Tactic Lawful Interception Operation on Fixed Network

Marketing Department

Decision Group Inc.

2013

Content

- **Tactic Lawful Interception**
- **3 Factors in Operation**
  - Decision Group Interceptor
  - Network Infrastructure
  - Target Traffic
- **Proposed Deployment**
- **Standard Operation Procedure**
  - Primary Data Analysis
  - Provision Data
  - Training Programs
- **Pros and Cons**
- **Customization Scope Confirmation**
- **Solution Package**
- **Estimated Cost for Budget Planning**
- **Wrap up**

Tactic Lawful Interception

- Tactic Lawful Interception Operation is the way investigator uses lawful interception device to receive the traffic from operator POP center or internet exchange gateway, and have it intercepted the communication traffic for crime investigation or intelligence collection
- It is for temporary deployment instead of permanent operation
- It must be used for specific case by authorized personnel.
- Traffic must be directed into one point by the help of network management staff of operator or international exchange gateway
- Target user provision data may not be available directly from traffic but it can be available by link analysis on the intercepted data

3 Factors in Operation

- Effective lawful interception device for traffic interception, traffic decoding, content reconstruction and data analysis – **Decision Group Systems**
- Appropriate interception point in network infrastructure of operator or international exchange gateway – **Telecom Network**
- Target traffic directed into Police Data Center by the help of operator's network management system – **Warrant Order from Police**

Decision Group Interceptor 1

Major System for non-HTTPS – E-Detective

- E-Detective is to collect common non-HTTPS data packets by mirroring traffic from access edge router or PDN Gateway
- Upon receiving traffic, ED will decode it and reconstruct it based on the protocol or service type
- All data will be saved as
  - Reconstructed content
    - CDR/IRI: in Database
    - Communication Content: as associated media file
  - Raw Data – pcap file
- Major throughput is around 500Mbps

Decision Group Interceptor 2

Major System for HTTPS - HTTPS/SSL Interceptor

- Takes Man-In-the-Middle attack on influx HTTPS traffic to decode and reconstruct all HTTPS traffic back to original content and save CDR into database
- Takes Certificate replacement mechanism to eliminate the warning message or security control in target browser end
- Provide primary data analysis for identity and criminal scope clarification
- Collect evidence for legal prosecution process
- Provide online alarm with specified keywords
- Maximum system throughput: 300Mbps

Data Access at Network

Mobile Network

- In mobile network, Decision Group ED and HTTPS/SSL must be deployed with the PDN gateway, and HTTPS/SSL will be as transparency proxy cache engine with target HTTPS traffic whereas ED just takes mirroring traffic from PDN GW

Fixed Network

- In Fixed network, Decision Group ED and HTTPS/SSL must be deployed with BRAS, and HTTPS/SSL will be as transparency proxy engine with target HTTPS traffic whereas ED just takes mirroring traffic from BRAS

- In order to have traffic load balance control, multiple devices can be deployed with load balancer.
- All target HTTPS traffic will be directed into HTTPS/SSL Interceptor for processing and reverted to original network backhaul.

