Decision Computer Group

HTTPS/SSL NETWORK PACKET FORENSICS DEVICE

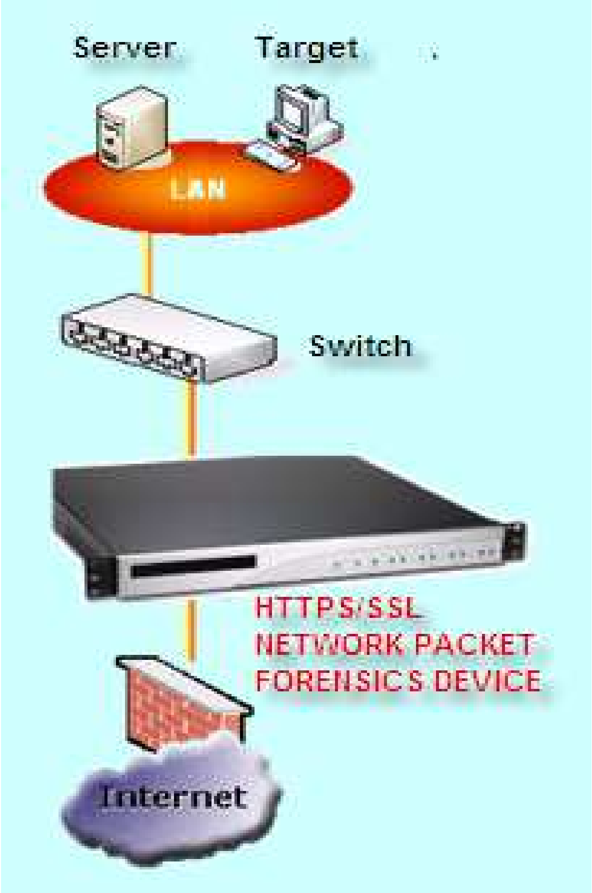
Surmounting The Peak of Computer Forensics Technology

Moving forward with the security of networking and computer forensics

E-DETECTIVE®

DECISION INDUSTRIAL AUTOMATION

HTTPS/SSL NETWORK PACKET FORENSICS DEVICE



E-DETECTIVE®

SSL(Secure Sockets Layer)

A Technical Security Standard to secure the safety of Internet packets transmitting between server and browser.

SSL is an Enterprise Standard adopted by millions of websites to safeguard their on-lined transaction. It ensures the privacy and integrity of transmitted data during the transaction process. Each web server requires one SSL certificate to protect its safety of linkage.

HTTPS - Encryption HyperText Transfer Protocol

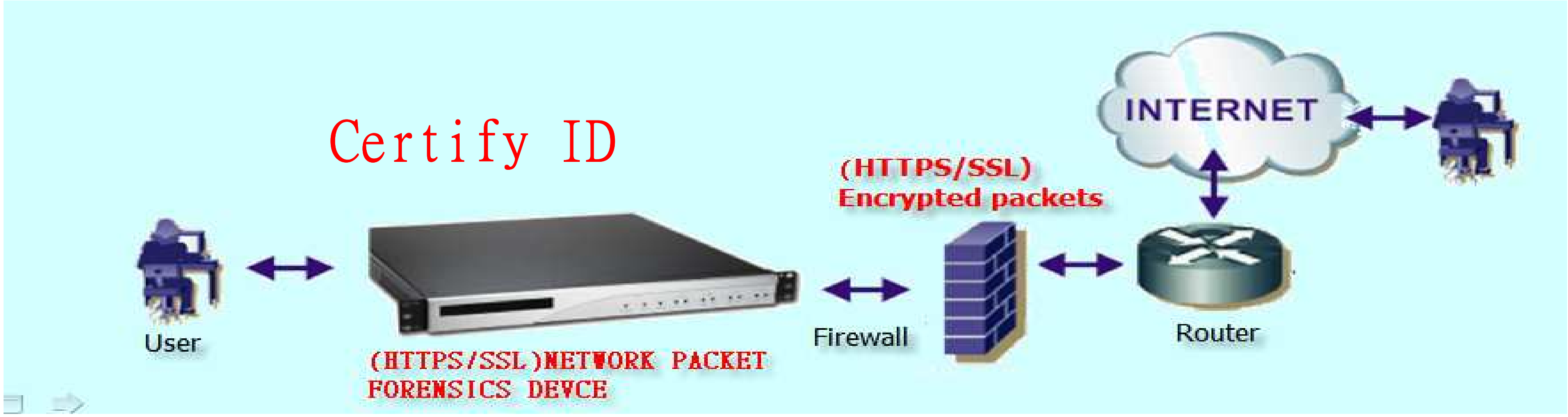
1. It is the safeguarded version of HTTP to securing the safety of transmitted data.
2. Engaged with SSL layer, the transmission of data for HTTP is fully protected to form a secured base of HTTPs.
3. HTTPs is a combination of HTTP and SSL. It does not use the HTTP's Port and is able to certify ID of each internet packet.（Between the HTTP and the TCP）。
4. HTTPs was originally developed by Netscape, it provides ways to certify IDs and encrypt the communication data.
5. SSL is often used for E-Commence System such as online payment.

Operating Theory (1)

1. Utilizing Man in the middle attack (MiTM)

or Monkey in the middle concept

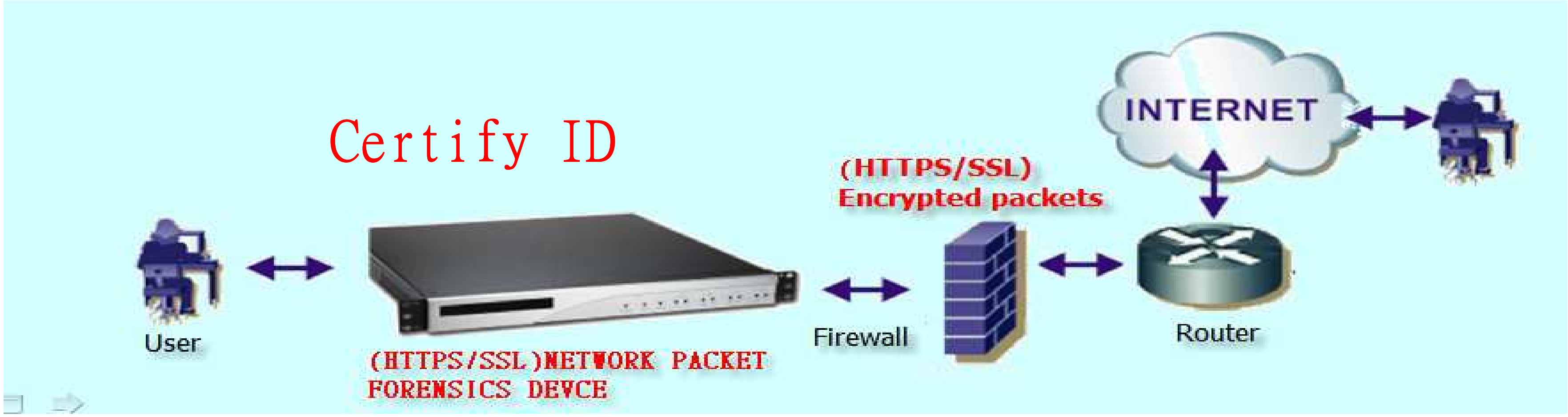
This system pretends as gateway/proxy to get public keys (Decryption/Encryption keys) by cheating when the data is transferred via Internet in order to decrypt the information.



Operating Theory (2)

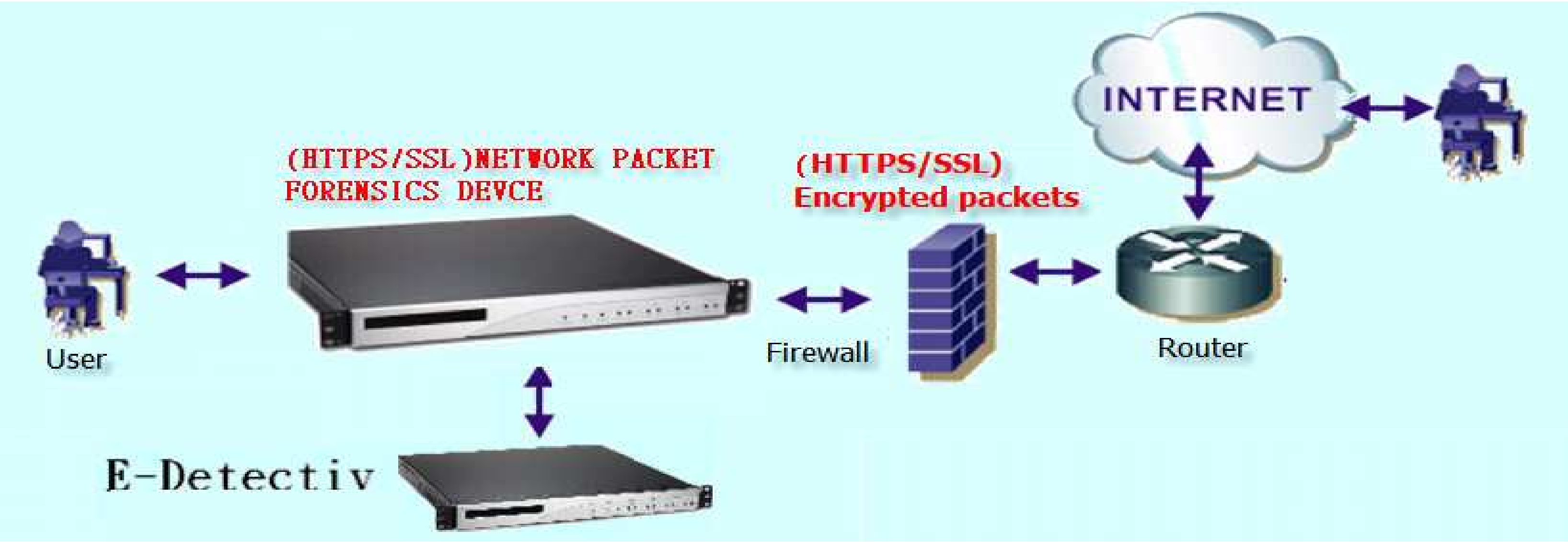
2. Offline Decryption and Decoding

HTTPS/SSL Network Forensic Device can decrypt and decode (integration with E-Detective system) HTTPS web content if the private key used is known.



