



NIT

Network Investigation Toolkit

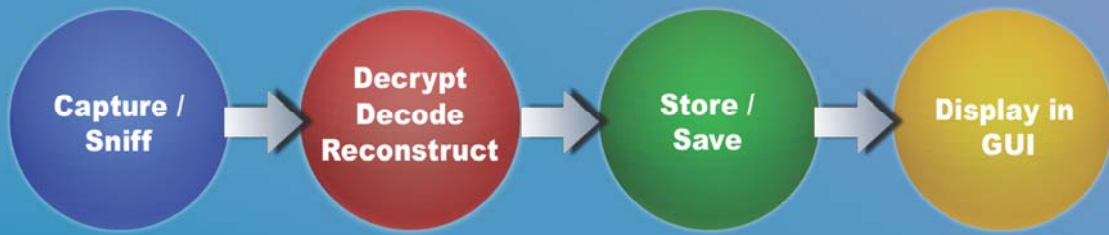
The Most Powerful Tool for Internet Content Monitoring and Forensics Analysis Combined with both LAN and WLAN Interception



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

Hard Disk Information : 91G / Used : 3.5G / Available : 83G / Available (%) : 96%

MODE: * AP STA

AP	SCAN	MANUAL	AUTO	BSSID	CH	MB/S	KEY STR.	BEA	PACKETS	ESSID	STA
1	Manual	Auto		00:11:07:F7:A1:5F	6	48	WPA	11	629	22 linksys	0
2	Manual	Auto		00:18:39:EF:43:08	6	48	WEP	0	49	0 Elaine	0
3	Manual	Auto		00:1B:5D:AF:14:E1	6	54	WEP	10	213	168 2WIRE9	0
4	Manual	Auto		00:1B:5D:AF:43:08	7	54	WEP	12	266	8	1
5	Manual	Auto		00:1D:7E:2B:53:26	1	48	WPA	4	506	7 yeshome	0
6	Manual	Auto		00:1F:83:26:7B:01	6	54	WEP	3	88	1 2WIRE8	0

Count: 6, Total: 1, in page 1 | Rows per page: 20 | Submit | Update

2. Import Analysis - WEP Decryption

Hard Disk Information : 91G / Used : 3.5G / Available : 83G / Available (%) : 95%

Please Choose Rawdata Source:

RAWDATA SOURCE: DETACH PATH: /state/opensslraw

WIRELESS: 00:11:07:F7:A1:5F raw 122023797-636K Wireless WEP-1201-44IM

Manual Wireless Packet Analysis

Crack time: 1 * min. Copy: 128 * Bit

SUCCESS: 2008-12-10 02:52:19 / 00:11:95:55:F6:F1 | A1B2C3D4E5F6A7B8C9D0E1F2A3

AP	PARSER	CRACK	BSSID	CH	MB/S	KEY	BEACONS	PACKETS	ESSID
1			00:1F:30:42:BA:36	-1	-1	WEP	0	81	
2			00:11:95:55:F6:F1	6	48	WEP	22329	908	James271
3			00:11:95:55:F6:F1	6	54	WEP	34497	578401	decision_test
4			00:13:10:82:B1:3C	6	48	WEP	3308	7	linksys
5			00:14:7F:2F:F4:A9	6	48	WEP	20653	157	SpeedTouch11ADAS
6			00:14:95:4F:F4:EA	6	54	WEP	158	0	2WIRE445
7			00:14:95:49:98:11	6	54	WEP	227	0	2WIRE944
8			00:14:8F:23:85:A5	6	48	WPA	5347	47	1681601517
9			00:16:96:33:AA:40	6	48	WPA	6439	64	linksys_SES_7955
10			00:18:39:EF:43:08	6	48	WEP	2246	47414	linksys
11			00:18:3F:05:0D:11	6	54	WEP	208	0	2WIRE385

