

# iMonitor

## *Development of IP Technology and Lawful Interception on Internet Access*

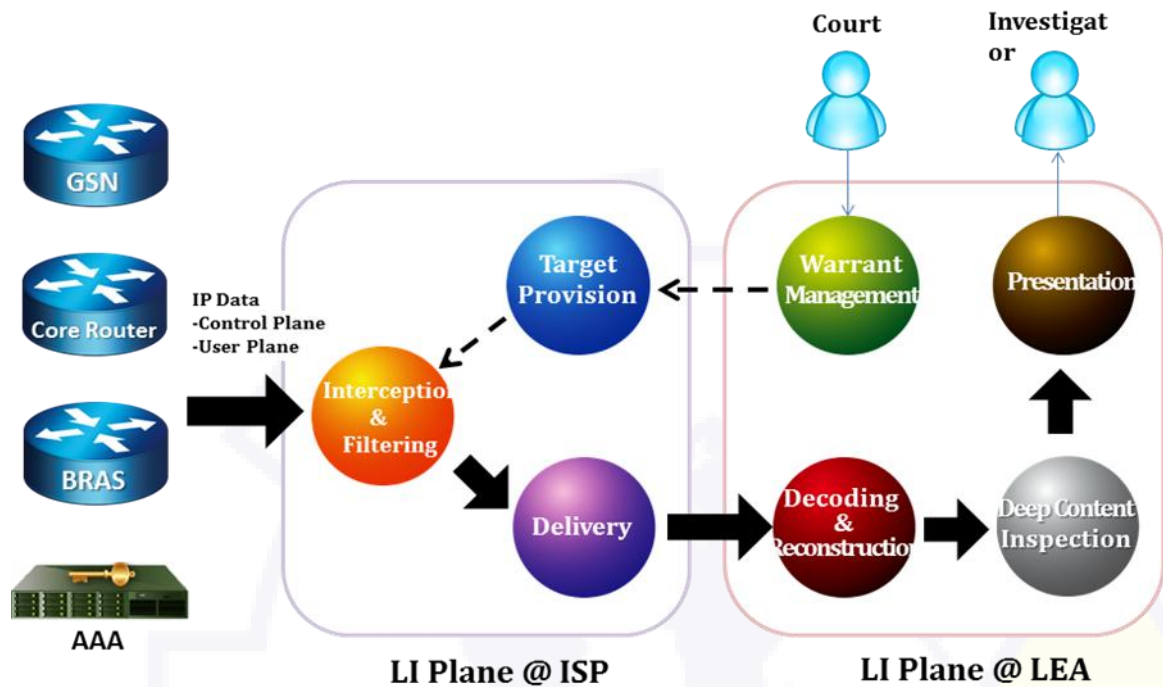
Legacy voice switch technology is always the core of electronic communication from the age of PSTN to mobile phone network nowadays. By fast progress with technology of IP network, it is a trend that most people communicate each other through application service platform (E-Mail · MSN or Whats App...etc) by Internet access, so do criminals.

It is absolutely necessary and mandate to conduct lawful interception (LI) operation on internet access service based on the justice causes of cyber crime investigation and home land security. Though there is difference between IP network and voice switch network in term of technology, legal liability of lawful interception operation on IP network is the same with that on voice switch network:

“Internet service provider should offer communication content and information of target to law enforcement agency”

To fulfill state LI mandate, it is obliged for all internet access service providers (ISP) to transmit data packets (communication content) and access log (information) of target subscribers to the remote monitoring facility of law enforcement agency (LEA). For such process, ETSI defines the handover interface for the data delivery from ISP to the law enforcement monitoring facility (shortly called LEMF). However, the crime investigation practice on IP data interception is beyond that, the investigator has to do

forensic jobs on the collected data, IP packets, and identify the meaningful clues from huge data is another big challenge. Without the appropriate solution, LI on IP packets can help little on crime investigation neither for homeland security.



### *Solution from Decision Group: iMonitor*

DG provides the monitoring center solution for law enforcement agency:

iMonitor, which is a centralized ETSI-compliant LEMF system with several advanced post-interception analysis to fulfill crime investigation process. The major features are as below:

#### **- Connect Multiple ISP(mediation device)**

iMonitoring system locates in LEA site as the LEMF defined by ETSI standard and is able to monitor several ISPs simultaneously. For each ISP, there is a correspondent HI

collection module. Adding one ISP into the monitoring list is to add one HI collection module with the proper configuration.

