

# Decision Computer Group

## E-Detective System (Wired)

*Moving forward with the security of networking and computer forensics*

**E-DETECTIVE®**

Decision Computer - All rights reserved  
2007

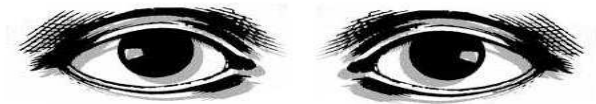


# Agenda

- ❖ Introduction of E-Detective System
- ❖ Why Internet Surveillance is needed?
- ❖ Who needs E-Detective System?
- ❖ Types of Companies that need E-Detective System
- ❖ E-Detective System Application
- ❖ Operation or Function of E-Detective
  - Emails, IM, FTP, P2P, Telnet, Web Browsing Log, Online Game
  - Web mail Token Analyzer
  - IP/ PC Names
  - Auditing Specific Target
  - Powerful Search Record and Data Mining
  - Data Backup
  - Reporting
  - Expanded Storage
- ❖ E-Detective System Models
- ❖ Some Reference Sites
- ❖ Frequently Asked Questions
- ❖ Comparison of E-Detective system and other software products
- ❖ Q&A



# E-DETECTIVE®



## Professional Network Behavior Recording, Auditing, Forensics, Legal Interception and Digital Property Preservation System



Decision Computer - All rights reserved  
2007



# Introduction to E-Detective System

**E-DETECTIVE**®



## Protecting business benefits and promoting office efficiency

A surveillance system for Internet activities designed for sniffing packets from LAN network, decode and convert the raw data captured to original or exact format of Emails (SMTP, POP3, Web Mails), FTP, P2P, Instant Message (MSN/ICQ/AOL/Yahoo/QQ), Telnet, Website Browsing, VoIP and Webcam (Forensics usage – for YAHOO and MSN), Online Game Logs, URL Web Browsing, SSL/HTTPS (another equipment) and such protocols.

Designed through



Decision Computer - All rights reserved  
2007



# Why Internet Surveillance is Needed?

Previously, companies can just use **PROXY and BLOCK OFF** Internet sites and applications such as IM (Yahoo, MSN ...) etc.

Now, with so many no-cost communication tools available in the Internet, the customers of these companies demand that these channels be **opened up** such as Email, Instant Messenger etc.

This has caused the following:

- a) Abuse by staff. Indulging in personal related issues over the internet rather than being productive at work.
- b) Invitation of virus and spam mails.
- c) Cookies with “malicious intent” penetrating the network
- d) Bandwidth wastage – downloading from P2P (Bittorent, Emule etc.)
- e) Staff sabotage
- f) Company data lost

**A need to protect company information and helps in Internal Assault investigation!**



# Types of Companies that need E-Detective System:

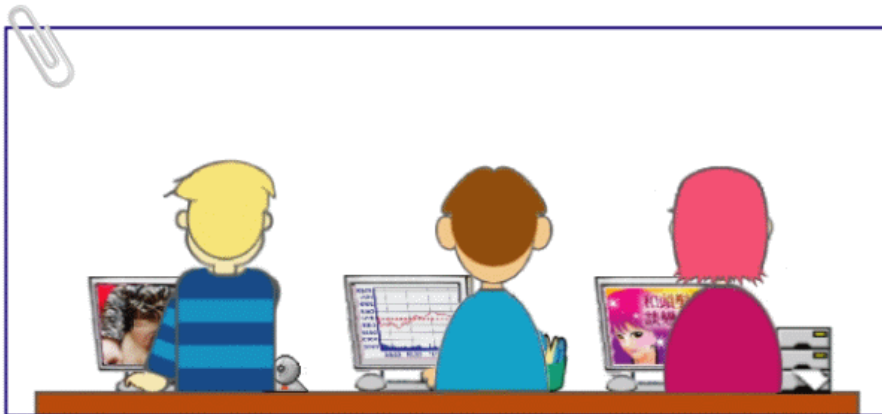
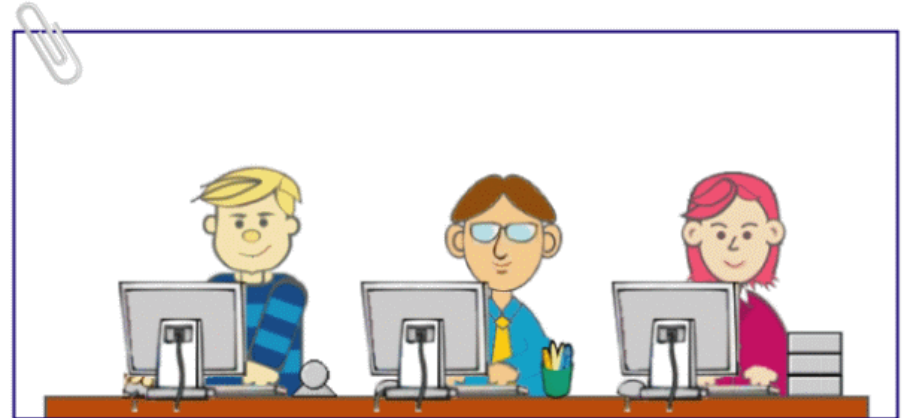


1. **Financial, Banking and Investment** Companies where all transactions and communications need to be monitored and archived.
2. Companies like **marketing, design house, high technology and R&D** firms, which critically need to prevent leakage of data. Staffs communicate with customers or vendors through web-based system need E-Detective to archive data.
3. **Schools, colleges, institutions and universities** that want to monitor students and staffs online activities.
4. **Government sectors and ministries** that want to protect important information from leakage.
5. **Any company** which want to monitor, backup and archive daily data.



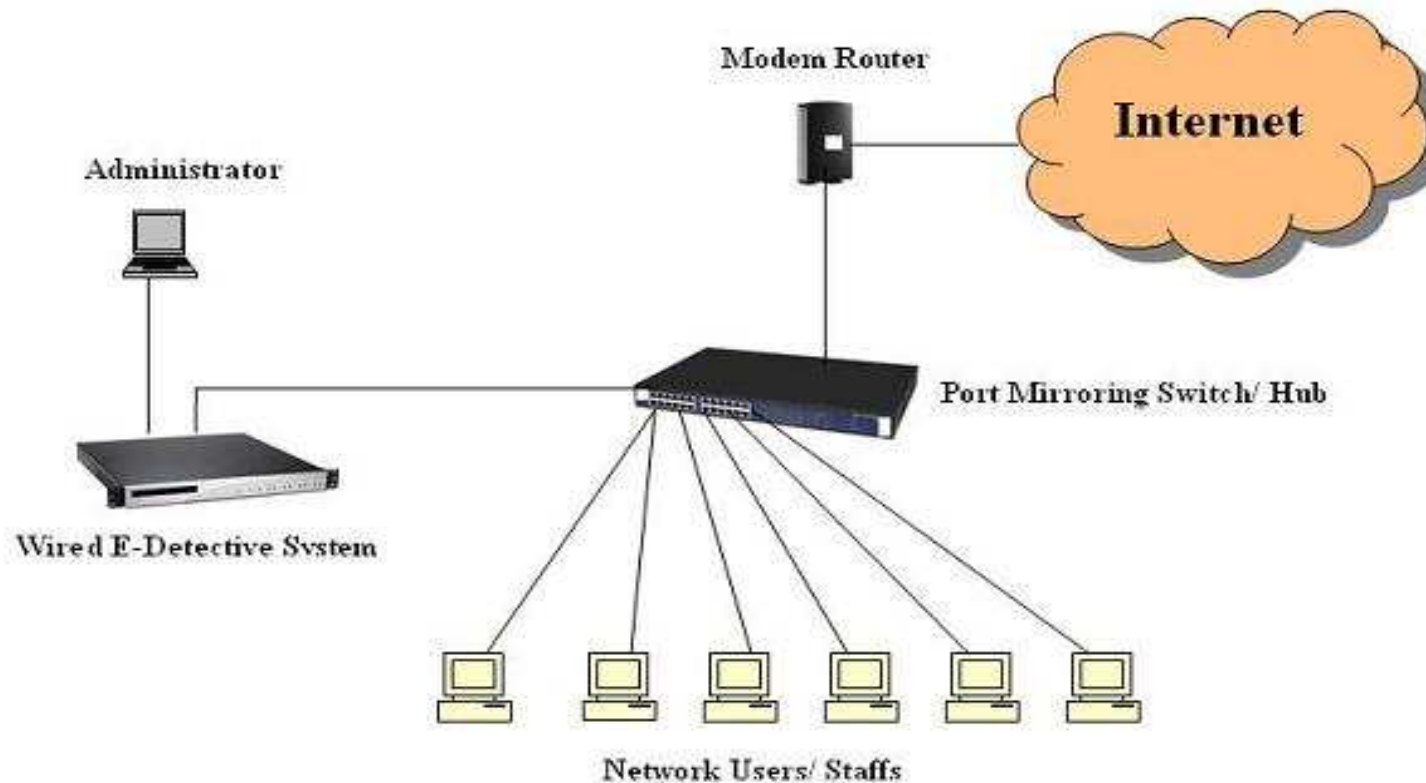
# What your staffs are doing?

