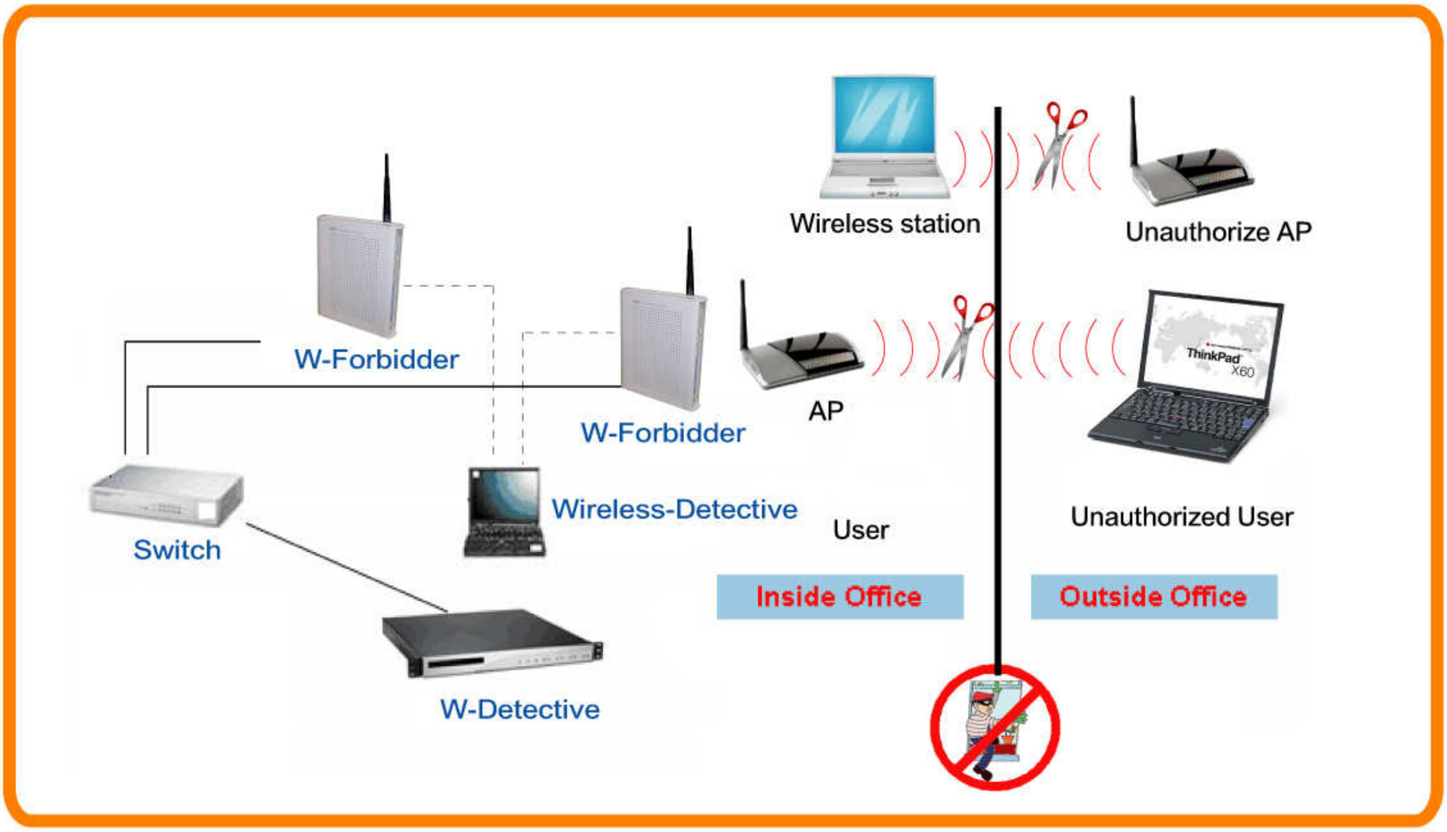
WLAN-FORBIDDER®

Wireless Local Area Network (W-LAN) Monitoring, Auditing and Security System



The WLAN-FORBIDDER system is designed to monitor, audit, decode and analyze the data packets being transmitted to and from your wireless local area network.

The primary function of the WLAN-FORBIDDER system is to ensure the security of your network by identifying and immediately preventing or terminating unauthorized connections to or from your wireless local area network.

