

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®

2007/9/22



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

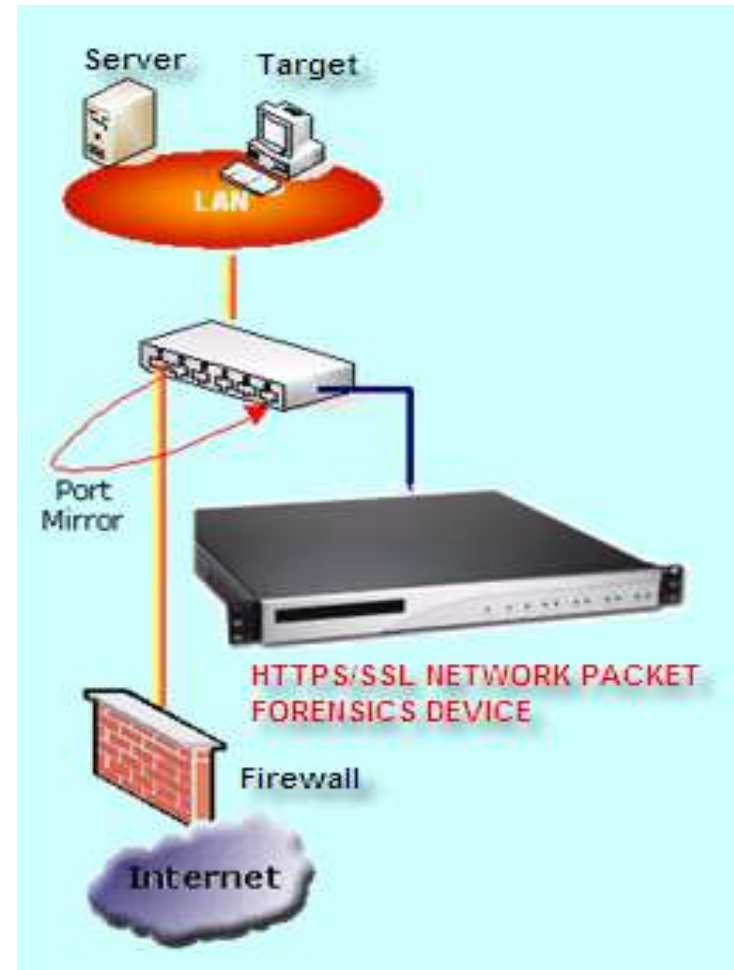
One of primary auditing features is it is able to be integrated with E-DETECTIVE system and its database, in order to exchange/decode/analyze the data. It can be integrate with E-DETECTIVE in one appliance or it can be a standalone device.



Decrypting Packets by Known Public Keys

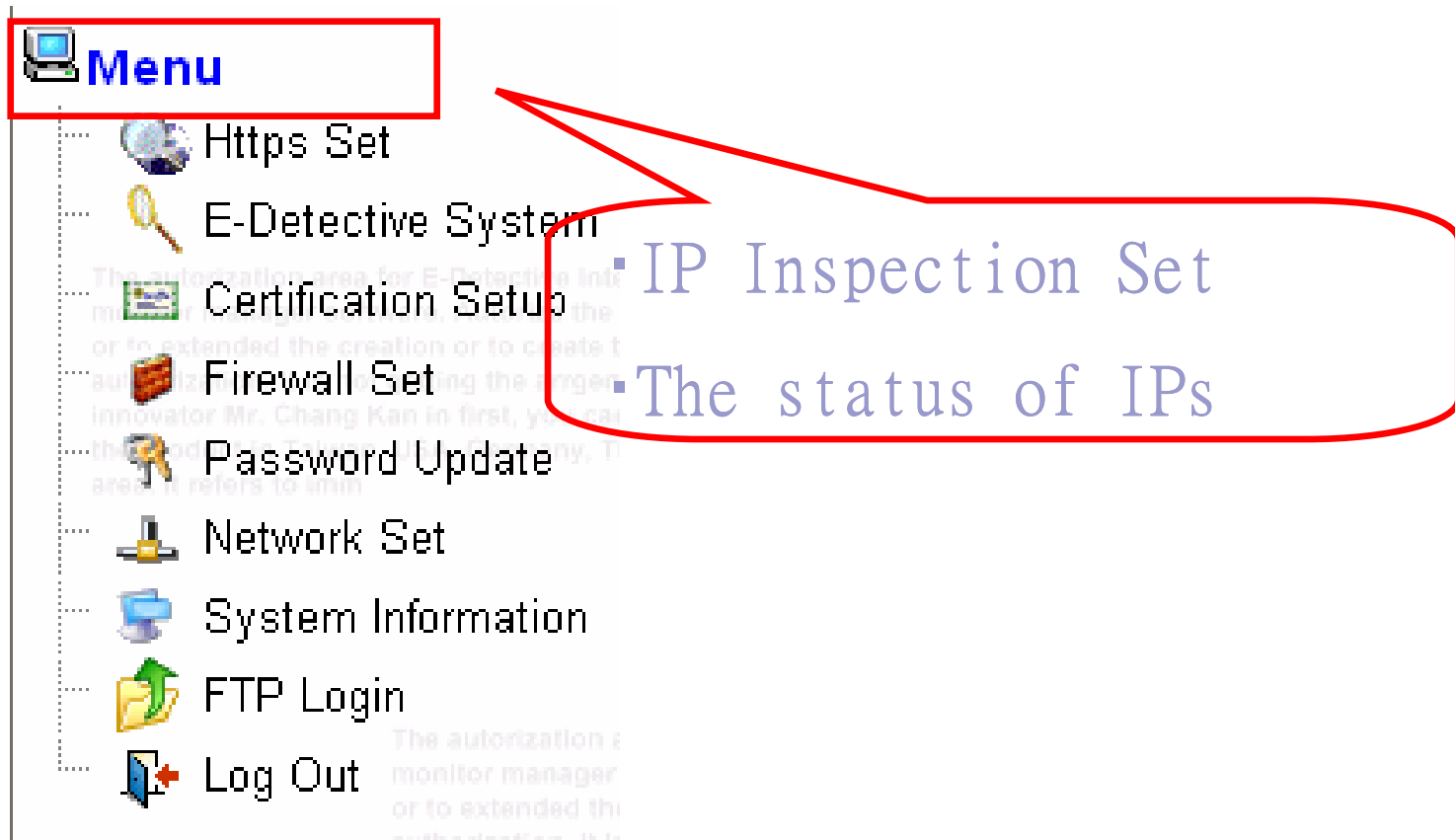
Able to Cooperate with SSL server and obtain its public keys in order to decrypt all data related to this SSL server.

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



User Interface

Menu – Https Set



User Interface

Https Set

Menu

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

HTTPS SET

Target IP 1

No reconnoitre any target.

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

Entering IPs you want to inspect here.

User Interface

Https Set

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

The screenshot displays a web application interface. On the left, there is a sidebar with a 'Log Out' button. The main content area features a table with four columns: 'Target IP', 'Connect web(URL)', 'Data', and 'Time'. The table contains ten rows of data, with alternating green and light blue background colors for each row. A red callout box highlights the table, and a red arrow points from the text 'Showing the latest status of inspected IPs, the info is auto-refreshed.' to the table. Above the table, there are two buttons: 'Delete' and 'START'. The 'START' button is highlighted with a red box. The interface also includes some faint, illegible text on the right side.

