



7<sup>th</sup> Dec., KL, Malaysia, ISS World 2016

http://

@

**Crime Investigation and  
Prevention with  
Network Investigation Toolkit - NIT 2.0**

**Decision Group**

**2016**

# Agenda

- ❖ **Cybercrime via Wi-Fi Network**
- ❖ **Tactic Wireless Interception – NIT 2.0**
- ❖ **Enhanced Wireless Interception Deployment**
  - Multiple-point Interception Deployment
  - Options
- ❖ **Full Wireless Interception Deployment**
- ❖ **Operation of NIT 2.0**
- ❖ **Case Study**
- ❖ **Conclusion**

# Cybercrime via Wireless Network

- ❖ **Most internet users often access corporate or public free Wi-Fi network via mobile device under friendly BYOD environment**
- ❖ **Such cybercrime are either done by criminal rings anonymous or disgruntled employees within office**
  - Drug dealing or cyber gambling
  - Communication from hidden corners
  - Confidential corporate information leakage
  - Spreading messages of rumor or instant photos to others
- ❖ **Crime through public Wi-Fi network can prevent from being tracked down by police via wireless mobile network**
- ❖ **Spilled-over RF of private Wi-Fi networks without protection is still common in the residential area**

# Crime Investigation and Prevention

- ❖ **Target at suspects' online activities**
- ❖ **Collect more evidence on suspicious online activities of mails, social media...etc.**
- ❖ **Clarify all facts, criminal scope and motives through data scoping and link analysis**
- ❖ **Present all results into investigation report and forward it to legal process**

# Tactic Wi-Fi Interceptor

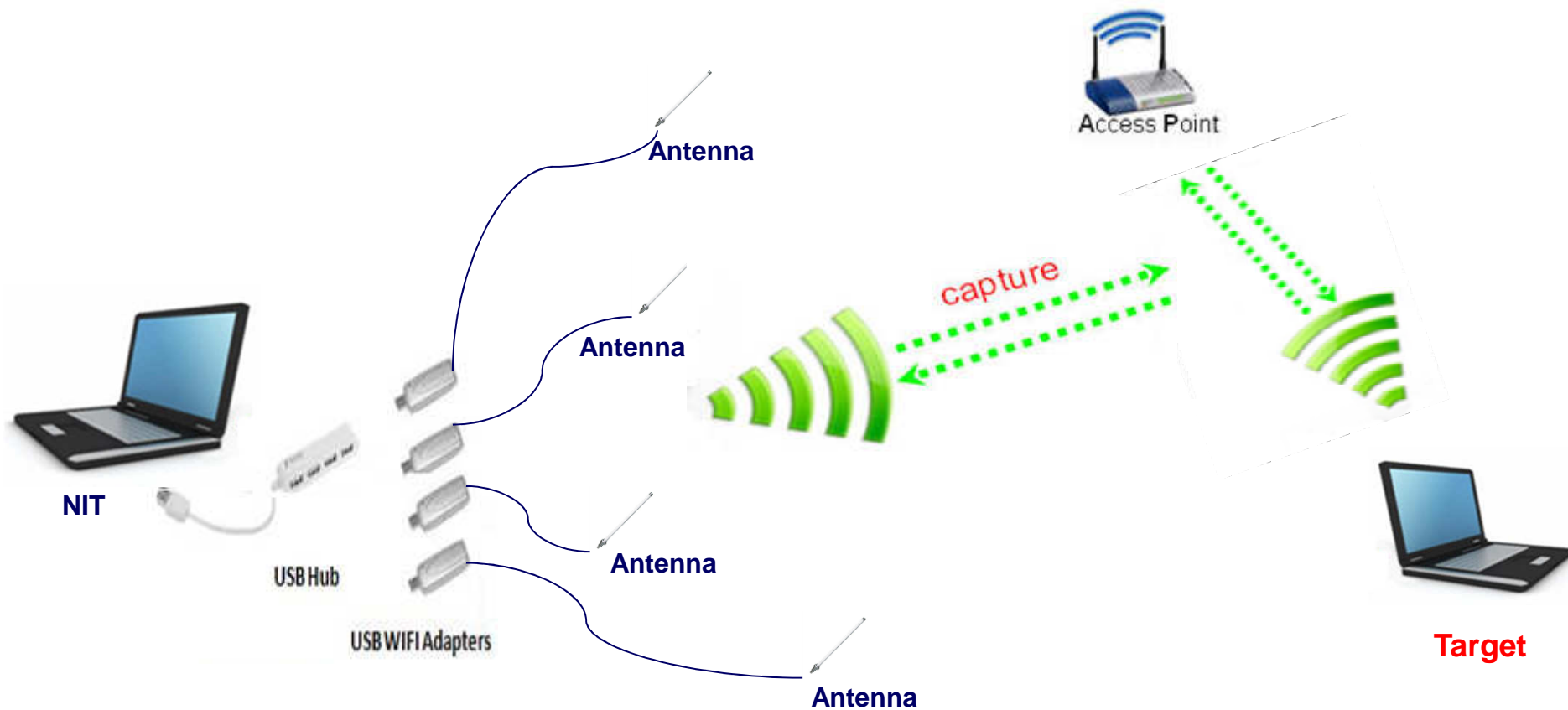
## ❖ Decision Group NIT 2.0 for Anti-Internal Threats