“Seems normal on the surface ...”



“What? Porno site? Stock trading?  
E-Shopping? Staffs using Office hours  
for personal interest,

# E-Detective System Uses Sniffer Technology

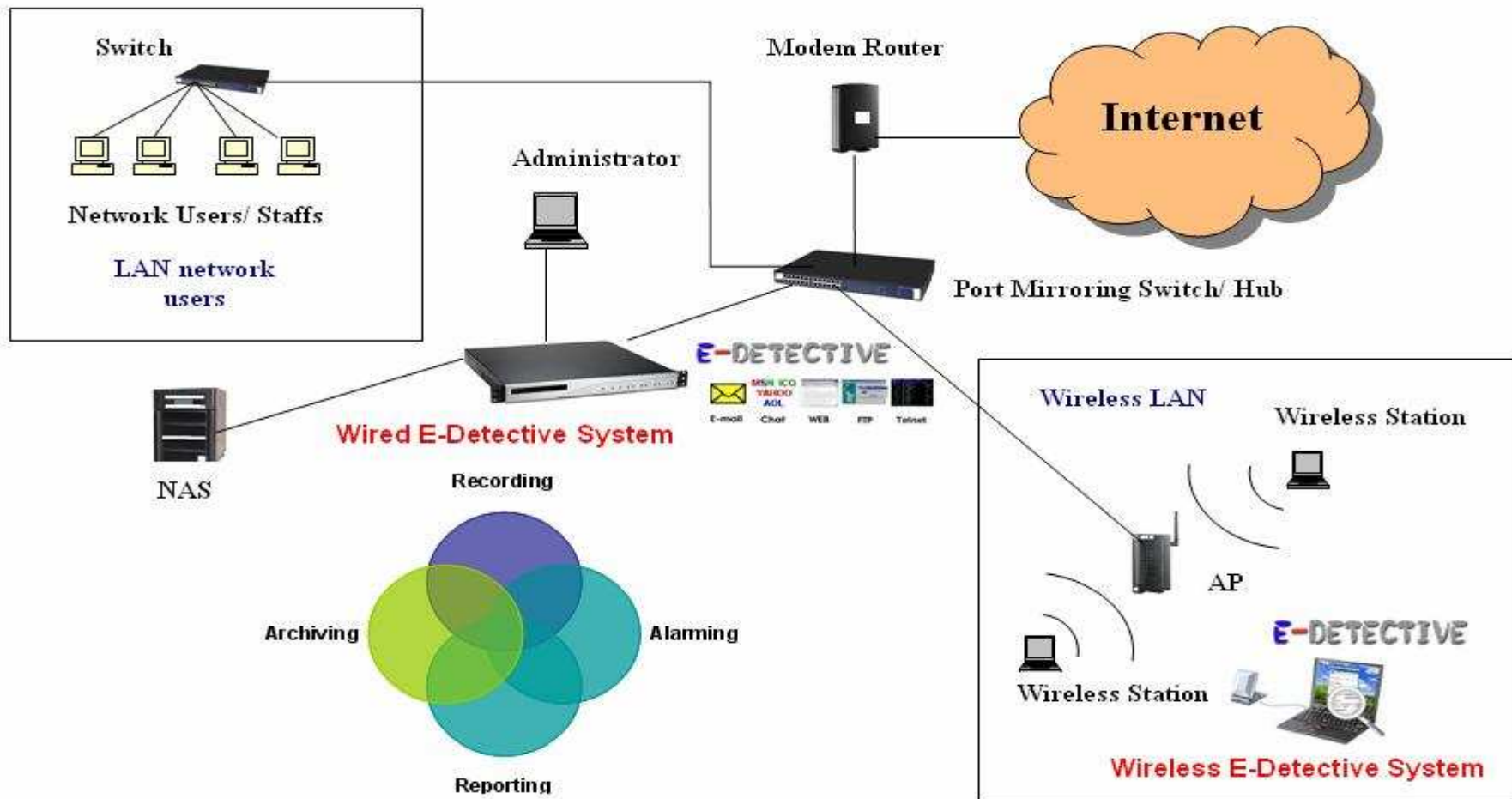


- Uses HUB, Port Mirroring/SPAN port Switch (Smart Switch, L2 Switch) or TAP to copy network TCP/UDP packets to E-Detective system.
- Can be remotely managed anywhere in the World.

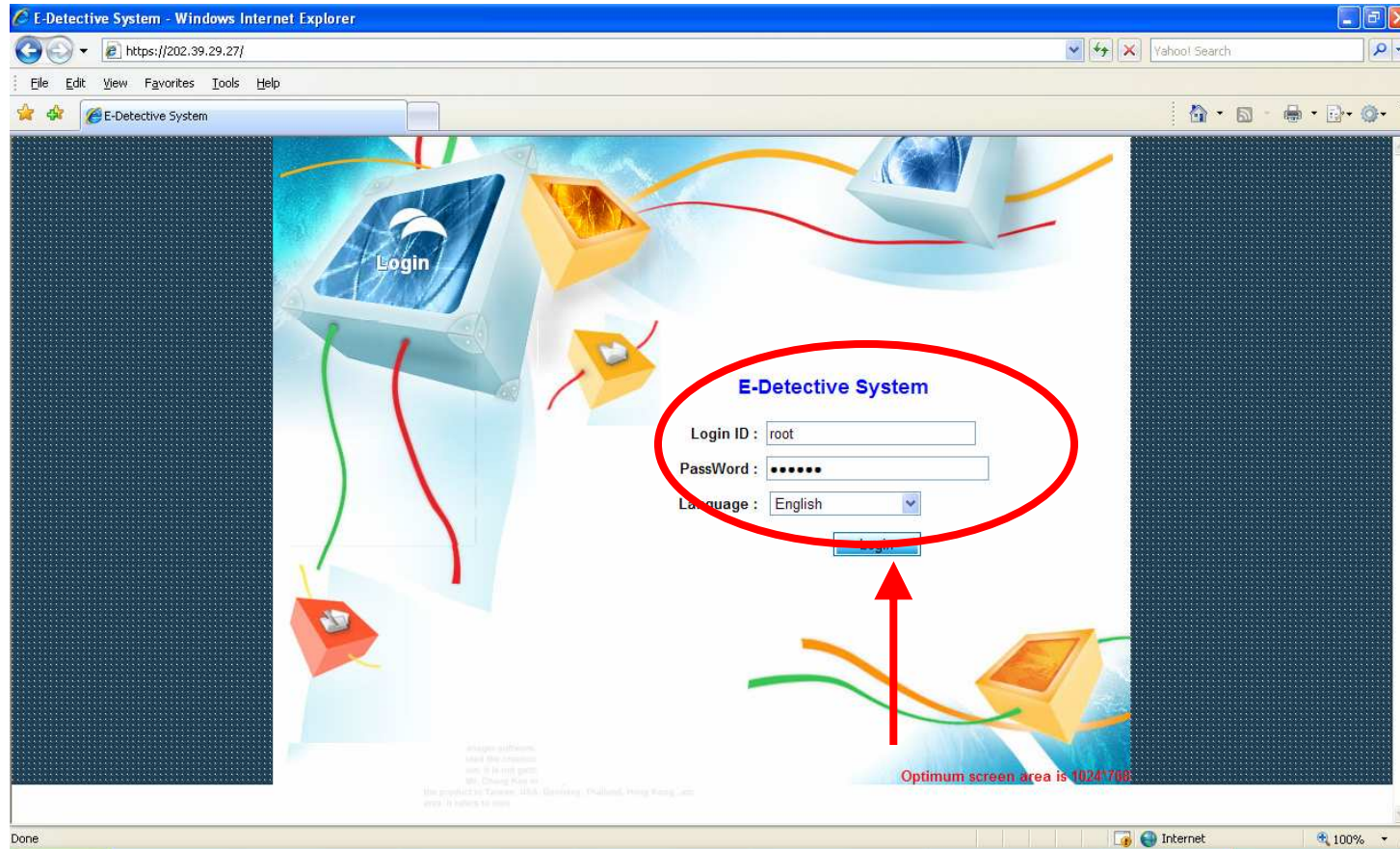


# A bigger picture of E-Detective System

## Wired and Wireless E-Detective System Application



# E-Detective is easy to operate



- 1) Just use **IE Browser** to login to ED system from local or remote site.
- 2) Uses https protocol for security protection
- 3) Multi **password, user's name** and **User's Group** for system login control

# Protocols supported E-Detective System



- E-Detective captures packets in the LAN network and decode (decrypted) the raw data captured into exact and real format of:
  - **Email** (POP3, SMTP, IMP4, Web mail),
  - **File Transfer Protocol FTP**,
  - **P2P file transfer** (Bittorent, eDonkey etc),
  - **Instant Messaging** (MSN, ICQ, AOL, YAHOO, QQ),
  - **TELNET**,
  - **HTTP URL Web Browsing and content**,
  - **VoIP & Webcam** (Forensics and enhanced feature).
  - **Online Games**
  - **SSL/ HTTPS (can be integrated into E-Detective system)**