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
192.168.1.84	cash.kingstone.com.tw	2007/May/24	11:41:41

User Interface

Https Set

HTTPS SET

Target IP 1	192.168.1.84	Delete
-------------	--------------	--------

Add row


Donnoitre any target.

START

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

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

START

Press this button to start inspecting.

User Interface

Https Set

The screenshot shows the 'HTTPS SET' application window. It has a title bar with a globe icon and the text 'HTTPS SET'. Below the title bar, there is a section for adding target IP addresses. It contains three rows, each with a label 'Target IP 1', 'Target IP 2', and 'Target IP 3' respectively, followed by a text input field and a 'Delete' button. The input fields contain the IP addresses 192.168.1.22, 192.168.1.84, and 192.168.1.15. Below this section is an 'Add row' button. Further down, there is a section titled 'Reconnoitre IP :'. It contains a list of three IP addresses: 192.168.1.22, 192.168.1.84, and 192.168.1.15. At the bottom of the window, there are two buttons: 'UPDATE' and 'STOP'.

Target IP	Delete
192.168.1.22	Delete
192.168.1.84	Delete
192.168.1.15	Delete

Add row

Reconnoitre IP :

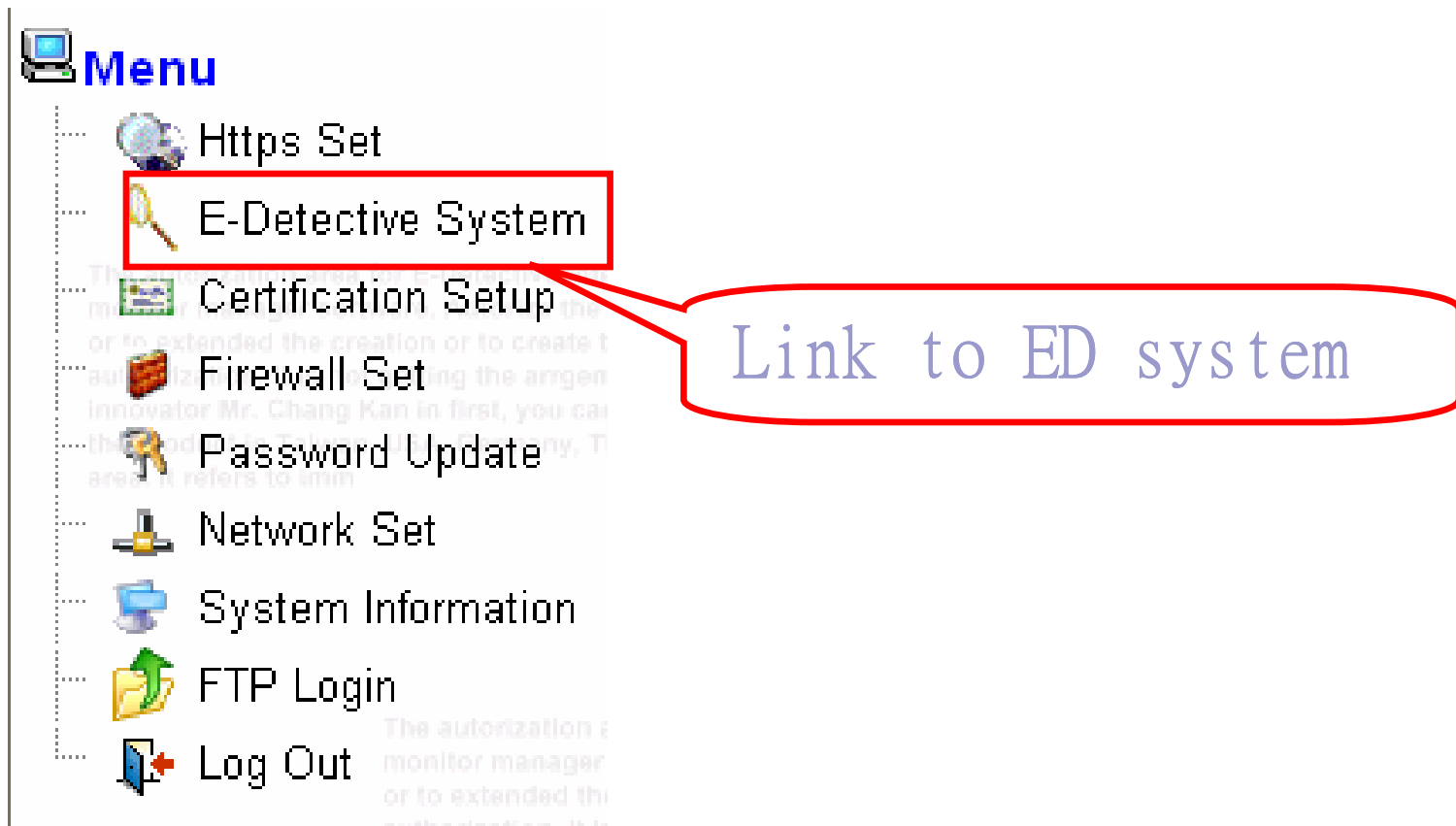
- 192.168.1.22
- 192.168.1.84
- 192.168.1.15