### **- Warrant Management**

For a crime inspection case, the investigator may apply the warrant for monitoring a set of targets. The target can be an ISP account or an IP address or a 3G MSISDN (phone number)...Warrant management system is to manage the life cycle of the warrants and execute the target provision and target removal by syncing the warrant information to mediation devices in ISPs. In the same time, it keeps each warrant have its independent working space: the investigator is constrained to access the intercepted data belonged to those targets in the specific warrant which is applied by himself.

### **-Intercepted data forensics: protocol decoding and reconstruction**

There are two types of collected data:

IRI: describes the session context information from ISP control plane for the specific targets.

CC: the IP packets intercepted from ISP user plane which are related to the specific targets.

Regarding to ETSI standard, the monitoring facility has to correlate the IRI and CC by targets. Unfortunately, only network forensics professionals can “understand” CC: to recognize the exact behaviors represented by those IP packets. What we expect is: if

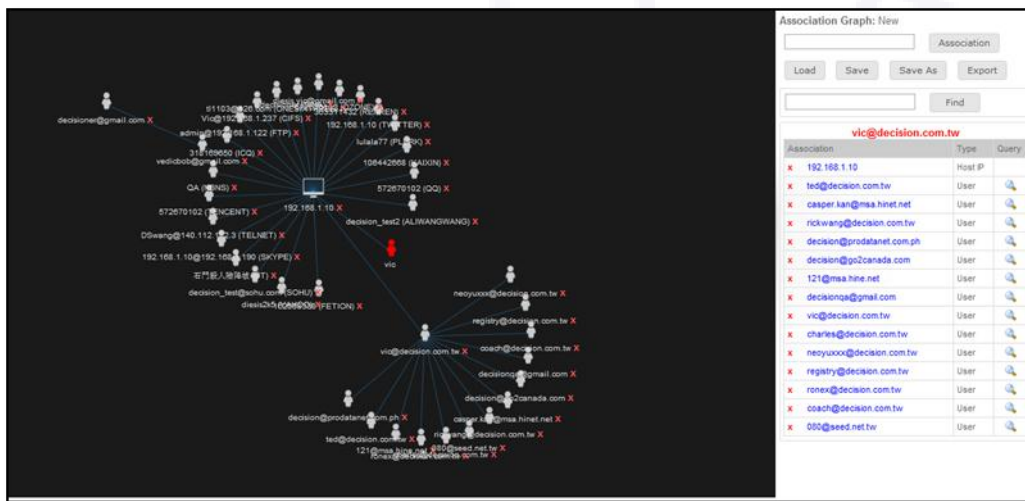
these packets are about MSN behaviors, show the text conversation instead of raw data. For this gap, the heart of iMonitor is protocol decoding and reconstruction engine: generating the human-readable content by different protocol from those IP packets. Moreover, iMonitor presents the content on web server so that it can easily serve many users through IP network with little learning cost

The image displays several overlapping screenshots from the iMonitor application, demonstrating its capabilities in network traffic analysis and content reconstruction. Red arrows point to specific features:

- Top Screenshot:** A table of network traffic with columns for No., Date-Time, Account, and HOST. A red arrow points to a row with the account 'frankie' and HOST 'ST701'.
- Web Page Reconstruction:** A screenshot of 'THE STRAITS TIMES' news article titled 'Volcanoes erupts near Tokyo'. A red box highlights the page content, with a red arrow pointing to the text 'HTTP Web Page content can be reconstructed'.
- Whois Function:** A screenshot of the Whois function interface, with a red arrow pointing to the text 'Whois function provides you the actual URL Link IP Address'.
- Chat Log:** A screenshot of a chat conversation with columns for No., Date-Time, User Handle, and Message. A red arrow points to a message.
- Friend List:** A screenshot of a friend list for the account 'shmiily.d0613@msa.hinet.net', showing columns for No., Account, and Nickname.