Equipment Expansion

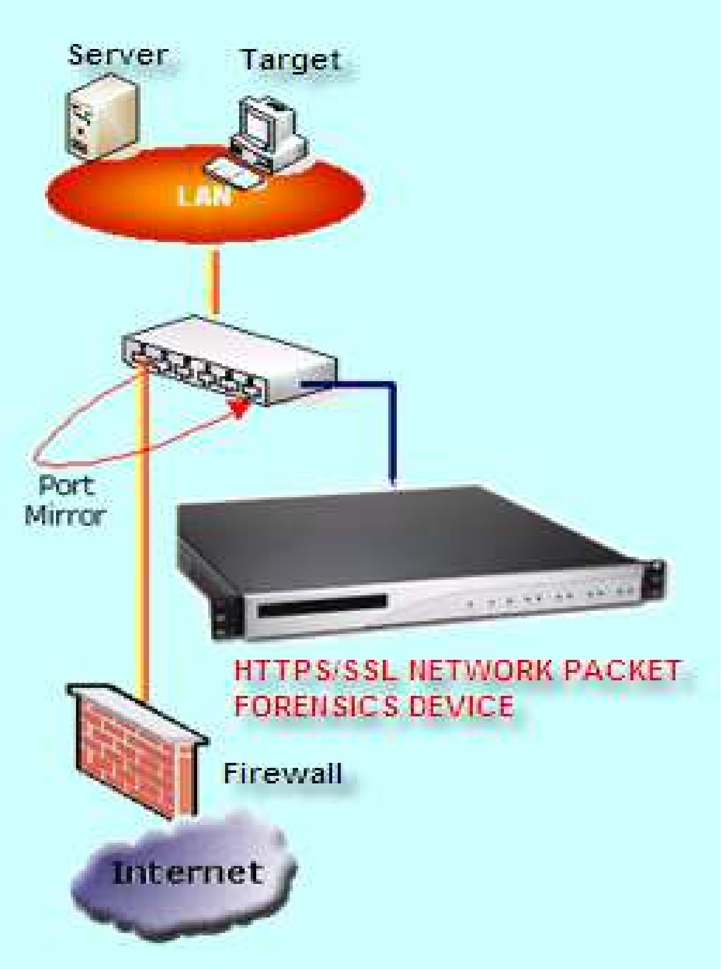
One of primary auditing features is it is able to be integrated with E-DETECTIVE system and its database, in order to exchange/decode/analyze the data. It can be integrate with E-DETECTIVE in one appliance or it can be a standalone device.



Decrypting Packets by Known Public Keys

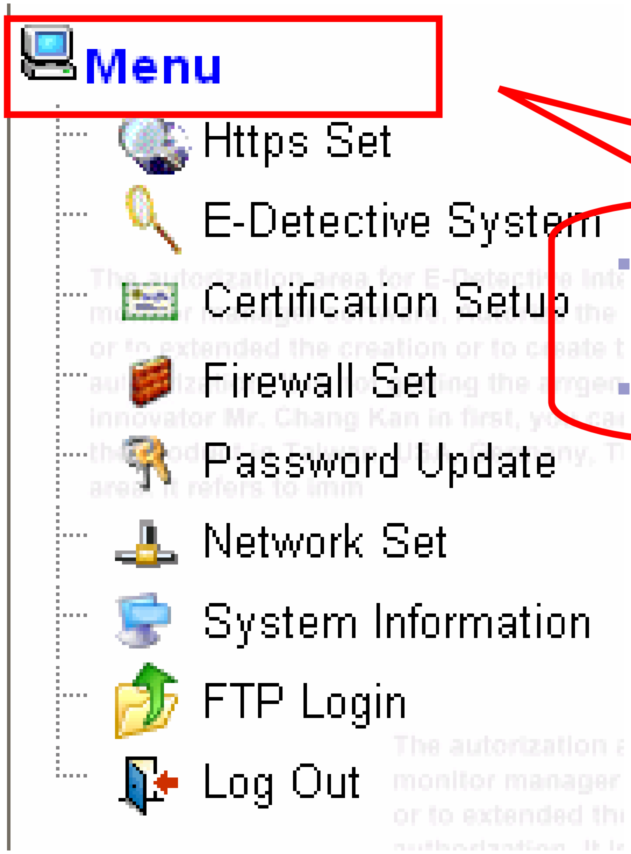
Able to Cooperate with SSL server and obtain its public keys in order to decrypt all data related to this SSL server.

Decrypting the HTTPS's packets by entering the existed authorized public keys.



User Interface

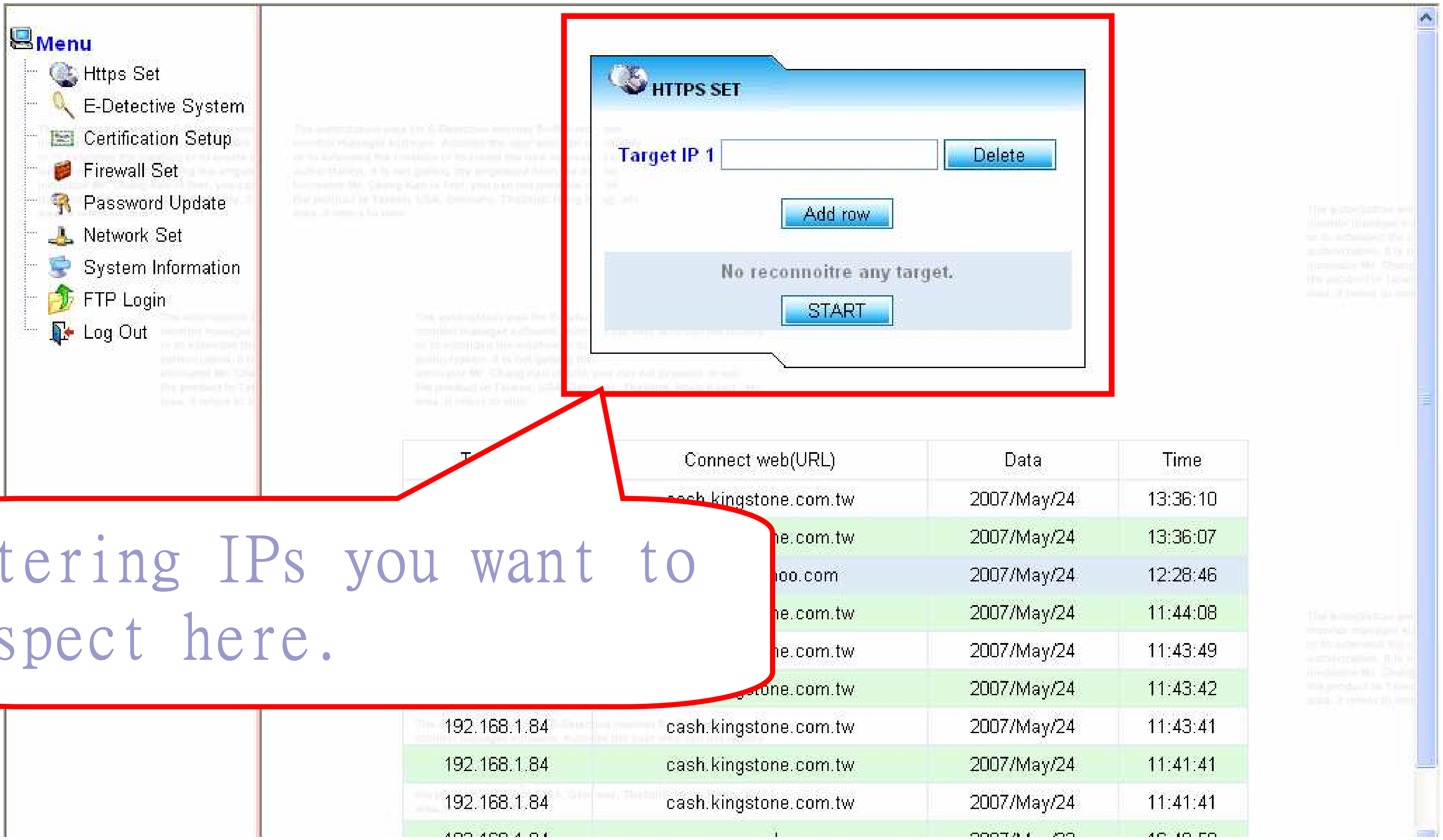
Menu – Https Set



- IP Inspection Set
- The status of IPs

User Interface

Https Set



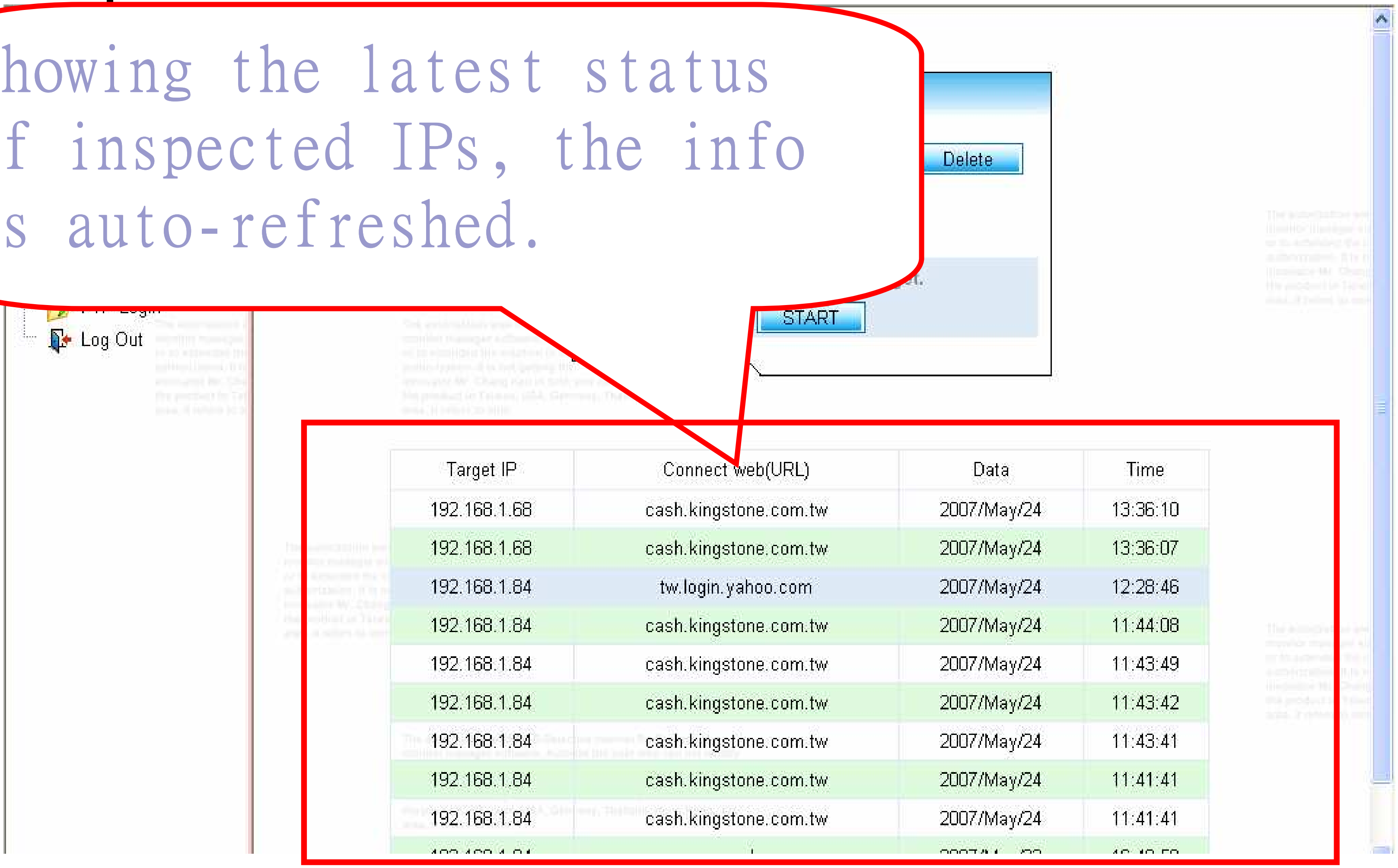
No reconnoitre any target.

