.
Ignore : Ignore is to hide the email and put its information into a list if the email is checked and then click the ignore link. If there are any coming emails which are the same as the emails in the list, the system will hide these coming emails. User won't be able to see them. But system still stores these emails.
Ignore and Delete : This link is to skip any emails and put those email's information into a list when the emails are checked and click this link. ED system not only to hide the emails but also not store them if there are any coming emails which are the same as the emails in the list.
Search : Users search the particular emails based on the specified conditions such as date, time, ip, receiver, sender...etc.
- [2] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted or ignored by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] :  : Place cursor on this icon to show recorded IP address.
- [6] :  Forward Email: To forward record to a specified email account.


- [7] :  Convertor: A Convertor to convert the subject's name if the subject's name is unreadable.
- [8] : Subject: Click on Email's subject to see the content or download mail record.
- [9] : Current page's information.
- [10] : First, Previous, Next and Last Page.

Ignore & Ignore and Delete:

The following UI called ignore list will be popped up if users click either the [Ignore] link or the [Ignore and delete] link because both of these two functions have the exactly same figure of UI.



Features in this Ignore list:

- [1] : Delete : Delete the records that are checked.
- [2] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] :  Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] : First, Previous, Next and Last Page.
- [5] : Current page's information.

In terms of [Ignore] function, its list records the Email's information such as sender, receiver, cc, subject and size that the user are not interested in seeing. If there are any comings Emails which are the same as the records from this list, these coming Emails will be hidden but still be stored.

In terms of [Ignore and Delete] function, its list records the Email's information such as the sender, receiver, cc, subject and size that the users do not want to store them into the system. If there are any comings Emails which are the same as the records from this list, these coming Emails will be auto-deleted.

Search:


Users click on [Search] link to popup the following UI and search the particular Emails according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

The screenshot shows a web browser window titled "https://192.168.1.90 - SMTP Search - Microsoft Internet...". The main content area is titled "SMTP Search" and contains a search form with the following fields:

Date:	2007-03-01	~	2007-03-27
Time:	[Dropdown]	:	[Dropdown] ~ [Dropdown] : [Dropdown]
IP:	[Text Input]		More IP...
Receiver:	[Text Input]		
Sender:	[Text Input]		
CC:	[Text Input]		
BCC:	[Text Input]		
Subject:	[Text Input]		
ID:	[Text Input]		


At the bottom of the form is a "Submit" button. The browser's status bar at the bottom shows "網際網路" (Internet).

Forward Email: 

The following UI will be popped up when click the icon . In the blank field users type the email account at where the email is forwarded.

The screenshot shows a web browser window titled "https://192.168.1.106 - E-Mail Forward - Microsoft Internet...". The main content area is titled "Forward E-Mail" and contains a simple form with a "Forward to:" label and a text input field. Below the input field are two buttons: "OK" and "Reset". The browser's status bar at the bottom shows "完成" (Done) and "網際網路" (Internet).

Convertor: 

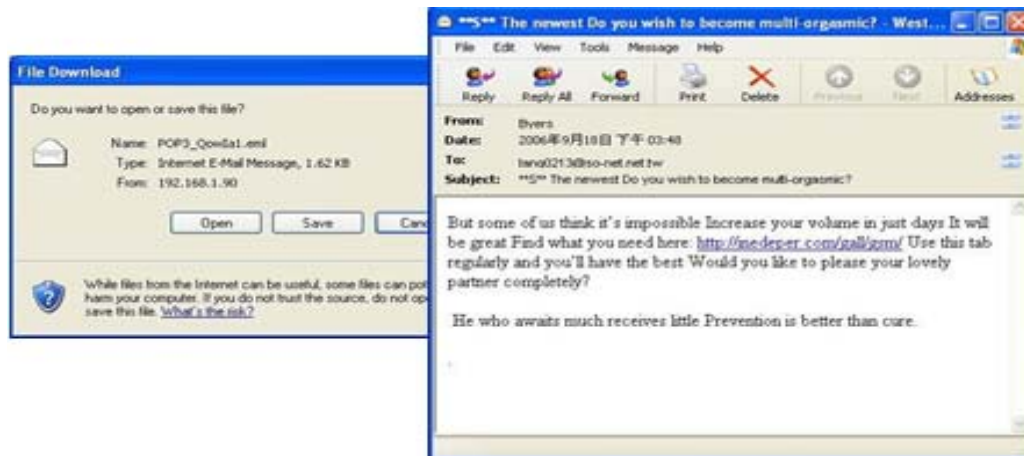
The following UI will be given if the icon  is clicked. Users use convertor to change the characters if the subject is unreadable. This convertor transfers the character in different formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).

The screenshot shows a web browser window titled "https://192.168.1.106/mail/sub_con.php?TYPE=POP3&_CHARSET=BI...". The main content area is titled "Convert Subject" and contains a form with a "Charsets:" dropdown menu, an "Original:" text input field, and a "View:" dropdown menu. The "Original:" field contains the text "安全學習地墊★喜寶嬰兒食品\買1組送1罐★". The "View:" dropdown menu is open, showing options: zh-tw, zh-ch, zh-sg, zh-hk, en, utf-8, and JP. Below the form is a "Submit" button. The browser's status bar at the bottom shows "完成" (Done) and "網際網路" (Internet).

Copyright © 2007 Decision Computer International Co., Ltd

View Email content:

Click on the link Email subject, the following two UIs will be given. Users choose open button to see mail's content or save it into computer.



3. Webmail [inbound]

E-Detective System records the webmail (Yahoo mail, Hotmail etc.) contents.

No.	<input type="checkbox"/>	Date-Time	IP	URL	Webmail Type
1.	<input type="checkbox"/>	2007-03-27 15:38:46	192.168.1.20	mail.gigigaga.com	gigigaga
2.	<input type="checkbox"/>	2007-03-27 15:38:46	192.168.1.20	mail.gigigaga.com	gigigaga
3.	<input type="checkbox"/>	2007-03-27 15:38:46	192.168.1.20	mail.gigigaga.com	gigigaga

Navigation: << 1 2 3 4 5 6 7 8 9 >>

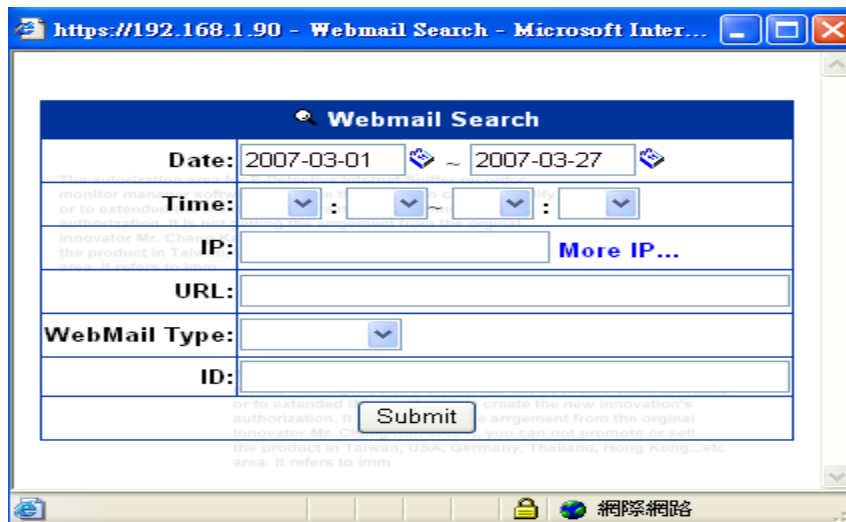
Page Info: Total 51, Total Page 17, Current Page 1

Features in this UI:


- [1] : Webmail: press to refresh
Delete: Delete the records that are checked.
Search : Users search the particular record based on the specified conditions such as dater, time, IP, URL...etc.
- [2] : Show Mode: Show the either IP or computer name for each record.
- [3] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [4] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [5] : Source code: To display the source code of webmail page.
- [6] : Forward Email: To forward record to a specified email account.
- [7] : Subject: Click on Email's subject to see the content or download mail record.
- [8] : First, Previous, Next and Last Page.
- [9] : Current page's information.

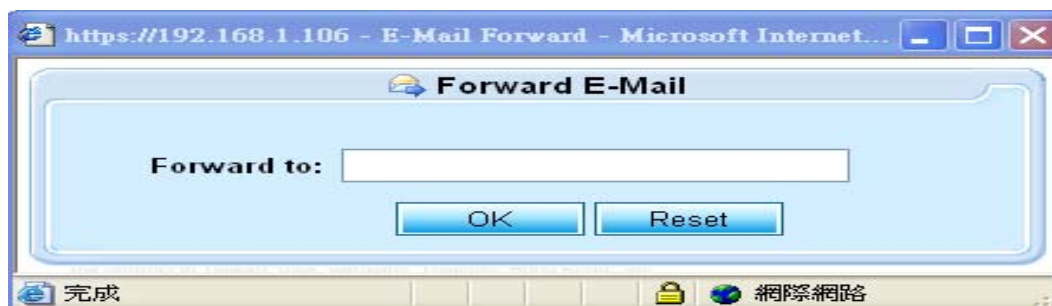
Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.



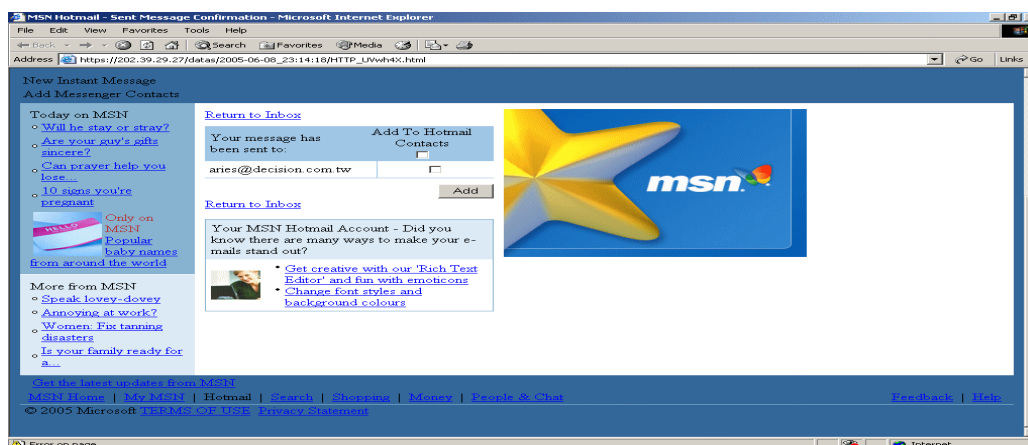
Forward Email: 

The following UI will be popped up when click the icon . In the blank field users type the email account at where the email is forwarded.



View Email content:

Click on the link [subject], the following UI will be given to view the content.








4. Webmail (Send) [outbound]

E-Detective System records the Emails' content if targets login to the webmail server (Yahoo, hotmail...etc) to send out emails.



Features in this UI:


- [1] : Webmail (Send) : Refresh the page.
Delete : Delete the email that is checked.
Search : Users search the particular emails based on the specified conditions such as date, time, ip, receiver, sender...etc.
- [2] : Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [4] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [5] :  : Place cursor on this icon to show recorded IP address.
- [6] :  Download: To download emails.
- [7] :  Forward Email: To forward record to a specified email account.
- [8] :  Converter: A Converter to convert the subject's name if the subject's name is unreadable.
- [9] : Subject: Click on Email's subject to see the content or download mail record.
- [10] : Current page's information.
- [11] : First, Previous, Next and Last Page.

Search:

Users click on [Search] link to popup the following UI and search the particular Emails according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.


Webmail (Send) Search	
Date:	2007-03-01 ~ 2007-03-27
Time:	HH:MM:SS
IP:	<input type="text"/> More IP...
Receiver:	<input type="text"/>
Sender:	<input type="text"/>
CC:	<input type="text"/>
BCC:	<input type="text"/>
Subject:	<input type="text"/>
WebMail Type:	<input type="text"/>
ID:	<input type="text"/>
<input type="button" value="Submit"/>	

Forward Email: 

The following UI will be popped up when click the icon . In the blank field users type the email account at where the email is forwarded.

Forward E-Mail	
Forward to:	<input type="text"/>
<input type="button" value="OK"/> <input type="button" value="Reset"/>	

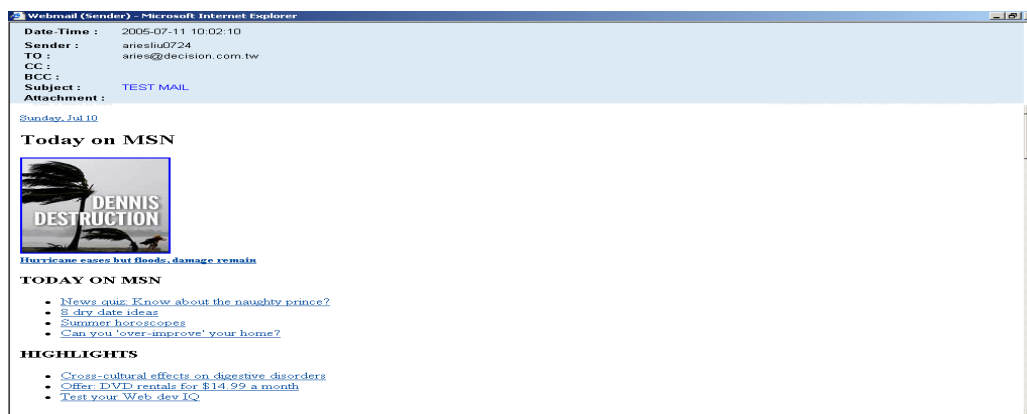
Convertor: 

The following UI will be given if the icon  is clicked. Users use convertor to change the characters if the subject is unreadable. This convertor transfers the character in different formats such as zh-ch (Chinese), zh-sg (Singapore), zh-tw (Taiwan), en (English), utf-8, JP (Japanese).



View Email content:

Click on the link called [subject] and the following UI will be given to view the content.




B. Instant Messengers (IM)

The instant messengers recording include:

1. MSN
2. ICQ / AOL
3. YAHOO
4. QQ


1. MSN

Recording MSN chatting includes relative information, like date, time, user id, IP, partner id, conversation, files transferred.



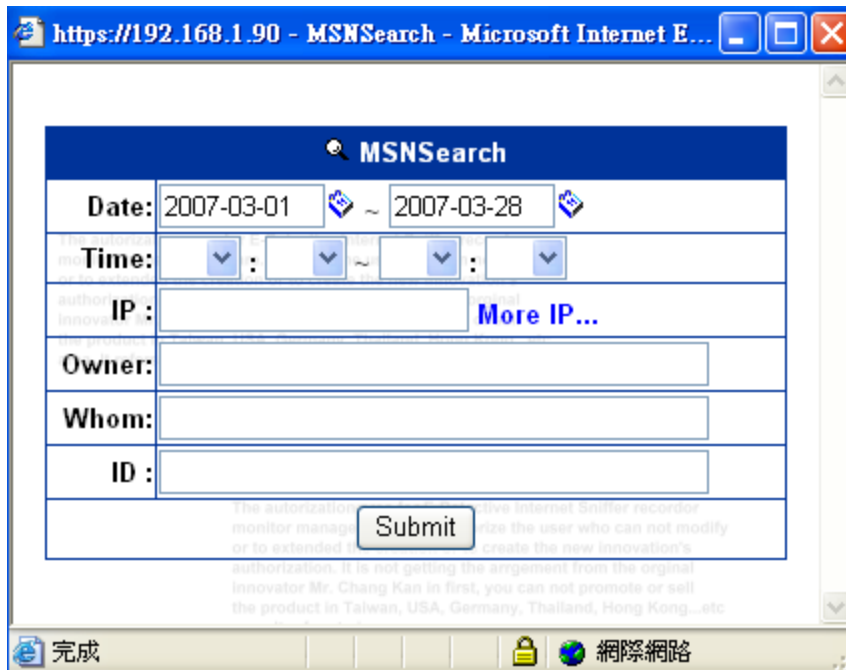
No.	<input type="checkbox"/>	Date-Time	IP	User Handle	Participants	Account	Conversation	Count
1.	<input type="checkbox"/>	2007-03-28 09:59:33	192.168.1.24	joe_3455@hotmail.com	williamchen@ms87.url.com.tw	NONE	Conversation	5 0
2.	<input type="checkbox"/>	2007-03-28 09:53:56	192.168.1.165	whoopshank@hotmail.com	karen58602045@yahoo.com.tw	NONE	Conversation	0
3.	<input type="checkbox"/>	2007-03-28 09:53:35	192.168.1.165	whoopshank@hotmail.com	joe_3455@hotmail.com	NONE	Conversation	0

Features in this UI:

- [1] : MSN : Refresh the page.
Delete : Delete the record that is checked.
Display Set: To set up whether the page is to display the information of attachment and conversation count or not.
Search : Users search the particular conversation records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] : Click on [Conversation] to view the conversation
- [6] : First, Previous, Next and Last Page.
- [7] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.



The screenshot shows a web browser window titled "https://192.168.1.90 - MSNSearch - Microsoft Internet E...". The main content area is a search form titled "MSNSearch". The form includes the following fields and controls:

- Date:** Two date pickers with values "2007-03-01" and "2007-03-28", separated by a tilde (~).
- Time:** Four dropdown menus for selecting hours, minutes, and seconds, separated by colons (:).
- IP:** A text input field with a "More IP..." link to its right.
- Owner:** A text input field.
- Whom:** A text input field.
- ID:** A text input field.
- Submit:** A button at the bottom of the form.

Below the form, there is a small block of text: "The authorization area for E-Detective Internet Sniffer recorder monitor manager authorize the user who can not modify or to extended the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc". At the bottom of the browser window, the status bar shows "完成" (Complete) and "網際網路" (Internet).

Display set:

The following UI will be given when click the link called [Display set]. The information of attachment and conversation count is shown if both of checkboxes are ticked.



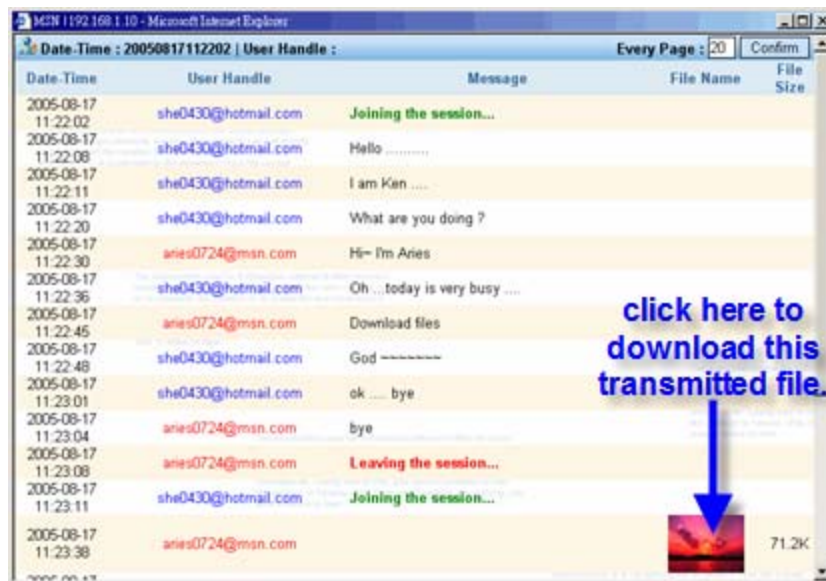
The screenshot shows a web browser window titled "https://192.168.1.90/...". The main content area displays two checkboxes, both of which are checked:

- Show Attachment** @
- Show Count**

Below these checkboxes is a "Submit" button. The same block of text from the previous screenshot is visible below the button: "The authorization area for E-Detective Internet Sniffer recorder monitor manager authorize the user who can not modify or to extended the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc". The status bar at the bottom shows "網際網路" (Internet).

MSN conversation:

Click on the link called [Conversation], the following UI will be given and then you could view the whole session of chatting and transferred files.




2. ICQ / AOL

Recording ICQ / AOL sessions includes relative information, like date, time, user id, IP, partner id, conversation, files transferred.

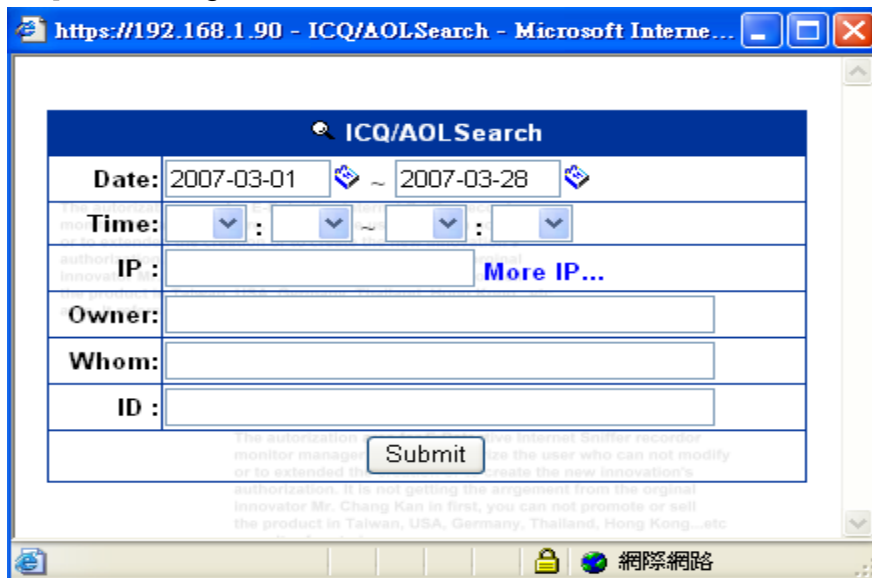
No.	<input type="checkbox"/>		Date-Time	IP	User Handle	Participants	Account	Conversation	Count
1.	<input type="checkbox"/>		2007-03-20 08:48:02	192.168.1.238	195188572	245014533	NONE	Conversation	5 6

Features in this UI:

- [1] : ICQ : Refresh the page.
Delete : Delete the record that is checked.
Search : Users search the particular conversation records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] : Click on [Conversation] to view the conversation
- [6] : First, Previous, Next and Last Page.
- [7] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.



The screenshot shows a web browser window titled "https://192.168.1.90 - ICQ/AOLSearch - Microsoft Internet Explorer". The main content area is titled "ICQ/AOLSearch" and contains a search form with the following fields:

- Date:** 2007-03-01 ~ 2007-03-28
- Time:** [Dropdown] : [Dropdown] ~ [Dropdown] : [Dropdown]
- IP:** [Text Input] [More IP...](#)
- Owner:** [Text Input]
- Whom:** [Text Input]
- ID:** [Text Input]

A "Submit" button is located below the form. Below the form, there is a small block of text: "The authorization area for E-Detective Internet Search monitor manager... authorize the user who can not modify or to extended the... create the new innovation's authorization. It is not getting the arrangement from the original innovator Mr. Chang Kan in first, you can not promote or sell the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc".

Display set:

The following UI will be given when click the link called [Display set]. The information of attachment and conversation count is shown if both of checkboxes are ticked.



The screenshot shows a web browser window titled "https://192.168.1.90/...". The main content area contains two checkboxes, both of which are checked:

- Show Attachment @
- Show Count

Below the checkboxes is a "Submit" button. Below the button, there is a small block of text: "The authorization area for E-Detective Internet Search monitor manager... authorize the user who can not modify or to extended the... create the new innovation's authorization. It is not getting the arrangement from the original innovator Mr. Chang Kan in first, you can not promote or sell the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc".

ICQ conversation:

Click on the link called [Conversation], the following UI will be given and then you could view the whole session of chatting and transferred files.

Date-Time : 2007-03-20 08:57:24 User Handle : 195188572		Every page : 100	Confirm
Date-Time	User Handle	Message	File Name
2007-03-20 08:57:24	195188572	11111	
2007-03-20 08:57:25	195188572	2222222222	
2007-03-20 08:57:26	195188572	3333333333333333	
2007-03-20 08:57:27	195188572	4444444444444	
2007-03-20 08:57:28	195188572	555555555555	
2007-03-20 08:57:31	195188572		206.5K
2007-03-20 08:57:32	195188572	<p>authorization. It is not getting the argement from the original innovator Mr. Chang Kan in first, you can not promote or sell the product in Taiwan, USA, Germany, Thailand, Hong Kong, etc area. It refers to imn</p> <p>click here to download transferred file.</p>	57.3K
2007-03-20 08:57:35	195188572		60.1K
2007-03-20 08:58:17	245014533	81	


Total 9 , Total Page 1 , Current Page 1

3. YAHOO

Recording Yahoo messenger chatting includes relative information like date, time, user id, IP, partner id, conversation, transferred files and video conference.

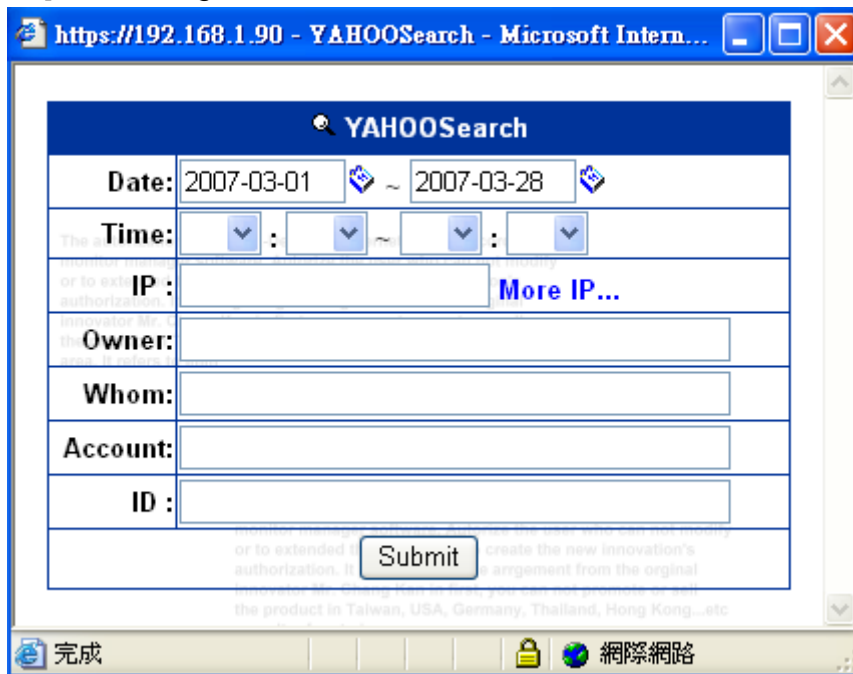
No.	<input type="checkbox"/>	Date-Time	IP	User Handle	Participants	Account	Conversation	Count
1.	<input type="checkbox"/>	2007-03-20 08:48:57	192.168.1.238	raulraul6	superuserdemo	NONE	Conversation	1

Features in this UI:

- [1] : YAHOO : Refresh the page.
Delete : Delete the record that is checked.
Search : Users search the particular conversation records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] : Click on [Conversation] to view the conversation.
- [6] : First, Previous, Next and Last Page.
- [7] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.