## -Deep Content Inspection

Although everything is decoded or reconstructed, the most challengeable thing is to find the crime-related clues in huge data. iMonitor provides the most powerful tool to search data by user-defined criteria. Moreover, the visual link analysis is provided to identify the communication relation in cyber world and even trace to the physical identity such as 3G Phone number or ISP account.



No.	Date-Time	Account	Sender	Receiver	CC	Subject	Size	Similar Search
1.	2008-07-02	FRANKIE-10.34.19	PC	decision@ed-system.s...	decision@ed-system.s...	support@ed...	94.90K	MY Email
2.	2008-07-02	FRANKIE-10.34.19	PC	decision@ed-system.s...	support@ed-system.sg	support@ed-system.sg	98.74K	Captured
3.	2008-07-02	FRANKIE-10.34.17	PC	decision@ed-system.s...	decision@ed-system.s...	support@ed...	94.91K	MY Email
4.	2008-07-02	FRANKIE-10.34.17	PC	decision@ed-system.s...	decision@ed-system.s...	support@ed...	79.37K	New York
5.	2008-07-02	FRANKIE-10.28.43	PC	wedetective2@hotmail...	support@ed-system.sg	support@ed-system.sg	14.50K	Africa
6.	2008-07-02	FRANKIE-10.28.43	PC	frankie decision@gma...	decision@ed-system.s...	decision@ed-system.s...	7.24K	Bush
7.	2008-07-02	FRANKIE-10.28.43	PC	fransynmy@yahoo.com	decision@ed-system.s...	decision@ed-system.s...	122.06K	Prospectors strike gold at I...
8.	2008-10-12	20:46:53	frankie	frankie@decision.com...	frankie@decision.com...	decision@e...	114.35K	COLOMBEY-LES-DEUX-EGUISES...
9.	2008-10-12	20:46:53	frankie	frankie@decision.com...	decision@ed-system.s...	support@ed...	158.22K	Europe - Econ Crsis...
10.	2008-10-12	20:46:53	frankie	frankie@decision.com...	frankie@decision.com...	decision@e...	114.37K	COLOMBEY-LES-DEUX-EGUISES...
11.	2008-10-12	20:46:53	frankie	frankie@decision.com...	decision@ed-system.s...	support@ed...	158.18K	Europe - Econ Crsis...
12.	2008-10-10	FRANKIE-nimsasi@inforsecure		mark@infor...	mark@infor...	mark@infor...	91.44K	RE: PO CoreIntercept Lottery...

Total 12 Total Page 1 Current Page 1

## Product Specification of iMonitor

- **Warrant Management**

- Target Type

- ISP account/RADIUS
    - CPE MAC address/RADIUS
    - IP address
    - MSISDN,
    - IMEI

- Warrant/Life Cycle Management

- Query for the warrant context
    - Set start-time and end-time for the warrant /target