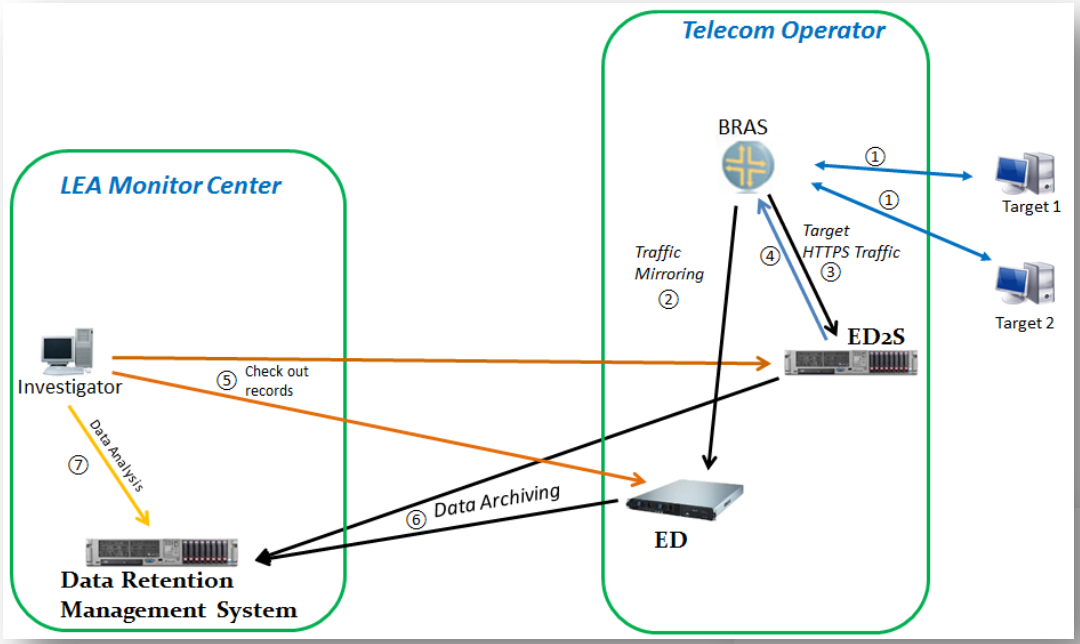
Target Traffic

- Network management staff can direct target HTTPS traffic into Decision Group HTTPS/SSL Interceptor by network management utilities of core network system
- The directed target traffic is of IP packet with original certificate of target online services.

Proposed Deployment Way

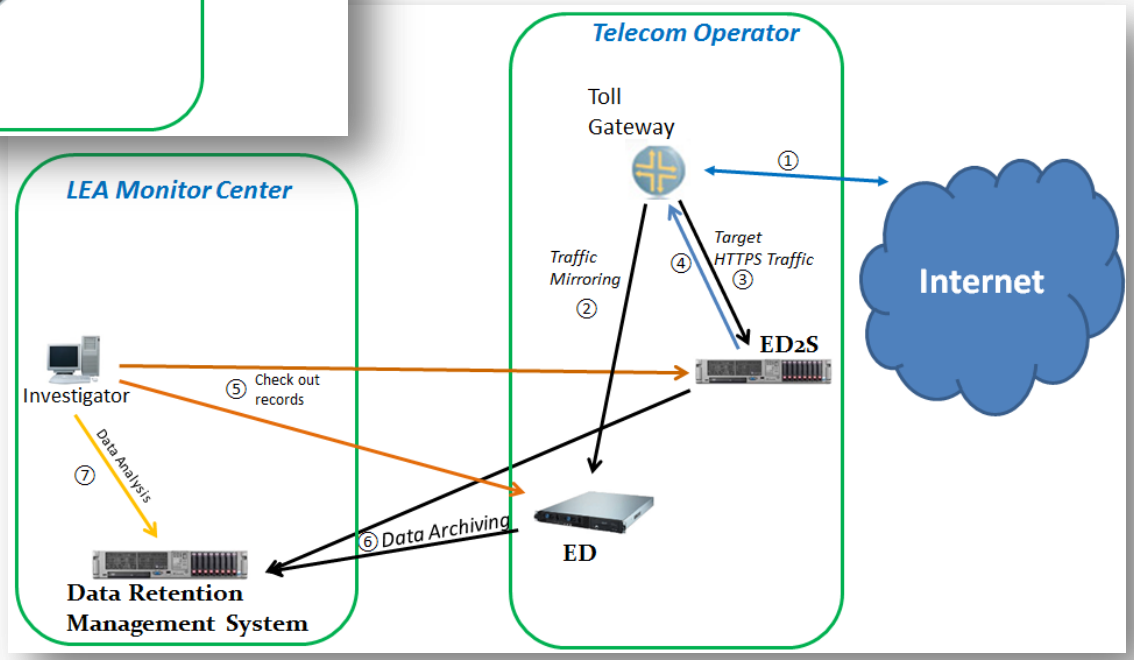
- 2 or 3 Decision Group Traffic Interceptors, based on target traffic volume, deployed with load balancer as Lawful Interception Network Segment (LINS)
- Target traffic directed from core network to LINS
- Processed traffic reverted back to core network from LINS
- There is a firewall to separate LINS and core network in POP or IEX Gw sites

Proposed Deployment on Fixed Network



Lawful Interception Network Suite (LINS) is consisted of ED, ED2S and Data Retention Management System in one set of mobile 14" rack trolley.