The screenshot shows a web browser window titled "https://192.168.1.90 - YAHOOsearch - Microsoft Intern...". The main content area is a search form with the following fields and options:

- Date:** 2007-03-01 ~ 2007-03-28
- Time:** Two dropdown menus for hour and minute, separated by a colon and a tilde (~), followed by another two dropdown menus for hour and minute.
- IP:** A text input field with a "More IP..." link to its right.
- Owner:** A text input field.
- Whom:** A text input field.
- Account:** A text input field.
- ID:** A text input field.

A "Submit" button is located at the bottom of the form. The browser's taskbar at the bottom shows the "完成" (Done) button, a lock icon, and the text "網際網路" (Internet).

Display set:

The following UI will be given when click the link called [Display set]. The information of attachment and conversation count is shown if both of checkboxes are ticked.



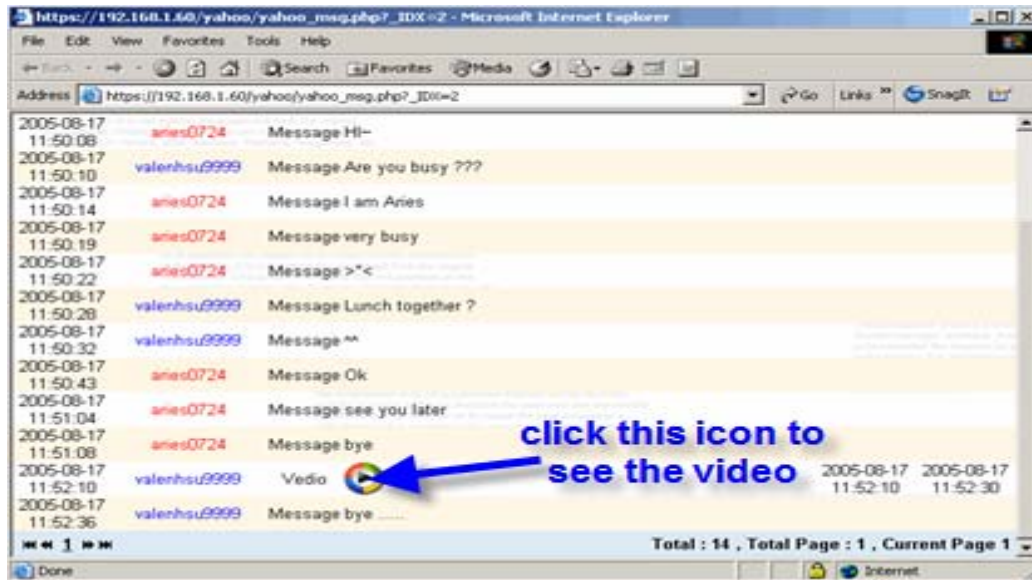
The screenshot shows a web browser window titled "https://192.168.1.90/...". The main content area contains two checkboxes, both of which are checked:

- Show Attachment @
- Show Count

Below the checkboxes is a "Submit" button. The browser's taskbar at the bottom shows a lock icon and the text "網際網路" (Internet).

YAHOO Conversation & Video Conference:

Click on the link called [Conversation], the following UI will be given and then you could view the whole session of chatting and files transferred or video conference.




4. QQ

QQ records date, time, users handle and IP address, participant handle and conversation content.

No.	<input type="checkbox"/>	4	Date-Time	IP	User Handle	Participants	Account	Conversation	Count
1.	<input type="checkbox"/>		2007-03-20 10:25:25	192.168.1.10	572670102	NULL	NONE	5 - Conversation	212
2.	<input type="checkbox"/>		2007-03-16 14:43:23	192.168.1.10	572670102	NULL	NONE	Conversation	38

Features in this UI:

- [1] : QQ : Refresh the page.
Delete : Delete the record that is checked.
Information: Link to downlad QQ cracker to decrypt records.
Search : Users search the particular conversation records based on the specified condtions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confim button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] :  Attachment: There will be a symbol appeared if there is more than one attachments included.
- [5] : Click on [Conversation] to view the conversation.
- [6] : First, Previous, Next and Last Page.
- [7] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

https://192.168.1.90 - QQSearch - Microsoft Internet Ex...

QQSearch

Date: 2007-03-01 ~ 2007-03-30

Time: : : ~ : :

IP: More IP...

Owner:

Whom:

ID :

Submit

The authorization area for E-Detective Internet Sniffer recorder monitor manager authorize the user who can not modify or to extended the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc

Display set:

The following UI will be given when click the link called [Display set]. The information of attachment and conversation count is shown if both of checkboxes are ticked.

https://192.168.1.90/...

Show Attachment @

Show Count

Submit

The authorization area for E-Detective Internet Sniffer recorder monitor manager authorize the user who can not modify or to extended the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc

Information- How to see the encrypted conversation:

The captured conversation in QQ will be all encrypted. This section tells users how to download the QQ cracker to decrypt the information.

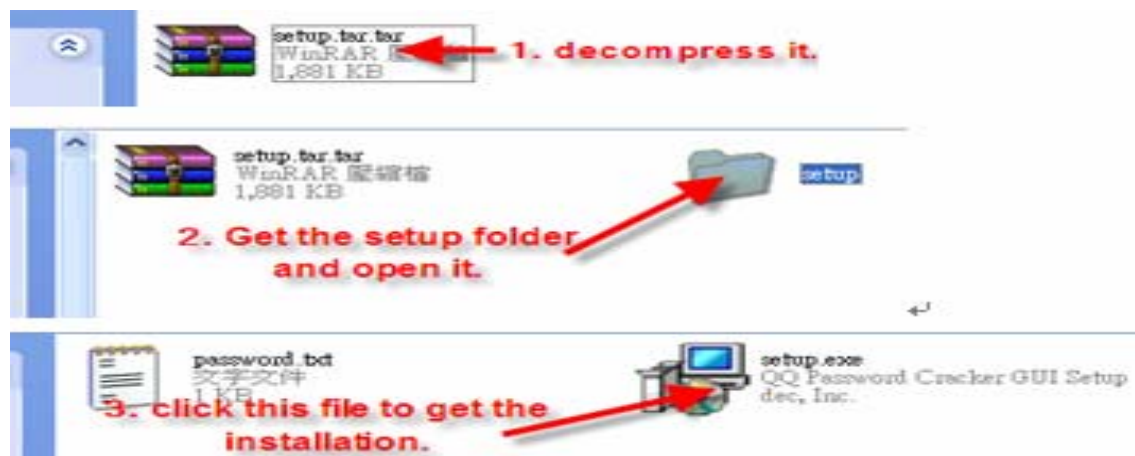
Step 1 – Download the QQ cracker:

The following diagram shows the steps to download the QQ cracker.

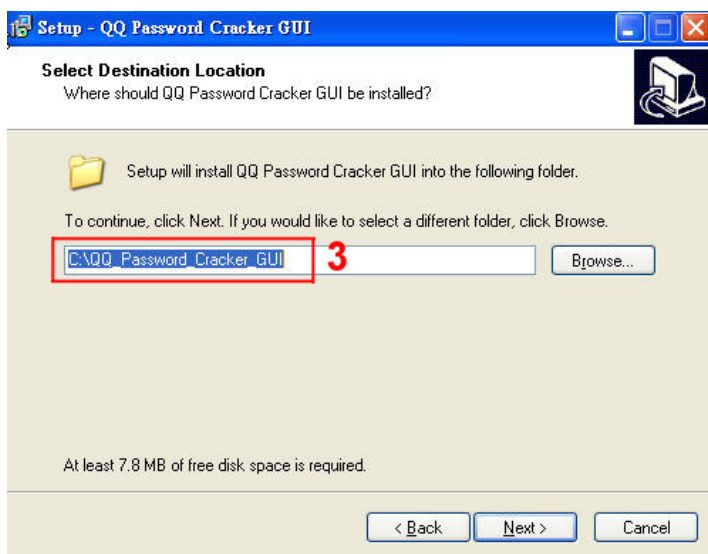
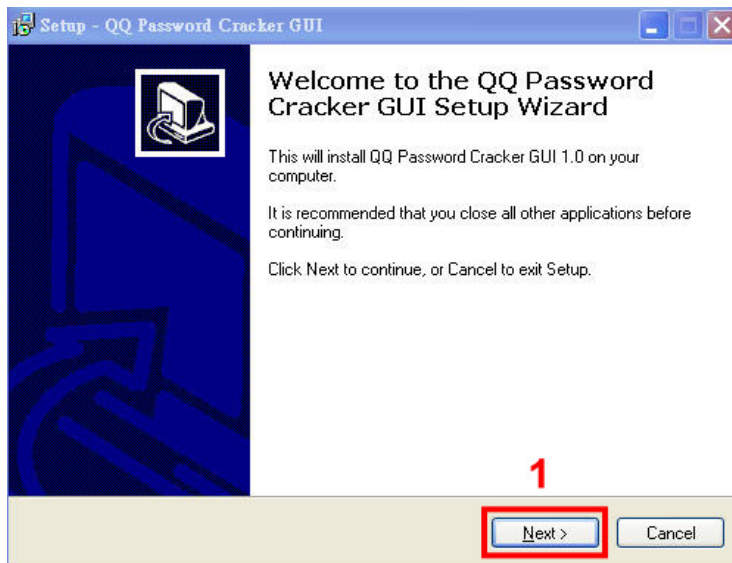


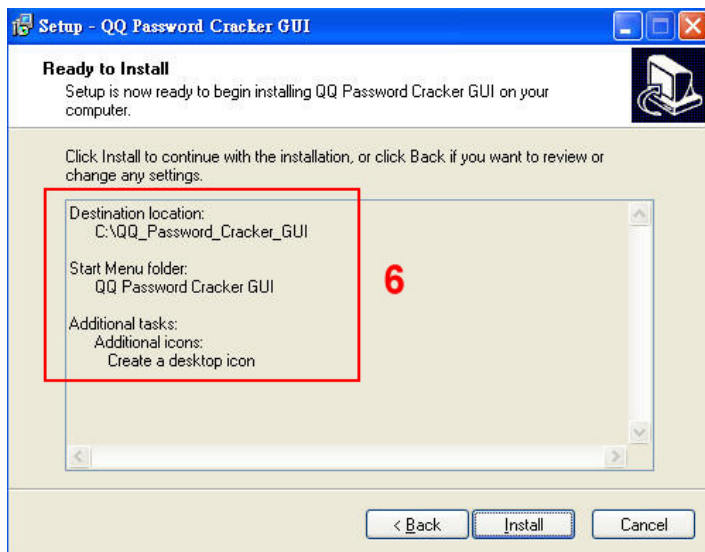
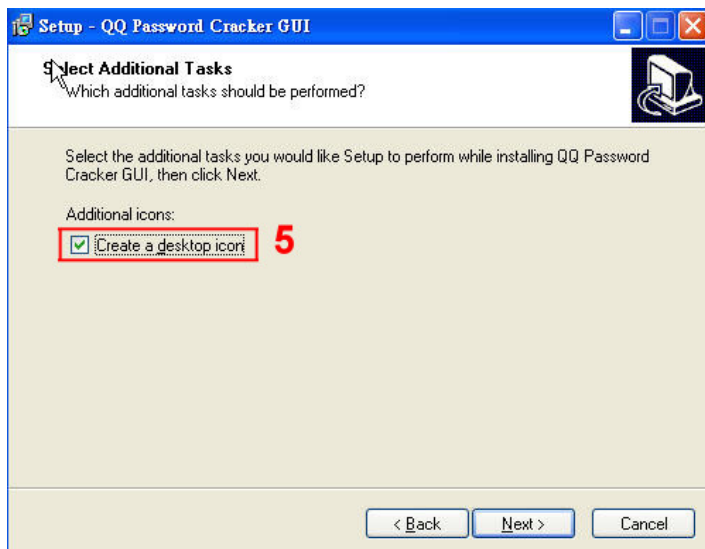
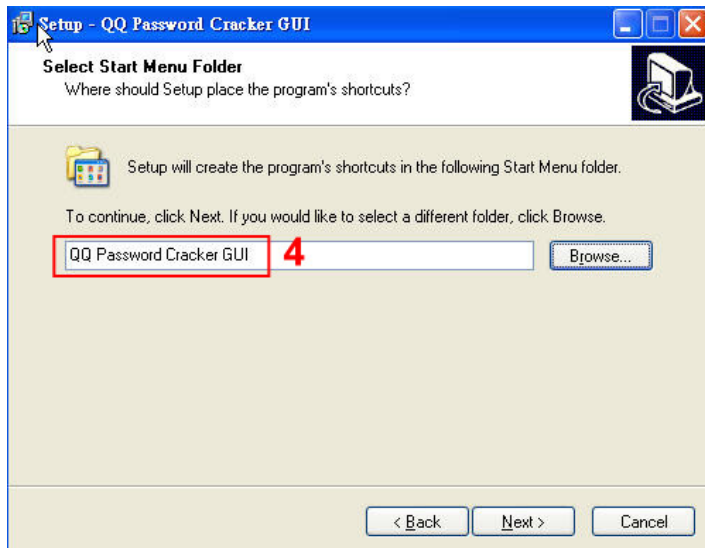
Step 2 – Install QQ cracker into computer.

Decompress the file called “setup.tar.tar” to get the folder called “setup”. Open it and press the setup.exe to get the installation.



The following diagrams show the steps of installation.

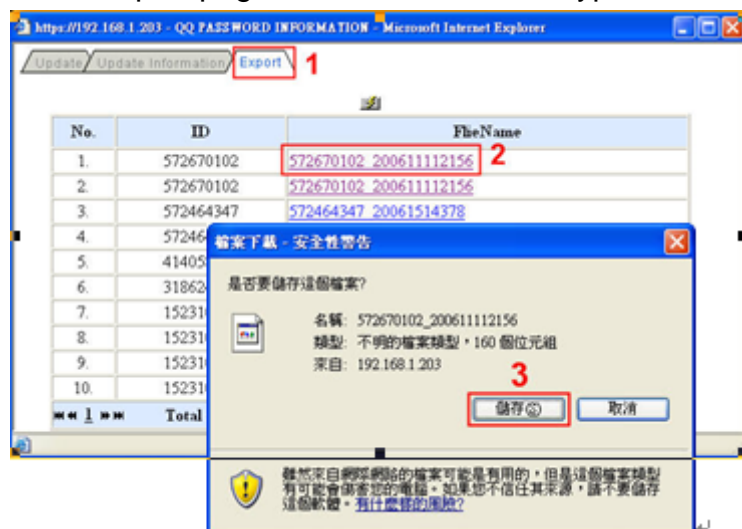




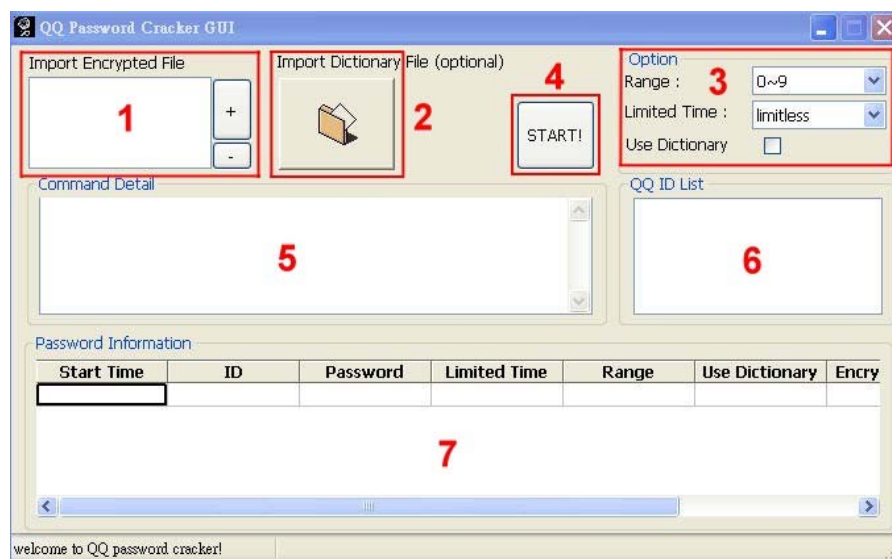


Step 3 – Decrypt the conversation.

Go to Export page to download the decrypted conversation file.



Run the QQ cracker and import the decrypted file you just download at the previous step.

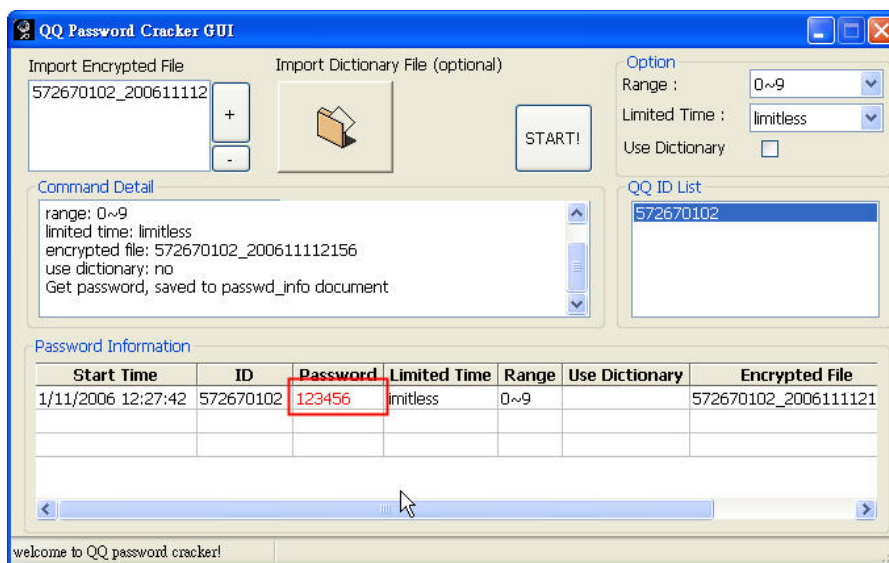


Item	statement
1	Import Encrypted File Choose + or - button, add or remove to run files.
2	Import Dictionary File Dictionary file records the general passwords which people may use. If you have own dictionary file, you can import it into this cracker when you decrypt the conversation.
3	Option Range – Setup the possible combinations of password. Limited Time – Setup the max time to get the key.

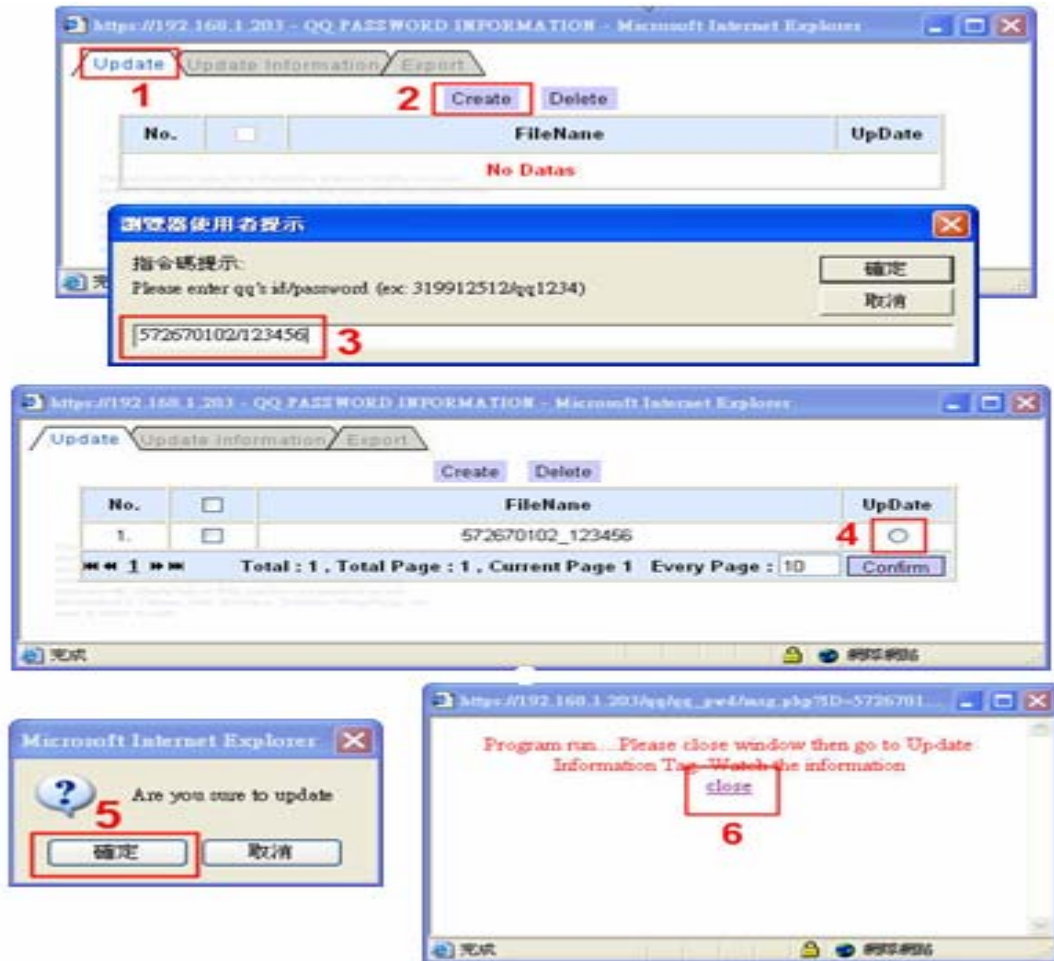
Copyright © 2007 Decision Computer International Co., Ltd

		Even if this cracker does not still get the password for you, the process will be stopped when time is out. Use Dictionary – Cracker uses the dictionary's information to do the password matching if the checkbox is ticked.
4	START	Start to run program button.
5	Command Detail	Show procedure for detailed information.
6	QQ ID List	Shows the history of QQ ID records.
7	Password Information	Shows the findings if password is found.

Get the password as shown in the following diagram.



The section illustrates how to decrypt the decrypted file in order to see its conversation with the following diagrams.



And then you can actually be able to see the conversation content.



The update page shows the decrypting procedures.

The screenshot shows a web browser window with the address bar displaying 'https://192.168.1.203 - QQ PASSWORD INFORMATION - Microsoft Internet Explorer'. The page has three tabs: 'Update', 'Update Information', and 'Export'. A table with three columns: 'No.', 'Date-Time', and 'Mssege' is displayed. The table contains five rows of data. A red box highlights the 'Update Information' tab and the table. A red arrow points to the 'Update Information' tab. At the bottom of the table, there is a 'Confirm' button. The browser's status bar shows '完成' and '網際網路'.

No.	Date-Time	Mssege
1	2006-01-16 10:26:42	Account: 572670102Password: 123456
2	2006-01-16 10:26:42	==Program start==
3	2006-01-16 10:26:42	Start decrypt login data
4	2006-01-16 10:26:42	get password key: 4280d89a5a03f812751f504cc10ee8a5
5	2006-01-16 10:26:42	decrypting [16][/datas/2006-01-06_19:03:17/572670102_200611112156]..... Success !!!!!!!

« 1 2 3 » Total: 14, Total Page: 3, Current Page: 1, Every Page: 5 Confirm

C. File Transfer

1. FTP

FTP records date, time, user IP, user ID, Password, and transferred files.

No.	Date-Time	IP	User	Pass	Action	FTP Server IP	File Name
1	2005-10-20 16:33:54	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
2	2005-10-20 16:32:17	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
3	2005-10-20 16:32:17	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
4	2005-10-20 16:30:26	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
5	2005-10-20 16:30:16	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
6	2005-10-20 16:29:47	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
7	2005-10-20 16:27:14	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
8	2005-10-20 16:27:05	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
9	2005-10-20 16:26:44	192.168.1.10	decision	*****	Download	192.168.1.249	index05.gif
10	2005-10-20 16:20:51	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php
11	2005-10-20 16:20:28	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php
12	2005-10-20 16:20:17	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php
13	2005-10-20 16:19:52	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php
14	2005-10-20 16:19:11	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php
15	2005-10-20 14:03:32	192.168.1.33	user	*****	Upload	192.168.1.93	requestion.php

Features in this UI:

- [1] : FTP : Refresh the page.
Delete : Delete the record that is checked.
Show Pass: Setup whether display password or not.
Search : Users search the particular records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be checked respectively or checked all by clicking the 1st one.
- [4] : FTP password.
- [5] : Click on the file name to download.
- [6] : First, Previous, Next and Last Page.
- [7] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

FTP Search	
Date :	2005-08-01 ~ 2005-08-17
Time :	: : ~ : : :
IP :	<input type="text"/> more...
User :	<input type="text"/>
Action :	<input type="text"/>
FTP Server IP :	<input type="text"/>
File Name :	<input type="text"/>
ID :	<input type="text"/>
<input type="button" value="Submit"/>	

2. P2P

Peer to Peer (P2P), two computers are directly connected for transmitting the data without going through anyone else.

The screenshot shows a web-based interface for monitoring P2P traffic. At the top, there is a navigation bar with a 'P2P' logo, a 'Delete' button, and a search field. Below this is a table with columns for 'No.', 'Date-Time', 'IP', 'Port', 'P-IP', 'P-Port', 'Tool', 'File name', and 'Action'. The table contains four rows of data, each representing a P2P connection. At the bottom of the interface, there is a footer with navigation links and summary statistics.

