

# **E** DETECTIVE<sup>®</sup>



## **E - Detective** Internet Content Monitoring and Forensics Analysis Stream

Email



Chat



Web



FTP



P2P



TELNET



Webcam Video



Video Stream



Online Game



VOIP

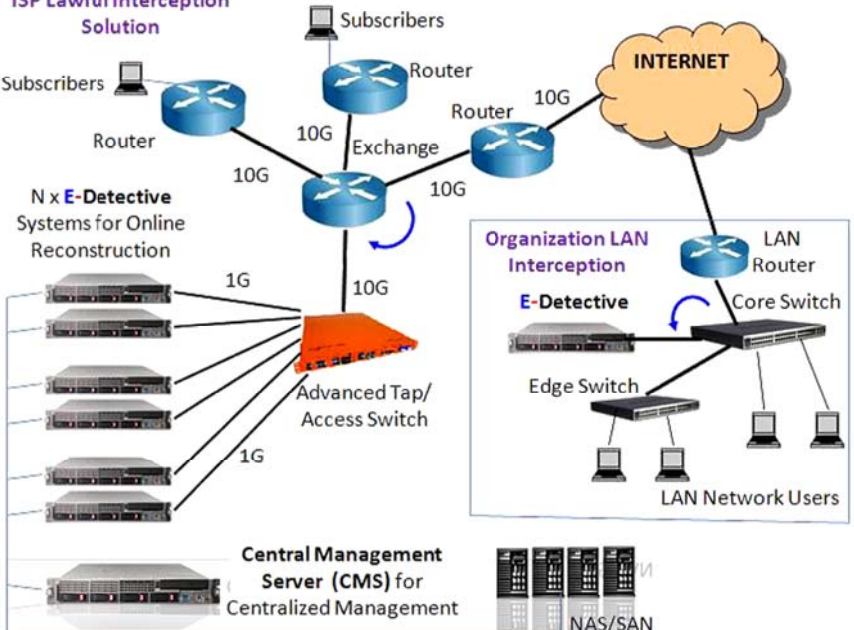


Internet content monitoring and auditing are important tasks for many organizations including small medium business, enterprises, finance services industry, Government agencies, forensics and intelligence agencies for different purposes. The reconstructed and archived Internet data can be used for legal evidence in case of any dispute. Government and intelligence agencies use such technology for protecting and defending the national security.

## E-Detective Implementation Diagram

### Total Throughput Statistical Report

Service Category	Daily Traffic			Weekly Traffic			Total Traffic			
	Quantity	Throughput	Report	Quantity	Throughput	Report	Quantity	Throughput	Report	
<b>Summary</b>	57,851	10,122,211 KB	MA	141,595	83,568,479 KB	MA	141,595	288,199,307 KB	MA	
<b>EMAIL</b>	10 POP3	1,020	775,356 KB	MA	2,434	14,092,089 KB	MA	2,434	22,295,304 KB	MA
<b>CHAT</b>	10 SKYPE	6	87,792 KB	MA	14	1,236,481 KB	MA	14	1,961,084 KB	MA
<b>FILE TRANSFER</b>	10 FTP	182	3,962,282 KB	MA	1,454	11,933,678 KB	MA	1,454	113,716,678 KB	MA
<b>ONLINE GAME</b>	10 HTTP Link	22,695	18 KB	MA	55,532	404 KB	MA	55,532	582 KB	MA
<b>HTTP</b>	10 HTTP Content	33,147	878,601 KB	MA	64,202	10,861,888 KB	MA	64,202	26,368,179 KB	MA



## Internet Protocols Reconstruction (sample screenshots)

### Email - Webmail

No.	Date/Time	Sender	Receiver	CC	Subject	Type	Search
1	2008-12-10 08:25:06	admin@xxx.com	admin@xxx.com		xxx	Text	Search
2	2008-12-10 08:25:06	admin@xxx.com	admin@xxx.com		xxx	Text	Search