# POP3/SMTP/ Web mail Log

**1** POP3 | Delete | Ignore | Ignore and Delete | Search

**2** Every Page : 15 Confirm

No	Date-Time	Sender	Receiver	CC	Subject	Size
1.	2005-10-20 10:48:54	mika@decision.com	mika@decision.com.tw		test	2.7K
2.	2005-10-20 10:45:59	Star.Council@rlformat.com	seven.times@msa.hinet.net		None A Star For Someone Specia	4.6K
3.	2005-10-20 10:33:16	seven.times@msa.hinet.net	ken@decision.com.tw		For tools	633.1K
4.	2005-10-20 10:29:25	553kenny@411now.com	ken@decision.com.tw		Cheap software	5.2K
5.	2005-10-20 10:29:25	hugo-leu@prolific.com.tw			Call+Alt+Delete	31.2K
6.	2005-10-20 10:18:33	technical@signetech.com				
7.	2005-10-20 10:13:58	decision@decision.com.tw				
8.	2005-10-20 10:12:50	sweep@garden.seed.net.tw				
9.	2005-10-20 10:07:38	jerome@computersofmexico.c...				
10.	2005-10-20 09:58:06	postmaster@klhb.gov.tw				
11.	2005-10-20 09:57:03	sweep@garden.seed.net.tw				
12.	2005-10-20 09:41:29	invemail@featuremarketing....				
13.	2005-10-20 09:40:24	sweep@garden.seed.net.tw				
14.	2005-10-20 09:24:47	ulcer@gordon.org				
15.	2005-10-20 09:03:24	casper.kan@msa.hinet.net				

**3** **4** **5** **6**

https://192.168.1.60/mime/eml/9/index.html - Microsoft Internet Explorer

Subject	Date/Time
From	ken@decision.com.tw,
To	ken@decision.com.tw,
CC	
BCC	
Date	2005-08-17 10:21:36.0
Source	POP3 s9v9sO.eml.txt
Attachment	
IP	192.168.1.20
DATETIME	2005-08-17 10:28:05.0

----- Original Message -----

From:

To:

Subject

Size

Source File ...



# IM - MSN, ICQ, AOL, Yahoo, QQ Log

DECISION


MSN | Delete | Display Set | Search - 1














2 - Show Mode : ☒ IP ☐ Name | Every Page : 15 | Confirm





No	Date-Time	IP	User Handle	Participants	Conversation	Count
1.	2005-10-20 14:20:52	192.168.1.20	she0430@hotmail.com	yvonne033@hotmail.com	5 - Conversation	2
2.	2005-10-20 14:20:02	192.168.1.20	she0430@hotmail.com	yaooay@hotmail.com	Conversation	3
3.	2005-10-20 14:11:53	192.168.1.10	aries0724@msn.com	natsuki0925@hotmail.co.jp	Conversation	2
4.	2005-10-20 14:07:19	192.168.1.20	she0430@hotmail.com	bany1013@hotmail.com	Conversation	6
5.	2005-10-20 13:54:54	192.168.1.10	aries0724@msn.com	nia9041613@hotmail.com	Conversation	2
6.	2005-10-20 13:41:04	192.168.1.20	she0430@hotmail.com			
7.	2005-10-20 13:14:19	192.168.1.20	she0430@hotmail.com			
8.	2005-10-20 12:53:04	192.168.1.21	hider			
9.	2005-10-20 12:49:46	192.168.1.21	hider			
10.	2005-10-20 12:46:19	192.168.1.21	hider			
11.	2005-10-20 12:44:50	192.168.1.21	hider			
12.	2005-10-20 12:43:42	192.168.1.10	aries			
13.	2005-10-20 12:19:20	192.168.1.22	ming30			
14.	2005-10-20 12:19:24	192.168.1.20	she0430@hotmail.com			
15.	2005-10-20 12:03:50	192.168.1.14	seve			

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2

# FTP Log





 FTP |  Delete |  Show Pass |  Search

2


Show Mode : ☒ IP ☐ Name | Every Page : 15

Confirm

No.	<input type="checkbox"/>	Date-Time	IP	User	Pass	Action	FTP Server IP	File Name
1.	<input type="checkbox"/>	2005-10-20 16:33:54	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
2.	<input type="checkbox"/>	2005-10-20 16:32:17	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
3.	<input type="checkbox"/>	2005-10-20 16:32:17	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
4.	<input type="checkbox"/>	2005-10-20 16:30:26	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
5.	<input type="checkbox"/>	2005-10-20 16:30:16	192.168.1.10	decision	*****	Upload	192.168.1.249	requestion.php
6.	<input type="checkbox"/>	2005-10-20 16:29:47	192.168.1.10	decision	*****			
7.	<input type="checkbox"/>	2005-10-20 16:27:14	192.168.1.10	decision	*****			
8.	<input type="checkbox"/>	2005-10-20 16:27:05	192.168.1.10	decision	*****			
9.	<input type="checkbox"/>	2005-10-20 16:26:44	192.168.1.10	decision	*****			
10.	<input type="checkbox"/>	2005-10-20 16:20:51	192.168.1.33	user	*****			
11.	<input type="checkbox"/>	2005-10-20 16:20:28	192.168.1.33	user	*****			
12.	<input type="checkbox"/>	2005-10-20 16:20:17	192.168.1.33	user	*****			
13.	<input type="checkbox"/>	2005-10-20 16:19:52	192.168.1.33	user	*****			
14.	<input type="checkbox"/>	2005-10-20 16:19:11	192.168.1.33	user	*****			
15.	<input type="checkbox"/>	2005-10-20	192.168.1.33		*****			

File Download

Do you want to open or save this file?




Name: FTP\_FILE\_uUyDT6.jpg

Type: JPEG Image, 467 KB

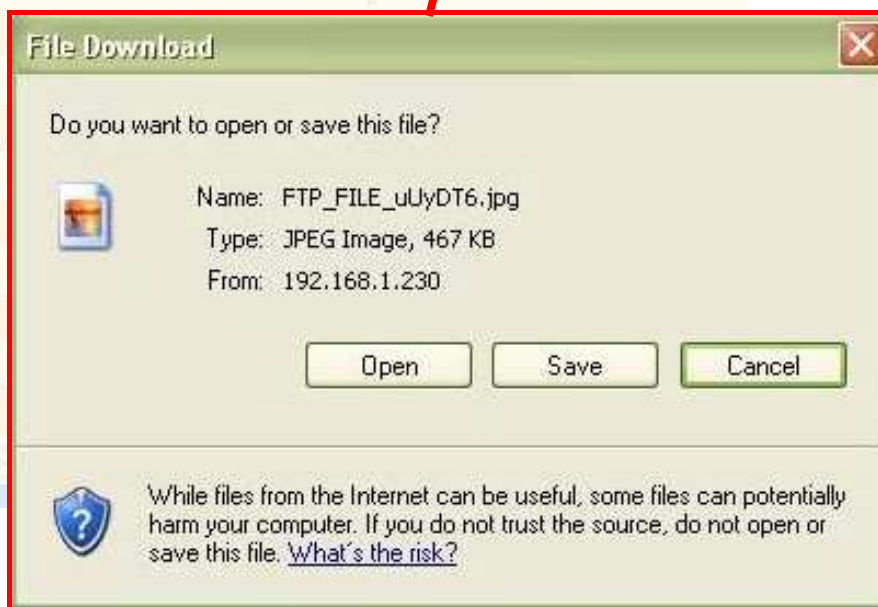
From: 192.168.1.230

Open

Save



While files from the Internet can be useful, some files can



**Date, Time, IP, server IP,  
password, Action, File  
name, File Content ...**

# Peer to Peer Communication (P2P) Log



No	Date-Time	IP	Port	P-IP	P-Port	Tool	File name	DIR
1	2007-05-16 16:59:54	192.168.1.36	1263	140.112.13.175	11373	Foxy 1.8.6.0	AV-??D?-???D??F ?'??(????k??).rm...	Download
2	2007-05-16 16:59:30	192.168.1.36	1212	125.232.119.155	5386	Foxy 1.8.6.0	13?b?H?C?? (1).MPG	Download
3	2007-05-16 16:58:58	192.168.1.36	1212	125.232.119.155	5386	Foxy 1.8.6.0	13?b?H?C?? (1).MPG	Download
4	2007-05-16 16:56:26	192.168.1.36	1099	123.110.5.242	18993	Foxy 1.8.6.0	?j???H-3-2007?-5??1???W?M 1.mpg	Download
5	2007-05-16 16:55:21	192.168.1.36	1037	210.203.40.24	11420	Foxy 1.8.6.0	AV-??D?-???D??F ?D? ?'??...	Download