No.	Date-Time	IP	Port	P-IP	P-Port	Tool	File name	Action
1	2007-03-30 14:42:58	192.168.1.24	3041	59.115.197.204	19763	Foxy 1.9.0.0	老天爷给我爱73.mmb	Download
2	2007-03-30 14:42:57	192.168.1.24	3040	61.224.143.159	10690	Foxy 1.9.0.0	老天爷给我爱73.mmb	Download
3	2007-03-30 14:42:32	192.168.1.24	3023	220.143.35.3	7504	Foxy 1.9.0.0	75-老天爷给我爱.mmb	Download
4	2007-03-30 14:42:05	192.168.1.24	2965	122.127.68.22	6575	Foxy 1.9.0.0	老天爷给我爱73.mmb	Download

Features in this UI:

- [1] : P2P : Refresh the page.
Delete : Delete the record that is checked.
Search : Users search the particular records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be ticked respectively or checked all by clicking the 1st one.
- [4] : IP: The target's IP at where you capture the data from.
- [5] : Port: Display what port number the target use to transfer data.
- [6] : P-IP: The IP address where the target transfers the data to.
- [7] : P-Port: Shows what port number used by second party.
- [8] : Tool: Shows what tool the targets use to transfer the data.
- [9] : File name: Show the transmitted file name.
- [10] : directory
- [11] : Click on the file name to download.
- [12] : First, Previous, Next and Last Page.
- [13] : Current page's information.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

The screenshot shows a web browser window titled "https://192.168.1.90 - P2P Search - Microsoft Intern...". The main content area is a form titled "P2P Search" with a search icon. The form contains the following fields and controls:

- Date:** Two date pickers showing "2007-03-01" and "2007-03-30" with a tilde (~) between them.
- Time:** Four dropdown menus for hour, minute, second, and AM/PM, with a tilde (~) between the first two.
- IP:** A text input field with a "More IP..." link to its right.
- Port:** A text input field.
- P-IP:** A text input field.
- P-Port:** A text input field with a "record" and "not modify" label to its right.
- Tool:** A dropdown menu with a tilde (~) to its right.
- File Name:** A text input field with a "hang" label to its right.
- Action:** A dropdown menu.
- ID:** A text input field.

At the bottom of the form is a "Submit" button. The browser's status bar at the bottom shows "完成" (Completed) and "網際網路" (Internet).

D. WEBSITE

When targets surf websites, E-Detective system will record those addresses (URLs) and contents.

1. HTTP

HTTP records date, time, user IP /user name, URL. Content is retrieved by clicking on the hyperlink (URL) to access the website on internet.



No.	Date-Time	IP	URL
1.	2005-10-20 17:01:50	192.168.1.22	m5.mail2000.com.tw - 4
2.	2005-10-20 17:01:46	192.168.1.22	m5.mail2000.com.tw
3.	2005-10-20 17:01:40	192.168.1.22	m5.mail2000.com.tw
4.	2005-10-20 17:00:39	192.168.1.22	zfmir.nease.net
5.	2005-10-20 17:00:39	192.168.1.22	zfmir.nease.net
6.	2005-10-20 17:01:20	192.168.1.22	m5.mail2000.com.tw
7.	2005-10-20 17:00:59	192.168.1.50	www.mxie.com
8.	2005-10-20 16:58:55	192.168.1.21	storage.msn.com
9.	2005-10-20 16:58:12	192.168.1.22	gserver.eneas.com.tw
10.	2005-10-20 16:58:12	192.168.1.22	gserver.eneas.com.tw
11.	2005-10-20 16:58:12	192.168.1.22	gserver.eneas.com.tw
12.	2005-10-20 16:59:39	192.168.1.22	zfmir.nease.net
13.	2005-10-20 16:59:39	192.168.1.22	zfmir.nease.net
14.	2005-10-20 17:00:35	192.168.1.22	m5.mail2000.com.tw
15.	2005-10-20 17:00:30	192.168.1.50	mail.opi.yahoo.com

Features in this UI:

- [1] : HTTP: Refresh this page.
Delete: Delete the record that is ticked.
Search : Users search the particular records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be ticked respectively or checked all by clicking the 1st one.
- [4] : Click on [URL] to access the web site
- [5] : First, Previous, Next, Last page
- [6] : Current page information

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.


The screenshot shows a web browser window titled "HTTP - Microsoft Internet Explorer". The main content area displays a search form titled "HTTP Search". The form includes several input fields: "Date" with a range from "2005-08-01" to "2005-08-17", "Time" with four dropdown menus for hour, minute, and second, "IP" with a text box and a "more..." link, "URL" with a text box, and "ID" with a text box. A "Submit" button is located at the bottom of the form. Below the form, there is a small, faint copyright notice: "The automatic... Microsoft Internet Explorer recorder... monitor manager software. Authorize the user who can not modify or to extended the creation or to create the new Innovation's".

2. Web Page [URL Content]

E-Detective System records original contents of the webpage such as javascript, pictures. Those original contents were surfed by targets at that time.

No.	Date-Time	IP	URL
1.	2005-10-20 17:06:40	192.168.1.22	210.200.181.213
2.	2005-10-20 17:06:38	192.168.1.24	202.43.196.230
3.	2005-10-20 17:05:28	192.168.1.24	203.112.80.102
4.	2005-10-20 17:06:29	192.168.1.22	210.200.181.213
5.	2005-10-20 17:06:28	192.168.1.22	210.200.181.213
6.	2005-10-20 17:06:20	192.168.1.22	210.200.181.213
7.	2005-10-20 17:06:08	192.168.1.22	210.200.181.213
8.	2005-10-20 17:06:06	192.168.1.22	210.200.181.213
9.	2005-10-20 17:06:04	192.168.1.22	210.200.181.213
10.	2005-10-20 17:06:03	192.168.1.14	202.43.196.52
11.	2005-10-20 17:04:55	192.168.1.22	220.163.176.214
12.	2005-10-20 17:05:39	192.168.1.50	207.68.178.16
13.	2005-10-20 17:05:38	192.168.1.50	207.68.178.16
14.	2005-10-20 17:05:50	192.168.1.22	210.200.181.213
15.	2005-10-20 17:05:47	192.168.1.22	210.200.181.213

Features in this page:

- [1] : URL Content: press to refresh.
Delete: Delete record which is ticked.
Search : Users search the particular records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be ticked respectively or checked all by clicking the 1st one.
- [4] :  : Click on the red icon to view the source codes
- [5] : Click on [URL] to view the page
- [6] : First, Previous, Next, Last page
- [7] : Current page information

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

URL Content Search	
Date :	2005-08-01 ~ 2005-08-17
Time :	: : ~ : : :
IP :	<input type="text"/> more...
URL :	<input type="text"/>
ID :	<input type="text"/>
<input type="button" value="Submit"/>	

Source code:

The following UI will be popped up to show the source code of webpage.

```
<script language="JavaScript">
//
var pathString;
var MSAAdsEmbed=0, MSAAdsUseFlash=0, MSNAdsBGColor="#FFFFFF",
MSNAdsMENU="FALSE", MSNAdsWIDTH=234, MSNAdsHEIGHT=60;

function dlWrite_762226() {document.write('&lt;a target="_blank"
href="http://g.msn.com/0AD0001V/762226.2??
PID=2660571&amp;UUI=A&amp;TargetID=1058095&amp;AN=573572015&amp;PG=IMST
src="http://global.msads.net/ads/10867/0000010867_0000000000000000198396.jpg" width=234
height=60 border="0" alt="Click&amp;#32;here&amp;#33;" /&gt;&lt;/a&gt;');}
var g_bShowFlash=false;
if (navigator.appVersion.indexOf("Win")&gt;=0 &amp;&amp; parseFloat(navigator.appVersion.substr
(navigator.appVersion.indexOf("MSIE")+5))&gt;=4) {document.write('&lt;SCR' + 'IPT
LANGUAGE=VBScript&gt; \n');document.write('on error resume next \n');document.write
('g_bShowFlash = ( IsObject(CreateObject("ShockwaveFlash.ShockwaveFlash.4"))
\n');document.write('&lt;/SCR' + 'IPT&gt;');}
if(g_bShowFlash == true)</pre></div><div data-bbox="145 908 621 926" data-label="Page-Footer"><p>Copyright © 2007 Decision Computer International Co., Ltd</p></div><div data-bbox="492 936 517 952" data-label="Page-Footer"><p>50</p></div>
```

E. Telnet

E-Detective System records the browsing process from stem to stern when targets go online via Telnet.

1. Telnet

Telnet function records date, time, User IP, and Telnet Server IP. Click on it then the session information will be displayed.



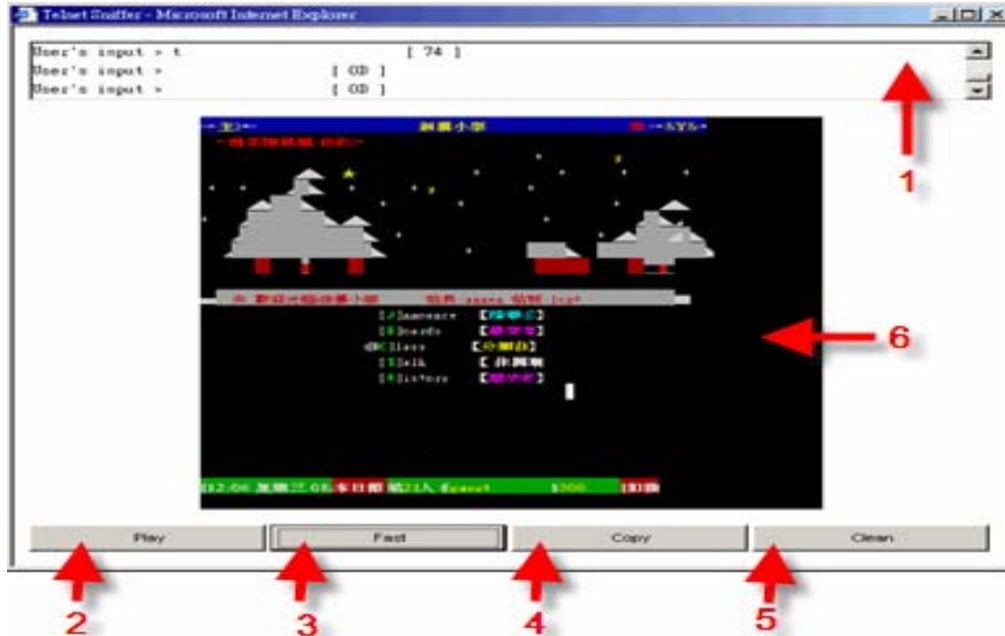
No.	Date-Time	IP	User	Pass	Server	Record File	Size
1.	2005-10-18 19:53:16	192.168.1.245			59.104.212.56	Record File	83B
2.	2005-10-18 17:09:38	192.168.1.245			59.104.212.56	Record File	83B
3.	2005-10-18 13:18:03	192.168.1.20			140.131.7.3	Record File	11.2K
4.	2005-10-18 06:34:46	192.168.1.245			59.104.212.204	Record File	83B
5.	2005-10-18 03:34:45	192.168.1.245			59.104.212.204	Record File	83B
6.	2005-10-18 01:13:42	192.168.1.245			59.104.212.204	Record File	83B
7.	2005-10-17 23:12:47	192.168.1.245			59.104.212.204	Record File	83B
8.	2005-10-17 21:34:29	192.168.1.245			59.104.212.204	Record File	83B
9.	2005-10-17 20:11:08	192.168.1.245			59.104.212.204	Record File	83B
10.	2005-10-17 16:04:34	192.168.1.245			211.74.187.98	Record File	104.4K
11.	2005-10-17 14:34:45	192.168.1.245			211.74.187.98	Record File	61.9K
12.	2005-10-17 13:28:38	192.168.1.245			211.74.187.98	Record File	83B
13.	2005-10-15 16:14:59	192.168.1.45			140.117.11.2	Record File	2.1K
14.	2005-10-15 16:08:05	192.168.1.24			140.112.18.32	Record File	142.6K
15.	2005-10-15 15:40:15	192.168.1.24			140.112.18.32	Record File	107.6K

Features in this page:

- [1] : TELNET: press to refresh
Delete: Delete the record that is checked.
Search : Users search the particular records based on the specified conditions such as date, time, ip...etc.
- [2] : Show Mode: To display either IP or computer name on this UI.
Every Page: It is to display how many records per page. Users input the number and press the confirm button to set up.
- [3] : Checkbox: Records could be deleted by checking the checkbox. The checkboxes could be ticked respectively or checked all by clicking the 1st one.
- [4] : Click on [Record File] to view the session of Telnet or BBS
- [5] : First, Previous, Next, Last page
- [6] : Current page information.

View the browsing process:

The following UI will be popped up when users click the link [Record File]. This UI acts as a video player. Users can view the browsing process from stem to stern by press



Features in this page:

- [1] : This field on the top of this UI is to show the user's input.
- [2] : Play: To show the information once a character.
- [3] : Fast: To show the information once a line.
- [4] : Copy: To copy the information selected on the top field.
- [5] : Clean: To clear up the information on the black screen.
- [6] : Black screen: Information displayed on this screen.

Search:

Users click on [Search] link to popup the following UI and search the particular record according to the conditions such as the Date, Time, and IP....etc. Press the [Submit] button to get the wanted records.

The screenshot shows a web browser window titled 'Telnet Search - Microsoft Internet Explorer'. The main content area is a form titled 'Telnet Search'. The form has four input fields: 'Date' with a date range from '2005-08-01' to '2005-08-17', 'Time' with dropdown menus for hour, minute, and second, 'IP' with a text input field and a 'more...' link, and 'ID' with a text input field. Below the form is a 'Submit' button.

F. SETTING

1. Network Set

The screenshot displays three configuration panels for network settings:

- NETWORK SET - DEVICE SET:** Features a table with columns for DEVICE, MODE, CAPTURE, and STATUS. A 'SetIP' button is located above the table.
- Network Set - DNS Set:** Includes a table with columns for Configuration, Default, and New Set. It has a 'Reset' button.
- Network Set - System Set:** Contains system action buttons (Shut Down, Reboot), current system time (2006-09-18 11:31:40), server time selection (Year, Month, Day, Hour, Minute), and time zone selection (+8).

DEVICE	MODE	CAPTURE	STATUS
eth0	MANAGE	C	192.168.1.69 255.255.255.0 192.168.1.255 192.168.1.1
eth1	-	-	
eth2	-	-	

Configuration	Default	New Set
Primary	168.95.1.1	
Second		

System Action : Shut Down Reboot
Current System Time : 2006-09-18 11:31:40
Server Time : 2006 09 18 11 30 Setup
Correct Time Zone : +8 Setup

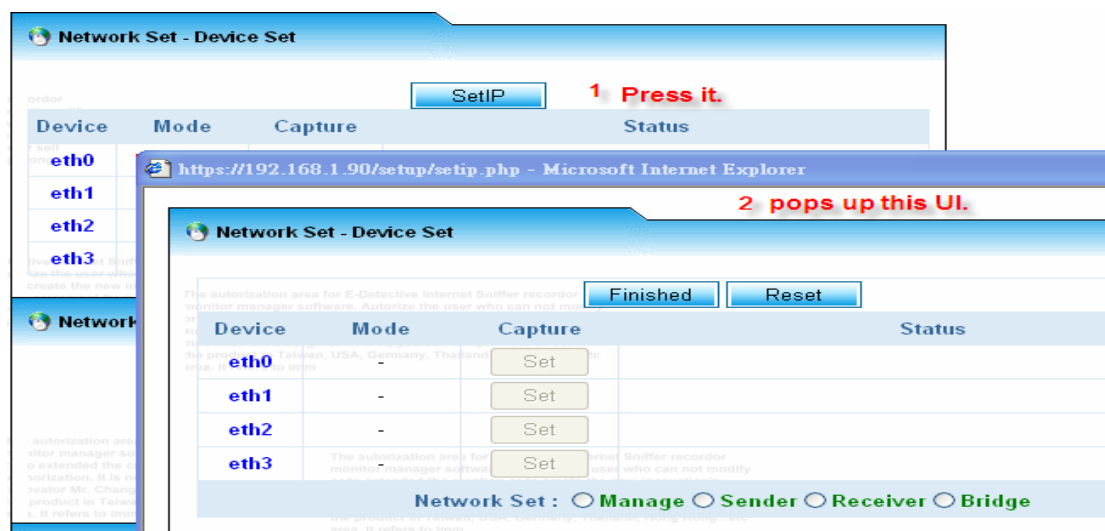
Features in this page:

- Device Set: Setup the system operation mode. The next section will give more detail what those operation modes are and how to setup the operation mode properly.
- DNS Set: Setup the DNS IP. The IP can be obtained from your ISP providers.
- System Set: Adjusting the system time.

Device Sets:

This section introduces what the system operation modes the user may choose to set up for your ED system and gives an instruction in how to set up those operation modes step by step.

The following UI will be popped up once pressing the button [SetIP].



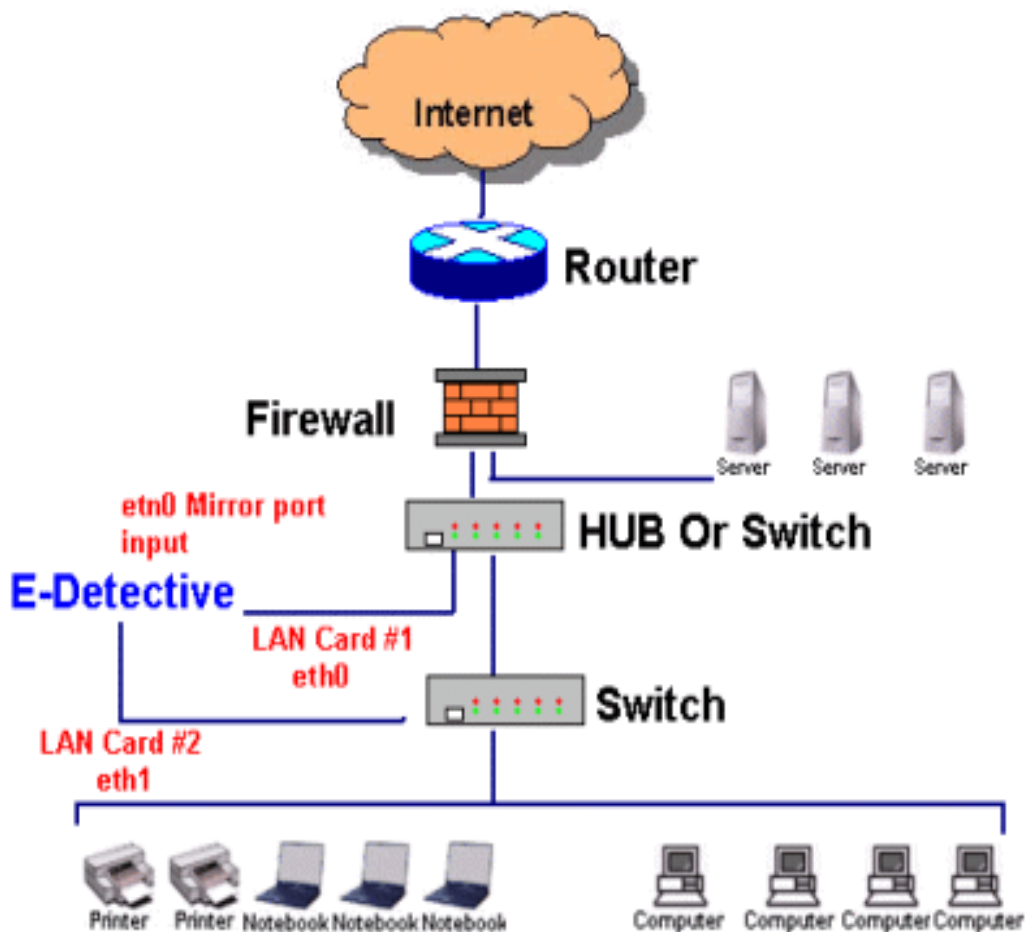
Simply says in the ED system's behaviors, there are basically two behaviours happened during the operation. One is to capture the data from targets; another is to manage/analyse the data captured. These two behaviours can be operated together in only one NIC card or separately operated in the different NIC cards.

There are mainly 4 modes of operation for E-Detective which include the following:

- [1] : Mirror Mode:
- [2] : Sniffer Mode:
- [3] : Bridge Mode:
- [4] : Sender/Receiver Mode:

Mirror Mode:

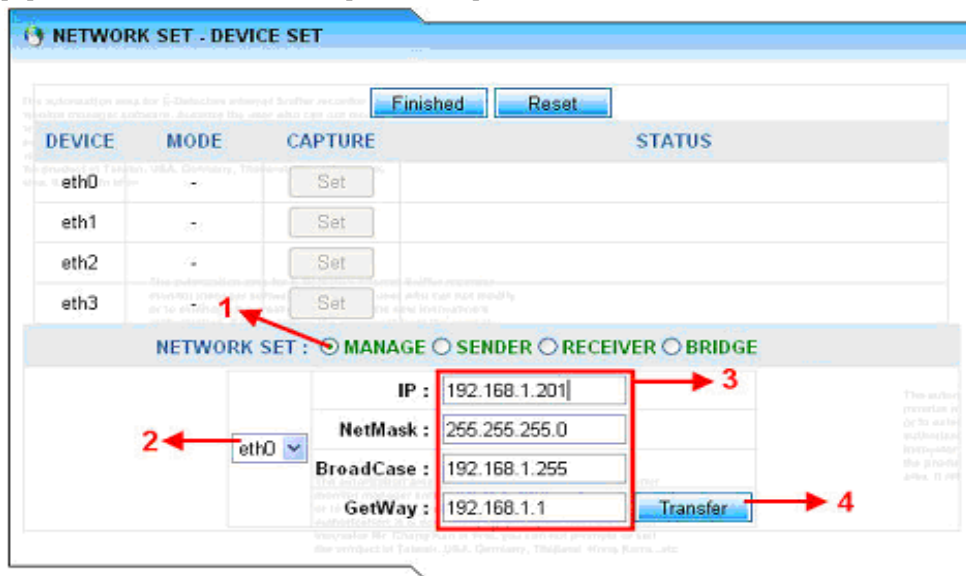
In terms of Mirror Mode, it uses two NIC cards to operate, one is for capturing the data, and another is for managing the data. The following diagram shows the concept of how this mode is operated. The number 1 NIC card on the port called "eth0" is connected to the top HUB/Switch to capture the data. The number 2 NIC card on the port called "eth1" can be randomly connected to top/sub Hub/Switch.



This section illustrates the way of how to set up the Mirror Mode with the following diagrams step by step:

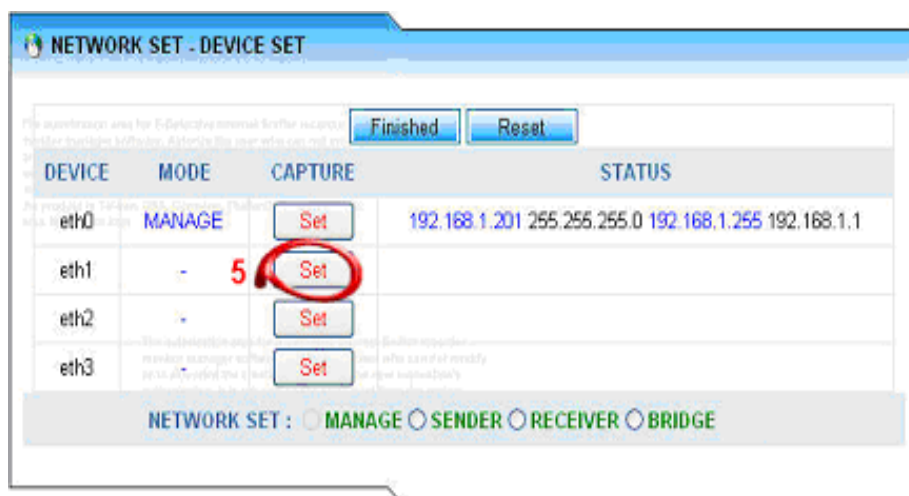
Step 1: Management Setup.

- [1] : Ticking the option “MANAGE”
- [2] : Selecting the NIC card called “eth0”.
- [3] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [4] : Press the button [Transfer] to submit.



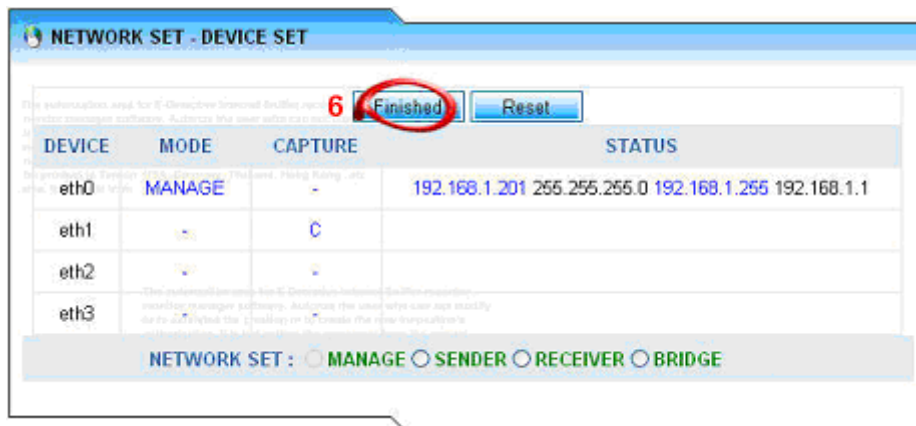
Set2: Capture Setup.

- [5] : Pressing the button [Set] on Device eth1 or eth2 or eth3. To set up which NIC card is to capture the data.



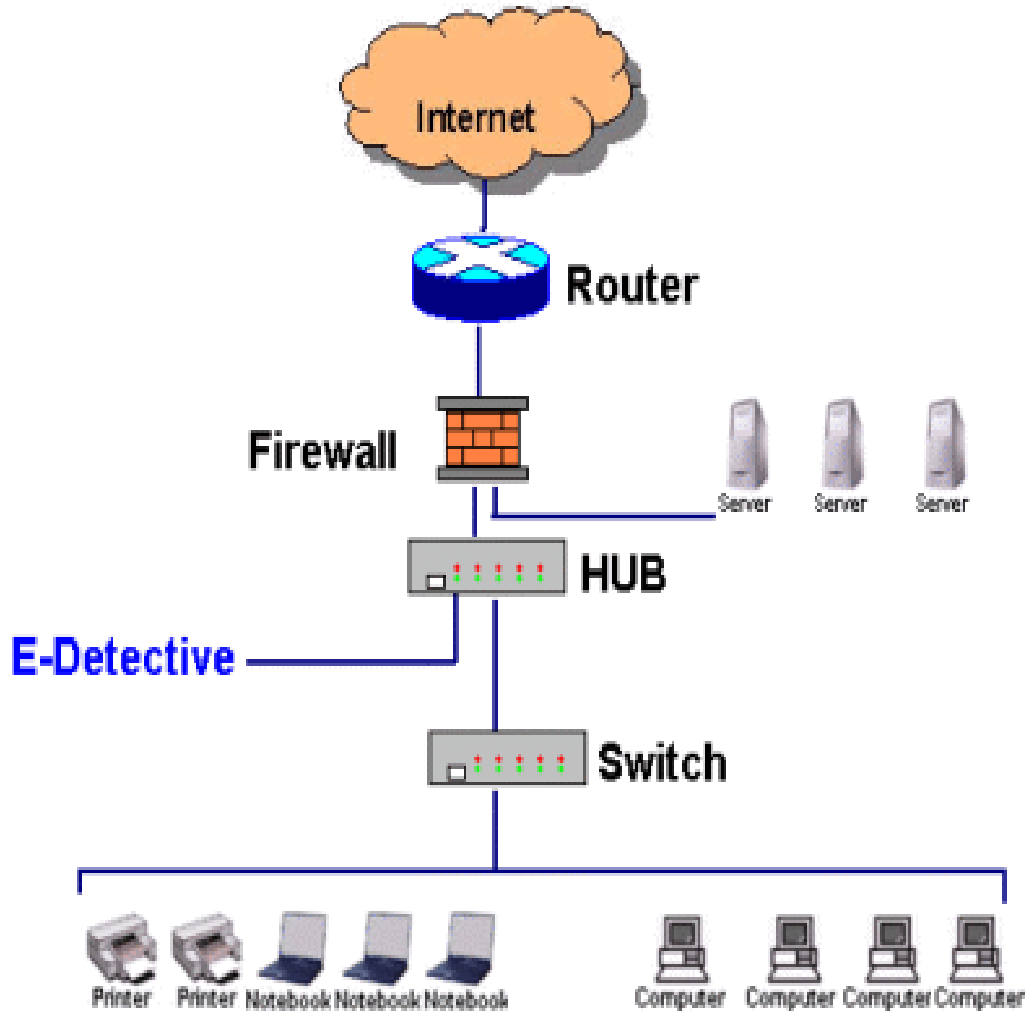
Set3: Finish Setup:

[6] : Pressing the button [Finished], the system will reboot and setup mirror mode for you.



