



NIT

Network Investigation Toolkit

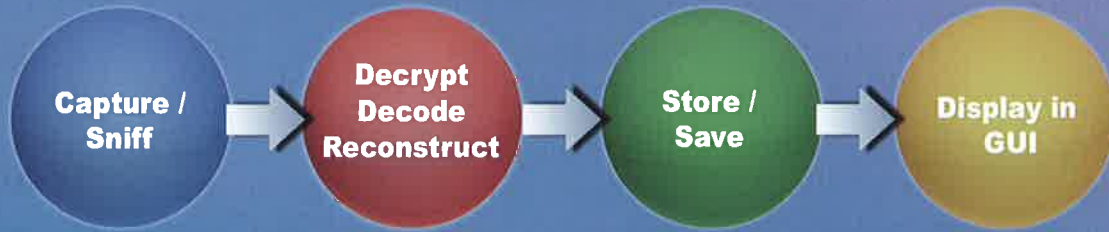
**The Most Powerful Tool for Internet Content
Monitoring and Forensics Analysis
Combined with both LAN and WLAN Interception**



Network Investigation Toolkit (NIT) is designed specially for LEA such as Police, Military, Criminal Investigation Agencies, National Security Agencies, Cyber Security Agencies, Counter Terrorism Department, Forensics Investigator etc. to conduct network based forensics investigation whether it is on a wired or wireless LAN networks.



Application Flow



Wireless Interception

Information obtainable from a WLAN AP/ Wireless Router:

1. BSSID of AP (MAC address)
2. Channel
3. The number of STAs
4. The number of encrypted packet
5. The number of data packet
6. Additional information of AP (the manufacturer of AP, the manufacturer of AP IC component has to be authenticated through international registration)
7. Noise level and signal level
8. SSID or ESSID
9. Type of Wireless LAN: Probe, Ad-hoc or Infra-red
10. WEP (wired equivalent privacy protocol) status
11. The amount of transferred Wireless LAN packet

Information obtainable from a station (STA) includes:

1. The number of encrypted packet through this STA
2. The number of packet through this STA
3. IP Address of STA
4. MAC Address of STA
5. The manufacturer of STA (the one has been authenticated)
6. The highest transferring rate of STA
7. Noise level and signal level of STA
8. Type of STA (Established, To-DS or From-DS)

Wired Interception

1. Supporting Throughput/Load :

Up to 350 Mbps

2. Appliance Based : Yes

3. Deployment :

Mirror Mode, Bridge Mode, Sniffer Mode

4. Services/Support 150 Protocols :

Email (POP3, SMTP, IMAP), Webmail (Yahoo(Standard and 2.0 versions), Gmail), Instant Messenger/Chat (Yahoo, MSN, ICQ, AOL, QQ, Gtalk, Skype), HTTP, FTP, P2P (P2P Details Log-BitTorrent, eMule/eDonkey etc.), Online Games, Telnet / BBS, VOIP (IM), Webcam, VOIP (Standard), HTTPS

5. System Access :

HTTPS Remote Monitoring

6. Group/User :

Yes, with Authority Management function.

7. Data Backup : Yes

Restore Server, NAS/SAN based FTP server etc.

8. Web Browser Access :

Yes (using IE, Mozilla etc.)

9. Data Mining and Search :

Free Text Search, Condition Search, Similar Search Function, Association Search

10. Alert/Notification : Yes

Alert/Notification by parameters, by Key Words

11. Throughput Alert : Yes

12. Station Management :

Yes (NetBIOS, Active Directory info)

13. Storage Management : Yes

14. Upgrade :

Web based Upgrade

15. Reports : Yes

Comprehensive reporting. Total throughput statistical report with top-down view. Per user reporting with top-down view.