T	Connect web(URL)	Data	Time
	cash.kingstone.com.tw	2007/May/24	13:36:10
	e.com.tw	2007/May/24	13:36:07
	oo.com	2007/May/24	12:28:46
	e.com.tw	2007/May/24	11:44:08
	e.com.tw	2007/May/24	11:43:49
	one.com.tw	2007/May/24	11:43:42
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:43:41
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:41:41
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:41:41

Entering IPs you want to inspect here.

User Interface

Https Set

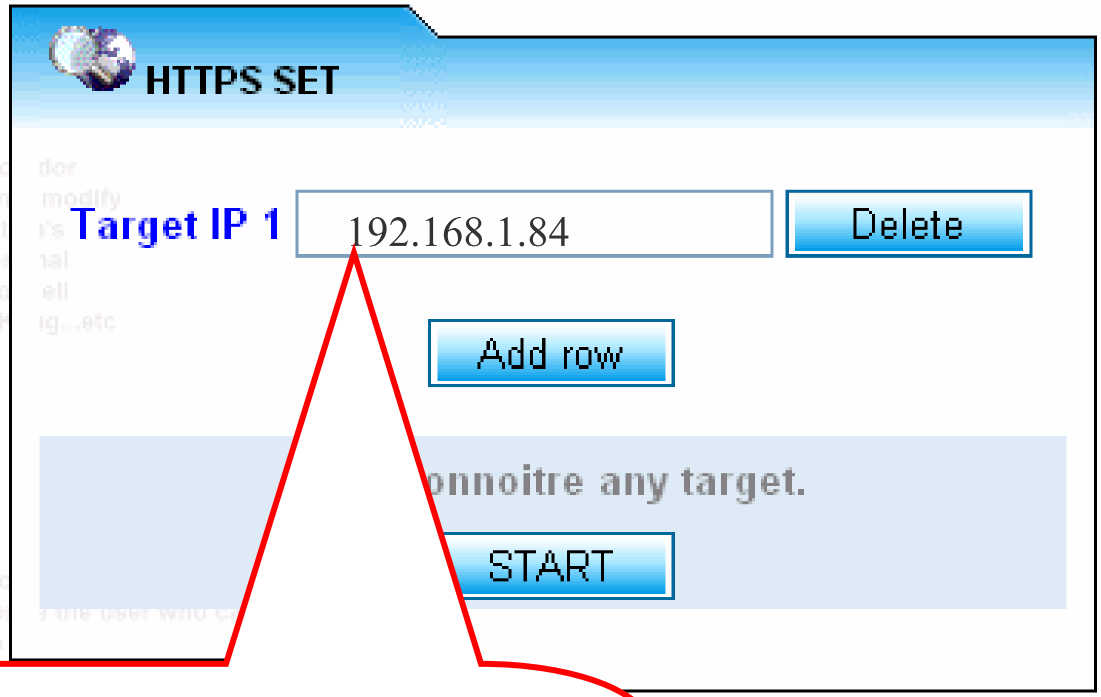


Showing the latest status of inspected IPs, the info is auto-refreshed.

Target IP	Connect web(URL)	Data	Time
192.168.1.68	cash.kingstone.com.tw	2007/May/24	13:36:10
192.168.1.68	cash.kingstone.com.tw	2007/May/24	13:36:07
192.168.1.84	tw.login.yahoo.com	2007/May/24	12:28:46
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:44:08
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:43:49
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:43:42
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:43:41
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:41:41
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:41:41

User Interface

Https Set



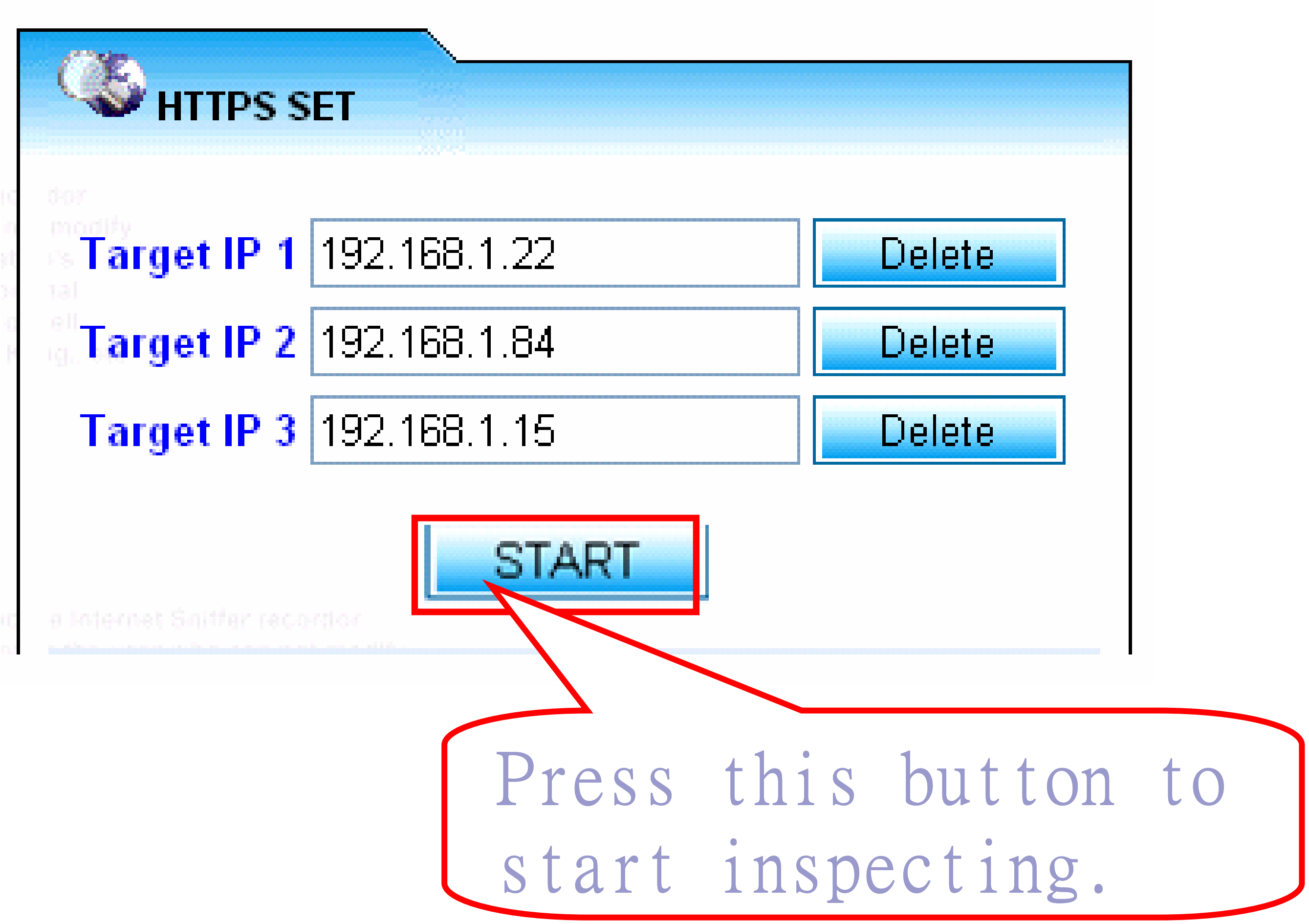
Target IP 1: 192.168.1.84

onnoitre any target.

Entering the IP on the blank field, users press the button “Add row” to add more IPs.

User Interface

Https Set



Target IP 1: 192.168.1.22

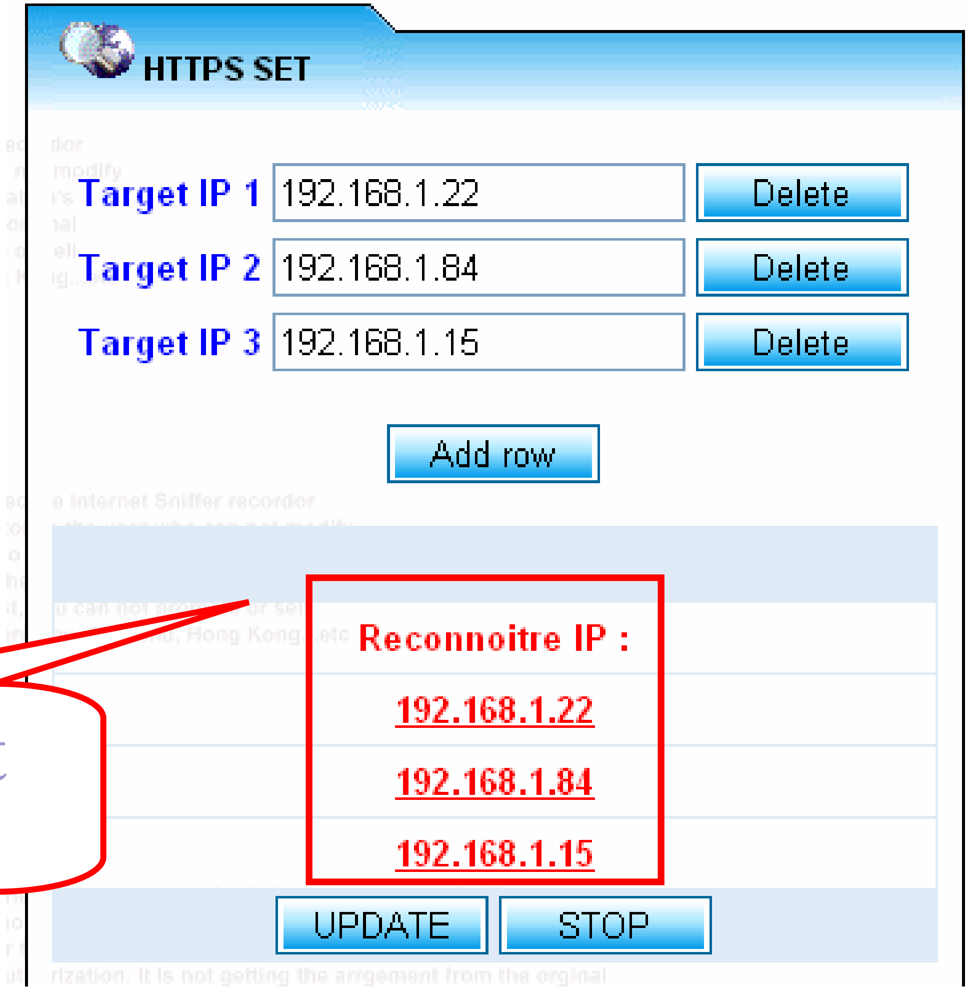
Target IP 2: 192.168.1.84

Target IP 3: 192.168.1.15

Press this button to start inspecting.