Sniffer Mode:

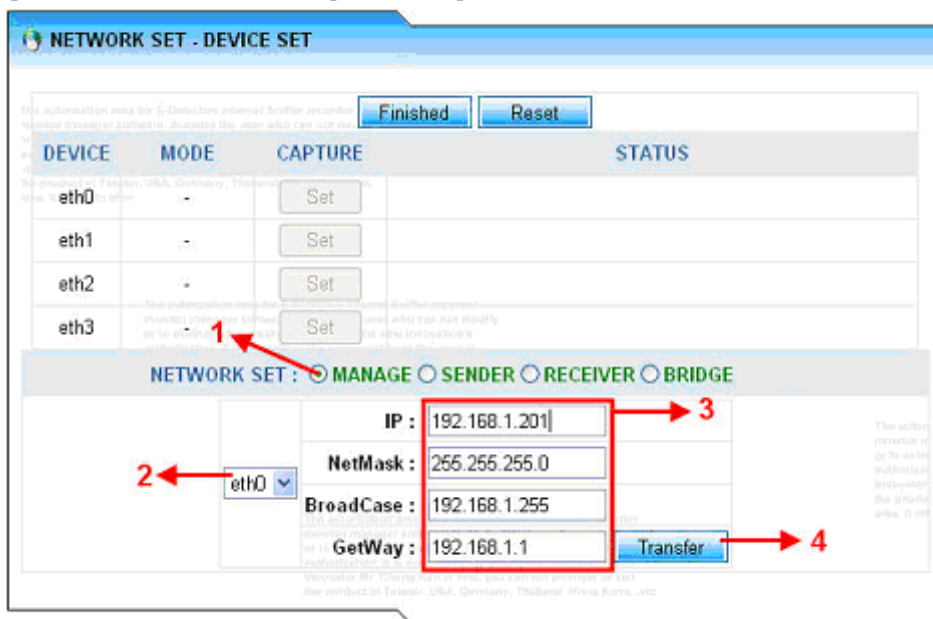
This mode uses one NIC card to capture and manage the data. The following diagram shows the concept of how this mode is operated.



This section illustrates the way of how to set up the Sniffer Mode with the following diagrams step by step:

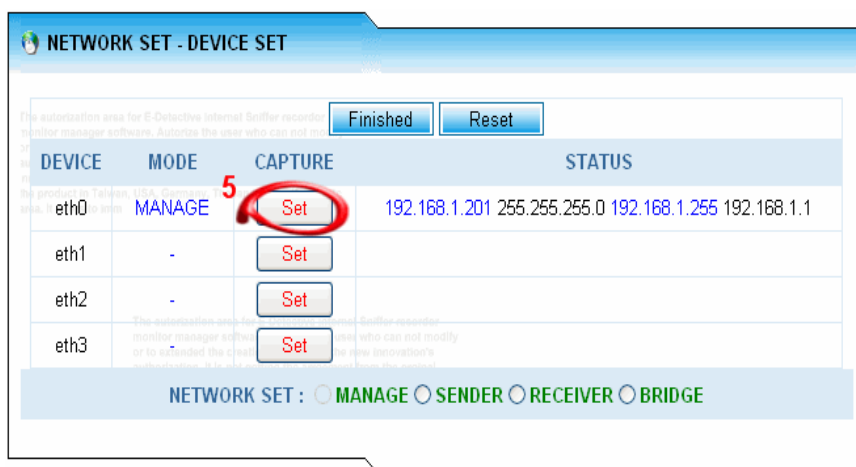
Step 1: Management Setup.

- [1] : Ticking the option “MANAGE”
- [2] : Selecting the NIC card called “eth0”.
- [3] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [4] : Press the button [Transfer] to submit.



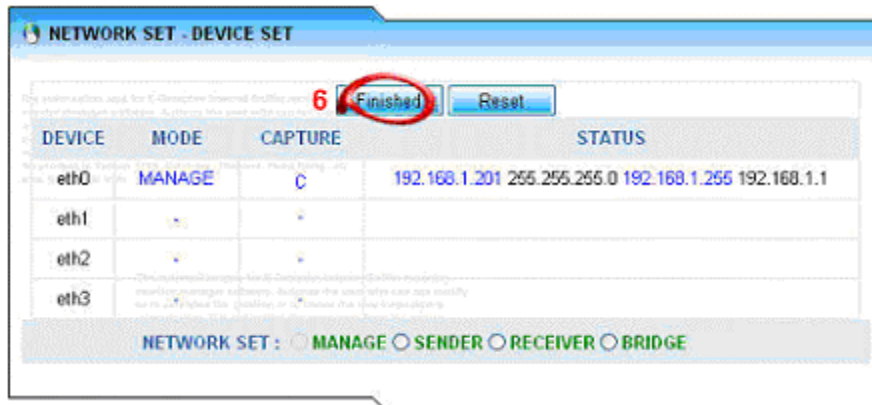
Set2: Capture Setup.

- [5] : Pressing the button [Set] on Device eth0 to set up which NIC card is to capture the data.



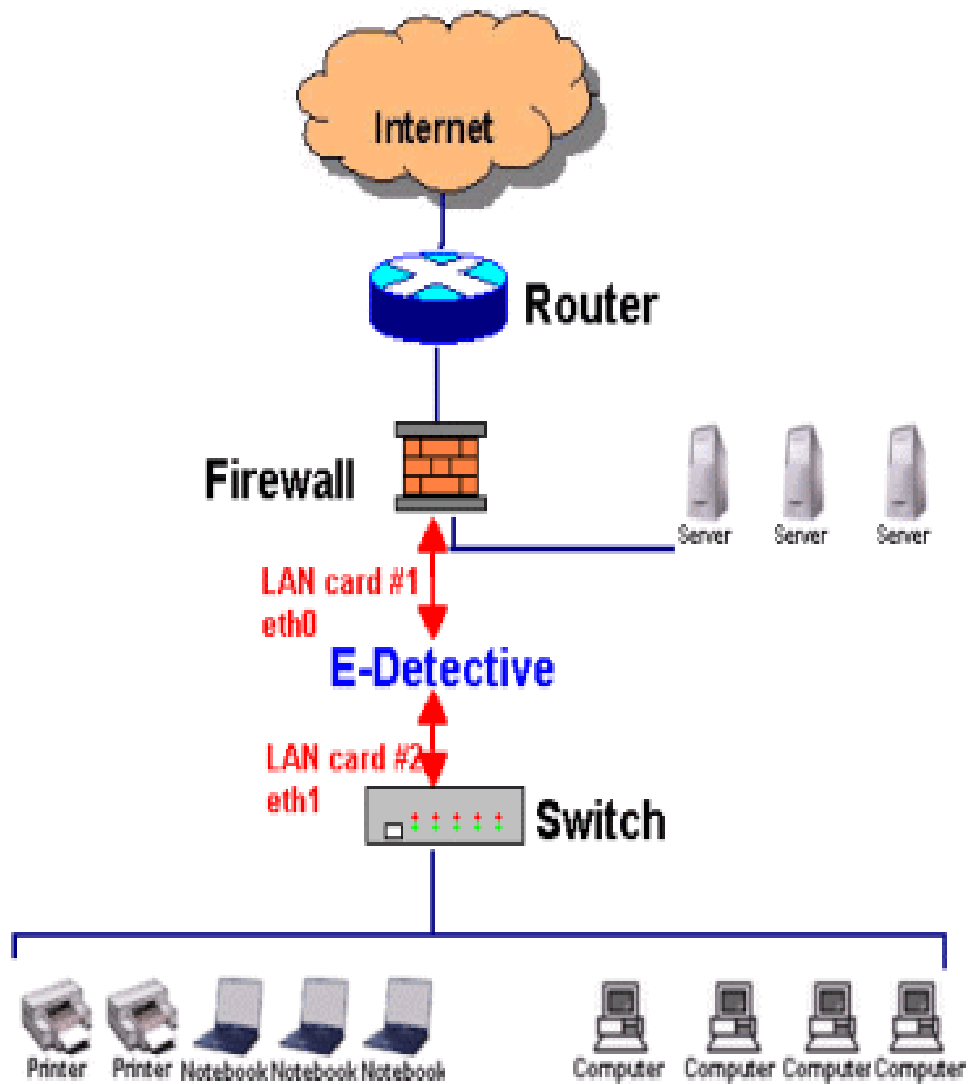
Set3: Finish Setup:

[6] : Pressing the button [Finished], the system will reboot and setup Sniffer mode for you.



Bridge Mode:

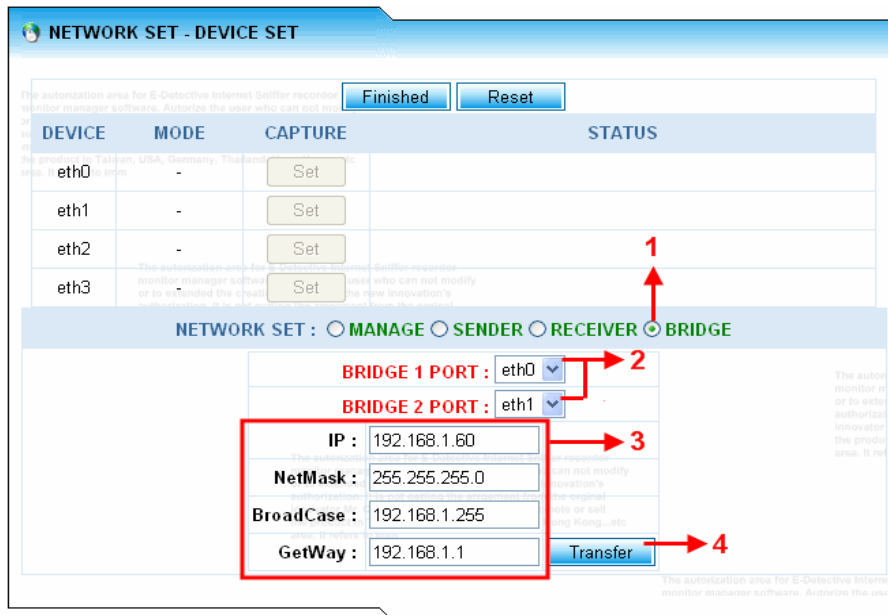
This mode uses two or three NIC cards to operate in the ED system. The following diagram shows the concept of how this mode is operated.



This section illustrates the way of how to set up the Bridge Mode with the following diagrams step by step:

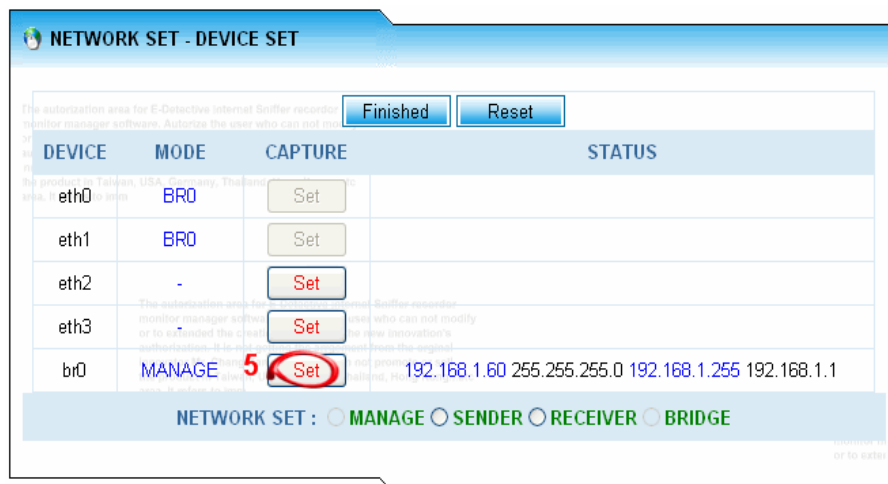
Step 1: Bridge Setup.

- [1] : Ticking the option “BRIDGE”
- [2] : Selecting two NIC cards as shown on the following diagram.
- [3] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [4] : Press the button [Transfer] to submit.



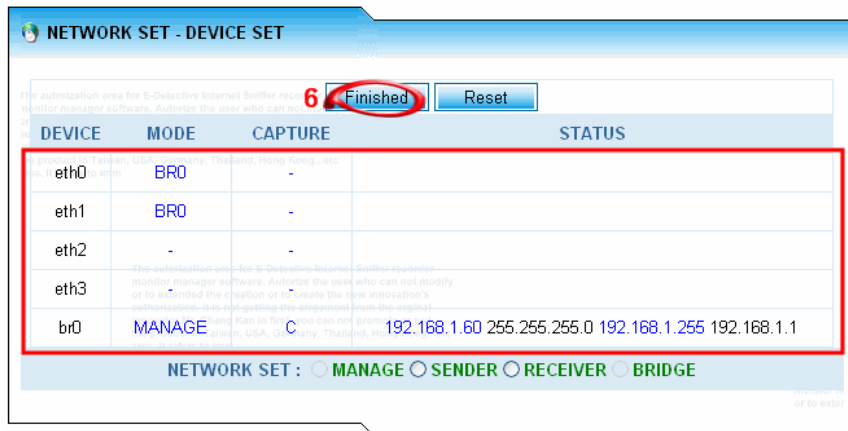
Set2: Capture Setup.

- [5] : This step produces one visual device called “br0” to manage the data. Suggest Users here to choose this visual device “br0” to capture the data as well.



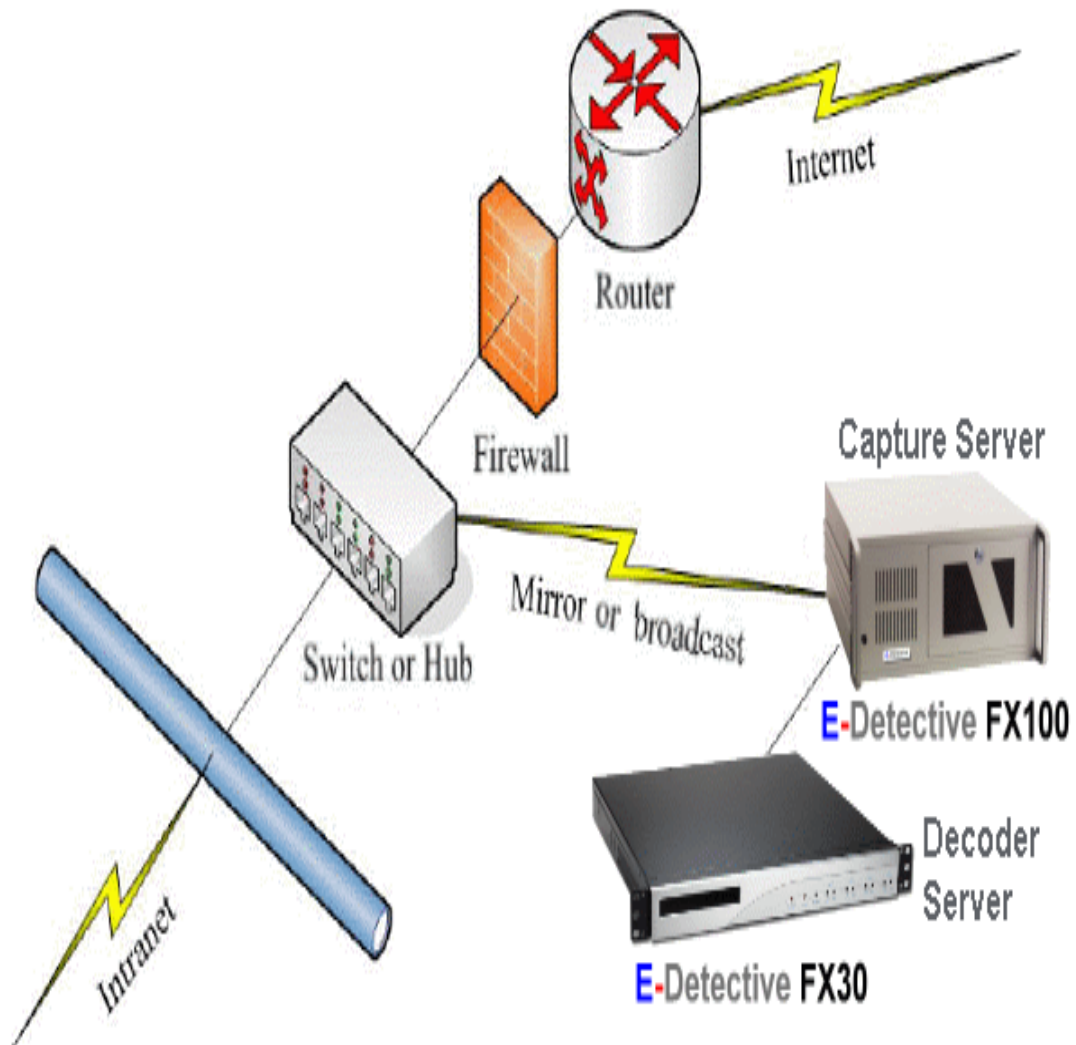
Set3: Finish Setup.

[6] : Pressing the button [Finished], the system will reboot and setup the Bridge mode for you.



SENDER/ RECEIVER Mode:

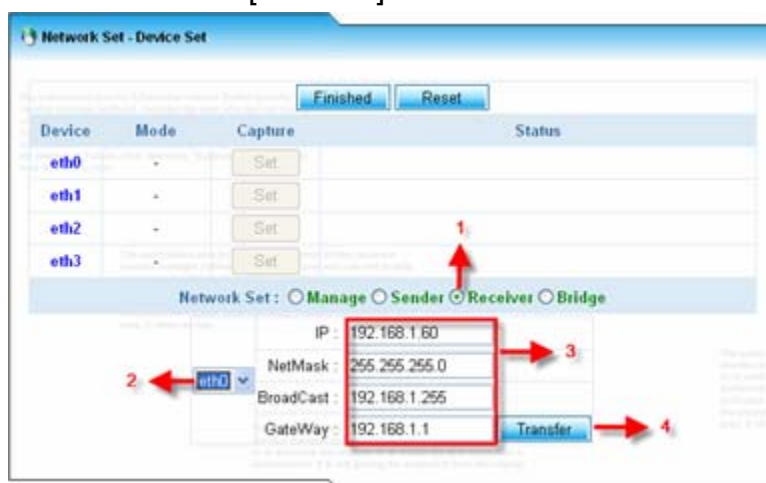
This mode uses two machines to operate in the ED system. One is called Sender to capture the data and then send those data to another machine called receiver. The receiver will manage/analyse the captured data once it receives the data from the sender. The following diagram shows the concept of how this mode is operated.



This section illustrates the way of how to set up the Sender/Receiver Mode with the following diagrams step by step:

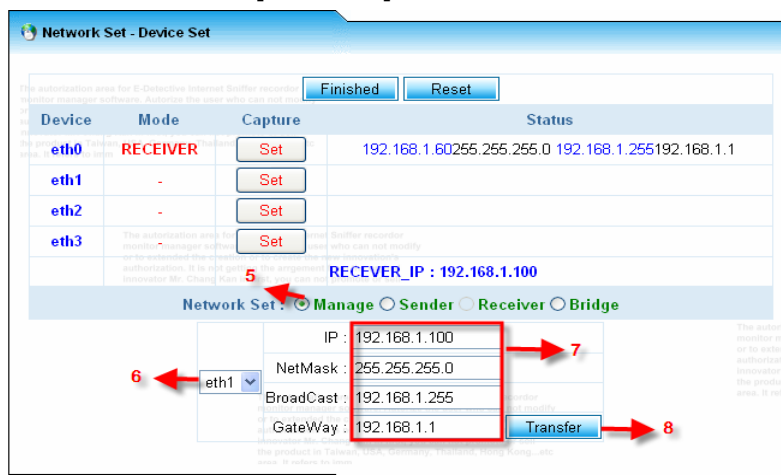
Step 1: Receiver Setup:

- [1] : Ticking the option "RECEIVER"
- [2] : Selecting one NIC card as shown on the following diagram.
- [3] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [4] : Press the button [Transfer] to submit.



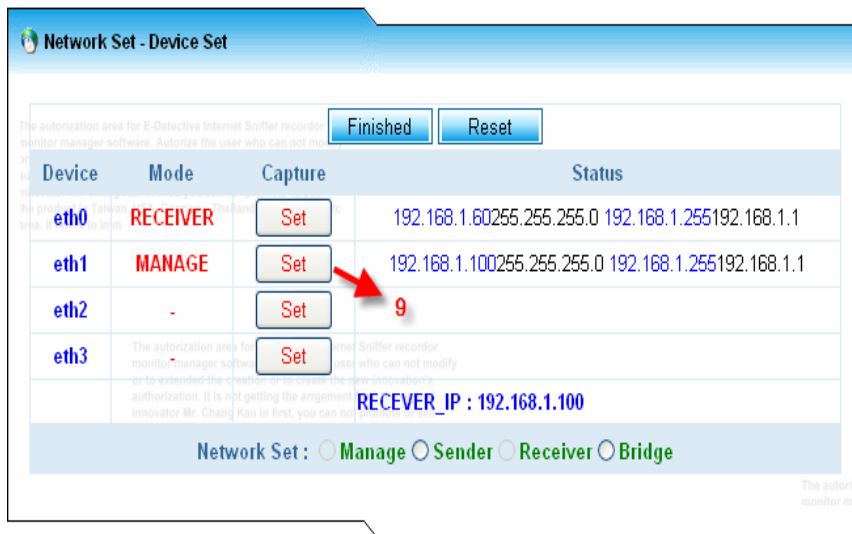
Step 2: Management Setup:

- [5] : Ticking the option "MANAGE".
- [6] : Selecting one NIC card as shown on the following diagram.
- [7] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [8] : Press the button [Transfer] to submit.



Step 3: Capture Setup:

[9] : Press the button [Set] to set up which NIC card to capture the data.



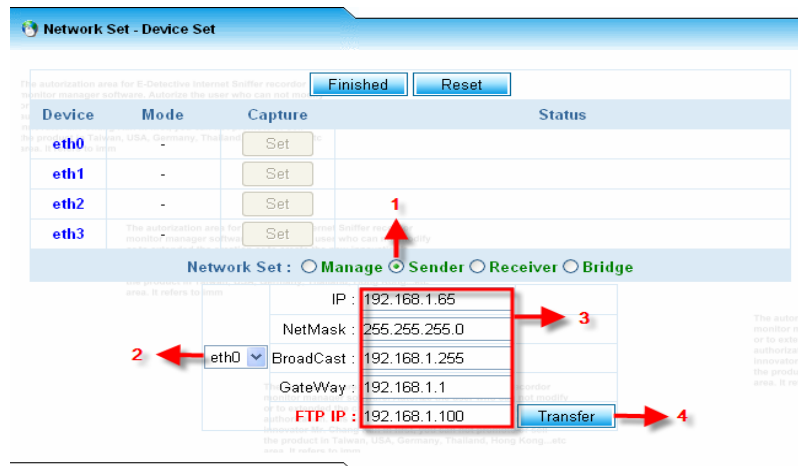
Step 4: Finish Setup:

[10] : Pressing the button [Finished], the system will reboot and setup the Receiver mode for you.



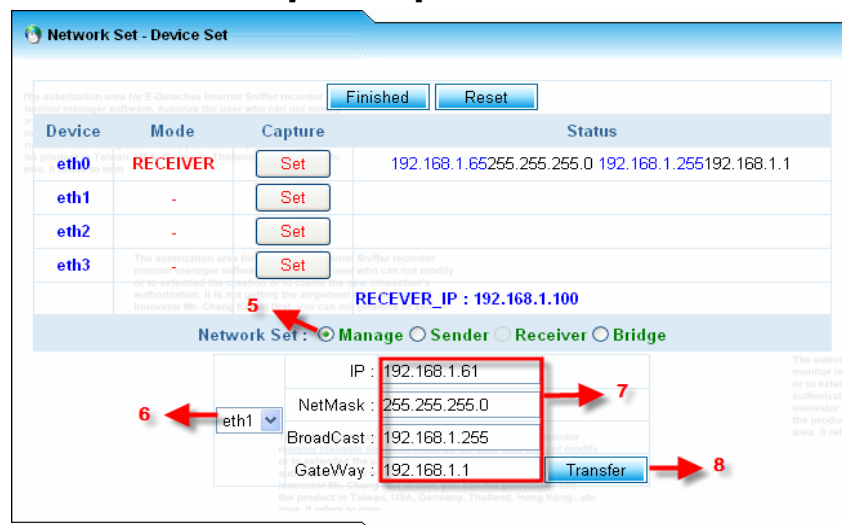
Step 1: Sender Setup:

- [1] : Ticking the option "SENDER"
- [2] : Selecting one NIC card as shown on the following diagram.
- [3] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are. The FTP IP is the receiver's ip address at where the data will be sent to.
- [4] : Press the button [Transfer] to submit.



