

Network Investigation Toolkit (NIT)

Cyber crime (Illegal and unauthorized Internet usage) has increased in recent years due to open communications policy in many countries all over the world. The initial effort to prevent, curb and detect these illegal usage activities by using content filtering and application or service blocking solutions have failed as there are too many back door paths. Terrorists start to love the Internet and exploit all possible way of communications among themselves through the Internet. Politicians start to make use of Internet to spread their propaganda and message to their supporters. Illegal betting organizations make use of Internet for illegal transactions. Drugs and weapons dealers exploit the Internet to close on drug and weapons smuggling deals. School and universities students download unauthorized MP3s, Movies and Software from the Internet. More and more people start to make use of Internet for their own benefits in all sorts of ways. The "Online Population" has increased tremendously in recent years.

Network Investigation Toolkit (NIT) is designed specially by Decision Group 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. NIT is a portable unit (laptop based) 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. The 3.5G/HSDPA USB Adapter is included in the package for user to remote access and manage the system.

NIT Implementation Diagrams:

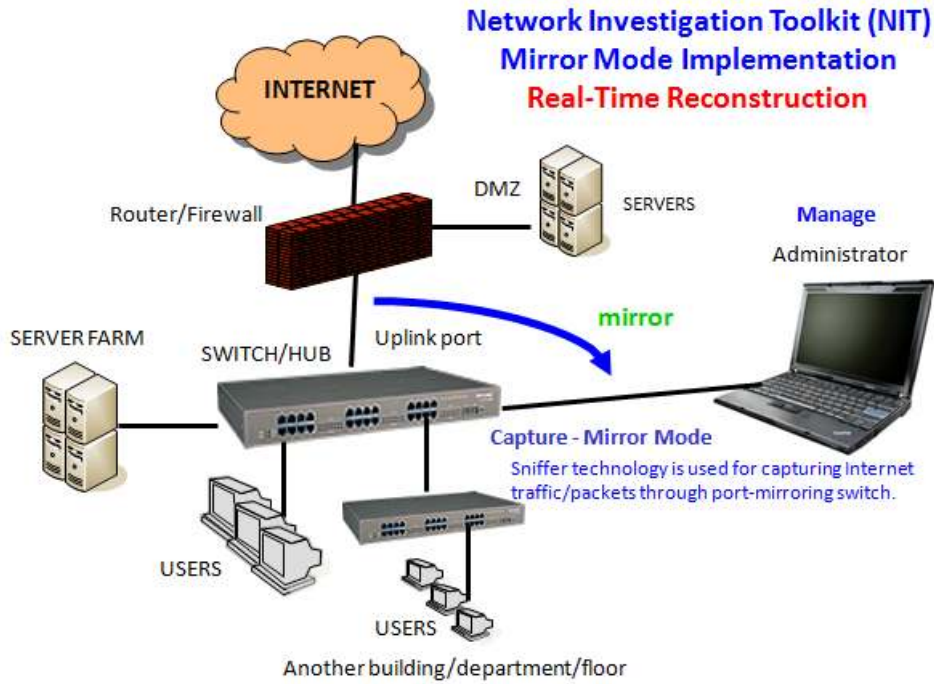


Diagram: NIT – Wired LAN Interception (Mirror Mode Implementation)