« 1 2 3 4 5 6 7 8 9 » Total 3493 , Total Page 699 , Current Page 1

**Date/Time, IP, port, Transfer Tool,  
Transferred File Name,...etc.**



**URL Address, IP,  
URL Content**



# Telnet Log

**1** Telnet | Delete | Search

**2** Show Mode : ☒ IP ☐ Name | Every Page : 15 | Confirm

No.	Date-Time	IP	User	Pass	Server	Record File	Size
1.	2005-10-18 19:53:16	192.168.1.245			59.104.212.56	Record File	83B
2.	2005-10-18 17:09:38	192.168.1.245			59.104.212.56	Record File	83B
3.	2005-10-18 13:18:03	192.168.1.20			140.131.7.7	Record File	11.2K
4.	2005-10-18 06:34:46	192.168.1.245					
5.	2005-10-18 03:34:45	192.168.1.245					
6.	2005-10-18 01:13:42	192.168.1.245					
7.	2005-10-17 23:12:47	192.168.1.245					
8.	2005-10-17 21:34:29	192.168.1.245					
9.	2005-10-17 20:11:08	192.168.1.245					
10.	2005-10-17 16:04:34	192.168.1.245					
11.	2005-10-17 14:34:45	192.168.1.245					
12.	2005-10-17 13:28:38	192.168.1.245					
13.	2005-10-15 16:14:59	192.168.1.45					
14.	2005-10-15 16:08:05	192.168.1.24					
15.	2005-10-15 15:40:15	192.168.1.24					

**4** Record File

**5** 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363

# Online Game Log



No	<input type="checkbox"/>	Date-Time	IP	Port	Sever-IP	Sever-Port	Name
1	<input type="checkbox"/>	2007-05-16 12:23:48	192.168.1.15	4966	210.208.86.12	80	Kartrider
2	<input type="checkbox"/>	2007-05-15 17:14:16	192.168.1.15	3085	210.208.86.12	80	Kartrider
3	<input type="checkbox"/>	2007-05-14 11:26:02	192.168.1.21	3430	211.76.177.154	80	Hot
4	<input type="checkbox"/>	2007-05-14 10:17:55	192.168.1.21	2625	210.208.86.12	80	Kartrider

« 1 »

Total 4 , Total Page 1 , Current Page 1

**Date/Time, IP, Port, Game Name,...etc.**

# Web mail Token Analyzer (WTD)

Allow user to define the web mail types for recognition and categorization by E-Detective system.

**Web Mail Token Analyzer**

Save Load Upload

URL Signature String : email.about.com/gi/dynamic/

Field	Value	Action	Prefix Token	Suffix Token	Action
From :	"Decision" <decision_test@fastmail.fm>	Analysis	lass="DatTd" width="95%">	<a href="/mail?MLS=MR-*	Search
To :		Analysis			Search
CC :		Analysis			Search
BCC :		Analysis			Search
Subject :		Analysis			Search
Date :		Analysis			Search

HTML Source Code :

```
<!DOCTYPE html
PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">
<html lang="en-US"><head><title>View - Re: wtd test</title>
<meta name="revisit-after" content="30 days">
<meta name="rating" content="general">
<meta name="distribution" content="global">
<link rel="prev" href="/mail?MLS=MR-**22*;SMB-MF-TP=0;SMB-MF-SF=Date_1;SMR-MI=22;SMR-PT=;Ust=433c89e41081641b9;SMR-FM=1;SMB-CF=8175321;SMB-MF-DR=
<link rel="next" href="/mail?MLS=MR-**22*;SMB-MF-TP=0;SMB-MF-SF=Date_1;SMR-MI=22;SMR-PT=;Ust=433c89e41081641b9;SMR-FM=1;SMB-CF=8175321;SMB-MF-DR=
<link rel="up" href="/mail?MLS=MR-**22*;SMB-MF-TP=0;SMB-MF-SF=Date_1;SMR-MI=22;SMR-PT=;Ust=433c89e41081641b9;SMR-FM=1;SMB-CF=8175321;SMB-MF-DR=
<link rel="stylesheet" type="text/css" href="/styles/defaults.css">
<link rel="stylesheet" type="text/css" href="/pages/fastmail/styles/professionalblue2004-ie7.css">
</head>
<body class="body">
<form method="post" action="http://www.fastmail.fm/mail?Ust=433c89e41081641b9;UDm=49" enctype="application/x-www-form-urlencoded" name="memail">
<input value="MR-**22*" name="MLS" type="hidden">
<input value="0" name="SMB-MF-TP" type="hidden">
<input value="Date_1" name="SMB-MF-SF" type="hidden">
<input value="22" name="SMR-MI" type="hidden">
<input value="" name="SMR-PT" type="hidden">
<input value="1" name="SMR-FM" type="hidden">
<input value="8175321" name="SMB-CF" type="hidden">
<input value="20" name="SMB-MF-DR" type="hidden">
<input value="MR-ST*" name="MFeedbackSignal" type="hidden">
<input value="" name="charset" type="hidden">
<noscript><input type="hidden" name="nojs" value="1"></noscript>
<table width="100%" cellpadding="0" cellspacing="1" border="0" class="TblBox"><tr><td>
<table class="HdrTbl" border="0" cellpadding="3" width="100%"><tr align="left" valign="middle"><td class="HdrIcon" nowrap><div></div></td><td nowrap><font class="HdrDsc" face="Verdana, Arial, Helvetica, sans-serif"
size="+2">View</font></td><td width="100%"><table border="0" cellspacing="0" width="100%"><tr align="center" valign="middle"><td class="HdrScrTd"><a
```

**HTTP Connection Setup**

Server URL : https://192.168.1.207

Login Username : root

Login Password : .....

☐ Use HTTP Proxy

Proxy IP :

Proxy Port :

Proxy Username :

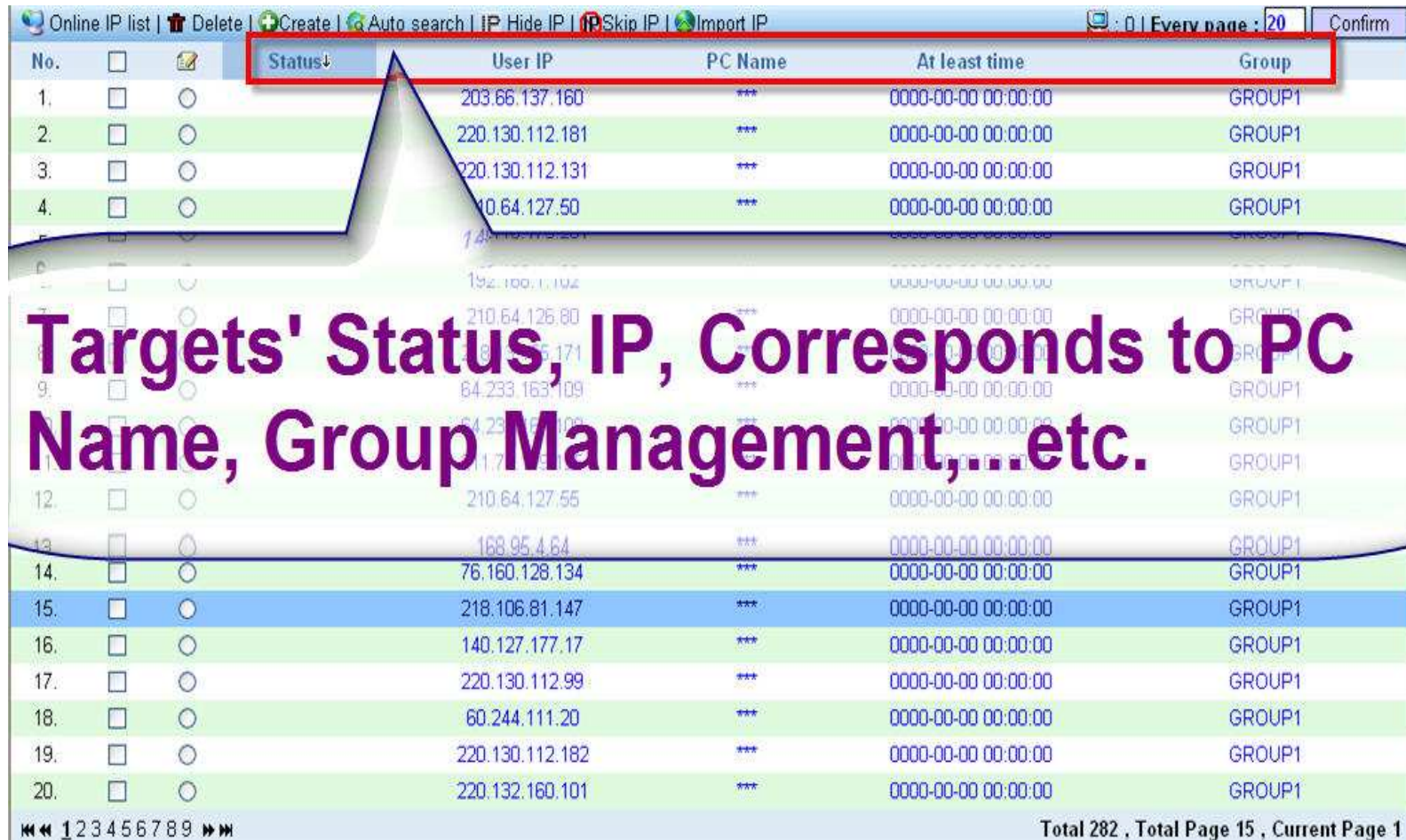
Proxy Password :