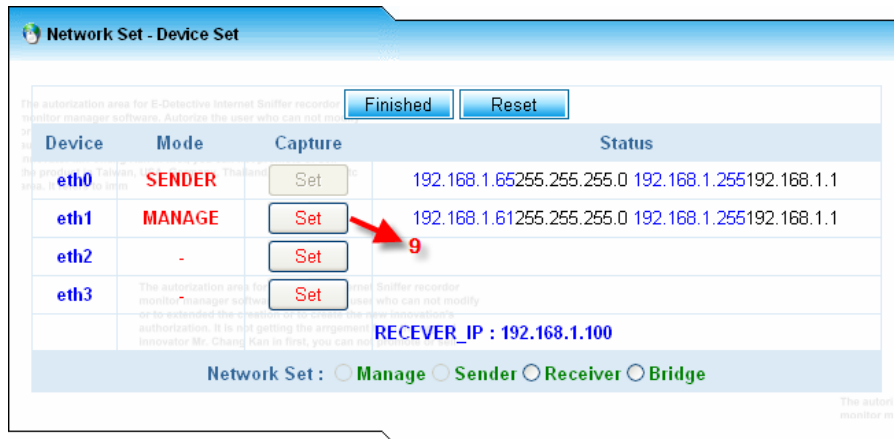
Step 2: Management Setup:

- [5] : Ticking the option "MANAGE".
- [6] : Selecting one NIC card as shown on the following diagram.
- [7] : Setup the information of IP, Mask IP, Broadcast IP and Getway IP. Please check with your network administrators if you are not sure what those IPs are.
- [8] : Press the button [Transfer] to submit.



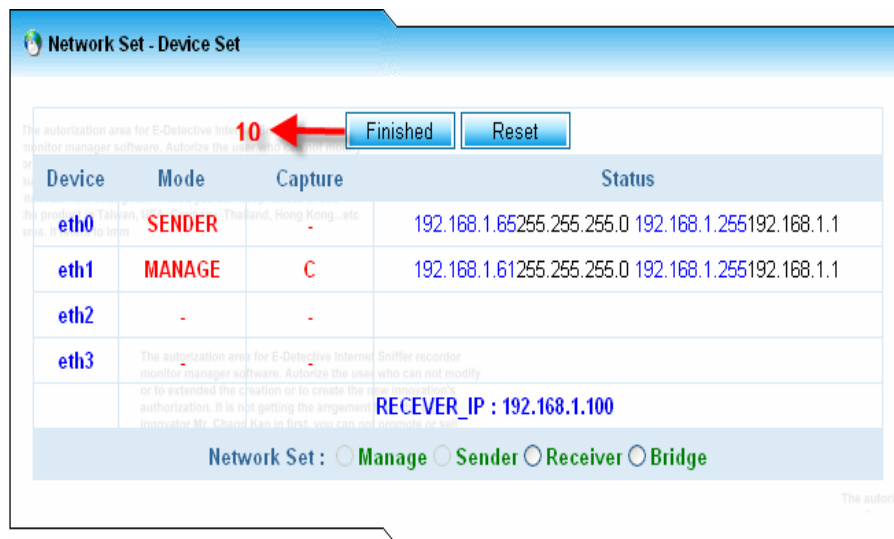
Step 3: Capture Setup:

[9] : Press the button [Set] to set up which NIC card to capture the data.



Step 4: Finish Setup:

[10] : Pressing the button [Finished], the system will reboot and setup the Sender mode for you.



DNS Set:

Enter the primary and secondary DNS provided from your IPS provider; press the button [Reset] to set up.

Configuration	Default	New Set
Primary	192.168.1.3	<input type="text"/>
Second		<input type="text"/>

Shutdown/Reboot System & Time adjusting:

Users here can shutdown or reboot the system and adjust the system time.

! If you want restore the system to initiation, Please input com port key, then reboot!

System Action :

Current System Time : 2007-04-14 10:03:42

Server Time : 2007 04 14 09 48

Year Month Day Hour Minute

Correct Time Zone : +8

2. Storage

It shows hard disk utilisation information which includes hard disk capacity, utilisation, and space left. Warning message is issued to administrator while utilisation reaches the threshold. The statuses of memory and server port number are also provided here.

HD status

-Detective Internet Sniffer recorder
-Authorize the user who can not modify

HD size	Used	Available size	Available(%)
53G	11G	40G	79%

System of Memory status

-Detective Internet Sniffer recorder
-Authorize the user who can not modify

Type	Total (KB)	Available Size (KB)	Available(%)
MEMORY	511632	6584	1%
Swap	1052248	1052248	100%

Update

-Detective Internet Sniffer recorder
-Authorize the user who can not modify

Type	Byte	Size
RX	2047655540	(1.9GiB)
TX	0	(0.0b)

Server status

-Detective Internet Sniffer recorder

Type	Status	Port
ftp	Open	21
ssh	Open	22
smtp	Open	25
pop3	Open	110
rpcbind	Open	111
auth	Open	113
https	Open	443
mysql	Open	3306
ajp13	Open	8009

3. Services

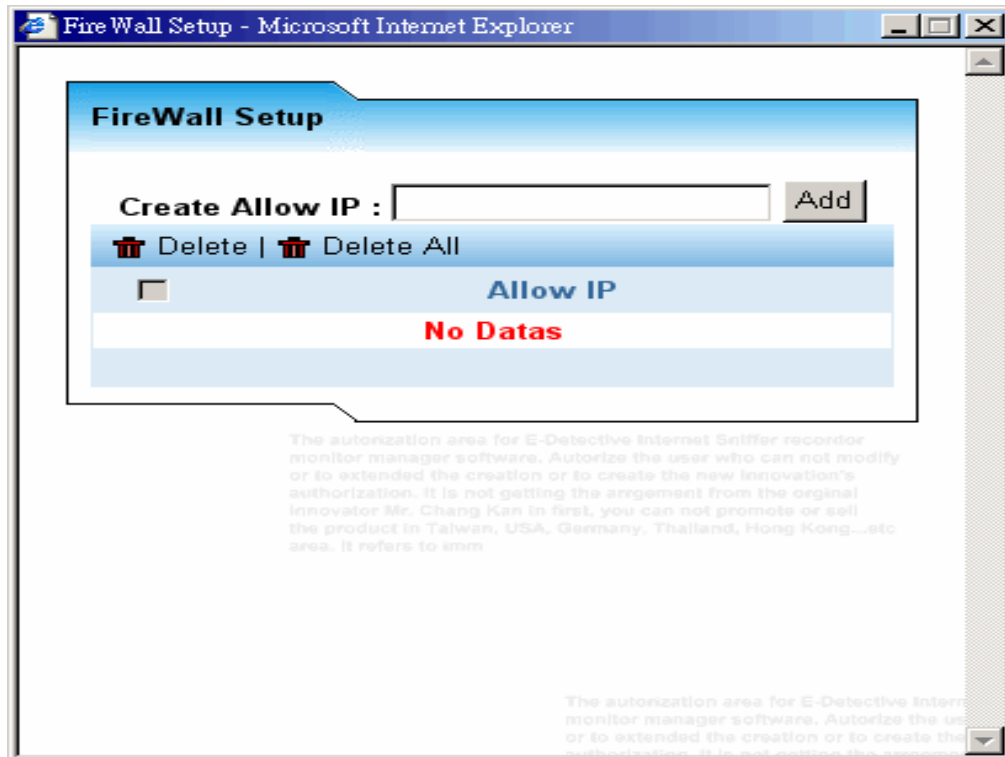
Users press the buttons [Stop] to activate/de-activate the services as shown on the following diagram.

Server Setup		
Service	Status	Action
SSH	Start	Stop
Mail Server	Start	Stop
Convert	Stop	Start
Capture Data	Start	Stop
Java Parser	Start	Stop
Web Packet Parser	Stop	Start
Packet Parser	Start	Stop
AD Server	Stop	Start
Proxy	Stop	Start
Flow	Stop	Start
POP3	Start	Stop
IMAP	Start	Stop
SMTP	Start	Stop
FTP	Start	Stop
P2P	Start	Stop
MSN	Start	Stop
ICQ	Start	Stop
YAHOO	Start	Stop
QQ	Start	Stop
Telnet	Start	Stop
Correct Time Zone	Stop	Start
FireWall	Start	Setup

Service	Function Description
SSH	Carries out the far-end segment
Mail Server	To carry out data transmission via FTP. To carry out the function of sending system emails.
Convert	To carry out the conversion of codes.
Capture Data	To capture the internet packets.
Java Parser	Java execution environment. To carry out the navigation bar.
Web packet Parser	To handle the data related to web page such as http, http content, webmail, and webmail sender in ED system.
Packet Parser	To handle all data that is not related to the data handled by Web packet parser.
AD server	To carry out the function of recording/displaying the administrators' name for each target.
Proxy	Whether handle the data captured from proxy server or not.
Flow	To carry out the function of flow monitoring in ED system.
POP3	To carry out the function of POP3 in ED system.
IMAP	To carry out the function of IMAP in ED system.
SMTP	To carry out the function of SMTP in ED system.
FTP	To carry out the function of FTP in ED system.
P2P	To carry out the function of P2P in ED system.
MSN	To carry out the function of MSN in ED system.
ICQ	To carry out the function of ICQ in ED system.
Telnet	To carry out the function of telnet in ED system.
correct Time zone	To carry out the function of adjusting system time.
FireWall	To activate/de-activate the function. Function: Users can be able to specify what IPs can access into ED system.

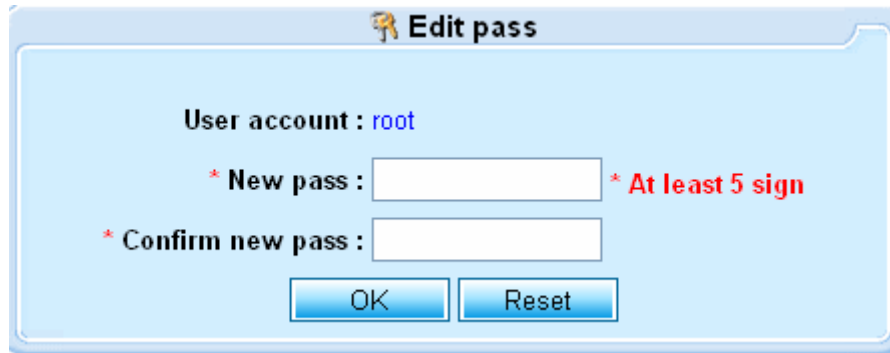
FireWall:

It creates specific IP for allowing login to E-Detective System.



4. Edit Password

User can be able to change his/her password here; the password might be the combination of numbers, letters, and special characters. Remember to contains at least 5 of numbers or letters or special characters.



Edit pass

User account : root

* New pass : * At least 5 sign

* Confirm new pass :

OK Reset

5. Backup Data

Auto Backup:

Auto backup

Auto backup time: 02 Hour

1 Time : Hour: 02, Day: , Month: , Week:

2 Status : Stop Start

3 OK **4** Reset

BackUp Modules

5 Modules : POP3 SMTP IMAP
 FTP MSN ICQ
 YAHOO HTTP DYNAMIC
 WEBMAILR WEBMAILS TELNET
 QQ P2P

6 OK

Notify target

Receiver : **7** **8** OK

Delete

No	Receiver
1.	sunny@decision.com.tw

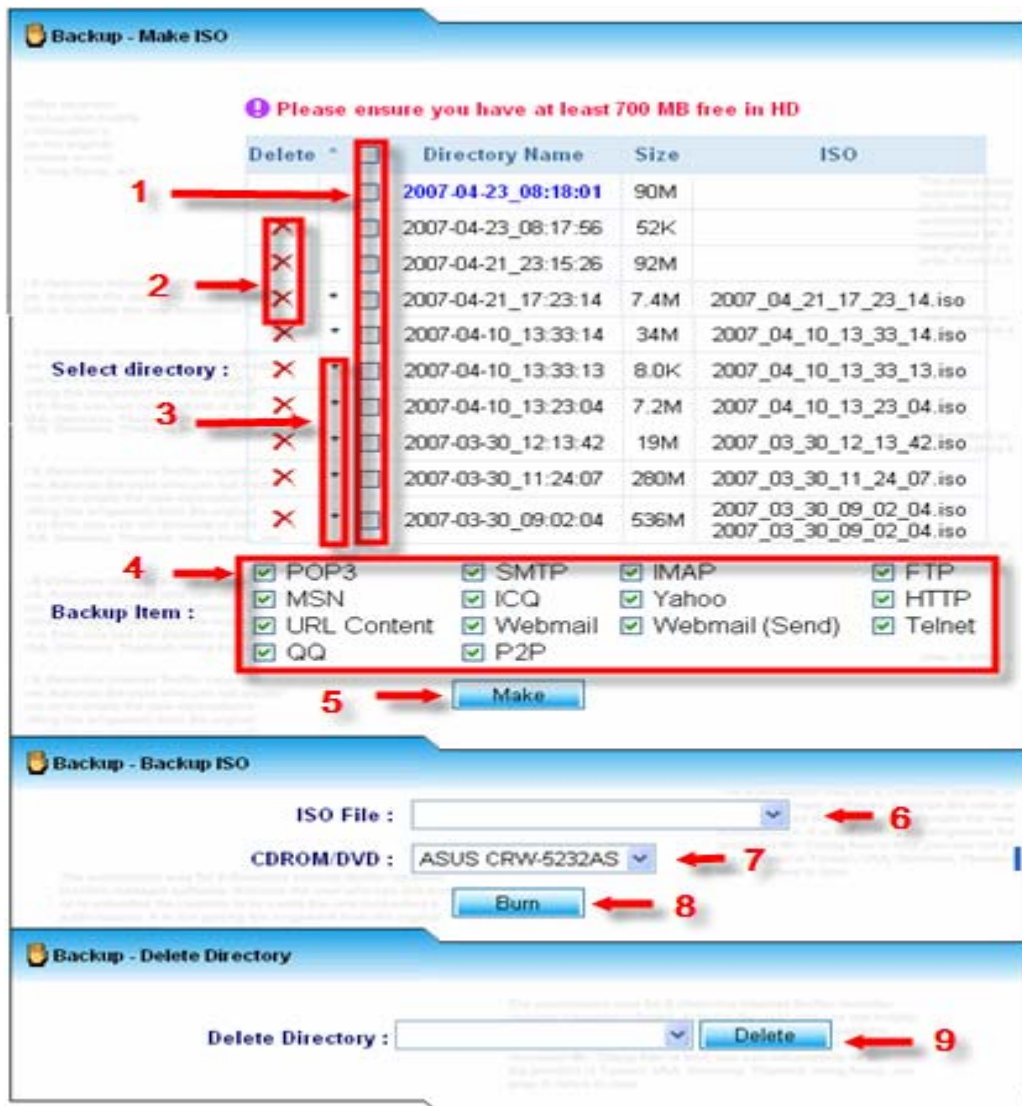
9

Total 1, Total Page 1, Current Page 1

Features in this page:

- [1] : Time: Automatic backup could be scheduled daily, weekly or monthly.
- [2] : Status: To Stop or Start auto-backup function.
- [3] : This button [OK] is to submit the time specified.
- [4] : This button [Reset] is to clear up time specified.
- [5] : Modules: User ticks which data type the system should auto-bakcup.
- [6] : This button [OK] is to submit the modules selected.
- [7] : User inputs the Email account on this field to set up where the notification is sent to when the backup file is generated.
- [8] : This button [OK] is to submit the Email account.
- [9] : Checkbox: Emails could be deleted by checking the checkbox. The checkboxes could be ticked respectively or checked all by clicking the 1st one.

Backup:



Features in this page:

- [1] : Checkbox: Ticking one or several checkboxes to make the backup file. Checkbox could be ticked respectively or checked all by clicking the 1st one.
- [2] : This symbol is a link to delete the rawdata. Rawdata presents the information on the ED system.
- [3] : This symbol should be appeared if the rawdata has been taken to backup an ISO file.
- [4] : User chooses which data type should be involved in the backup file.
- [5] : This button [Make] is to start making the ISO file once pressing the button.
- [6] : The ISO files will get into this drop down list once the ISO file is

generated. User selects the ISO file here and burns it into the CD.

- [7] : ED system auto-scans the CDROM/DVD from user's computer. User is able to choose which device to burn the ISO file.
- [8] : This button [Burn] is to start burning the data into the CD.
- [9] : User selects which backed-up ISO file you want the system to delete and then press the button [delete] to start deleting.

FTP Backup:

The FTP Backup function here provides the function to transmit the backed-up ISO file to a server specified via FTP. The time to transmit the data is at 02:00 AM per day if this function is activated.

FTP Login Information

1 Ftp Host : 192.168.1.249

2 User : alluser

3 Password : ●●●●●●●●

4 Port Number : 21

5 Directory : ISO_FILE

6 → ON OFF

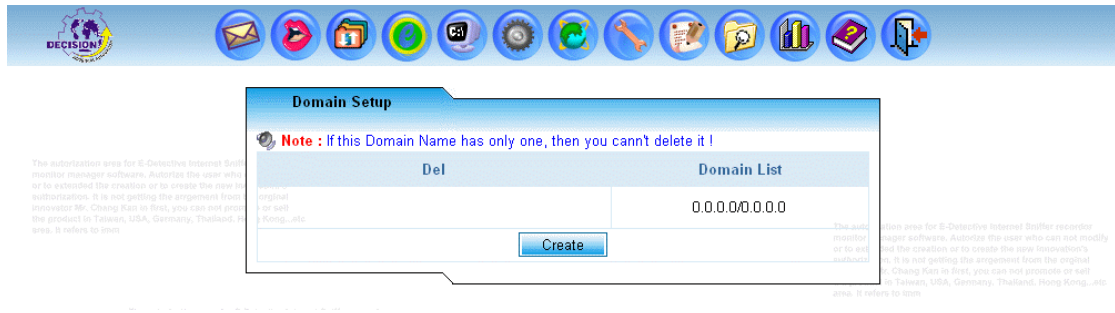
7 →

Features in this page:

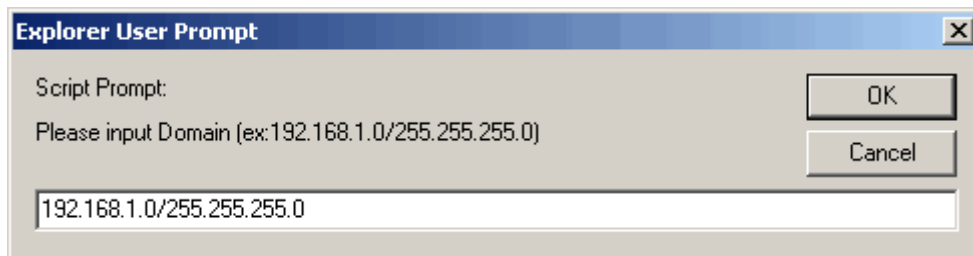
- [1] : Ftp Host: The FTP address at where the backed-up ISO file is sent to.
- [2] : User: The FTP username account.
- [3] : Password: The FTP password.
- [4] : Port Number: The FTP port number used to transmit the data.
- [5] : Directory: The directory in where the backed-up ISO file is saved.
- [6] : ON/OFF is to activate/dis-activate the FTP backup function.
- [7] : The button [Submit] is to submit the conditions specified. The button [Reset] is to clear up all values on each field.

6. Domain

This function is to add the IP Domain where the information is captured from.



Click on [Create], and add a new Domain as following format [network/ subnet mask].



7. Network Rules

E-Detective specifies specific network access rule in specific time. E-Detective will issue warning Email to both the one who breaks the rule and the administrator. This function corrects network access behaviour automatically and no impact to the network. Administrator may establish policy by press [Create] and [confirm] when set; modify the policy by [Reset]. You may set up policy to rule the access activities of web surfing, Email, file transferring, ICQ, AOL, MSN, Yahoo chatting, Telnet, and webmail.

Note: warning message is issued within one hour after the violation occurred

Columns display:

- Date-Time
- Type
- IP
- Inform Account-1
- Inform Account-2
- Rule

You might also sort the data by above columns by a simply clicking on the title.

No.	Date-Time	Type	IP	Inform Account-1	Inform Account-2	Rule
3	2005-10-21 10:19:06	MSN	192.168.1.33	vic@decision.com.tw	aries@decision.com.tw	Rule
2	2005-10-21 10:17:57	MSN	192.168.1.10	ken@decision.com.tw	pan@decision.com.tw	Rule
1	2005-10-21 10:16:54	YAHOO	192.168.1.20	aries@decision.com.tw	ken@decision.com.tw	Rule

Features in this page:

- [1] : Rules Of Using Network: press to refresh
Delete: check the checkbox and press [Delete] to delete records
Create: [create] popup create window
- [2] : records per page<100
- [3] : Single delete or delete all
- [4] : Click on [Rule] to view the rule
- [5] : First, Previous, Next, Last page
- [6] : Current page information

To create a new rule: fill what you want to define as followings and then press

[Confirm].

Account : Insert domain or user IP

Type : 「POP3」
「SMTP」
「FTP」
「MSN」
「ICQ」
「YAHOO」
「HTTP」
「URL CONTENT」
「WEBMAILR」
「WEBMAILS」
「TELNET」 - TELNET Server IP

Rule : 「POP3」 - E-mail Address or XXX.com.tw
「SMTP」 - E-mail Address or XXX.com.tw
「FTP」 - FTP id, Server IP
「MSN」 - specific MSN ID
「ICQ」 - specific ICQ ID
「YAHOO」 - specific YAHOO ID
「HTTP」 -insert keyword e.g. Yahoo, Hinet
「URL CONTENT」 - insert keyword e.g.Yahoo, Hinet
「WEBMAILR」 - insert keyword e.g.Yahoo, Hinet and server
type
「WEBMAILS」 - insert keyword e.g.Yahoo, Hinet and server
type
「TELNET」 - specific TELNET IP
「ATTACHMENT」 - check the checkboxes

Setup Time : Format 「hour : minute」 24HR

Allow : 「YES」 allow to access in specific intervals, 「NO」 deny to
access in specific intervals, send warning Email while
violation occurs.

Inform User E-mail Address
account-1 :

Inform Administrator E-mail Address
account-2 :

New Configuration - Microsoft Internet Explorer

New Configuration

Account : BY IP BY DOMAIN Ex: 192.168.1.60

Type : POP3

Rule : E-mail : Sender Receiver CC
 Attachment : Yes No

SetupTime : [] : [] ~ [] : []

Allow : Yes No

Inform account-1 : []

Inform account-2 : []

8. Setup Mail

User provides one Email account and its SMTP name for ED system in order to send out the system Emails such as daily report, warning emails.

Features in this page:

- [1] : Local/Remote: The SMTP name. User ticks the local one if you have set up the mail server locally.
- [2] : Sender Email: User provides one Email account for ED system for sending out the system Emails.
- [3] : Server requires authentication: Tick this option if the mail server used requires authentication.
- [4] : Provides the account name and its password here for authentication.
- [5] : The button [OK] is to submit the setting.
- [6] : The button [Reset] is to clear up the setting.
- [7] : The button [Send Test] is to test this function based on the given conditions.

Testing the Mail Server Adopted:

The following diagram is popped up when user presses the button [Send Test] at the previous diagram in this Setup Mail section. User inputs the Email account where the message is sent to and press the button [Send] to test the function to see whether it works or not.

G. STATUS

1. Backup Record

Database logfile is listed 10 records per page. Press [All Record] to view all the records.

The screenshot shows a web-based application interface for 'DataBase Logfiles'. At the top, there is a navigation bar with various icons. Below it, a message box states: 'Message : Only show top 10, Choose all record can look for all logfile'. The main content area contains a table with columns for 'No.', a checkbox, and 'Backup Logfile'. The table lists 10 records, each with a filename ending in '.sql.tgz'. To the right of the table is an 'All Record' button. The interface also includes several informational text blocks on the left and right sides, which appear to be repeated or partially obscured text from another document.

No.	<input type="checkbox"/>	Backup Logfile
1.	<input type="checkbox"/>	2005-10-21.sql.tgz
2.	<input type="checkbox"/>	2005-10-20.sql.tgz
3.	<input type="checkbox"/>	2005-10-19.sql.tgz
4.	<input type="checkbox"/>	2005-10-18.sql.tgz
5.	<input type="checkbox"/>	2005-10-17.sql.tgz
6.	<input type="checkbox"/>	2005-10-16.sql.tgz
7.	<input type="checkbox"/>	2005-10-15.sql.tgz
8.	<input type="checkbox"/>	2005-10-14.sql.tgz
9.	<input type="checkbox"/>	2005-10-13.sql.tgz
10.	<input type="checkbox"/>	2005-10-12.sql.tgz

Press [All Record] to view all the records in the following window.

The screenshot shows a browser window titled 'https://202.39.29.27 - Database Backup Logfile List ...'. The main content area displays a window titled 'DataBase Logfiles List' with a table showing the first three records from the previous screenshot. The logfiles are listed as blue hyperlinks.

No.	Logfile
1.	2005-10-21.sql.tgz
2.	2005-10-20.sql.tgz
3.	2005-10-19.sql.tgz

2. Port number

This function offers users to inspect each protocol for system and set port number value, it can establish AD, MSN proxy port number manually.

Service	Status
Proxy	8080
SMTP(to)	25
SMTP(from)	25
POP3(from)	110
POP3(to)	110
IMAP(from)	143
IMAP(to)	143
FTP	21
Msn Port	1863
Msn Proxy	3128
Msn Proxy	8080
TELNET	23
YAHOO	5050
YAHOO	20
YAHOO	23
YAHOO	25
YAHOO	5101
YAHOO	5100
YAHOO	81
YAHOO	5001
ICO	5190
AD	88
OO UTP	8000
OO TCP	80
OO TCP	443
OO TCP	0

Submit Default Set

3. Online IP

E-Detective automatically searches IPs on network. If there is no IP list, the amount of IPs is granted by license. Automatic searching is not targeting on specific target. To target specific users, you might need to establish a target list. You may also group them for better management. To specify a target IP, please choose group function and edit the IP, hostname and group, press [online IP info] to view current status.

Columns display:

- Status
- Pc IP
- Pc Name
- At Least Time
- Group

You might also sort the data by above columns by a simply clicking on the title.

