

P2P 軟體對網路安全的威脅與 封包分析

新波科技

劉楨民

0932-212913, 02-2331-0789

電子郵件 dmliu@ms4.hinet.net

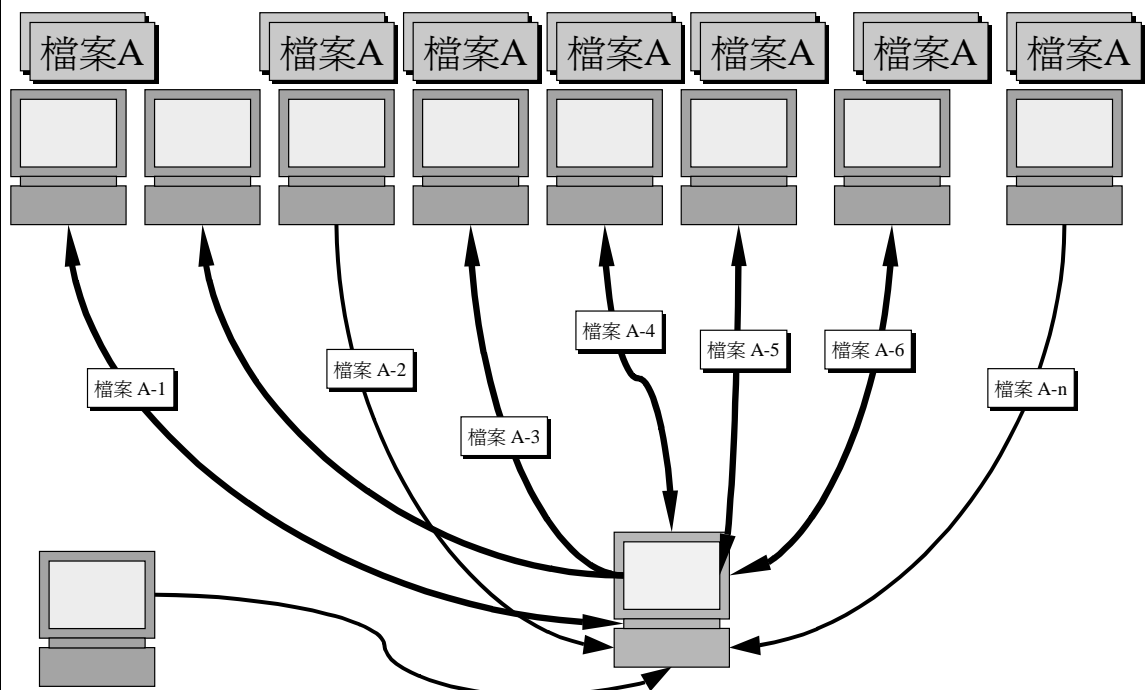
P2P 軟體對網路安全的威脅

- 甚麼是 P2P 軟體？
- P2P軟體的種類
- P2P 軟體可能影響網路安全的問題
- P2P 軟體誤用的漏洞範例
- 偵測 P2P 通訊的方式
- Q&A

甚麼是 P2P 軟體？

- P2P , Peer to Peer, 點對點通訊傳輸工具
- 傳統 HTTP/FTP 傳送檔案方式，採取用戶與主機的通訊模式(Client-Server Mode)
- 新制 P2P 檔案傳送，採取用戶與用戶的通訊模式，P2P傳送檔案的時候，可以同時連接多個下載點，分散式下載檔案。
- P2P可以快速完成檔案下載的目標。
- Skype也是P2P的一種應用工具。