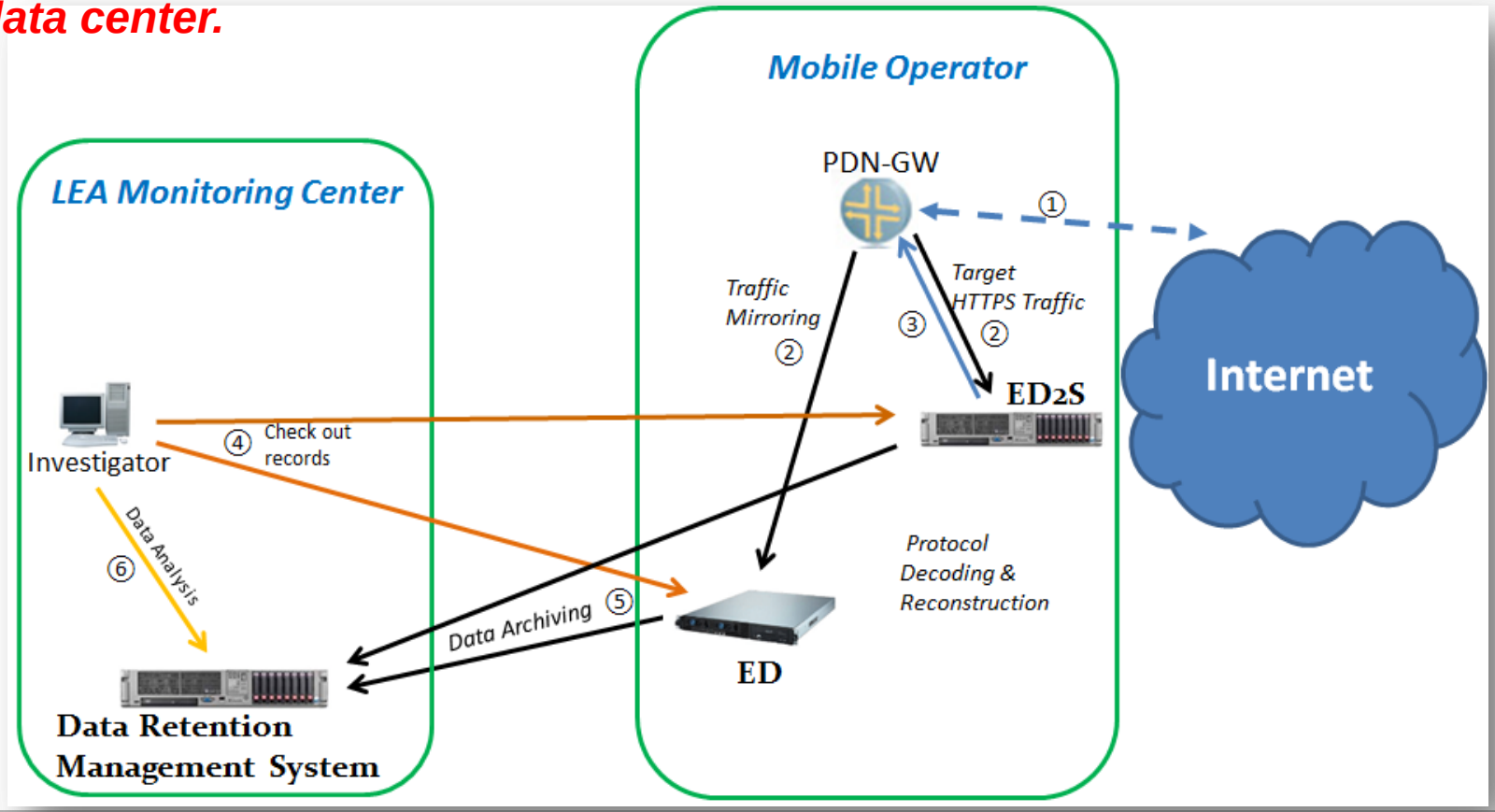
The deployment of LINS can be outside Telecom data center in order to protect operation confidentiality, but it has restriction on distance from data center.



Proposed Deployment on Mobile Networks

The deployment of LINS can be outside Telecom data center in order to protect operation confidentiality, but it has restriction on distance from data center.