No.	Status	Pc IP	Pc Name	At Least Time	Group
1.	<input type="checkbox"/> -4	192.168.1.30	潘峙豪	2005-10-21 08:57:39	GROUP1
2.	<input type="checkbox"/>	192.168.1.10	龍哥	2005-10-21 09:00:53	GROUP1
3.	<input type="checkbox"/>	192.168.1.22	劉志杰	2005-10-21 09:01:35	GROUP1
4.	<input type="checkbox"/>	192.168.1.12	***	2005-10-21 08:55:26	GROUP1
5.	<input type="checkbox"/>	192.168.1.14	***	2005-10-21 08:55:47	GROUP1
6.	<input type="checkbox"/>	192.168.1.15	汪得孝	0000-00-00 00:00:00	GROUP1
7.	<input type="checkbox"/>	192.168.1.51	洪士為	0000-00-00 00:00:00	GROUP1
8.	<input type="checkbox"/>	216.155.193.130	***	0000-00-00 00:00:00	GROUP1
9.	<input type="checkbox"/>	192.168.1.21	***	2005-10-20 17:18:03	GROUP1
10.	<input type="checkbox"/>	192.168.1.20	***	2005-10-21 08:48:16	GROUP1
11.	<input type="checkbox"/>	192.168.1.36	***	2005-10-20 14:58:35	GROUP1
12.	<input type="checkbox"/>	192.168.1.32	***	2005-10-20 15:12:18	GROUP1
13.	<input type="checkbox"/>	192.168.1.93	***	2005-10-20 17:51:22	GROUP1
14.	<input type="checkbox"/>	156.110.90.114	***	0000-00-00 00:00:00	GROUP1
15.	<input type="checkbox"/>	192.168.1.91	***	0000-00-00 00:00:00	GROUP1

Features in this page:

[1] : Online IP List: press to refresh

Delete: check the checkbox and press [Delete] to delete records

Create: [Create] to create IP

Auto Search: [Auto Search] popup search window and edit IP range to search

Hide IP:[Hide IP] to hide the IP records

Skip IP:[skip IP] to skip the IP from recording

Import:[Import] import targeting IP list from Excel file.

Copyright © 2007 Decision Computer International Co., Ltd

- [2] : records per page<100
- [3] : Single delete or delete all
- [4] : Edit IP to modify IP's Information
- [5] : First, Previous, Next, Last page
- [6] : Current page information

Add an IP:

Single adding:

Click on [Create] to popup the window and insert IP, name and group. Click on [Create] to add.

Create IP Information				
PC IP	PC Name	Status	At Least Time	Group
<input type="text"/>	<input type="text"/>			GROUP1

monitor manager software. Authorize the user who c...
or to extended the creation or to create the new inn...

Create Close

Multiple IPs adding:

Press [Auto Search] and then insert IP range to search IPs, check IPs on the list and then press [Update] to add.

Search Range

IP Range : Confirm

Ex : 192.168.1.1,192.168.1.255

Search List

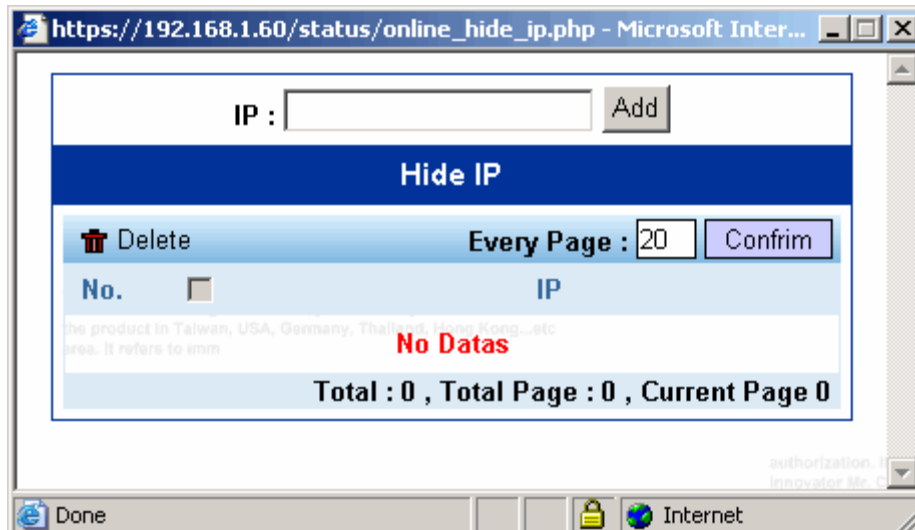
Update Total / Version : 17/65535

No.	IP	User	Group
No Datas			

Hide IP records:

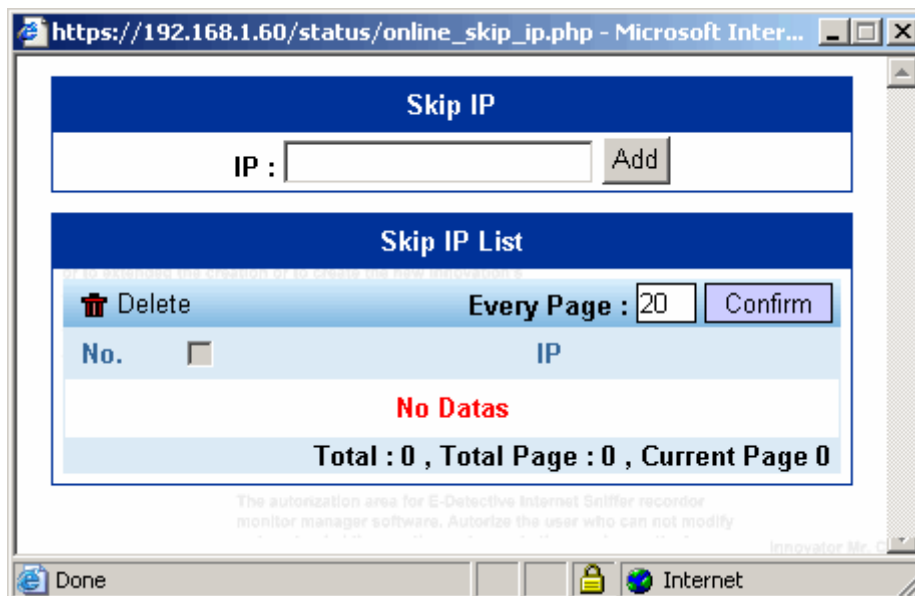
Press [Hide IP]. Edit the IP that you want to hide.

Note: Record of the hidden IP is recorded on the background.



Skip IP :

Click on [Skip] and insert specific IP. Press [Add] to add the IP to [Skip IP List].



Input

Import targeting IP list from Excel file.

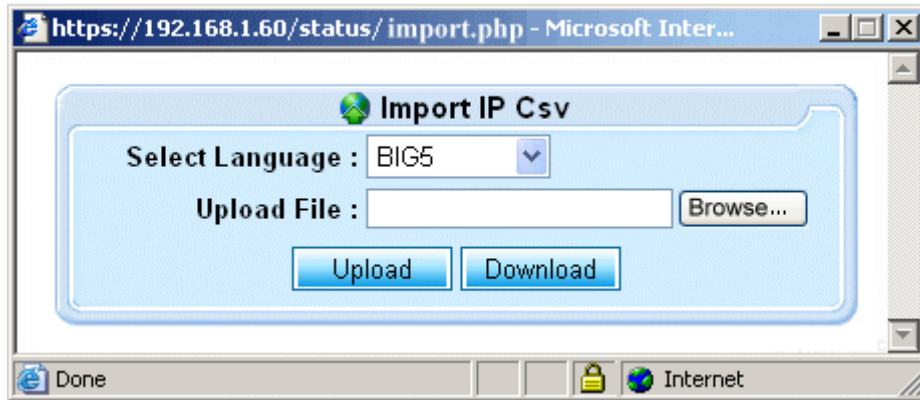
Format : IP ; NAME ; GROUP

Note 1: Save Excel file as *.CSV

Note 2: No Chinese Big5 Name, please convert big5 code to Unicode.

Note 3: Setting the value of GROUP at [No.] column of [TOOL] = > [Group Set] page.

Copyright © 2007 Decision Computer International Co., Ltd



Excel format :

	A	B	C	D	E
1	192.168.1.1	Arise	1		
2	192.168.1.2	Eric	1		
3	192.168.1.3	Bill	1		
4	192.168.1.4	Alex	1		
5	192.168.1.5	Joe	1		
6	192.168.1.6	Peter	1		
7	192.168.1.7	Mary	1		
8	192.168.1.8	Jean	1		
9	192.168.1.9	May	1		
10	192.168.1.10	Joanne	1		

IP

Name

Group No.

4. Login List

This shows the System log for security control. It displays the IP lists that tried to login to E-Detective System (whether login success or login fail).

Columns display:

- IP
- Login ID
- Login Time
- Language
- Status

You might also sort the data by above columns by a simply clicking on the title.

No.	IP	Login ID	Login Time	Language	Status
1.	192.168.1.10	root	2005-10-21 11:30:45	English	Login Success
2.	192.168.1.10	root	2005-10-21 10:44:29	English	Login Success
3.	192.168.1.10	root	2005-10-21 10:44:29	English	Login Success
4.	192.168.1.10	root	2005-10-21 09:03:04	English	Login Success
5.	192.168.1.10	root	2005-10-21 09:03:01	English	Login Success
6.	192.168.1.33	root	2005-10-20 12:08:41	English	Login Success
7.	192.168.1.33	root	2005-10-20 11:31:28	English	Login Success
8.	192.168.1.10	root	2005-10-20 10:11:34	English	Login Success
9.	192.168.1.33	root	2005-10-18 09:11:36	English	Login Success
10.	192.168.1.33	root	2005-10-18 09:11:29	English	Login Fail
11.	192.168.1.25	root	2005-10-17 11:19:25	English	Login Success
12.	192.168.1.25	root	2005-10-17 10:56:50	English	Login Success
13.	192.168.1.25	root	2005-10-17 10:39:09	English	Login Success
14.	192.168.1.33	root	2005-10-17 09:39:12	GB_chinese	Login Success
15.	192.168.1.33	root	2005-10-17 09:24:19	GB_chinese	Login Success

Features in this page:

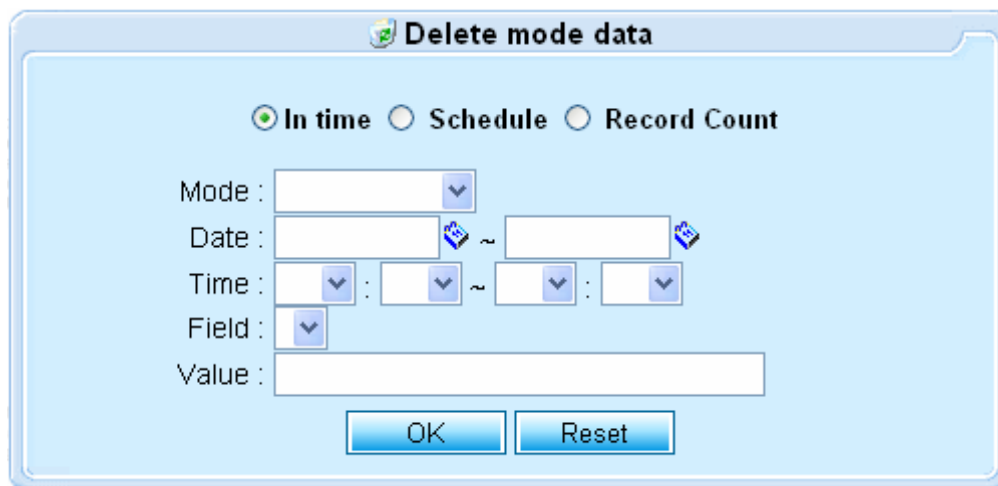
- [1] : Login List: press to refresh
Delete: check the checkbox and press [Delete] to delete records
- [2] : records per page < 100
- [3] : Single delete or delete all
- [4] : First, Previous, Next, Last page
- [5] : Current page information

H. TOOL

1. Delete Data

In Time:

User deletes data based on specific service or protocol such as Email, Ftp, Chat, Http, Webmail, and Telnet in the menu.



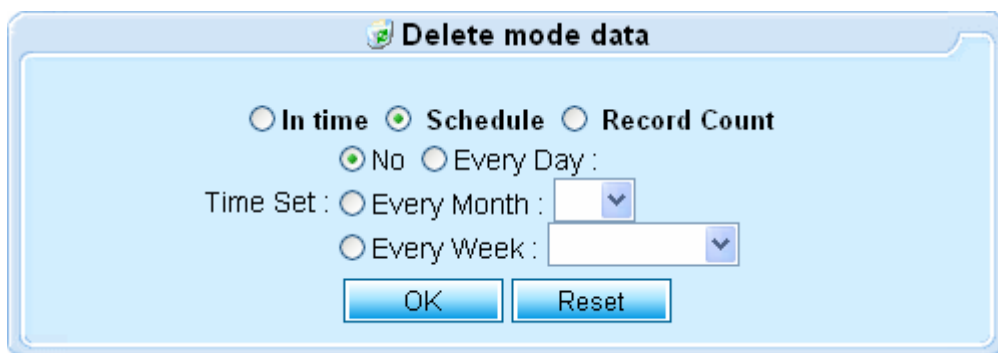
The screenshot shows a dialog box titled "Delete mode data". At the top, there are three radio buttons: "In time" (selected), "Schedule", and "Record Count". Below this, there are several input fields: "Mode:" with a dropdown menu, "Date:" with two date pickers separated by a tilde (~), "Time:" with four time pickers (hour, minute, hour, minute) separated by colons and a tilde (~), "Field:" with a dropdown menu, and "Value:" with a text input field. At the bottom, there are two buttons: "OK" and "Reset".

Features in this page:

- Mode: choose what data type you want to delete, e.g. POP3.
- Date & Time: Delete the data within the period specified.
- Field: To specify the item of record such as IP, sender, receiver.
- Value: The value of the item of record.

Schedule:

User deletes all records at the time specified.

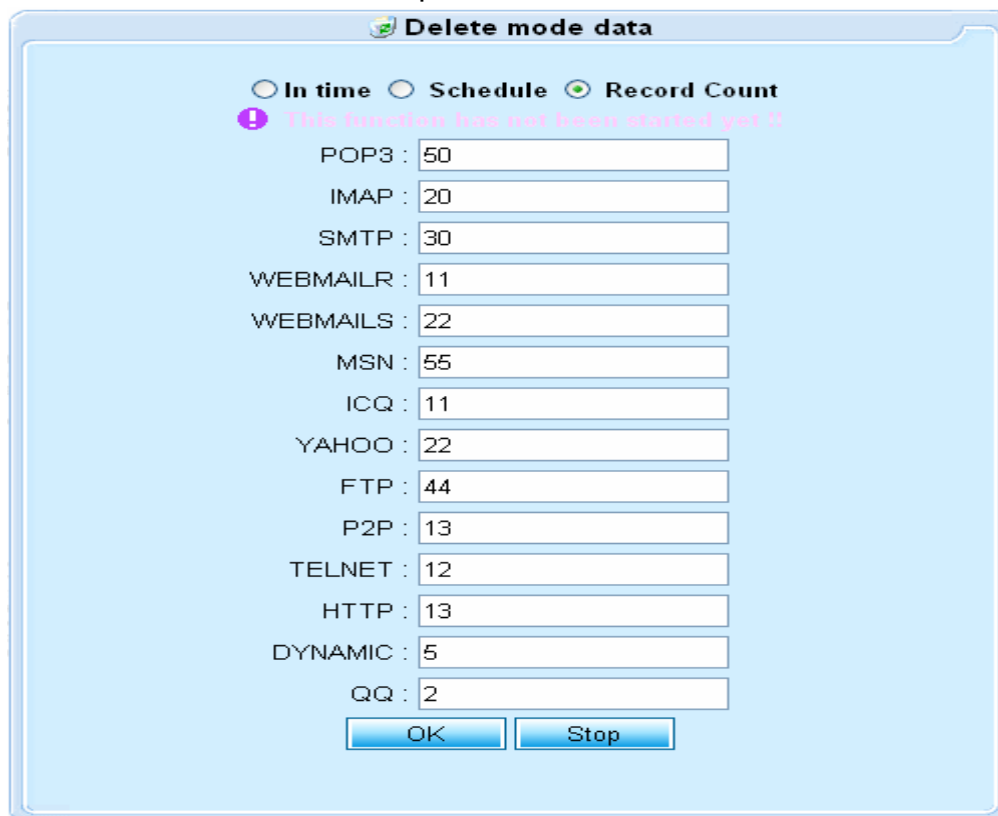


The screenshot shows the same "Delete mode data" dialog box, but with the "Schedule" radio button selected. Below the radio buttons, there are two sub-options: "No" (selected) and "Every Day:". Under "Every Day:", there are two more options: "Every Month:" with a dropdown menu, and "Every Week:" with a dropdown menu. The "OK" and "Reset" buttons are at the bottom.

Record Count:

User specifies the number of threshold for each type of data. The number here means the number of limited record for each type of data. Only the latest number of records is left if the actual number of record exceeds the threshold specified.

For example: The threshold number for the data type POP3 is 50. The actual number of records for POP3 is 55. ED system will delete the first 5 oldest records in the POP3 and keep the latest 50 records.

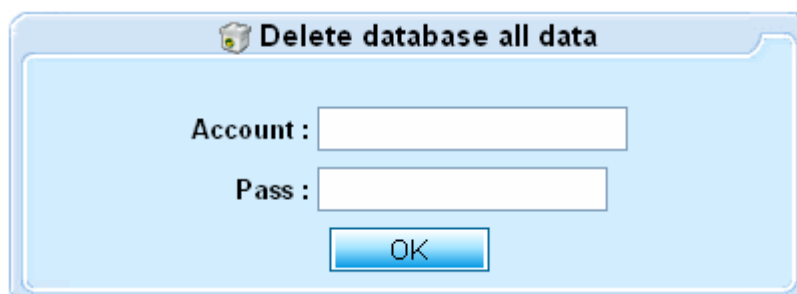


The screenshot shows a dialog box titled "Delete mode data" with a shield icon. It contains three radio buttons: "In time", "Schedule", and "Record Count", with "Record Count" selected. Below the radio buttons is a pink warning message: "This function has not been started yet!!". The dialog lists various data types with corresponding input fields for their record counts: POP3 (50), IMAP (20), SMTP (30), WEBMAILR (11), WEBMAILS (22), MSN (55), ICQ (11), YAHOO (22), FTP (44), P2P (13), TELNET (12), HTTP (13), DYNAMIC (5), and QQ (2). At the bottom, there are "OK" and "Stop" buttons.

Data Type	Record Count
POP3	50
IMAP	20
SMTP	30
WEBMAILR	11
WEBMAILS	22
MSN	55
ICQ	11
YAHOO	22
FTP	44
P2P	13
TELNET	12
HTTP	13
DYNAMIC	5
QQ	2

Delete All Data:

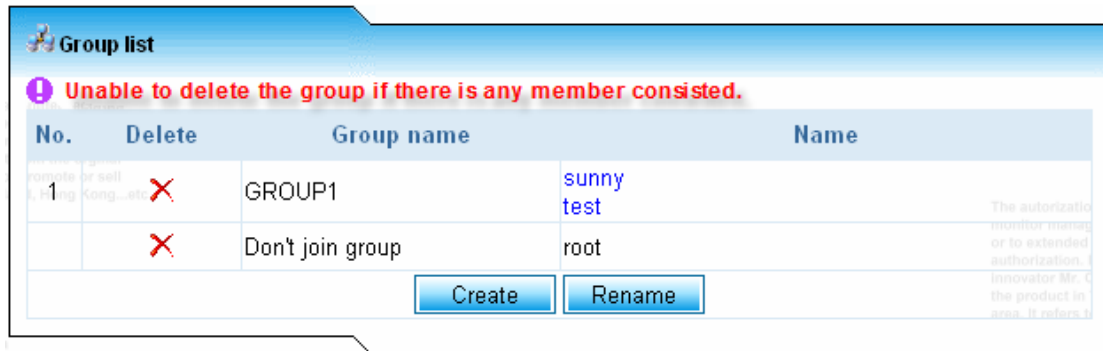
User inputs his/her account and password on the following diagram to delete all data.



The screenshot shows a dialog box titled "Delete database all data" with a shield icon. It contains two input fields: "Account" and "Pass". Below the input fields is an "OK" button.

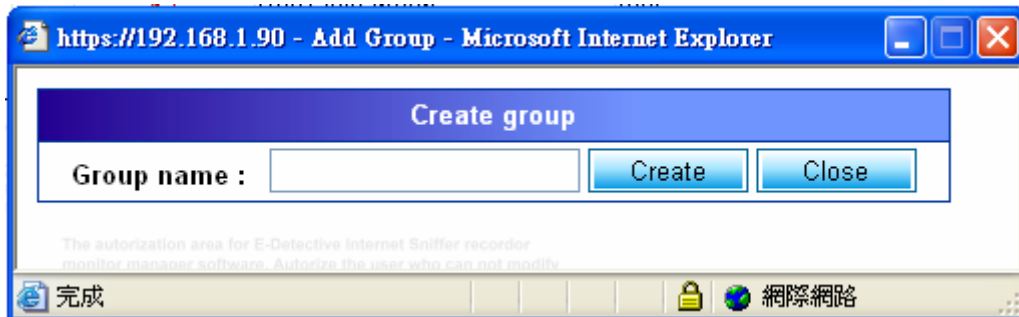
2. Group Set

The following diagram shows the group list and the members consisted.



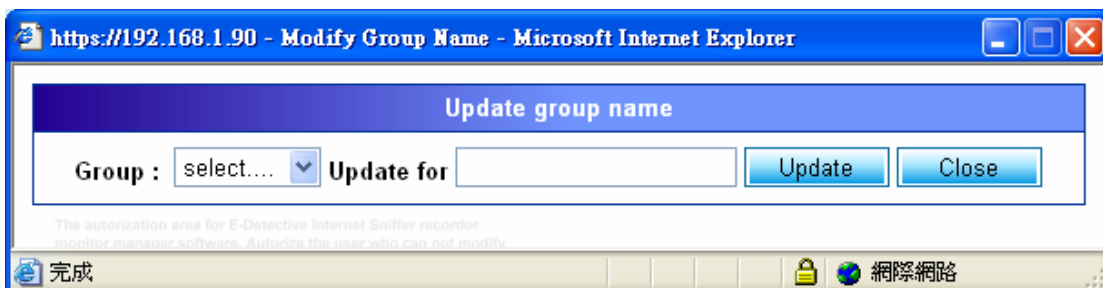
Create New Group:

The following diagram is popped up if user presses the button [Create] on the Group List windows above. User inputs the group name and press the button [Create] on the following windows to create new group.



Rename the group:

The following diagram is popped up if user presses the button [Rename] on the Group List windows. User selects which group you want to modify and type the new name on the blank field, press the button [Update].



3. Add Users

User is able to create new accounts for other users to login to ED system. Type the user name and password; assign one this new member to specific group on the drop down list. Press the button [OK] to make this creatation.



The image shows a 'Create User' dialog box with a light blue background and a title bar containing a small icon and the text 'Create User'. The dialog contains three required fields, each marked with a red asterisk: 'Login name' with an empty text input box; 'Password' with an empty text input box and a red note '* At least 5 sign' to its right; and 'Group' with a dropdown menu currently showing 'Choose...'. At the bottom of the dialog are two buttons: 'OK' and 'Reset'.

4. System Warning

System warning consists of four main features as following:

- Alarm administers by Email if actual data size in HD capacity exceeds the threshold specified.
- Upload the custom-made warning message.
- System daily report.

HD Alarmer & Custom-Made Warning File.



Features in this page:

- [1] : Set up the percentage of threshold; if actual total data size in HD capacity exceeds the percentage specified, ED system sends out the warning file.
- [2] : Upload the custom-made warning file.
- [3] : X : To delete the warning file.

User specifies Email account and which Warning File the system sends to.



Features in this page:

- [4] : Type the Email account where the warning file sends to.
- [5] : The subject of the warning file.
- [6] : Select which warning file that the system sends.
- [7] : X : To delete the Email account where the ED system sends warning file to.

Copyright © 2007 Decision Computer International Co., Ltd

Daily Report

Warning - Dairy report of system status

Forward :

Subject :

OK

No.	Del	Forward	Subject
1	X	cat@stmail.fju.edu.tw	Dairy report of system status
2	X	sunny@decision.com.tw	Dairy report of system status
3	X	ja824@pchome.com.tw	ja824@pchome.com.tw

Features in this page:

- [8] : Type the subject and the Email account where the daily report is sent to and press the button [OK] to submit.
- [9] : X : To delete the Email account where the ED system sends the daily report to.

5. Flow Warning

Flow warning function sends the warning message to both administrators and the people who deplete too much internet resource to download/upload files.

Show Monitored IP

Press the link [Show Monitored IP] to show the targets who are being monitored. The information for each target is shown as the following diagram.

Show All IP | Admin Mail | Edit Monitored IP | Interval Time : 72H 2007-04-21 13:19:36~2007-04-24 13:19:36 :20 Confirm

NO	IP	In(GigaBits)	OUT(GigaBits)	Total(GigaBits)	CheckSize	Client Mail
1	192.168.1.20	0	0	0	0.0001	cat@stmail.fju.edu.tw
2	192.168.1.21	0	0	0	20	math824@gmail.com
3	192.168.1.34	0	0	0	10	taipeidecision@aol.com

Total , Total Page 1 , Current Page

Show All IP

Press the link [Show All IP] to show all online targets whom the ED system captures the information from. The information for each target here is shown as the following diagram.

Show Monitored IP | Edit Admin Mail | Edit Monitored IP | Search IP | Interval Time : 72H 2007-04-21 13:27:29~2007-04-24 13:27:29 Every page : 20 OK

NO	IP	In(GigaBits)	OUT(GigaBits)	Total(GigaBits)
No Data				

Total 0 , Total Page 0 , Current Page 1

Edit Admin Mail

The following window is popped up if the link [Edit Admin Mail] is pressed. User adds the Email accounts here and then the warning will be sent to those Email accounts specified if there is any target monitored exceeds the quota.

Administrator Mail list

Input area for E-Detective Internet Manager software. Authorize the administrator to add the creation or to create the new innovation's.