- Target on either Access Point or Linked Devices on Wi-Fi network
- Works on both modes of spilled-over RF wave for non-HTTPS interception and MiTM for HTTPS interception
- Capable of protocol decoding with 140+ protocols and online services
- Presents full reconstructed intercepted communication contents of mail, webpages, Facebook, Gmail, ...etc.
- With traffic statistic report for investigation
- Works with external WPA Cracking System against unknown APs for WPA key availability
- Portable form factor for hand carry or sedentary form factor for security surveillance on mob event
- Capable of blocking all Wi-Fi traffic within designated area

# Advantages

- ❖ Easily implemented and powerful system performance
- ❖ Long distance of RF scanning capability and high gain rate (92%+) of RF capture
  - By multiple external high gain antenna
- ❖ Online decoding capability on 140+ online services and protocols with full presentation of both meta data and reconstructed content
- ❖ Case management for investigation on cybercrime instances
- ❖ Co-work with WPA Cracking system for both WEP and WPA key management
- ❖ Equipped with data scoping and analysis tool for report utilities
- ❖ Comply fully with ISO 27037 standard for digital data forensic procedure

# Multiple-point Wireless Interception



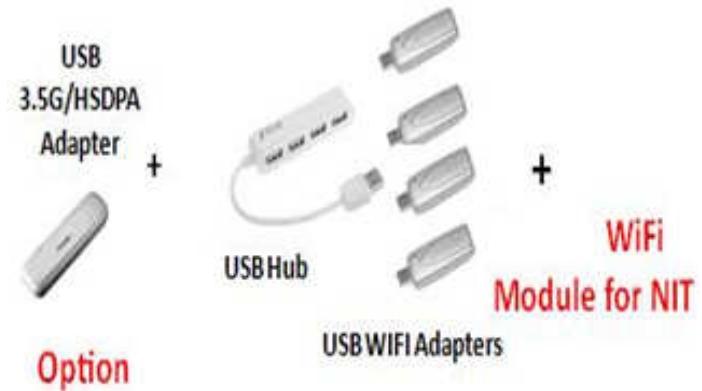
# Options

## ❖ For Extended Wireless Interception

- USB Hub X2
- WiFi Dongle X4
- 8 dB Antenna X4

## ❖ For Backend Communication

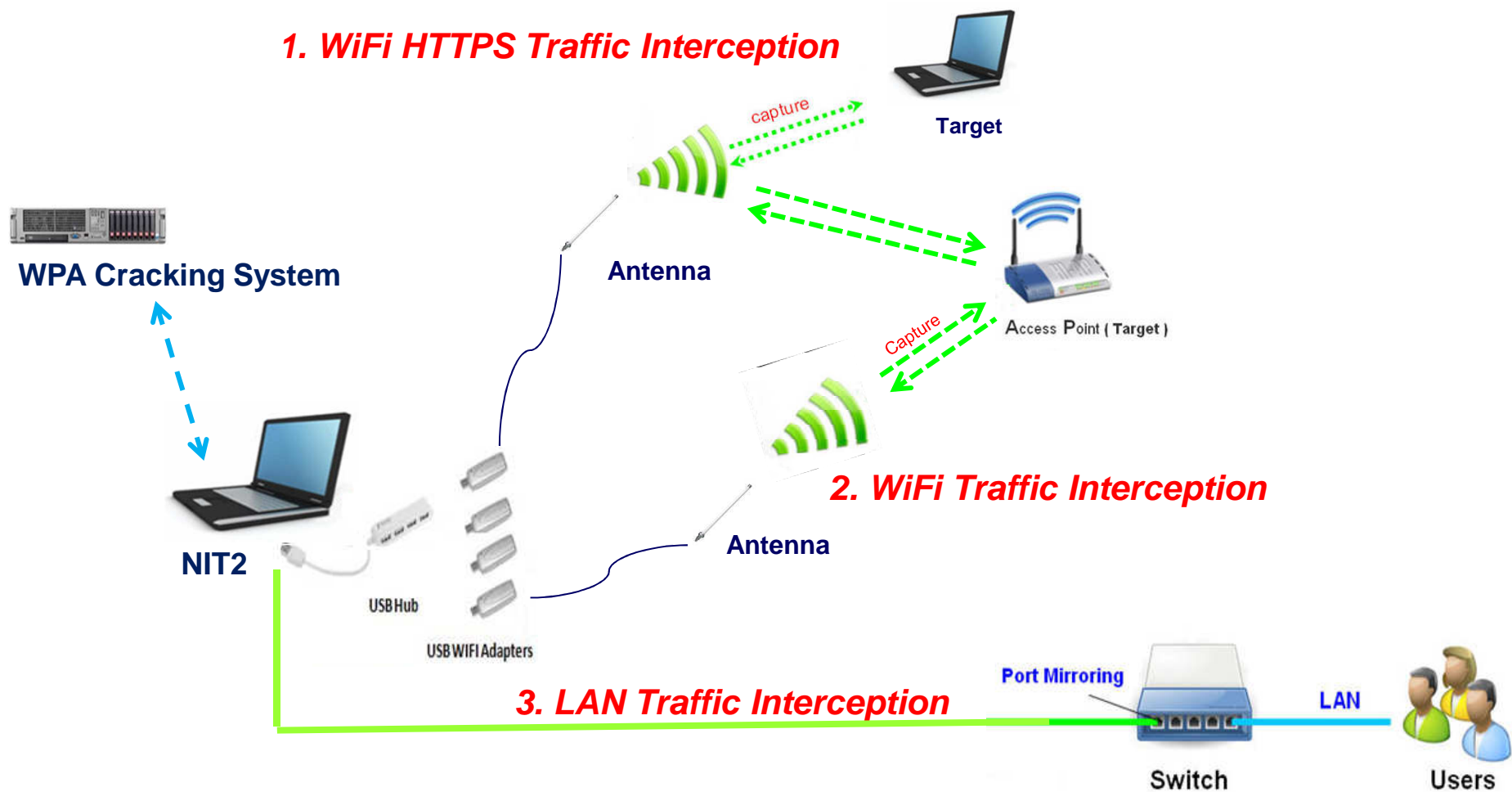
- 3.5G/HSPDA USB Dongle

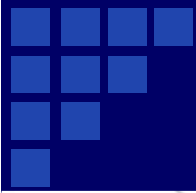


Antenna



# Full Deployment for HTTPS and LAN Interception





# SYSTEM OPERATION



# Packets Collecting

- packet collect and parsing :

System Management - Capture Mode Management Version - Logout

Case Name :training Event Name :WD-2014-06-11 16:09:21 Mode Name :Wireless Status :  Start  Stop

Home(Case List)

Add Case

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-06-11 15:42:08	training	1	admin		Enter
2014-06-10 15:21:55	default	0	admin		Enter