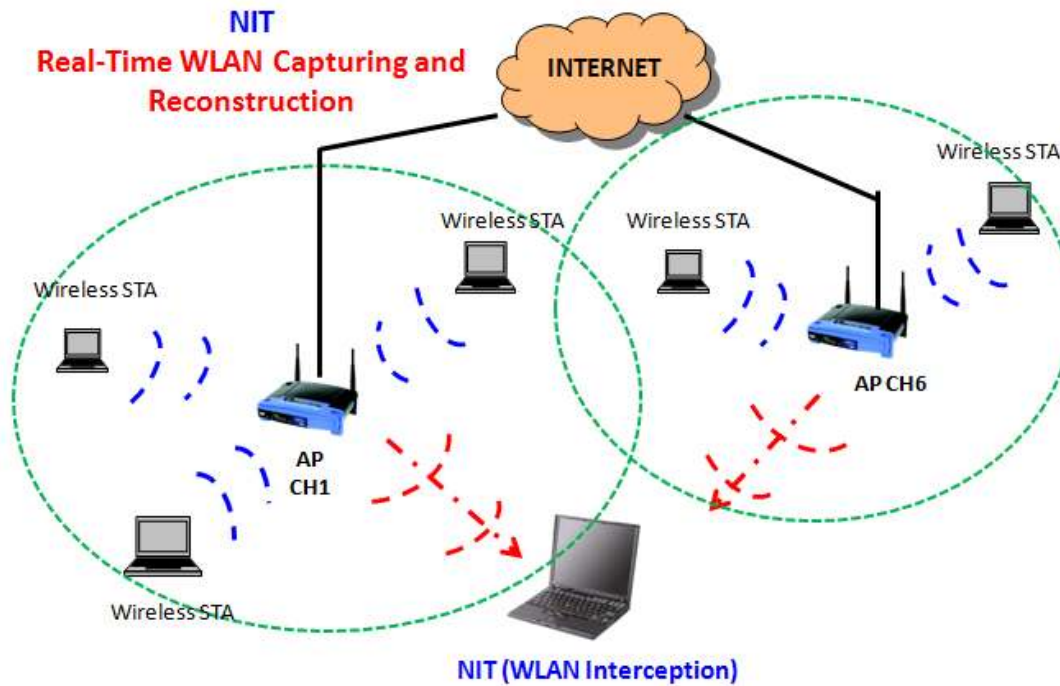


Diagram: NIT – Wireless LAN Interception

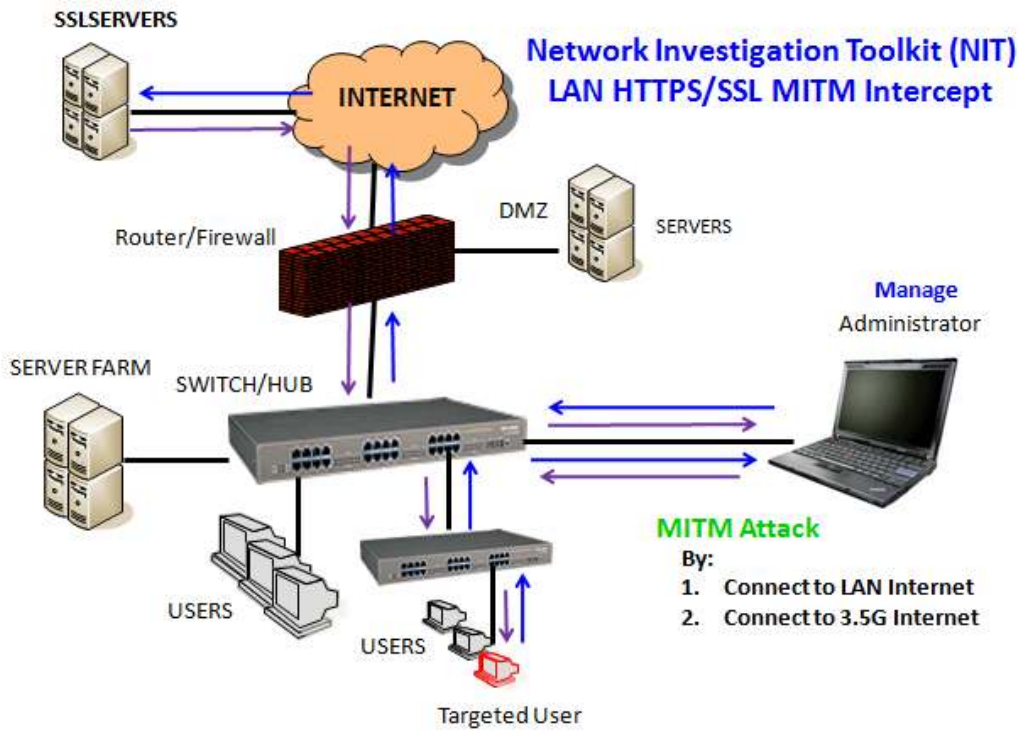


Diagram: NIT – LAN HTTPS/SSL MITM Interception

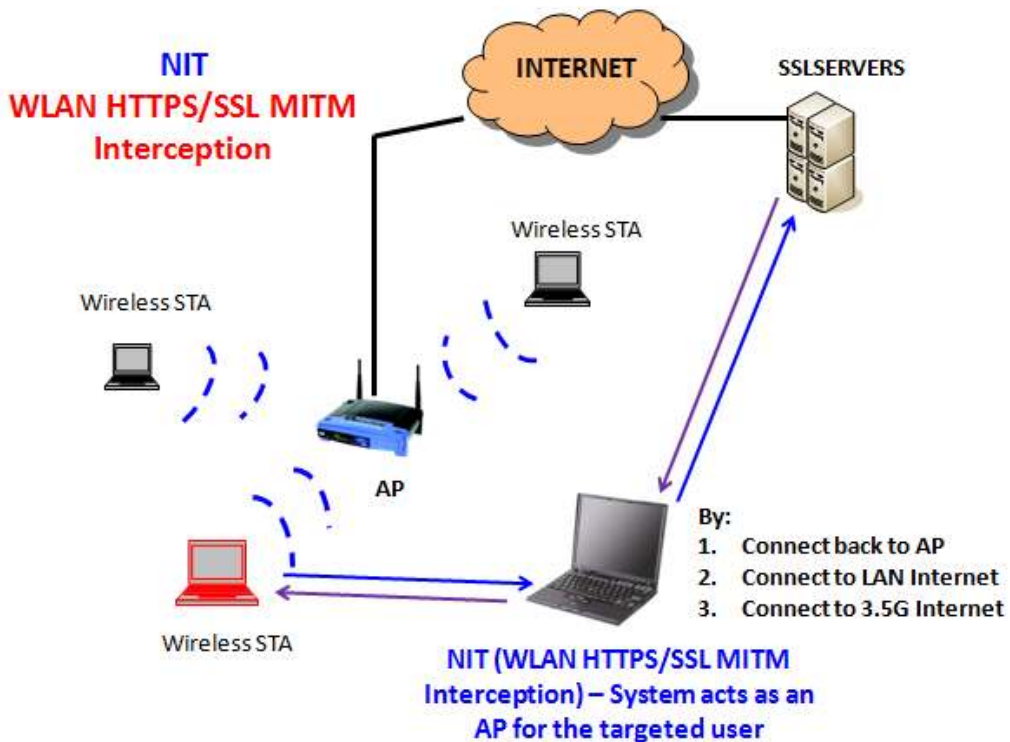



Diagram: NIT – WLAN HTTPS/SSL MITM Interception

NIT Standard Specifications:

Network Investigation Toolkit (NIT)	
Sample Product Photo (for illustration only)	 <p>USB 3.5G/HSDPA Adapter</p> <p>Lenovo ThinkPad X200</p> <p>USB Hub</p> <p>USB WiFi Adapters</p>
General Features and Functions	
Appliance Based	Yes, complete with hardware and software.
Hardware	1 x Lenovo ThinkPad X200 Laptop with internal Wi-Fi Adapter and Ethernet LAN Adapter. 4 x External USB Wi-Fi Adapters (for up to 4 WLAN Channels Capturing). 1 x 3.5G/HSPDA USB Network Adapter (for Remote Access)
Level and Size of Implementation	Ethernet LAN and Wireless LAN Interception and Internet Content Reconstruction. Ethernet LAN size (50 users or approximately 10-20 Mbps Throughput). Wireless LAN (up to 4 Channels capturing concurrently.)
Ethernet LAN and Wireless LAN Interception	Real-Time Capturing and Reconstruction.
Mode of Operation	Ethernet LAN Interception, Wireless LAN (802.11b/g/n) Interception, HTTPS/SSL Interception and Offline Raw Data Reconstruction
Implementation - Ethernet LAN Interception	Capture Ethernet LAN traffic (up to about 50 users or 10-20 Mbps throughput) through the built-in Ethernet LAN Adapter. Provides Real-Time Capturing and Reconstruction.
