Decision Group Inc.

Decision Group Inc.

2016

Contents

- Introduction and Company Brief

- Corporate Milestones

- Globalized Company

- Solution and Technology

- Solution Position in the Market

- Conclusion

Introduction

- Decision Group is a company providing powerful cyber security solutions to enterprises, government sector, law enforcement agencies, and telecom service providers.

- In worldwide Cyber Security market, DG is significant on his competence and uniqueness in functionality and efficiency.

- Now Decision Group provides full spectrum of product portfolio covering wired, wireless, decoding center, data management, SSL and VoIP security, training and development toolkit.

- Decision Group has 30 year experience in ICT industry since 1986, and now there are 2 business divisions: Network Forensic Business and Industry Automation

Company Brief

- **Decision Group was established in 1986 with 30-year experience in ICT industry.**

  ❖ **CEO: Casper Kan Chang　　張 侃**

  ❖ **Staff: 42 Formal and 12 Contracted employees**

  ❖ **Core Business: Software and Hardware R&D with Development and Manufacturing**

  ❖ **Strong R&D Capability :　40 professional engineers with 8 Ph D. & 12 Masters**

- **2015 Turnover : US$ 7.6M**

- **Market in 2016:**

  - Asia　　　42%　Europe　　　15%,

    America　　14%,

    Africa　　　29%
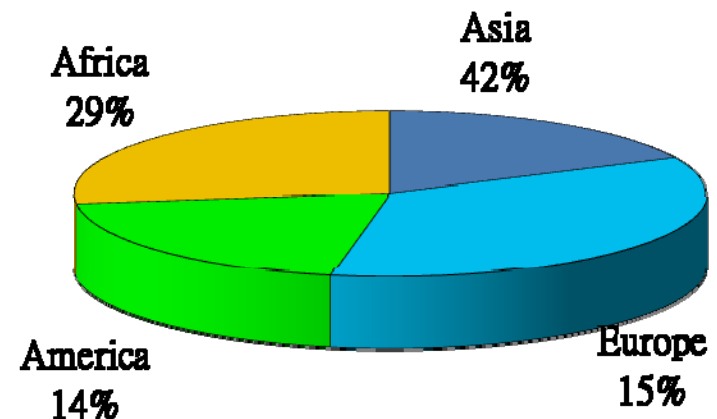
Management Team

- **Casper Chang**
  Chairman & CEO
  - Founder of Decision Group
  - Original Software Architect of DG Solutions
  - Owns several patented industry automation controllers
  - Designed first patented BIOS firmware of LAN card for Taiwan IT industry in 1984

- **Isabelle Huang**
  Chief Operation Officer
  - Joined Decision Group as COO from 2007
  - Started up an IT trading company
  - Managing Director in Poland office from 2003 to 2005
  - Managing Director & VP in China office from 1999 to 2003
  - International sales/marketing/management in Taiwan IT industry from 1981 to 1999

