NIT2

Network Investigation Toolkit / 2nd Generation

The Most Powerful Tactic Tool for Internet Content Monitoring and Forensics Analysis on Both Wired and Wireless Networks

Network Investigation Toolkit 2 (NIT2) is working as the most extensive tactic tool for LEA staff to conduct digital forensic investigation and corporate IT security officer to mitigate IT risk and internal threats on both wired and wireless networks.

DECISION GROUP

The Most Powerful System for both LEA Staff and Corporate IT Security Officers

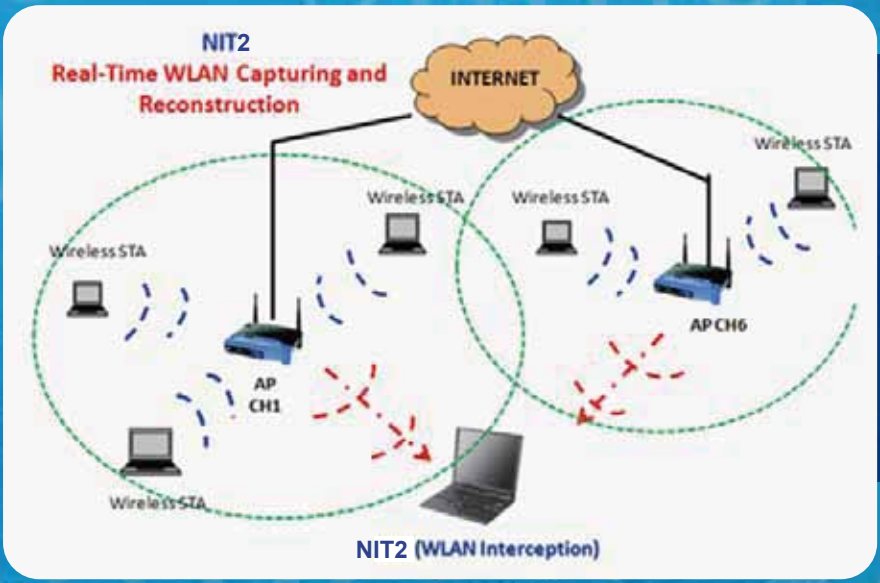
Four Major Functions of NIT2 -

1. Interception on Wireless Traffic over the Air
2. RF Jamming on Wireless Traffic over the Air
3. Interception on Wired Traffic in the LAN
4. As Cache Engine for Interception on HTTPS Traffic at both LAN and WLAN

Five Important Roles of NIT2 -

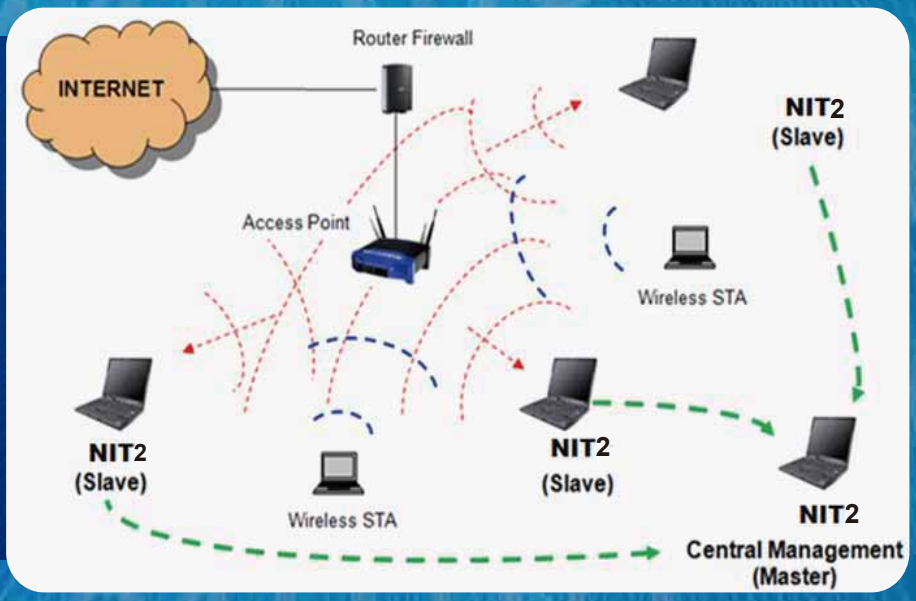
1. Independent Tactic Network Monitoring Tool
2. Frontend Tactic Lawful Interception Device
3. RF Jamming Weapon Against Unknown Intruders and Disgruntled Employees over the Air
4. Content Reconstruction System for Raw Network Traffic Data
5. Primary Investigation Analysis Tool on Intercepted Data