UPDATE STOP

The last input
of IPs

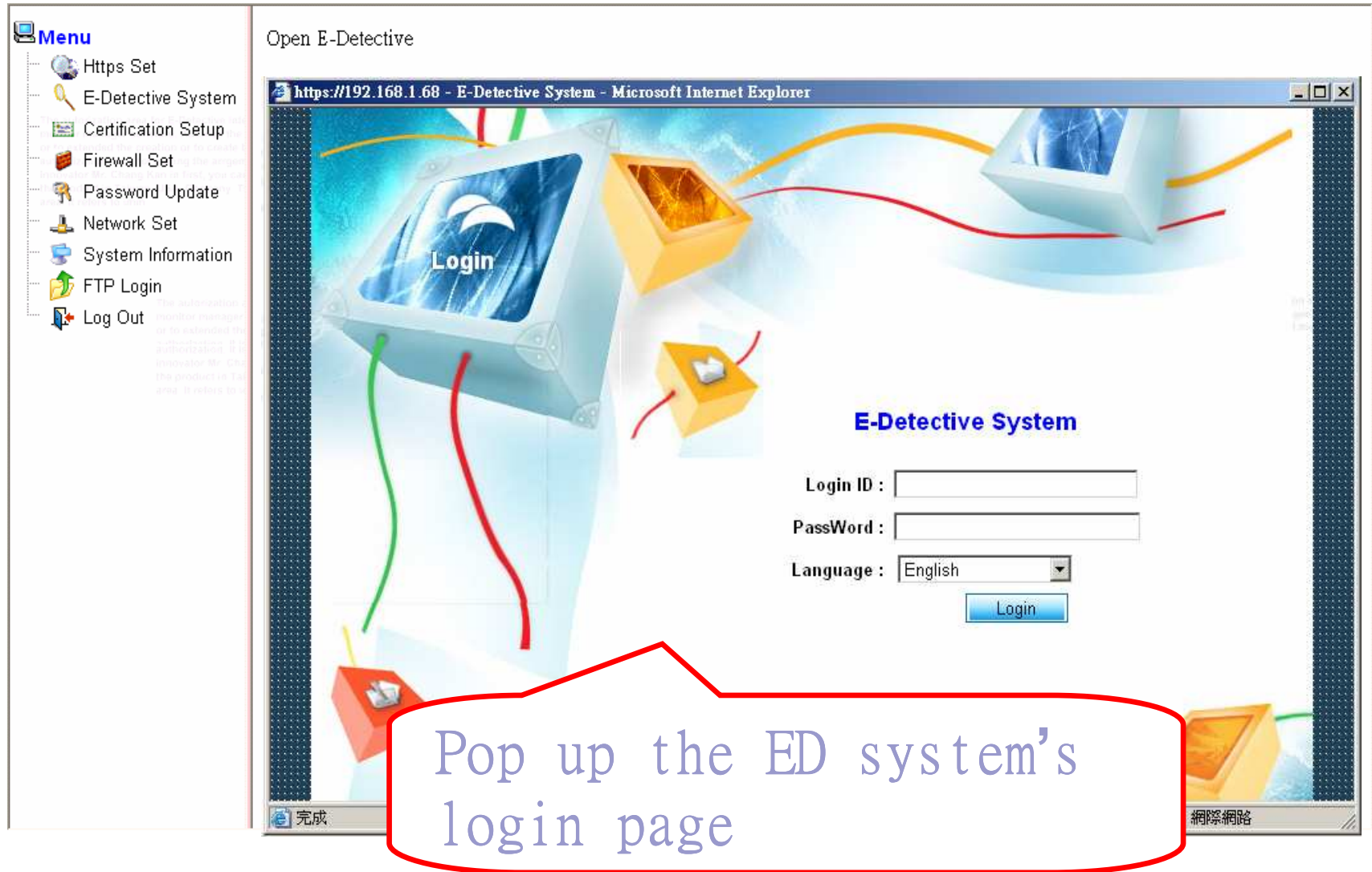
User Interface

Menu – E-Detective System



User Interface

E-Detective



User Interface

E-Detective

The info of Date/Time, IP, URL.

The screenshot shows the E-Detective System web interface. At the top, there's a navigation bar with icons for various functions. Below it, a search bar and a 'Show Mode' dropdown (set to IP) are visible. The main area contains a table with the following columns: No., Date-Time, IP, and URL Content. A red box highlights the first three columns. A red arrow points to a URL in the fourth column, with a callout box stating 'Click this URL to show the content'.

No.	<input type="checkbox"/>	Date-Time	IP	URL Content
28.	<input type="checkbox"/>	2007-05-17 14:51:34	192.168.1.84	www.google.com
29.	<input type="checkbox"/>	2007-05-17 14:51:32	192.168.1.84	www.google.com
30.	<input type="checkbox"/>	2007-05-17 14:51:25	192.168.1.84	www.google.com
31.	<input type="checkbox"/>	2007-05-17 14:51:25	192.168.1.84	www.google.com
32.	<input type="checkbox"/>	2007-05-17 14:29:32	192.168.1.84	cash.k...
33.	<input type="checkbox"/>	2007-05-17 14:28:59	192.168.1.84	cas...
34.	<input type="checkbox"/>	2007-05-17 14:28:59	192.168.1.84	cas...
35.	<input type="checkbox"/>	2007-05-17 14:28:59	192.168.1.84	cas...
36.	<input type="checkbox"/>	2007-05-11 09:06:53	192.168.1.84	www.google.com
37.	<input type="checkbox"/>	2007-05-11 09:06:30	192.168.1.84	www.google.com

Click this URL to show the content

User Interface

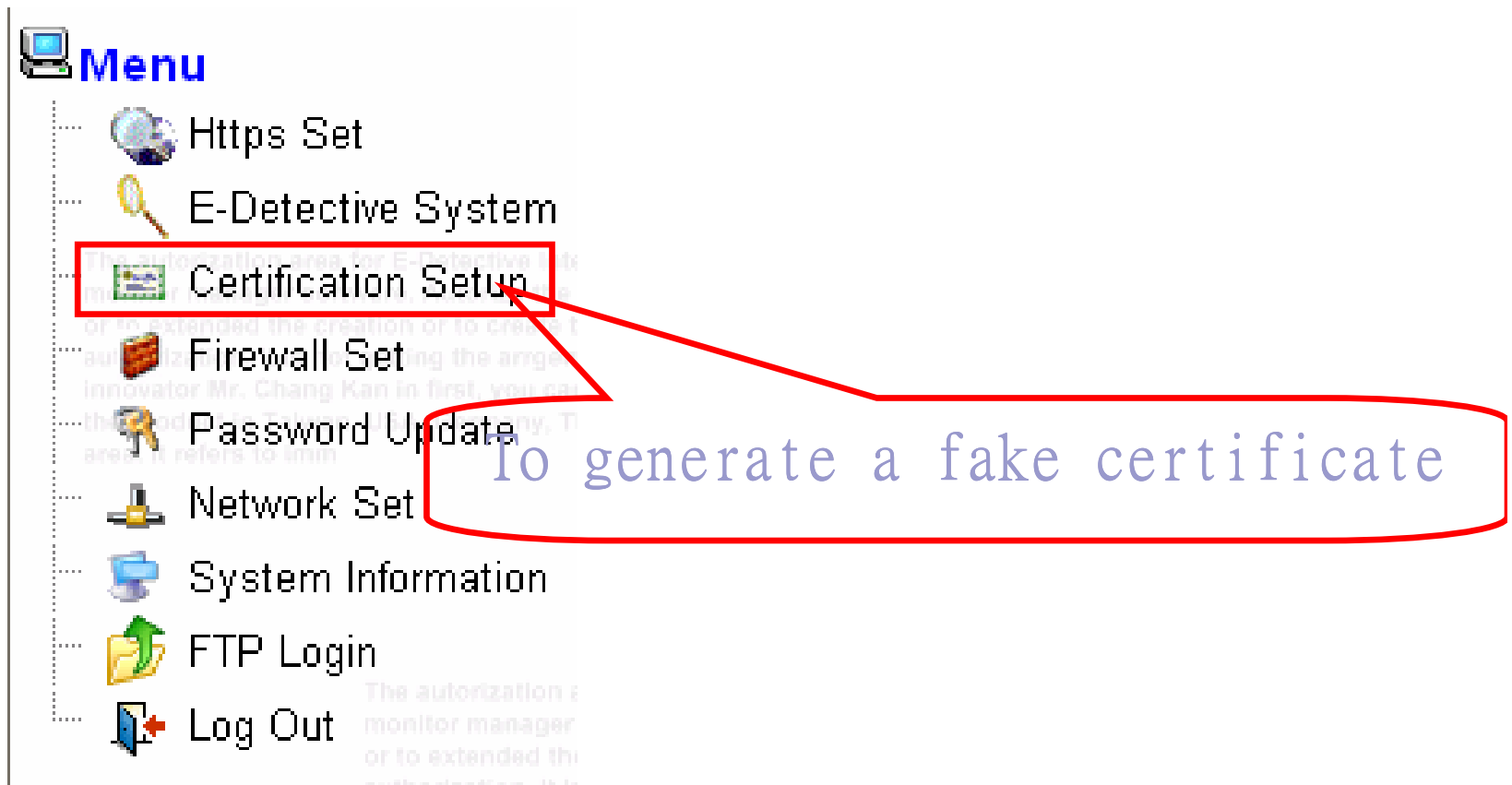
E-Detective

Webpage's content



User Interface

Menu – VERISIGN SETUP



User Interface

Verisign Setup



The screenshot shows a web form titled "Certification Setup" with a header bar containing a logo and the title. The form fields are as follows:

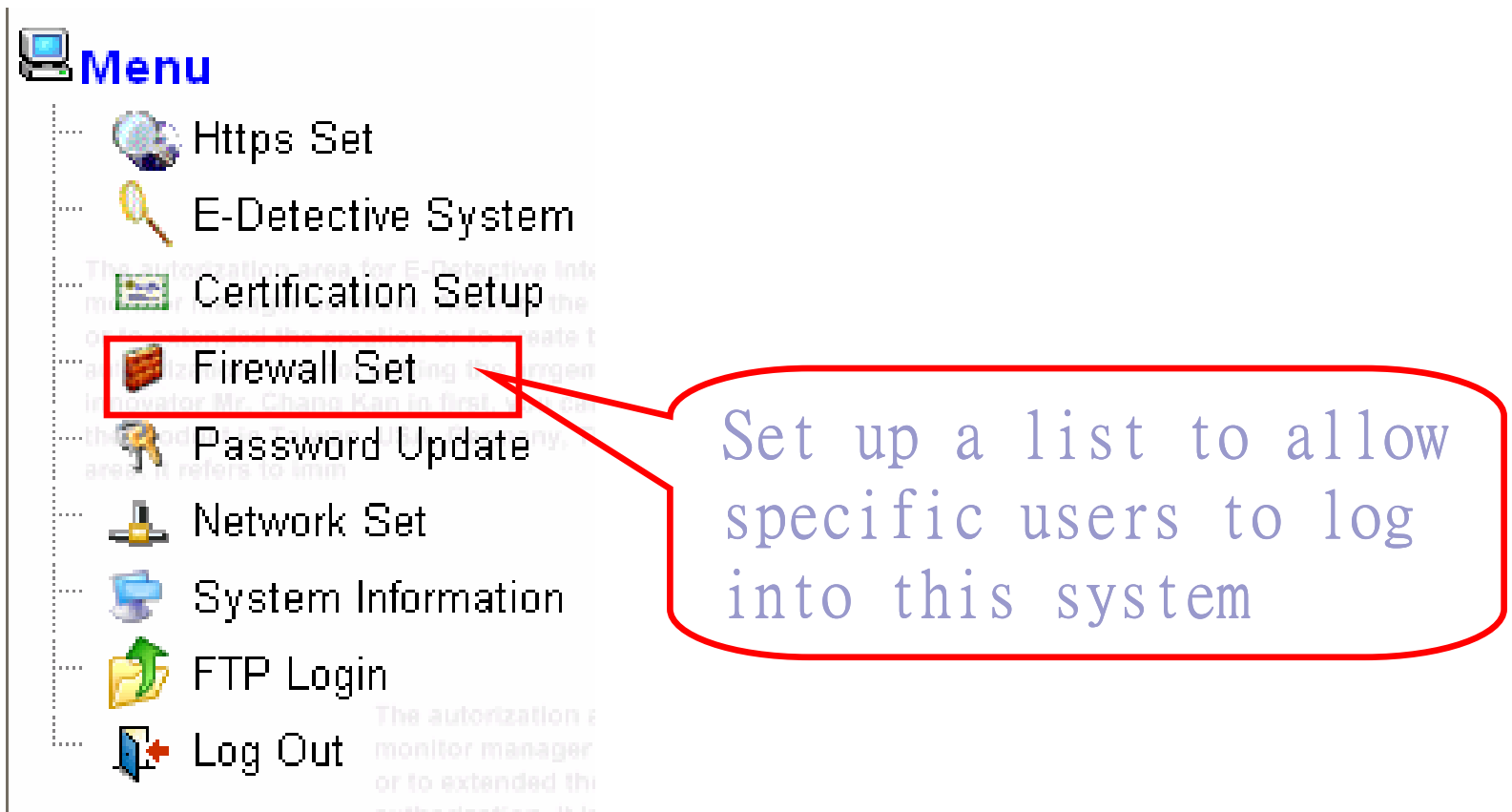
Field Label	Value
Country :	TW
State or Province :	Taiwan
Locality Name :	Taipei
Organization Name :	Decision
Organizational Unit :	Development
Common Name :	www.decision.com.tw

At the bottom of the form are two buttons: "UPDATE" and "RESET".

Entering the fake info to
produce a fake certificate

User Interface

Menu – Firewall Set



User Interface

Firewall Set

FireWall Set

Create Allow IP :

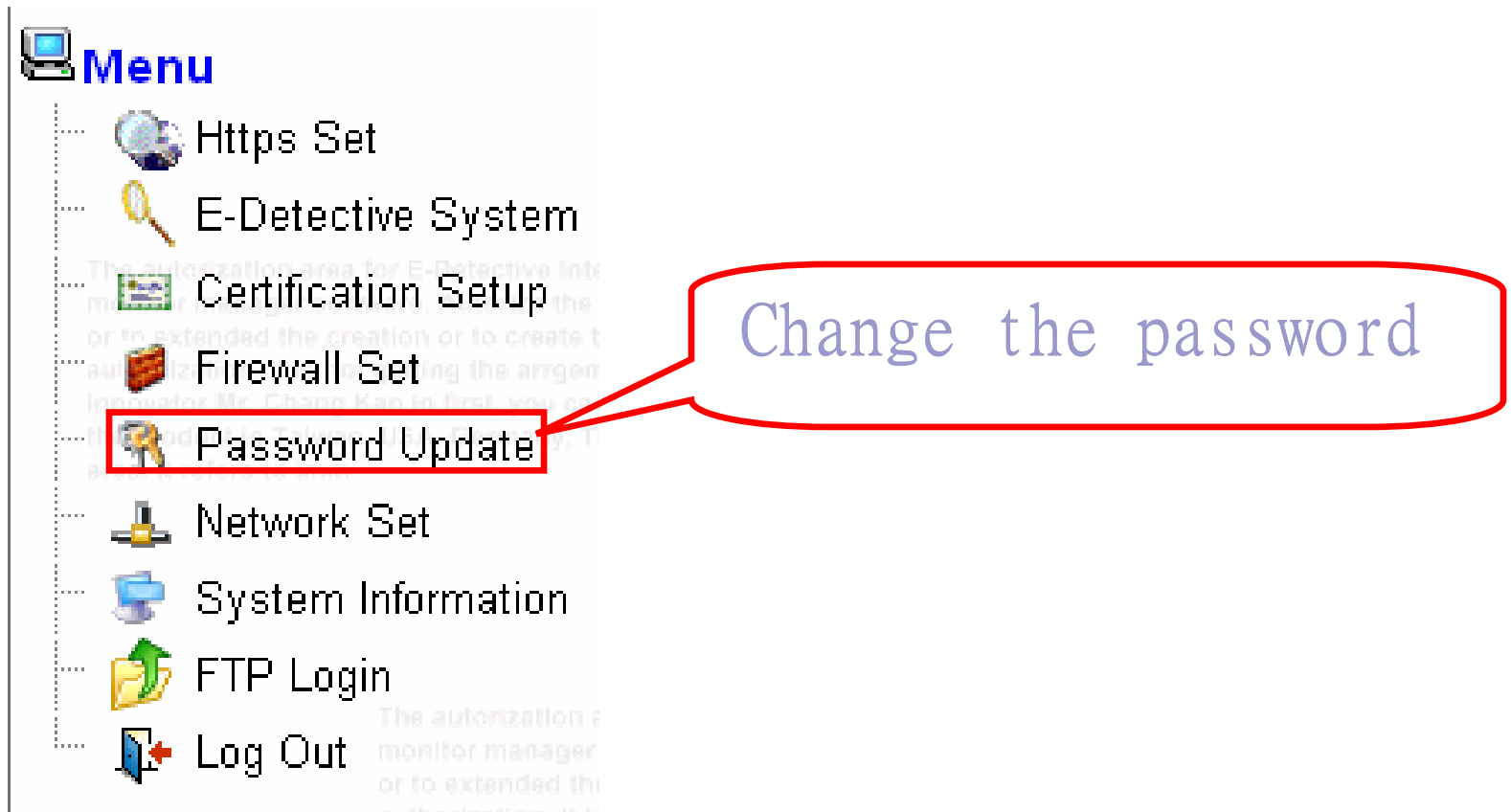
|

<input type="checkbox"/>	Allow IP
<input type="checkbox"/>	192.168.1.3
<input type="checkbox"/>	192.168.1.84