- **Ted Chao**
  Chief Marketing Officer
  - Representative in Middle East region in Institute for Information Industry
  - Business consultant in Boos Allen & Hamilton, Asia
  - Enterprise Business Director in Lucent Technology Taiwan
  - Enterprise Marketing Director in HP Taiwan
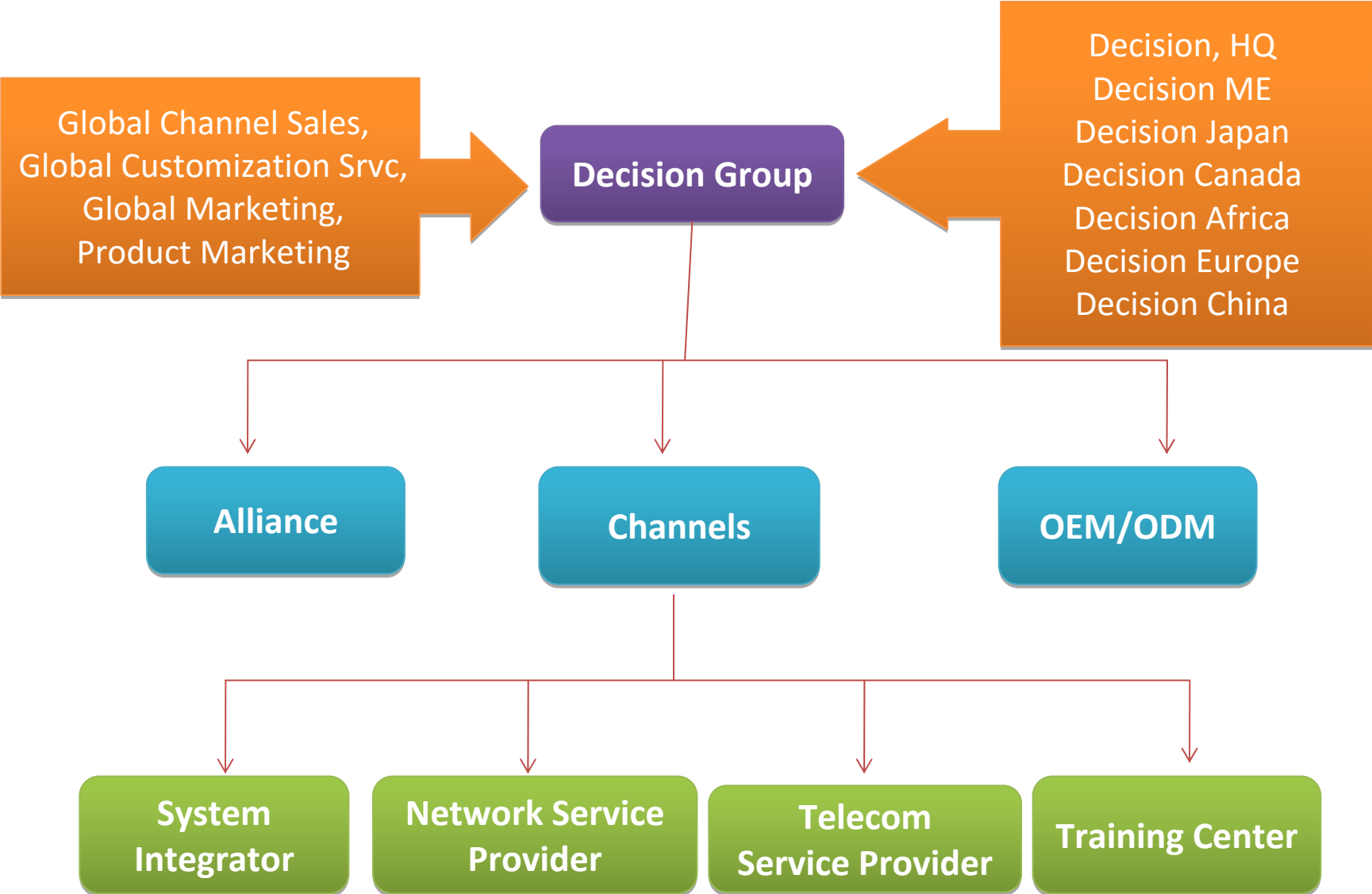 - Enterprise Product Marketing Director in Compaq Taiwan

- **William Chen**
  Chief Technology Officer
  - Senior manager of R&D Division Dept. of Alpha Network
  - R&D manager of IALink Inc. Co.,
  - R&D manager of Lineo
  - 8 years experiences of software engineers management
  - 10 years experiences of software development
  - 10 years experiences of software architecture designer

Corporate Milestones

Year	Milestones
2015	Announced Satellite Digital Signal Analysis System
2014	Announced location data surveillance in mobile internet access
2013	Announced mediation device with fixed and LTE networks for LI deployment
2012	Announced Central Management System with DRMS for 3 tier infrastructure on large scale of distributed network at national scale, and ED2S system
2011	Announced ETSI Compliant E-Detective/LI system with IMS for Telecom All IP Networks , and Enterprise Data Guard System with Database Transaction Auditing
2010	Announced Data Retention Management System, 10Gb E system support
2009	Announced VOIP decoding center in market
2007	Announced offline multiple protocol decoding center
2006	Announced 802.11 a/b/g/n multi-station forensic product (under patent) with capability of WEP/WPA Key breaking, HTTPS code breaking and positioning
2004	First announced HTTPS code breaking product in market
2002	First announced wireless network forensic product in Asia countries
2000	First announced wired network forensic product in Asia countries

Globalized Company

Global Channel Sales, Global Customization Srvc, Global Marketing, Product Marketing → **Decision Group** ← **Decision, HQ / Decision ME / Decision Japan / Decision Canada / Decision Africa / Decision Europe / Decision China**

Decision Group
- **Alliance**
- **Channels**
  - **System Integrator**
  - **Network Service Provider**
  - **Telecom Service Provider**
  - **Training Center**
- **OEM/ODM**

