E DETECTIVE®

NIT
Network Investigation Toolkit

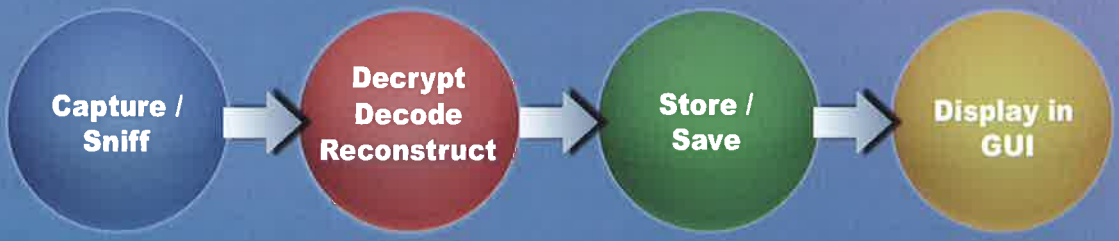
The Most Powerful Tool for Internet Content Monitoring and Forensics Analysis Combined with both LAN and WLAN Interception

- Email
- Chat
- Web
- FTP
- P2P
- TELNET
- Video Stream
- Online Game
- VOIP
- HTTPS/SSL

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.

DECISION GROUP

Application Flow



Wireless Interception

Information obtainable from a WLAN AP/ Wireless Router:

1. BBSID 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:

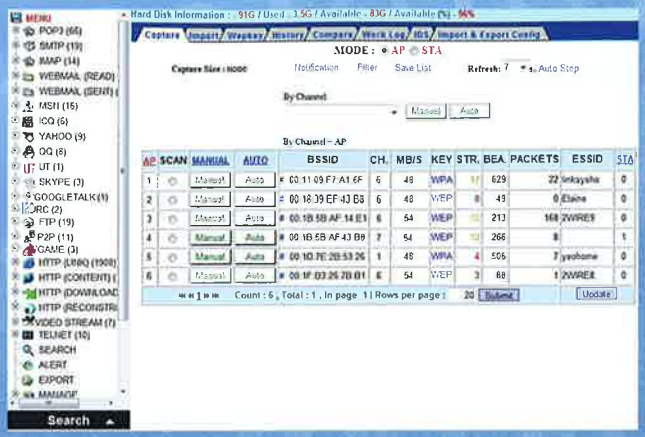
1. The number of encrypted packet through this STA
2. The number of packet through this STA
3. IP Address of STA
4. MAC Address of STA
5. The manufacturer of STA (the one has been authenticated)
6. The highest transferring rate of STA
7. Noise level and signal level of STA
8. Type of STA (Established,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

Wired Interception

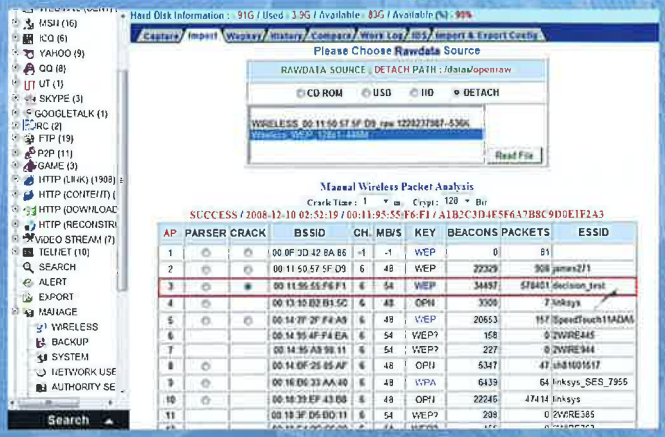
1. **Supporting Throughput/Load :**
   Up to 350 Mbps
2. **Appliance Based :** Yes
3. **Deployment :**
   Mirror Mode, Bridge Mode, Sniffer Mode
4. **Services/Support 150 Protocols :**
   Email (POP3, SMTP, IMAP), Webmail (Yahoo(Standard and 2.0 versions), Gmail), Instant Messenger/Chat (Yahoo, MSN, ICQ, AOL, QQ, Gtalk, Skype), HTTP, FTP, P2P (P2P Details Log-BitTorrent, eMule/eDonkey etc.), Online Games, Telnet / BBS,VOIP (IM), Webcame, 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