Peer to Peer, 點對點通訊傳輸工具

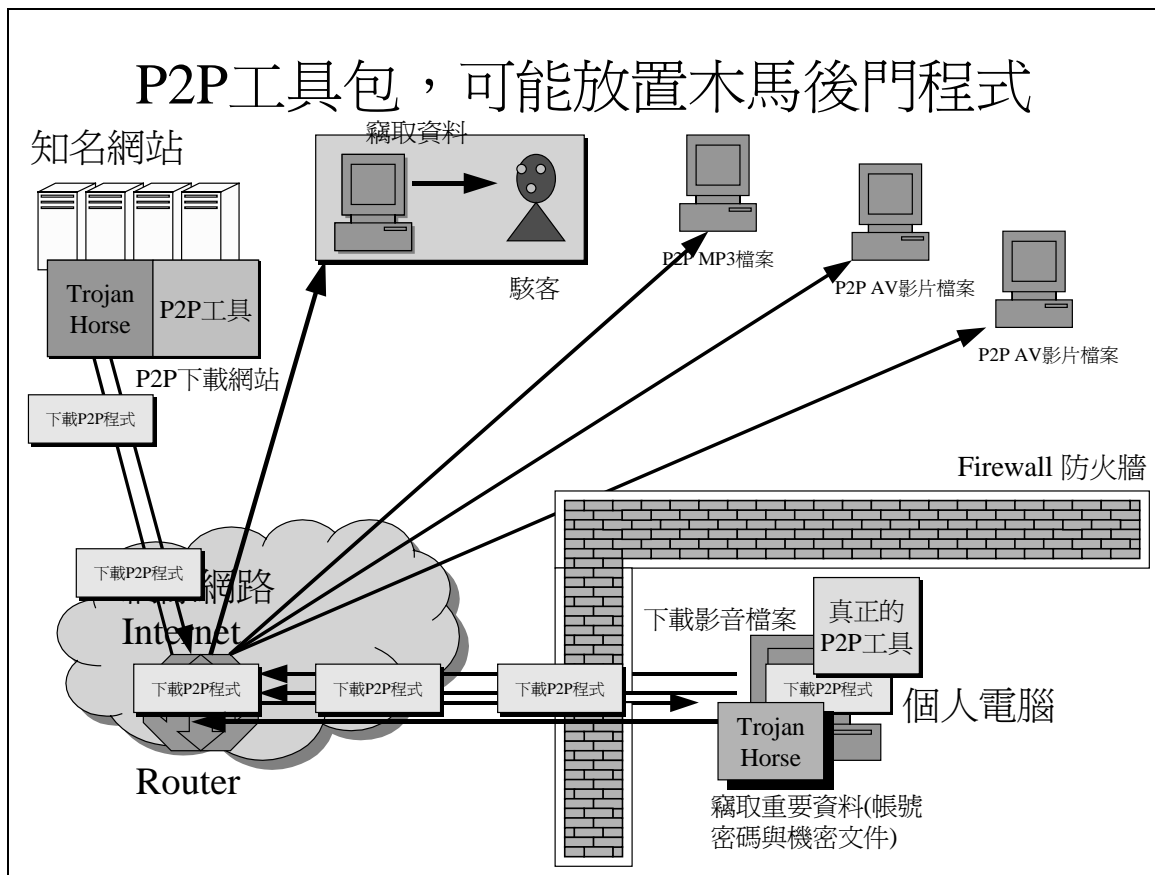


P2P軟體的種類

- BitTorrent系列(BT)，BitTorrent, BitComet, BTspirit、BitTorando等等
- eMule系列，eMule, eDonkey
- GnuTella系列，GnuTella, ezPeer, Mixie,
- FastTrack系列，FastTrack, Kazaa,
- WinMx系列，WinMx, Winny,

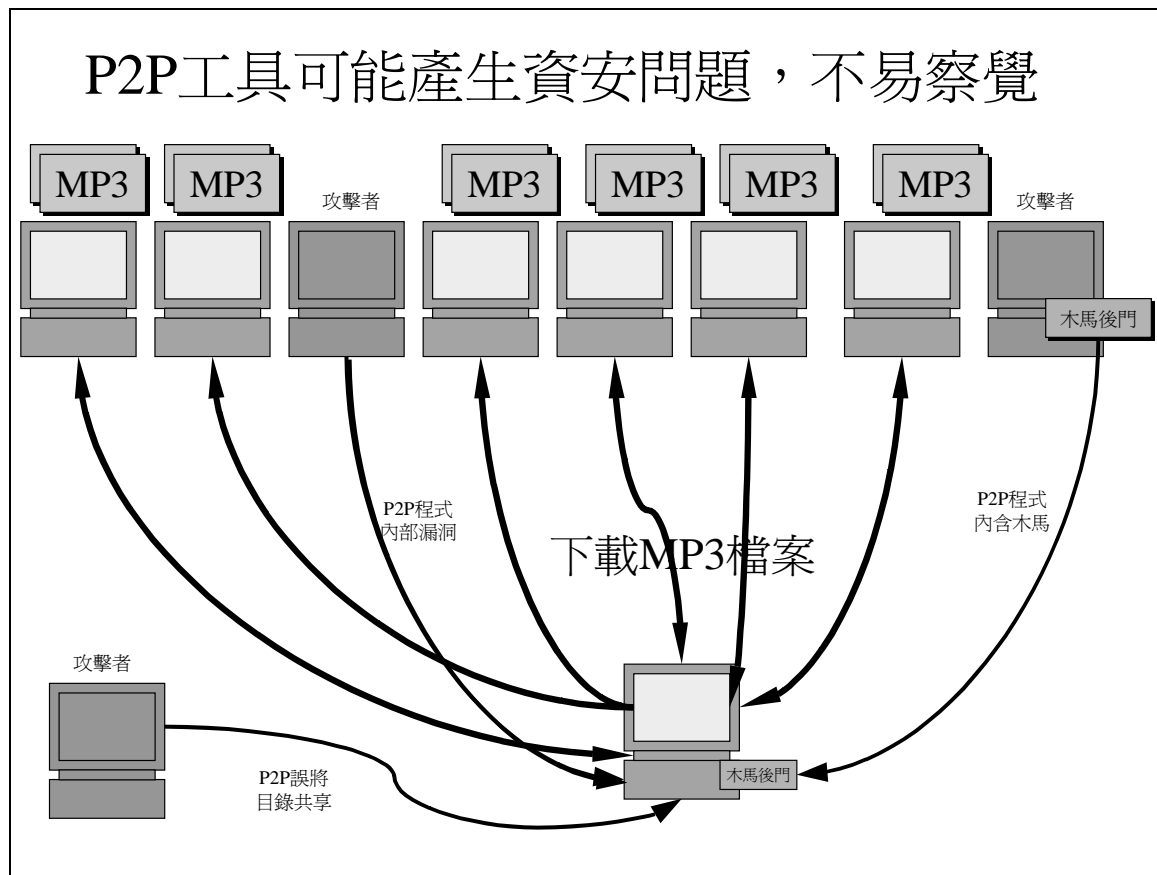
P2P 軟體可能影響網路安全的問題

- P2P工具包，可能被惡意人員放置木馬後門程式，與病毒蠕蟲。
- P2P軟體本身的漏洞，造成駭客入侵。
- 使用P2P軟體時，誤將本機目錄開放共享。
- 使用P2P下載影音檔案，多半為mp3與mpeg, avi等等檔案，可能造成侵權行為。
- 使用P2P下載色情影片，影響正常工作與政府形象。