User Interface

Https Set



HTTPS SET

Target IP 1: 192.168.1.22 Delete

Target IP 2: 192.168.1.84 Delete

Target IP 3: 192.168.1.15 Delete

Add row

Reconnoitre IP :

192.168.1.22

192.168.1.84

192.168.1.15

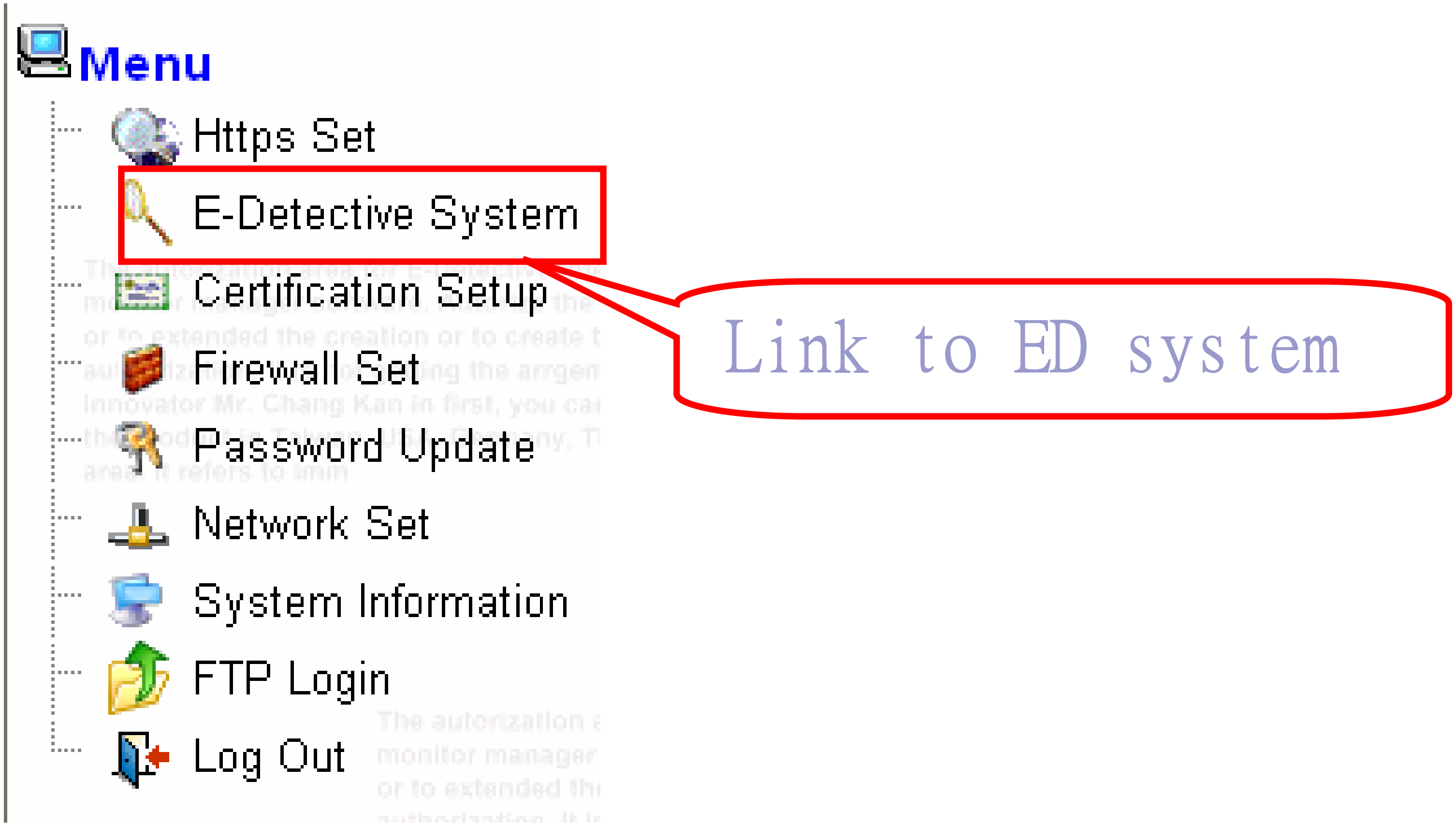
UPDATE STOP

The last input of IPs

2007/9/22

User Interface

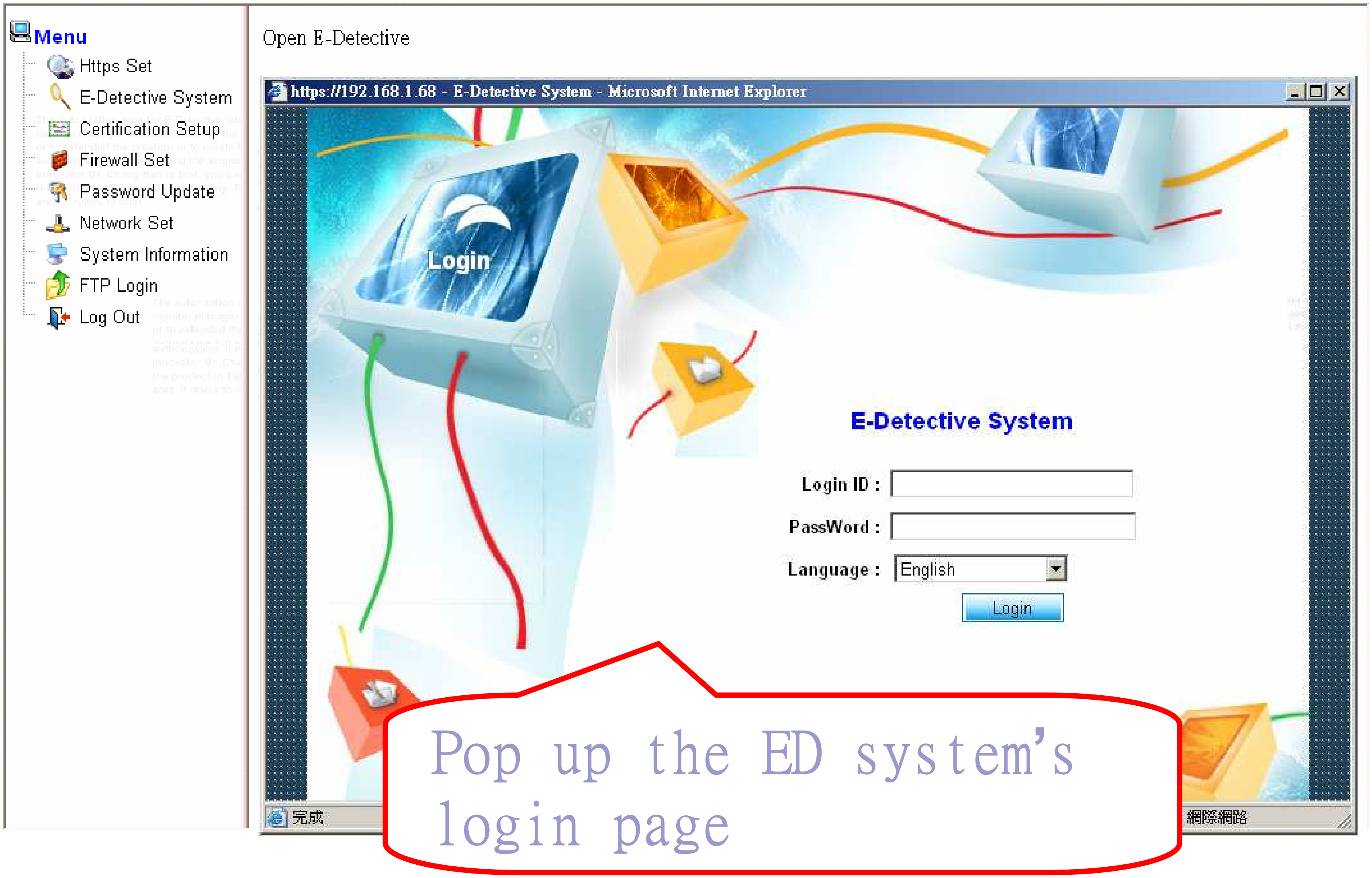
Menu – E-Detective System



Link to ED system

User Interface

E-Detective



Menu
- Https Set
- E-Detective System
- Certification Setup
- Firewall Set
- Password Update
- Network Set
- System Information
- FTP Login
- Log Out

Open E-Detective

https://192.168.1.68 - E-Detective System - Microsoft Internet Explorer

E-Detective System

Login ID :

PassWord :

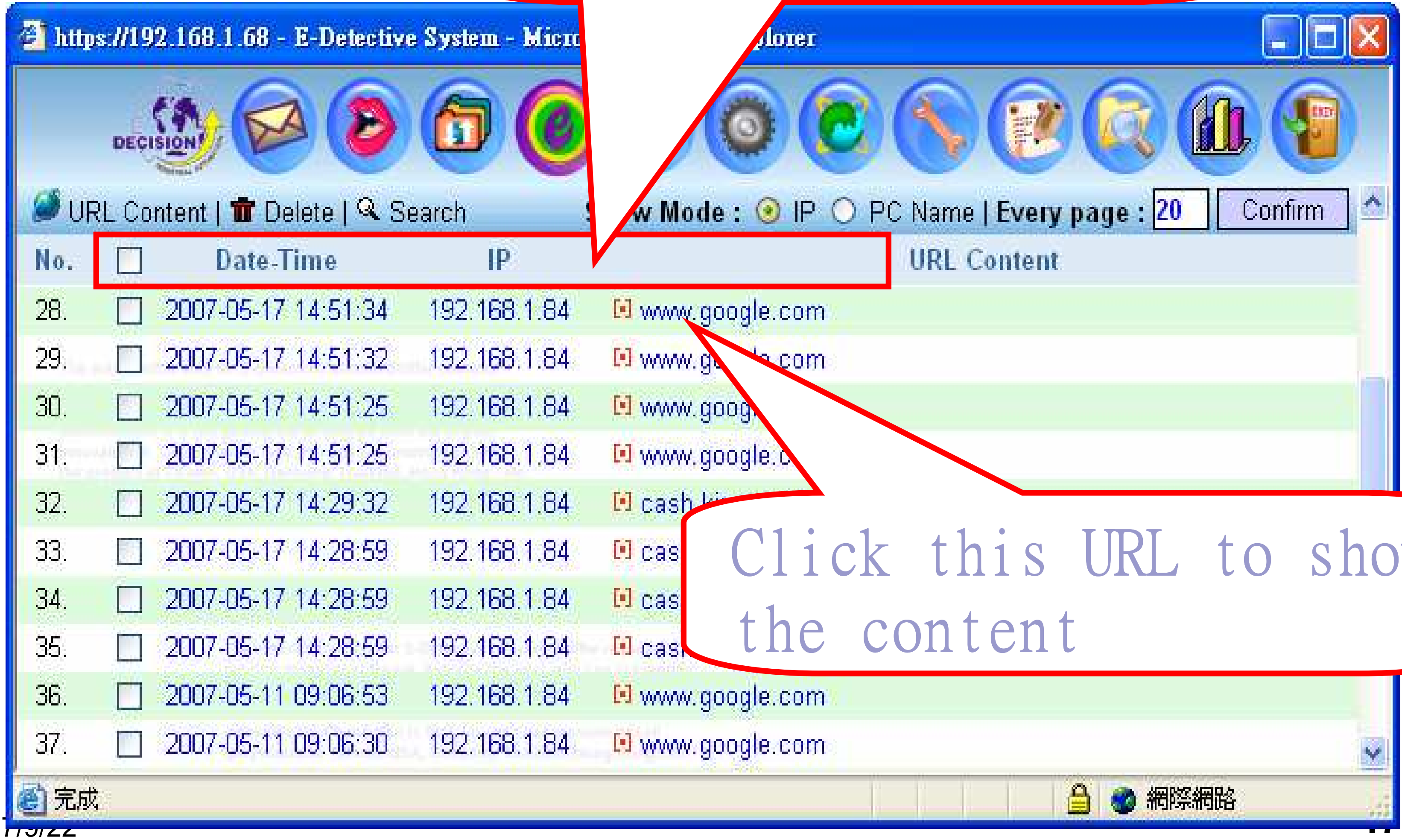
Language : English

Pop up the ED system's login page

User Interface

E-Detective

The info of Date/Time, IP, URL.