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

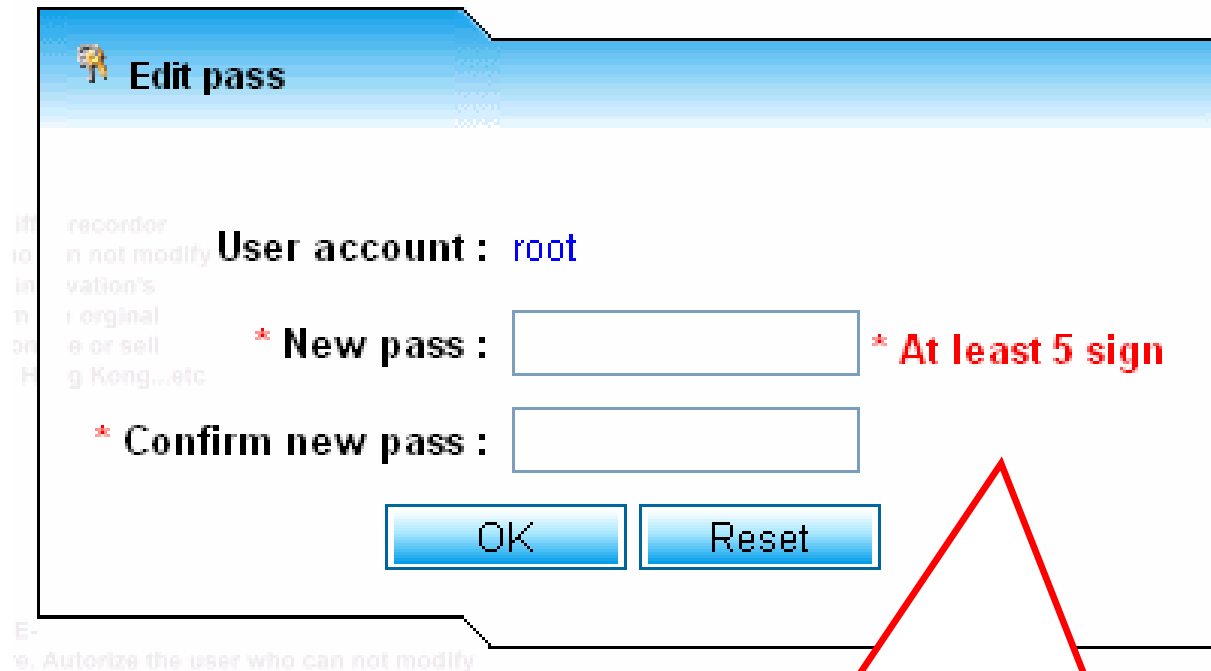
User Interface

Menu – Password Update



User Interface

Password update



The screenshot shows a dialog box titled "Edit pass" with a key icon. It displays "User account : root". There are two input fields: "* New pass :" and "* Confirm new pass :". To the right of the first field is a red note "* At least 5 sign". At the bottom are "OK" and "Reset" buttons. A red line points from the bottom of the dialog box to a callout box below.

Edit pass

User account : root

* New pass : * At least 5 sign

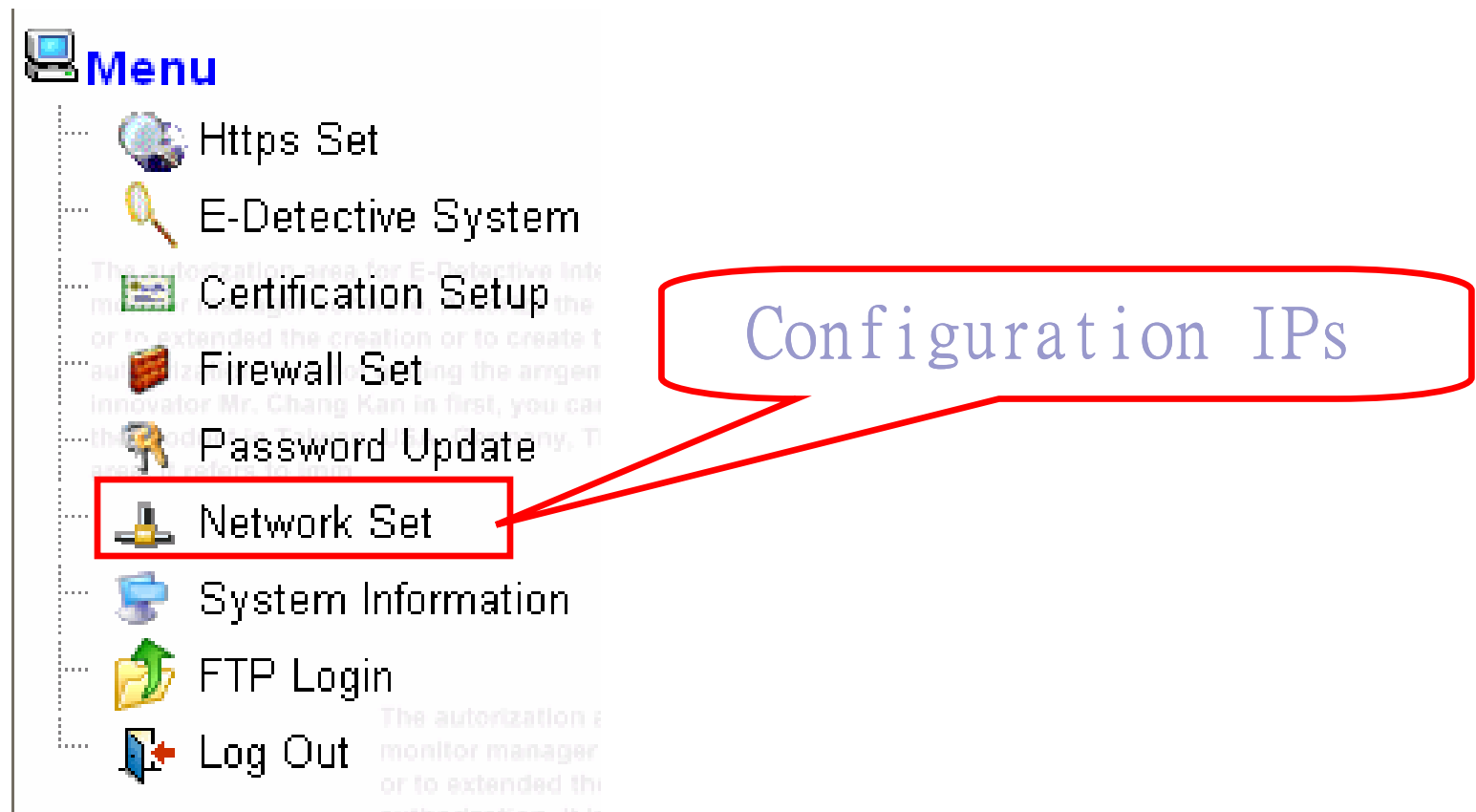
* Confirm new pass :

