Network Investigation Toolkit – NIT3

Interception at
- Ethernet LAN traffic through mirror port (or by network tap).
- WLAN traffic (up to 4 different WLAN channels).
- Ethernet LAN HTTPS/SSL traffic by MITM attack.
- WLAN HTTPS/SSL traffic by MITM attack.
- Distributed Deployment with Multiple NIT System.

Data Decoding by
- Real-time raw data decoding and reconstruction.
- Offline raw data decoding and reconstruction.

Forensics analysis and investigation.

Solution for :
Lawful Enforcement Agencies
(Police Intelligence, Military Intelligence, National Security, Counter Terrorism, Cyber Security, Defense Ministry etc)
and IT Security Management of Enterprises.

From 2017, add New in NIT :
- Proven Real-World Operations
- Man-Pack operation from setup to use within 1 min – Pack & Go!
- Able to intercept more than 180+ Protocols
- 3~5 Hours Man-Pack operations with a single charge
- Highly Mobility
- Very Long Range from 100M to 1000M

Frequency
- 2.4 GHz /5.0 GHz

Intercept and Display TLS/SSL and Non-TLS/SSL
- Web Browser : Chrome, Firefox, Internet Explorer with account and password
- Webmail : Gmail, Yahoo mail, Hotmail with account and password (Addition wording, Please confirm)
- Protocol : Email (SMTP, POP3, IMAP)
  : File Transfer (FTP, P2P File Sharing)
  : VoIP (SIP)
  : Video Streaming (FLV and MPEG-4 Format)
- Social Media : Facebook, Twitter with account and password

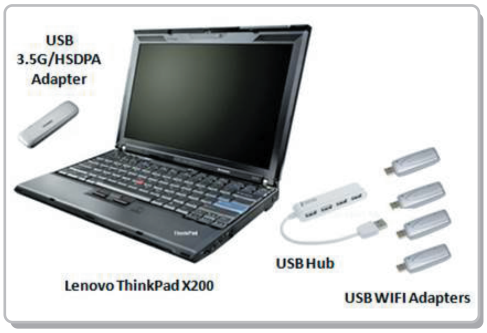
Certificate Authority
- Can install a certificate authority (CA) on the device for HTTPS identity

Data Management
- Raw Data : PCAP
- Reconstruction and Arrangement

Interception Method and Display
- SSID
- IP Address
- Mac Address

More function
- Remote Access
- IMSI Number

Environment
- Battery run time up to 5 hours



NIT Implementation Mode – LAN

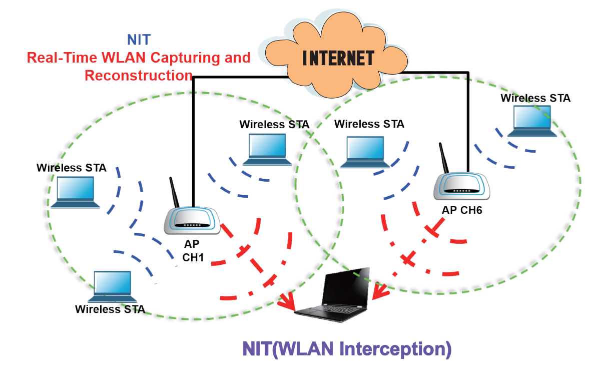


Diagram: NIT - Wired Lan Interception(Mirror Mode Implementation)

NIT Implementation Mode- WiFi

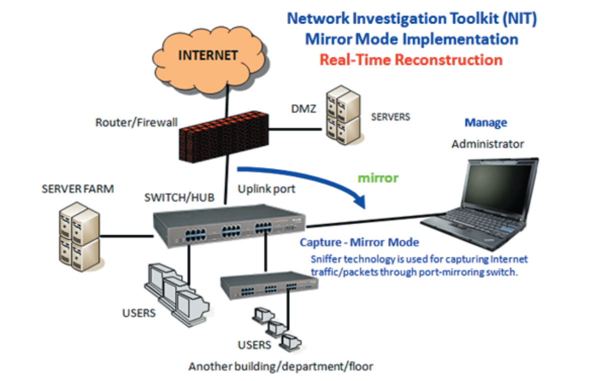

Network Investigation Toolkit (NIT)
Mirror Mode Implementation
Real-Time Reconstruction
INTERNET
DMZ
SERVERS
Router/Firewall
Manage
Administrator
mirror
SERVER FARM
SWITCH/HUB
Uplink port
Capture - Mirror Mode
Sniffer technology is used for capturing Internet traffic/packets through port-mirroring switch.
USERS
USERS
Another building/department/floor

Diagram: NIT – Wired LAN Interception (Mirror Mode Implementation)

NIT Implementation Mode – LAN HTTPS

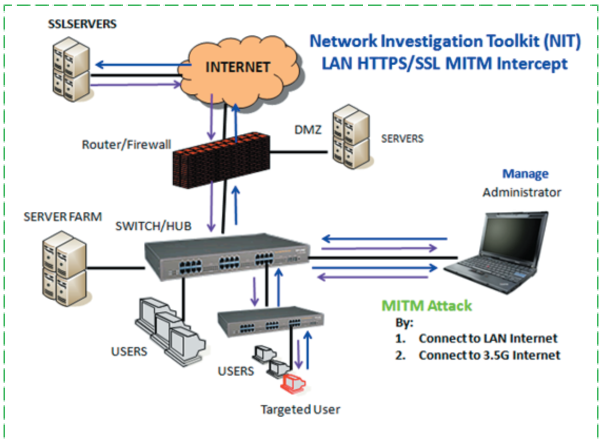
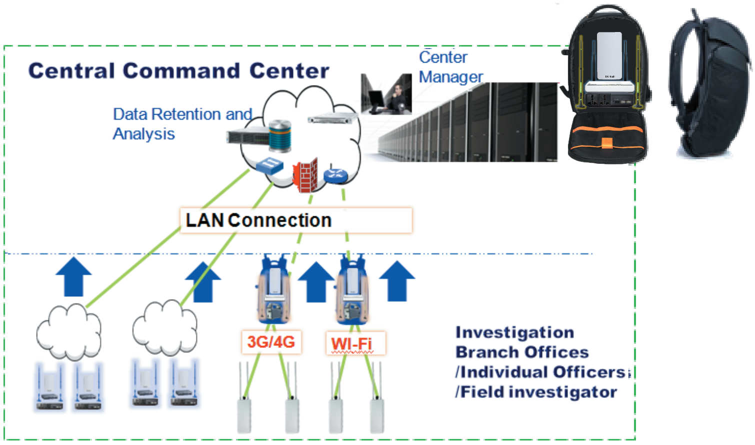


Diagram: NIT – LAN HTTPS/SSL MITM Interception

NIT3 Deployment Diagram


Central Command Center
Center Manager
Data Retention and Analysis
LAN Connection
3G/4G
WI-Fi
Investigation Branch Offices /Individual Officers /Field investigator