Network Forensics and Lawful Interception Total Solutions Provider

- E-Detective
- Wireless-Detective
- E-Detective Decoding Centre
- Enterprise Data Guard System
- E-Detective LEMF Solution Suite
- Centralized Management System
- Data Retention Management System
- HTTPS/SSL Interceptor
- Satellite Digital Signal Analysis System
- VoIP Detective
- FIT (Forensics Investigation Toolkit)
- NIT (Network Investigation Toolkit)
- Network Packet Forensic Analysis Training
- Cyber Crime Investigation Training
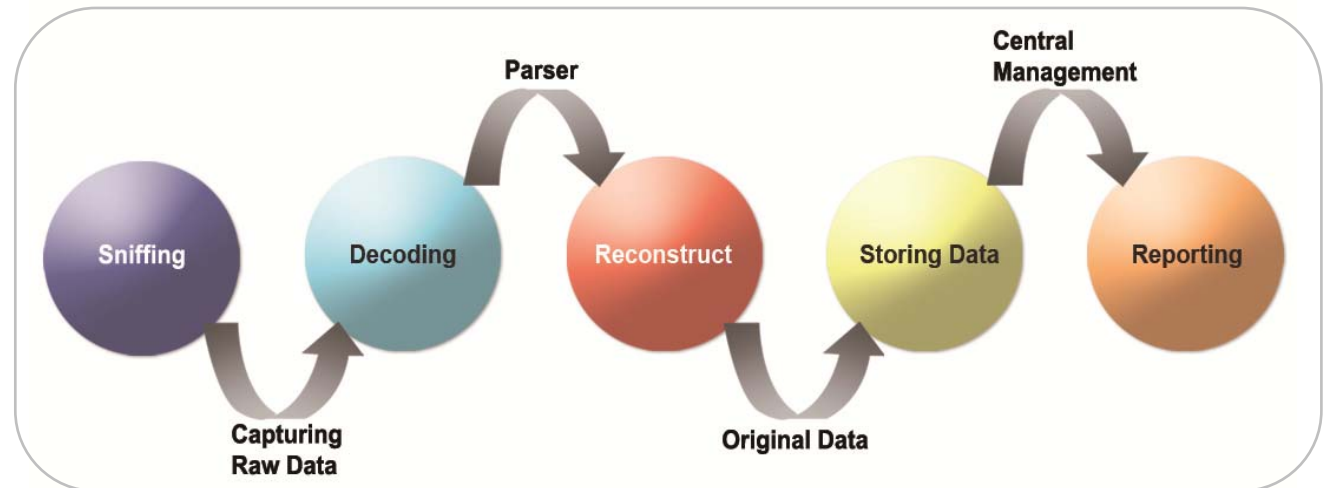- National Security Surveillance Training
- Lawful Interception Training

DECISION
INDUSTRIAL AUTOMATION

E-Detective

LAN Internet Monitoring & Forensics Analysis System

Best Solution for:

- **Auditing and Record Archiving for ISO 27001, SOX, HIPPA...etc.**
- **Internet Monitoring/Network Behavior Recording**
- **Tactic Forensics Analysis and Investigation for LEA**

Most Advanced Device for Data Leakage Protection, Lawful Interception and Network Forensic

