



Mobile Forensic System Network Investigation Toolkit



Agenda

- ▶ Internal Threat and Counter Action
- ▶ Tactic Wireless Interception – NIT
- ▶ Enhanced Wireless Interception Deployment
 - Multiple-point Interception Deployment
 - Options
- ▶ WPA Cracking System
- ▶ Full Wireless Interception Deployment
- ▶ Operation and Management of NIT 2.0
- ▶ Conclusion

Internal Threat

- ▶ Most usually access corporate WiFi network by known ID and MAC address under friendly BYOD environment
- ▶ Most are either done by disgruntled employees or malice industrial spy with stolen ID
 - Confidential corporate information leakage
 - Spreading messages of blackmail or harassment
 - Cyber bullying or discrimination
 - Cybercrimes
- ▶ Outsider or industrial spy with stolen ID usually passes internal confidential data to foreign unknown AP
- ▶ It impacts employee morale and corporate governance
- ▶ It hurts corporate business and reputation

Internal Threat Prevention

- ▶ Target at suspicious online activities
- ▶ Collect more evidence on suspicious online activities of mails, FB, tweets...etc.
- ▶ Clarify all facts, criminal scope and motives through data scoping and link analysis
- ▶ Present all results into investigation report and forward it to legal process

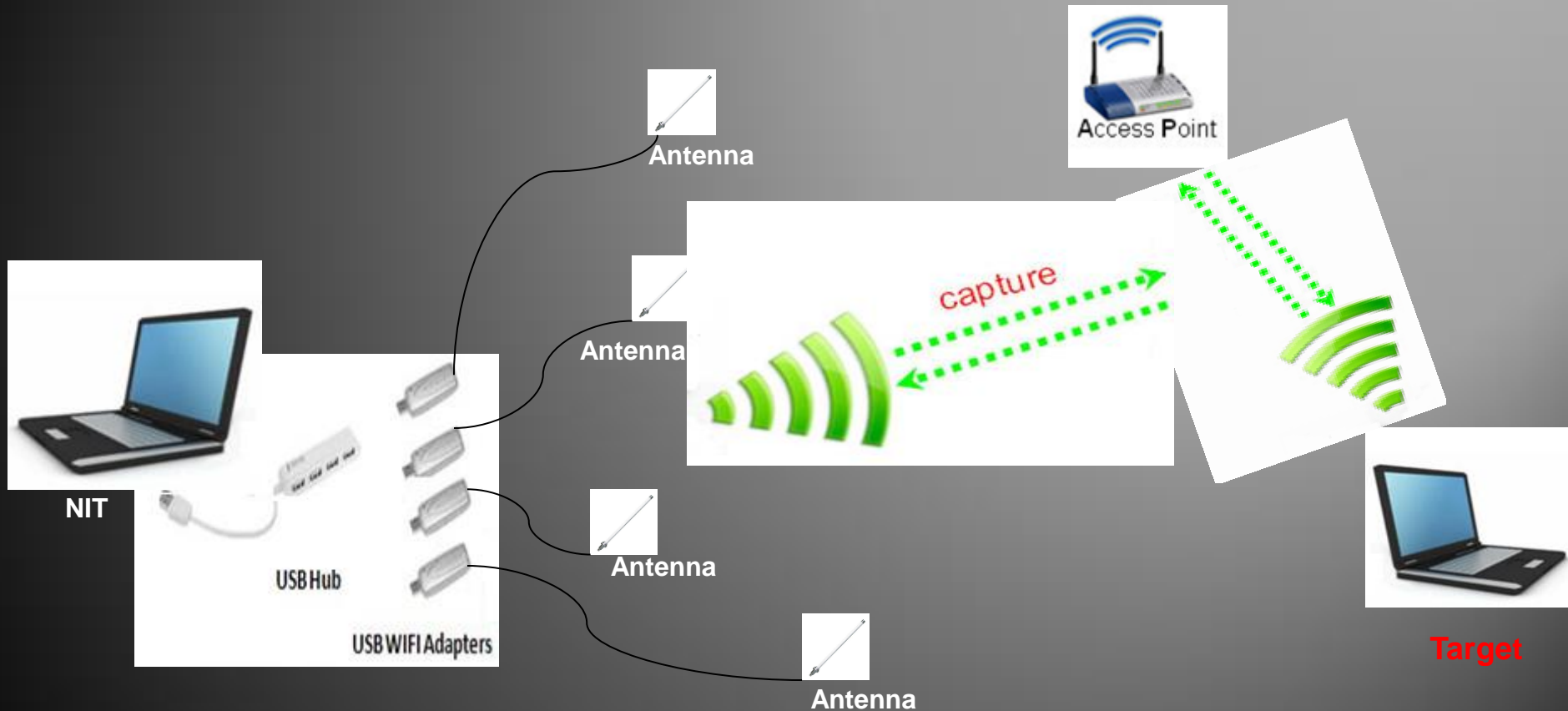
Tactic Wireless Interceptor

- ▶ MFS NIT for Anti-Internal Threats
 - Target on either Access Point or Linked Devices on wireless network
 - Works on both modes of over-spilled RF wave for non-HTTPS interception and MiTM for HTTPS interception
 - Capable of protocol decoding with 140+ protocols and online services
 - Presents full reconstructed intercepted communication contents of Facebook, Gmail, Twitter, WhatsApp, ...etc.
 - With traffic statistic report for investigation
 - Works with external WPA Cracking System against unknown APs for WPA key availability
 - Portable form factor for hand carry or sedentary form factor for security surveillance

Advantages

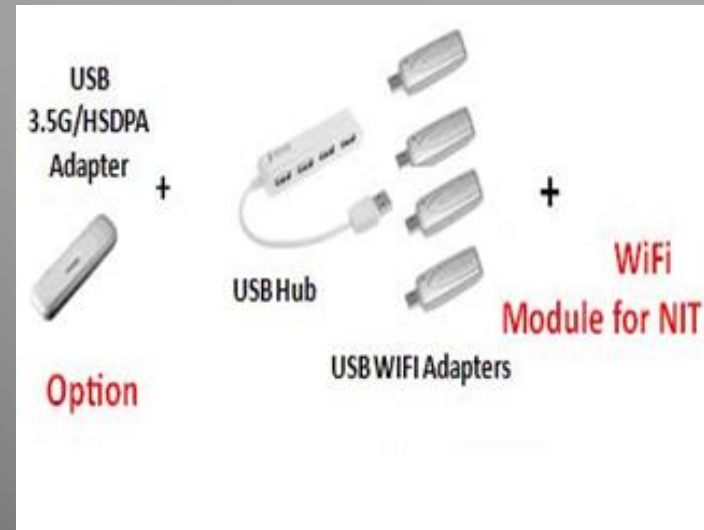
- ▶ Easily implemented and powerful system performance
- ▶ Long distance of RF scanning capability and high gain rate (92%+) of RF capture
 - By multiple external high gain antenna
- ▶ Online decoding capability on 140+ online services and protocols with full presentation of both CDR and reconstructed content
- ▶ Case management for investigation on internal threats or cybercrime instances
- ▶ Co-work with WPA Cracking system for both WEP and WPA key management
- ▶ Equipped with data scoping and analysis tool for report utilities
- ▶ Comply fully with ISO 27037 standard for digital data forensic procedure

Multiple-point Wireless Interception



Options

- ▶ For Extended Wireless Interception
 - USB Hub X2
 - WiFi Dongle X4
 - 8 dB Antenna X4
- ▶ For Backend Communication
 - 3.5G/HSPDA USB Dongle



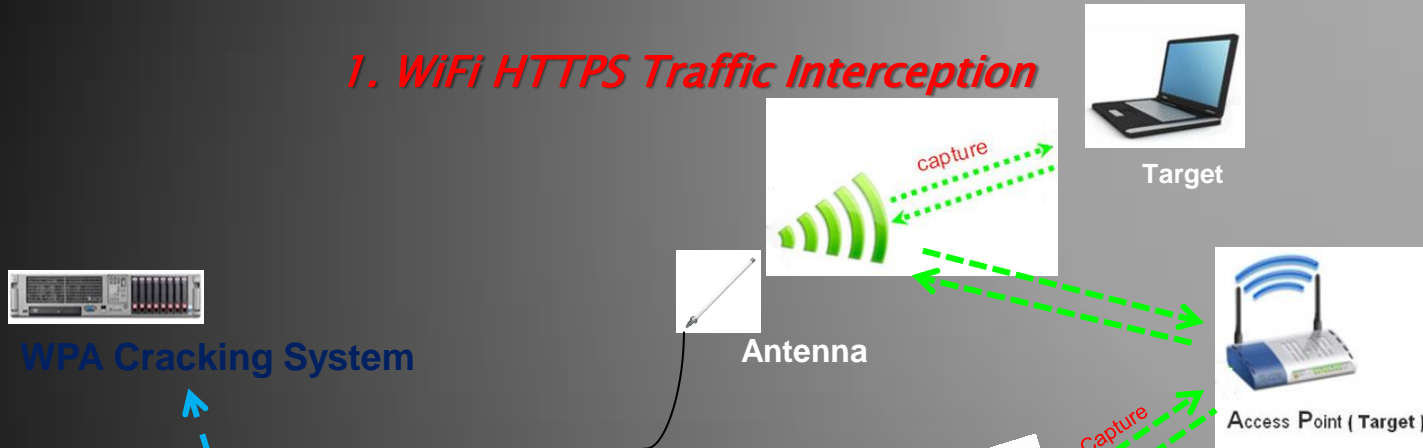
Antenna

WPA Cracking System

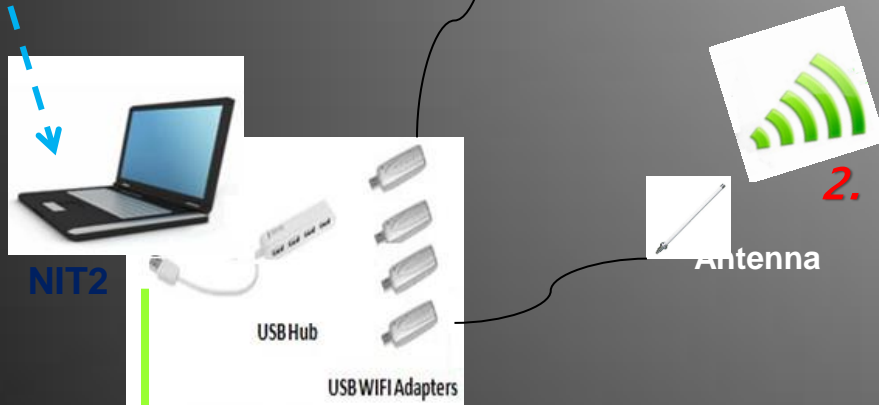
- ▶ Work on cracking process with unknown key of WPA-PSA and WPA-802.1X
- ▶ Elapsed period by the complexity of key architecture
 - Varied from 20 minutes to few days
- ▶ 2 different deployment ways for enhanced key cracking speed
 - Deployment by Individual system with multiple GPUs
 - Deployment by multiple systems for parallel processing