Okay Cancel



# IP / PC name (Homologue)

## - Users Management



Online IP list | Delete | Create | Auto search | IP Hide IP | IP Skip IP | Import IP | 0 | Every page : 20 | Confirm

No.	<input type="checkbox"/>	<input type="checkbox"/>	Status↓	User IP	PC Name	At least time	Group
1.	<input type="checkbox"/>	<input type="radio"/>		203.66.137.160	***	0000-00-00 00:00:00	GROUP1
2.	<input type="checkbox"/>	<input type="radio"/>		220.130.112.181	***	0000-00-00 00:00:00	GROUP1
3.	<input type="checkbox"/>	<input type="radio"/>		220.130.112.131	***	0000-00-00 00:00:00	GROUP1
4.	<input type="checkbox"/>	<input type="radio"/>		10.64.127.50	***	0000-00-00 00:00:00	GROUP1
5.	<input type="checkbox"/>	<input type="radio"/>		140.127.177.17	***	0000-00-00 00:00:00	GROUP1
6.	<input type="checkbox"/>	<input type="radio"/>		192.168.1.102	***	0000-00-00 00:00:00	GROUP1
7.	<input type="checkbox"/>	<input type="radio"/>		210.64.126.80	***	0000-00-00 00:00:00	GROUP1
8.	<input type="checkbox"/>	<input type="radio"/>		8.15.15.171	***	0000-00-00 00:00:00	GROUP1
9.	<input type="checkbox"/>	<input type="radio"/>		64.233.163.109	***	0000-00-00 00:00:00	GROUP1
10.	<input type="checkbox"/>	<input type="radio"/>		64.233.163.109	***	0000-00-00 00:00:00	GROUP1
11.	<input type="checkbox"/>	<input type="radio"/>		11.7.15.1	***	0000-00-00 00:00:00	GROUP1
12.	<input type="checkbox"/>	<input type="radio"/>		210.64.127.55	***	0000-00-00 00:00:00	GROUP1
13.	<input type="checkbox"/>	<input type="radio"/>		168.95.4.64	***	0000-00-00 00:00:00	GROUP1
14.	<input type="checkbox"/>	<input type="radio"/>		76.160.128.134	***	0000-00-00 00:00:00	GROUP1
15.	<input type="checkbox"/>	<input type="radio"/>		218.106.81.147	***	0000-00-00 00:00:00	GROUP1
16.	<input type="checkbox"/>	<input type="radio"/>		140.127.177.17	***	0000-00-00 00:00:00	GROUP1
17.	<input type="checkbox"/>	<input type="radio"/>		220.130.112.99	***	0000-00-00 00:00:00	GROUP1
18.	<input type="checkbox"/>	<input type="radio"/>		60.244.111.20	***	0000-00-00 00:00:00	GROUP1
19.	<input type="checkbox"/>	<input type="radio"/>		220.130.112.182	***	0000-00-00 00:00:00	GROUP1
20.	<input type="checkbox"/>	<input type="radio"/>		220.132.160.101	***	0000-00-00 00:00:00	GROUP1

1 2 3 4 5 6 7 8 9 >>> Total 282 , Total Page 15 , Current Page 1

**Targets' Status, IP, Corresponds to PC Name, Group Management,...etc.**

# Powerful Search Record and Data Mining

Search All - Microsoft Internet Explorer

**Search Conditions**

Search The Condition		Search Mode
Date :	<input type="text"/> ~ <input type="text"/>	All
Time :	<input type="text"/> : <input type="text"/> : <input type="text"/> ~ <input type="text"/> : <input type="text"/> : <input type="text"/>	
Source IP :	<input type="text"/>	
E-Mail Address :	<input type="text"/> <input type="checkbox"/> Sender <input type="checkbox"/> Receiver <input type="checkbox"/> CC <input type="checkbox"/> BCC	
Subject :	<input type="text"/>	
Webmail Type :	<input type="text"/>	
FTP Server :	<input type="text"/>	
FTP User :	<input type="text"/>	
MSN Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
ICQ Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
Yahoo Account :	1. <input type="text"/> 2. <input type="text"/> <input type="checkbox"/> User Handle <input type="checkbox"/> Participants	
URL :	<input type="text"/>	
Telnet User :	<input type="text"/>	
Other :	<input type="text"/>	

Reset Search Close

**SEARCH KEY**  
Support By IP, Mail  
Account, Date, Time,  
Keyword, Attach  
file ... etc

https://202.39.29.27 - Data Mining - Microsoft Internet Explorer

HELLO

The authorization area for E-Detective Internet Sniffer recorder monitor manager software. Authorize the user who can not modify or to extended the version or to create the new version's authorization. It is not getting the argument from the original innovator Mr. C31 Kan in first, you can not provide or sell the product in Taiwan, USA, Germany, Thailand, Hong Kong, etc area. It refers to ipm

2 0 0

# Auditing the Specific Targets

Notification Service

Create a New Notification Setup

click

Delete	Notification Condition		Action	Captured
X	ICQ	User Account is 192.168.1.237	Fw to: decision_test@pchome.com.tw	Modify 0
X	IMAP	IP is 192.168.1.237	Fw to: decision_test@pchome.com.tw	Modify 0
X	MSN	User Account is decision_service_center@hotmail	Fw to: chang_kan@decision.com.tw; math824@grr	Modify 1
X	MSN	IP is 192.168.1.237	Fw to: decision_test@pchome.com.tw	Modify 0
X	POP3	IP		
X	QQ	User Account		
X	SMTP	IP		
X	WebmailS	IP		
X	YAHOO	User Account		

1

Date Type

Not

https://192.168.1.90/notification/rule\_edit.php - Microsoft Internet Explorer

Create a New Notification Setup

Notification Condition		Forward to
POP3	Sender	Add
IMAP	Sender	Add
SMTP	Sender	Add
Webmails	Sender	Add
MSN	User Account	Add
Yahoo	User Account	Add
ICQ	User Account	Add
QQ	User Account	Add

完成 網際網路

# Data Backup

**Auto Backup**  
Please check HD!

Time : Hour Day Month Week  
Status : ☐ Stop ☐ Start  
OK Reset

**Backup Modules**

Modules : ☒ POP3 ☒ SMTP ☒ IMAP  
☒ FTP ☒ MSN  
☒ YAHOO ☒ HTTP  
☒ WEBMAILR ☒ WEBMAIL  
☒ QQ ☒ P2P  
OK

**Notify target**

Receiver :

Delete

No	Receive
1.	<input type="checkbox"/> sunny@decision.com.tw

1 1 Total 1, Total Page 1

**Manual Backup**

<input checked="" type="checkbox"/>	*	<input type="checkbox"/>	2007-03-30_17:05:47	8.4M	2007_03_30_17_05_47.iso
<input checked="" type="checkbox"/>	*	<input type="checkbox"/>	2007-03-30_16:51:27	14M	2007_03_30_16_51_27.iso
<input checked="" type="checkbox"/>	*	<input type="checkbox"/>	2007-03-30_16:51:26	8.0K	2007_03_30_16_51_26.iso
<input checked="" type="checkbox"/>	*	<input type="checkbox"/>	2007-03-30_16:42:44	18M	2007_03_30_16_42_44.iso

Backup Item : ☒ POP3 ☒ SMTP ☒ IMAP ☒ FTP  
☒ MSN ☒ ICQ ☒ Yahoo ☒ HTTP  
☒ URL Content ☒ Webmail ☒ Webmail (Send) ☒ Telnet  
☒ QQ ☒ P2P  
Make

US CRW-5232AS  
um  
Delete

**FTP Login Information**

This iso image will be uploaded and deleted at two o'clock every day!