The Wireless-Detective subsystem of the WLAN-FORBIDDER system is designed to monitor the wireless traffic being transmitted from the computers in your network to your wireless network access points. It will also identify connections by your computers to unauthorized access points that are not part of your wireless local network.

The W-FORBIDDER subsystem of the WLAN-FORBIDDER system monitors both authorized and unauthorized wireless access points. The W-FORBIDDER system prevents or immediately terminates any connections between the computers in your wireless network and unauthorized access points. It also prevents unauthorized users from connecting to your wireless local area network/access points.

A significant benefit of the WLAN-FORBIDDER system is that it identifies and prevents either malicious or accidental disclosure of secrets, proprietary information and intellectual property.

When combined with the W-Detective Network Monitoring and Auditing system, the WLAN-FORBIDDER system can provide complete network monitoring, auditing, security and traffic analysis.

DECISION COMPUTER INTERNATIONAL CO,. LTD.
Address : 4/F No. 31, Alley 4, Lane 36, Sec.5, Ming-Shen East Road Taipei, Taiwan
Phone No : +886 2 2766-5753 Cell Phone: +886 933 941831
Fax No : +886 2 2766 5702
E - Mail : decision@ms1.hinet.net
URL: www.edecision4u.com/forensics.html
Contact: Casper / Managing Director

WLAN-FORBIDDER SPECIFICATIONS :

The W-FORBIDDER subsystem prevents or immediately terminates any connections between the computers in your wireless network and unauthorized access points. The following is a list of W-FORBIDDER functions and capabilities:

1. Analyze data packets and traffic from the following wireless standards: 802.11, 802.11a, 802.11b and 802.11g.
2. Monitor and ensure your computers are connected only to authorized wireless access points; identify, prevent and terminate connections to unauthorized access points.
3. Provide legl or authorized AP registration and delete registered AP functions.
4. Identify and analyze MAC addresses, IP addresses, fake MAC addresses and fake IP addresses.
5. The W-FORBIDDER system comes with at least two directional antenna units that can quickly identify the signal direction, approximate location and source of a wireless access point or device. Simultaneously, the W-FORBIDDER antenna units provide wireless network coverage/connections for a 10-50 meter range.
6. The W-FORBIDDER system includes Wired Equivalent Privacy (WEP) decryption functions. If the WEP key is known, the W-FORBIDDER system can capture and decrypt raw data into application layer format in real time. If the WEP key is unknown, the W-FORBIDDER system is able to crack the WEP key once it has captured enough raw data (this varies from network to network).
7. Provide optional interface functions that can support ESSD settings, BSSID settings, and IP and timing alteration options for the system manager.
8. Identify the location of unauthorized wireless access points.
9. Monitor, capture, decode, record, audit and analyze all traffic on your wireless network.
10. Once it is identified that a computer in your wireless network has connected to an unauthorized access point, the W-FORBIDDER system issues a warning message to the network administrator and can then either capture and decode the traffic or terminate the connection in accordance with predefined system settings.
11. To prevent unauthorized connections, the W-FORBIDDER system can act as a computer in your wireless network, connect to any unauthorized access points, and then send a message to the unauthorized access points to stop accessing/connecting to your wireless network.

Wireless-Detective

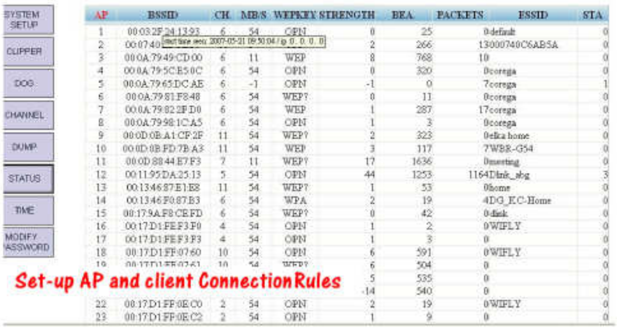
The Wireless-Detective subsystem provides the following functions and capabilities:

1. Scanning, monitoring, capturing, decoding and analysis of wireless data packets to include the following standards: 802.11, 802.11a, 802.11b and 802.11g.
2. Captured raw data files can be stored in a tcpdump format. The raw data files can be divided and stored in various sizes according to date, time and file size.
3. Raw data files are captured in standard tcpdump format, which can easily be read and analyzed by packet analysis software such as Ethereal.
4. The raw data files can be copied (burned) onto CD-ROMs or DVDs.