P2P 軟體可能影響網路安全的問題

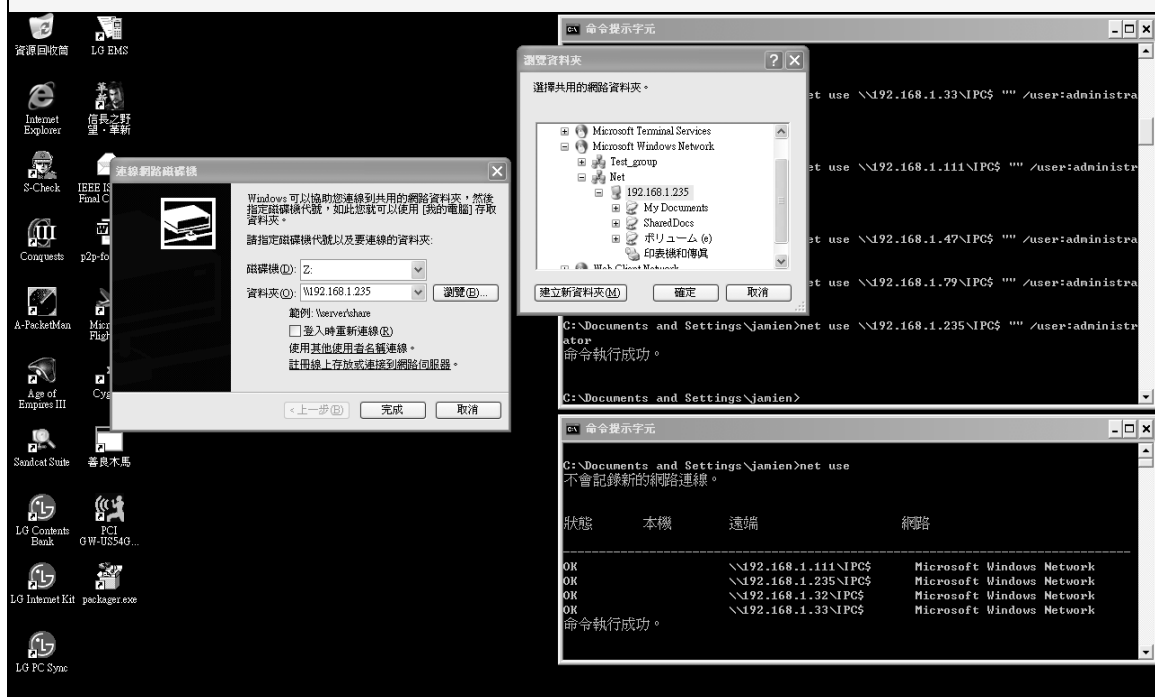
- 使用P2P軟體工具，誤將MyDocument目錄分享出來。
- 如果該主機登入帳號為空密碼(或簡單密碼)，對網路安全會產生立即危險。
- 測試指令 (DOS-Command Line 模式)
 - `net use \\IP位址\IPC$ "" /user:administrator`
- 以下為實際範例。