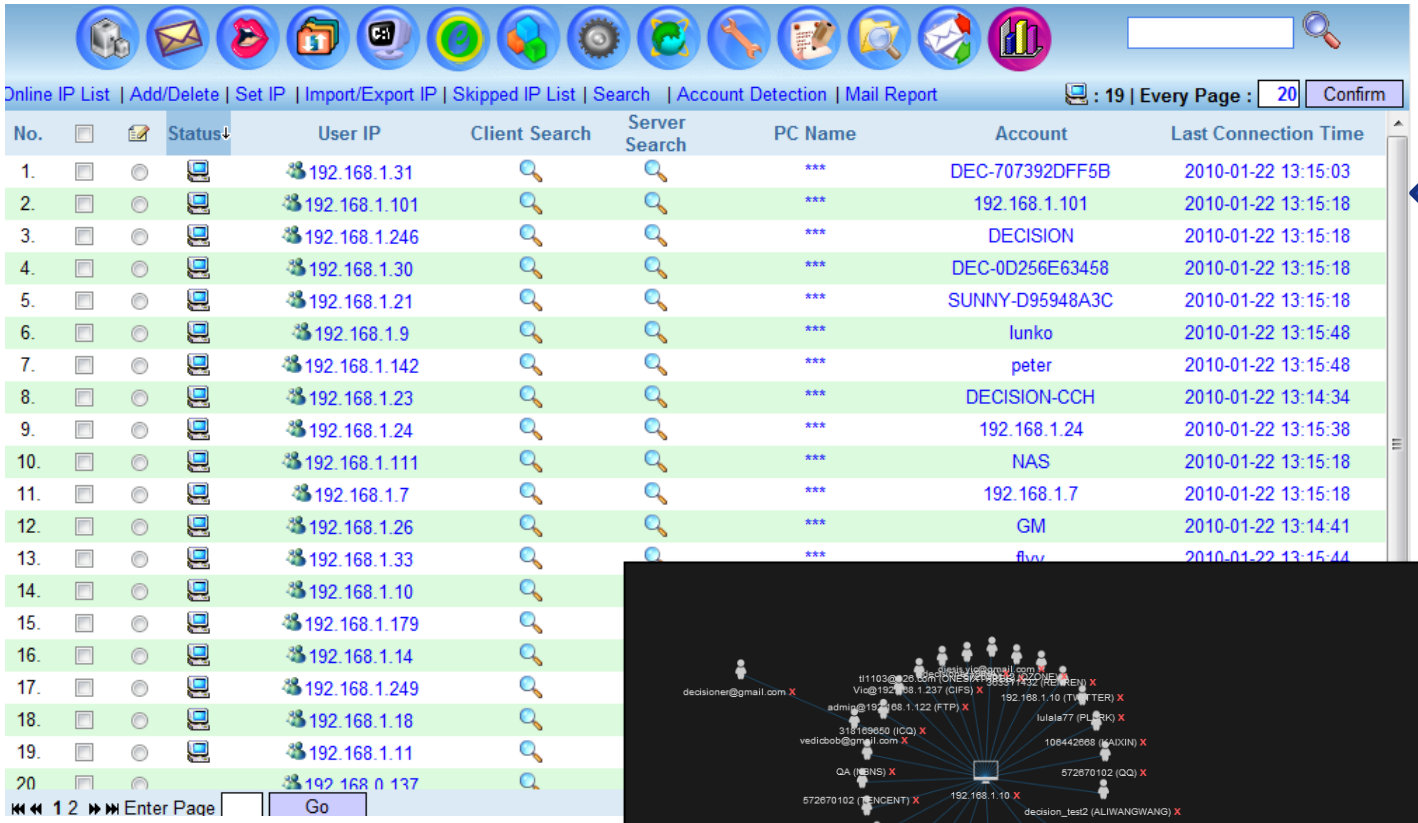
Lawful Interception Network Suite (LINS) is consisted of ED, ED2S and Data Retention Management System in one set of mobile 14" rack trolley.