1
E-mail
Webmail
Hotmail
2
MSN ICQ
YAHOO
AOL
QQ
Chat
3
WEB
4
FTP
5
Telnet
6
P2P
7
ON Line
Game

The Powerful Communication Protocols & Interpreted Applications of W-Detective and Wireless-Detective

1.Set authorized AP/STA



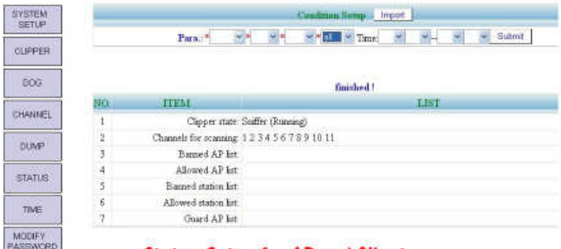
SYSTEM SETUP | CLIPPER | DOG | CHANNEL | DUMP | STATUS | TIME | MODIFY PASSWORD

AP	BSSID	CH.	MB/S	WEPKEY	STRENGTH	BEA	PACKETS	ESSID	STA
1	00:03:2F:24:13:93	6	54	OPN	0	25	0	default	0
2	00:07:40				2	266	1	3000740C6AB5A	0
3	00:0A:79:49:CD:00	6	11	WEP	8	768	1	0	0
4	00:0A:79:5C:E5:0C	6	54	OPN	0	320	0	corega	0
5	00:0A:79:65:DC:AE	6	-1	OPN	-1	0	7	corega	1
6	00:0A:79:81:F8:48	6	54	WEP?	0	11	0	corega	0
7	00:0A:79:82:2F:D0	6	54	WEP	1	287	17	corega	0
8	00:0A:79:98:1C:A5	6	54	OPN	1	3	0	corega	0
9	00:0D:0B:A1:CF:2F	11	54	WEP?	2	323	0	elka home	0
10	00:0D:0B:FD:7B:A3	11	54	WEP	3	117	7	WBR-G54	0
11	00:0D:88:44:E7:F3	7	11	WEP?	17	1636	0	meeting	0
12	00:11:95:DA:25:13	5	54	OPN	44	1253	1164	Dlink_abg	3
13	00:13:46:87:E1:E8	11	54	WEP?	1	53	0	home	0
14	00:13:46:F0:87:B3	6	54	WPA	2	19	4	DG_KC-Home	0
15	00:17:9A:F8:CE:FD	6	54	WEP?	0	42	0	dlink	0
16	00:17:D1:FE:F3:F0	4	54	OPN	1	2	0	WIFLY	0
17	00:17:D1:FE:F3:F3	4	54	OPN	1	3	0		0
18	00:17:D1:FF:07:60	10	54	OPN	6	591	0	WIFLY	0
19	00:17:D1:FF:07:61	10	54	WEP?	6	504	0		0
					5	535	0		0
					-14	540	0		0
22	00:17:D1:FF:0E:C0	2	54	OPN	2	19	0	WIFLY	0
23	00:17:D1:FF:0E:C2	2	54	OPN	1	9	0		0

start time secs: 2007-05-21 09:50:04 / ip: 0. 0. 0. 0

Set-up AP and client Connection Rules

2.Set rules for Forbidden AP/STA



SYSTEM SETUP | CLIPPER | DOG | CHANNEL | DUMP | STATUS | TIME | MODIFY PASSWORD

Condition Setup Import

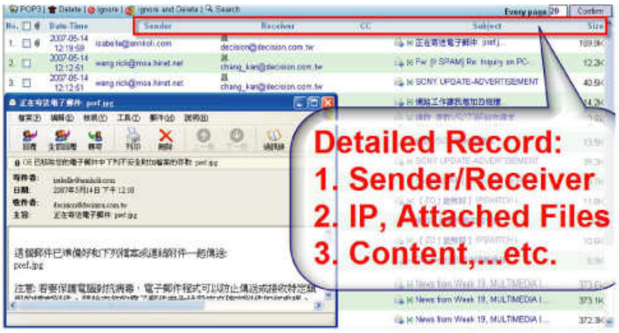
Para.: * Time: Submit

finished !