Full Deployment for HTTPS and LAN Interception

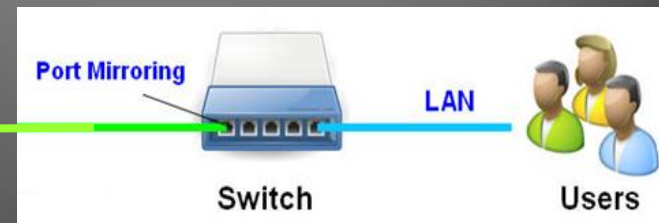
1. WiFi HTTPS Traffic Interception



2. WiFi Traffic Interception



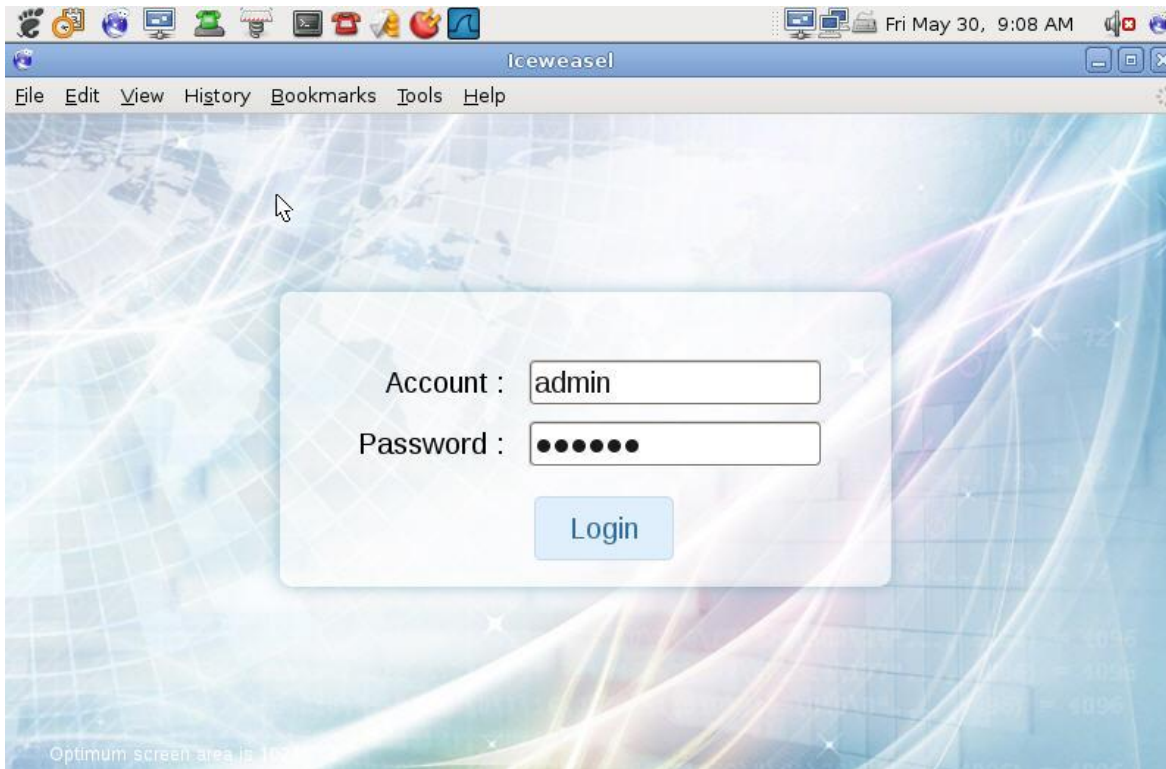
3. LAN Traffic Interception



System Operation



Login



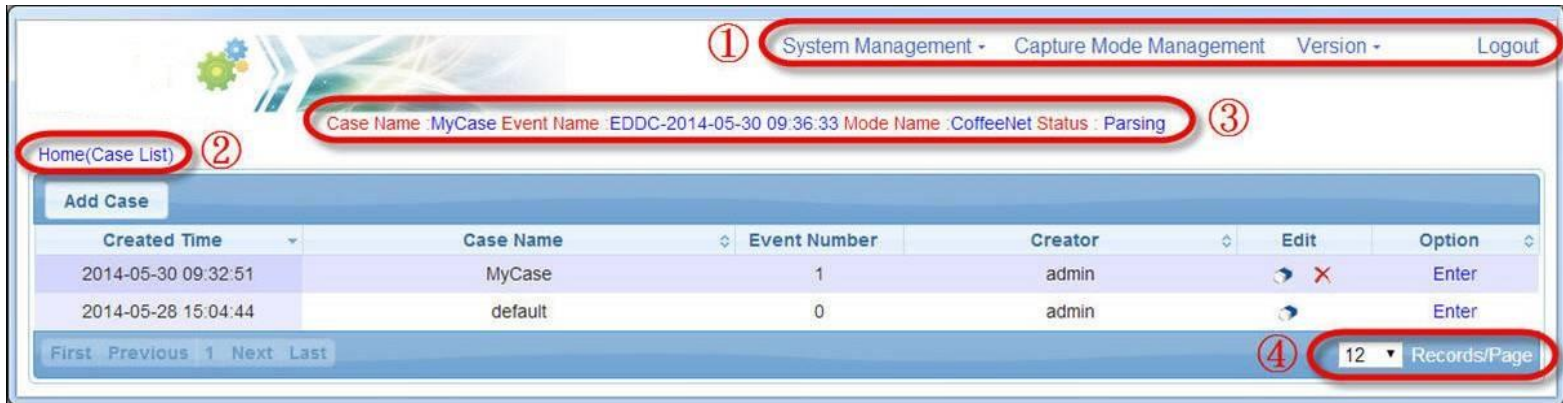
Default

Account : **admin**




Password : **000000**

Main Page

- Main page



The screenshot shows the MFS Main Page interface. It features a navigation bar at the top with links for 'System Management', 'Capture Mode Management', 'Version', and 'Logout'. Below the navigation bar, there is a breadcrumb trail: 'Home(Case List)'. A status bar displays 'Case Name : MyCase Event Name : EDDC-2014-05-30 09:36:33 Mode Name : CoffeeNet Status : Parsing'. The main content area includes an 'Add Case' button and a table of cases. The table has columns for 'Created Time', 'Case Name', 'Event Number', 'Creator', 'Edit', and 'Option'. The first row shows a case named 'MyCase' created on 2014-05-30 09:32:51 by 'admin'. The second row shows a case named 'default' created on 2014-05-28 15:04:44 by 'admin'. At the bottom right, there is a pagination control showing '12 Records/Page'.

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-05-30 09:32:51	MyCase	1	admin	 	Enter
2014-05-28 15:04:44	default	0	admin		Enter

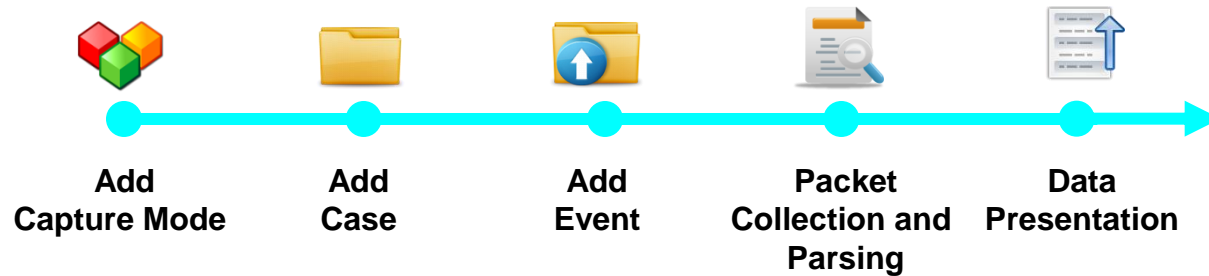
Row1: System function

Row2: Page Path

Row3: Work Status

Row4: Every Page

Workflow

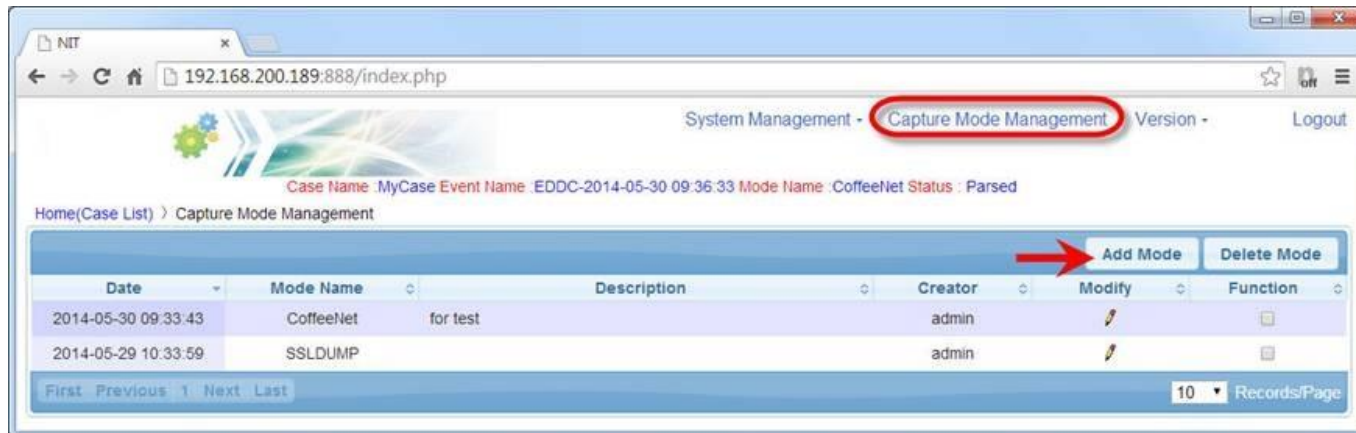


The system can perform only one job simultaneously

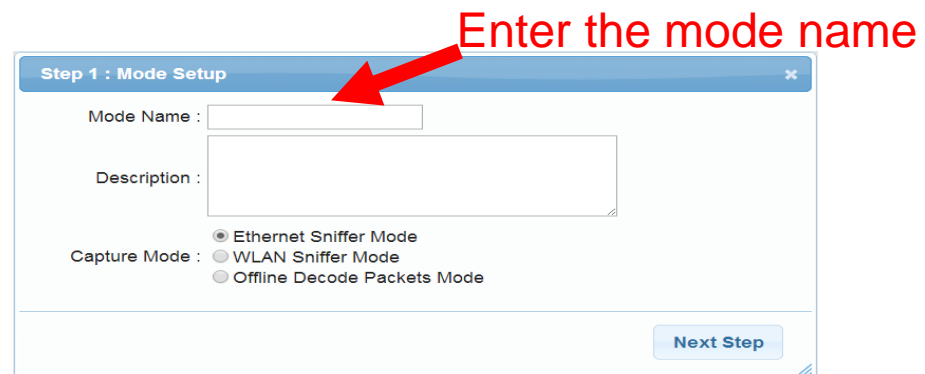
- Start a capture job
 - a. add **mode**
 - b. add **case**
 - c. add **event**
 - d. packet collection and parsing
 - e. data presentation

New Capture Job Adding

- Add mode : create the user defined mode by real situation



Enter the mode name



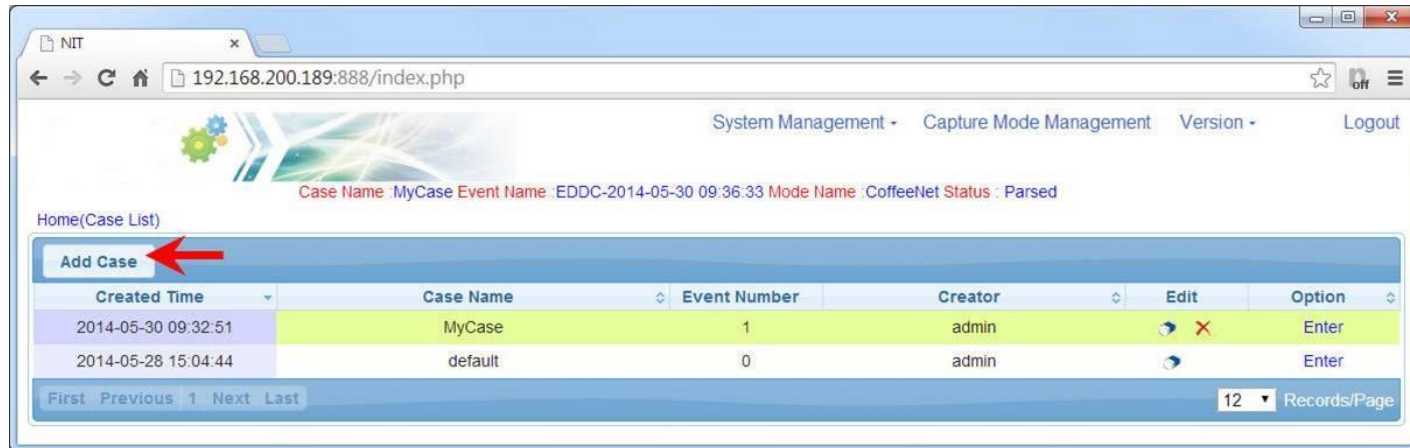
The form is titled 'Step 1 : Mode Setup'. It contains the following fields and options:

- Mode Name :
- Description :
- Capture Mode :
 - Ethernet Sniffer Mode
 - WLAN Sniffer Mode
 - Offline Decode Packets Mode




A 'Next Step' button is located at the bottom right of the form. A red arrow points from the text 'Enter the mode name' to the 'Mode Name' input field.