First Previous 1 Next Last 12 Records/Page

Message

Function	Message
Case Name	training
Event Name	WD-2014-06-11 16:09:21
Creator	admin
Created Time	2014-06-11 16:09:24
Mode Name	Wireless
Capture Mode	WLAN Sniffer Mode
HTTPS/SSL Module Enable	No
Status	Stop
Rawdata Path	/home/admin/cases/training

Close

# Data Presentation

## ■ Data Presentation :

The screenshot displays a web application interface with a navigation bar at the top containing 'System Management - Capture Mode Management Version - Logout'. Below the navigation bar, there is a status bar with 'Case Name : training Event Name : WD-2014-06-11 16:09:21 Mode Name : Wireless Status : Start Stop'. The main content area is divided into two sections. The top section, titled 'Home(Case List)', contains an 'Add Case' button and a table with columns: Created Time, Case Name, Event Number, Creator, Edit, and Option. The table has two rows: one for 'training' (Event Number 1, Creator admin) and one for 'default' (Event Number 0, Creator admin). The bottom section, titled 'Home(Case List) Case : training', contains an 'Add Event' button, a search bar, and a table with columns: No., Event Name, Created Time, Mode Name, Capture Mode, Mail, Chat, SNS, Web, Files, and Others. The table has one row for 'EDDC-2014-06-11 17:17:21' (Created Time 2014-06-11 17:17:35, Mode Name import, Capture Mode Offline Decode Packets Mode, Mail 30, Chat 4, SNS 32, Web 2765, Files 21, Others 584). A red arrow points from the 'Option' column of the first row in the top table to the 'Mail' column of the first row in the bottom table.

Created Time	Case Name	Event Number	Creator	Edit	Option
2014-06-11 15:42:08	training	1	admin	↔ ✕	Enter
2014-06-10 15:21:55	default	0	admin	↔	Enter

No.	Event Name	Created Time	Mode Name	Capture Mode	Mail	Chat	SNS	Web	Files	Others
1	EDDC-2014-06-11 17:17:21	2014-06-11 17:17:35	import	Offline Decode Packets Mode	30	4	32	2765	21	584

**Mail** : POP3,SMTP,IMAP,WebMail

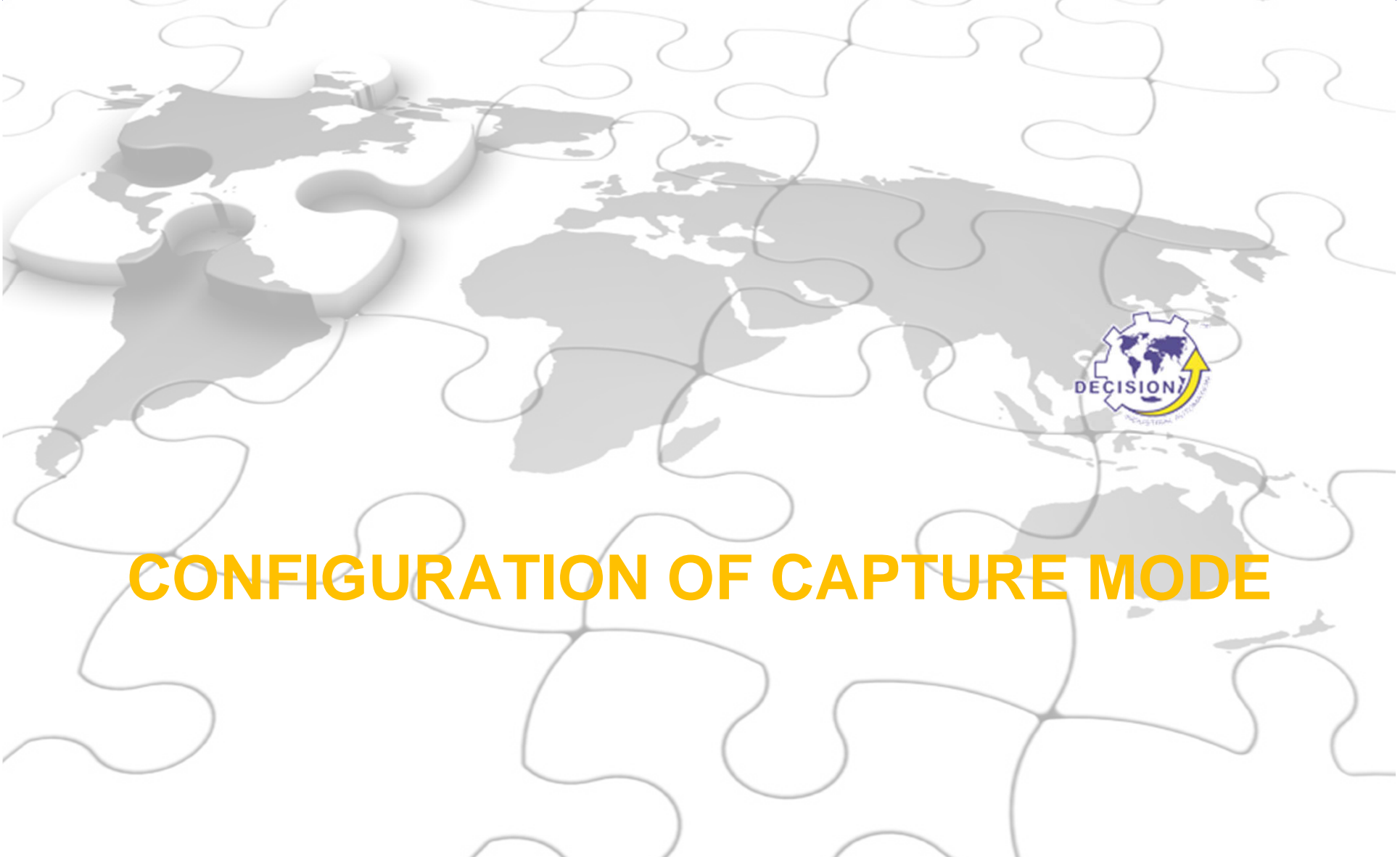
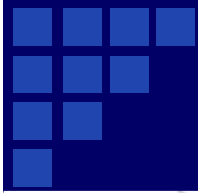
**Chat** : Yahoo,ICQ,Skype etc.