Wireless-Detective

WLAN Analytics/Forensics/Legal Interception System

- Support Wireless LAN 802.11a/b/g/n Scanning Packet Capturing
- Automatically WEP Key Cracking (WPA Optional Module)
- Decode and Reconstruct WLAN packets
- Capture/Decode/Display are All-in-One
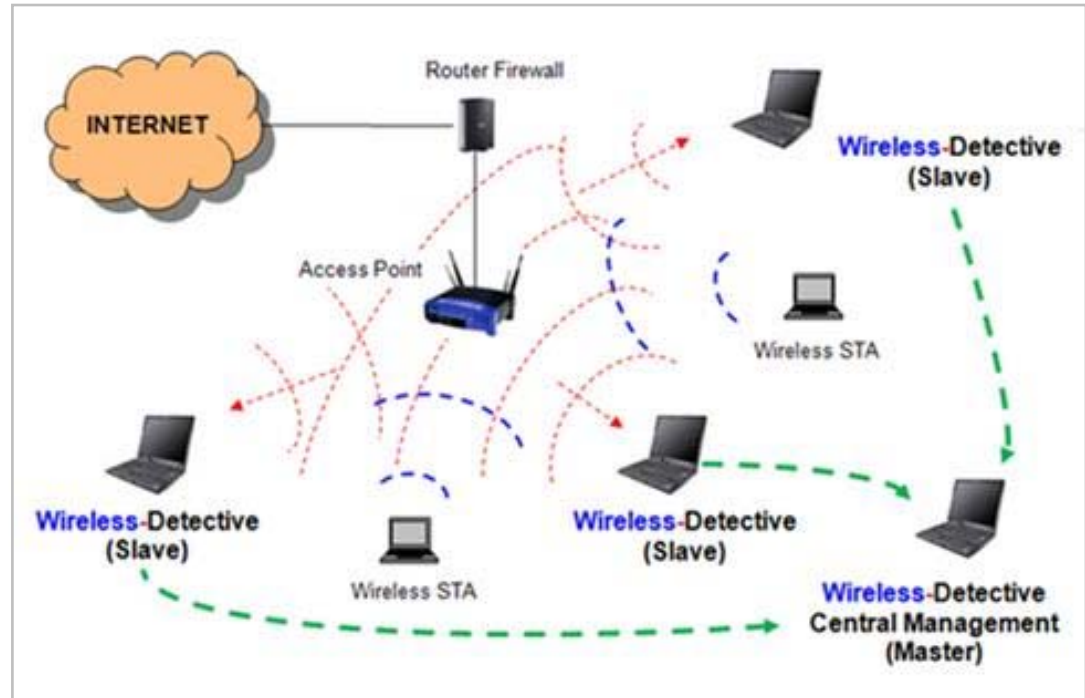
Important Tool for Lawful Enforcement Agencies such as Police, Military, Forensics, and Enterprise Auditing and Legal Department.

The Powerful Lightest Forensic Device in The World

E-Detective / Law Enforcement Management Solution Suite

- **Features:**
  - Full spectrum of LI solutions for both telco operator and LEA
  - As a lawful interception system for dealing with both circuit switch and packet switch telecom networks
  - Handling intercepted data with provision record from AAA or HSS based on LEA warrant order
  - For packet data networks, DG LI solutions can
    - Decoding all data packets associated with protocol based on session with both CDRs of network and application levels
    - Exporting metadata in standard XML or ASN.1 format
    - Compliance with ETSI TS 101 671, ETSI ES 201 671 and 3GPP TS 33.106
  - For circuit switch network, our LI solutions can covert SS7/ISUP/VoIP into CDR and voice files respectively
  - Customized project-based solutions from iMediator to iMonitor

- *iMediator*
- *iMonitor*
- *EDDM*
- *iMedia Gateway*
- *Data Retention Management System*
- *Centralized Management System*