Capture Job Starting

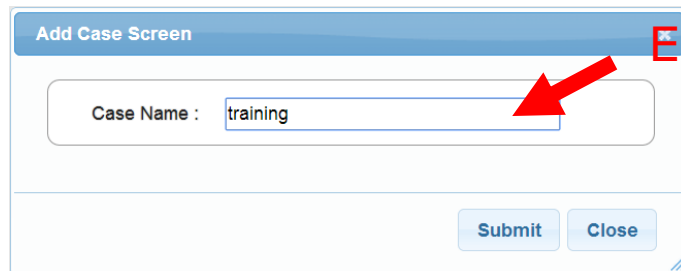
- Add case : used for storing events and event records



The screenshot shows a web browser window with the URL 192.168.200.189:888/index.php. The page title is 'System Management - Capture Mode Management Version - Logout'. Below the title, there is a navigation bar with 'Home(Case List)'. A red arrow points to the 'Add Case' button. Below the button is a table with the following data:

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-05-30 09:32:51	MyCase	1	admin	 	Enter
2014-05-28 15:04:44	default	0	admin		Enter

At the bottom of the table, there are navigation links: 'First Previous 1 Next Last' and a dropdown menu showing '12 Records/Page'.

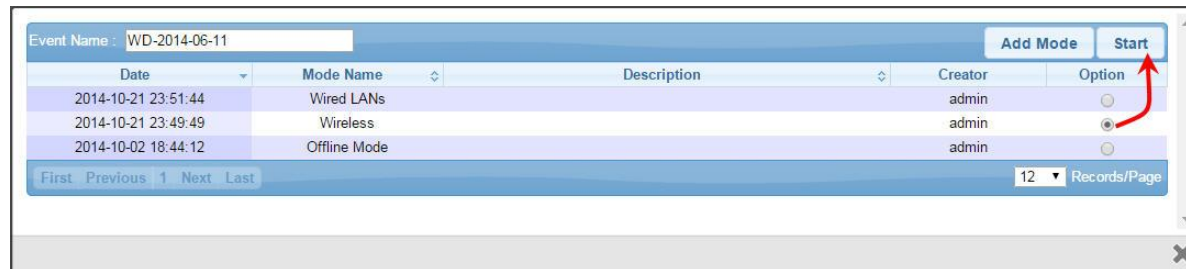
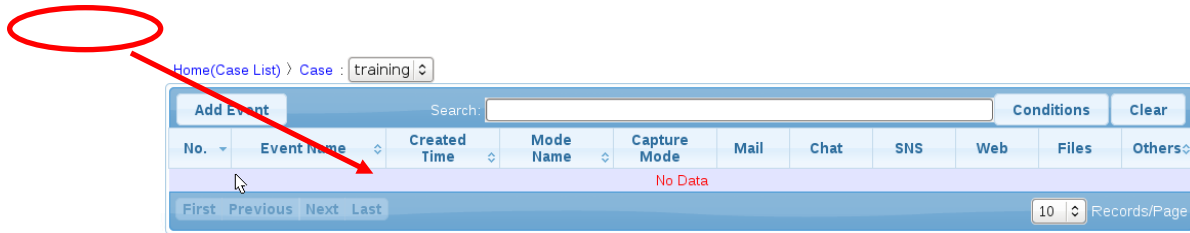


The screenshot shows a form titled 'Add Case Screen'. It has a text input field for 'Case Name' with the value 'training'. A red arrow points to the input field. Below the input field are two buttons: 'Submit' and 'Close'.

Enter the case name

New Event Adding

- Add event : start a capture activity



Packets Collecting

- packet collect and parsing :

System Management - Capture Mode Management Version - Logout

Case Name : training Event Name : WD-2014-06-11 16:09:21 Mode Name : Wireless Status : Start Stop

Home(Case List)

Add Case

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-06-11 15:42:08	training	1	admin		Enter
2014-06-10 15:21:55	default	0	admin		Enter

First Previous 1 Next Last 12 Records/Page

Message

Function	Message
Case Name	training
Event Name	WD-2014-06-11 16:09:21
Creator	admin
Created Time	2014-06-11 16:09:24
Mode Name	Wireless
Capture Mode	WLAN Sniffer Mode
HTTPS/SSL Module Enable	No
Status	Stop
Rawdata Path	/home/admin/cases/training

Close

Data Presentation

- Data Presentation :



System Management - Capture Mode Management Version - Logout

Case Name : training Event Name : WD-2014-06-11 16:09:21 Mode Name : Wireless Status : Start Stop

Home(Case List)

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-06-11 15:42:08	training	1	admin		Enter
2014-06-10 15:21:55	default	0	admin		Enter

12 Records/Page

Home(Case List) Case : training

No.	Event Name	Created Time	Mode Name	Capture Mode	Mail	Chat	SNS	Web	Files	Others
1	EDDC-2014-06-11 17:17:21	2014-06-11 17:17:35	import	Offline Decode Packets Mode	30	4	32	2765	21	584

10 Records/Page

Mail : POP3,SMTP,IMAP,WebMail

Chat : Yahoo,ICQ,Skype etc.

SNS : Facebook, Twitter,Plurk

Web : Video Stream,Web page, HTTP file upload/download

Files : FTP,P2P,Dropbox,Evernote

Others : Telnet,Online game,Web password etc.

Configuration of Capture Mode



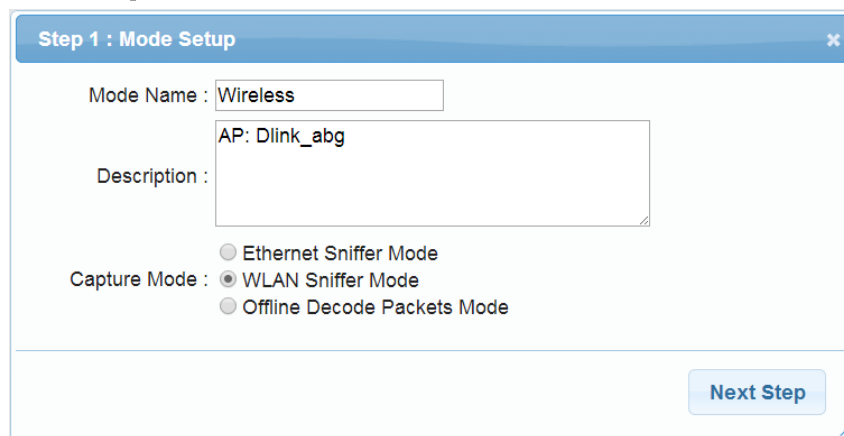
Capture Mode Management

- WLAN Sniffer Mode without HTTPS



WLAN Sniffer Mode I

- Step 1 : mode setup



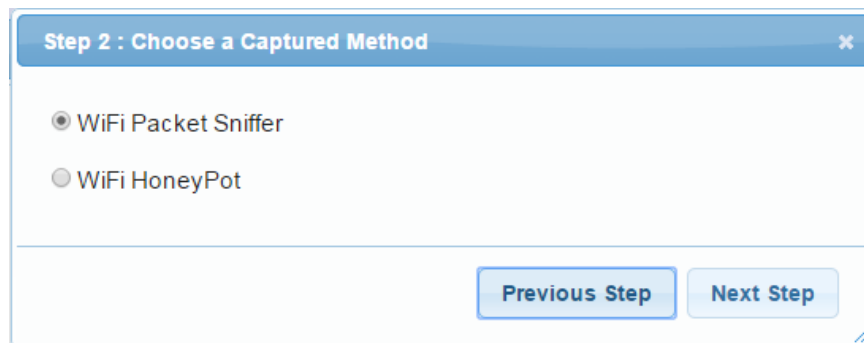
Step 1 : Mode Setup

Mode Name :

Description :

Capture Mode : Ethernet Sniffer Mode
 WLAN Sniffer Mode
 Offline Decode Packets Mode

- Step 2 : Choose a captured method

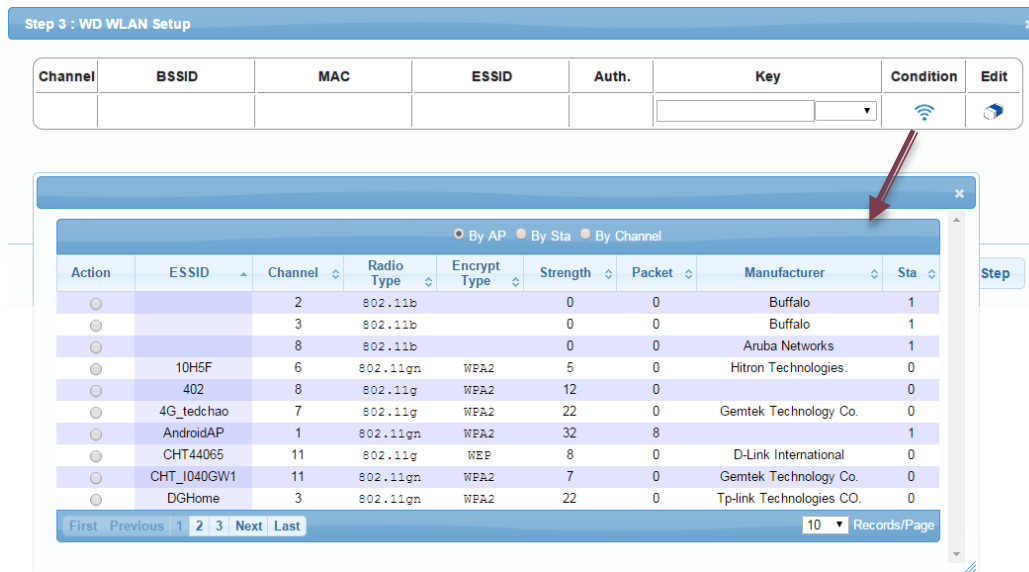


Step 2 : Choose a Captured Method

WiFi Packet Sniffer
 WiFi HoneyPot

WLAN Sniffer Mode II

- Step 3 : select capture target



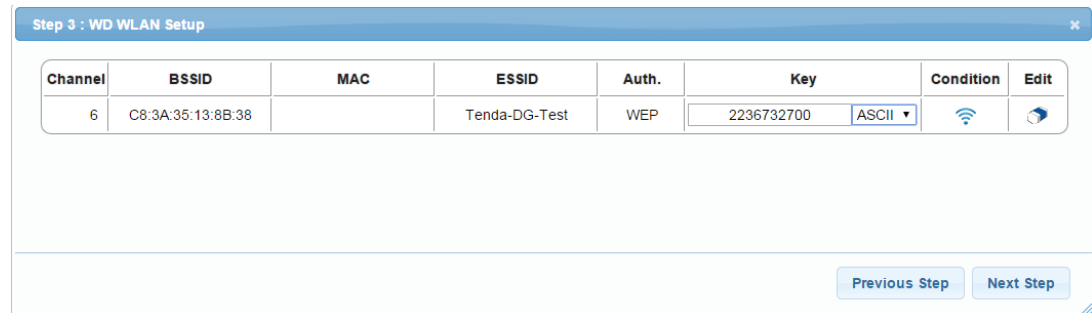
The screenshot shows the 'Step 3 : WD WLAN Setup' window. At the top, there is a table with columns: Channel, BSSID, MAC, ESSID, Auth., Key, Condition, and Edit. Below this is a larger window displaying a list of WLAN networks. The list has columns: Action, ESSID, Channel, Radio Type, Encrypt Type, Strength, Packet, Manufacturer, and Sta. A red arrow points to the 'By AP' radio button at the top of the list window.

