Decision Computer Group

Network Packet Source Forensic Device

Moving forward with the security of networking and computer forensics

E-DETECTIVE®

DECISION INDUSTRIAL AUTOMATION

Features

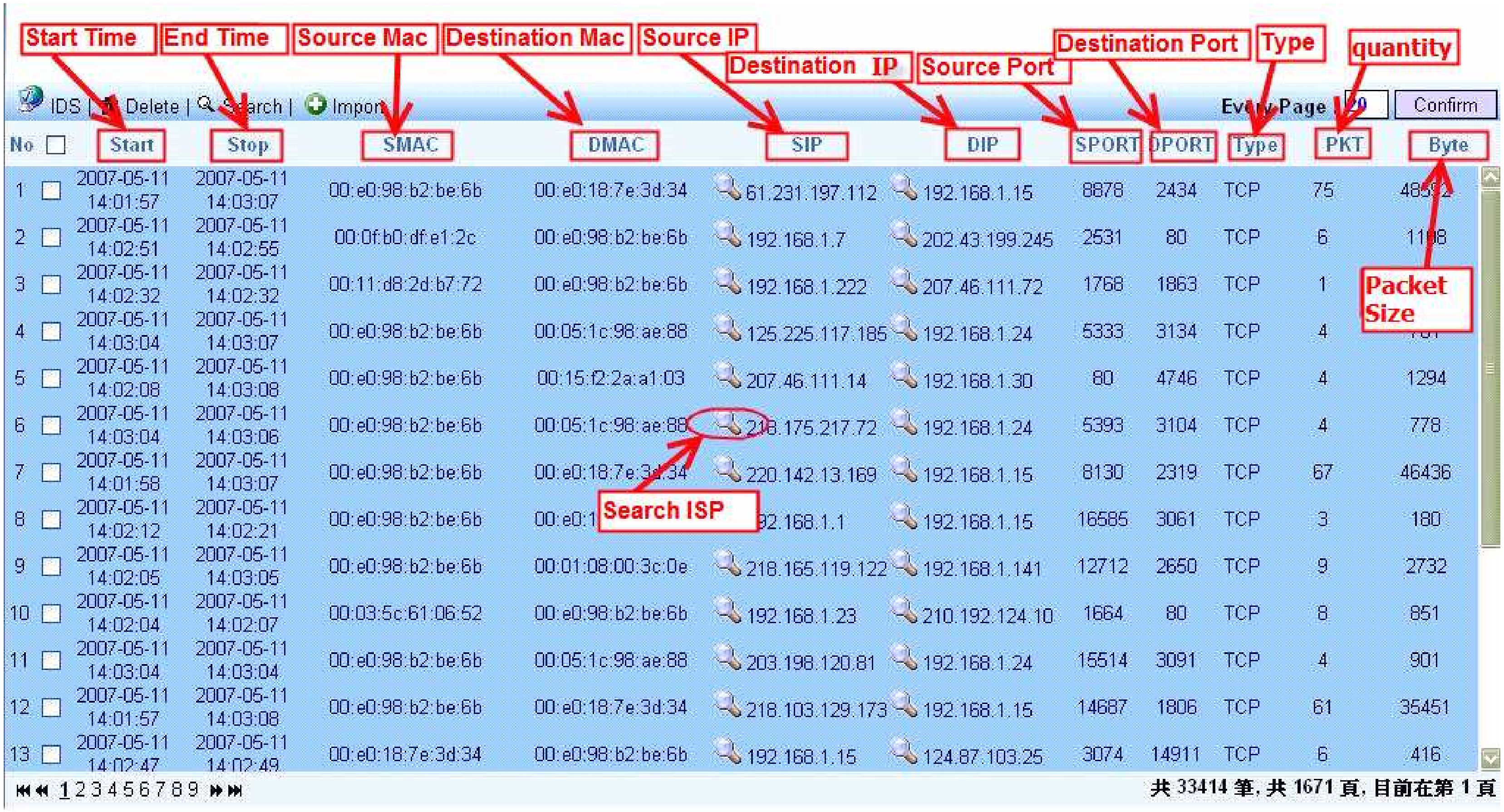
Objective: To trace the source and destination MAC and IP addresses or Internet traffic for analyzing and forensic purpose. With the knowledge of source and destination IP addresses, the location of source and destination IP addresses can be traced.