Ftp Host : 192.168.1.249  
User : alluser  
Password :   
Port Number : 21  
Directory : ISO\_FILE  
☐ ON ☒ OFF  
Submit Reset

# FTP Auto Backup

# Report – Single and Group Report

Report

Report by Group

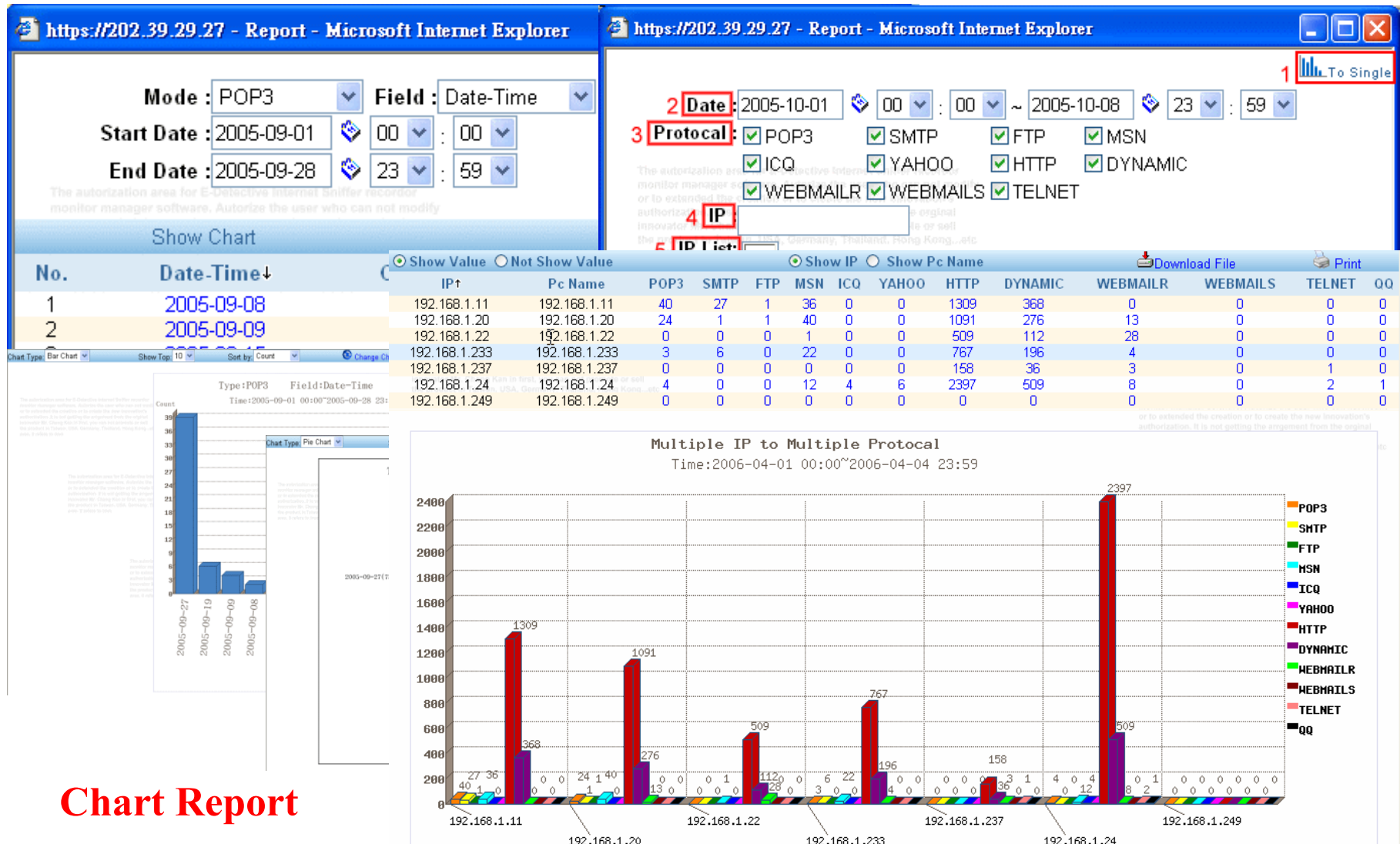


Chart Report

Decision Computer - All rights reserved  
2007



# Report – Statistical Report List

## Network Services Usage Report

E-Detective System - Windows Internet Explorer

https://192.168.1.207/frame/main.php

E-Detective System

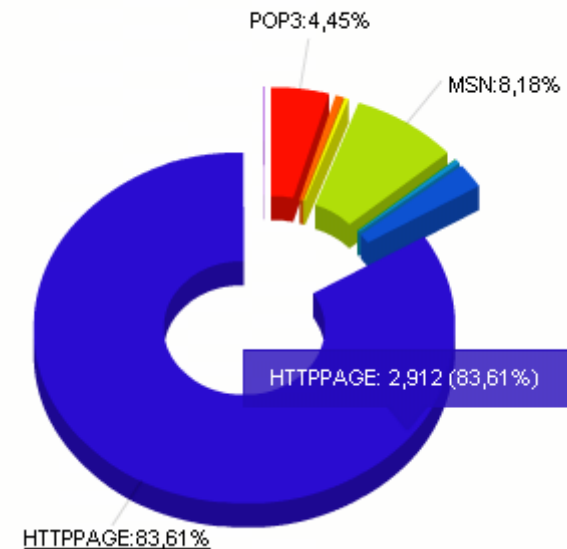
URL Content | Delete | Search

Show Mode : IP PC Name | Every page :

No.	Date-Time	IP	URL Content
1.	2007-09-03 15:22:27	192.168.1.136	linux.vbird.org
2.	2007-09-03 15:19:39	192.168.1.138	ad.doubleclick.net
3.	2007-09-03 15:19:37	192.168.1.138	ad.doubleclick.net
4.	2007-09-03 15:19:37	192.168.1.138	ad.doubleclick.net
5.	2007-09-03 15:19:34	192.168.1.138	mail01.mail.com
6.	2007-09-03 15:19:33	192.168.1.138	ad.doubleclick.net
7.	2007-09-03 15:19:33	192.168.1.138	ad.doubleclick.net
8.	2007-09-03 15:19:12	192.168.1.138	ad.doubleclick.net
9.	2007-09-03 15:19:12	192.168.1.138	ad.doubleclick.net
10.	2007-09-03 15:19:10	192.168.1.138	ad.doubleclick.net
11.	2007-09-03 15:19:08	192.168.1.138	mail01.mail.com
12.	2007-09-03 15:19:07	192.168.1.136	linux.vbird.org
13.	2007-09-03 15:19:06	192.168.1.138	ad.doubleclick.net
14.	2007-09-03 15:19:05	192.168.1.138	ad.doubleclick.net
15.	2007-09-03 15:19:05	192.168.1.138	www.mail.com
16.	2007-09-03 15:19:05	192.168.1.138	www.mail.com
17.	2007-09-03 15:19:05	192.168.1.138	www.mail.com
18.	2007-09-03 15:19:05	192.168.1.138	www.mail.com
19.	2007-09-03 15:19:04	192.168.1.138	www.mail.com
20.	2007-09-03 15:19:04	192.168.1.138	www.mail.com

Total 2,902 Total Page 146 Current Page 1

## Network Services Usage Report

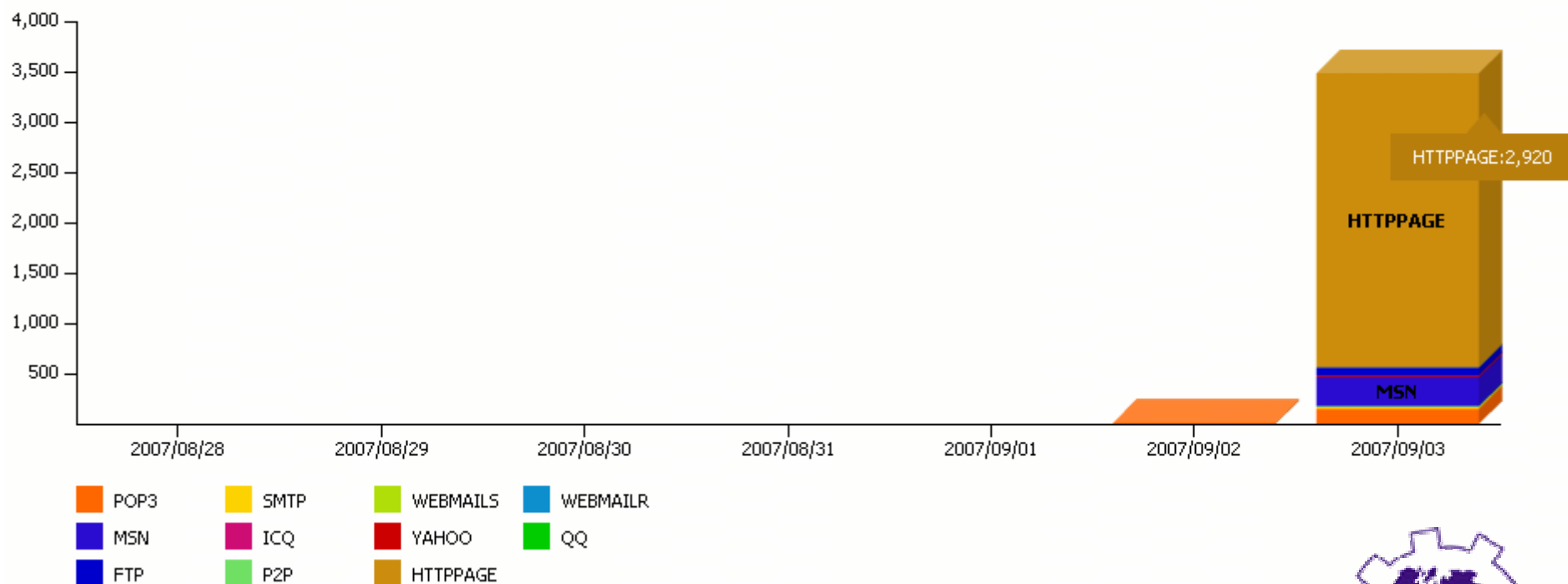


# Report – Statistical Report List

## Network Services Usage Weekly Report

chart by amCharts.com

### Network Services Usage Weekly Report



Decision Computer - All rights reserved  
2007



# Report – Statistical Report List

## Top Users of Network Services

### Top Users of Network Services

Daily

Weekly

Summary



	User Account			Count
1	192.168.1.25		Relations	44
2	192.168.1.23		Relations	36
3	192.168.1.10		Relations	30
4	192.168.1.6		Relations	
5	192.168.1.138		Relations	
6	192.168.1.4		Relations	
7	192.168.1.7		Relations	
8	192.168.1.29		Relations	

https://192.168.1.207/report/t...  
prt/tree.php?IP=192.168.1.25 Certificate Error