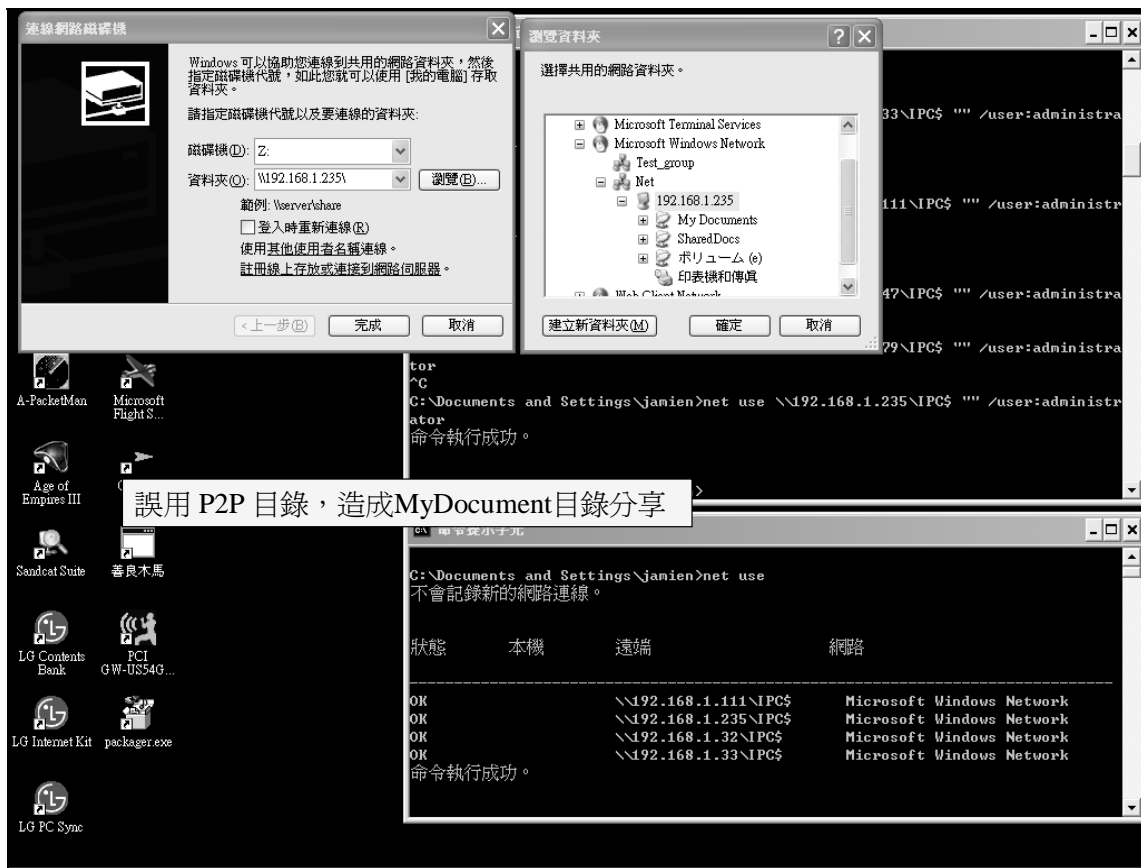




輸入連接指令 `net use \\IP位址\IPC$ "" /user:administrator`

輸入檢視指令 `net use`





如何偵測與阻擋P2P通訊?

- 多數IPS/IDP/UTM軟硬體均號稱可以阻擋(偵測)P2P工具
 - P2P啓始點IP位址阻擋方式。
 - 通訊流量監控方式。
 - 關鍵字詞偵測方式。
- P2P通訊採用動態Port編號，對點IP位址也非固定IP位址。
- 建議學習P2P通訊的封包分析方式
 - 內網IP位址對外網多點IP位址的通訊。
 - 重要通訊特徵(關鍵字詞與下載歌曲名稱)