**SNS** : Facebook, Twitter, Plurk

**Web** : Video Stream, Web page, HTTP file upload/download

**Files** : FTP, P2P, Dropbox, Evernote

**Others** : Telnet, Online game, Web password etc.



# CONFIGURATION OF CAPTURE MODE

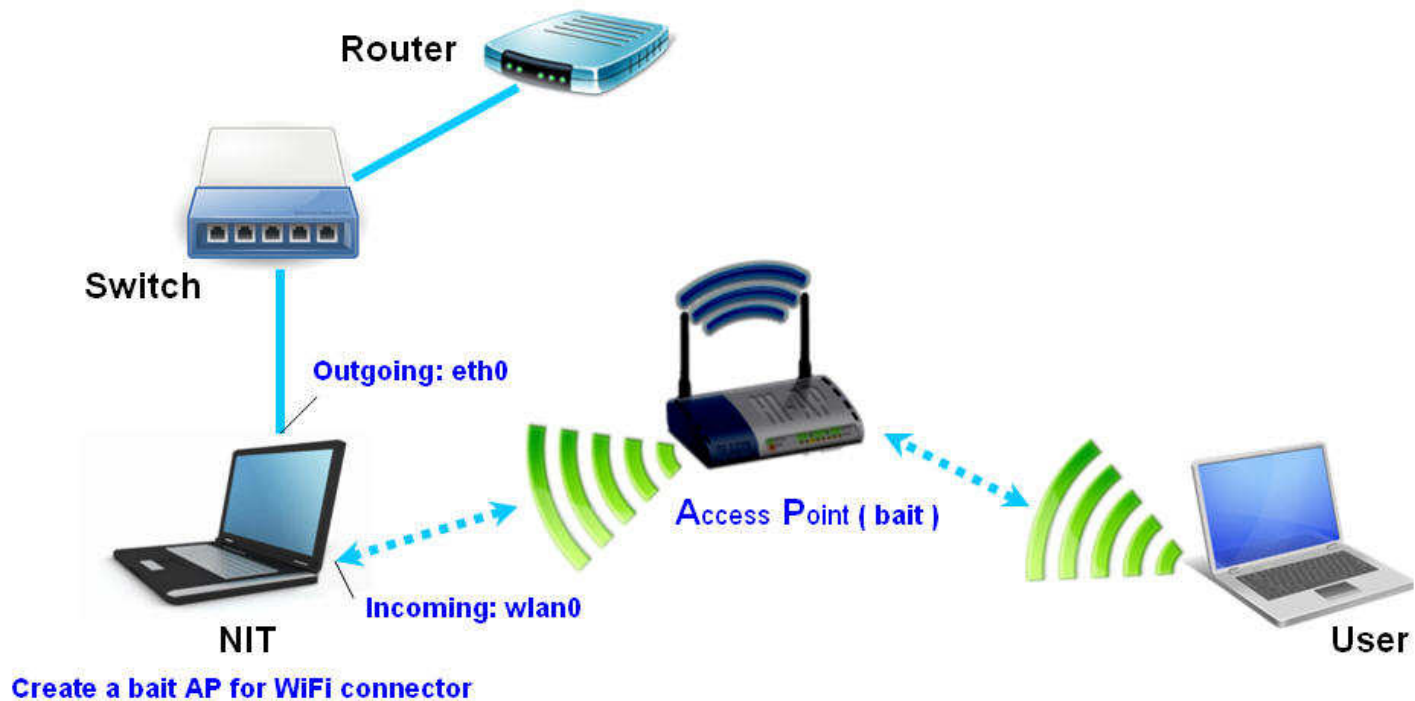
# Capture Mode Management

- WLAN Sniffer Mode without HTTPS



# Capture mode management


- WLAN Sniffer Mode with HTTPS





# Certificate



- Browser Certificate Warning
    - Once the HTTPS/SSL function is enabled in Transparent Proxy connection mechanism, the browser will pop up a connection security warning message or abnormally terminate the incoming webpage when target user opens the HTTPS webpage.
    - For such issue, there are two options provided to solve it.
- 



# Build-in Certificate

- Build-in Certificate
  - Use the system certificate for verification: press Export button to download and install key.zip certificate file in the target user computer.
  - Press Modify button, you can import and edit information for the certificate content.