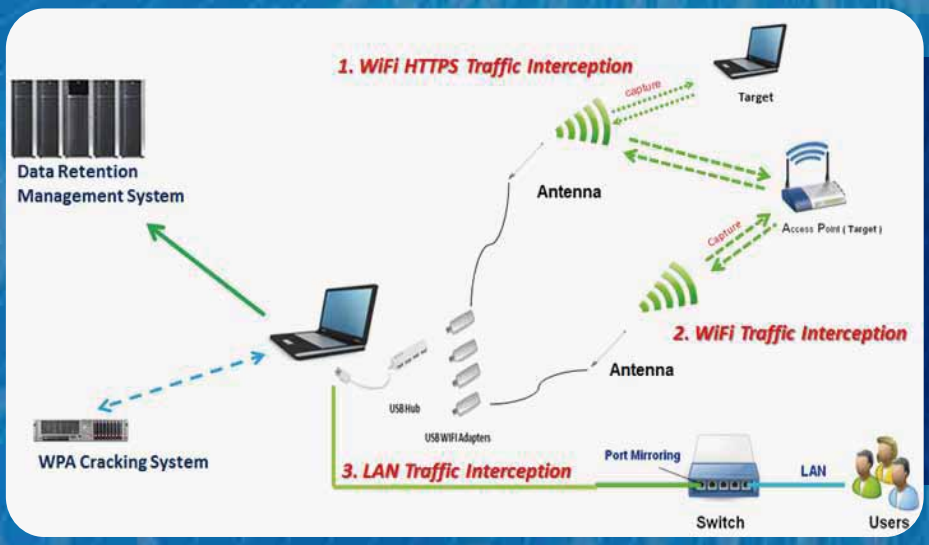
It is the Must-to-Have Weapon for Law Enforcement Agency and Corporate against Cybercrimes and Internal Threats



Single System with Multiple High Gain Antenna for Wi-Fi Traffic Monitoring by Different Channels

Multiple Systems for Wi-Fi Traffic Monitoring with Enhanced Capability of RF Reception on Target AP or Mobile Devices





Streamline Process of Wi-Fi and Wired Interception with WPA Cracking System and DRMS

DECISION GROUP

The Most Powerful System for both LEA Staff and Corporate IT Security Officers

Four Major Functions of NIT2 -

1. Interception on Wireless Traffic over the Air
2. RF Jamming on Wireless Traffic over the Air
3. Interception on Wired Traffic in the LAN
4. As Cache Engine for Interception on HTTPS Traffic at both LAN and WLAN

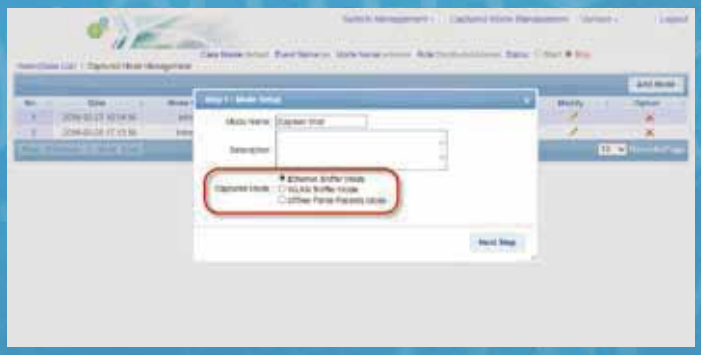
Five Important Roles of NIT2 -

1. Independent Tactic Network Monitoring Tool
2. Frontend Tactic Lawful Interception Device
3. RF Jamming Weapon Against Unknown Intruders and Disgruntled Employees over the Air
4. Content Reconstruction System for Raw Network Traffic Data
5. Primary Investigation Analysis Tool on Intercepted Data

It is the Must-to-Have Weapon for Law Enforcement Agency and Corporate against Cybercrimes and Internal Threats

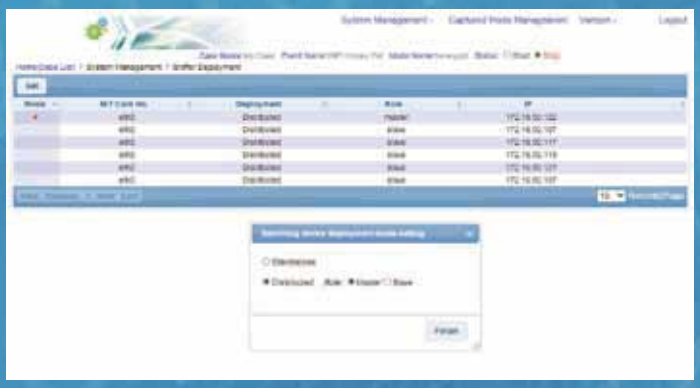
Function and Management (sample screenshots)