High Performance Passive LI Platform compliance with ETSI Standard

Enterprise Data Guard System

- ❖ **DB Monitor on Transactions of MySQL, MS SQL Server and Oracle DB**
  - ▪ SQL Command and Action Record with DB Name, User Account of Network and DB, User IP, Date/Time Stamp
- ❖ **Internal Email Activity Monitor & Audit**
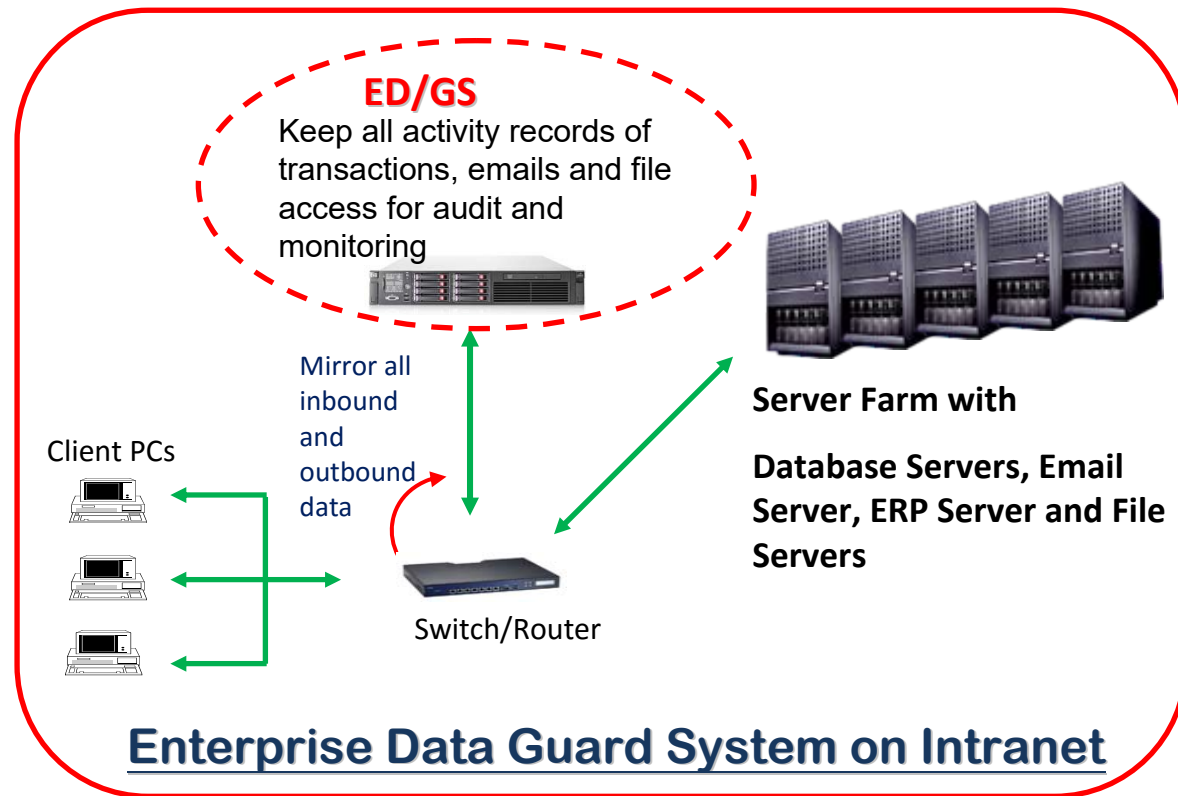 - ▪ Email Content with Sender, cc & bcc List, User IP, Date/Time Stamp and Attached Files
- ❖ **Access Record and Audit of File Server**
  - ▪ File Access Record with User Account, IP, File Server Name, Action, Date/Time Stamp
- ❖ **Centralized Skype Monitor Center**
- ❖ **Full Text Search and Cross-Check**
- ❖ **Online Warning Trigger by Designated Keywords**

ED/GS
Keep all activity records of transactions, emails and file access for audit and monitoring

Mirror all inbound and outbound data

Client PCs

Switch/Router

Server Farm with

Database Servers, Email Server, ERP Server and File Servers

Enterprise Data Guard System on Intranet

Complete Solution for Corporate Auditing and Data Leakage Protection

Data Retention Management System

- Data Retention Management System (DRMS) is designed for viewing Intercepted Data centrally from multiple frontend E-Detective, ED2S, NIT2/WD and iMonitor/EDDM Systems.

- Provides a User Friendly GUI, and easy to import and view the Contents especially for large amount of Intercepted Data.

- Capable to view multiple data Files at the same time.

- Works with E-Detective and ED2S systems by Automatic transport function via FTP, and allows reconstructed Data File in each frontend system to be stored in DRMS Server centrally.

- Search and Advance Search functions provided for data scoping and primary link analysis.

- Easy Management of reconstructed Data Files centrally with multiple E-Detective and ED2S systems.

- Integration with 3rd party data or text mining, link analysis system or Hadoop File System

Large Volume Data Manipulation and Centralized Data Processing with 3rd Party Analysis System

Centralized Management System

Deployment with:

- **Central Access Management for all Users on Intercepted Data with Different Authentication in Distributed Environment**
- **Remote System Management on Multiple ED, ED2S, ED/LEMF and NIT2 through Secured Connection**
- **Remote System and Data Management on Data Retention Management System through Secured Connection**
- **Separate Processes of Data Collection, Decoding, User Access, and Data Management in Order to Fulfill State Mandates**
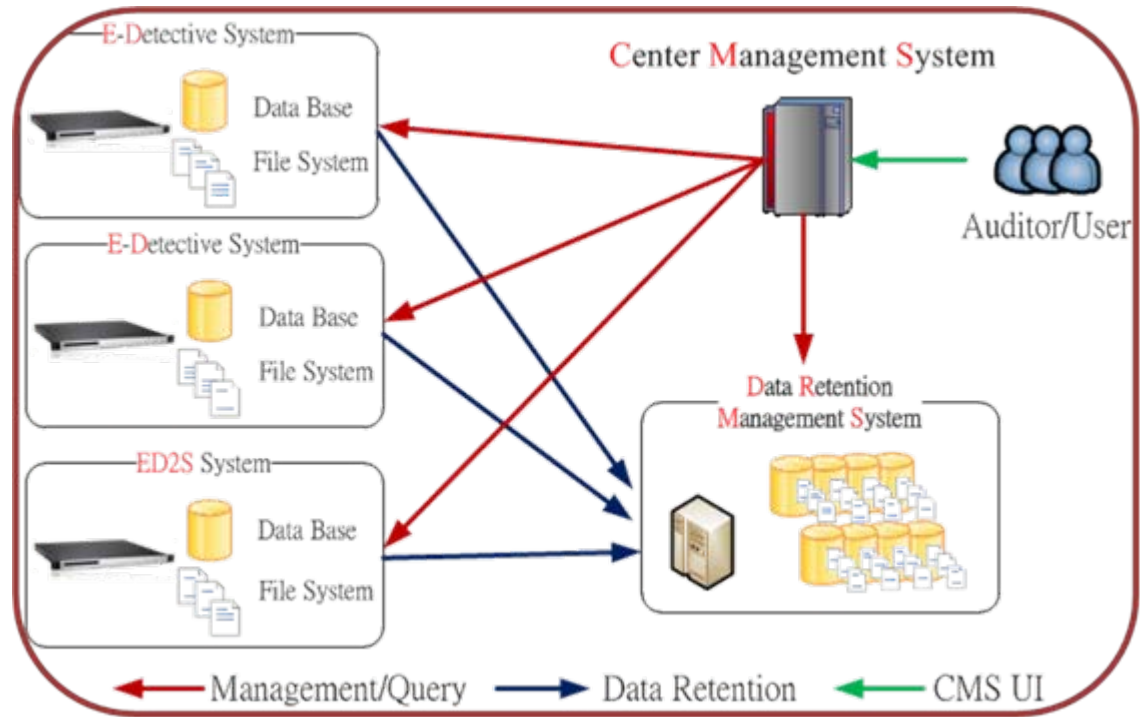
Suitable for Deployment in Network Service Providers, Global Enterprises, and Law Enforcement Authority
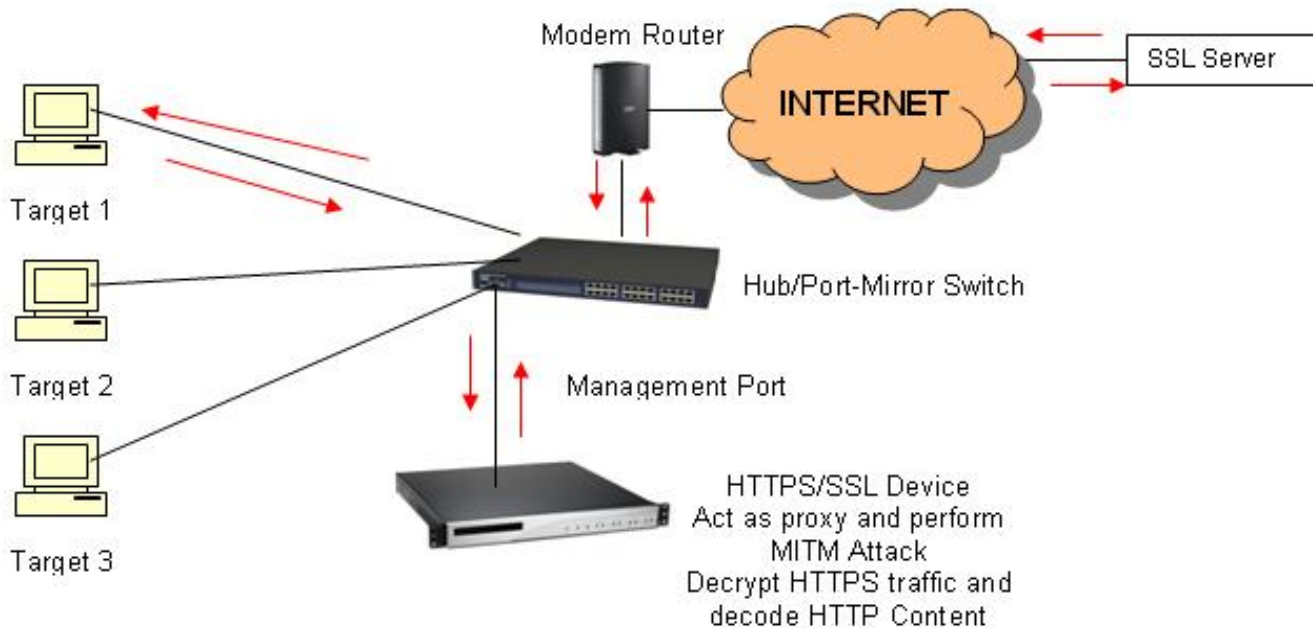
E-Detective Decoding Centre