Action	ESSID	Channel	Radio Type	Encrypt Type	Strength	Packet	Manufacturer	Sta
<input type="radio"/>		2	802.11b		0	0	Buffalo	1
<input type="radio"/>		3	802.11b		0	0	Buffalo	1
<input type="radio"/>		8	802.11b		0	0	Aruba Networks	1
<input type="radio"/>	10H5F	6	802.11gn	WPA2	5	0	Hitron Technologies.	0
<input type="radio"/>	402	8	802.11g	WPA2	12	0		0
<input type="radio"/>	4G_tedchao	7	802.11g	WPA2	22	0	Gemtek Technology Co.	0
<input type="radio"/>	AndroidAP	1	802.11gn	WPA2	32	8		1
<input type="radio"/>	CHT44065	11	802.11g	WEP	8	0	D-Link International	0
<input type="radio"/>	CHT_J040GW1	11	802.11gn	WPA2	7	0	Gemtek Technology Co.	0
<input type="radio"/>	DGHome	3	802.11gn	WPA2	22	0	Tp-link Technologies CO.	0

Radio Type:

802.11b/802.11g/802.11a/802.11gn/802.11an

Encrypt Type: OPN / WEP / WPA / WPA2



The screenshot shows the 'Step 3 : WD WLAN Setup' window with a single WLAN network selected. The table below shows the details of the selected network.

Channel	BSSID	MAC	ESSID	Auth.	Key	Condition	Edit
6	C8:3A:35:13:8B:38		Tenda-DG-Test	WEP	2236732700 ASCII		

At the bottom of the window, there are 'Previous Step' and 'Next Step' buttons.

WLAN Sniffer Mode III

- Step 4 : port setup

Step 4 : Port Setup

Service	Port	Action	Description
AD	88	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Active Directory Service
FTP	21,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	FTP Service
GAME	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Online game Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Message Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Voice Service
ICQ	5190,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
IMAP	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IMAP Service
IRC	6667	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IRC chat
MSN	1863	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service

Previous Step Finish

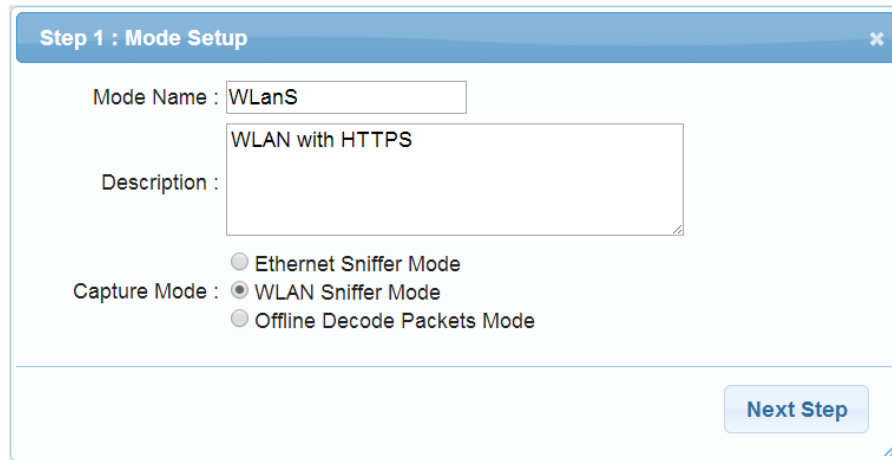
Capture Mode Management

- WLAN Sniffer Mode with HTTPS



WLAN Sniffer Mode with HTTPS

- Step 1 : mode setup



Step 1 : Mode Setup

Mode Name :

Description :

Capture Mode :

- Ethernet Sniffer Mode
- WLAN Sniffer Mode
- Offline Decode Packets Mode

Next Step

- Step 2 : Choose a captured method



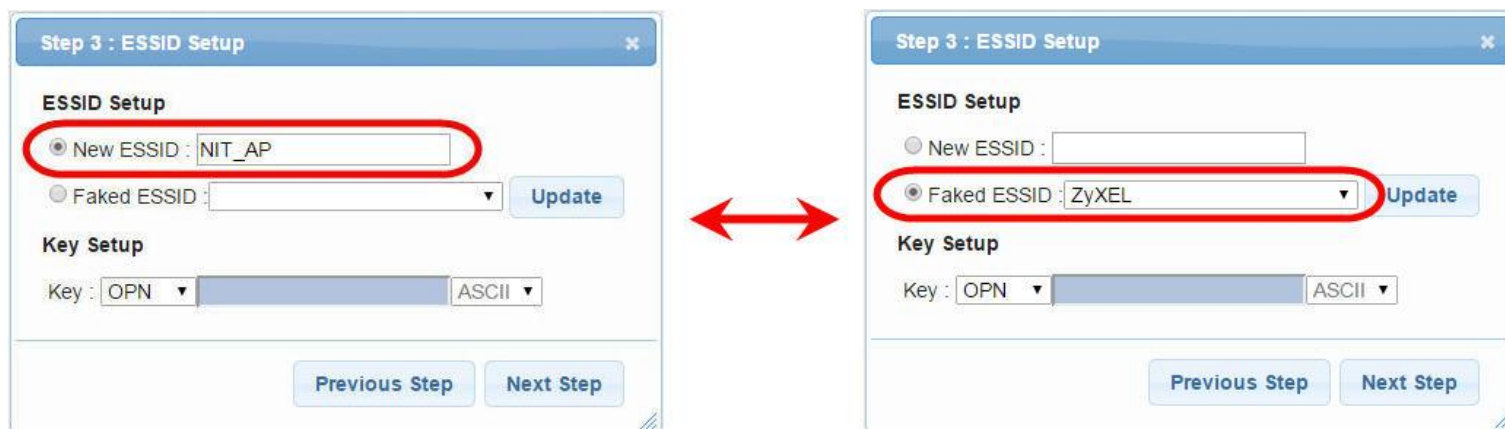
Step 2 : Choose a Captured Method

- WiFi Packet Sniffer
- WiFi HoneyPot

Previous Step Next Step

WLAN Sniffer Mode with HTTPS

- Step 3 : setting Fake AP-ESSID



Step 3 : ESSID Setup

ESSID Setup

New ESSID : NIT_AP

Faked ESSID : [Empty] Update

Key Setup

Key : OPN [Empty] ASCII

Previous Step Next Step

Step 3 : ESSID Setup

ESSID Setup

New ESSID : [Empty]

Faked ESSID : ZyXEL Update

Key Setup

Key : OPN [Empty] ASCII

Previous Step Next Step

- Step 4 : setting Fake AP-DHCP



Step 4 : DHCP Server Setup

Gateway : 10.0.0.254

Subnet : 10.0.0.0

Netmask : 255.0.0.0

IP Range : 10.0.0.99 ~ 10.0.0.200

Previous Step Next Step

WLAN Sniffer Mode with HTTPS

- Step 5 : select MITM device



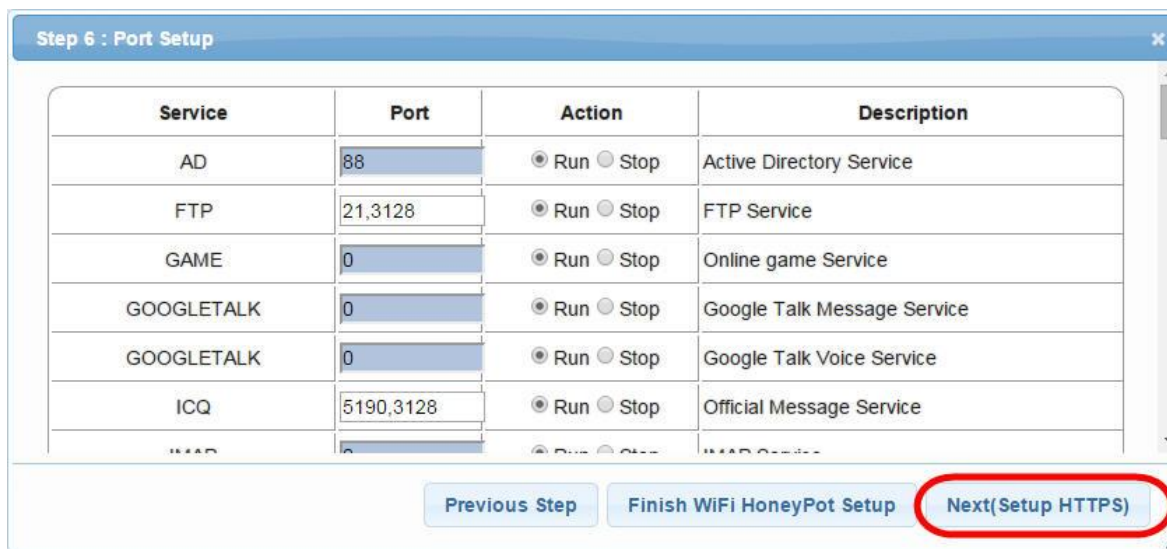
Step 5 : In & Out Interface Setup

Out Interface : eth0

In Interface : wlan3

Previous Step Next Step

- Step 6 : port setup



Step 6 : Port Setup

Service	Port	Action	Description
AD	88	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Active Directory Service
FTP	21,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	FTP Service
GAME	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Online game Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Message Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Voice Service
ICQ	5190,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
WAP	5	<input checked="" type="radio"/> Run <input type="radio"/> Stop	WAP Service

Previous Step Finish WiFi HoneyPot Setup **Next(Setup HTTPS)**

WLAN Sniffer Mode with HTTPS

- Step 7 : Certificate



Step 7 : Transparent Proxy(About SSL)

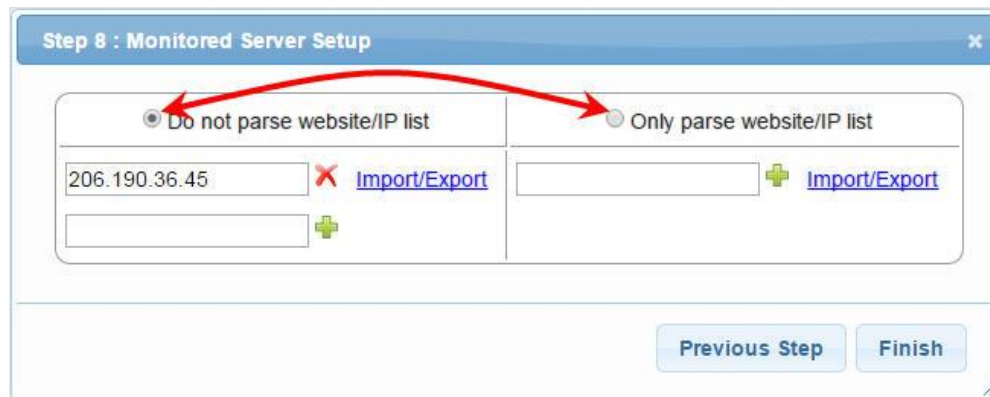
Use Build-in Certificate [Modify](#) [Export](#)
 Import Legal Certificate [Certificate Import](#) [Key Import](#)

Certificate Information

Issued To	Issued By
Country : AU	Country : AU
State or Province : Some-State	State or Province : Some-State
Locality Name :	Locality Name :
Organization Name : Network-Recorder	Organization Name : Network-Recorder
Organization Unit :	Organization Unit :
User :	User :

[Previous Step](#) [Next Step](#)

- Step 8 : setting target



Step 8 : Monitored Server Setup

Do not parse website/IP list Only parse website/IP list

206.190.36.45 ✖ Import/Export	<input type="text"/> + Import/Export
<input type="text"/> +	