- Warrant working context management

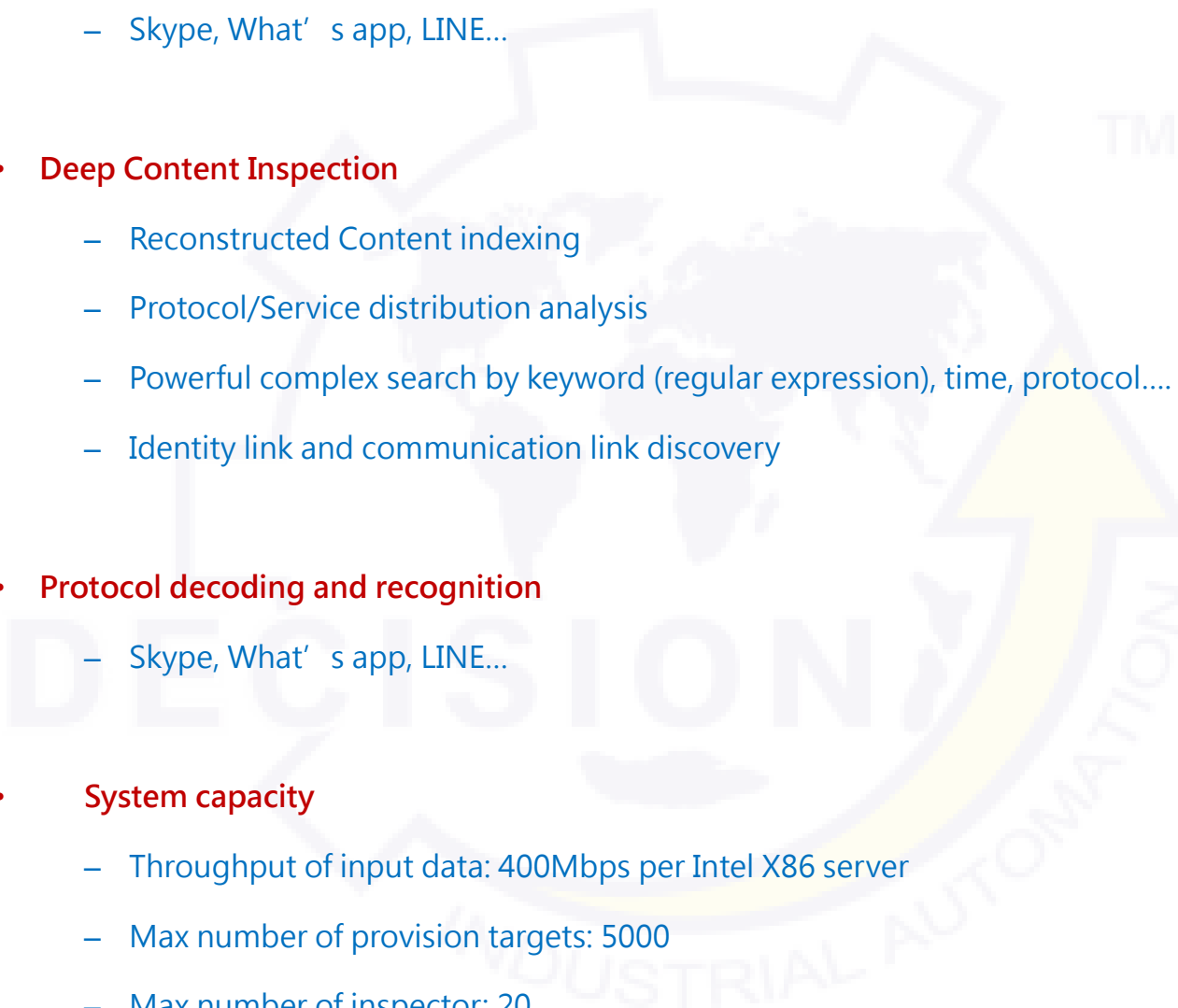
- Each inspector(officer) has an independent working space for the warrant she/he applies

- **LEMF interface**

- ETSI TS 102 232-1/3/5
  - DG proprietary interface

- **Protocol decoding and reconstruction**

- Instant Message: MSN IM, Yahoo IM, Gtalk, XMPP, Facebook IM...

- Mail: POP3, SMTP, Hotmail, Gmail, Windows Live, Sina...
  - VoIP: SIP, H.323, RTP, Codec(G.711/G.729)
  - Social Network: Facebook, Plurk, Twitter, Youtube...
  - Other common protocols: HTTP, Telnet, FTP, ....
  - **Protocol decoding and recognition**
    - Skype, What' s app, LINE...
  - **Deep Content Inspection**
    - Reconstructed Content indexing
    - Protocol/Service distribution analysis
    - Powerful complex search by keyword (regular expression), time, protocol....
    - Identity link and communication link discovery
  - **Protocol decoding and recognition**
    - Skype, What' s app, LINE...
  - **System capacity**
    - Throughput of input data: 400Mbps per Intel X86 server
    - Max number of provision targets: 5000
    - Max number of inspector: 20
    - High Availability
      - Active/Active: 1+1
- 

- Active/Stand by: N+1
- Basic hardware spec
  - HP DL380G: CPU 2.4GHz, 16GB DRAM, 300G SAS HDD



**Decision Group Inc.**

Address: 4/F No. 31, Alley 4, Lane 36, Sec.5,  
Ming-Shan East Road Taipei, Taiwan.

Phone: +886227665753

Fax: +886227665702

Sales Email: [decision@decision.com.tw](mailto:decision@decision.com.tw)

Global Website: [www.edecision4u.com](http://www.edecision4u.com)

Chinese/Traditional Website:  
[www.internet-recordor.com.tw](http://www.internet-recordor.com.tw)