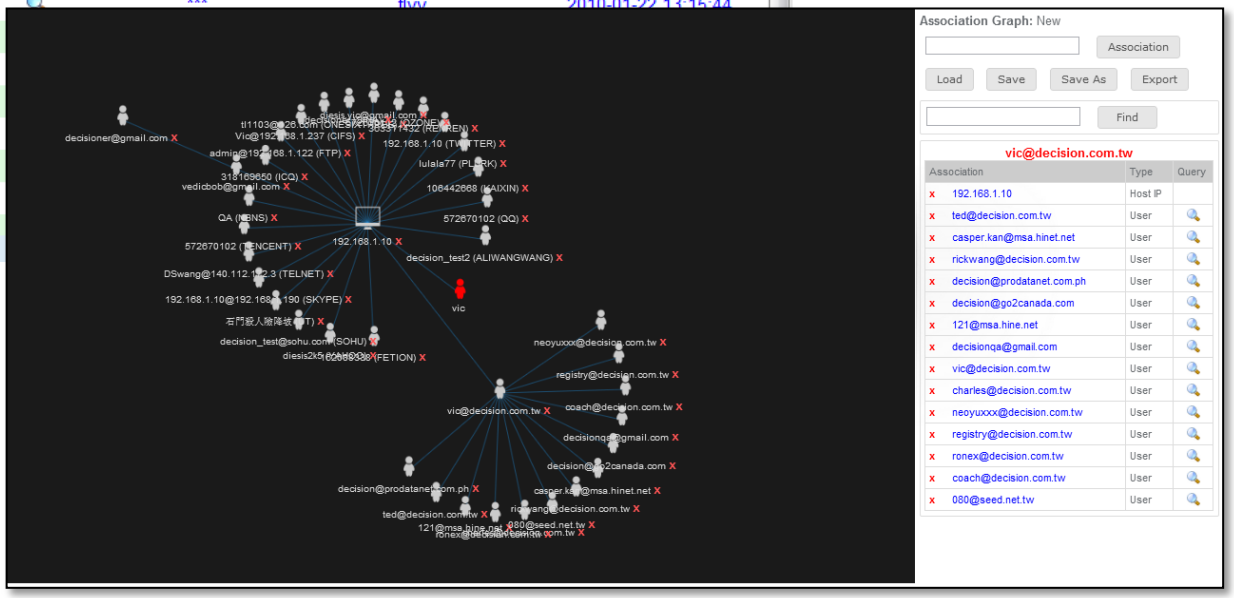
Primary Data Analysis

- **Search Operation**
  - For evidence collection by keywords
  - For intercepted record viewing
- **Condition Search Operation**
  - For scope analysis on target's activities
  - For comparison on intercepted data
- **Association Search Operation**
  - For link analysis on target identities with both network and application levels
  - For scope analysis on target's activities and counterparts

Data Provision Utilities



Network Session Level - Account linking list with IP, but Telco operator should provide AAA data first



Application Session Level - Link Association among IP, Account name, MAC

Target Services 1

Item	Type	Protocol/Service	Function Level			Remark
			Fully Decoded	Partial Decoded	Log only - Pen register	
1	email	POP3	yes			
		SMTP	yes			
		IMAP	yes			
2	webmail	Yahoo Mail	yes			
		Gmail	yes			HTTPS
		Windows Live Hotmail	yes			
		Hinet webmail	yes			
		Hotmail Standard	yes			
		PCHome	yes			
		URL website	yes			
		Giga website	yes			
		Yam website	yes			
		Sina website	yes			
		Seednet website	yes			
		126 Mail	yes			
		mail.163.com	yes			
		Sohu.com	yes			
		prodata Mail	yes			
		go2canada Mail	yes			
		REDIFF Mail	yes			
		Zimbra Mail	yes			
		intljob Mail	yes			
		mediahub Mail	yes			
		QQ Mail	yes			
		TOM Mail	yes			
		Gawab	yes			
		doxinternational Mail	yes			
		canu Mail	yes			
		nocglobal mail	yes			

Target Services 2

3	Instant Messaging	Yahoo Messenger		yes		1.Message 2.File 3.Friend List
		Windows Live Messenger 2011 (MSN)		yes		1.Message 2.File 3.Friend List
		IRC	yes			1. Message
		ICQ		yes		1.Message 2.File 3.Friend List
		UT Chat Room	yes			1. Message
		Gtalk		yes		1. Message
		Yahoo Web Chat	yes			1. Message
		MSN Web Chat	yes			1. Message
		QQ		yes		1.Message(With agent or password) 2.File (Only for sniffer) 3.Friend List(Only by sniffer with password)
		Skype		yes		1.with agent (1)message (2)file (3)voice 2. direct from network (1)voice log
		Facebook IM		yes		Only message
4	Social Networking	Facebook	yes			1.wall 2. friend list 3. album 4. message 5. account/password 6. HTTP or HTTPS
		Twitter	yes			Only wall; HTTPS
		Plurk	yes			Only wall; HTTPS
		Ren-ren	yes			only wall
		Wretch		yes		with photo album password(Only for FED)
5	Cloud service	FTP	yes			
		dropbox	yes			
		Box	yes			
		Evernote	yes			