https://192.168.1.68 - E-Detective System - Micro plorer

URL Content | Delete | Search

w Mode : ● IP ○ PC Name | Every page : 20 Confirm

No.	□	Date-Time	IP	URL Content
28.	□	2007-05-17 14:51:34	192.168.1.84	www.google.com
29.	□	2007-05-17 14:51:32	192.168.1.84	www.g e.com
30.	□	2007-05-17 14:51:25	192.168.1.84	www.goog
31.	□	2007-05-17 14:51:25	192.168.1.84	www.google.c
32.	□	2007-05-17 14:29:32	192.168.1.84	cash.ki
33.	□	2007-05-17 14:28:59	192.168.1.84	cas
34.	□	2007-05-17 14:28:59	192.168.1.84	cas
35.	□	2007-05-17 14:28:59	192.168.1.84	cas
36.	□	2007-05-11 09:06:53	192.168.1.84	www.google.com
37.	□	2007-05-11 09:06:30	192.168.1.84	www.google.com

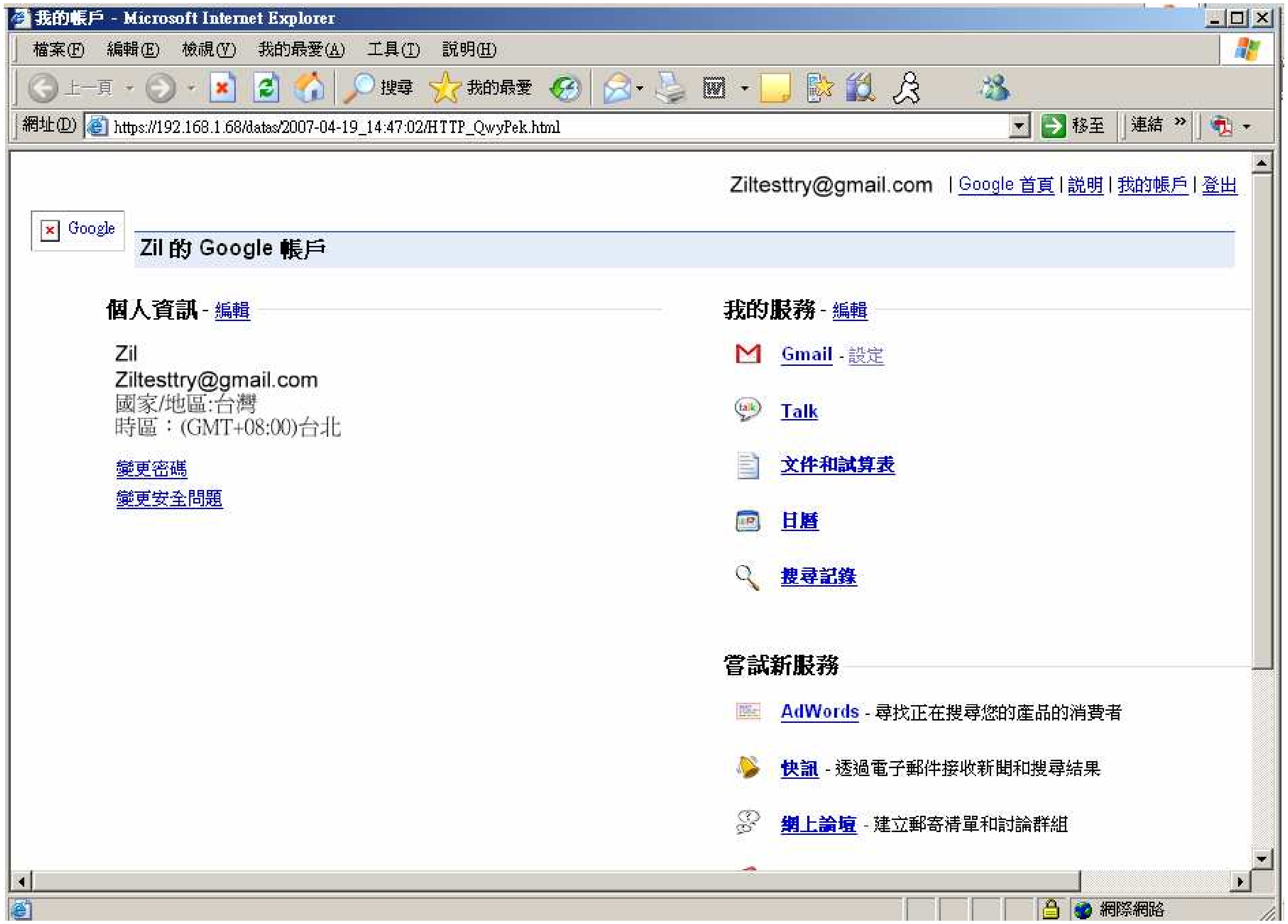
完成 網際網路

Click this URL to show the content

User Interface

E-Detective

Webpage's content


我的帳戶 - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛
網址(D)
移至 連結

https://192.168.1.68/datas/2007-04-19_14:47:02/HTTP_QwyPek.html

Ziltesttry@gmail.com | Google 首頁 | 說明 | 我的帳戶 | 登出

Google

Zil 的 Google 帳戶

個人資訊 - 編輯