1. Interception Function



2. Association Search

3. Target Credential

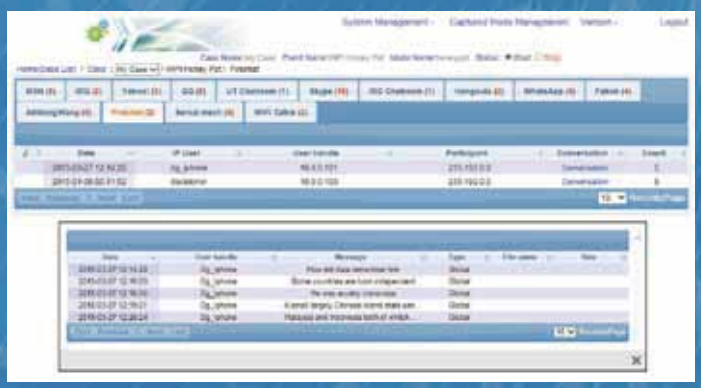


4. Email/Webmail

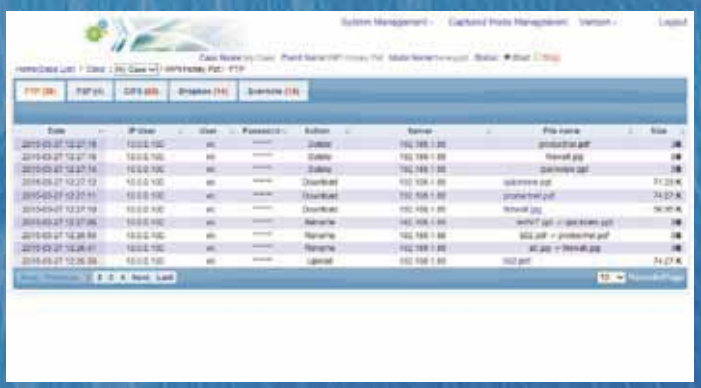
5. Facebook

6. Web Browsing

7. FireChat



8. FTP



Who benefits from **Network Investigation Toolkit 2** System ?

WHO	Human Resources	Fraud Examiners	Institution
	LI Lab Analyst	Anti-Narcotic Units	Enterprises
	Computer Forensics Examiners	Anti-Corruption Units	Government
	Banking and Financial Institution	Homeland Security	Military Intelligence
	Prosecuters	Prison Security	School Master
WHAT	Black Mail	Financial Statement	Students' Records
	Employee HR Record	Sex Harassment	Cyber Bullying
	Business Plans	PLM Document	Social Riot Planning
	Cybercriminal Transaction	Intellectual Property	Customer Records
	Voice Conversion	Databases	EMR
WHERE	Corporate Offices	School/Campus	Government Offices
	Internet Cafe	Airport	Hospital
	Bank	Shopping Mall	Prison
OBJECT	Email and Webmail	File Transfer - FTP, P2P	Micro Blog
	Web - HTTP	Mobile APP Services	Telnet
	Messenger / Chat	Social Media	VoIP Call

NIT2 is an appliance of tactic system (laptop based) with comprehensive network forensics features, and it can be carried to any location for cyber investigation task. NIT2 can be used to intercept all communication on the target networks for digital content collection as legal evidence, and to track IP addresses and IDs of both source and destination sides with timestamp. The significant capability of NIT2 system is in the integration of various functions to conduct real-time interception on both HTTPS and non-HTTPS traffic from both wired and wireless networks as well as to reconstruct content offline from designated raw pcap data files.

***Network Investigation Toolkit 2* Model**

Model	Photo	HDD Size	RAM	Coverage
ANIT		**500G**	**4G**	**Indoor** = 0-20Meters **Outdoor** = 0-60Meters (line of sight)

Hardware specification may be changed by supplier without further notice.

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 : The multiple system deployment function of NIT2 appliance is under the patent protection of Taiwan with ID I462605, of which patent has also been protected in CHINA, ASEAN, US, JAPAN, EUROPEAN COMMISSION region and others.

We accept customization request for project base requirement.

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
Phone : +886 2 27665753 Fax : +886 2 27665702
Email : decision@decision.com.tw
decision@ms1.hinet.net