Step 4 : Transparent Proxy

Use Build-in Certificate  Import Legal Certificate

Modify Export Certificate Import Key Import

Certificate Information

Issued To	Issued By
Country : AU	Country : AU
State or Province : Some-State	State or Province : Some-State
Locality Name :	Locality Name :
Organization Name : Network-Recorder	Organization Name : Network-Recorder
Organization Unit :	Organization Unit :
Common Name :	Common Name :

Previous Step Next Step

# Certificate Import

- Legal Certificate Import
  - If you has a legitimate certificate and key, you can upload and replace the build-in certificate
  - Please choose the Certificate Import and Key Import button to upload it.

Step 4 : Transparent Proxy

Use Build-in Certificate  Import Legal Certificate

Modify Certificate Import Key Import Export

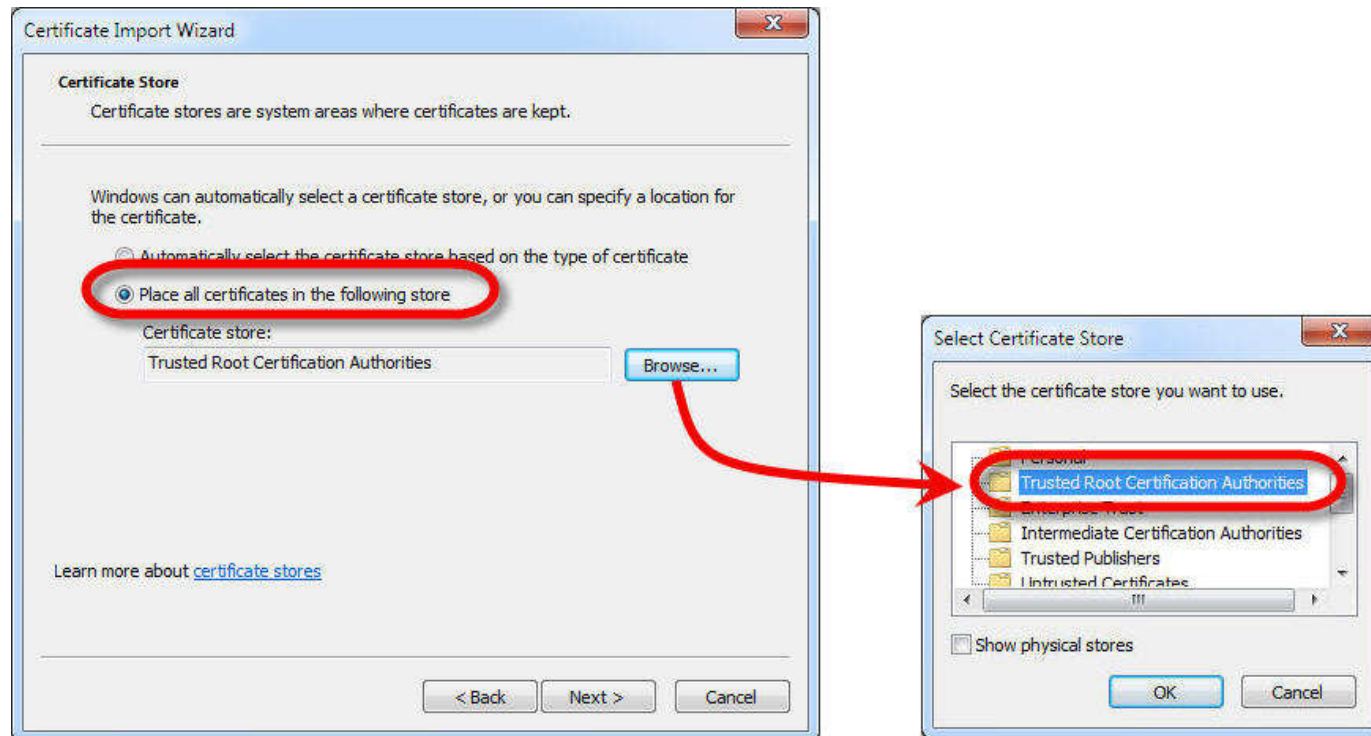
Certificate Information

Issued To	Issued By
Country : AU	Country : AU
State or Province : Some-State	State or Province : Some-State
Locality Name :	Locality Name :
Organization Name : Network-Recorder	Organization Name : Network-Recorder
Organization Unit :	Organization Unit :
Common Name :	Common Name :