Zil
Ziltesttry@gmail.com
國家/地區:台灣
時區：(GMT+08:00)台北

變更密碼
變更安全問題

我的服務 - 編輯

Gmail - 設定

Talk

文件和試算表

日曆

搜尋記錄

嘗試新服務

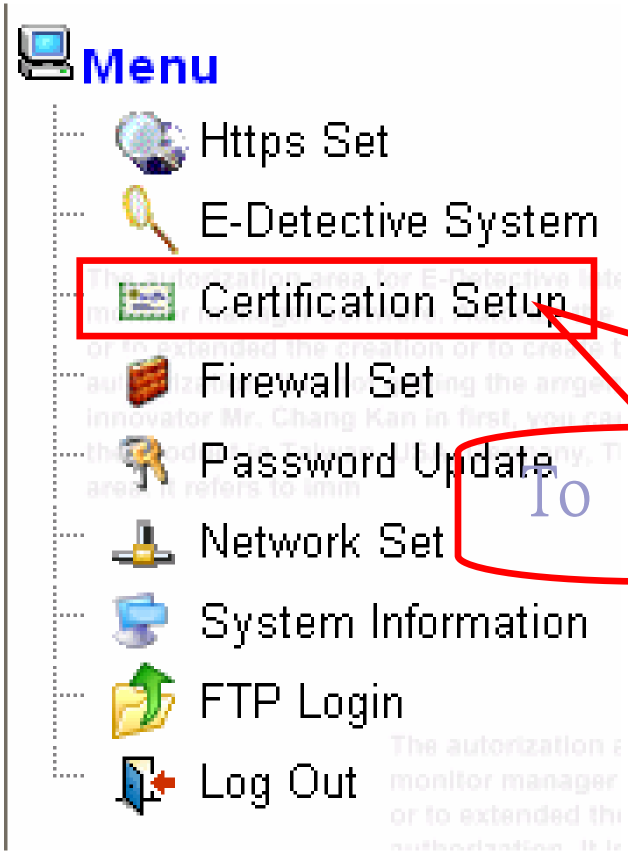
AdWords - 尋找正在搜尋您的產品的消費者

快訊 - 透過電子郵件接收新聞和搜尋結果

網上論壇 - 建立郵寄清單和討論群組

User Interface

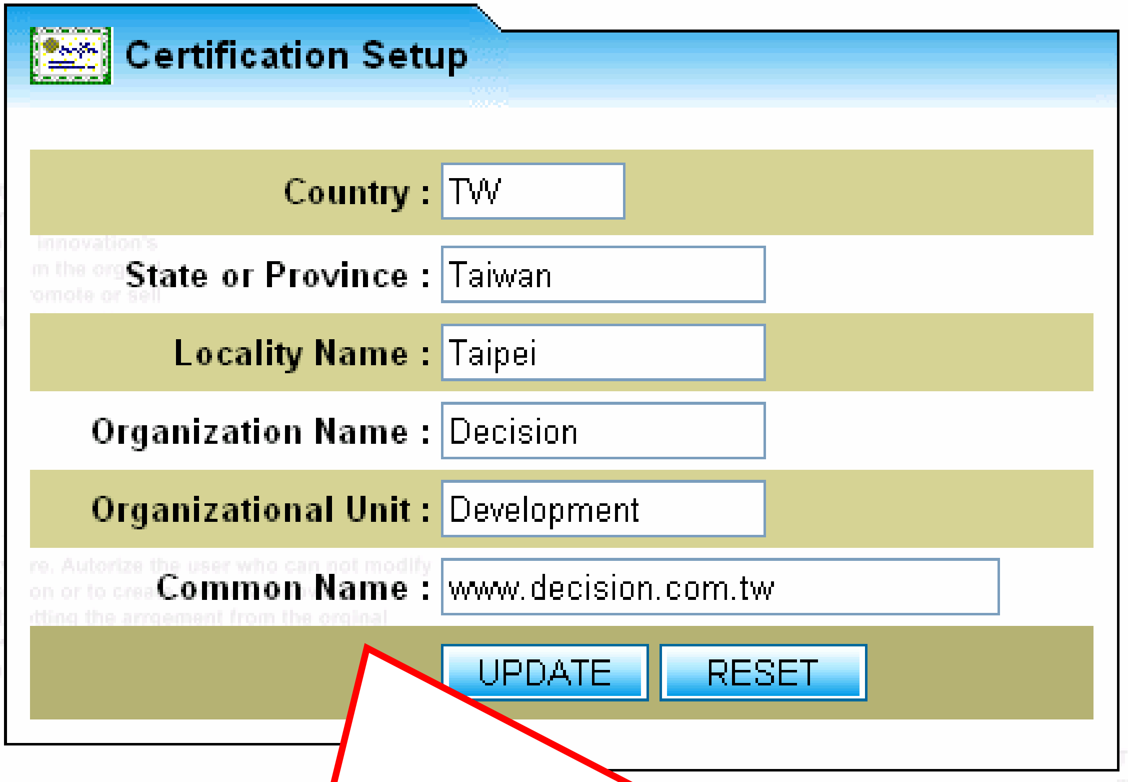
Menu – VERISIGN SETUP



To generate a fake certificate

User Interface

Verisign Setup



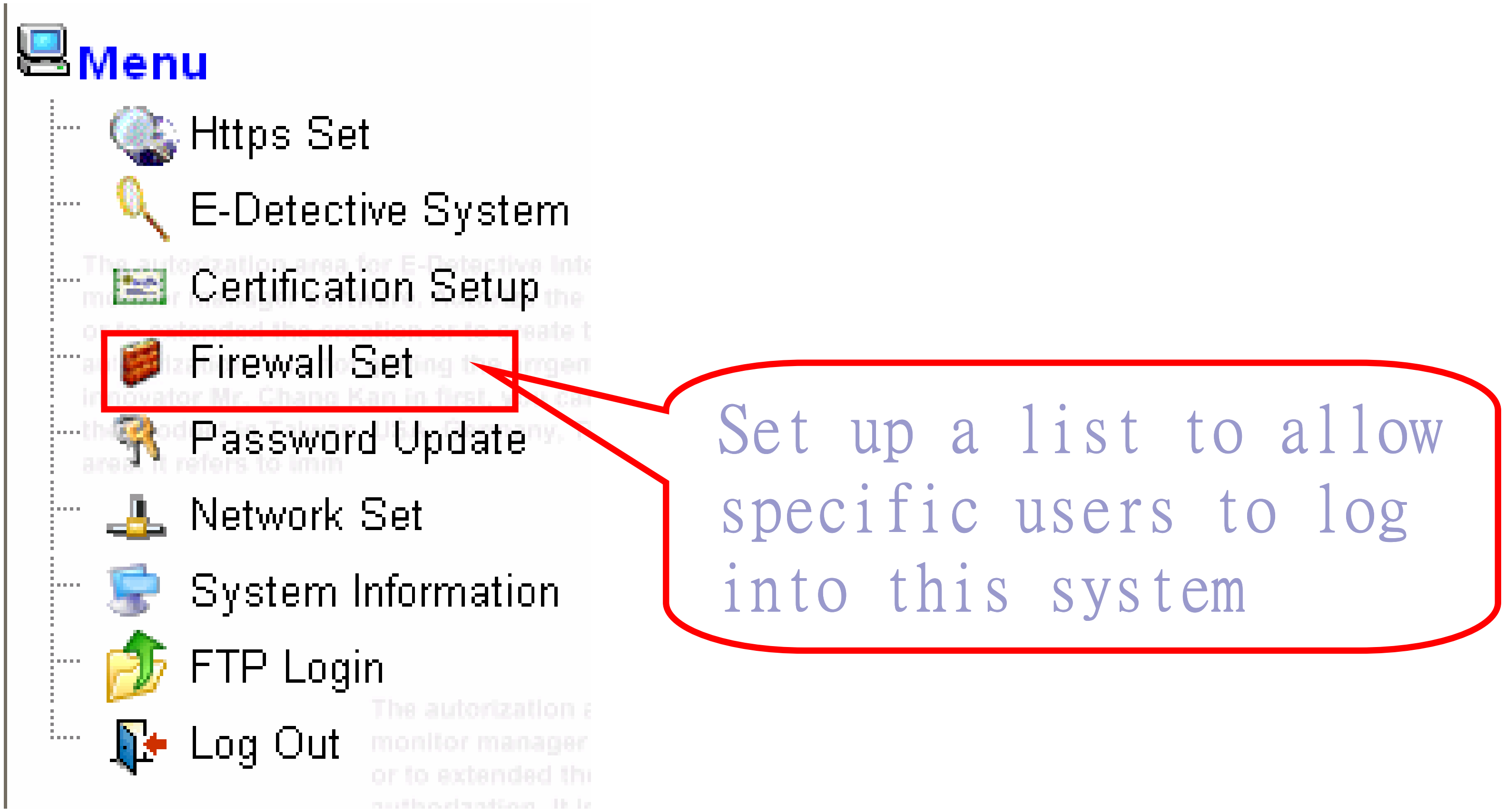
Certification Setup

Country :	TW
State or Province :	Taiwan
Locality Name :	Taipei
Organization Name :	Decision
Organizational Unit :	Development
Common Name :	www.decision.com.tw

Entering the fake info to produce a fake certificate

User Interface

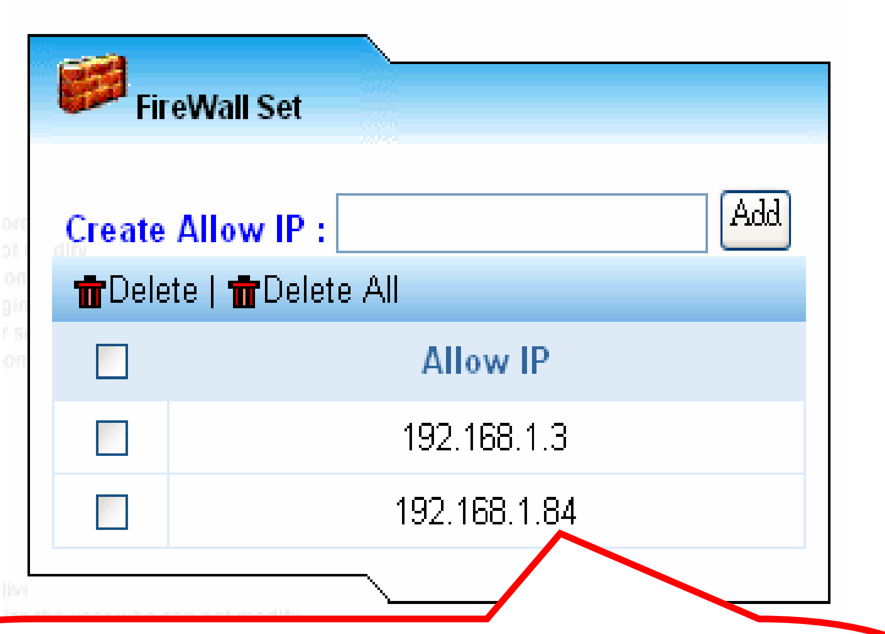
Menu – Firewall Set



Set up a list to allow specific users to log into this system

User Interface

Firewall Set



Create Allow IP : Add

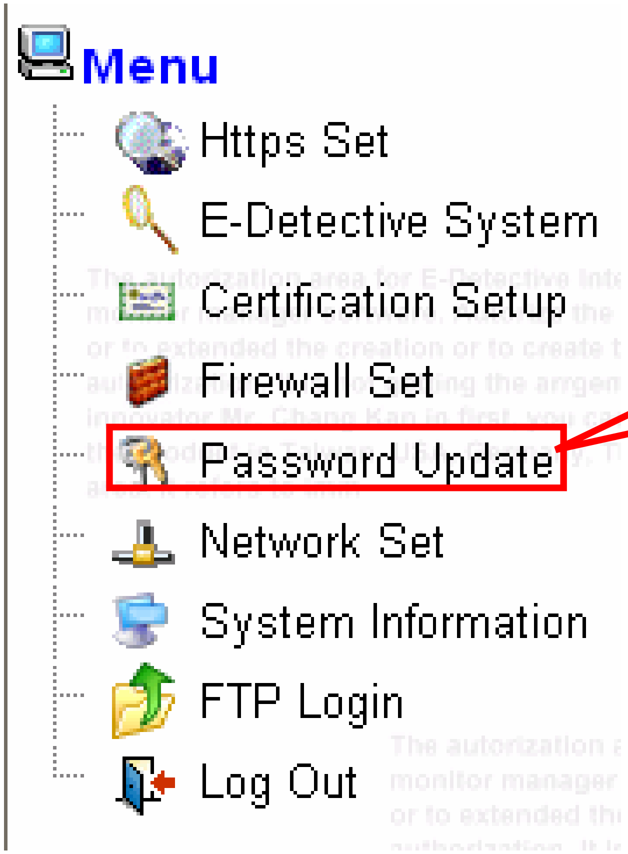
Delete | Delete All

□	Allow IP
□	192.168.1.3
□	192.168.1.84

An allowed list to specify which IP is able to access this system.