Target Services 3

6	P2P	BitTornado			yes	IP list of each node provided
		BitComet			yes	
		uTorrent			yes	
		BitSpirit			yes	
		Azureus			yes	
		BitLord			yes	
		BitBuddy			yes	
		Flashget 1.81			yes	
		Foxy			yes	
		BitTorrent			yes	
		BitTyrant			yes	
		ezpeer+			yes	
		eDonkey			yes	
		Kazaa			yes	
		LimeWare			yes	
		BearShare			yes	
		eMule			yes	
7	VoIP	SIP	yes			1.codec list (1)G711a (2)G711u (3)G726(high/low) (4)G729(high/low) (5)iLBC(high/low)
8	Video Streaming	FLV Format	yes			Youtube, Metacafe, Yahoo!, Google Video
9	HTTP	Link	yes			
		Webcontent	yes			
		Upload	yes			only for multipart protocol
		Download	yes			default rule exe;zip;rar;torrent;doc;pdf;xls;txt;mp3;avi;rm;rmvb;asf;mpg;mpeg;ape;
10	Telnet	VT Terminal Simulation (VT320)	yes			Automatic playback
11	MS-Net	Active Directory Service	yes			account profile interception combined with agent in AD server
12	Database	MySQL Server		yes		1.Database name 2.Logon account 3.password 4.timestamp 5.SQL Command 6.Only for EDGS
		MS SQL Server		yes		
		Oracle DB Server		yes		
13	CIFS	MS MyShare Services			yes	1.host name 2.logon account 3.files uploaded and downloaded 4.timestamp 5.size 6.Only for EDGS

Training Program

NPFAT

- Network Packet Forensic Analysis Training
- Basic Introduction on Network Protocol and Services
- Understand the data format of each online service
- For field investigators and lab analysts

Cyber Crime Investigation

- Cyber Crime Investigation Practical Training
- Cyber Investigation Skill on Internet, telephony
- Data Analysis for Criminal Investigation
- Legal Prosecution Procedure
- Practical Drill and Seminar with Senior Police
- Co-held with National Taiwan Central Police University
- For field investigators

Pros and Cons

Disadvantages

- For temporary lawful interception within 2 months (< 60 days)
- Rely on operator's help for target traffic filtering
- Reply on operator's help for user session data correlation

Advantages

- Perform online data interception, decoding and reconstruction
- Perform HTTPS and associated certificate release operation
- Flexible and quick deployment in target network infrastructure

Customization Scope Confirmation

- **Based on Lawful Interception Law, below items need to be confirmed in system log report utility first:**
  - User data in profile
  - Case data in profile
  - User investigation report format with case ID, warrant approval data, time period and telco operator
- **State root trust certificate implementation**
- **Provision data preloaded from Radius of Telco operator**

Planned Solution Package

Software

- Decision Group E-Detective X3
- Decision Group HTTPS/SSL Interceptor X3
- VoIP Module X4 (optional)
- Data Retention Management System X1
- CMS X1 (optional)

Hardware within one 14U mobile rack (as trolley)

- 3X Frontend Servers – PC server with 2X CPU, 32GB memory, 1.2TB HDD, 3X 1 Gbps NIC ports, 1X DVD Drive
- Devices – 12 port switch; VPN router with firewall function; load balancer; UPS; 22U standard 19”rack with wheels, KVM switch and cabling
- DRMS Server – PC server with 2 CPU, 16GB memory, 2~5 TB HDD, 2X 1 Gbps NIC ports , 1X DVD Drive **(placed in LEA Monitor Center)**
- CMS Server (optional) – PC server with 2X CPU, 16GB Memory, 300~500GB, 2X 1 Gbps NIC ports, 1X DVD Drive **(placed in LEA Monitor Center)**

Training Programs

- Operation Training (1 day)
- Network Packet Forensic Analysis Training (3 days)
- Cyber Crime Investigation Training (5 days)

Customization Service

- Customization Report Utilities
- Root Trust Certificate Mechanism
- AAA data uploading mechanism