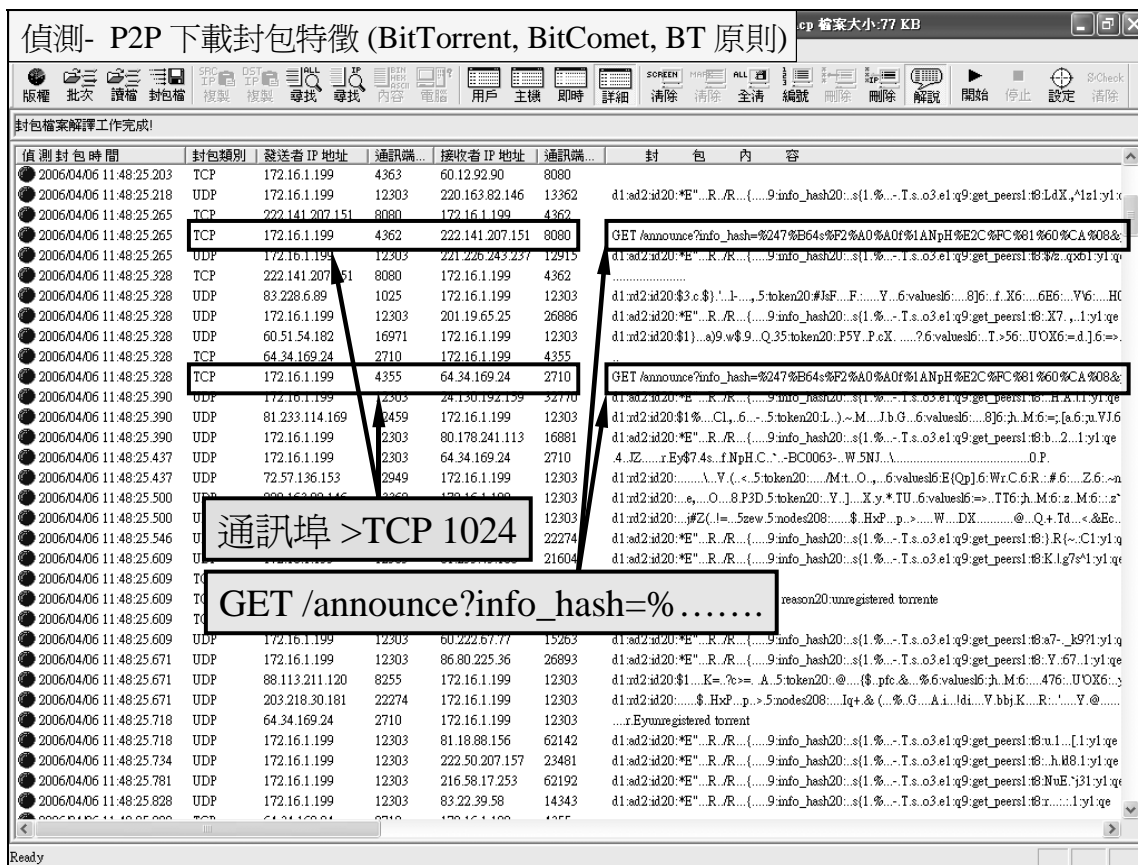
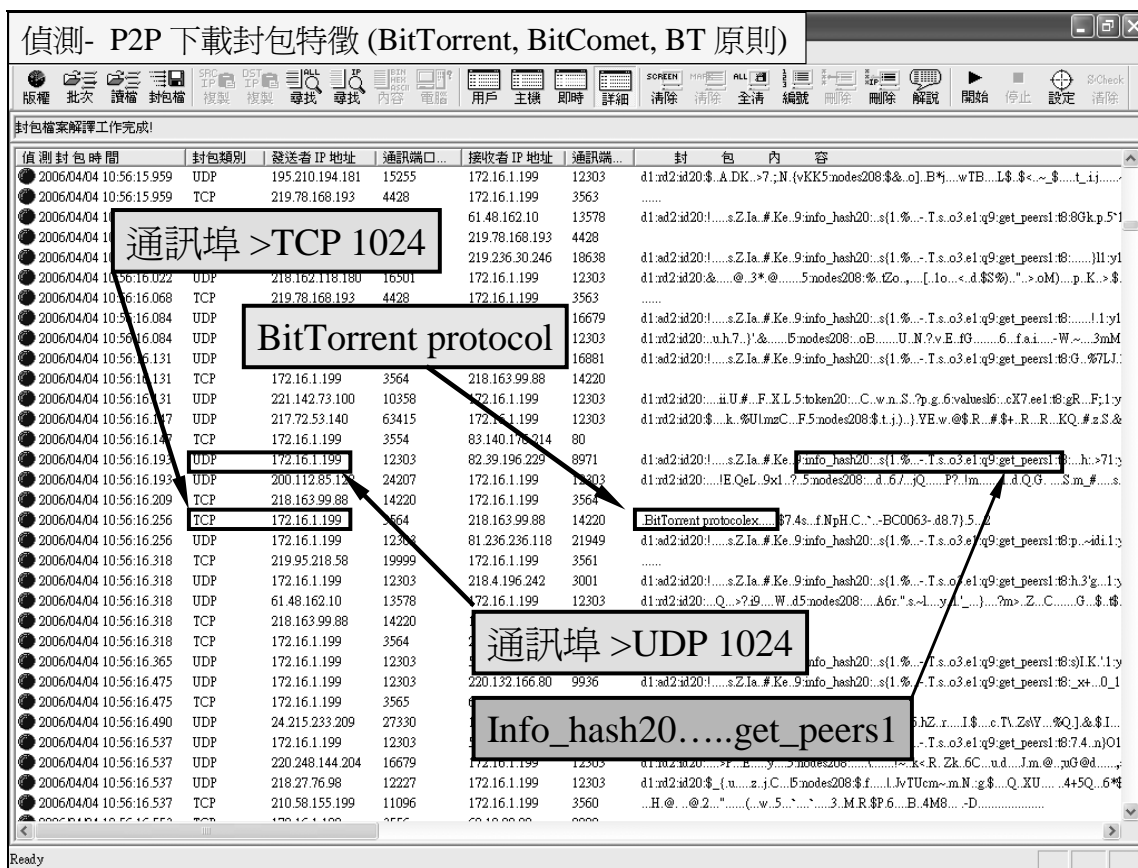
偵測- P2P 通訊封包特徵 (一般通用原則)

封包檔案解譯工作完成!