Implementation - Wireless LAN (802.11b/g/n) Interception	Capture Wireless LAN traffic (Manually select from 1-4 Diff. Channels or 1-4 Diff. Stations through external USB Wi-Fi Adapters. Provides Real-Time Capturing and Reconstruction. Support cracking of WEP Key.
Implementation - Wireless MITM Attack (via Ethernet)	Intercept HTTPS/SSL traffic on Wireless LAN user using external USB Wi-Fi Adapter and connect back to Internet through System internal LAN Ethernet Adapter connection.
Implementation - Wireless MITM Attack (via Wireless)	Intercept HTTPS/SSL traffic on Wireless LAN user using external USB Wi-Fi Adapter and connect back to Internet through System internal Wi-Fi Adapter connection.
Implementation - Wireless MITM Attack (via 3G)	Intercept HTTPS/SSL traffic on Wireless LAN user using external USB Wi-Fi Adapter and connect back to Internet through the used of 3/3.5G external USB Modem connection.
Implementation - Ethernet LAN MITM Attack (via Ethernet)	Intercept HTTPS/SS traffic on Ethernet LAN user using the internal Ethernet LAN Adapter and connect back to Internet through the same Ethernet LAN Adapter connection.
Implementation - Offline Raw Data Import and Parsing	Yes, available. Up to 100 cases can be created. 100 raw data files to be imported at once. Total raw data files imported cannot be more than 10 GB.

