

E DETECTIVE®



E - Detective Internet Content Monitoring and Forensics Analysis

Stream

Email



Chat



Web



FTP



P2P



TELNET



Webcam Video



Video Stream



Online Game



VOIP



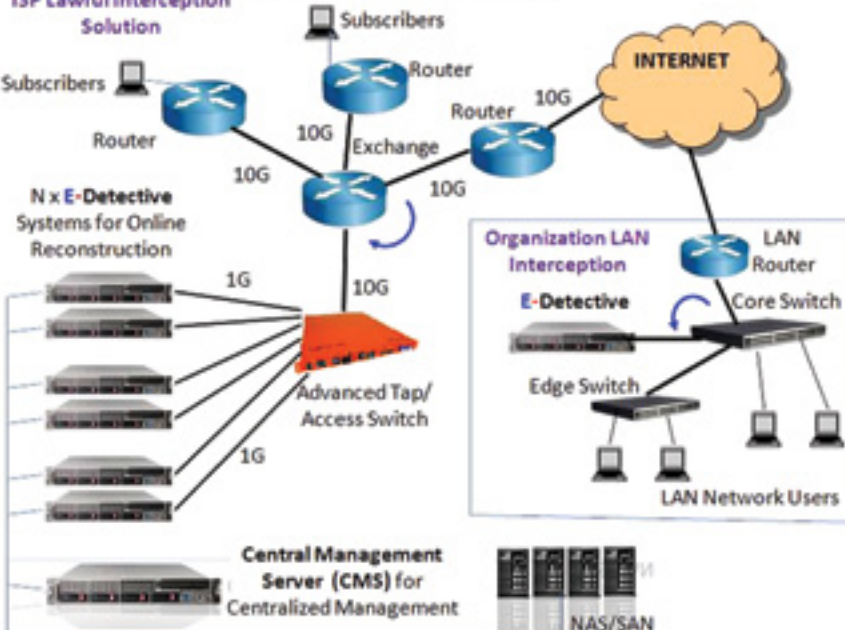
Internet content monitoring and auditing are important tasks for many organizations including small medium business, enterprises, finance services industry, Government agencies, forensics and intelligence agencies for different purposes. The reconstructed and archived Internet data can be used for legal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

E-Detective Implementation Diagram

ISP Lawful Interception Solution

Total Throughput Statistical Report

| Service Category | Quantity | Throughput | Repeat Quantity | Throughput | Repeat Quantity | Throughput |
|------------------|--------------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Summary | 17,891,162,271,442 | 1,401,288,488,474,442 | 1,401,288,488,474,442 | 1,401,288,488,474,442 | 1,401,288,488,474,442 | 1,401,288,488,474,442 |
| EMAIL | 1,000 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| IM | 400 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| WWW | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| FTP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| TELNET | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SSH | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SMTP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| POP3 | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| IMAP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| LDAP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SNMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| ICMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| IGMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| OSPF | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| BGP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| HTTP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| HTTPS | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SSH | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| FTP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| TELNET | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SMTP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| POP3 | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| IMAP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| LDAP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| SNMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| ICMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| IGMP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| OSPF | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |
| BGP | 100 | 175,280,442 | 2,444 | 1,401,288,474,442 | 2,444 | 1,401,288,474,442 |



Internet Protocols Reconstruction (sample screenshots)

Email - Webmail

| No. | Date/Time | Sender | Receiver | IP | Subject | Size | Attachment |
|-----|---------------------|-------------------|---------------------|-------------|------------|------|------------|
| 1 | 2008-10-10 10:10:10 | sender@domain.com | receiver@domain.com | 192.168.1.1 | Test Email | 1024 | |
| 2 | 2008-10-10 10:10:10 | sender@domain.com | receiver@domain.com | 192.168.1.1 | Test Email | 1024 | |

IM - Chat

| No. | Date/Time | Sender | Receiver | IP | Content | Size |
|-----|---------------------|-------------------|---------------------|-------------|-----------|------|
| 1 | 2008-10-10 10:10:10 | sender@domain.com | receiver@domain.com | 192.168.1.1 | Test Chat | 1024 |
| 2 | 2008-10-10 10:10:10 | sender@domain.com | receiver@domain.com | 192.168.1.1 | Test Chat | 1024 |

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

| No. | Date/Time | Method | URL | IP | Content | Size |
|-----|---------------------|--------|------------------------|-------------|-----------------|------|
| 1 | 2008-10-10 10:10:10 | GET | http://www.example.com | 192.168.1.1 | HTTP/1.1 200 OK | 1024 |
| 2 | 2008-10-10 10:10:10 | POST | http://www.example.com | 192.168.1.1 | HTTP/1.1 200 OK | 1024 |

Administrative and Management (sample screenshots)

Search - Keyword, Condition, Association

| No. | Date/Time | Category | Description | IP Address | Related System |
|-----|---------------------|----------|-----------------|-------------|----------------|
| 1 | 2008-10-10 10:10:10 | Search | Keyword: test | 192.168.1.1 | System A |
| 2 | 2008-10-10 10:10:10 | Search | Condition: test | 192.168.1.1 | System A |