### IM - Chat

No.	Date/Time	Account	User Name	Participants	Conversation	Count	Search
1	2008-12-10 08:11:11	admin@xxx.com	admin@xxx.com	admin@xxx.com	xxx	1	Search
2	2008-12-10 08:11:11	admin@xxx.com	admin@xxx.com	admin@xxx.com	xxx	1	Search

### HTTP (Link, Content, Reconstruct, Upload / Download, Video Stream)

No.	Date/Time	Account	Content	Search
481	2008-12-10 08:29:37	admin@xxx.com	xxx	Search
482	2008-12-10 08:29:37	admin@xxx.com	xxx	Search

## Administrative and Management (sample screenshots)

### Search - Keyword, Condition, Association

Date/Time	Category	Description	Functions	Related Account
2008-12-09 11:53:08	Upload	Upload: Backup JPG	Association	admin@xxx.com
2008-12-09 11:53:08	Upload	Upload: E-Public_UploadManual...	Association	admin@xxx.com

### Alert - Notification

No.	Date/Time	Alert Name	Alert	Status
1	2008-12-10 08:01:01	Alert Name	Alert	Alert
2	2008-12-10 08:01:01	Alert Name	Alert	Alert

### Backup - Archive

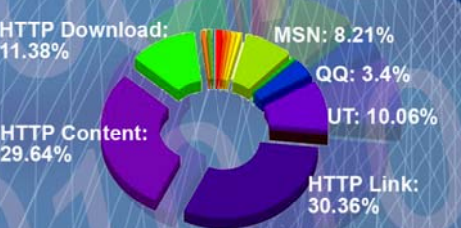
Backup Categories

Categories: POP3, WEBMAIL, SKYPE, GOOGLETALK, GAME, HTTP/LINK, VIDEO STREAM, SMTP, WEBMAIL/S, YAHOO, SKYPE, POP, HTTP/LINK, VIDEO STREAM, TELNET

### Online Userlist Report

No.	IP	Account	Last Connection Time	Group
1	192.168.1.179	WORKGROUP	2008-12-10 08:01:01	GROUP1
2	192.168.1.179	WORKGROUP	2008-12-10 08:01:01	GROUP1

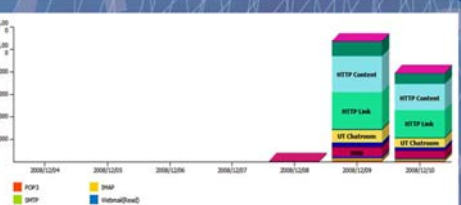
### Network Service Usage Report



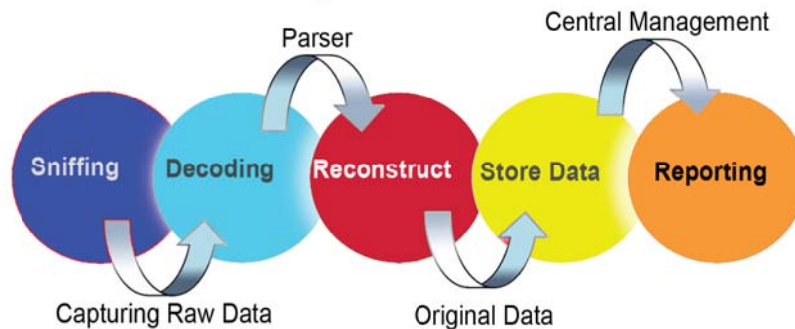
### Top Websites

Rank	Web Server URL	Count	User
1	plala.net	7,301	TOP N
2	log2002.webmail.hist.net	1,410	TOP N
3	small.chinese.com.tw	1,365	TOP N

### Network Service Weekly Report



## E-Detective System Architectural Design & Flow



One of the MOST COMPLETE “Content Reconstruction” system in the world!