### Relationship between Account and IP Address

192.168.1.25

FTP	user
SMTP	dc@decision.com.tw
POP3	dc

Internet 100%

# Report – Statistical Report List

## Top Web Sites

### Top Web Sites

**Daily** **Weekly** **Summary**

	Web Server URL			Count	User												
1	192.168.1.117			922	TOP 10												
2	<div>Top Web Sites (Top 10)</div> <div>192.168.1.117</div> <table><tr><th></th><th colspan="2">IP</th><th>Count</th><th colspan="2">User Behavior</th></tr><tr><td>1</td><td>192.168.1.21</td><td>Relations</td><td>922</td><td>Daily Usage</td><td>Weekly Usage</td></tr></table>						IP		Count	User Behavior		1	192.168.1.21	Relations	922	Daily Usage	Weekly Usage
						IP		Count	User Behavior								
1						192.168.1.21	Relations	922	Daily Usage	Weekly Usage							
3																	
4																	
5																	
6																	
7	www.msn.com			93	TOP 10												
8	ad.doubleclick.net			84	TOP 10												
9	tw.yahoo.com			81	TOP 10												
10	tw.pvc.news.yahoo.com			68	TOP 10												
11	linux.vbird.org			63	TOP 10												
12	www.programmer-club.com			56	TOP 10												
13	74.6.234.80			43	TOP 10												
14	tw.search.yahoo.com			40	TOP 10												
15																	

# Report – Statistical Report List

## Online Users List

E-Detective System - Windows Internet Explorer

https://192.168.1.207/frame/main.php

File Edit View Favorites Tools Help

E-Detective System

Online IP list | Delete | Create | Auto search | IP Hide IP | Skip IP | Import IP

4 | Every page : 20 Confirm

No.	Status	User IP	PC Name	At least time	Group	User Behavior		
1.		192.168.1.21	***	2007-09-03 16:27:56	GROUP1	Daily Usage	Weekly Usage	Relations
2.		192.168.1.23	***	2007-09-03 16:28:02	GROUP1	Daily Usage	Weekly Usage	Relations
3.		192.168.1.29	***	2007-09-03 16:27:24	GROUP1	Daily Usage	Weekly Usage	Relations
4.		192.168.1.36	***	2007-09-03 16:27:42	GROUP1	Daily Usage	Weekly Usage	Relations
5.		192.168.1.6	***	2007-09-03 16:20:03	GROUP1	Daily Usage	Weekly Usage	Relations
6.		192.168.1.68	***	2007-09-03 16:02:02	GROUP1	Daily Usage	Weekly Usage	Relations
7.		192.168.1.129	***	2007-09-03 11:45:03	GROUP1	Daily Usage	Weekly Usage	Relations
8.		192.168.1.117	***	2007-09-03 14:55:02	GROUP1	Daily Usage	Weekly Usage	Relations
9.		192.168.1.201	***	2007-09-03 14:57:02	GROUP1	Daily Usage	Weekly Usage	Relations
10.		192.168.1.138	***	2007-09-03 16:27:03	GROUP1	Daily Usage	Weekly Usage	Relations
11.		192.168.1.7	***	2007-09-03 12:21:54	GROUP1	Daily Usage	Weekly Usage	Relations
12.		192.168.1.4	***	2007-09-03 16:10:05	GROUP1	Daily Usage	Weekly Usage	Relations
13.		192.168.1.25	***	2007-09-03 16:27:03	GROUP1	Daily Usage	Weekly Usage	Relations
14.		192.168.1.10	***	2007-09-03 16:16:04	GROUP1	Daily Usage	Weekly Usage	Relations
15.		192.168.1.207	***	2007-09-03 16:27:03	GROUP1	Daily Usage	Weekly Usage	Relations
16.		192.168.1.136	***	2007-09-03 16:26:19	GROUP1	Daily Usage	Weekly Usage	Relations
17.		192.168.1.148	***	2007-09-03 16:24:31	GROUP1	Daily Usage	Weekly Usage	Relations

1 17

Total 17 Total Page 1 Current Page 1

Internet 100%

# Report – Statistical Report List

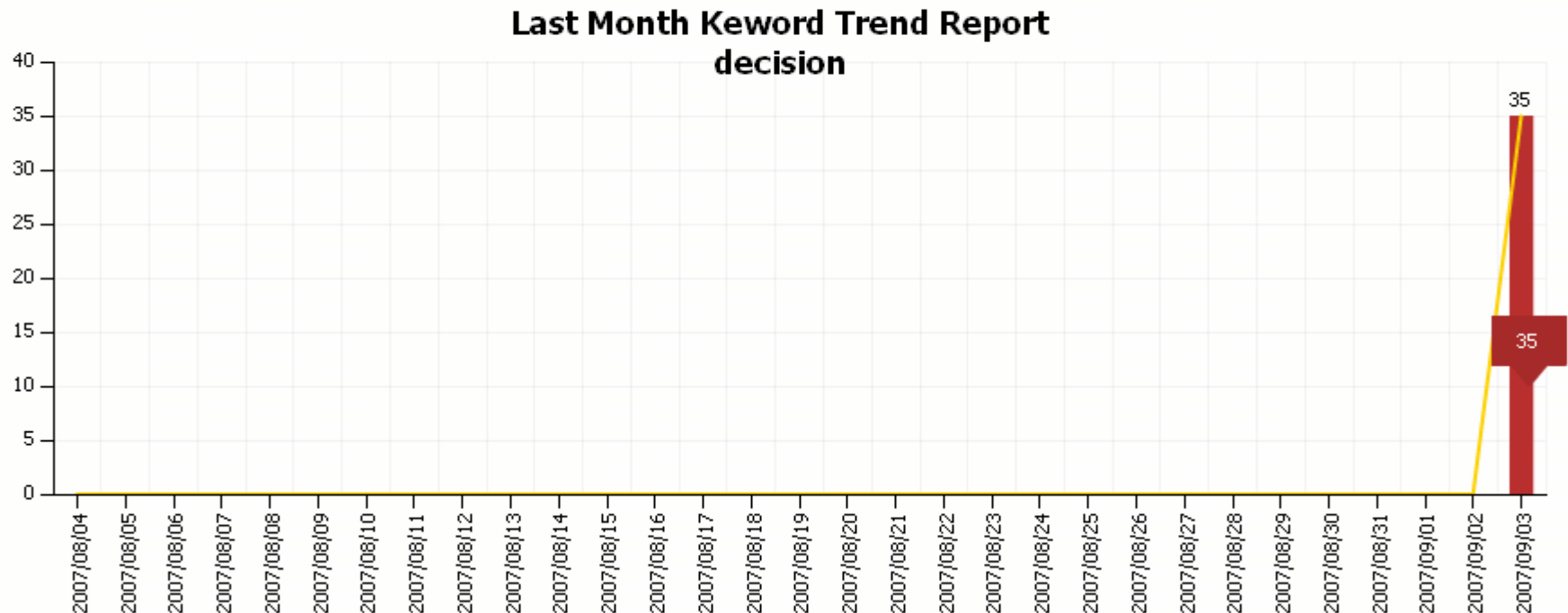
## Last Month Keyword Trend Report

Last Month Keword Trend Report

decision

Submit

chart by amCharts.com

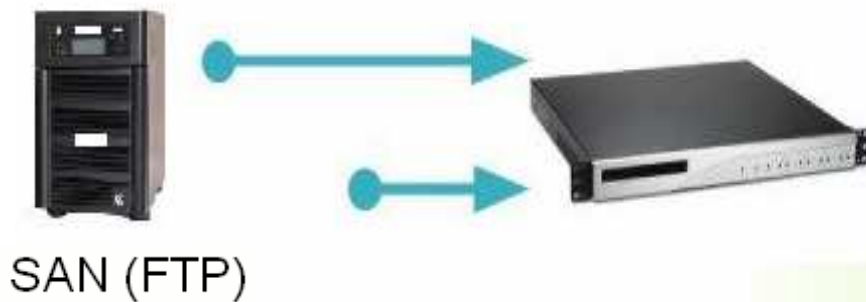


Decision Computer - All rights reserved  
2007



## Expanded storage

E-Detective System supports Expanded storage such as NAS, SAN (FTP), CD Libraries, Tape Storage, etc



Co-work with NAS, SAN  
or DVD-CD Library

# E-Detective Models

We provide some E-Detective system modules to customers.  
We challenge all sort of technical designs to meet the need of customers.