16. Schedule Reporting : Yes

Provide daily log report in Excel format

Administration and Management (sample screenshots)

1. Scanning Available Wireless Networks

Hand Disk Information: 91G / Used: 3.5G / Available: 87G / Available (%): 95%

MODE: AP STA

AP	SCAN	MANUAL	AUTO	BSSID	CH	MB/S	KEY	STR.	BEA.	PACKETS	ESSID	SIG
1				00 11 09 F7 A1 6F	6	48	WPA	11	629	22	lokayaka	0
2				00 10 39 EF 43 D8	6	48	WEP	0	49	0	Elinee	0
3				00 10 5B AF 14 81	6	54	WEP	0	213	168	ZWRE45	0
4				00 10 6B AF 43 D9	7	54	WEP	0	266	8	1	1
5				00 10 7E 20 53 D6	1	48	WPA	4	565	7	7yobaka	0
6				00 1F 03 26 70 01	6	54	WEP	3	88	1	ZWRE45	0

2. Import Analysis - WEP Decryption

Hand Disk Information: 91G / Used: 3.9G / Available: 87G / Available (%): 95%

Please choose Rawdata Source

RAWDATA SOURCE: DETACH PATH: /data/openrow

MODE: CO ROM USD IID DETACH

File: WIRELESS_00_11_50_57_SF_03.pcap (229273067-5304)

Manual Wireless Packet Analysis

AP	PARSER	CRACK	BSSID	CH	MB/S	KEY	BEACONS	PACKETS	ESSID
1			00 0F 3D 42 8A 86	-1	-1	-	0	81	
2			00 11 50 57 SF 03	6	48	WEP	22329	208	james271
3			00 11 50 57 SF 03	6	54	WEP	34457	57401	decision_test
4			00 13 10 02 B1 5C	6	48	WPA	3300	7	lokayaka
5			00 14 7F 2F F4 A9	6	48	WEP	20653	187	SpeedFuch1MADAM
6			00 14 5F AF 4A EA	6	54	WEP	168	0	ZWRE45
7			00 14 35 AB 9B 11	6	54	WEP	227	0	ZWRE45
8			00 14 0F 25 85 AF	6	48	WPA	5347	47	lsh1001617
9			00 16 06 23 AA 40	6	48	WPA	6439	64	linksy_SES_7955
10			00 10 39 EF 43 D8	6	48	WPA	2246	47414	linksy
11			00 1B 3F 06 D0 11	6	54	WEP	228	0	ZWRE45

Internet Raw Data Reconstruction (sample screenshots)

1. Email - Webmail

CATEGORY: POP3 192.168.1.11

NO.	DATE/TIME	FROM	TO	CC	SUBJECT	ACCOUNT	PASS
1	2008-07-02 02:34:19	decision@ed...	support@ed...		NO RE	support@	eddec
2	2008-07-02 02:34:19	decision@ed...	decision@ed...	support@ed...	MY Email	support@	eddec
3	2008-07-02 02:34:17	decision@ed...	decision@ed...		NY New York	decision	eddec
4	2008-07-02 02:34:17	decision@ed...	decision@ed...	support@ed...	MY Email	decision	eddec
5	2008-07-02 02:34:13	ksystems@ed...	decision@ed...		Prospectors strike gold at Irish m...	decision	eddec
6	2008-07-02 02:34:13	backle.deci...	decision@ed...		NO RE	decision	eddec
7	2008-07-02 02:34:13	news@bellc...	support@ed...		SDP Approved Compensation Wor...	support@	eddec
8	2008-07-02 02:28:43	charles@st...	support@ed...		NO RE	support@	eddec
9	2008-07-02 02:28:43	ajya@cent...	support@ed...		Mega policy proposition	support@	eddec
10	2008-07-02 02:28:43	support@ed...	support@ed...		NO RE	support@	eddec
11	2008-07-02 02:28:43	support@ed...	support@ed...		Message you sent blocked by our b...	support@	eddec
12	2008-07-02 02:28:43	support@ed...	support@ed...		NO RE	support@	eddec
13	2008-07-02 02:28:43	support@ed...	support@ed...		NO RE	support@	eddec
14	2008-07-02 02:28:43	support@ed...	support@ed...		NO RE	support@	eddec
15	2008-07-02 02:28:43	support@ed...	support@ed...		NO RE	support@	eddec

2. IM - Chat

CATEGORY: YAHOO 192.168.1.11

NO.	DATE/TIME	SCREEN NAME	PARTICIPANTS	CONVERSATION COUNT
1	2008-07-02 02:40:06	wedetective1	wedetective2	CONVERSATION 15