Previous Step Next Step

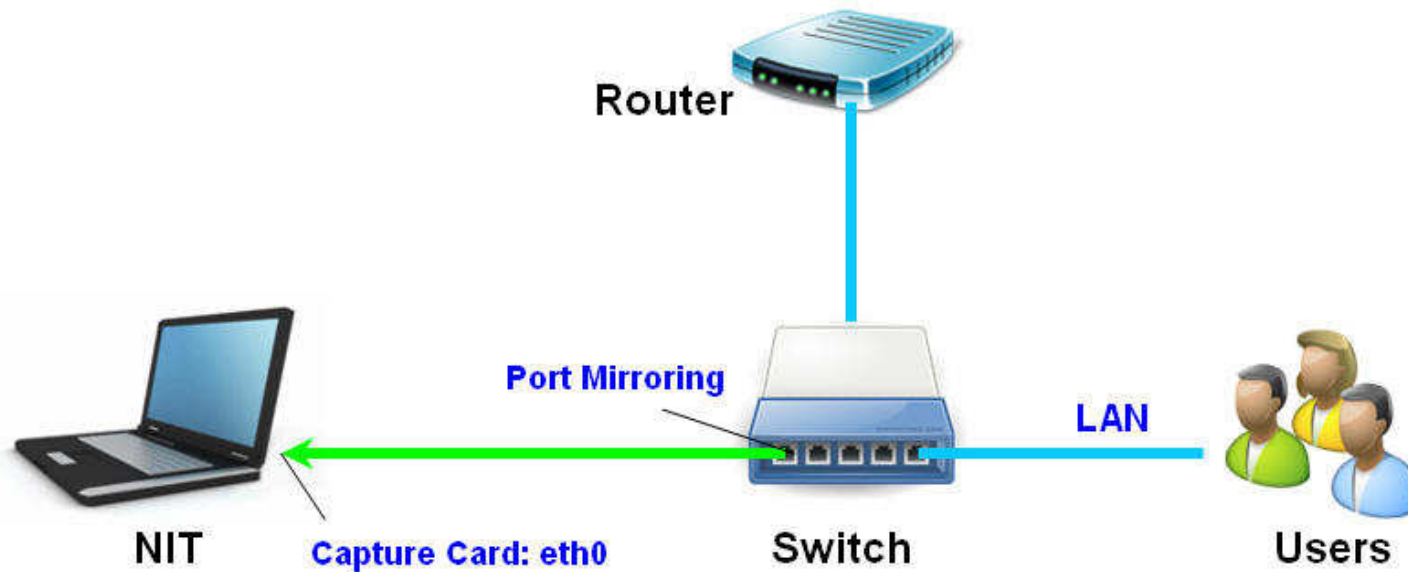
# Certificate Installation

- Install Certificate File into Target
  - After decompressing key.zip, please click the file of server.crt to invoke Certificate Import Wizard
  - Select *install certificate function* and install the certificate to the Trusted Root Certification Authorities.