User Interface

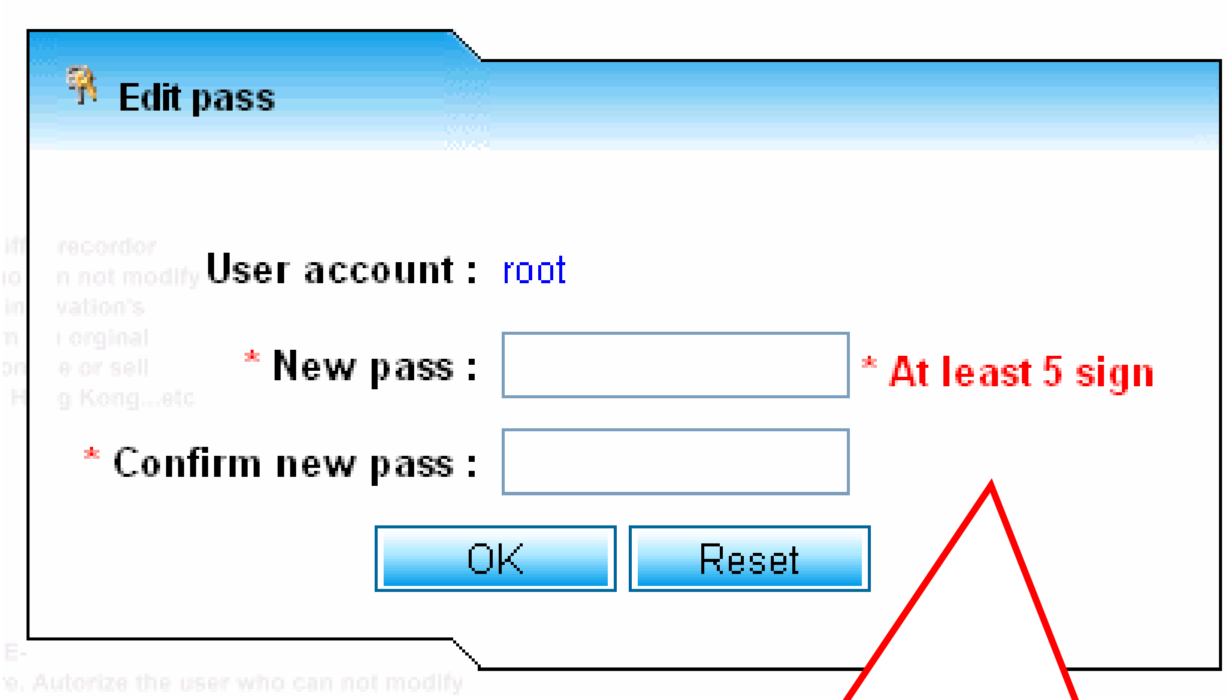
Menu – Password Update



Change the password

User Interface

Password update



User account : root

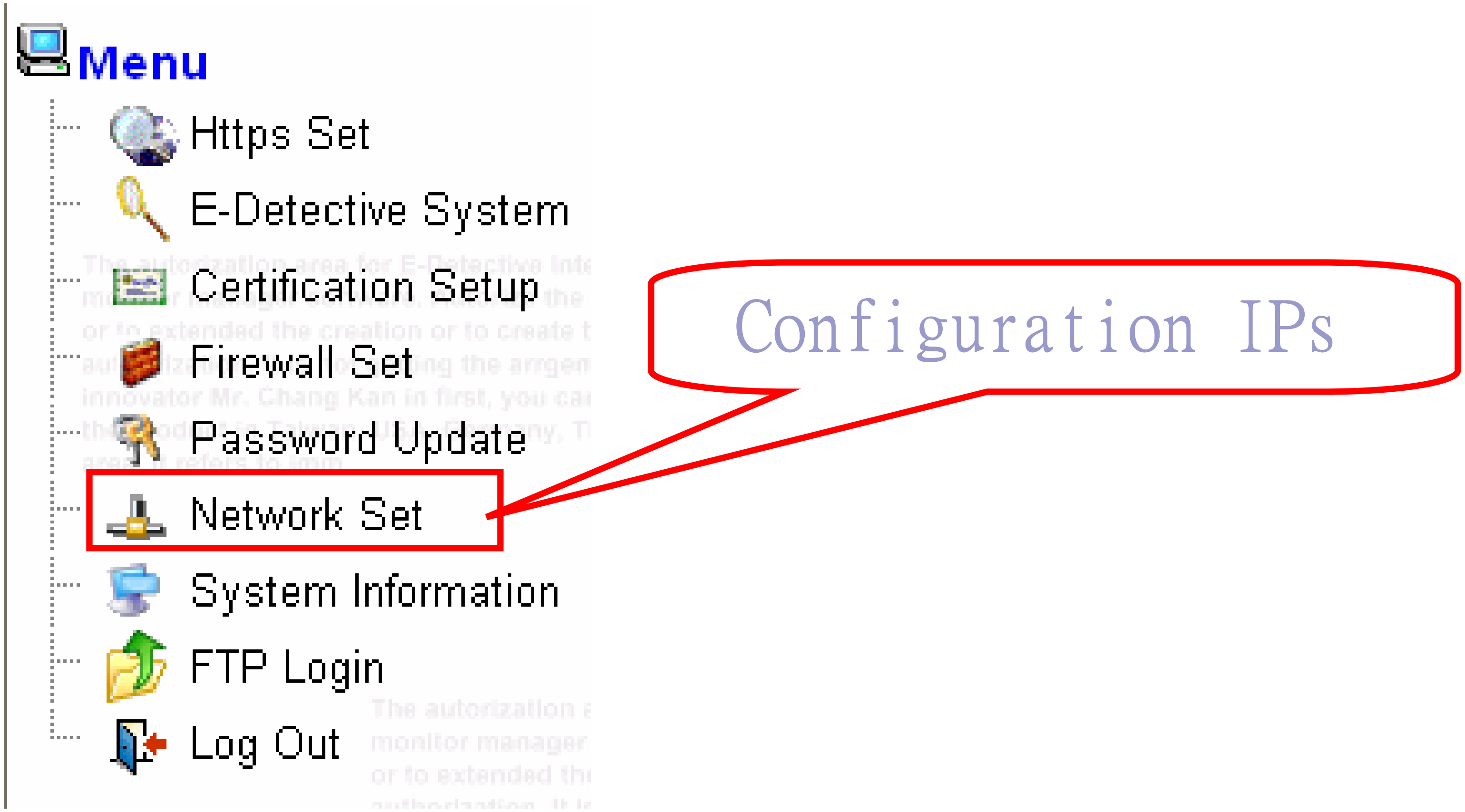
* New pass : * At least 5 sign

* Confirm new pass :

Providing the function to change the password

User Interface

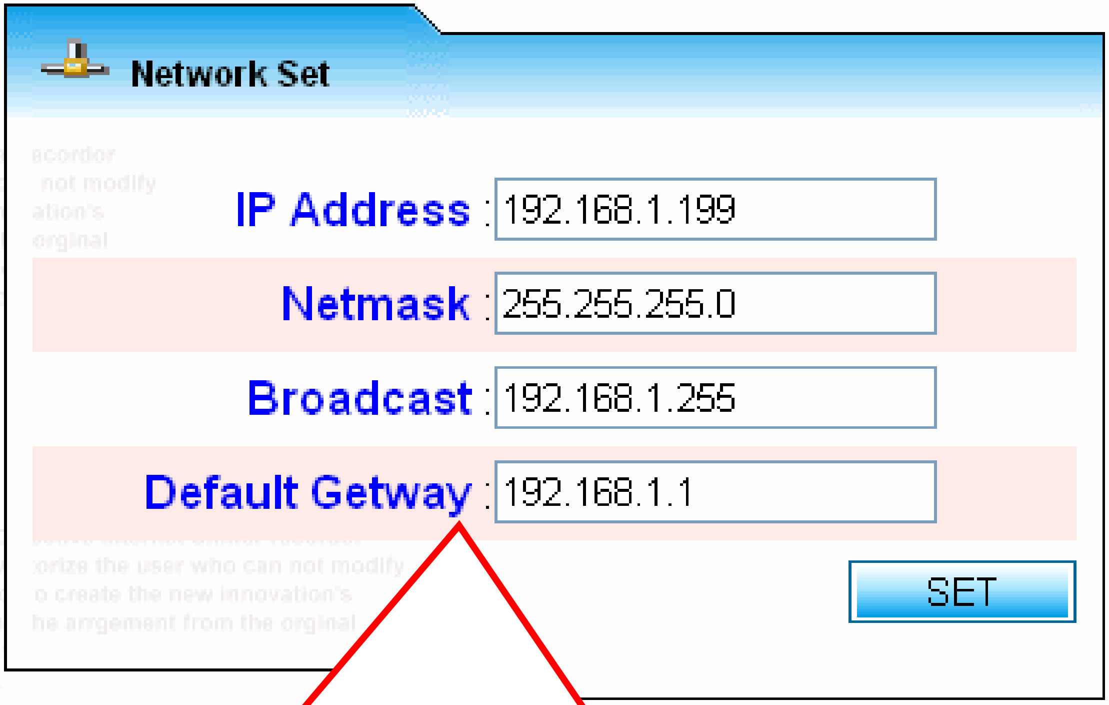
Menu – Network Set



Configuration IPs

User Interface

Network Set



Network Set

IP Address : 192.168.1.199

Netmask : 255.255.255.0

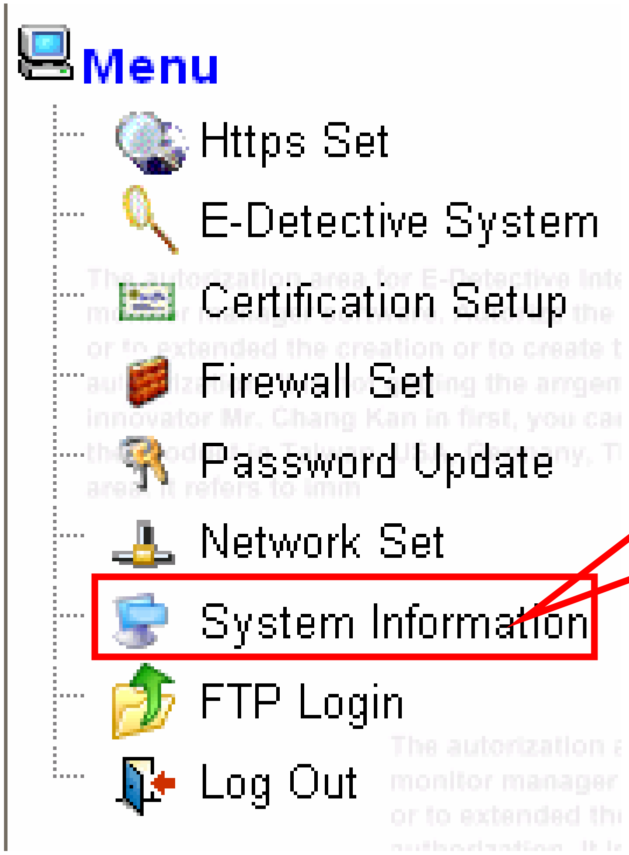
Broadcast : 192.168.1.255

Default Getway : 192.168.1.1

Configuration of IP, Mask IP, Broadcast IP, Geteway IP

User Interface

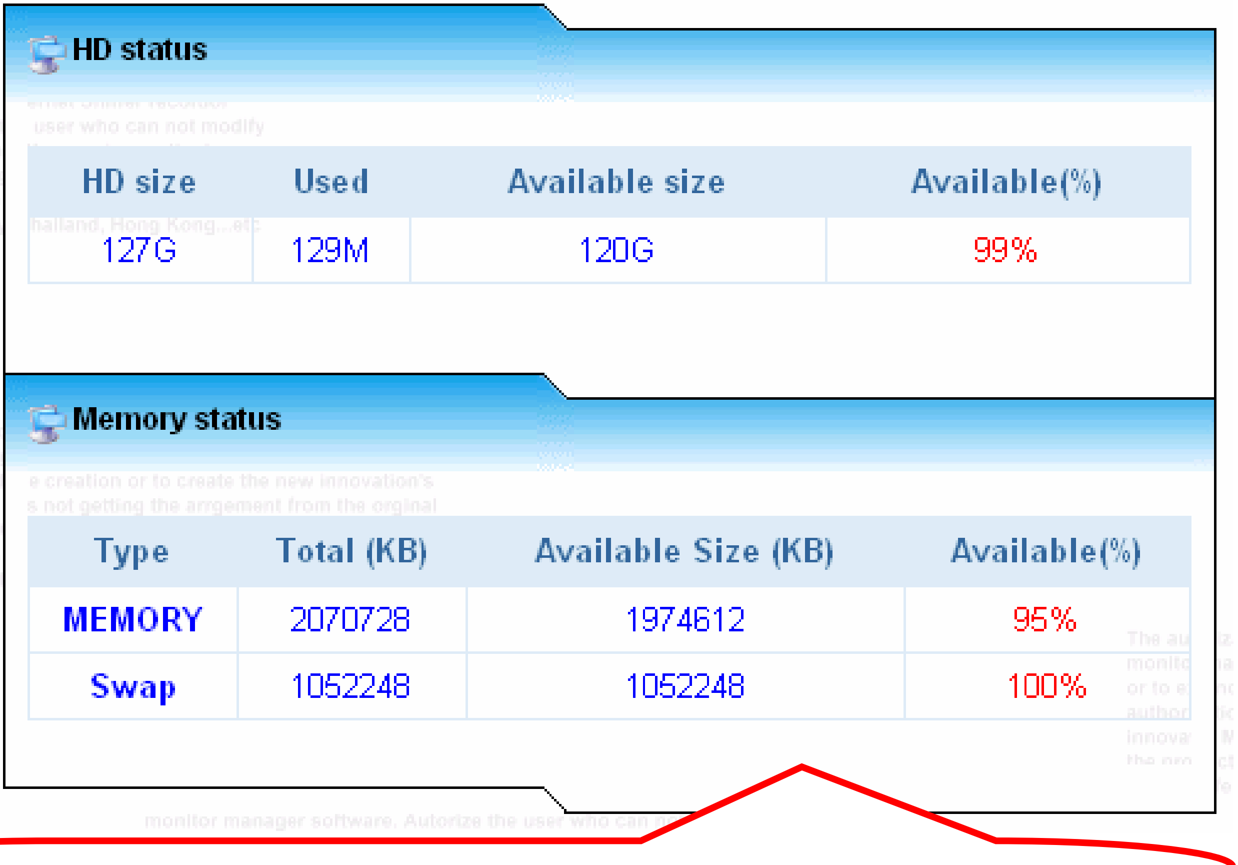
Menu – System Info



To show the status of HD and Memory

User Interface

System Info



HD status

HD size	Used	Available size	Available(%)
127G	129M	120G	99%

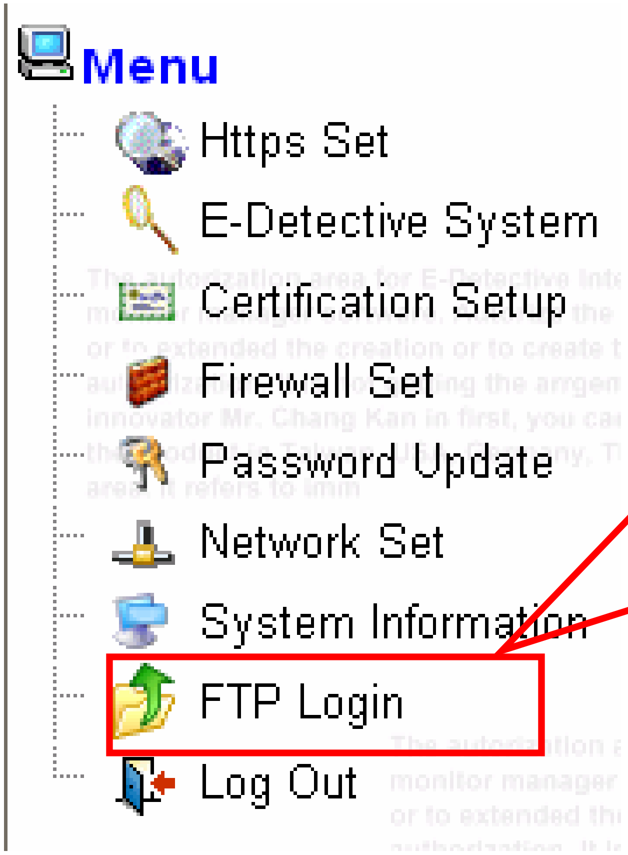
Memory status

Type	Total (KB)	Available Size (KB)	Available(%)
MEMORY	2070728	1974612	95%
Swap	1052248	1052248	100%