Wrap up

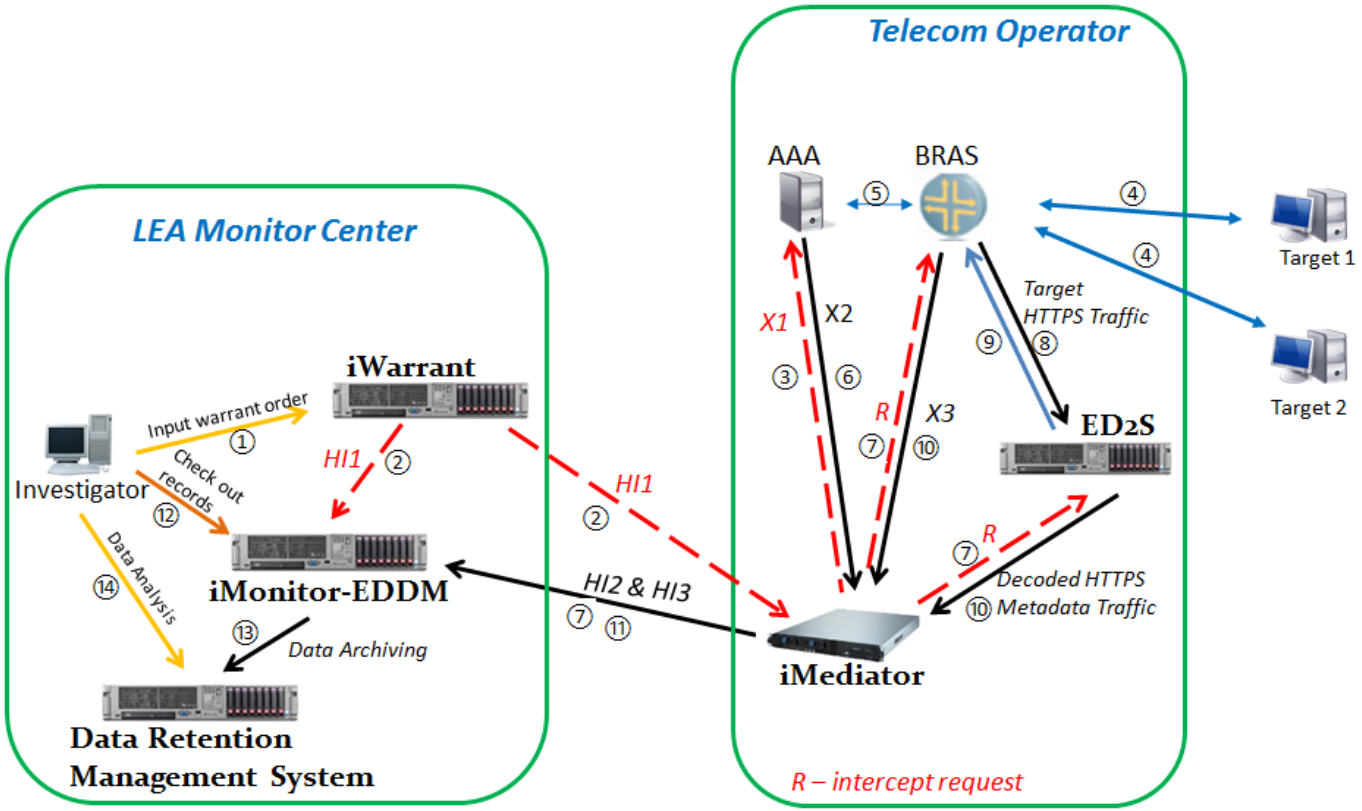
- The tactic lawful interception solution provided by Decision Group is proven to be the best, flexible and cost/performance network monitoring device for law enforcement authority.
- Customization service provided by Decision Group will be most trustful way for law enforcement authority to utilize this solution with standard operation procedure.
- Network Investigation Training for law enforcement authority by experienced field cyber policemen and scholars in Taiwan will be the best one for seamless lawful interception system building up solution.

Future Upgrade Plan

- All upgraded procedure will be compliant with ETSI standard
- The tactic Fixed network lawful Interception solution can be upgraded to permanent passive lawful interception platform
- To add an iMediator in BRAS inside POP Center of ISP
- The decoded traffic from DG system will move to iMediator for correlation with target user provision data
- All decoding and content reconstruction task moves to backend LEA monitor center