NO.	ITEM	LIST
1	Clipper state:	Sniffer (Running)
2	Channels for scanning:	1 2 3 4 5 6 7 8 9 10 11
3	Banned AP list:	
4	Allowed AP list:	
5	Banned station list:	
6	Allowed station list:	
7	Guard AP list:	

Status Setup for AP and Client

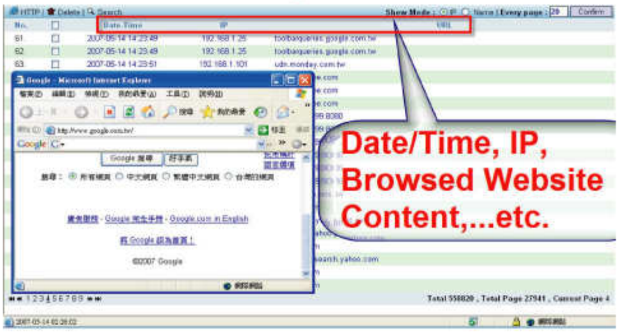
3.POP3/SMTP/Web/Mail



POP3 | Delete | Ignore | Ignore and Delete | Search
Every page 20 Confirm
No. Date-Time Sender Receiver CC Subject Size

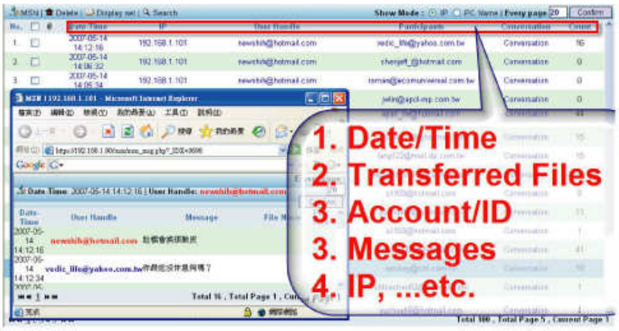
Detailed Record:
1. Sender/Receiver
2. IP, Attached Files
3. Content,...etc.

4.URL Browsing



Date/Time, IP,
Browsed Website
Content,...etc.

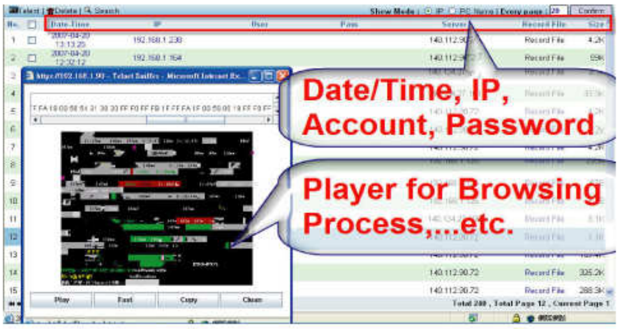
5.IM-MSN, ICQ, YAHOO, QQ



MSN | Delete | Display net | Search
Show Mode: IP PC Name | Every page 20 Confirm
No. Date-Time IP User Handle Participants Conversation Count

1. Date/Time
2. Transferred Files
3. Account/ID
3. Messages
4. IP, ...etc.

6.Telnet

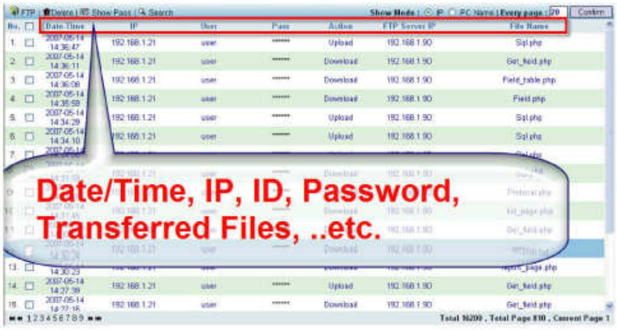


Telnet | Delete | Search
Show Mode: IP PC Name | Every page 20 Confirm
No. Date-Time IP User Pass Server Record File Size
Play Fast Copy Close

Date/Time, IP,
Account, Password

Player for Browsing
Process,...etc.