Add

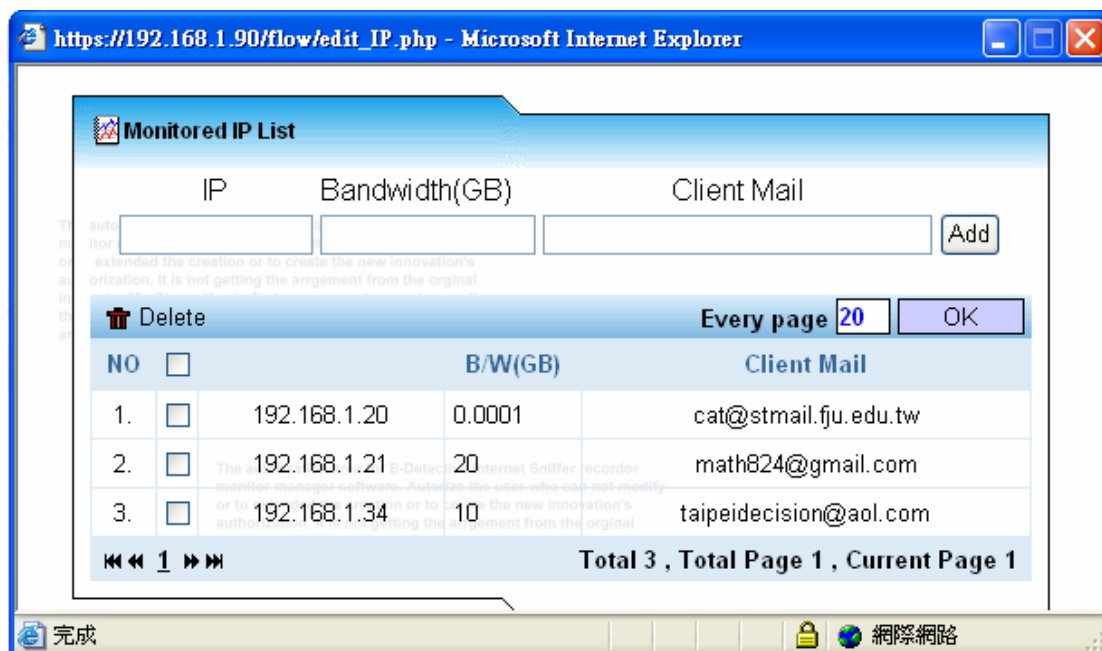
Delete Every page 20 OK

NO	<input type="checkbox"/>	Admin Mail
1.	<input type="checkbox"/>	decision_test@pchome.com.tw
2.	<input type="checkbox"/>	sunny@decision.com.tw

« 1 » Total 2 , Total Page 1 , Current Page 1

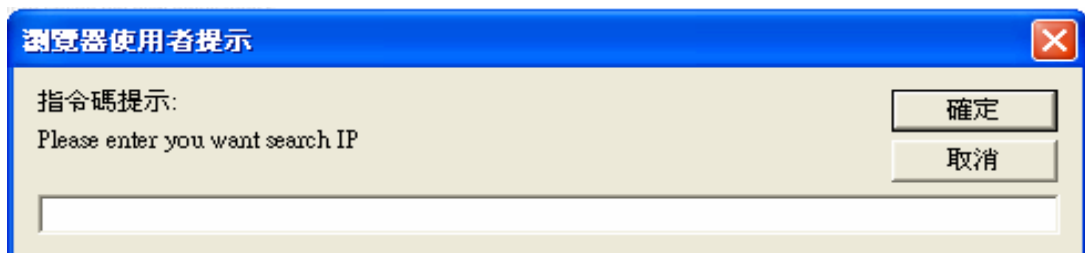
Edit Monitored IP

User creates the IPs you want the ED system to monitor their flow, or modifies their information. Bandwidth (GB) in the following diagram means how much quota you assign to the specific IP. Quota is total size of downloading/uploading the files.



Search IP

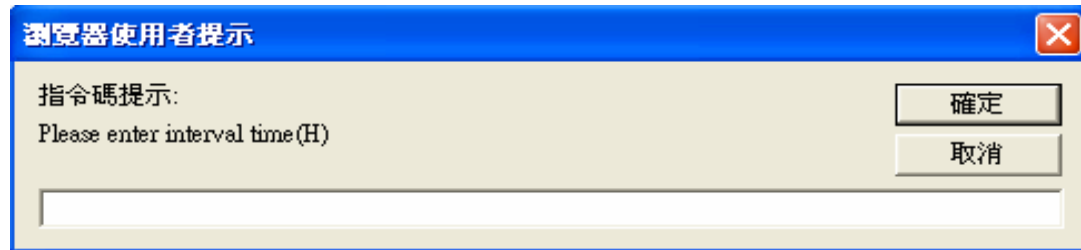
A search engine searches the information of the specific IP.



Interval Time (H)

The interval time here means to count the actual data size of downloading/uploading files occurred in the specific hours ago for each target.

For example: The interval time here is 5 hours. ED system time is currently at 12:00 on 12/Dec/2007. ED system will then count the total size of information occurred between 07:00 12/Dec/2007 and 12/Dec/2007 for each target.

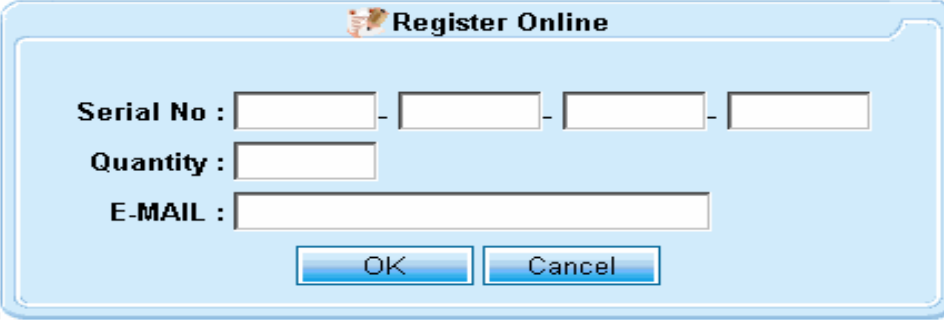


I. REGISTER

E-Detective system is activated via online certificated registration.

- Serial No
- Quantity (license of users)
- E-MAIL

Note: Registration shall be done via Internet.



The image shows a dialog box titled "Register Online" with a small icon of a person. It contains three input fields: "Serial No" (a four-part field with hyphens), "Quantity" (a single field), and "E-MAIL" (a single field). Below the fields are two buttons: "OK" and "Cancel".

Serial No : - - -

Quantity :

E-MAIL :

OK Cancel

J. Data Search

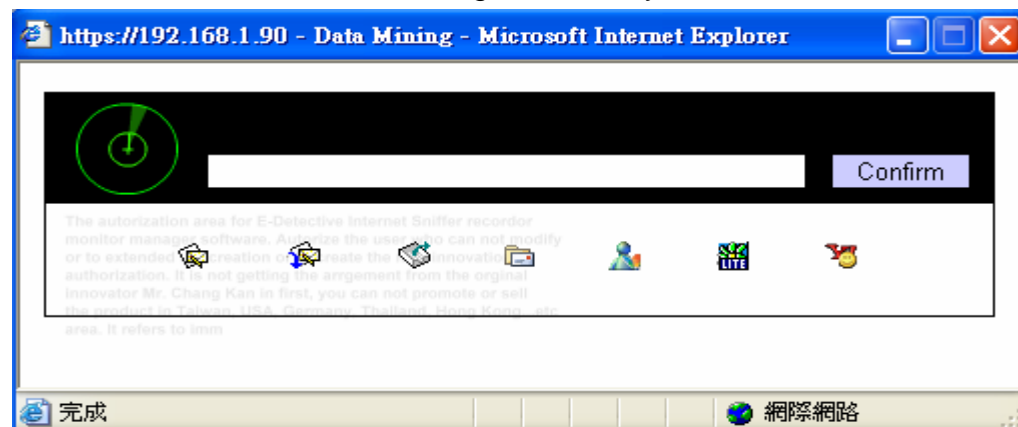
1. Data Mining

E-Detective Data Mining uses the user's key word in data statement to easily find out the data from (E-mail / POP3, SMTP, IMAP, Web-mail sender, Msn, Icq, Yahoo). It compares the content as well as arranges out the relative keyword message.

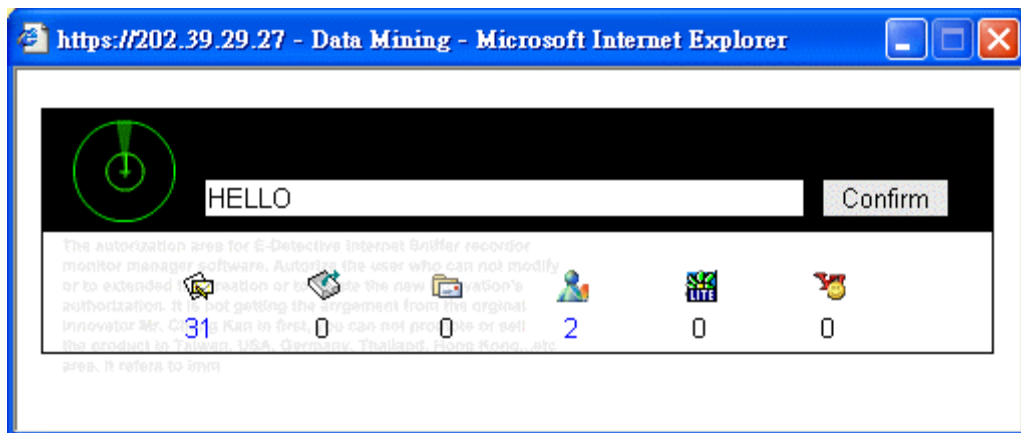
1. Search by keyword is completely supported by the way of Boolean Logic.

- Key word
- “&” and “AND”
- OR
- “NOT” not include
- “NEAR”

User can key in the searching keyword, press [Confirm], then the system will auto find out all the data including relative keyword.



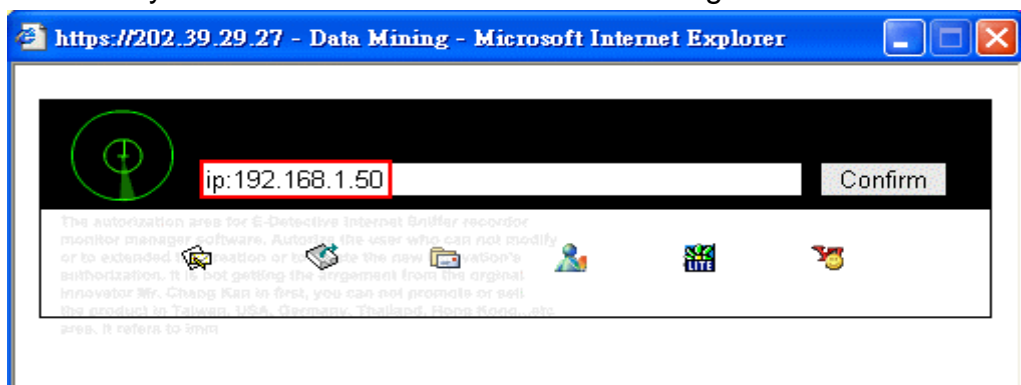
The system will connect to the main page and show the searching data after selecting the numerical number.



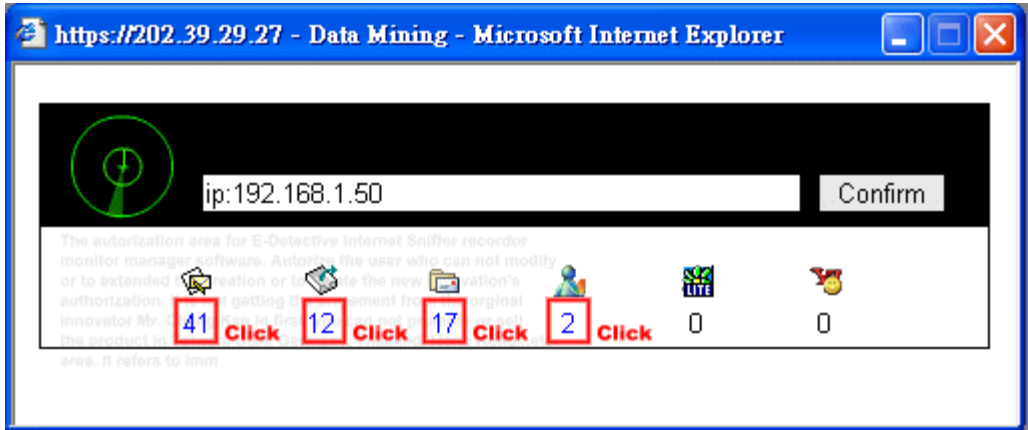
No.	Date-Time	Sender	Receiver	CC	BCC	Subject	Size
1.	2005-10-21 14:04:28	brandhill@decision.com...	decision_test@hotmail...			Fw: Find PC8255 card in Windows XP	4K
2.	2005-10-21 14:04:25	brandhill@decision.com...	decision_test@hotmail...			Fw: PCCOMB-Problem	3.4K
3.	2005-10-21 14:04:21	brandhill@decision.com...	decision_test@hotmail...			Fw: Attention Casper	3K
4.	2005-10-21 14:04:15	brandhill@decision.com...	decision_test@hotmail...			Fw: NT Drivers	6.7K
5.	2005-10-14 18:16:19	decision@decision.com.t...	schz@keba.co.at schz...			PCCOMB-Problem (need urgent reply)	14.9K
6.	2005-10-14 14:05:59	decision@decision.com.t...	Engineering@Systeme...			PC Com pricing	20.9K
7.	2005-10-12 17:32:41	decision@decision.com.t...	schz@keba.com			inquiry	765.9K
8.	2005-10-12 11:01:44	decision@decision.com.t...	OGun@arrowil.com			PI for the order PO: OF031427	2.7K
9.	2005-10-11 20:36:30	decision@decision.com.t...	schz@keba.com			inquiry	1.9K
10.	2005-10-11 15:40:05	decision@decision.com.t...	rstocker@akumen.com			E-Detective: Internet forensic appliance	246.6K
11.	2005-10-11 15:11:30	decision@decision.com.t...	rstocker@akumen.com	decision...		Fw: E-Detective: Internet forensic appliance	236.3K
12.	2005-10-11 14:51:51	decision@decision.com.t...	bliss@singnet.com.sg			payment for the last shipment	5.8K
13.	2005-10-11 08:12:10	decision@decision.com.t...	chang_kan@decision.c...			Fw: E-Detective: Internet forensic appliance	13.3K
14.	2005-10-10 09:54:28	decision@decision.com.t...	rstocker@akumen.com	decision...		Fw: E-Detective: Internet forensic appliance	11.7K
15.	2005-10-07 13:10:51	decision@decision.com.t...	chang_kan@decision.c...			Fw: E-Detective: Internet forensic appliance	38.6K

2. Searching IP

User can key in "ip:" and add the IP number that for searching. Press [Confirm] then the system will auto search the data including the relative IP.



The system will connect to the main page and show the searching data after selecting the numerical number.



MSN | Delete | Display Set | Search Show Mode : IP Name | Every Page : 15 Confirm

No.	<input type="checkbox"/>	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	<input type="checkbox"/>	2005-10-08 11:45:30	192.168.1.50	she0430@hotmail.com	decision_msn@hotmail.com	Conversation	20
2.	<input type="checkbox"/>	2005-10-03 14:11:29	192.168.1.50	dc040201@hotmail.com	she0430@hotmail.com	Conversation	65
3.	<input type="checkbox"/>	2005-10-03 14:11:29	192.168.1.50	she0430@hotmail.com	dc040201@hotmail.com	Conversation	63

Total : 3 , Total Page : 1 , Current Page 1

2. Search

The system provides advance search function. Information or data recorded can be searched based on the setting search statement.

Search Conditions

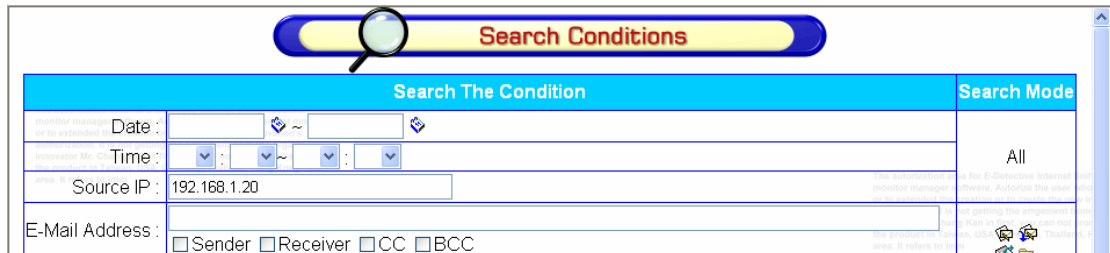
Search The Condition		Search Mode
Date :	<input type="text"/> ~ <input type="text"/>	All
Time :	<input type="text"/> : <input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/> : <input type="text"/>	
Source IP :	<input type="text"/>	
E-Mail Address :	<input type="text"/> <input type="checkbox"/> Sender <input type="checkbox"/> Receiver <input type="checkbox"/> CC <input type="checkbox"/> BCC	
Subject :	<input type="text"/>	
Webmail Type :	<input type="text"/>	
FTP Server :	<input type="text"/>	
FTP User :	<input type="text"/>	
P2P Tool :	<input type="text"/>	
P2P File :	<input type="text"/>	
MSN Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	All
ICQ Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
Yahoo Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
QQ Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
URL :	<input type="text"/>	
Telnet User :	<input type="text"/>	
Other :	<input type="text"/>	
<input type="button" value="Reset"/> <input type="button" value="Search"/> <input type="button" value="Close"/>		

Item	Description	sample
FTP Server	The FTP IP address	192.168.1.249
FTP User	The FTP user account	
URL	Uniform Resource Locator.	www.yahoo.com.au
Telnet User	The user account	
Other	Searching the related information from all data type by the keyword.	Movie, casper, Tom

Example 1

Searching the records belonged to the specific source IP.

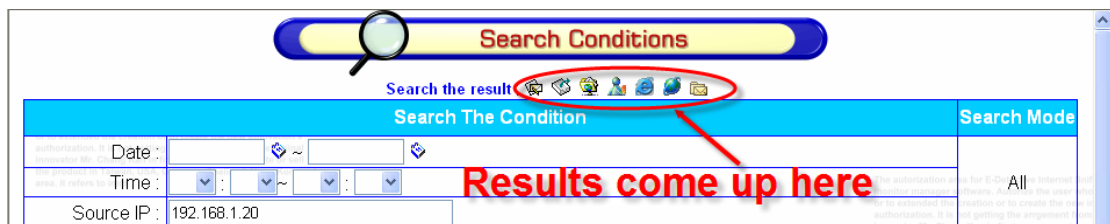
Step 1: Type the Source IP “192.168.1.20” and press the button [search].



The screenshot shows a web interface titled "Search Conditions". At the top, there is a search bar with a magnifying glass icon. Below it is a form with the following fields:

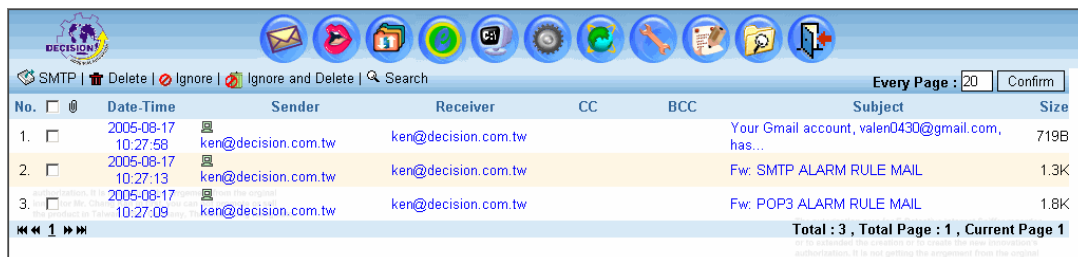
Search The Condition		Search Mode
Date :	<input type="text"/> ~ <input type="text"/>	All
Time :	<input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/>	
Source IP :	<input type="text" value="192.168.1.20"/>	
E-Mail Address :	<input type="checkbox"/> Sender <input type="checkbox"/> Receiver <input type="checkbox"/> CC <input type="checkbox"/> BCC	

Step 2: Result will be shown.



The screenshot shows the same "Search Conditions" form as in Step 1. A magnifying glass is over the search button. A red circle highlights a set of icons (SMTP, POP3, IMAP, etc.) above the form. A red arrow points from the text "Results come up here" to the icons.

Step 3: Press the SMTP icon above, the records will be shown as the following diagram.



The screenshot shows the results of a search for SMTP records. The table has the following columns: No., Date-Time, Sender, Receiver, CC, BCC, Subject, and Size. The results are as follows:

No.	Date-Time	Sender	Receiver	CC	BCC	Subject	Size
1.	2005-08-17 10:27:58	ken@decision.com.tw	ken@decision.com.tw			Your Gmail account, valen0430@gmail.com, has...	719B
2.	2005-08-17 10:27:13	ken@decision.com.tw	ken@decision.com.tw			Fw: SMTP ALARM RULE MAIL	1.3K
3.	2005-08-17 10:27:09	ken@decision.com.tw	ken@decision.com.tw			Fw: POP3 ALARM RULE MAIL	1.8K

At the bottom of the table, it says "Total : 3 , Total Page : 1 , Current Page 1".

Example 2

Searching the records belonged to the specific source IP or Msn account.

Step 1: Type the Source IP "192.168.1.20", Msn account "she0430@hotmail.com" and press the button [search].

Search The Condition		Search Mode
authorization ID : Date :	<input type="text"/> ~ <input type="text"/>	All Internet
area it refers to : Time :	<input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/>	
Source IP :	<input type="text" value="192.168.1.20"/>	USA, Germany, Thailand
E-Mail Address :	<input type="text"/>	
	<input type="checkbox"/> Sender <input type="checkbox"/> Receiver <input type="checkbox"/> CC <input type="checkbox"/> BCC	
Subject :	<input type="text"/>	
Webmail Type :	<input type="text" value="Germany, Thailand, Hong Kong, etc"/>	
FTP Server :	<input type="text"/>	
FTP User :	<input type="text"/>	
P2P Tool :	<input type="text"/>	
P2P File :	<input type="text"/>	
MSN Account :	1. <input type="text" value="she0430@hotmail.com"/> 2. <input type="text"/>	
		<input checked="" type="checkbox"/> User Handle <input checked="" type="checkbox"/> Participants

Step 2: Result will be shown.

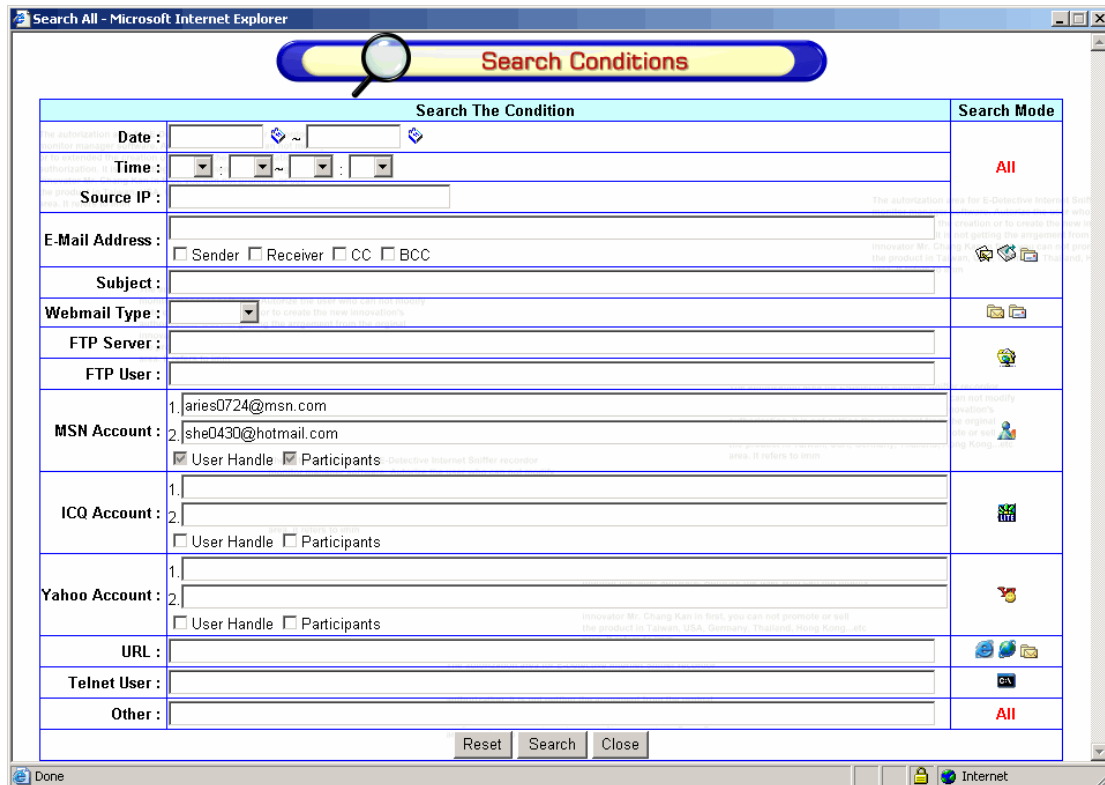
Search The Condition		Search Mode
authorization ID : Date :	<input type="text"/> ~ <input type="text"/>	All Internet
area it refers to : Time :	<input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/>	
Source IP :	<input type="text" value="192.168.1.20"/>	USA, Germany, Thailand
E-Mail Address :	<input type="text"/>	
	<input type="checkbox"/> Sender <input type="checkbox"/> Receiver <input type="checkbox"/> CC <input type="checkbox"/> BCC	
Subject :	<input type="text"/>	
Webmail Type :	<input type="text" value="Germany, Thailand, Hong Kong, etc"/>	
FTP Server :	<input type="text"/>	
FTP User :	<input type="text"/>	
P2P Tool :	<input type="text"/>	
P2P File :	<input type="text"/>	
MSN Account :	1. <input type="text" value="she0430@hotmail.com"/> 2. <input type="text"/>	
		<input checked="" type="checkbox"/> User Handle <input checked="" type="checkbox"/> Participants

Step 3: Press the MSN icon above, the records will be shown as the following diagram.

No.	<input type="checkbox"/>	<input type="checkbox"/>	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	<input type="checkbox"/>	<input type="checkbox"/>	2007-04-24 08:39:42	192.168.1.20	she0430@hotmail.com	kenlee6979@hotmail.com	Conversation	23
2.	<input type="checkbox"/>	<input type="checkbox"/>	2007-04-24 08:31:48	192.168.1.20	she0430@hotmail.com	ssm3188@hotmail.com	Conversation	0
3.	<input type="checkbox"/>	<input type="checkbox"/>	2007-04-23 14:56:08	192.168.1.20	she0430@hotmail.com	sunny624@pchome.com.tw	Conversation	2
4.	<input type="checkbox"/>	<input type="checkbox"/>	2007-04-23 14:18:47	192.168.1.20	she0430@hotmail.com	test3@decision.com.tw	Conversation	5

Example 3

Searching the records belonged to the specific Msn account.



The data finding based on the searching statement is user reference account and participant reference account. User reference account as [aries0724@msn.com] and participant reference account [she0343@hotmail.com].

No.	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19
2.	2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

Total : 2 , Total Page : 1 , Current Page 1

So it can categorize as two combined groups:

1. User reference account as [aries0724@msn.com] and participant reference account [she0343@hotmail.com].
2. User reference account as [she0343@hotmail.com] and participant reference account [aries0724@msn.com].