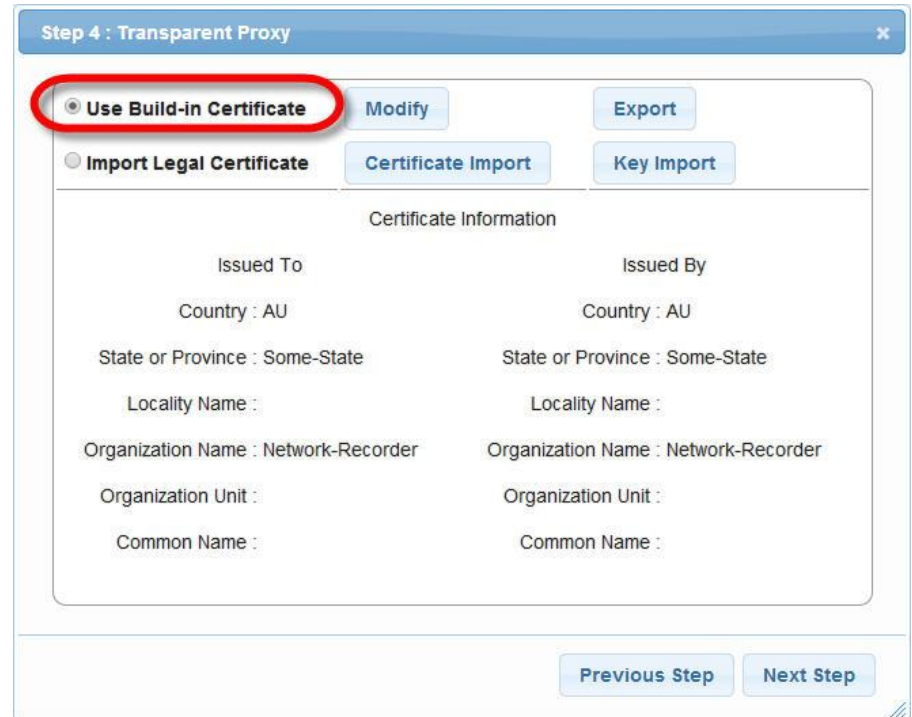
[Previous Step](#) [Finish](#)

Certificate

- **Browser Certificate Warning**
 - Once the HTTPS/SSL function is enabled in Transparent Proxy connection mechanism, the browser will pop up a connection security warning message or abnormally terminate the incoming webpage when target user opens the HTTPS webpage.
 - For such issue, there are two options provided to solve it.

Build-in Certificate

- Build-in Certificate
 - Use the system certificate for verification: press Export button to download and install key.zip certificate file in the target user computer.
 - Press Modify button, you can import and edit information for the certificate content.



Step 4 : Transparent Proxy

Use Build-in Certificate Import Legal Certificate

Modify Export
Certificate Import Key Import

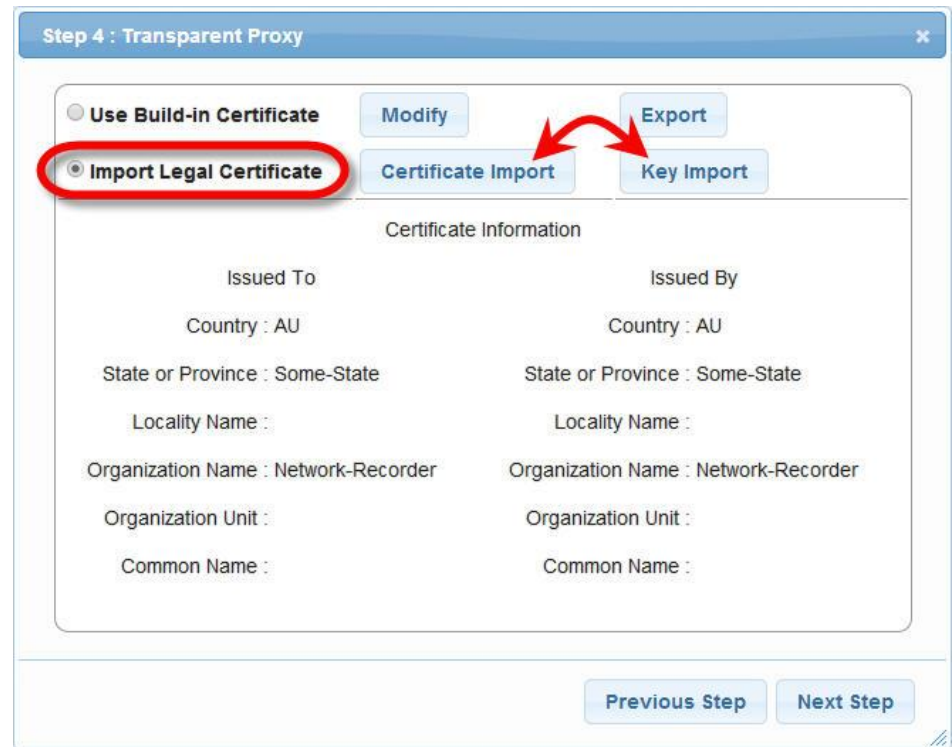
Certificate Information

Issued To	Issued By
Country : AU	Country : AU
State or Province : Some-State	State or Province : Some-State
Locality Name :	Locality Name :
Organization Name : Network-Recorder	Organization Name : Network-Recorder
Organization Unit :	Organization Unit :
Common Name :	Common Name :

Previous Step Next Step

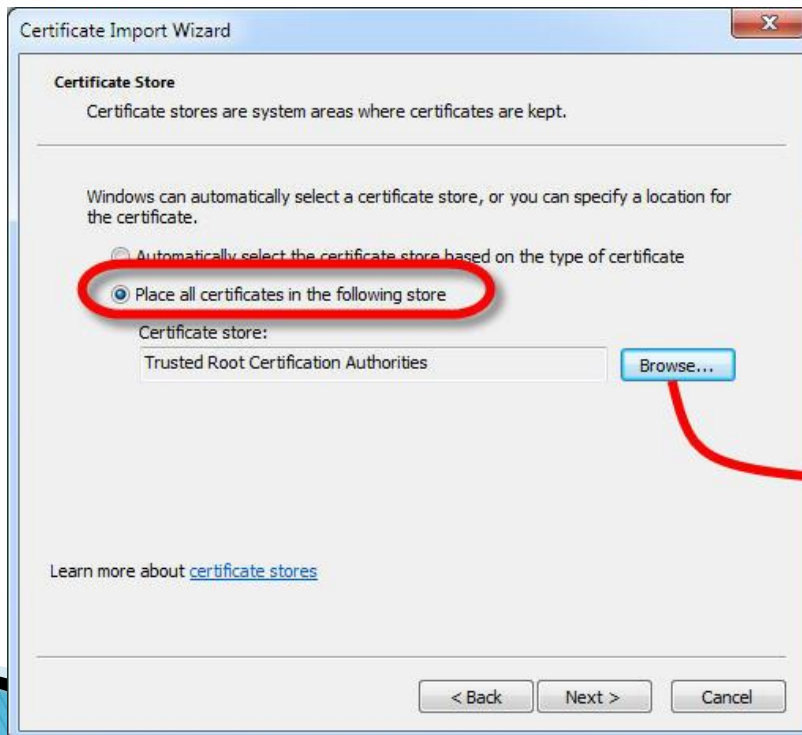
Certificate Import

- Legal Certificate Import
 - If you has a legitimate certificate and key, you can upload and replace the build-in certificate
 - Please choose the Certificate Import and Key Import button to upload it.

A screenshot of a software configuration window titled "Step 4 : Transparent Proxy". The window has a blue header bar with the title and a close button. Below the header, there are two radio buttons: "Use Build-in Certificate" (unselected) and "Import Legal Certificate" (selected and circled in red). To the right of these buttons are "Modify" and "Export" buttons. Below the radio buttons are two buttons: "Certificate Import" and "Key Import", both of which have red arrows pointing to them from the "Export" button. Below these buttons is a section titled "Certificate Information" containing two columns of fields. The left column is labeled "Issued To" and the right column is labeled "Issued By". Both columns have the same values: "Country : AU", "State or Province : Some-State", "Locality Name :", "Organization Name : Network-Recorder", "Organization Unit :", and "Common Name :". At the bottom right of the window are "Previous Step" and "Next Step" buttons.

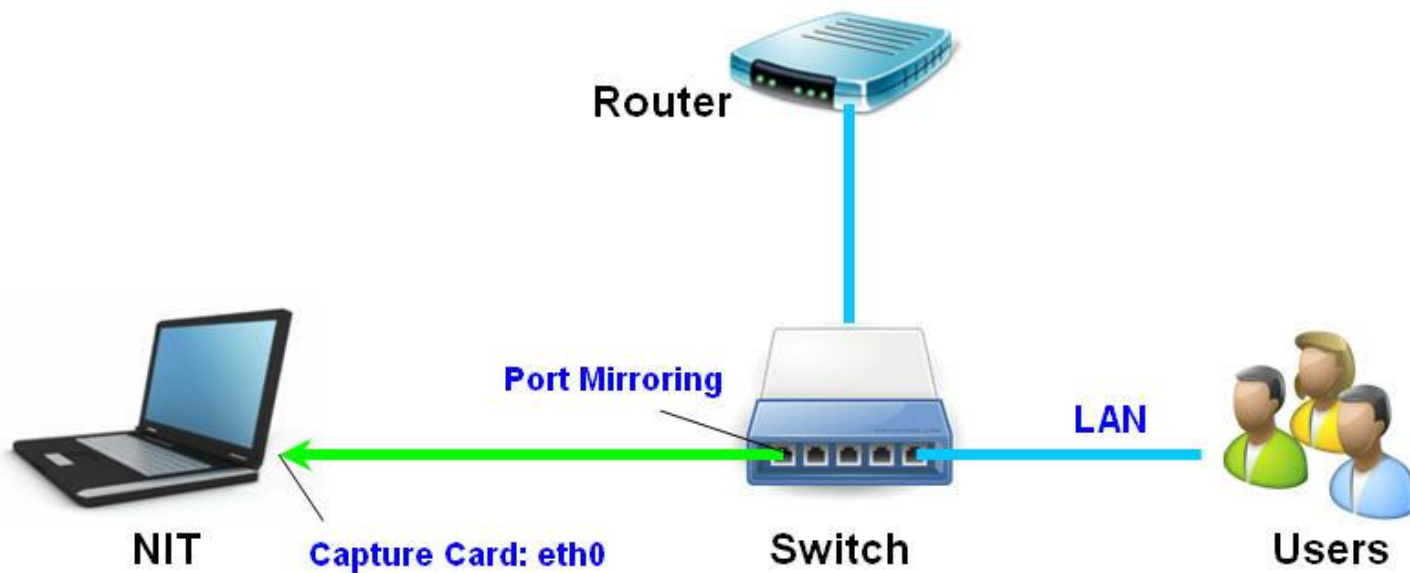
Certificate Installation

- Install Certificate File into Target
 - After decompressing key.zip, please click the file of server.crt to invoke Certificate Import Wizard
 - Select *install certificate function* and install the certificate to the Trusted Root Certification Authorities.



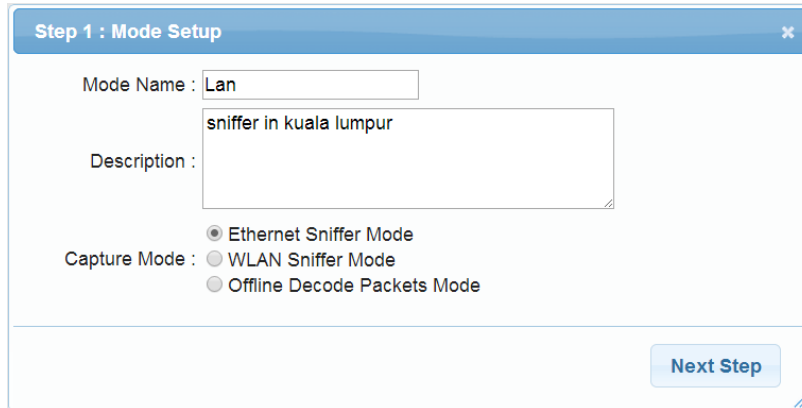
Capture mode management

- Ethernet Sniffer Mode without HTTPS



Ethernet Sniffer Mode I

- Step 1 : mode setup

A screenshot of a software dialog box titled "Step 1 : Mode Setup". It contains a "Mode Name" field with the text "Lan", a "Description" field with the text "sniffer in kuala lumpur", and three radio button options under "Capture Mode": "Ethernet Sniffer Mode" (selected), "WLAN Sniffer Mode", and "Offline Decode Packets Mode". A "Next Step" button is located at the bottom right.