首次偵測時間	偵測封包時間	封包類...	發送者IP地址	通訊端...	接收者IP地址	通訊端...	封包內容
2006/03/14 09:47:17	2006/03/14 09:47:17	TCP	64.62.194.27	18080	172.16.1.100	1165
2006/03/14 09:47:17	2006/03/14 09:47:17	TCP	172.16.1.100	1165	64.62.194.27	18080
2006/03/14 09:47:20	2006/03/14 09:47:20	TCP	172.16.1.100	1185	218.167.47.218	7884
2006/03/14 09:47:20	2006/03/14 09:47:20	TCP	172.16.1.100	1184	218.171.165.228	7884
2006/03/14 09:47:21	2006/03/14 09:47:21	TCP	218.171.165.228	7884	172.16.1.100	1184
2006/03/14 09:47:35	2006/03/14 09:47:35	TCP	172.16.1.100	1188	59.114.143.50	5100
2006/03/14 09:49:08	2006/03/14 09:49:08	TCP	172.16.1.100	1257	202.86.150.73	12247
2006/03/14 09:49:09	2006/03/14 09:49:09	TCP	172.16.1.100	1258	59.115.232.91	5100
2006/03/14 09:49:10	2006/03/14 09:49:10	TCP	172.16.1.100	1251	140.129.60.62	5100
2006/03/14 09:49:10	2006/03/14 09:49:10	TCP	172.16.1.100	1250	220.139.45.95	7884
2006/03/14 09:49:11	2006/03/14 09:49:11	TCP	172.16.1.100	1253	218.169.84.76	3599
2006/03/14 09:49:13	2006/03/14 09:49:13	TCP	172.16.1.100	1259	61.230.104.61	7890
2006/03/14 09:49:14	2006/03/14 09:49:14	TCP	61.230.104.61	7890	172.16.1.100	1259
2006/03/14 09:49:15	2006/03/14 09:49:15	TCP	61.231.181.122	7884	172.16.1.100	1260
2006/03/14 09:49:16	2006/03/14 09:49:16	TCP	172.16.1.100	1260	61.231.181.122	7884
2006/03/14 09:49:18	2006/03/14 09:49:18	TCP	172.16.1.100	1262	218.174.137.237	7890
2006/03/14 09:49:21	2006/03/14 09:49:21	TCP	172.16.1.100	1261	211.23.128.22	5100
2006/03/14 09:49:22	2006/03/14 09:49:22	TCP	202.139.72.207	5102	172.16.1.100	1263
2006/03/14 09:49:22	2006/03/14 09:49:22	TCP	172.16.1.100	1263	220.139.72.207	5102
2006/03/14 09:49:23	2006/03/14 09:49:23	TCP	172.16.1.100	1264	203.70.2.44	7884
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	172.16.1.100	1270	59.116.170.145	16983
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	59.116.170.145	16983	172.16.1.100	1270
2006/03/14 09:49:24	2006/03/14 09:49:24	TCP	172.16.1.100	1267	61.61.178.163	7890
2006/03/14 09:49:25	2006/03/14 09:49:25	TCP	218.174.137.237	7890	172.16.1.100	1262
2006/03/14 09:49:27	2006/03/14 09:49:27	TCP	59.115.132.77	5100	172.16.1.100	1273
2006/03/14 09:49:27	2006/03/14 09:49:27	TCP	172.16.1.100	1273	59.115.132.77	5100
2006/03/14 09:49:28	2006/03/14 09:49:28	TCP	172.16.1.100	1272	59.116.145.189	7884
2006/03/14 09:49:28	2006/03/14 09:49:28	TCP	172.16.1.100	1271	219.86.27.34	5100
2006/03/14 09:49:30	2006/03/14 09:49:30	TCP	172.16.1.100	1276	61.216.102.188	5100
2006/03/14 09:49:31	2006/03/14 09:49:31	TCP	172.16.1.100	1277	61.217.155.196	5100
2006/03/14 09:49:40	2006/03/14 09:49:40	TCP	172.16.1.100	1279	218.171.113.164	7884
2006/03/14 09:49:44	2006/03/14 09:49:44	TCP	172.16.1.100	1282	210.192.215.52	5100

通訊埠 > TCP 1024

172.16.1.100 單點對外多點



[illegible]

A-PacketMan 偵測 - ezPeer 下載封包特徵

HTTP/1.1 206 Partial Content. Server: mxie 0.6.4.0 (MXIE 1.0.3.0). Content-type: application/octet-stream. Accept-Ranges: bytes. Content-Range: bytes 524288-1048575/3962670. Content-Length: 524288. Connect

偵測封包時間	封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊端...	封包內容
2006/04/10 15:40:12.500	TCP	172.16.1.199	4849	61.60.201.228	5100	GET /uri-res/N2R?um.shal P5S250S5XYRKGZEYE5R2RNMJLULEW55G HTTP/1.1 Host 6
2006/04/10 15:40:12.546	TCP	172.16.1.199	4855	220.139.223.210	5100	
2006/04/10 15:40:12.703	TCP	61.60.201.228	5100	172.16.1.199	4849
2006/04/10 15:40:13.437	TCP	172.16.1.199	4821	59.115.50.188	7884	is=IIWoH
2006/04/10 15:40:13.484	TCP	61.60.201.228	5100	172.16.1.199	4849	HTTP/1.1 206 Partial Content. Server: mxie 0.6.4.0 (MXIE 1.0.3.0). Content-type: application/
2006/04/10 15:40:13.546	TCP	61.60.201.228	5100	172.16.1.199	4849	...v...(k...?O...65Uv9)d...t...Eq...w...Xf...P...Ag...H...b...J...M...3...A...
2006/04/10 15:40:13.546	TCP	61.60.201.228	5100	172.16.1.199	4849	n...z...V...n...p...%VQ...L...Z...r...P...%*Z...e...%QM...%...%...SW...K...M...J...r...W...Z...
2006/04/10 15:40:13.593	TCP	61.60.201.228	5100	172.16.1.199	4849	fj)...Z...70...W...v...w...%...yP[q...V...e...w...c...4...K...Q...o...z...f...i)...2...L...j...i...G...I...
2006/04/10 15:40:13.593	TCP	59.115.50.188	7884	172.16.1.199	4821	
2006/04/10 15:40:13.593	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.656	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.656	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.718	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.765	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.765	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.812	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.812	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.828	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.875	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.921	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.937	TCP	61.60.201.228	5100			
2006/04/10 15:40:13.984	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.031	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.093	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.093	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.140	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.203	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.203	TCP	220.139.223.210	5100			
2006/04/10 15:40:14.250	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.250	TCP	61.60.201.228	5100			
2006/04/10 15:40:14.265	TCP	220.139.223.210	5100			
2006/04/10 15:40:14.265	TCP	59.115.50.188	7884			
2006/04/10 15:40:14.318	TCP	61.60.201.228	5100			