OK Reset

Providing the function to
change the password

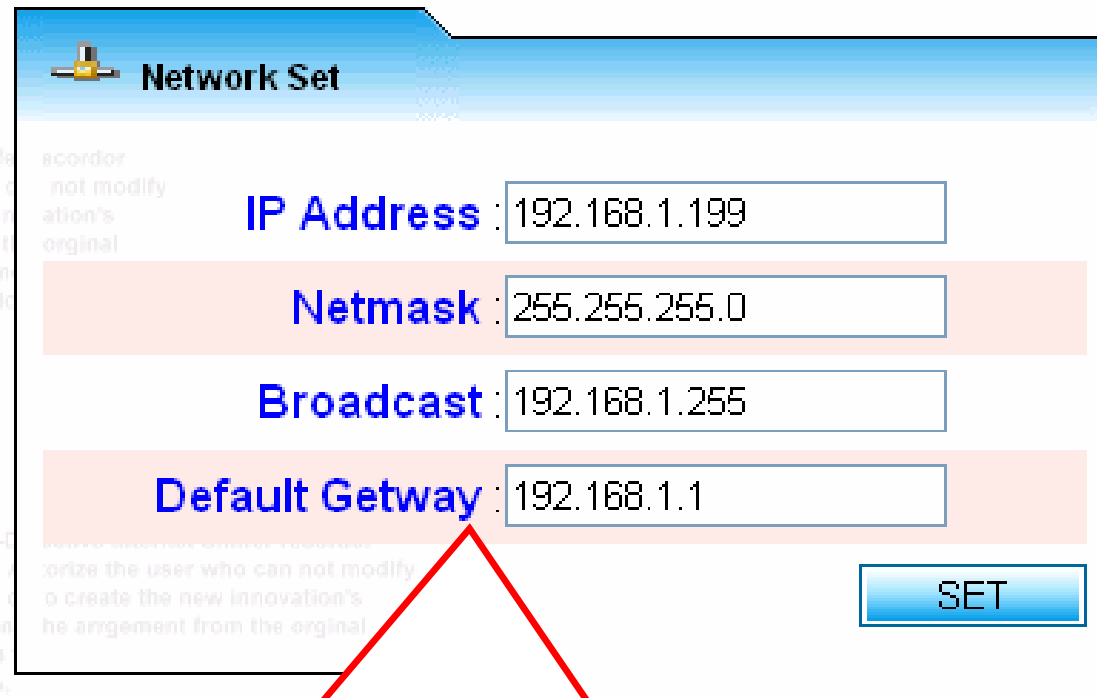
User Interface

Menu – Network Set



User Interface

Network Set



The image shows a 'Network Set' configuration window. It has a title bar with a network icon and the text 'Network Set'. Below the title bar, there is a section with a blue header and a white body. The body contains four input fields, each with a label and a value. The labels are 'IP Address', 'Netmask', 'Broadcast', and 'Default Getway'. The values are '192.168.1.199', '255.255.255.0', '192.168.1.255', and '192.168.1.1' respectively. The 'Netmask' and 'Broadcast' fields are highlighted with a light orange background. The 'Default Getway' field is also highlighted with a light orange background. A blue 'SET' button is located at the bottom right of the window. A red arrow points from the 'Default Getway' field to a red-bordered box below the window.

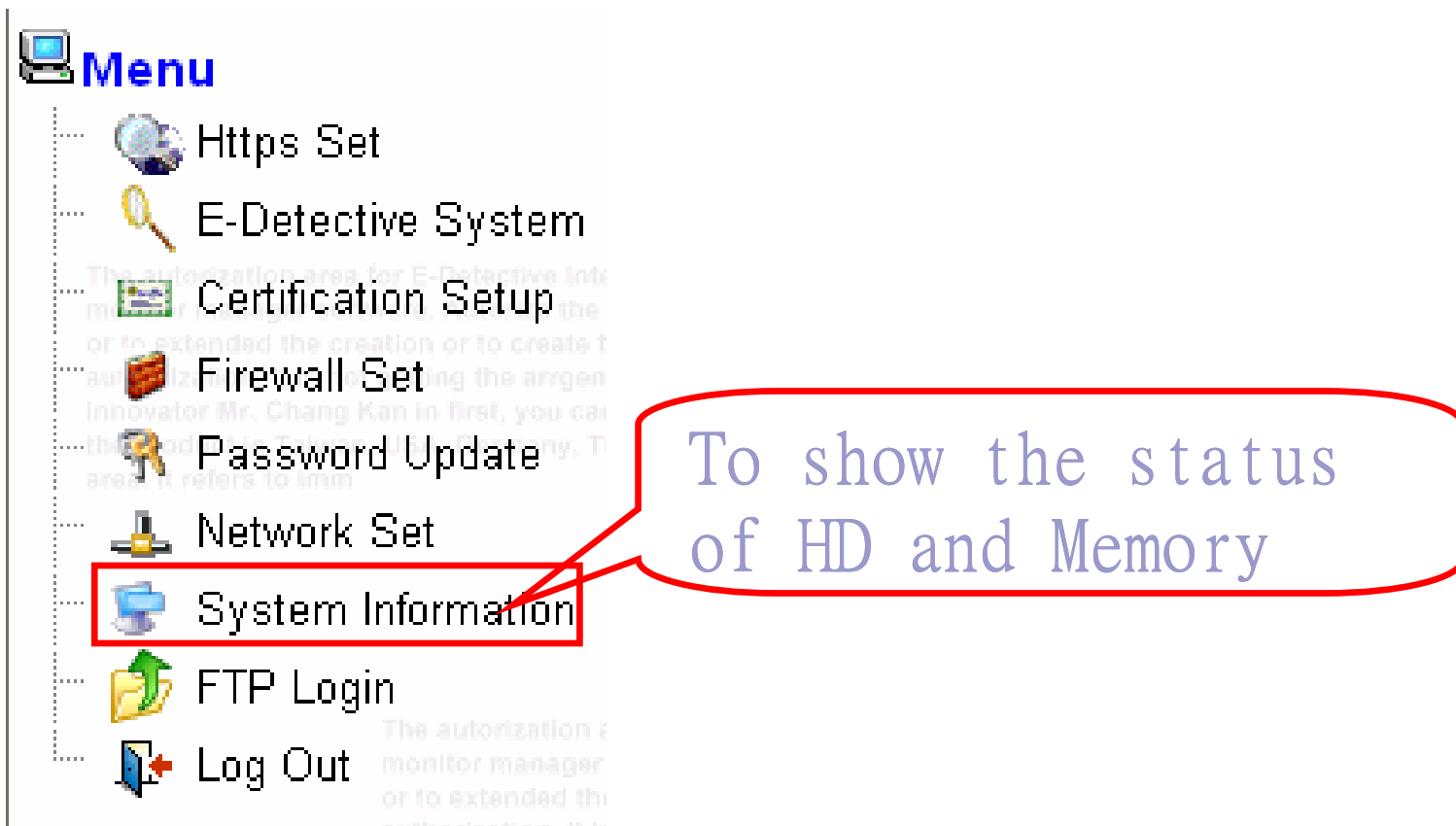
Field	Value
IP Address	192.168.1.199
Netmask	255.255.255.0
Broadcast	192.168.1.255
Default Getway	192.168.1.1