Step 1 : Mode Setup

Mode Name : Lan

Description : sniffer in kuala lumpur

Capture Mode : Ethernet Sniffer Mode
 WLAN Sniffer Mode
 Offline Decode Packets Mode

Next Step

- Step 2 : HTTPS/SSL enable

A screenshot of a software dialog box titled "Step 2 : HTTPS/SSL Mode Enable". It contains two radio button options: "No" (selected) and "Yes". At the bottom, there are two buttons: "Previous Step" and "Next Step".

Step 2 : HTTPS/SSL Mode Enable

No
 Yes

Previous Step Next Step

- Step 3 : select capture device

Step 3 : Capture LAN is ✕

etho

Previous Step
Next Step

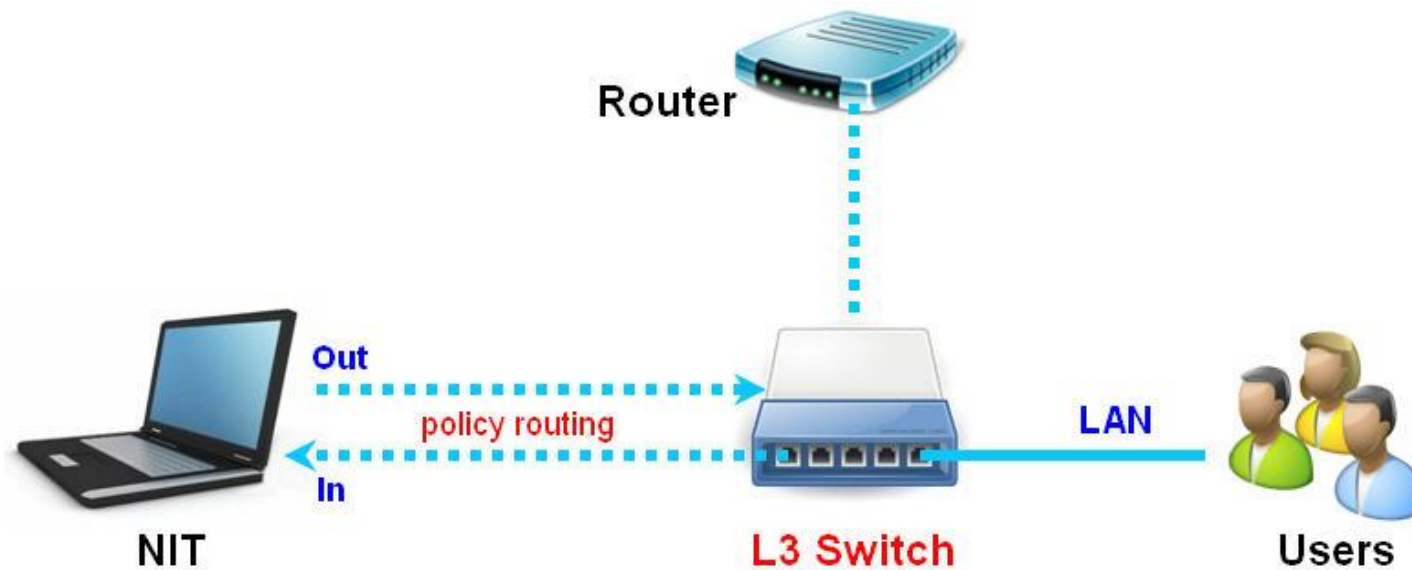
- Step 4 : port setup

Step 4 : Port Setup ✕

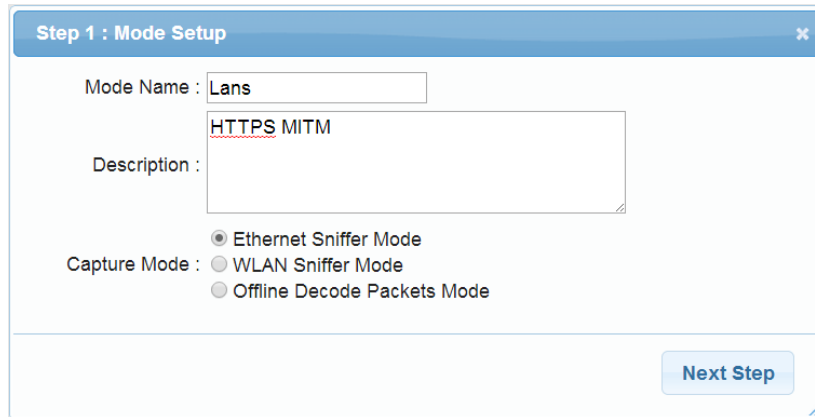
Service	Port	Action	Description
AD	<input type="text" value="88"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Active Directory Service
FTP	<input type="text" value="21,3128"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	FTP Service
GAME	<input type="text" value="0"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Online game Service
GOOGLETALK	<input type="text" value="0"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Message Service
GOOGLETALK	<input type="text" value="0"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Voice Service
ICQ	<input type="text" value="5190,3128"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
IMAP	<input type="text" value="0"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IMAP Service
IRC	<input type="text" value="6667"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IRC chat
MSN	<input type="text" value="1863"/>	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service

Previous Step
Finish

- Ethernet Sniffer Mode with Transparent Proxy



- Step 1 : mode setup



Step 1 : Mode Setup

Mode Name :

Description :

Capture Mode : Ethernet Sniffer Mode
 WLAN Sniffer Mode
 Offline Decode Packets Mode

Next Step

- Step 2 : HTTPS/SSL enable



Step 2 : HTTPS/SSL Mode Enable

No
 Yes

Previous Step Next Step

- Step 3 : Certificate

Step 4 : Transparent Proxy

Use Build-in Certificate [Modify](#) [Export](#)

Import Legal Certificate [Certificate Import](#) [Key Import](#)

Certificate Information

Issued To	Issued By
Country : AU	Country : AU
State or Province : Some-State	State or Province : Some-State
Locality Name :	Locality Name :
Organization Name : Network-Recorder	Organization Name : Network-Recorder
Organization Unit :	Organization Unit :
Common Name :	Common Name :

[Previous Step](#) [Next Step](#)

- Step 4 : setting target



Step 4 : Monitored Server Setup

Do not parse website/IP list

Only parse website/IP list

206.190.36.45  [Import/Export](#)

 [Import/Export](#)



Previous Step Next Step

A screenshot of a software window titled "Step 4 : Monitored Server Setup". The window has a blue header bar with a close button. Below the header, there are two radio buttons: "Do not parse website/IP list" (which is selected) and "Only parse website/IP list". Under the first radio button, there is a text input field containing "206.190.36.45" with a red "X" icon and an "Import/Export" link. Below this is another empty text input field with a green "+" icon. Under the second radio button, there is an empty text input field with a green "+" icon and an "Import/Export" link. At the bottom right, there are two buttons: "Previous Step" and "Next Step". A red curved arrow points from the "Only parse website/IP list" radio button to the "Do not parse website/IP list" radio button. A mouse cursor is pointing at the green "+" icon under the first radio button.

- Step 5 : select MITM device



Step 5 : In & Out Interface Setup

Out Interface : eth0

In Interface : eth0

Previous Step Next Step

A screenshot of a software window titled "Step 5 : In & Out Interface Setup". The window has a blue header bar with a close button. Below the header, there are two dropdown menus: "Out Interface" and "In Interface", both set to "eth0". At the bottom, there are two buttons: "Previous Step" and "Next Step".

- Step 6 : port setup

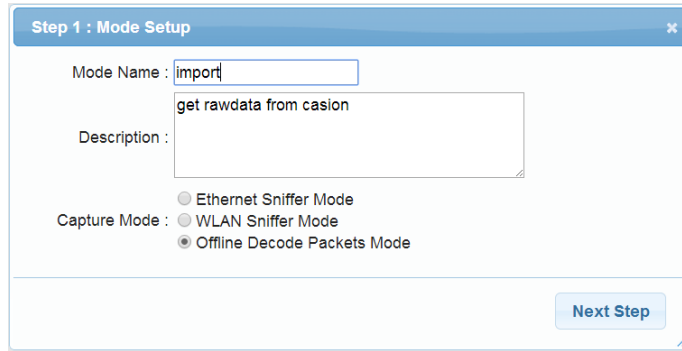
Step 6 : Port Setup

Service	Port	Action	Description
AD	88	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Active Directory Service
FTP	21,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	FTP Service
GAME	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Online game Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Message Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Voice Service
ICQ	5190,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
IMAP	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IMAP Service
IRC	6667	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IRC chat
MSN	1863	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
MSN	443	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Peer-to-peer Data
MSN	3128,8080	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Message Service via HTTP Proxy

Previous Step Finish

Offline Decode Packets Mode

- Step 1 : mode setup



Step 1 : Mode Setup

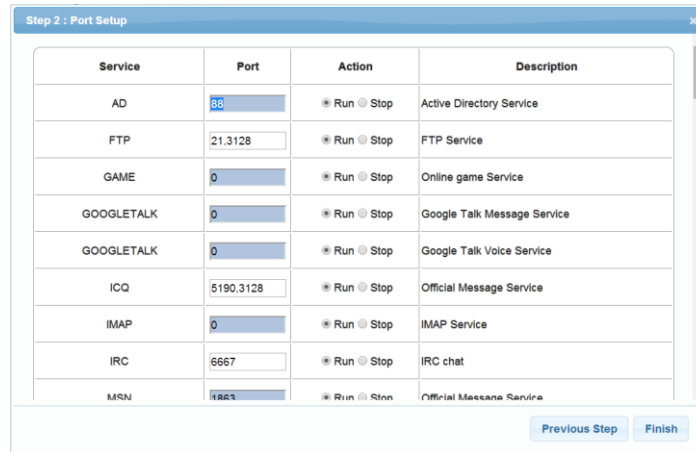
Mode Name : import

Description : get rawdata from casion

Capture Mode : Ethernet Sniffer Mode
 WLAN Sniffer Mode
 Offline Decode Packets Mode

Next Step

- Step 2 : port setup



Step 2 : Port Setup

Service	Port	Action	Description
AD	88	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Active Directory Service
FTP	21,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	FTP Service
GAME	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Online game Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Message Service
GOOGLETALK	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Google Talk Voice Service
ICQ	5190,3128	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Message Service
IMAP	0	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IMAP Service
IRC	6667	<input checked="" type="radio"/> Run <input type="radio"/> Stop	IRC chat
MSN	1823	<input checked="" type="radio"/> Run <input type="radio"/> Stop	Official Messana Service

Previous Step Finish

Offline Decode Packets Mode

- Step 3 : Import Packet File

Path : /home/admin/media/disk/pcap

2
Read

<input type="checkbox"/>	Category	Format	Size	Last modified Date
<input checked="" type="checkbox"/>	yam20091102.pcap	Wired	3.85 M	2010-09-30 16:18:26
<input checked="" type="checkbox"/>	yahoold-20091102.cap	Wired	1.69 M	2010-09-30 16:18:26
<input checked="" type="checkbox"/>	yahoofile.pcap	Wired	48.85 K	2010-09-30 16:18:26
<input checked="" type="checkbox"/>	yahoo2_0.cap	Wired	1.30 M	2010-09-30 16:18:28
<input checked="" type="checkbox"/>	yahoo2-20091102.pcap	Wired	2.11 M	2010-09-30 16:18:38
<input checked="" type="checkbox"/>	yahoo.pcap	Wired	3.71 M	2010-09-30 16:18:28
<input checked="" type="checkbox"/>	yahoo.cap	Wired	1.17 M	2010-09-30 16:18:30
<input checked="" type="checkbox"/>	yahoo-web.pcap	Wired	777.24 K	2010-09-30 16:18:30
<input checked="" type="checkbox"/>	wow.cap	Wired	47.06 K	2010-09-30 16:18:32
<input checked="" type="checkbox"/>	windowslive.cap	Wired	1.21 M	2010-09-30 16:18:32
<input type="checkbox"/>	ut.pcap	Wired	306.15 K	2010-09-30 16:18:34