NO.	DATE/TIME	SCREEN NAME	TYPE	MESSAGE	TIME	END TIME
1	2008-07-02 02:40:06	wedetective2	MESSAGE	hello	02:40:07	
2	2008-07-02 02:40:07	wedetective2	MESSAGE	good morning	02:40:09	
3	2008-07-02 02:40:09	wedetective2	MESSAGE	how r u?	02:40:19	
4	2008-07-02 02:40:21	wedetective1	MESSAGE	am fine	02:40:21	
5	2008-07-02 02:40:22	wedetective1	MESSAGE	thank you	02:40:22	
6	2008-07-02 02:40:22	wedetective1	FILE	[Image]	02:40:22	
7	2008-07-02 02:40:22	wedetective1	FILE	[Image]	02:40:22	
8	2008-07-02 02:40:22	wedetective1	FILE	Customer Request Form.pdf	02:40:22	
9	2008-07-02 02:40:22	wedetective1	MESSAGE	thank you!!!	02:40:22	
10	2008-07-02 02:40:22	wedetective2	MESSAGE	welcome	02:40:22	
11	2008-10-23 09:28:18	wedetective1	AUDIO	[Audio]	2008-07-02 2008-07-02	02:40:22 02:41:23
12	2008-10-23 09:28:18	wedetective1	AUDIO	[Audio]	2008-07-02 2008-07-02	02:41:92 02:41:38

3. HTTP - Web Browsing

CATEGORY: HTTPRECONSTRUCT 192.168.1.11

No.	Date/Time	HTTP Content
1	2008-07-02 02:42:27	http://www.msn.com/online/signhome.aspx
2	2008-07-02 02:43:48	http://img.inside.msn.yahoo.com/convict_ad.php
3	2008-07-02 02:43:48	http://img.comtocon.com/yms.php
4	2008-07-02 02:43:48	http://msn.com/content/amp
5	2008-07-02 02:43:48	http://img.inside.msn.yahoo.com/convict_ad.php

URL: http://192.168.1.11 URL: http://localhost Count: 4, Total: 1, In page: 1 Rows per page: 20

SSL now available for citizens of Dubai (and others)

YOU CAN NOW SEARCH SECURELY WITH SEARCHING.COM

4. Telnet

CATEGORY: TELNET 192.168.1.11

NO.	DATE/TIME	ACCOUNT	PASSWORD	SERVER	FILE NAME
1	2008-10-24 02:14:42	PAJB		10.113.13.5	FILE NAME
2	2008-10-24 02:14:42	paist		10.113.17.154	FILE NAME
3	2008-10-24 02:14:42			10.115.25.23	FILE NAME
4	2008-10-24 02:14:42			10.113.31.81	FILE NAME

Count: 4, Total: 1, In page: 1 Rows per page: 20

Play | Stop | Fast | Reset

5. FTP

CATEGORY: FTP 192.168.1.11

NO.	DATE/TIME	ACCOUNT	PASSWORD	ACTION	FILE NAME
1	2008-09-22 01:21:12	vc	vc	Download	192.168.1.249 / FILE211.M
2	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / 01.ppt.JPG
3	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / install_ADM.exe
4	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / icons.ppt
5	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / ip.ppt.ppt
6	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / ip.ppt.ppt
7	2008-09-22 01:21:02	vc	vc	Download	192.168.1.249 / ip.ppt.ppt

Count: 7, Total: 1, In page: 1 Rows per page: 20

File Download

Do you want to open or save this file?

Name: FTP_012112.JPG
Type: JPG Image, 12.18 KB
From: 192.168.1.249

6. P2P

CATEGORY: P2P 192.168.1.11

NO.	DATE/TIME	TOOL	FILENAME	Last Accessed	Send Through	Receive	Detail
1	2008-09-22 01:56:50	Foxy 1.9.0	迅雷 迅雷快传.生...	2008-09-22 01:58:42	0B	5.2M	Detail
2	2008-09-22 01:56:51	Foxy 1.9.0	迅雷 迅雷快传.生...	2008-09-22 02:02:58	0B	6.4M	Detail
3	2008-09-22 01:56:55	Foxy 1.9.0	迅雷 迅雷快传.生...	2008-09-22 01:57:03	0B	6.4M	Detail
4	2008-09-22 01:31:31	BitTorrent	Not Available	2008-09-22 01:40:68	26 KB	1.1M	Detail
5	2008-09-22 01:31:32	BitTorrent	Not Available	2008-09-22 01:38:12	3.5K	641.7K	Detail