## E-Detective Models & Spec

Model Number	PIC	Client Supported	HDD SIZE	DUD	External Storage Support	Infrastructure
ED-FX6		10-49	80G	-	-	Single
ED-FX30		50-200	160G	✓	-	Single
ED-FX100		201-999	120G-300G Max.	✓	Support	Double
ED-FX120		above1000	120G-300G Max.	✓	Support	Double





# Frequently Asked Questions (1)

1. What is E-Detective?

E-Detective is an Internet Surveillance, Professional Network Behavior Recording, Auditing, Forensics, Legal Intercept, Digital Property Reservation system.

2. Compare E-Detective to Firewall, IDS, IPS and UTM systems, what are the major differences between them?

E-Detective does not interfere the network activities or condition. It uses sniffer technology to sniff packets from mirror port of a switch or hub and decode, reconstruct the Internet raw data and display them in original format (real and exact content). It is a system to trace back every evidence of confidential information loss through the Internet (protect from Internal sabotage). While Firewall, IDS, IPS and UTM systems can create policies, rules and limit or block access to some services and applications (protect from outside attack).

3. Is E-Detective system a software or an appliance?

E-Detective system is an appliance (Software loaded into hardware equipment).

4. What Operating System E-Detective used?

E-Detective uses customized Debian (Linux OS) from our team of Engineers.



## Frequently Asked Questions (2)

5. How many version of E-Detective is available?

E-Detective consists of Wired E-Detective system (working on LAN network) and Wireless E-Detective system (working on WLAN 802.11a/b/g network). The Wired E-Detective system can be further classified into Standard Wired E-Detective System and Forensics Wired E-Detective system. The major different is Forensics Wired E-Detective system has some features not found in Standard E-Detective system such as VOIP and Webcam features, interface to import raw data for decoding/parser etc.

6. What type of protocols decoded my E-Detective system?

E-Detective system can decode and reconstruct Emails (POP3, SMTP, IMAP, Web Mails), FTP, P2P, Telnet, Instant Messages (MSN, Yahoo, ICQ, AOL, QQ), Online Games, HTTP Web Browsing URL and Contents etc.

7. What management function E-Detective system provides?

Data backup (Auto, Manual, FTP), Reporting, Search and Data Mining, Auditing Specific Target, Creating Rules and Warning/Alarming, Delete Data and others.



## Frequently Asked Questions (3)

8. In what format E-Detective captures and save the raw data?  
E-Detective capture and save the raw data in tcp dump format. By using any network analyzer tool such as Ethereal, the capture file can be opened and analyze.
9. Does E-Detective supports any other raw data format for data decoding and reconstruction.  
Yes, E-Detective supports raw data save in format like pcap, cap. These raw data can be imported into E-Detective system for decoding and reconstruction purpose.
10. For Emails capturing and reconstruction, are Lotus Notes and Microsoft Exchange server based emails supported?  
We don't support Lotus Notes and Microsoft Exchange because both these systems have their own archiving/backup server system where administrator can retrieve emails from the server easily. Besides, both of them are using their own proprietary and encryption that we don't intend to break. If SMTP Gateway is used, then E-Detective system can decode the emails content.



# Frequently Asked Questions (4)

11. What web mails is supported by E-Detective system?

Web Mails supported by E-Detective Hinet, Hotmail Standard, PCHome, Yahoo Mail Standard, URL, Giga, Yam, Sina, Seednet, mail.tom.com, mail.163.com, Sohu.com etc. Hotmail Live, Yahoo Beta Mail and Gmail which use AJAX web client are in our road map.

12. Why I can't record and playback VOIP and Webcam sessions?

Please make sure that you have Forensic Wired E-Detective system or Wireless E-Detective system. This feature is not included in Standard Wired E-Detective system. MSN and Yahoo Messenger are updated often and E-Detective needs to have the latest parser to decode the VOIP and Webcam session. Therefore, please check with our support team regarding your version of MSN and Yahoo Messenger used. For playback of recorded VOIP and Webcam session for MSN Messenger, some configurations need to be set on the E-Detective system. For playback of recorded VOIP and Webcam session for Yahoo, there is no setting needed to be set on the system itself. However for Yahoo VOIP playback, GIPS codecs is needed. Please refer to our support team or user manual for more details.



# Frequently Asked Questions (5)

13. If the network is DHCP based, how can a user/staff be tracked?  
It is advisable to use static IP instead of DHCP. However, AD Server can be used to solve this problem.
14. Can E-Detective system tracks user by MAC address?  
Yes, E-Detective can track user by MAC address. Search user by MAC address is available. Besides, MAC address is can be seen when the pointer is pointed on the IP address.
15. Can E-Detective system searches keywords of different language?  
Yes, E-Detective system uses unicode format. As long as the keywords are sent or received in unicode format, E-Detective can search for the particular keyword.
16. What application is Data Mining limited to?  
Current version of E-Detective can provide data mining for Emails (POP3, SMTP, IMAP, Web Mails) and Instant Messages (Yahoo, MSN, ICQ,QQ, AOL). Providing data mining services for Web Content will utilize lots of processing power due to large Web database. However, our R&D team will come out with the version that can support HTML Web content keywords search (data mining) in the near future.

# Comparison of ED and Other software (1)

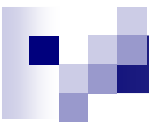
<u>Features</u>	<b>E-Detective</b>	<b>Other software products</b>
<b>Software or Hardware?</b>	Both	Only Software
<b>Standalone / Network?</b>	Network	Both (depends on software)
<b>Install to each PC?</b>	No	Yes
<b>Remote Access?</b>	Yes	Yes
<b>Software customizable</b>	Yes	No
<b>Number of Users</b>	can be more than 2000 users	small limited number
<b>Difficult to install?</b>	Easy	Hectic
<b>Method of Monitoring</b>	Reconstruct Entire Internet Contents	Normally using screen capture
<b>Can capture attachments?</b>	Yes	No
<b>Can capture VOIP messages?</b>	Yes	No
<b>Can capture Webcam transmissions?</b>	Yes	No
<b>Data Mining (Keywords)</b>	Yes	No
<b>Warning / Alarm</b>	Yes	No
<b>Search function</b>	Yes	Yes
<b>Data Backup / Archiving</b>	Yes	No
<b>Scalable Storage</b>	Yes	Yes
<b>Reports</b>	Yes	Yes
<b>Customizable Reports</b>	Yes	Yes

# Comparison of ED and Other software (2)

Internet Protocol Reconstructed	E-Detective system	Other software product
<b>1. Email</b>		
a. POP 3	Yes (with attachment)	Yes (mostly no attachment)
b. SMTP	Yes (with attachment)	Yes (mostly no attachment)
c. IMAP	Yes (with attachment)	N.A
d. Web mail - Yahoo, Hotmail, etc	Yes (with attachment)	Yes (mostly no attachment)
<b>2. Instant Messages</b>		
a. Yahoo Messenger	Yes	Yes (but not file transfer)
b. MSN Messenger	Yes	Yes (but not file transfer)
c. ICQ	Yes	Yes (but not file transfer)
d. AOL	Yes	Yes (but not file transfer)
e. QQ (Chinese ICQ)	Yes	N.A
<b>3. FTP</b>		
a. Upload	Yes	Yes (only log)
b. Download	Yes	Yes (only log)
<b>4. URL / HTTP Browsing (Link)</b>	Yes	Yes
<b>5. HTTP Web Content</b>	Yes	Yes
<b>6. Telnet</b>	Yes (including playback)	N.A.
<b>7. Online Games</b>	Yes	N.A.
<b>8. P2P Communications</b>	Yes	Yes (but less info)
<b>9. HTTPS Content</b>	Yes (Integration with HTTPS/SSL Device)	NO
<b>10. VOIP and Webcam</b>	Yes (MSN and YAHOO)	NO
<b>11. HTTP Download</b>	Yes	N.A

Decision Computer - All rights reserved

2007



# Wired E-Detective superior than other software products

1. Wired E-Detective is a complete appliance (software + hardware) with backup system.
2. Wired E-Detective is network based product (supporting thousands of users) which does not interfere network activities. Unlike other software products, which are normally standalone and supported very small network size. Installing Wired E-Detective is easier than installation other software products.
3. Wired E-Detective comes with powerful management function which includes: search and data mining, reporting, archiving etc which normally can't be found in other software products.



## Q & A

We support remote software update (By Internet Connection)  
and function **customization** based on user requirements

For more information, please visit E-Detective system  
website

[www.ed-system.sg](http://www.ed-system.sg)

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



Contact us at Email: [vincent@decision.com.tw](mailto:vincent@decision.com.tw)

[frankie@decision.com.tw](mailto:frankie@decision.com.tw)



**YOUR Revolutionary Technology for Surveillance and  
Audit of Internet Activities!!**

**Our  
Awards!**



**World  
Recognition!**

**Thank You!!!**

Decision Computer - All rights reserved  
2007