Classifying and analyzing Internet packets and providing reports of communication protocol for application session.

Report’s info:

1. Port
2. Source MAC and Destination MAC
3. Source IP and Destination IP
4. Packet’s format (UTP/TCP/ICMP)
5. Quantity (Packets)
6. Data Length

User Interface

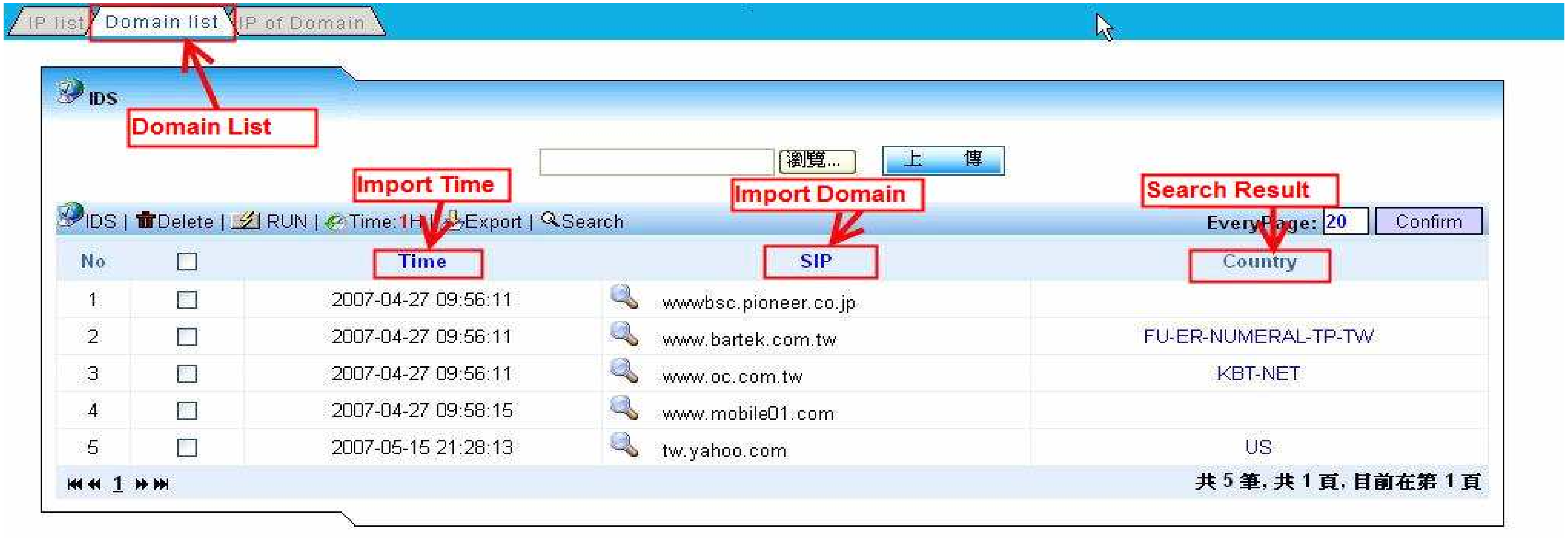


No □	Start	Stop	SMAC	DMAC	SIP	DIP	SPORT	DPORT	Type	PKT	Byte
1 □	2007-05-11 14:01:57	2007-05-11 14:03:07	00:e0:98:b2:be:6b	00:e0:18:7e:3d:34	61.231.197.112	192.168.1.15	8878	2434	TCP	75	[illegible]
2 □	2007-05-11 14:02:51	2007-05-11 14:02:55	00:0f:b0:df:e1:2c	00:e0:98:b2:be:6b	192.168.1.7	202.43.199.245	2531	80	TCP	6	[illegible]
3 □	2007-05-11 14:02:32	2007-05-11 14:02:32	00:11:d8:2d:b7:72	00:e0:98:b2:be:6b	192.168.1.222	207.46.111.72	1768	1863	TCP	1	[illegible]
4 □	2007-05-11 14:03:04	2007-05-11 14:03:07	00:e0:98:b2:be:6b	00:05:1c:98:ae:88	125.225.117.185	192.168.1.24	5333	3134	TCP	4	[illegible]
5 □	2007-05-11 14:02:08	2007-05-11 14:03:08	00:e0:98:b2:be:6b	00:15:f2:2a:a1:03	207.46.111.14	192.168.1.30	80	4746	TCP	4	1294