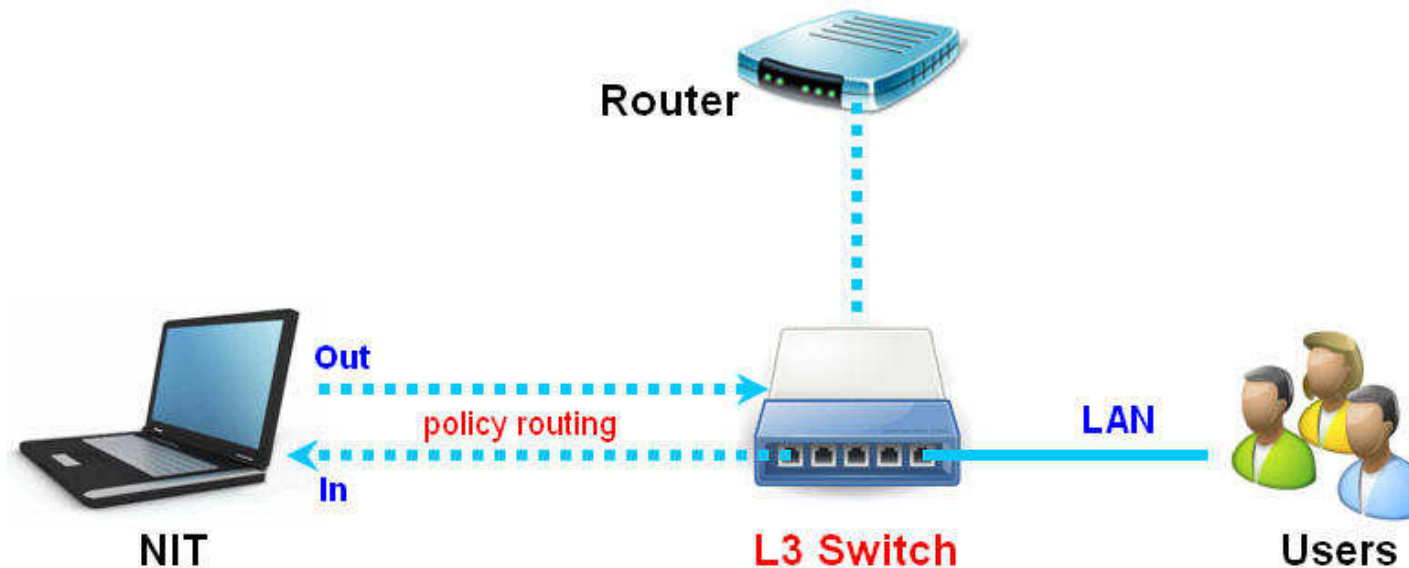
# Capture mode management

- Ethernet Sniffer Mode without HTTPS



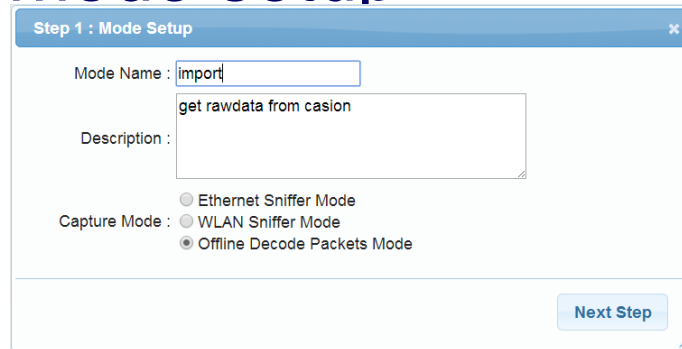
# Capture mode management

- Ethernet Sniffer Mode with Transparent Proxy



# Offline Decode Packets Mode

- Step 1 : mode setup



Step 1 : Mode Setup

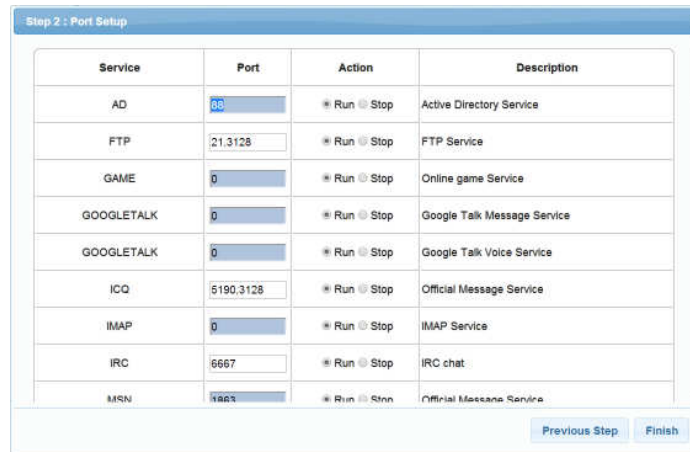
Mode Name : import

Description : get rawdata from casion

Capture Mode :  Ethernet Sniffer Mode  
 WLAN Sniffer Mode  
 Offline Decode Packets Mode

Next Step

- Step 2 : port setup



Step 2 : Port Setup

Service	Port	Action	Description
AD	389	Run Stop	Active Directory Service
FTP	21,3128	Run Stop	FTP Service
GAME	0	Run Stop	Online game Service
GOOGLETALK	0	Run Stop	Google Talk Message Service
GOOGLETALK	0	Run Stop	Google Talk Voice Service
ICQ	5190,3128	Run Stop	Official Message Service
IMAP	0	Run Stop	IMAP Service
IRC	6667	Run Stop	IRC chat
MSN	1863	Run Stop	Official Messana Service

Previous Step Finish

# Offline Decode Packets Mode

- Step 3 : Import Packet File



# Correlation of Target Network User Identities

## ❖ User Identities from Intercepted Data

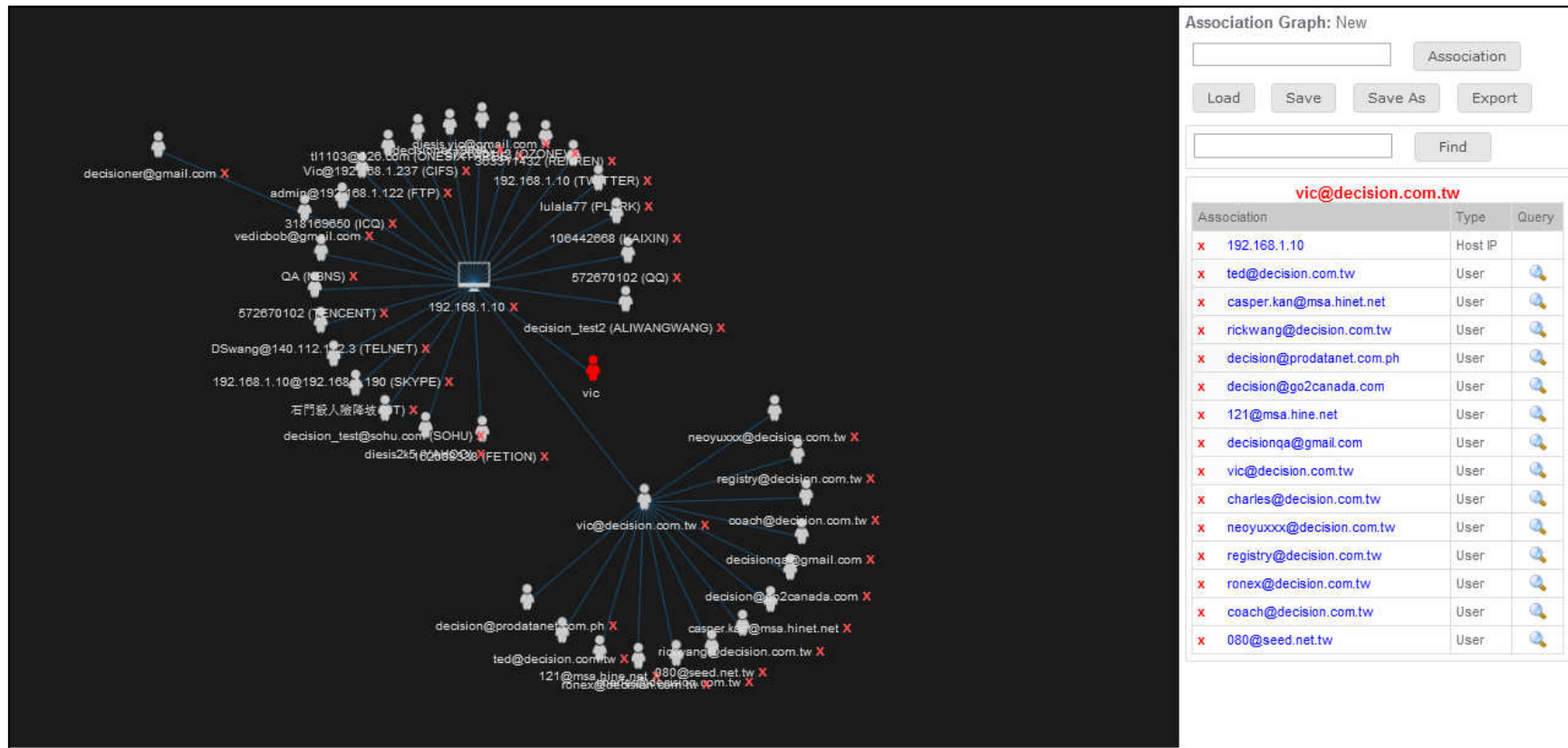
- Network Access Level (network layer) – IP, MAC
- Online Service Level (application/OTT layer) – eMail Address, account ID of social media...etc.