Lawful Interception on Fixed Network

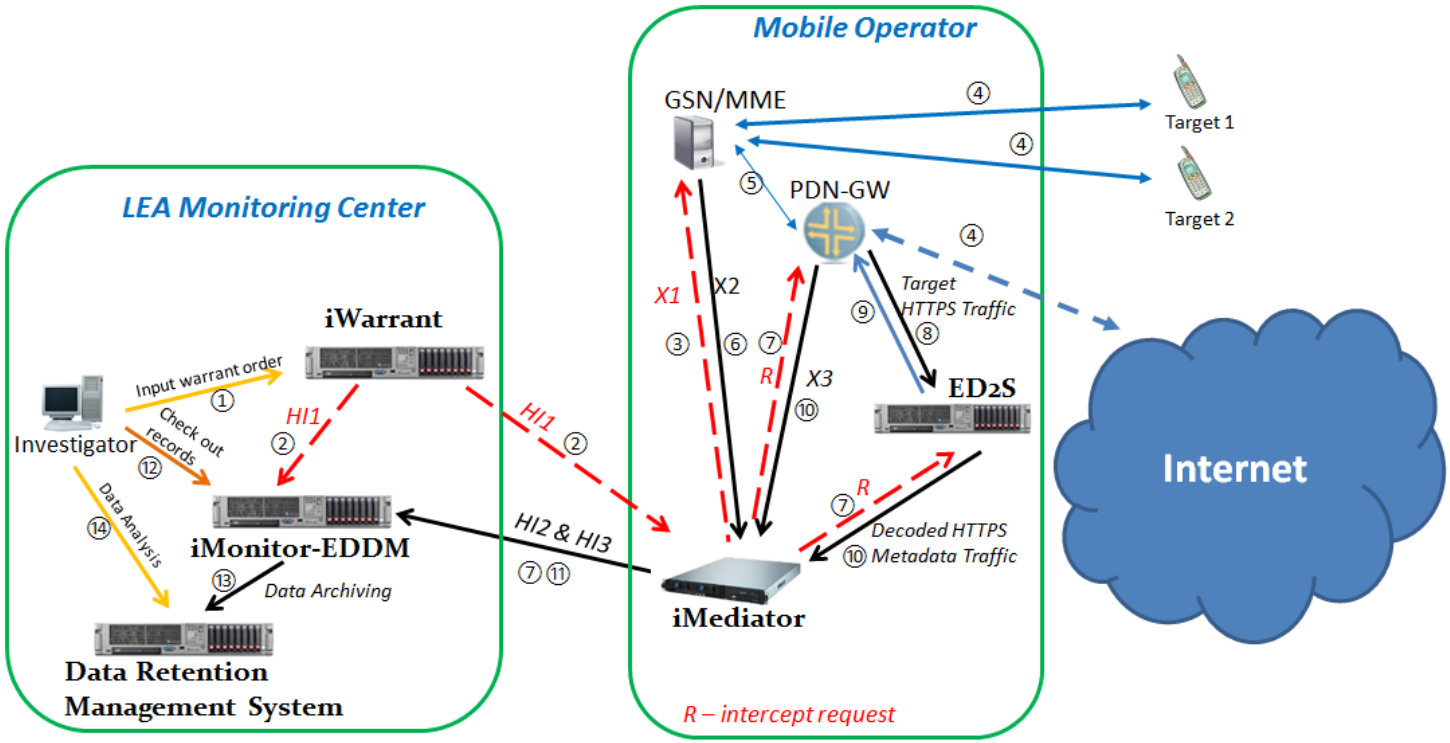
- *Investment protection*
- *No telco operator intervention*
- *For both fixed and mobile networks*



- By introducing iMediator, the solution can be upgraded into permanent lawful interception system on digital and voice data interception without intervention of Telco operator
- Entire procedure is compliant with ETSI standard
- It can be integrated with LI system for Fixed Network and protect current investment

Lawful Interception on Mobile Networks

- *Investment protection*
- *No telco operator intervention*
- *For both fixed and mobile networks*



- By introducing iMediator, the solution can be upgraded into permanent lawful interception system on digital and voice data interception without intervention of Telco operator
- Entire procedure is compliant with ETSI standard
- It can be integrated with LI system for mobile Network and protect current investment

Advantages from Decision Group

- **Full spectrum of solutions, training programs and services**
- **Highest integration with Telco equipments without impact on backhaul network traffic**
- **Excellence support on protocol decoding and content reconstruction**
  - 140+ protocols support
  - Regular update service
- **Self-developed turnkey solutions and modules**
- **Local Arabic technical support**
- **Investment protection**

Q&A

Proposal will be submitted after this review report is approved