6 □	2007-05-11 14:03:04	2007-05-11 14:03:06	00:e0:98:b2:be:6b	00:05:1c:98:ae:88	218.175.217.72	192.168.1.24	5393	3104	TCP	4	778
7 □	2007-05-11 14:01:58	2007-05-11 14:03:07	00:e0:98:b2:be:6b	00:e0:18:7e:3d:34	220.142.13.169	192.168.1.15	8130	2319	TCP	67	46436
8 □	2007-05-11 14:02:12	2007-05-11 14:02:21	00:e0:98:b2:be:6b	00:e0:1[illegible]	[illegible]2.168.1.1	192.168.1.15	16585	3061	TCP	3	180
9 □	2007-05-11 14:02:05	2007-05-11 14:03:05	00:e0:98:b2:be:6b	00:01:08:00:3c:0e	218.165.119.122	192.168.1.141	12712	2650	TCP	9	2732
10 □	2007-05-11 14:02:04	2007-05-11 14:02:07	00:03:5c:61:06:52	00:e0:98:b2:be:6b	192.168.1.23	210.192.124.10	1664	80	TCP	8	851
11 □	2007-05-11 14:03:04	2007-05-11 14:03:04	00:e0:98:b2:be:6b	00:05:1c:98:ae:88	203.198.120.81	192.168.1.24	15514	3091	TCP	4	901
12 □	2007-05-11 14:01:57	2007-05-11 14:03:08	00:e0:98:b2:be:6b	00:e0:18:7e:3d:34	218.103.129.173	192.168.1.15	14687	1806	TCP	61	35451
13 □	2007-05-11 14:02:47	2007-05-11 14:02:49	00:e0:18:7e:3d:34	00:e0:98:b2:be:6b	192.168.1.15	124.87.103.25	3074	14911	TCP	6	416