## Specifications and Features

<b>Supporting Throughput/Load</b>	Up to 600 Mbps
<b>Supporting Corporation Size</b>	Very scalable, > 6000 online users
<b>Appliance Based</b>	Yes
<b>Deployment</b>	Mirror Mode, Bridge Mode, Sniffer Mode, Double Layer Architecture
<b>Services/ Protocols</b>	<p>Email POP3, SMTP, IMAP</p> <p>Webmail Yahoo (Standard and Beta versions), Gmail (Newer and Older versions), Windows Live Hotmail, Hinet, PCHome, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com</p> <p>Instant Messenger/ Chat Yahoo, Windows Live Messenger (MSN), ICQ, AOL, QQ, UT Chat Room, Google Talk, IRC, Skype VOIP Log - includes File Transfer through IM in some supported protocols</p> <p>HTTP HTTP Link (URL), HTTP Content, HTTP Reconstruct, HTTP Upload/Download, Video Stream, HTTP Request, <a href="#">Social Network Service (Facebook, Twitter, Plurk)</a></p> <p>FTP FTP Upload/Download</p> <p>P2P P2P Details Log - BitTorrent, eMule/eDonkey etc.</p> <p>Online Games 80++ Online Games</p> <p>Telnet/BBS With playback</p> <p>VOIP Yahoo Messenger VOIP</p> <p>Webcame Video MSN Messenger, Yahoo Messenger Webcam</p>
<b>Management</b>	<p>System Access HTTPs Remote Monitoring</p> <p>Group/User Yes</p> <p>Data Backup Yes, Restore Server, NAS/S AN based FTP server etc.</p> <p>Web Browser Access Yes (using IE, Mozilla etc.)</p> <p>Data Mining and Search Yes (Search by Parameters, Search by Key Words), Similar Search Function, User Account Relationship tracing</p> <p>Alert/Notification Yes. Alert/Notification by parameters, by Key Words</p> <p>Throughput Alert Yes</p> <p>Station Management Yes ( NetBIOS, Active Directory info)</p> <p>Storage Management Yes</p> <p>Upgrade Web based Upgrade</p>
<b>Reporting</b>	<p>Reports Yes, Comprehensive reporting. Total throughput statistical report with top-down view. Per user reporting with top-down view.</p> <p>Schedule Reporting Yes, provide daily log report in Excel format</p>

# Who benefits from E-Detective® System?

WHO	Human Resources Case Developer Computer Forensics Examiners Banking and Financial Institution Prosecutors	Fraud Examiners White Collar Crime Units Gang Units Homeland Security Legal Units	Educational Institution Enterprises Government Corporation
WHAT	Source Code Employee Information M&A Plans Business Plans Patient Information	Financial Statement Competitive Information Technical Document Intellectual Property Databases	Students' Records R&D Design P&L Report Customer Records
WHERE	Benefits Providers Chart Board Business Partners	Blog Customers Spyware Site	Competitors Terrorist
HOW	Email and Webmail Web - HTTP Instant Messaging / Chat	File Transfer - FTP, P2P HTTP Upload/Download	Online Games Telnet

## E-Detective® Models

Model	Photo	Online IP	HDD Size	DVD/CD ROM	External Storage
ED-FX06N	 (Embedded)	10-49	250G	N/A	Support
ED-FX30N	 (1U Server)	50-200	320G	N/A	Support
ED-FX100	 (1U Server)	201-1000	customizable	YES	Support
ED-FX120	 (2U Server)	above 1000	584G-1T customizable	YES	Support

Compliance Solution for Sarbanes-Oxley Act (SOX), Health Insurance Portability and Availability Act (HIPAA), Electronic Discovery (E-Discovery), Gramm-Leach-Bliley Act (GLBA), Securities and Exchange Commission (SEC), National Association Of Securities Dealers (NASD) and others - many other internal corporate policies.

Note : We accept customization request for special project design. We welcome OEM and ODM partners, Distributors and Resellers across the Globe.

Distributor / Partner :



### DECISION GROUP

URL : [www.decision.com.tw](http://www.decision.com.tw)  
[www.edecision4u.com](http://www.edecision4u.com)

Address : 4/F No.31, Alley 4, Lane 36, Sec. 5,  
Ming-Sheng East Rd, Taipei Taiwan ROC.

Pone : +886 2 27665753 Fax : +886 2 27665702

Email : [decision@decision.com.tw](mailto:decision@decision.com.tw)  
[decision@ms1.hinet.net](mailto:decision@ms1.hinet.net)