No.	DATE/TIME	ACTION	FILENAME	IP	PORT	P-PORT	Throughput
1	2008-09-22 01:56:50	DOWNLOAD	116.166.223.118	51640	10685	5228	
2	2008-09-22 01:56:50	DOWNLOAD	122.121.234.193	51641	12044	5858	
3	2008-09-22 01:56:51	DOWNLOAD	220.138.99.218	51644	20850	5008	
4	2008-09-22 01:56:51	DOWNLOAD	123.240.150.114	51639	21096	4778	
5	2008-09-22 01:56:53	DOWNLOAD	218.175.178.239	51648	12076	3.2K	
6	2008-09-22 01:57:02	DOWNLOAD	61.230.72.116	51669	18783	4888	
7	2008-09-22 01:57:03	DOWNLOAD	61.223.101.26	51658	12607	5318	
8	2008-09-22 01:57:03	DOWNLOAD	210.169.192.75	51666	9507	6278	
9	2008-09-22 01:57:05	DOWNLOAD	61.57.145.189	51642	14254	4513	
10	2008-09-22 01:57:23	DOWNLOAD	61.216.21.120	51677	22068	514.3K	
11	2008-09-22 01:58:09	DOWNLO	220.139.206.230	51649	6576	512.6K	
12	2008-09-22 01:58:33	DOWNLOAD	116.168.223.118	51833	10685	515.6K	
13	2008-09-22 01:58:34	DOWNLOAD	220.138.99.218	51641	20650	5008	
14	2008-09-22 01:58:34	DOWNLO	123.240.150.114	51637	21096	4548	

Who benefits from **Network Investigation Toolkit System** ?

WHO	Human Resources Case Developer Computer Forensics Examiners Banking and Financial Institution Prosecutors	Fraud Examiners White Collar Crime Units Gang Units Homeland Security Legal Units	Educational Institution Enterprises Government Corporation
WHAT	Source Code Employee Information M&A Plans Business Plans Patient Information	Financial Statement Competitive Information Technical Document Intellectual Property Databases	Students' Records R&D Design P&L Report Customer Records
WHERE	Benefits Providers Chart Board Business Partners	Blog Customers Spyware Site	Competitors Terrorist
HOW	Email and Webmail Web - HTTP Instant Messaging / Chat	File Transfer - FTP, P2P HTTP Upload/Download	Online Games Telnet

NIT is a portable unit (laptop based) of appliance with comprehensive network forensics features which can be carried at any location for network based investigation task. NIT can be used to intercept on targeted networks or users to collect the necessary evidences and trace out the source of communication. The unique capability of this system is its combination of various features and functions to conduct LAN real-time interception, WLAN real-time interception, HTTPS/SSL MITM interception on both LAN and WLAN networks as well as offline analysis and reconstruction of pre-captured raw data files.

Network Investigation Toolkit Model

Model	Photo	HDD Size	RAM	Coverage
Network Investigation Toolkit System		160G	1G	Indoor = 0 - 20 meters Outdoor = 0 - 60 meters (line of sight)

System Description :

1. Appliance laptop with both Internal-WiFi adapter and LAN adapter
2. 4 x External USB WiFi adapter (For up to 4 WLAN Channels Capturing)
3. 1 x USB Hub (Active one)
4. 1 x 3.5G / HSPDA (Supplied by local operator)

Note : We accept customization request for special project design. We welcome OEM and ODM partners, distributors and resellers across the world.

Distributor / Partner :



DECISION GROUP

URL : www.decision.com.tw
www.edecision4u.com

Address : 4/F No.31, Alley 4, Lane 36, Sec. 5,
Ming-Sheng East Rd, Taipei Taiwan ROC.

Pone : +886 2 27665753 Fax : +886 2 27665702

Email : decision@decision.com.tw
decision@ms1.hinet.net