⏮ ⏪ 1 2 3 4 5 6 7 8 9 ⏩ ⏭

共 33414 筆, 共 1671 頁, 目前在第 1 頁

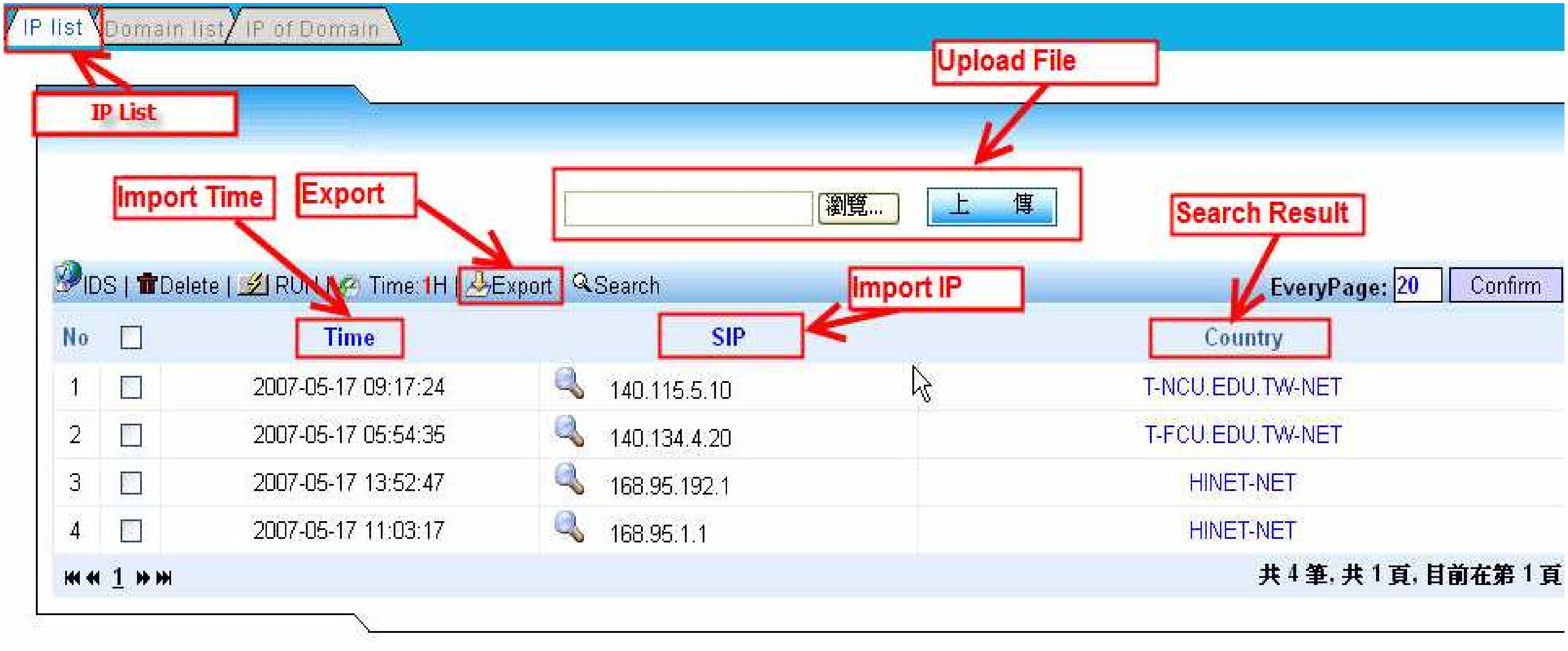
Predefined the relationship between IP and domain, and import this info into the system in order to find out the IP’s domain by IP itself or find out a group of IPs of domain by domain itself.



No	□	Time	SIP	Country
1	□	2007-04-27 09:56:11	wwwbsc.pioneer.co.jp	
2	□	2007-04-27 09:56:11	www.bartek.com.tw	FU-ER-NUMERAL-TP-TW
3	□	2007-04-27 09:56:11	www.oc.com.tw	KBT-NET
4	□	2007-04-27 09:58:15	www.mobile01.com	
5	□	2007-05-15 21:28:13	tw.yahoo.com	US

共 5 筆, 共 1 頁, 目前在第 1 頁

IP and ISP’s related info



No	□	Time	SIP	Country
1	□	2007-05-17 09:17:24	140.115.5.10	T-NCU.EDU.TW-NET
2	□	2007-05-17 05:54:35	140.134.4.20	T-FCU.EDU.TW-NET
3	□	2007-05-17 13:52:47	168.95.192.1	HINET-NET
4	□	2007-05-17 11:03:17	168.95.1.1	HINET-NET

共 4 筆, 共 1 頁, 目前在第 1 頁

Integration with E-Detective system

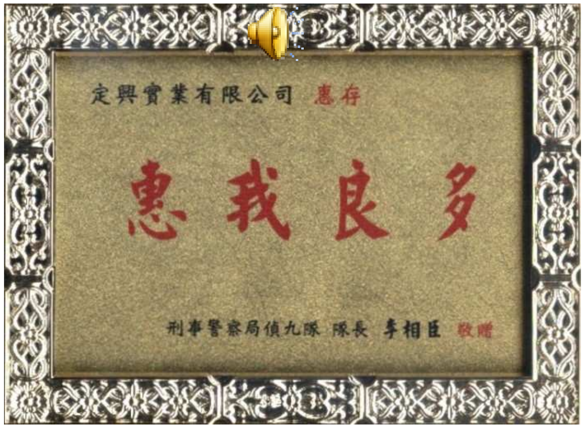
Network Packet Source Forensics Device is able to be integrated with E-DETECTIVE System in order to classify and to analyze internet packets.

E DETECTIVE

Employee Internet Management Appliance

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

Our Awards!



定興實業有限公司 惠存

惠我良多

刑事警察局偵九隊 隊長 李相臣 敬贈

World Recognition!

Thank You!!!

DECISION

INDUSTRIAL AUTOMATION