1

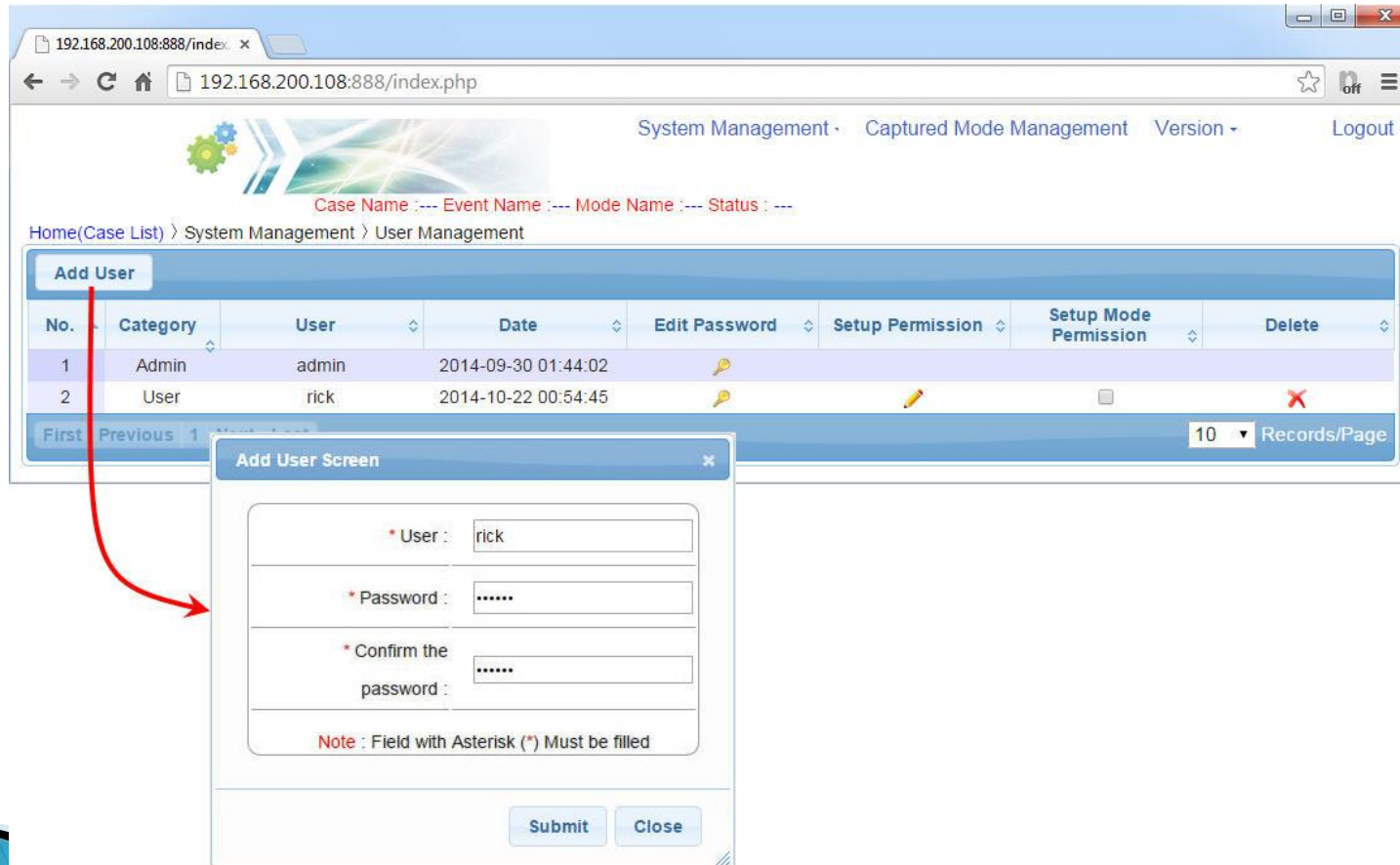
X

System Management



User Management

- User Management
 - Add User:



The screenshot displays a web application interface for user management. The main window shows a table of users with columns for No., Category, User, Date, Edit Password, Setup Permission, Setup Mode Permission, and Delete. A modal dialog titled 'Add User Screen' is open, showing a form with fields for User, Password, and Confirm the password. A red arrow points from the 'Add User' button in the table to the modal dialog.

System Management · Captured Mode Management · Version · Logout

Case Name : --- Event Name : --- Mode Name : --- Status : ---

Home(Case List) > System Management > User Management

Add User

No.	Category	User	Date	Edit Password	Setup Permission	Setup Mode Permission	Delete
1	Admin	admin	2014-09-30 01:44:02				
2	User	rick	2014-10-22 00:54:45			<input type="checkbox"/>	

First Previous 1 10 Records/Page

Add User Screen

* User :

* Password :

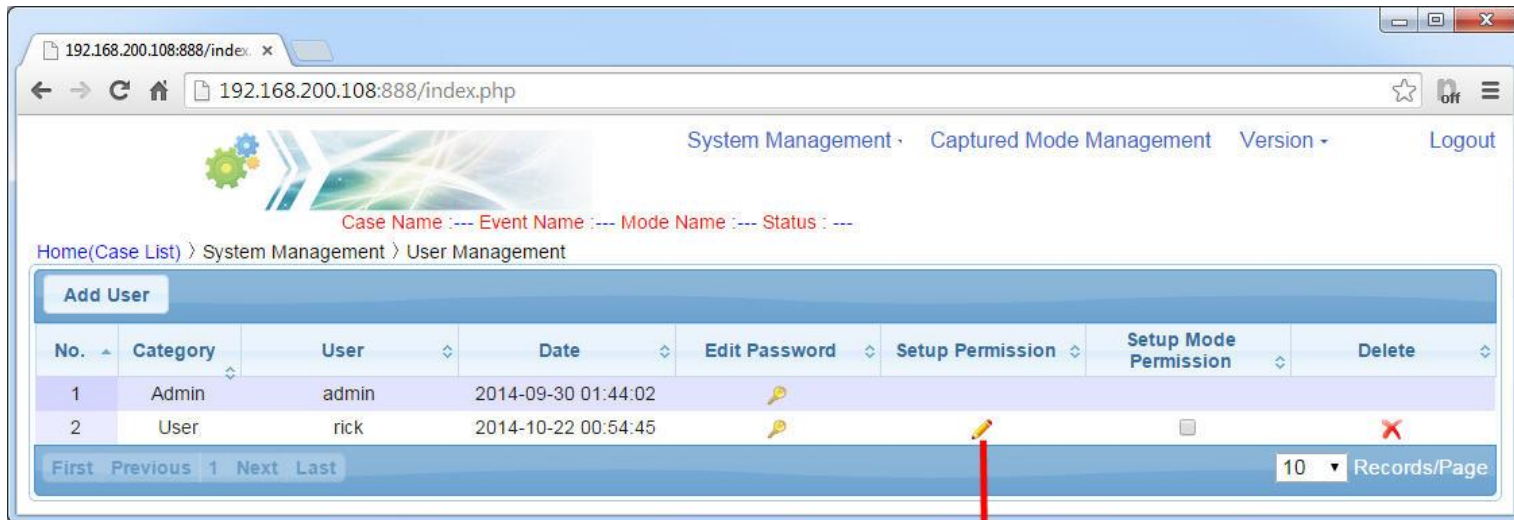
* Confirm the password :

Note : Field with Asterisk (*) Must be filled

Submit Close

User Authority Management

- Project Authority Setting :



192.168.200.108:888/index.php

System Management · Captured Mode Management · Version · Logout

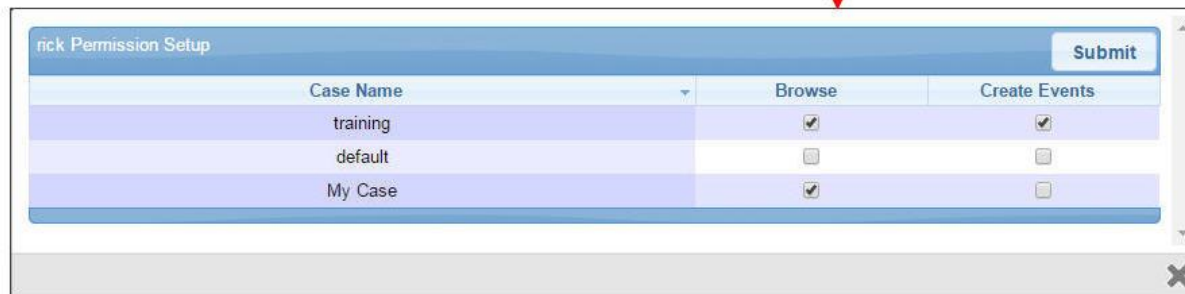
Case Name :--- Event Name :--- Mode Name :--- Status :---

Home(Case List) > System Management > User Management

Add User

No.	Category	User	Date	Edit Password	Setup Permission	Setup Mode Permission	Delete
1	Admin	admin	2014-09-30 01:44:02				
2	User	rick	2014-10-22 00:54:45			<input type="checkbox"/>	