System Management	Local Machine or Remote Access - Web GUI (by Firefox), VNC Remote Control.
Storage Size	Single HDD - Size:320GB
Internet Protocols Supported - Decode and Reconstruction	
Email	POP3, SMTP, IMAP
Webmail	Yahoo Mail, Gmail, Windows Live Hotmail, Hinet, Hotmail Standard, PCHome, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com, Gawab
Instant Messaging (IM/Chat)	Yahoo Messenger, Windows Live Messenger (MSN), IRC, ICQ, UT Chat Room, Gtalk, Yahoo Web Chat, MSN Web Chat, Skype Voice Call Duration Log
Skype (4.0) Text and Voice Chat Recording - Additional License Required	Skype Agent Implementation for LAN/Organization Networks
HTTP	Link, Content, Upload and Download, Video Streaming (Youtube, Metacafe, Google Video etc.)
HTTPS (for HTTPS/SSL Interception Only)	HTTPS Decoding and Reconstruction. Username and Password.
File Transfer	FTP Upload/Download, P2P File Sharing (BitTorrent, eMule/eDonkey, FastTrack, Gnutella)
Telnet	Support with Play Back
Online Games	Various Online Games like Ragnarok Online, Mapple Story, War of World Craft, ZT, FairyLand, Kin of king, Katrider, BnB, Mabinogi, Hotdance, Gatamped, Pangya, Heatproject, DTG, Superrich, O2jam, Seal, COCOCAN, Nage, Gersang, Laghaim, Hot, 3P, SF, Noritel, Elysium, Stoneage, A3, HE, ZU, Cabala, JY1, JY2, Wonderland, SAN, TS, LoveBox, SANGO, Dekaron, Cabal, Rohan, GVO, CG, DOMO, BO, SWDOL, DOMOFREE, RICHOL, RO, Mir3, JX, JX2, TTH, RF Online, SOL, Nobol, FDO, GHOSTSOUL, AL, CPW, 1003b, 9D, EverQuestII, Silkroad2, Metin, MS, SUN, Hero, HB, WE5, FongShen, FongShen2, Q3baby, SHE and Megaten.
VoIP (IM)	Yahoo Messenger and Gtalk voice (reconstruct back to GIPS format - GIPS Decoder with Codec is required to play back the audio file).
Webcam (IM)	Yahoo Messenger and Windows Live Messenger Webcam session
VoIP (Standard) - Additional License Required	SIP, H.323 RTP Voice Sessions (Supported Codecs includes G.711 u-law, G.711 a-law, G.723, G.726, G.729 and iLBC)
Analysis, Forensics, Administrative, Management Functions	
Raw Data (PCAP) Reserving Function	Yes, available.
Search	Free Text Search, Conditional Search.
Data Export Backup - Retention	Yes, export and backup entire system data external storage or burn in CD/DVD.
Detail Information of Targeted User/PC	Account (AD, Username etc.), IP Address, MAC Address, PC Name
Import and Export of Data for Analysis	Import Raw Data for Analysis. Export-Backup Entire System Data.
Reporting	Traffic Report
Other Features, Functions and Capabilities	

Target Market

Government Agencies, Lawful Enforcement Agencies (Military, Police, Intelligence, National Security, CID etc.)