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...	NONE	[Captured]	support@...	eddec
2	2008-07-02 02:34:19	decision@ed...	decision@ed...support		+ MY Email		
3	2008-07-02 02:34:17	decision@ed...	decision@ed...	NONE	+ New York	decision...	eddec
4	2008-07-02 02:34:17	decision@ed...	decision@ed...support		+ MY Email	decision...	eddec
5	2008-07-02 02:28:43	ksanyamy@y...	decision@ed...	NONE	+ Prospectors strike gold at Irish min...	decision...	eddec
6	2008-07-02 02:28:43	ksanyamy@y...	decision@ed...	NONE	+ Bush	decision...	eddec
7	2008-07-02 02:28:43	news@title...	support@ed...	NONE	+ SOF Approved Communication Wor...	support@...	eddec
8	2008-07-02 02:28:43	charles@ar...	support@ed...	NONE	+ Everything thought out. Everything ...	support@...	eddec
9	2008-07-02 02:28:43	jays@cent...	support@ed...	NONE	+ Mago jeffery proposition	support@...	eddec
10	2008-07-02 02:28:43	support@ed...	support@ed...	NONE	+ Dear support@ed-system.sj June 83% 0...	support@...	eddec
11	2008-07-02 02:28:43	postmaster...	support@ed...	NONE	+ "Message you sent blocked by our bu...	support@...	eddec
12	2008-07-02 02:28:43	yslanun_137	support@ed...	NONE	+ "Slam her everynight	support@...	eddec
13	2008-07-02 02:28:43	kusan2001@...	support@ed...	NONE	+ Leading the enlargement revolution	support@...	eddec
14	2008-07-02 02:28:43	edekra194@...	support@ed...	NONE	+ Top graduate from east academy	support@...	eddec
15	2008-07-02 02:28:43	an@herald...	support@ed...	NONE	+ PA/Secretary @ Sntac: \$2200PM. Apply...	support@...	eddec
16	2008-07-02 02:28:43	van20081@...	support@ed...	NONE	+ Post job Ad On Your Behalf 'FYC' Var...	support@...	eddec

2. IM - Chat

CATEGORY: YAHOO - 192.168.1.11

NO.	DATE / TIME	SCREEN NAME	TYPE	MESSAGE	PARTICIPANTS	CONVERSATION COUNTS
1	2008-07-02 02:40:06	wedetective2	MESSAGE	hello	wedetective1	CONVERSATION: 15
2	2008-07-02 02:40:07	wedetective2	MESSAGE	good morning		
3	2008-07-02 02:40:09	wedetective2	MESSAGE	how r u?		
4	2008-07-02 02:40:19	wedetective1	MESSAGE	Hi		
5	2008-07-02 02:40:21	wedetective1	MESSAGE	I am fine		
6	2008-07-02 02:40:22	wedetective1	MESSAGE	thank you		
7	2008-07-02 02:40:42	wedetective1	FILE			
8	2008-07-02 02:40:55	wedetective1	FILE	Customer Request Form.pdf		
9	2008-07-02 02:42:21	wedetective1	MESSAGE	thank you!!!		
10	2008-07-02 02:42:28	wedetective2	MESSAGE	WELCOME!!!		
11	2008-10-23 09:28:28	wedetective1	AUDIC			2008-07-02 2008-07-02 02:41:28
12	2008-10-23 09:28:14	wedetective1	AUDIC			2008-07-02 2008-07-02 02:41:28

3. HTTP - Web Browsing

CATEGORY: HTTPRECONSTRUCT - 192.168.1.11

No.	Date-Time	HTTP Content
1	2008-07-02 02:44:27	http://kavet.msn.com/vgn-vg-home.aspx
2	2008-07-02 02:43:00	http://tag.insider.msn.yahoo.com/client_ad.php
3	2008-07-02 02:38:48	http://tag.insider.msn.yahoo.com/client_ad.php
4	2008-07-02 02:38:34	http://insight.com/terminals.php
5	2008-07-02 02:38:30	http://tag.insider.msn.yahoo.com/client_ad.php

IP: 192.168.1.11 URL: http://insight.com DATE / TIME : 2008-07-02 02:37:42

SSL now available for citizens of Dubai (and others)!

YOU CAN NOW SEARCH SECURELY WITH ISHUNT.COM

Worried about having your traffic sniffed? Concerned about privacy? We've got your solution. A connection you communicate with us privately, bypassing caching servers and deep packet inspection hardware.

Thanks in no small part to the work of Spike, we are proud to offer SSL on 2 of our sites. <https://ishunt.com/terminals.com> and <https://ishunt.com/terminals.com> are all new valid urls for searching us. This should help you have issues with transparent proxies or mean people snooping on your connections, this should come as relief for you. We'll be evaluating how much extra load this places on our servers over the next few weeks, and if outpacing of people preferring to browse without or transparent security, we'll be investing in some dedicated SSL connections. (Sookie vgn1402) 's have hftn chips with some very nice linux kernel drivers I offloading, so they'd make our SSL staff faster, and be completely transparent.