First Previous 1 Next Last 10 Records/Page



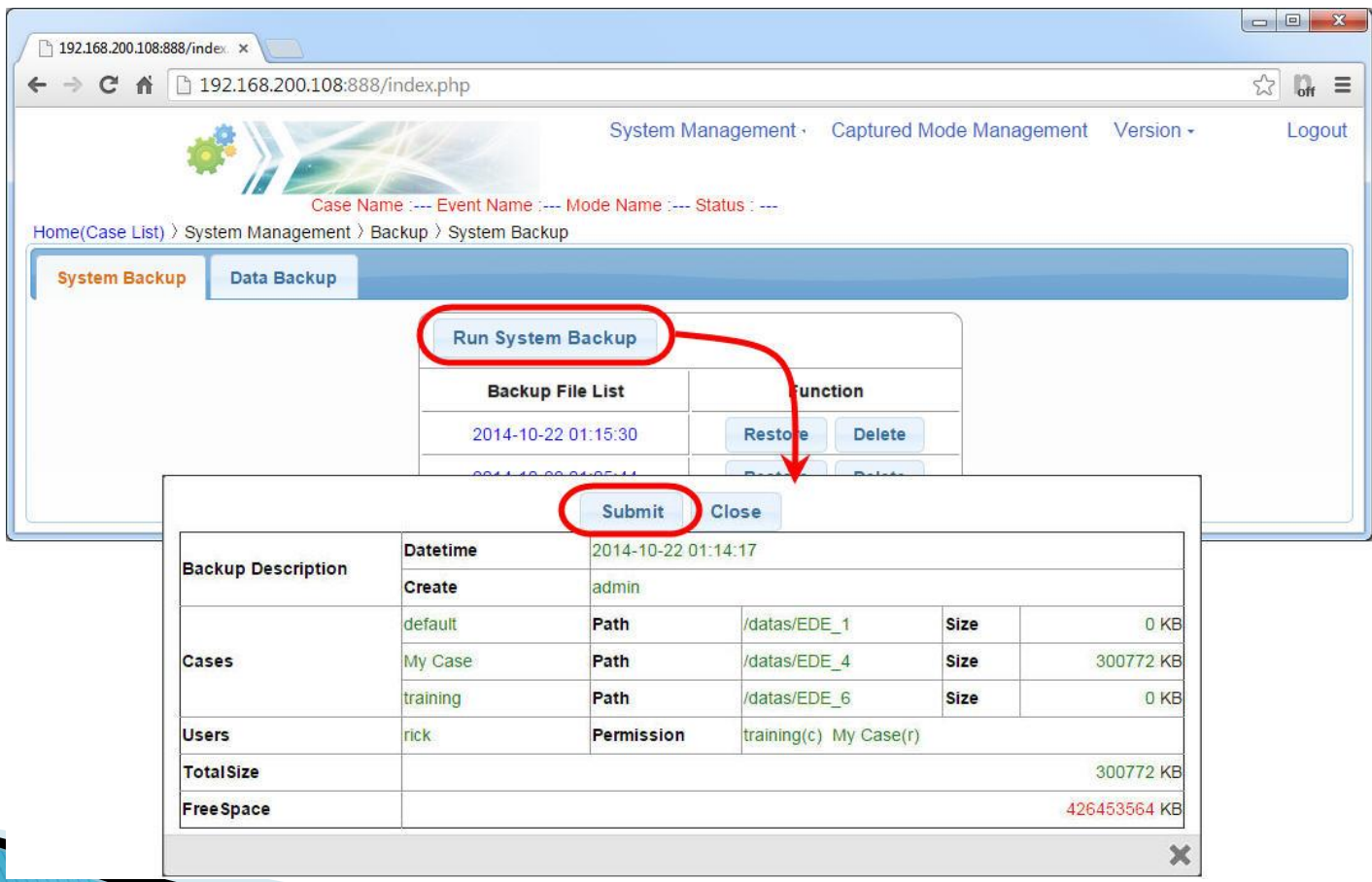
rick Permission Setup

Submit

Case Name	Browse	Create Events
training	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
default	<input type="checkbox"/>	<input type="checkbox"/>
My Case	<input checked="" type="checkbox"/>	<input type="checkbox"/>

System Backup Management

- Backup– System Backup
 - Add a new Backup file:

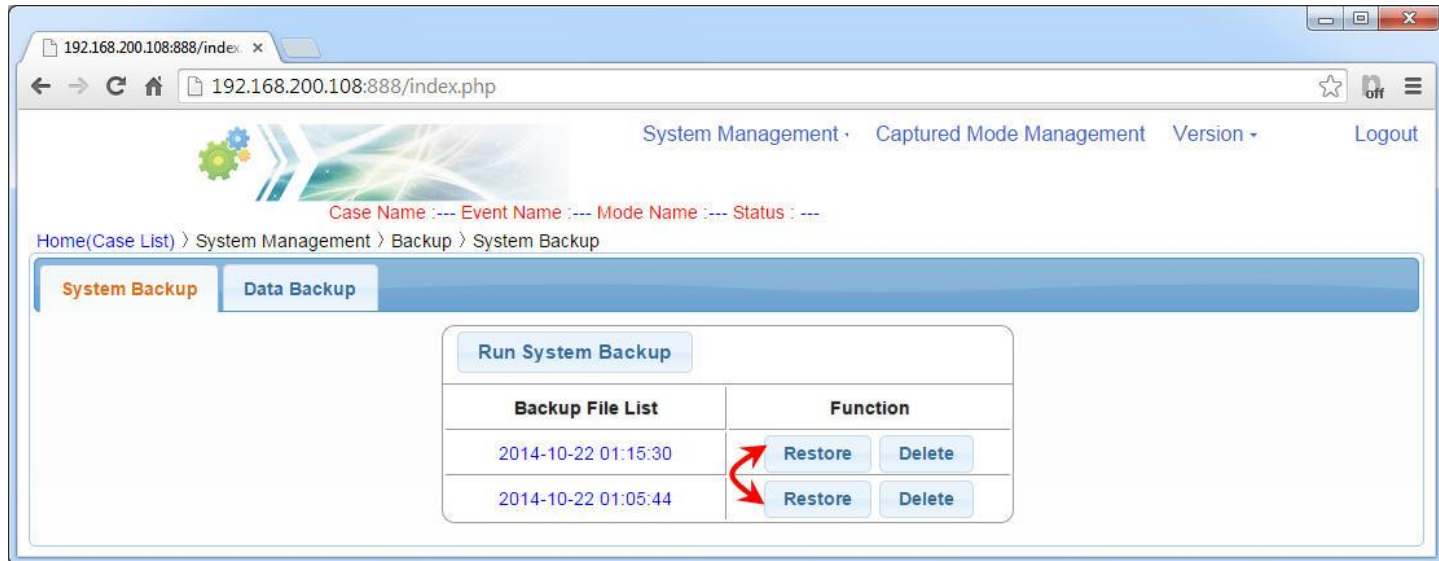


The screenshot shows a web browser window at 192.168.200.108:888/index.php. The page title is 'System Management · Captured Mode Management · Version · Logout'. The breadcrumb trail is 'Home(Case List) > System Management > Backup > System Backup'. There are two tabs: 'System Backup' (active) and 'Data Backup'. A 'Run System Backup' button is highlighted with a red circle and an arrow pointing to a 'Submit' button in a dialog box below. The dialog box contains the following information:

Backup Description	Datetime	2014-10-22 01:14:17			
	Create	admin			
Cases	default	Path	/datas/EDE_1	Size	0 KB
	My Case	Path	/datas/EDE_4	Size	300772 KB
	training	Path	/datas/EDE_6	Size	0 KB
Users	rick	Permission	training(c) My Case(r)		
TotalSize					300772 KB
FreeSpace					426453564 KB

System Restore

- System Restore :

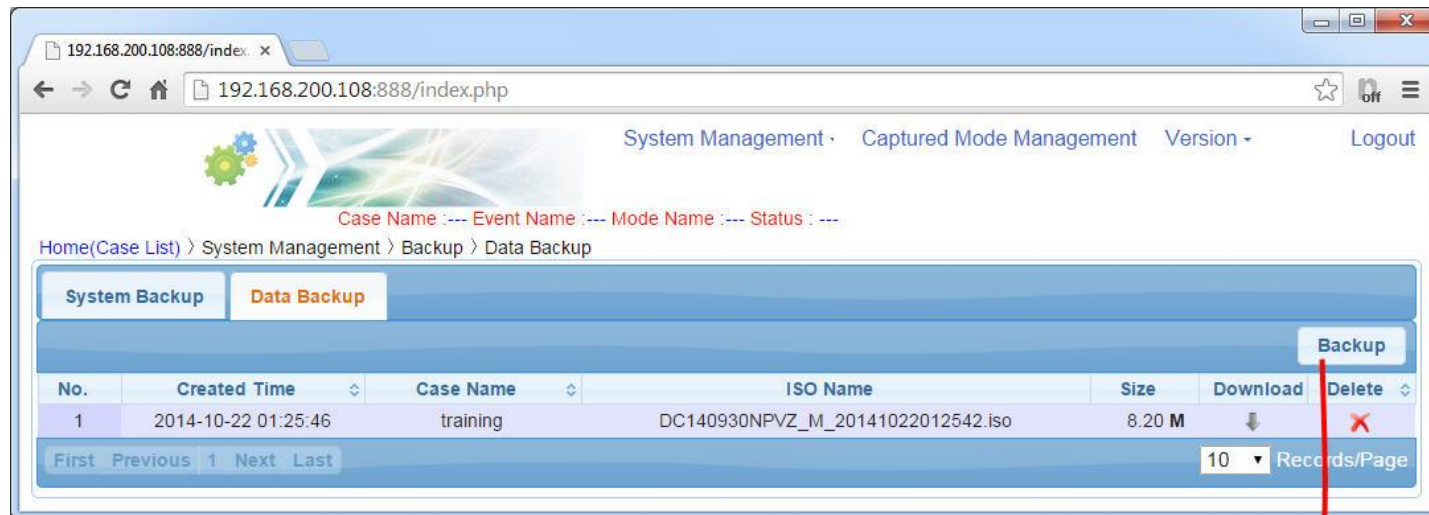


The screenshot shows a web browser window displaying a system management interface. The address bar shows the URL `192.168.200.108:888/index.php`. The page title is "System Management · Captured Mode Management · Version · Logout". The breadcrumb navigation is "Home(Case List) > System Management > Backup > System Backup". There are two tabs: "System Backup" (active) and "Data Backup". A "Run System Backup" button is visible. Below it is a table with two columns: "Backup File List" and "Function". The table contains two rows of backup data, each with "Restore" and "Delete" buttons. A red double-headed arrow is positioned between the "Restore" buttons of the two rows.

Backup File List	Function
2014-10-22 01:15:30	Restore Delete
2014-10-22 01:05:44	Restore Delete

Case Backup Management

- Backup– Data Backup
 - Backup a case:



192.168.200.108:888/index.php

System Management Captured Mode Management Version - Logout

Case Name : --- Event Name : --- Mode Name : --- Status : ---

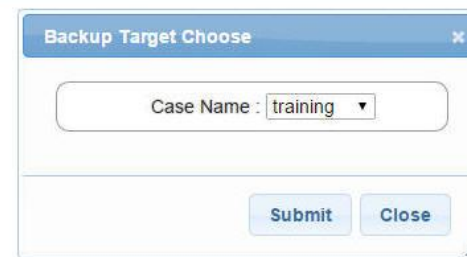
Home(Case List) > System Management > Backup > Data Backup

System Backup Data Backup

Backup

No.	Created Time	Case Name	ISO Name	Size	Download	Delete
1	2014-10-22 01:25:46	training	DC140930NPVZ_M_20141022012542.iso	8.20 M	↓	✖

First Previous 1 Next Last 10 Records/Page



Backup Target Choose

Case Name : training

Submit Close

System Update Management

- Version Update
 - Upload update file:



Update Package Load

Browse

- Execution update :



No..	Package name	Mode	Reboot	Size	Action
1	update_NIT-DEC-2.23.2001.182-N-test-140326-1703.tgz	Manual	No	6.83KB	Update

- Update History :



No.	Upload time	Package name	Total time	Mode	Result	Log
1	2014-05-30 11:37:15	update_NIT-DEC-2.23.2001.182-N-test-140326-1703.tgz	2014-05-30 11:37:18	Manual	Successful!	update.140530113715

Other System Management

- System Status :

Date	User	Severity	SUBJECT	Message
2014-05-29 08:36:15	admin	3	caseHandle	addCase: result is successful for case AAAAAAAAAAAAAA
2014-05-30 09:15:24	admin	3	caseHandle	deleteCase: result is successful for case AAAAAAAAAAAAAA
2014-05-30 09:32:55	admin	3	caseHandle	addCase: result is successful for case MyCase
2014-05-30 10:58:20	admin	3	userHandle	addUser: result is successful for user vic

First Previous 1 Next Last

10 Records/Page

- Language Select

Language Select

简体中文

繁體中文

English

日本語



More Than 140+ Internet Service Decoder



Generic E-Mail	POP3, IMAP, SMTP
Webmail	GMail, Yahoo, Hotmail, ... more than 21 webmails
Instant Message	MSN, Hangout, ICQ, ... more than 8 IMs
Web Page	Web Link, Content and Request
Web FTP	Upload/Download
Web Video	YouTube, GoogleVideo ...
File Transfer	FTP, P2P, ... more than 20 services
Telnet	Animated playback available
Asia On-Line Game	More than 81 games
VoIP	SIP, RTP (G.711, G.726, G.729, iLBC)
Social Network Service	Facebook, Twitter, Plurk ...
Mobile Online Applications	APP & Web Services on iPhone, Android ...
Database	Oracle, MS SQLServer, MySQL...



Conclusion

- ▶ DPI/DPC solution is fast-growing one in the market segments of Public Sector, FSI, Telco and LEA.
- ▶ It is just cross the chasm in the early majority stage of above segments
- ▶ Decision Group has lot of self-developed turnkey solutions, technologies, and product roadmap plan in this market.
- ▶ Fully meeting customer requirement and expectation is the top priority of Decision Group
- ▶ Good references and globalized services provided in different counties

»» Q & A