Showing the HD and Memory's usage

User Interface

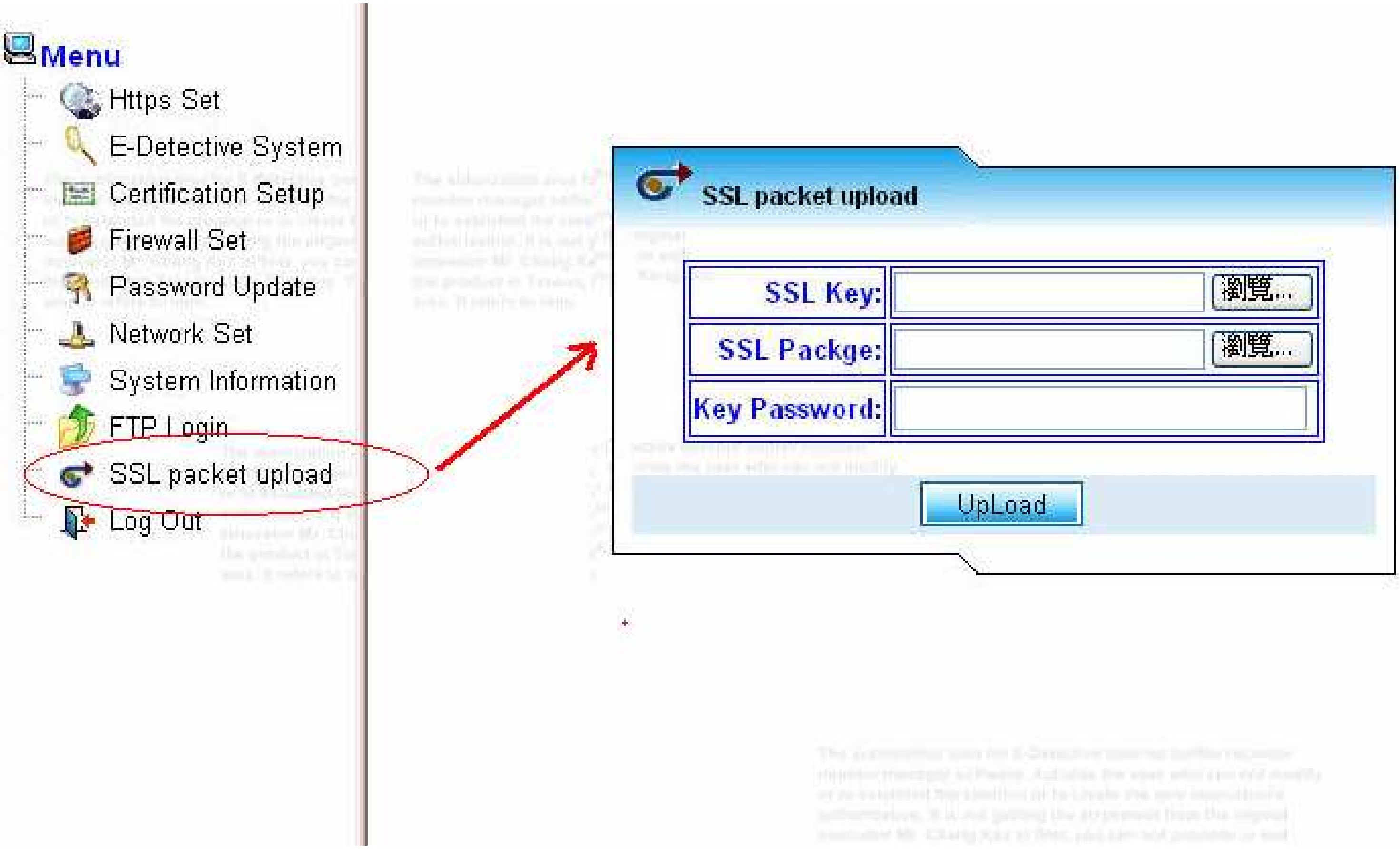
Menu – FTP



Providing the FTP way to transfer decrypted data to the specific ED system

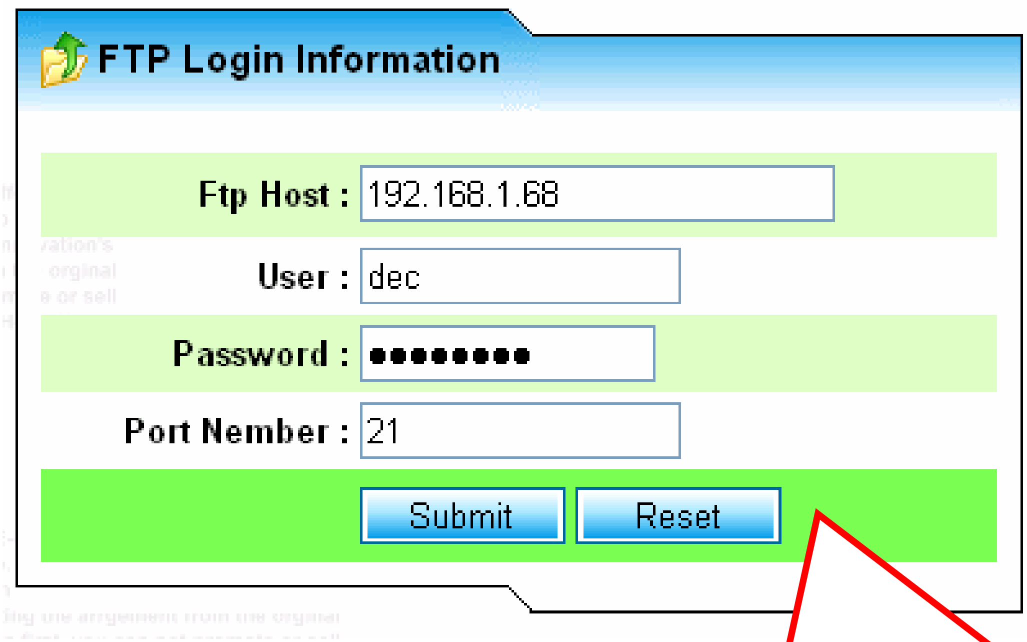
User Interface

Menu – SSL packet upload



User Interface

FTP – Upload to ED for HTTPS web reconstructing



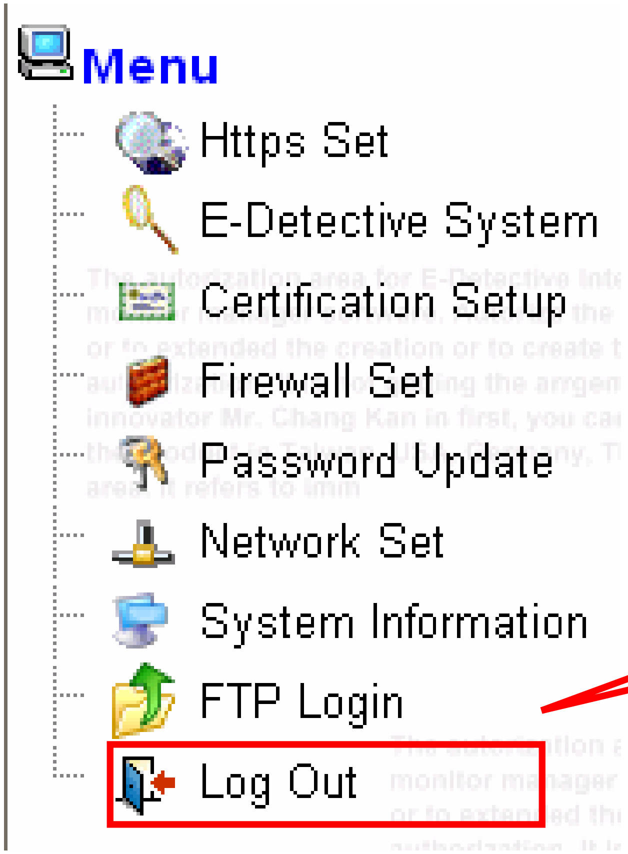
FTP Login Information

Ftp Host :	192.168.1.68
User :	dec
Password :	●●●●●●●●●
Port Nember :	21

Specifying where to send the decrypted data

User Interface

Menu – Log out



Log out

Frequently Asked Question (1)

1. **What is the major usage of HTTPS/SSL Network Forensic Device?**

   HTTPS/SSL Network Forensic Device (NFD) is used for decrypting of HTTPS/SSL Internet traffic, usually for forensic purpose. With the integration of E-Detective system with HTTPS/SSL NFD, the HTTPS web content can be decoded and displayed in exact web content. HTTPS/SSL NFD also can be used as vulnerability accessment tool to check on the security level of deployed encrypted network. If the network system can be decryted by HTTS/SSL NFD, it means that the network system is not secured and implementation of more secured network is needed.

2. **Who needs HTTPS/SSL NFD?**

   Government bodies, police and legal interception agencies, computer and network forensic department, banking and finance industry can use this device for their operation.

Frequently Asked Question (2)

3. **What method does HTTPS/SSL NFD used to decrypt HTTPS traffic?**
   HTTPS/SSL NFD utilizes two methods: 1. Man in the Middle Attack (MITM) and 2. Offline decryption (through available private key).

4. **Can HTTPS/SSL NFD capture username and password of user login into secure sites?**
   Yes, HTTPS/SSL NFD is able to capture login username and password for most of the sites (Google/Gmail, Hotmail Live, Yahoo Beta Mail etc) that require authentication.

5. **Can HTTPS/SSL NFD decrypt HTTPS web content and even the login username and password if the private key is available?**
   Yes, HTTPS/SSL NFD allows decryption of HTTPS Web content and login username and password if user has the private key. To view the content, it must integrate with E-Detective system.

Decision Computer Group

Q&A