4. Telnet

CATEGORY: TELNET - 192.168.1.11

NO.	DATE / TIME	ACCOUNT	PASSWORD	SERVER	FILE NAME
1	2008-10-24 02:14:42	[A]@B		140.113.13.5	FILE NAME
2	2008-10-24 02:14:42	guest		140.113.17.154	FILE NAME
3	2008-10-24 02:14:42			140.115.25.20	FILE NAME
4	2008-10-24 02:14:42			140.113.39.91	FILE NAME

5. FTP

CATEGORY: FTP - 192.168.1.10

NO.	DATE / TIME	ACCOUNT	PASSWORD	ACTION	FTP SERVER	FILE NAME
1	2008-09-22 01:21:12	vic	vic	Download	192.168.1.249	安装程序.rar
2	2008-09-22 01:21:02	vic	vic	Download	192.168.1.249	java.JPG
3	2008-09-22 01:20:59	vic	vic	Download	192.168.1.249	安装_AJN.exe
4	2008-09-22 01:20:55	vic	vic	Download	192.168.1.249	icons.ppt
5	2008-09-22 01:20:53	vic	vic	Download	192.168.1.249	googletalk-setup-zh-TW.exe
6	2008-09-22 01:20:53	vic	vic	Download	192.168.1.249	Cisco2003icons.ppt
7	2008-09-22 01:20:47	vic	vic	Download	192.168.1.249	Cisco_icons_1.ppt

Count: 7, Total: 1, in page 1 | Rows per page: 20 | Submit

File Download

Do you want to open or save this file?

Name: FTP_01407.JPG
Type: JPEG image, 12.2KB
From: 192.168.1.64:41

Open Save Cancel

While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save the file. [Visit this link.](#)

6. P2P

CATEGORY: P2P - 192.168.1.142

NO.	DATE/TIME	TOOL	FILENAME	Last Activated	Send Throughput	Receive Throughput	Detail
1	2008-09-22 01:56:50	Foxy 1.9.8.0	天影网络高速下载器...	2008-09-22 01:58:42	0B	5.2M	Detail
2	2008-09-22 01:56:24	Foxy 1.9.8.0	网络硬盘高速下载器...	2008-09-22 02:02:58	0B	8.4M	Detail
3	2008-09-22 01:56:05	Foxy 1.9.8.0	网络硬盘高速下载器...	2008-09-22 01:57:03	0B	6.4M	Detail
4	2008-09-22 01:56:05	BitTorrent	Not Available	2008-09-22 01:40:08	26.9K	1.1M	Detail
5	2008-09-22 01:38:12	BitTorrent	Not Available	2008-09-22 01:38:12	3.8K	541.7K	Detail

Count: 5, Total: 1, in page 1 | Rows per page: 20 | Submit


NO.	DATE/TIME	ACTION	IP:PORT	THROUGHPUT
1	2008-09-22 01:56:50	DOWNLOAD	118.166.223.118	10085 522B
2	2008-09-22 01:56:50	DOWNLOAD	122.121.234.193	51641 12044 508B
3	2008-09-22 01:56:51	DOWNLOAD	220.138.39.218	51644 20650 505B
4	2008-09-22 01:56:51	DOWNLOAD	123.240.150.114	51639 21096 477B
5	2008-09-22 01:56:53	DOWNLOAD	218.175.178.239	51648 12076 329B
6	2008-09-22 01:57:02	DOWNLOAD	61.230.72.116	51609 16783 485B
7	2008-09-22 01:57:03	DOWNLOAD	61.223.101.26	51658 12607 537B
8	2008-09-22 01:57:03	DOWNLOAD	218.169.179.75	51696 9597 521B
9	2008-09-22 01:57:03	DOWNLOAD	61.57.145.189	51642 14254 451B
10	2008-09-22 01:57:23	DOWNLOAD	61.216.21.120	51677 22068 514.3K
11	2008-09-22 01:58:09	DOWNLOAD	220.139.208.230	51649 6576 512.8K
12	2008-09-22 01:58:33	DOWNLOAD	118.166.223.118	51833 10855 515.8K
13	2008-09-22 01:58:34	DOWNLOAD	220.138.39.218	51841 20650 505B
14	2008-09-22 01:58:34	DOWNLOAD	123.240.150.114	51837 21096 454B

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 :