檢視封包資料內容

A-PacketMan 詳細封包資料

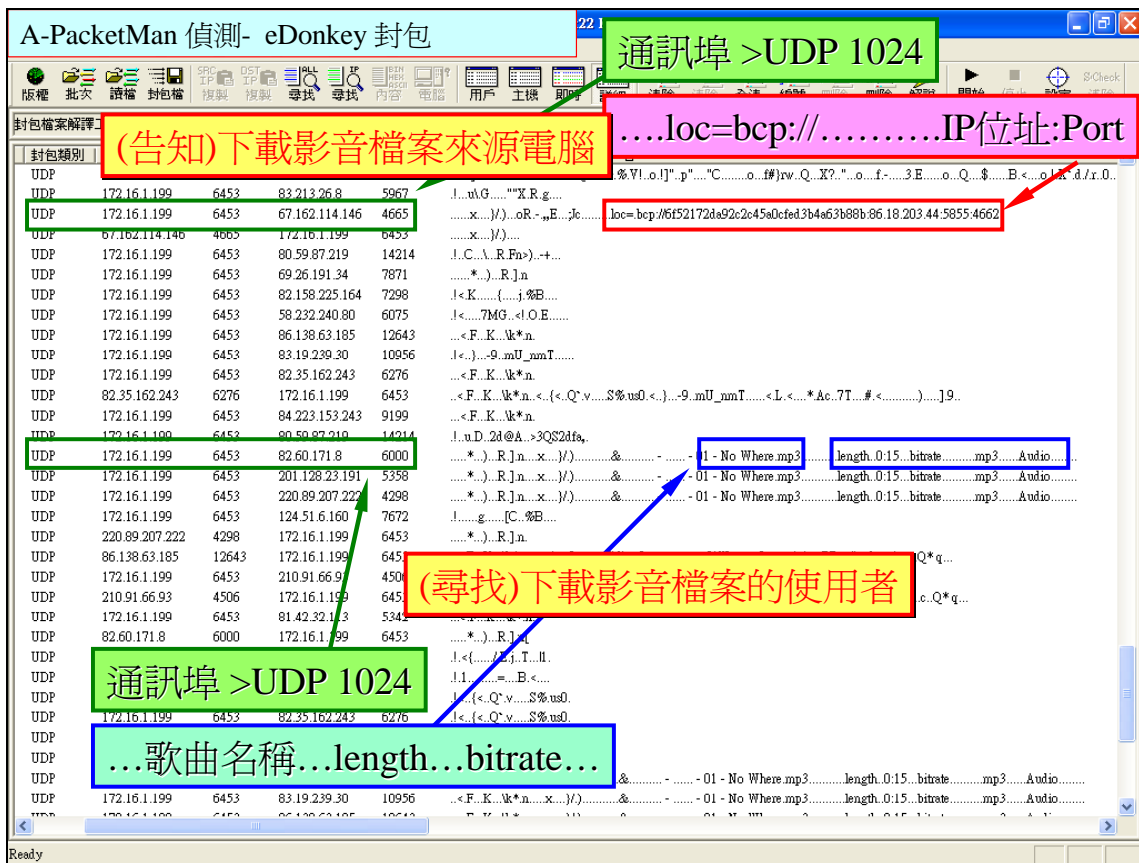
一般偵測資訊

HTTP/1.1 206 Partial Content...