SET

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

User Interface

Menu – System Info



User Interface

System Info

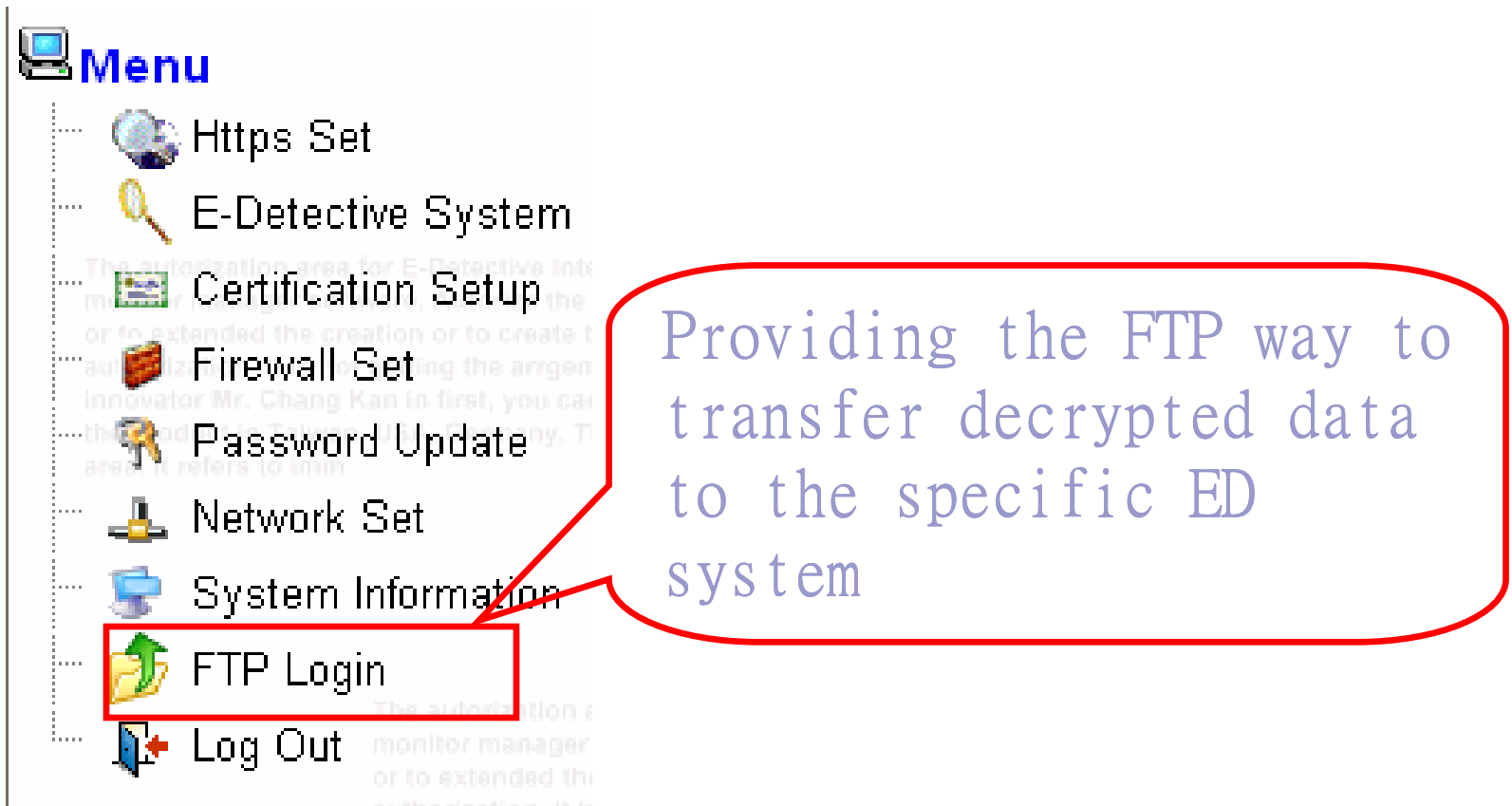
HD status			
user who can not modify			
HD size	Used	Available size	Available(%)
127G	129M	120G	99%

Memory status			
The au monito or to s author innova the non			
Type	Total (KB)	Available Size (KB)	Available(%)
MEMORY	2070728	1974612	95%
Swap	1052248	1052248	100%