❖ **Designed for Off-line Packet Reconstruction**

  ➢ **Protocol decoding engine with integration capability to other system**

❖ **Multi-Users and Case Base Management**

  ➢ **Administrator can create different project/case for different user/investigator to conduct Internet raw data parser and forensics analysis task on the system**

❖ **Various Content of Internet Applications Decoding**

  ➢ **Email (POP3, SMTP, IMAP), Webmail (Yahoo Mail, Gmail, Hotmail etc.) IM (Yahoo, MSN, ICQ, QQ, UT, IRC, Google Talk, Skype Voice Call Log), File Transfer (FTP, P2P), HTTP (Link, Content, Reconstruct, Upload/Download, Video Stream), Telnet, Online Games, VoIP, Webcam (Yahoo, MSN)…etc.**

❖ **EDDM is LI Version Product of EDDC**

Cutting-edge Offline Decoding Device

HTTPS/SSL Interceptor

- **Decrypting HTTPS/SSL Traffic**

- **Operation Modes**

  - **Transparency Proxy - Man in the Middle Attack**

  - **Forward Proxy**

  - **Passive Capture Mode**

- **Certificate Replacement by Customization (optional)**

HTTPS/SSL Network Forensic Device (MITM application)

Modem Router

SSL Server

INTERNET

Target 1

Target 2

Hub/Port-Mirror Switch

Management Port

Target 3

HTTPS/SSL Device
Act as proxy and perform
MITM Attack
Decrypt HTTPS traffic and
decode HTTP Content

**To view encrypted content,
a key is a needed**

The Powerful HTTPS/SSL Cracker for Mobile Network Interception

VoIP-Detective

User may opt to purchase the complete Appliance (Hardware + Software) or only purchase Software from us. User may use their own dedicated server for installing the software.

- Capable to intercept and capture (through Mirror Mode or Tap Deployment), decode and reconstruct VoIP RTP sessions.

- Supports voice calls of SIP.

- Supported CODECS: G.711-a law, G.711-u law, G.729, G.723 and ILBC.

- Capable to play back the reconstructed VoIP sessions.

The Appliance System for VoIP Monitoring System on Telecom Switch and IP-PBX

Network Investigation Toolkit Gen 2

What are the capabilities of NIT2?

- **Interception of Ethernet LAN traffic through mirror port (or by network tap).**
- **Interception of WLAN traffic (up to 4 different WLAN channels).**
- **Intercept ion of Ethernet LAN HTTPS/SSL traffic by MITM attack.**
- **Intercept ion of WLAN HTTPS/SSL traffic by MITM attack.**
- **Real-time raw data decoding and reconstruction.**
- **Offline raw data decoding and reconstruction.**
- **Forensics analysis and investigation.**

USB 3.5G/HSDPA Adapter

USB Hub

Lenovo ThinkPad X200

USB WIFI Adapters

Solution for:
Lawful Enforcement Agencies (Police Intelligence, Military Intelligence, National Security, Counter Terrorism, Cyber Security, Defense Ministry etc.

Combine ED, WD and EDDC into one portable system for field LEA agents

Satellite Digital Signal Analysis System

- **For generic digital signal analysis of satellite communication**

- **Present reconstructed content data of both unilateral download and upload links**

- **Provide signal analysis on both L2 and L3 levels**

- **Provide correlation analysis with both download and upload links**

- **Suitable for network forensic analysis on satellite digital communication**

Forensics Investigation Toolkit

Powerful Network Traffic Decoding and Reconstruction Tool

Best Solution for:

- Internet or Network Traffic Content Analysis (Network Administrator)

- Auditing of Internet or Network Traffics (Network Administrator)

- Network Forensics Analysis and Investigation (Government and LEA)

Forensics Investigation Toolkit (FIT) is a Windows based Application Software suitable for all group of users to analyze and forensically investigate on network traffic or the content of Internet/network raw data files by Wireshark tool.

* Working on the below platforms:

The Powerful Forensic Analysis Tool on Windows System

Network Packet Forensic Analysis Training

❖ **Introduction to Network Packet Forensic Analysis Training**

This 3-5 day course utilizes the knowledge of computer security concepts together with switched network topologies and gives students hands on practical exposure to critical knowledge base essential for network forensic investigations.