7.FTP



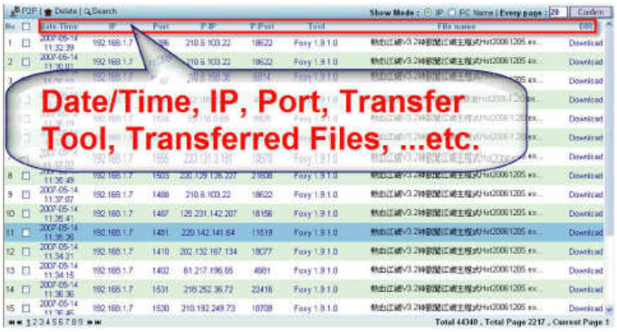
FTP | Delete | Show Pass | Search
Show Mode: IP PC Name | Every page: 20 Confirm

No.	Date-Time	IP	User	Pass	Action	FTP Server IP	File Name
1.	2007-05-14 14:36:47	192.168.1.21	user	******	Upload	192.168.1.90	Sql.php
2.	2007-05-14 14:36:11	192.168.1.21	user	******	Download	192.168.1.90	Get_field.php
3.	2007-05-14 14:36:08	192.168.1.21	user	******	Download	192.168.1.90	Field_table.php
4.	2007-05-14 14:35:59	192.168.1.21	user	******	Download	192.168.1.90	Field.php
5.	2007-05-14 14:34:29	192.168.1.21	user	******	Upload	192.168.1.90	Sql.php
6.	2007-05-14 14:34:10	192.168.1.21	user	******	Upload	192.168.1.90	Sql.php

Total 16200 , Total Page 810 , Current Page 1

Date/Time, IP, ID, Password,
Transferred Files, ..etc.

8.P2P

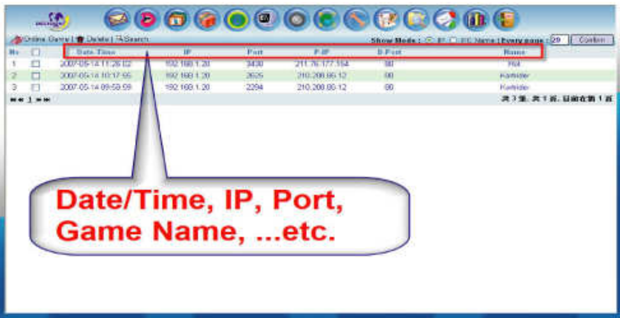


P2P | Delete | Search
Show Mode: IP PC Name | Every page: 20 Confirm
No. Date-Time IP Port P-IP P-Port Tool File Name

Date/Time, IP, Port, Transfer
Tool, Transferred Files, ...etc.

P2P file transmission is a serious concern for network managers and is a source of security leaks. Proper monitoring is necessary.

9.On-Line Game



Online Game | Delete | Search
Show Mode: IP PC Name | Every page: 20 Confirm

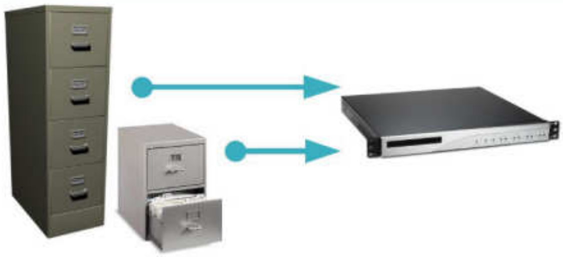
No.	Date-Time	IP	Port	P-IP	P-Port	Name
1	2007-05-14 11:26:02	192.168.1.20	3430	211.76.177.154	80	Hot
2	2007-05-14 10:17:55	192.168.1.20	2625	210.208.86.12	80	Karlstar
3	2007-05-14 09:58:59	192.168.1.20	2294	210.208.86.12	80	Karlstar

Date/Time, IP, Port,
Game Name, ...etc.

WLAN-FORBIDDER is the Best Solution to Ensure the Security of Your Wireless Local Area Network

For Enterprises
Financial Institutions
Banks
Governments
Universities

WLAN-FORBIDDER can connect to external storage to provide long-term back-up of data.



Can also work with a NAS, SAN or DVD/CD Library.

WLAN-FORBIDDER system components:

WL-F0-02

W-Forbidder

Wireless Connection Management System

EDWD-30

W-Detective

W-Detective Control / Auditing System

EDWD-X60

Wireless-Detective

Portable Wireless Control / Auditing System (Optional)