## ❖ Correlation between Network and Application/OTT Levels - Link Analysis










# Link Analysis

For correlation between account ID of network and application levels

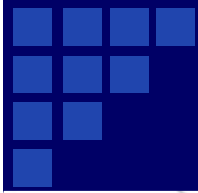


# More Than 140+ Internet Service Decoder



<b>Generic E-Mail</b>	<b>POP3, IMAP, SMTP</b>	
<b>Webmail</b>	<b>GMail, Yahoo, Hotmail, ... more than 21 webmails</b>	
<b>Instant Message</b>	<b>MSN, Hangout, ICQ, ... more than 8 IMs</b>	
<b>Web Page</b>	<b>Web Link, Content and Request</b>	
<b>Web FTP</b>	<b>Upload/Download</b>	
<b>Web Video</b>	<b>YouTube, GoogleVideo ...</b>	
<b>File Transfer</b>	<b>FTP, P2P, ... more than 20 services</b>	
<b>Telnet</b>	<b>Animated playback available</b>	
<b>Asia On-Line Game</b>	<b>More than 81 games</b>	
<b>VoIP</b>	<b>SIP, RTP (G.711, G.726, G.729, iLBC)</b>	
<b>Social Network Service</b>	<b>Facebook, Twitter, Plurk ...</b>	
<b>Mobile Online Applications</b>	<b>APP &amp; Web Services on iPhone, Android ...</b>	
<b>Database</b>	<b>Oracle, MS SQLServer, MySQL...</b>	





# CASE STUDY

# Case 1: Criminal Tracking

- ❖ **Locating MAC address of target suspect's mobile device**
- ❖ **Check the link pair of MAC address and IP addresses of target mobile device**
- ❖ **Find out the geo-location mapping of target based on the IP address within communication session**
  - IP may not be always reliable all the time, so you should pay attention on the pair of MAC address

## Case 2: Tracking eMail

- ❖ **Data scoping on intercepted email and webmail data within period by target network user IDs**
- ❖ **Confirm the factors below for case establishment**
  - Cyber identity verification on webmail services
  - Frequency of links among target email and webmail transaction records
  - Timestamp on each event

## Case 3: Rumors

- ❖ **Spreading un-identified information or news to ignite strong mood in office**
- ❖ **Data scoping on intercepted data within period by target keywords**
- ❖ **Confirm the factors below for case establishment**
  - Cyber identity verification on target services with keywords
  - Timestamp on each event

## Case 4: Abnormal External Access

- ❖ External access with fake identity into closed corporate network via spilled-over Wi-Fi networks
- ❖ Data scoping on intercepted data by target user ID within logon period
- ❖ Confirm the factors below for case establishment
  - IP address of non-registered MAC address
  - Logon identity vs multiple cyber identities of online service
  - Records of all transaction activities, especially data retrieval, system logon, information modification...etc.
  - Timestamp on each event

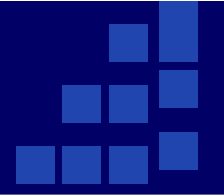
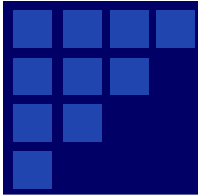
## Case 5: Checking out the Position

- ❖ **Some APPs use GPS data of mobile device for LBS**
- ❖ **Mapping target location and movement by intercepting GPS data of APP**
- ❖ **Confirm the factors below for case establishment**
  - Verify target identity, IP and MAC address
  - Check URL address used by the backend server of weather service, pushing ads...etc.
  - Confirm GPS data with IP address at the timestamp
  - Locate the corner of mobile device or trace the movement track of mobile device
  - Timestamp on each event



# Conclusion

- ❖ **DPI/DPC solution is fast-growing one in the market segments of Public Sector, FSI, Telco and LEA.**
- ❖ **It is just cross the chasm in the early majority stage of above segments**
- ❖ **Decision Group has lot of self-developed turnkey solutions, technologies, and product roadmap plan in this market.**
- ❖ **Fully meeting customer requirement and expectation is the top priority of Decision Group**
- ❖ **Good references and globalized services provided in different counties**



**decision@decision.com.tw**

**URL: <https://www.edecision4u.com>**

**Q & A**