2. Import Analysis - WEP Decryption

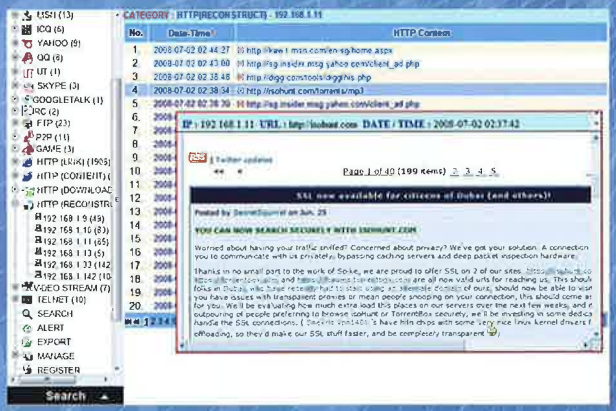


Internet Raw Data Reconstruction (sample screenshots)

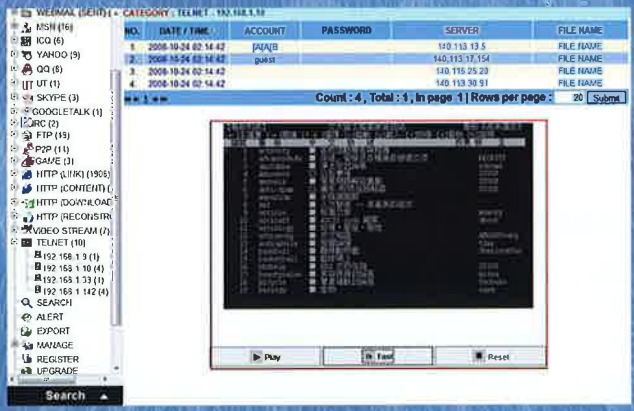
1. Email - Webmail

2. IM - Chat

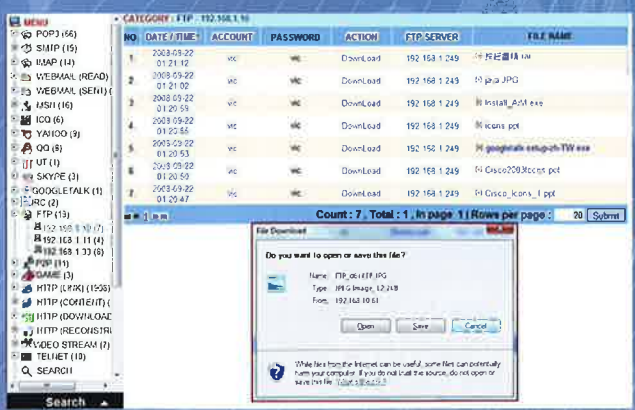
3. HTTP - Web Browsing



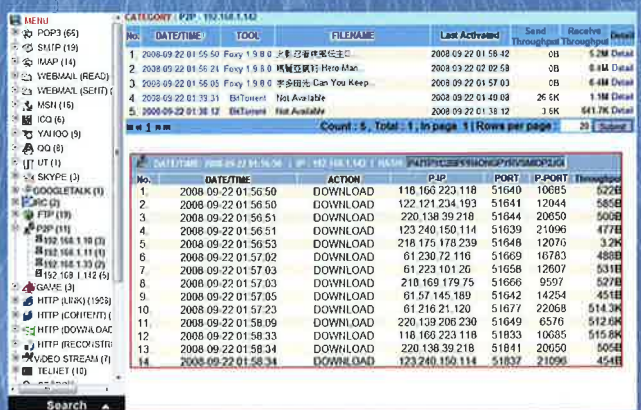
4. Telnet



5. FTP



6. P2P



Who benefits from Network Investigation Toolkit System ?

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

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