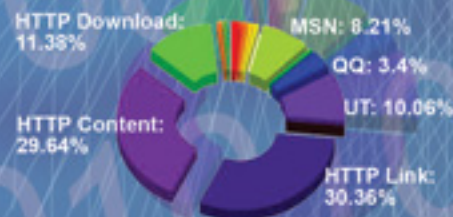
Alert - Notification

| No. | Date/Time | Alert Name | IP Address | Notification |
|-----|---------------------|------------|-------------|----------------|
| 1 | 2008-10-10 10:10:10 | Alert 1 | 192.168.1.1 | Notification 1 |
| 2 | 2008-10-10 10:10:10 | Alert 2 | 192.168.1.1 | Notification 2 |

Backup - Archive

| No. | Date/Time | Backup Name | IP Address | Archive |
|-----|---------------------|-------------|-------------|-----------|
| 1 | 2008-10-10 10:10:10 | Backup 1 | 192.168.1.1 | Archive 1 |
| 2 | 2008-10-10 10:10:10 | Backup 2 | 192.168.1.1 | Archive 2 |

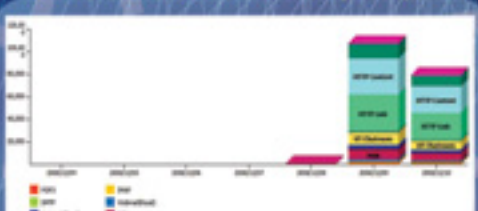
Network Service Usage Report



Online Userlist Report

| No. | Date/Time | IP Address | User Name | System |
|-----|---------------------|-------------|-----------|----------|
| 1 | 2008-10-10 10:10:10 | 192.168.1.1 | User 1 | System A |
| 2 | 2008-10-10 10:10:10 | 192.168.1.1 | User 2 | System A |

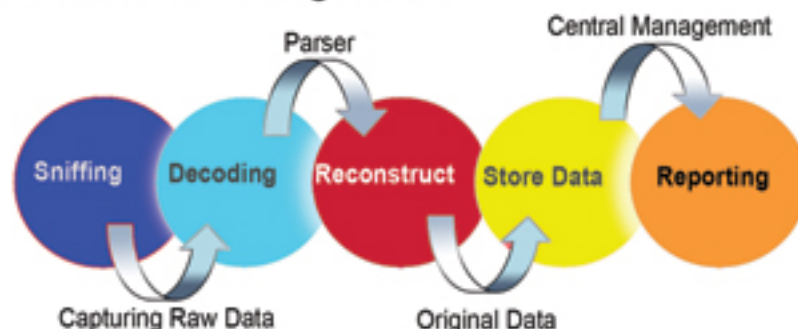
Network Service Weekly Report



Top Websites

| No. | Website URL | Count | Time |
|-----|------------------------|-------|----------|
| 1 | http://www.example.com | 1,234 | 10:10:10 |
| 2 | http://www.example.com | 1,234 | 10:10:10 |
| 3 | http://www.example.com | 1,234 | 10:10:10 |

E-Detective System Architectural Design & Flow



One of the MOST COMPLETE "Content Reconstruction" system in the world!





Specifications and Features

| | |
|------------------------------------|--|
| Supporting Throughput/Load | Up to 600 Mbps |
| Supporting Corporation Size | Very scalable, > 6000 online users |
| Appliance Based | Yes |
| Deployment | Mirror Mode, Bridge Mode, Sniffer Mode, Double Layer Architecture |
| Services/ Protocols | <p>Email Webmail (Read and Sent)</p> <p>POP3, SMTP, IMAP 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</p> <p>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</p> <p>HTTP Link (URL), HTTP Content, HTTP Reconstruct, HTTP Upload/Download, Video Stream, HTTP Request, Social Network Service (Facebook, Twitter, Plurk)</p> <p>FTP</p> <p>FTP Upload/Download</p> <p>P2P</p> <p>P2P Details Log - BitTorrent, eMule/eDonkey etc.</p> <p>Online Games</p> <p>80++ Online Games</p> <p>Telnet/BBS</p> <p>With playback</p> <p>VOIP</p> <p>Yahoo Messenger VOIP</p> <p>Webcame Video</p> <p>MSN Messenger, Yahoo Messenger Webcam</p> |
| Management | <p>System Access</p> <p>HTTPs Remote Monitoring</p> <p>Group/User</p> <p>Yes</p> <p>Data Backup</p> <p>Yes, Restore Server, NAS/S AN based FTP server etc.</p> <p>Web Browser Access</p> <p>Yes (using IE, Mozilla etc.)</p> <p>Data Mining and Search</p> <p>Yes (Search by Parameters, Search by Key Words), Similar Search Function, User Account Relationship tracing</p> <p>Alert/Notification</p> <p>Yes. Alert/Notification by parameters, by Key Words</p> <p>Throughput Alert</p> <p>Yes</p> <p>Station Management</p> <p>Yes (NetBIOS, Active Directory info)</p> <p>Storage Management</p> <p>Yes</p> <p>Upgrade</p> <p>Web based Upgrade</p> |
| Reporting | <p>Reports</p> <p>Yes, Comprehensive reporting. Total throughput statistical report with top-down view. Per user reporting with top-down view.</p> <p>Schedule Reporting</p> <p>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
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
decision@ms1.hinet.net