Showing the HD and Memory's usage

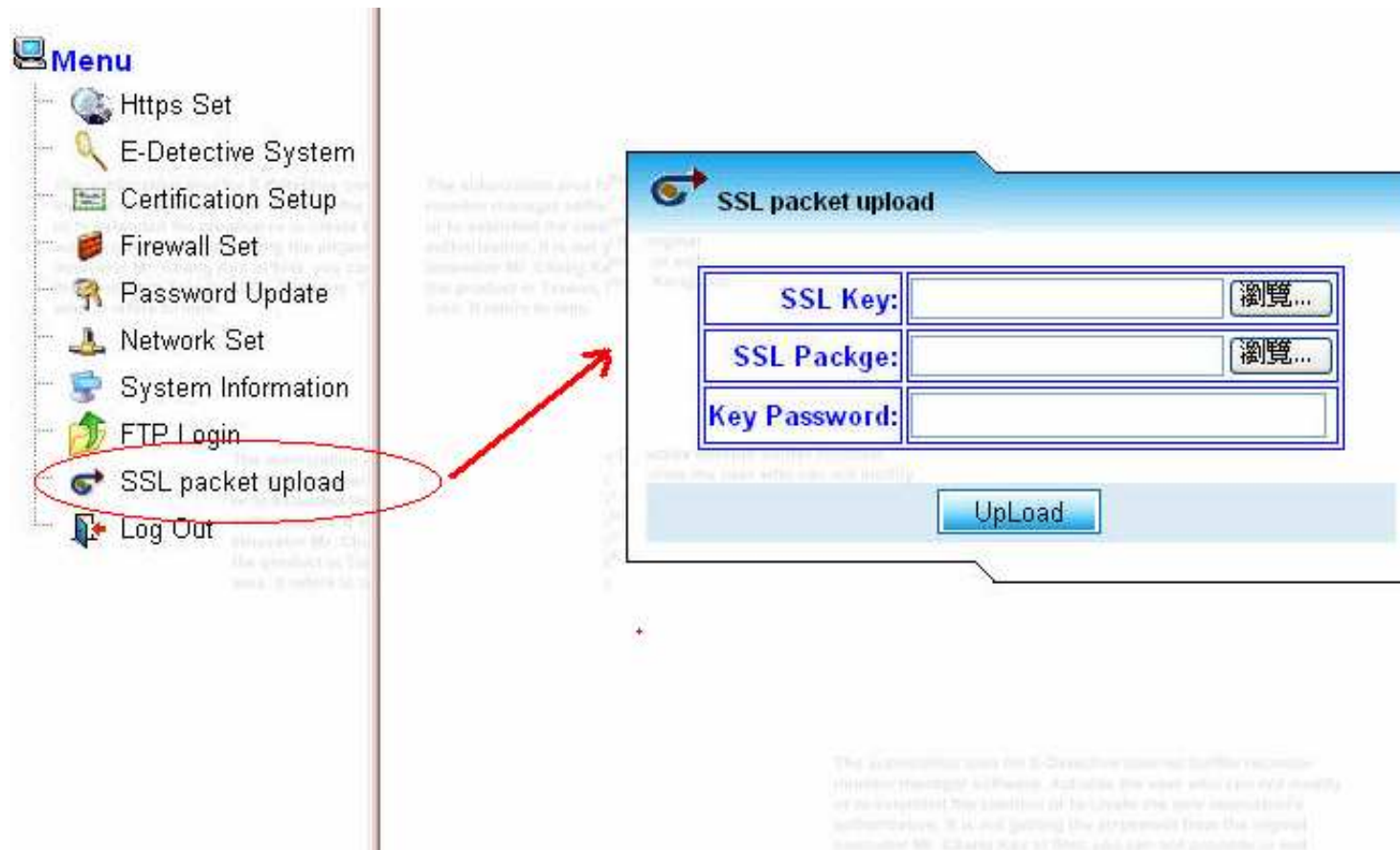
User Interface

Menu – FTP



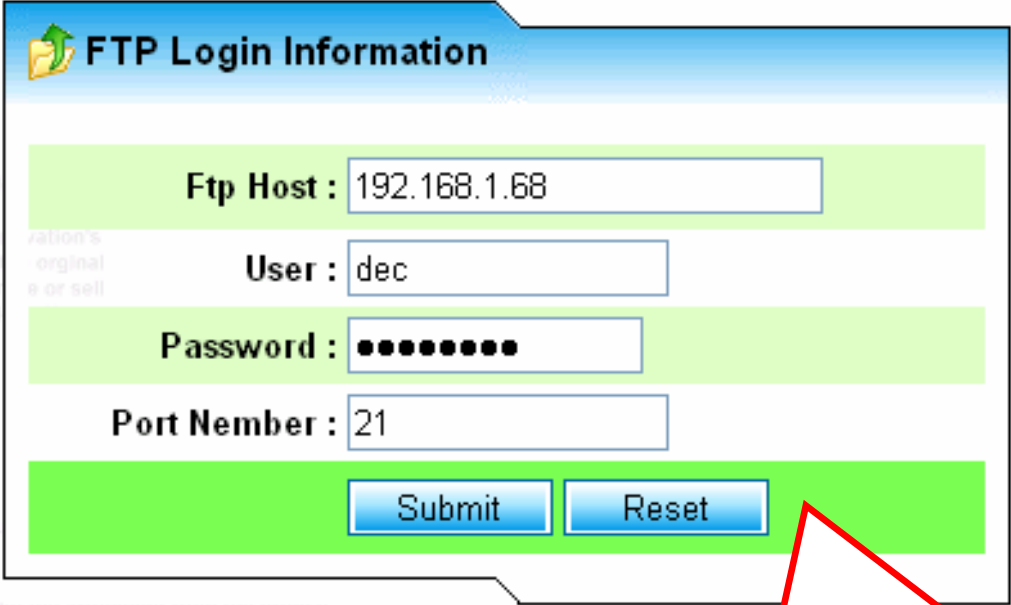
User Interface

Menu – SSL packet upload



User Interface

FTP – Upload to ED for HTTPS web reconstructing



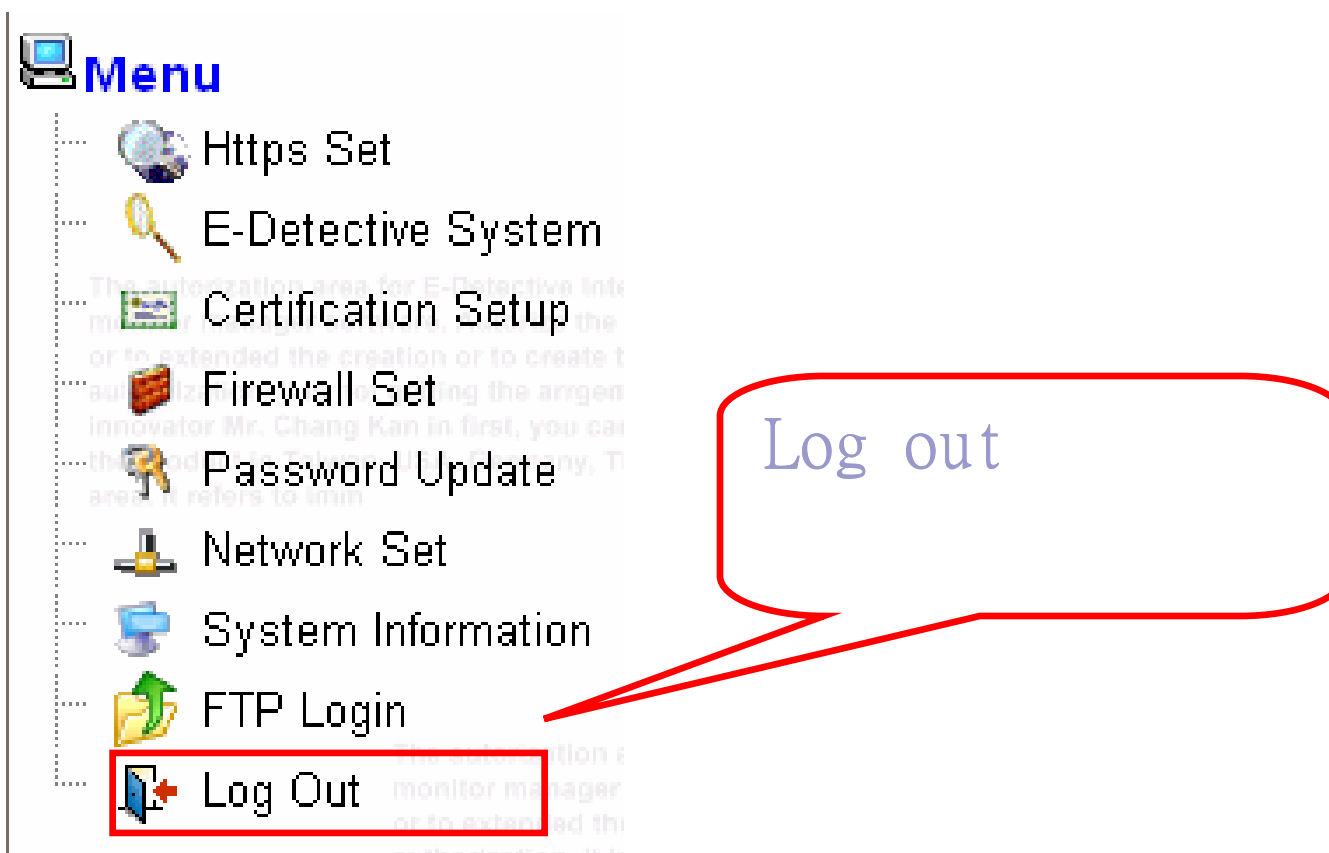
The image shows a web form titled "FTP Login Information" with a folder icon. It contains four input fields: "Ftp Host" with the value "192.168.1.68", "User" with the value "dec", "Password" with masked characters "••••••••", and "Port Number" with the value "21". At the bottom are "Submit" and "Reset" buttons. A red callout line points from the "Port Number" field to a text box below.

Ftp Host :	192.168.1.68
User :	dec
Password :	••••••••
Port Number :	21
<input type="button" value="Submit"/> <input type="button" value="Reset"/>	

Specifying where to send the decrypted data

User Interface

Menu – 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 assessment tool to check on the security level of deployed encrypted network. If the network system can be decrypted by HTTPS/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