Language instruction:

When you key in two textbox column, the first textbox column is as single account [dc@decision.com.tw], the second textbox column is as single account [web@decision.com], then checkbox column will be enable, but it is not allow to modify and searching the data like as below:

[(user reference account = dc@decision.com.tw and participant reference account = web@decision.com.tw) or (participant reference account = web@decision.com.tw and user reference account = dc@decision.com.tw)], then use "and" combining the other searching coulums.

Example 4

Key in two or three user reference accounts and one participant reference account at MSN/ ICQ/ YAHOO. [Select the pre-setting both reference accounts of source and destination. The first column is for user reference account (of source) and the other is for participant reference account (of destination)].

The data finding based on the searching statement are user reference account [aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinet.net] and participant reference account aries0724@msn.com].

No.	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	2005-08-17 15:13:24	192.168.1.25	dc040201@hotmail.com	she0430@hotmail.com	Conversation	3
2.	2005-08-17 11:50:00	192.168.1.33	diesis@ms62.hinet.net	she0430@hotmail.com	Conversation	18
3.	2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

Total : 3 , Total Page : 1 , Current Page 1

So it can categorize as three combined groups:

1. User reference account as [aries0724@msn.com] and participant reference

account [she0343@hotmail.com].

2. User reference account as [dc040201@hotmail.com] and participant reference account [she0430@hotmail.com].
3. User reference account as [diesis@ms62.hinet.net] and participant reference account [she0430@hotmail.com].

Language instruction:

When you key in two textbox column, the first textbox column is as [web@decision.com.tw ; ken@decision.com.tw] for multi-account (maximum only 3 multi-account), the second textbox column is as single account [web@decision.com] , then checkbox column will be enable, but it is not allow to modify and searching the data like as below :

[(Participant reference account = dc@decision.com.tw and user reference account = web@decision.com.tw) or (user reference account = ken@decision.com.tw)], then use "and" combining the other searching column.

Example 5

Key in one user reference account and two or three participant reference accounts at MSN/ ICQ/ YAHOO. [Select the pre-setting both reference accounts of source and destination, the first column is for user reference account (of source) and another one is for participant reference account (of destination)].

Search The Condition		Search Mode
Date :	<input type="text"/>	All
Time :	<input type="text"/>	
Source IP :	<input type="text"/>	
E-Mail Address :	<input type="text"/>	
Subject :	<input type="text"/>	
Webmail Type :	<input type="text"/>	
FTP Server :	<input type="text"/>	
FTP User :	<input type="text"/>	
MSN Account :	1. she0430@hotmail.com 2. aries0724@msn.com; dc040201@hotmail.com; diesis@ms62.hinet.net <input checked="" type="checkbox"/> User Handle <input checked="" type="checkbox"/> Participants	
ICQ Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
Yahoo Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
URL :	<input type="text"/>	
Telnet User :	<input type="text"/>	
Other :	<input type="text"/>	All

The data finding based on the searching statement are user reference account [she0430@hotmail.com] and participant reference account [aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinet.net].

No.	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
2.	2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@ms62.hinet.net	Conversation	18
3.	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19

Total : 3 , Total Page : 1 , Current Page 1

So it can categorize as three combined groups:

1. User reference account as [she0343@hotmail.com] and participant reference account [aries0724@msn.com]
2. User reference account as [she0430@hotmail.com] and participant reference account [dc040201@hotmail.com]
3. User reference account as [she0430@hotmail.com] and participant reference account [diesis@ms62.hinet.net]

Language instruction:

When you key in two textbox column, the first textbox column is as single account dc@decision.com.tw , the second textbox column is as multi-account [web@decision.com]; ken@decision.com.tw (maximum only 3 multi-account) , then checkbox column will be enable, but it is not allowed to modify and searching the data like as below :

User reference account = dc@decision.com.tw and participant reference account = web@decision.com.tw or participant reference account = ken@decision.com.tw, then use "and" combining the other searching column.

Example 6

Key in two or three user reference accounts and without key in participant reference account at MSN/ ICQ/ YAHOO. [Key in the account can be selected by pre-setting either user reference account or participant reference account or both. The first column is for user reference account (of source) and other is for participant reference account (of destination)].

The data finding based on the searching statement are user reference account or participant reference account [aries0724@msn.com or dc040201@hotmail.com or diesis@ms62.hinet.net].

No.	<input type="checkbox"/>	<input type="checkbox"/>	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 15:18:50	192.168.1.25	dc040201@hotmail.com	aries0724@msn.com	Conversation	3
2.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 15:18:50	192.168.1.10	aries0724@msn.com	dc040201@hotmail.com	Conversation	2
3.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
4.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 13:46:03	192.168.1.33	diesis@ms62.hinet.net	aries0724@msn.com	Conversation	3
5.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 13:46:03	192.168.1.10	aries0724@msn.com	diesis@ms62.hinet.net	Conversation	2
6.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 12:08:26	192.168.1.33	office_vic@hotmail.com	diesis@ms62.hinet.net	Conversation	3
7.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@ms62.hinet.net	Conversation	18
8.	<input type="checkbox"/>	<input type="checkbox"/>	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19

Total : 8 , Total Page : 1 , Current Page 1

So it can categorize as six combined groups:

1. User reference account as [aries0724@msn.com] and participant reference account will be as any account.
2. User reference account as [dc040201@hotmail.com] and participant reference account will be as any account.
3. User reference account as [diesis@ms62.hinet.net] and participant reference account will be as any account.
4. User reference account will be as any account and participant reference account as [aries0724@msn.com]
5. User reference account will be as any account and participant reference account as [dc040201@hotmail.com]
6. User reference account will be as any account and participant reference account as [diesis@ms62.hinet.net]

Language instruction:

1. When you key in the first textbox column as multi-account [dc@decision.com.tw, web@decision.com.tw] (maximum only 3 multi-account), then checkbox column will be enabled, the data will be searched like as below:
(user reference account = dc@decision.com.tw or user reference account = web@decision.com.tw), then use "and" combining the other searching coulumn.
2. When you key in the first textbox column as multi-account [dc@decision.com.tw, web@decision.com.tw] (maximum only 3 multi-account), then only select the participant account at checkbox column, the data will be serached like as below:
(participant reference account = dc@decision.com.tw or participant reference account = web@decision.com.tw) , then use "and" combining the other searching coulumn.
3. When you key in the first textbox column as multi-account [dc@decision.com.tw, web@decision.com.tw] (maximum only 3 multi-account), then select the participant account and user reference account at check box column, the data will be searched like as below:
(user reference account = dc@decision.com.tw or participant reference account = web@decision.com.tw or participant reference account = dc@decision.com.tw or user reference account = web@decision.com.tw) , then use "and" combining the other searching coulumn.

Example 7

Key in one user reference account and without key in participant reference account at MSN/ ICQ/ YAHOO. [Key in the account can be selected by pre-setting either user reference account or participant reference account or both. The first column is for user reference account (of source) and other is for participant reference account (of destination)].

The data finding based on the searching statement are user reference account or participant reference account [she0430@hotmail.com]

No.	☐	Ⓜ	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	☐	Ⓜ	2005-08-17 17:39:26	192.168.1.14	sevenrx8@hotmail.com	she0430@hotmail.com	Conversation	3
2.	☐	Ⓜ	2005-08-17 15:37:23	192.168.1.20	she0430@hotmail.com	wueden@hotmail.com	Conversation	3
3.	☐	Ⓜ	2005-08-17 15:13:24	192.168.1.25	dc040201@hotmail.com	she0430@hotmail.com	Conversation	3
4.	☐	Ⓜ	2005-08-17 15:13:24	192.168.1.20	she0430@hotmail.com	dc040201@hotmail.com	Conversation	2
5.	☐	Ⓜ	2005-08-17 15:03:39	192.168.1.20	she0430@hotmail.com	milkmay0935@hotmail.com	Conversation	2
6.	☐	Ⓜ	2005-08-17 14:35:11	192.168.1.20	she0430@hotmail.com	mptom007@hotmail.com	Conversation	3
7.	☐	Ⓜ	2005-08-17 13:51:53	192.168.1.20	she0430@hotmail.com	flyinghunters@hotmail.com	Conversation	3
8.	☐	Ⓜ	2005-08-17 13:47:47	192.168.1.20	she0430@hotmail.com	alexlin4@msn.com	Conversation	32
9.	☐	Ⓜ	2005-08-17 11:50:00	192.168.1.33	diesis@ms62.hinet.net	she0430@hotmail.com	Conversation	18
10.	☐	Ⓜ	2005-08-17 11:50:00	192.168.1.20	she0430@hotmail.com	diesis@ms62.hinet.net	Conversation	18
11.	☐	Ⓜ	2005-08-17 11:22:02	192.168.1.20	she0430@hotmail.com	aries0724@msn.com	Conversation	19
12.	☐	Ⓜ	2005-08-17 11:22:02	192.168.1.10	aries0724@msn.com	she0430@hotmail.com	Conversation	20

Total : 12 , Total Page : 1 , Current Page 1

So it can categorize as two combined groups:

1. User reference account as [she0430@hotmail.com] and participant reference account will be as any account.
2. User reference account will be any account and participant reference account is as [she0430@hotmail.com]

Language instruction:

1. When you key in the first textbox column as single account [dc@decision.com.tw] , then checkbox column will be selected only user reference account and serached the data like as below:
(user reference account = dc@decision.com.tw) then use "and" combining the other searching coulmn.
2. When you key in the first textbox column as single account [dc@decision.com.tw] , then checkbox column will be selected only participant reference account and serached the data like as below:
(participant reference account = dc@decision.com.tw) then use "and" combining the other searching coulmn.
3. When you key in the first textbox column as single account [dc@decision.com.tw] , then checkbox column will be selected both user reference account and participant reference account, then the data will be serached like as below:
(user reference account = dc@decision.com.tw or participant reference account = dc@decision.com.tw) , then use "and" combining the other searching coulmn.

K. Reporting

E-Detective support completely strategic decision control of chart and report. It can use user's requirement to set multi strategic decision analysis control report. By these detail analysis data, you may easily judge and understand more for using the internet activities and take advantage of the work efficiency.

The report can classify as:

1. Single functional report (Single Report)
(eg. IP of HTTP, the receiver of POP3 ...etc)
2. Group IP with Group Report (Group Report)
(eg. 192.168.0.2 and 192.168.0.5 compare with POP3, MSN, HTTP)

1. Single functional report (Single Report)

Step 1.

Identify the period that the specific mode (service) to be displayed in the report.

Mode: POP3 、SMTP 、FTP 、MSN 、ICQ 、YAHOO 、HTTP 、DYNAMIC 、WEBMAILR 、WEBMAILS 、TELNET

https://202.39.29.27 - Report - Microsoft Internet Explorer

Mode : POP3 Field : Date-Time

Start Date : 2005-09-01 00 : 00

End Date : 2005-09-28 23 : 59 Search

Please Click Search Button

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify or to extended the creation or to create the new innovation's authorization. It is not getting the arrangement from the original innovator Mr. Chang Kan in first, you can not promote or sell the product in Taiwan, USA, Germany, Thailand, Hong Kong...etc area. It refers to immn

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify or to extended the creation or to create the new innovation's

https://202.39.29.27 - Report - Microsoft Internet Explorer

Mode: POP3 Field: Date-Time

Start Date: 2005-09-01 00:00

End Date: 2005-09-28 23:59

Search

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify

Show Chart Every Page: 10 confirm

No.	Date-Time↓	Count	File count	File size
1	2005-09-08	2	0	60.5K
2	2005-09-09	4	0	102.3K
3	2005-09-15	2	0	62.6K
4	2005-09-19	6	0	164.7K
5	2005-09-27	39	34	1.2M

Navigation: << 1 >>> Total: 5, Total Page: 1, Current Page 1

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify or to extended the creation or to create the new innovation's

Step 2.

Show Chart

https://202.39.29.27 - Report - Microsoft Internet Explorer

Mode: POP3 Field: Date-Time

Start Date: 2005-09-01 00:00

End Date: 2005-09-28 23:59

Search

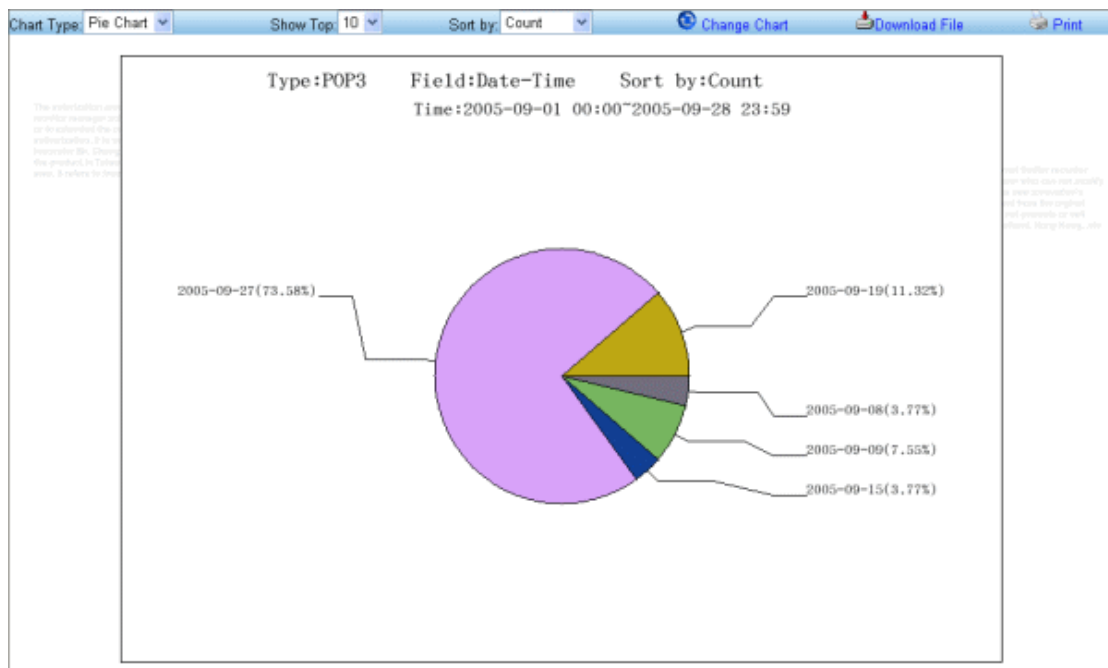
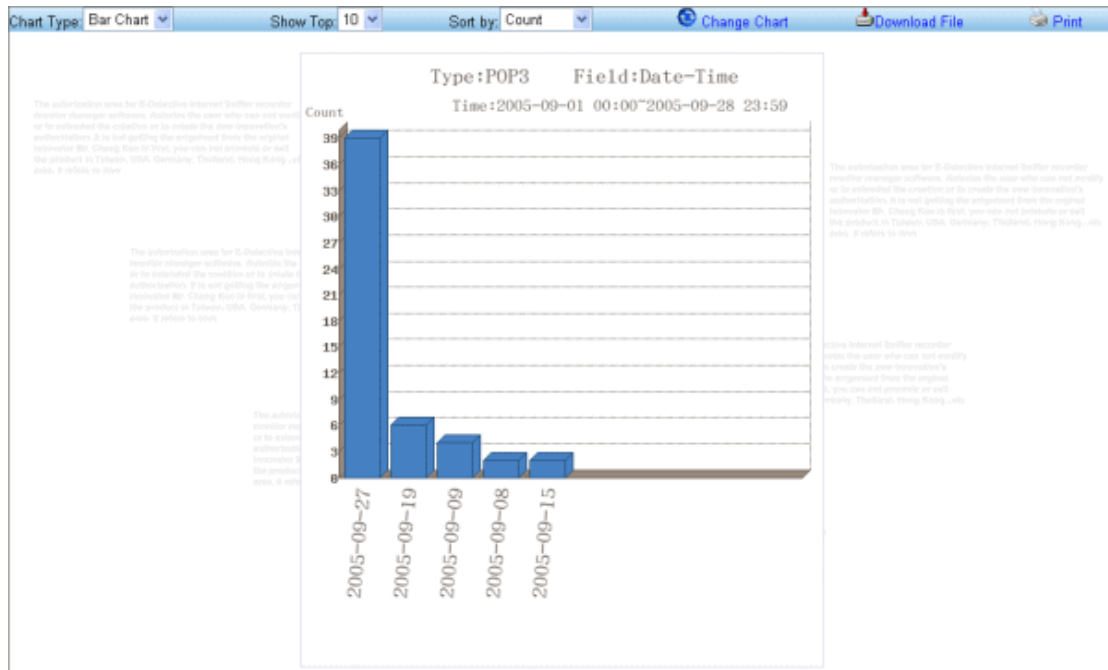
The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify

Show Chart Click Every Page: 10 confirm

No.	Date-Time↓	Count	File count	File size
1	2005-09-08	2	0	60.5K
2	2005-09-09	4	0	102.3K
3	2005-09-15	2	0	62.6K
4	2005-09-19	6	0	164.7K
5	2005-09-27	39	34	1.2M

Navigation: << 1 >>> Total: 5, Total Page: 1, Current Page 1

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify or to extended the creation or to create the new innovation's



Here can select

Chart Type :

- Bar Chart
- Pie Chart

Show Top : Can select to display the first 10, 20, 30 data.

Sort by : data type

- Count : total data.
- File count : all included attached file data.
- File size : all included attached file size.

Change Chart

Select Chart Type, Show Top, Sort by. Click Change Chart then can display you the type you would like to display.

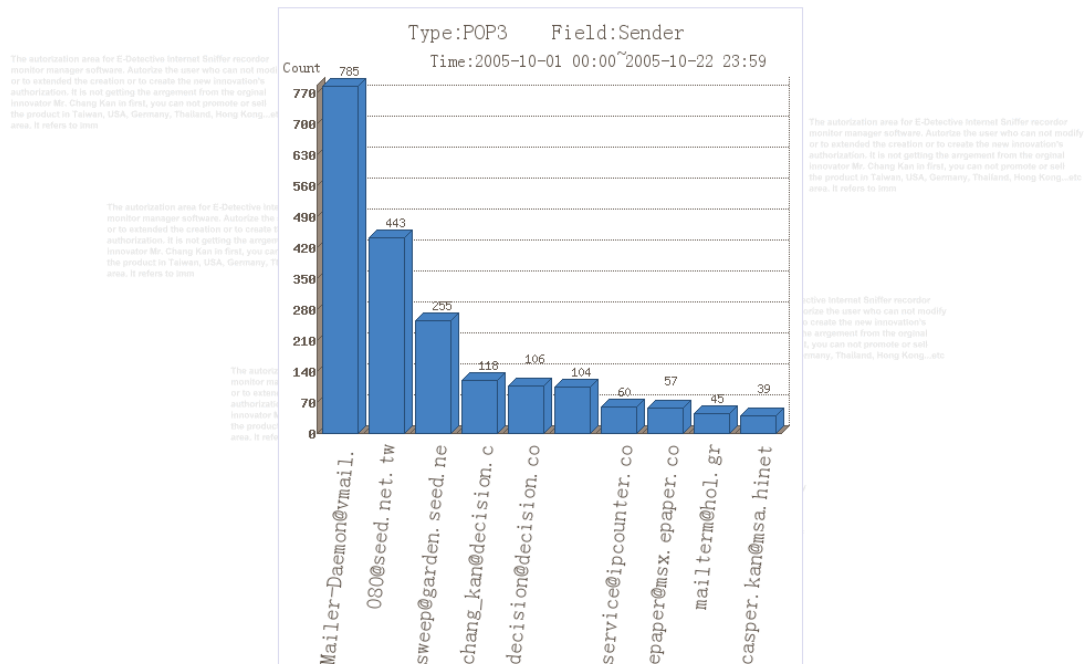
Download File

After clipping, it can download the file that shown on the present chart figure (.png).

Print

After clipping, it can print out the present chart figure.

Note : Because the charset of sender and receiver of POP3, SMTP , webmail , and the user handle and participants of YAHOO is not saved by unicode. When showing the chart, you can choose the correct charset (unicode, big5, gb2312)



2. Group IP with Group Report (Group Report)

The screenshot shows a web browser window with the URL `https://202.39.29.27 - Report - Microsoft Internet Explorer`. The interface includes the following elements:

- 1**: A bar chart icon labeled "To Single".
- 2**: A date range selector showing "Date: 2005-10-01 00:00 ~ 2005-10-08 23:59".
- 3**: A "Protocol:" section with checkboxes for POP3, SMTP, FTP, MSN, ICQ, YAHOO, HTTP, DYNAMIC, WEBMAILR, WEBMAILS, and TELNET.
- 4**: An "IP:" text input field.
- 5**: An "IP List:" dropdown menu with options "All IP" and "Selected IP".
- 6**: A "Show Chart" button.
- 7**: A table with columns "No." and "IP".
- 8**: A "confirm" button.
- 9**: A "Total : 35 , Total Page : 4 , Current Page 1" summary.

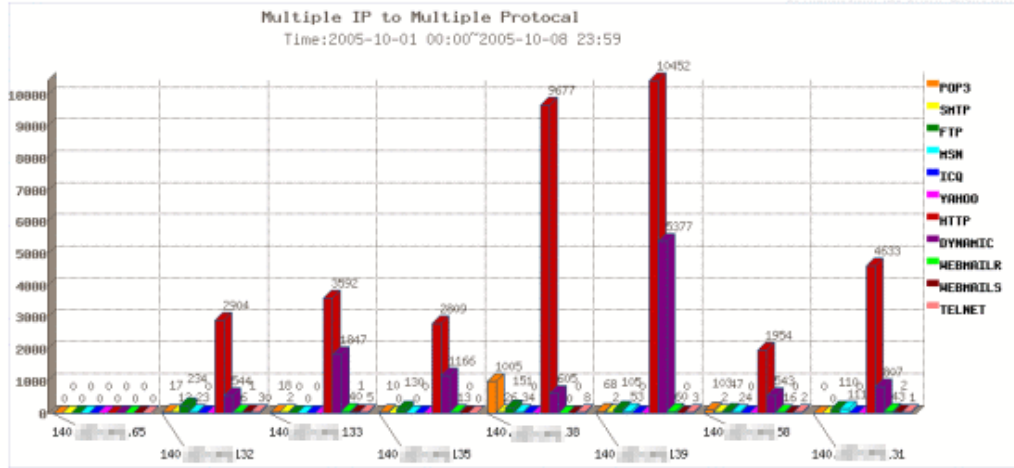
No.	IP
1	192.168.1.12
2	192.168.1.16
3	192.168.1.17
4	192.168.1.18
5	192.168.1.201
6	192.168.1.202
7	192.168.1.203
8	192.168.1.204
9	192.168.1.206
10	192.168.1.207

After select Group Report, it will display the following Group Report list

- [1] : Select the icon to directly connect to Single Report.
- [2] : The report given by the setting is for date.
- [3] : Select the report needs to statistic which type (default setting: ALL, it can choice multiple)
- [4] : Can add the new IP by manual. After key in the IP at the back of the text box, clip the mouse at the blank space on the screem, then the key in IP will be added in the IP list.
- [5] : IP list will be listed out the moment statistic IP. The selected IP (was blocked) will make into a statistic list at next page (default setting: ALL)
- [6] : Can be deleted the data that listed in the IP. There has two ways you can delete all or delete as you select.
- [7] : The record IP list that have listed in the present E-Detective system.
- [8] : By using the mouse to select any IP, it can be added the IP to the new IP list, the maximum can be selected 10 IP.
- [9] : Display the figure.

Copyright © 2007 Decision Computer International Co., Ltd

Show Value		Not Show Value		Download File										Print
IP#		POP3	SMTP	FTP	MSN	ICQ	YAHOO	HTTP	DYNAMIC	WEBMAILR	WEBMAILS	TELNET		
140	65	0	0	0	0	0	0	0	0	0	0	0		
140	32	17	12	234	23	0	0	2904	544	6	1	30		
140	33	18	2	0	0	0	0	3592	1847	40	1	5		
140	35	10	0	130	0	0	0	2809	1166	13	0	0		
140	38	1005	26	151	34	0	0	9677	605	0	0	8		
140	39	68	2	105	53	0	0	10452	5377	60	0	3		
140	58	103	2	47	24	0	0	1954	543	16	0	2		
140	31	0	0	110	111	0	0	4633	807	43	2	1		



Appendix A: Q&A

- e. I can not see any recording data after installation?

A:

1. Make sure if you registered. When register success, OpenRaw will execute.

Please input instructions at local host.

```
edetective:/# ps -x | grep OpenRaw
```

[This “|” is “Shift+”\”]

If OpenRaw is running correctly, you can see the following message.

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

```
./OpenRaw -t /datas/rawdata -i ethX
```

2. Please verify that system detect PCI WatchDog Card.

Please input the instruction at local host.

```
edetective:/# lspci -n | grep 6666
```

[This “|” is “Shift+”\”]

If PCI WatchDog Card is installed correctly; you can see the following message.

```
Class 1180: 6666:4100 (rev 02)
```

3. Please verify that there is IP address in “Online IP List”.

Note: Local host means you should directly connect monitor and keyboard to E-Detective server.

- f. How to change IP?

A:

Local Host: Please refer to “Installation Guide” “Chapter 4. System Configuration”;

Remote Control: Please refer to “ SETTING → Network Set ” in “User Manual” “Chapter 2. E-Detective Function Description”.

g. How to install hardware? Which mode is fit for Customer needs?

A: Please refer to "Installation Guide" "Chapter 2. Appliance Deployment".

Note: If you choose Mirror Mode, Switch Hub should provide mirror function.

h. Can not backup "E-Detective" data? Or can not burn CD?

A: Please make sure your CD-ROM is installed in IDE2 or 1st slot of the second bus wire.

i. Why files captured from FTP are *.txt?

A: Please right-click and select "save file as", then modify the extension to *.jpg, *.pdf, *.rar...etc.

j. Can not capture data from MSN, ICQ or AOL server?

A: Please open port 1863 and 5190 on firewall.

k. Can not access "E-Detective" by browser after turn on "E-Detective"?

A: Please login by "https://" not http://, e.g. https://192.168.1.60.

l. Only see IP address of Proxy server in records if I use Proxy server in gateway. Is it correct?

A: Yes, just receive recording data of Proxy server if it is in front of gateway.

m. Why those forwarding items in E-mail records can not be forwarded after setting?

A: All the settings will be initialed after one hour, and all the columns "Sender", "Receiver" and "Topic" should fit the forwarding rules.

n. After setting network access rules, "E-Detective" doesn't show any alarm to system administrator. How come?

A: It will be active after setting new rules for one hour.

o. Can not open email directly in POP3/SMTP?

A: Please delete all the update package of "outlook express" in "add/remove program" in "Control Panel".