❖ **Courses include**

- ✓ Introduction to Cyber Crime Investigation Process
- ✓ Study on Major Network Protocols
- ✓ Operation and Administration of E-Detective, Data Retention Management System, VoIP and HTTPS/SSL interception
- ✓ Practical Case Study and Drills

Cyber Crime Investigation Training

❖ Introduction to Cyber Crime Investigation Training

The objective of this course is to provide in-depth cyber investigation skills and associated theory to those law enforcement staff. All participants will learn the planned material through lecture, seminar, discussion and practical training in order to better understand the nature of cyber crime, the legal procedure, and learn the lesson of real cases from experienced investigators and experts.

❖ Courses include

- ✓ Cyber Crime with VoIP and Telecom

- ✓ Cyber Crime with Internet Services

- ✓ Legal Processes with Cyber Crime Investigation

- ✓ Methodology of Data Analysis for Cyber Crime Investigation

- ✓ Weakness of Common IT Systems

- ✓ Workshop on Drills

Co-work with National Taiwan Central Police University

Lawful Interception Training

Introduction to Lawful Interception

In order to keep up with fast-changing lawful interception technology on digital networks, we deliver the most updated content of LI framework, global standards, Decision Group LI solution suite and deployment methodology to LEA staffs, SI engineers, project managers and technical consultants.

Topic Includes

- ✓ Framework of Lawful Intercept
- ✓ ETSI and CALEA standard
- ✓ Deployment in different telecom networks
- ✓ Decision Group Lawful Intercept Solution Suite
- ✓ Data Analysis and Evidence Admissibility
- ✓ Case Study

National Security Surveillance Training

❖ Introduction to National Security Surveillance Training

Social riot is a common phenomenon in every country in the world. By advanced communication technology, fast spread of social uprising may cause a serious national security issue impacting on social and economic development.

In this course, we will introduce common nature of social uprising, how to conduct social sentinel surveillance, data analysis with practical case study.

❖ Topic include

- ✓ **National Security vs National Development**

- ✓ **Rumor and its Nature**

- ✓ **Social Sentinel vs Target Surveillance**

- ✓ **Methodology of Full Scale of Network Surveillance at National Level**

- ✓ **Deployment of Network Surveillance**

- ✓ **Case Study on Different Countries**

Restricted Participants

What We Provide

❖ **Solid Consulting and Delivery Services:**

- Clear objectives
- Appropriate surveillance systems
- Vulnerability assessment
- Deployment plan
- Legal procedure
- Data analysis/text mining

❖ **Extensive Training Programs:**

- Train-the-trainer
- Law enforcement officials and prosecutors
- Administrators

❖ **Future Development Plan:**

- Technology update and upgrade
- Technical skill shift
- Integration with backend warrant and lawful interception data analysis system

More Than 180+ Internet Service Decoder

Generic E-Mail	POP3, IMAP, SMTP
Webmail	GMail, Yahoo, … more than 18 webmails
Instant Message	Hangout, ICQ, … more than 6 IMs
Web Page	Web Link, Content and Request
Web FTP	Upload/Download
Web Video	YouTube, Vimeo …
File Transfer	FTP, P2P, … more than 23 services
Telnet	Animated playback available
Asia On-Line Game	More than 54 games
VoIP	SIP/RTP (G.711, G.723, G.729, iLBC)
Social Network Service	Facebook, Twitter…
Mobile Online Applications	APP & Web Services on iPhone, Android …
Database	Oracle, MS SQLServer, MySQL…

ORACLE iPhone

With multi-facets of functionality, DG Solution can be:

Enterprises & Governments
- Data Leakage Protection
- IT Auditing
- Employee Behavior Management
- Data Retention and Recovery

Internet Service Providers
- Network Flow Traffic Management
- Subscriber Behavior Management
- Quality of Service

LEA
- Lawful Interception Platform
- Tactical Server

Uniqueness of DG Solutions

Compared to our competitors', DG solutions have the greater advantages below:

- 140+ protocols and services decoding support

- Intercept on mobile online services of mobile devices (BYOD)

- VoIP support with versatile of CODEC engine

- HTTPS/SSL decryption support

- Wired and wireless modules available

- Highest throughput with 1.2Gbps

- On-line real-time decoding and content reconstruction

- Flexible implementation with cluster, single or multi-tiers, centralized or distributed, and disaster recovery configurations as well as with SAN, NAS or iSCSI external storages

- Easily integration with report system, data warehouse, BI and Hadoop File System from 3rd party

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

Protect your Information,
Secure your Business
Q & A