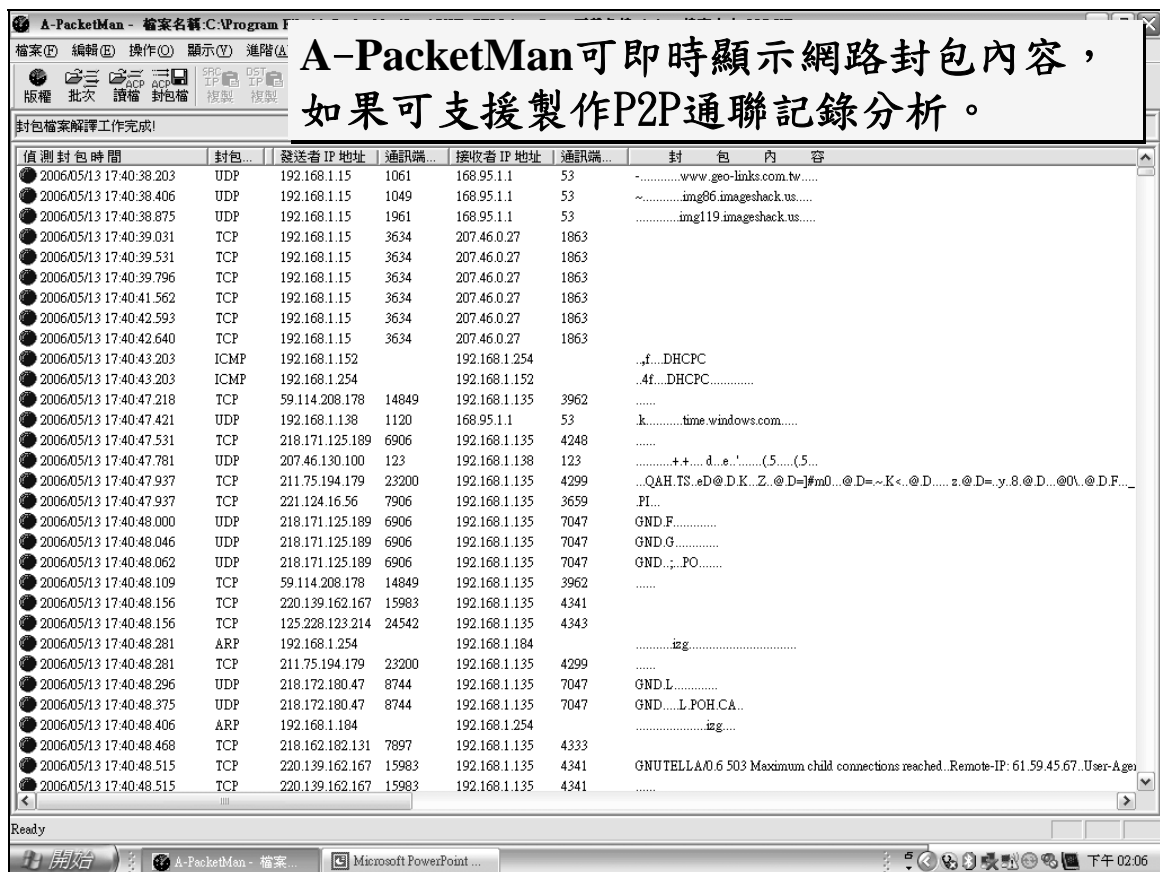
顯示中文碼

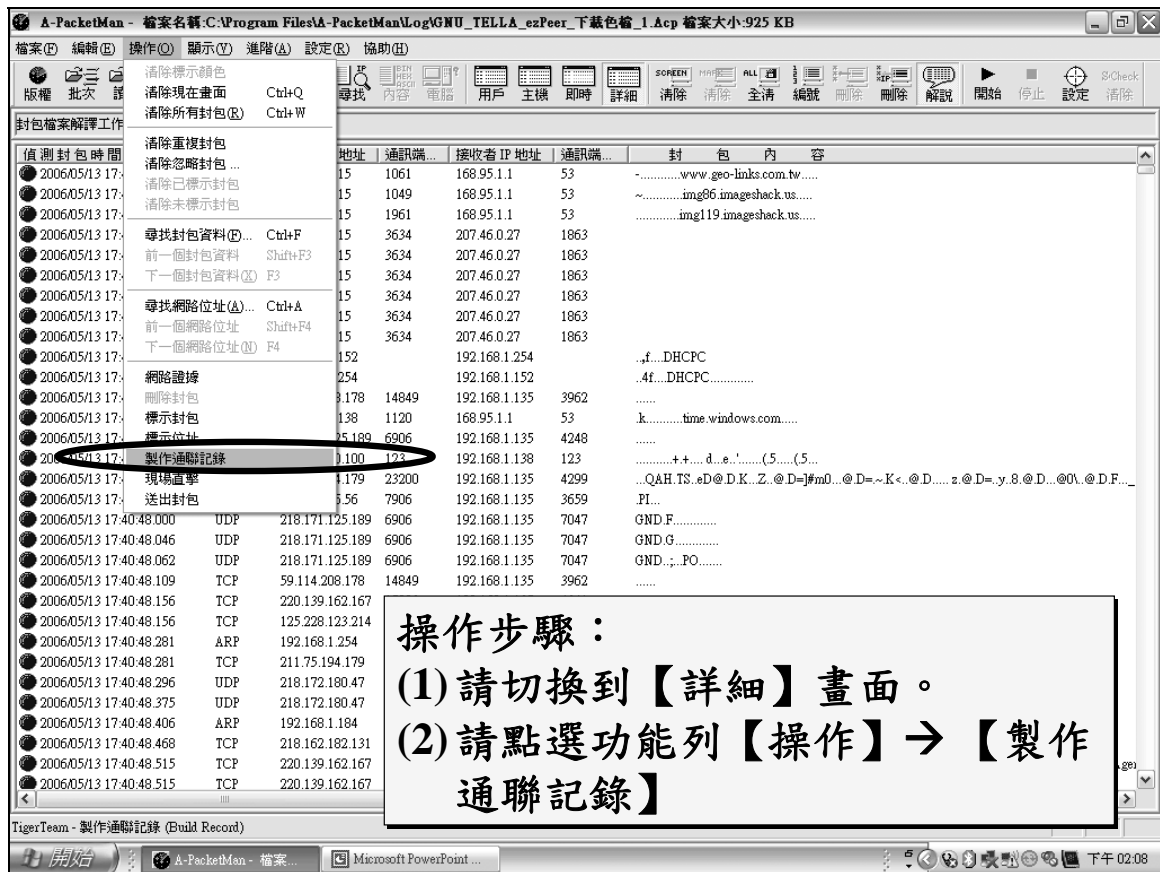
下載歌曲名稱

Addr:	0000	HEX:	00	DEC:	0	BIN:	00000000	OCT:	0	ASCII:	...							
Addr:	02E0	59	52	4B	47	5A	45	59	45	35	52	32	52	4E	4D	4A	4C	YRKGYE5R2RNMJL
	02F0	55	4C	45	57	35	35	47	20	32	30	36						



- P2P軟體會影響網路頻寬甚鉅。T3線路，只要少數人員使用P2P工具，會塞爆網路。
- P2P軟體不易阻擋，因為多數P2P工具會自動變更Port與IP位址。
- 新版本P2P軟體，可能會更刁鑽難纏。
- 使用封包分析工具，可以隨即找出P2P用戶。

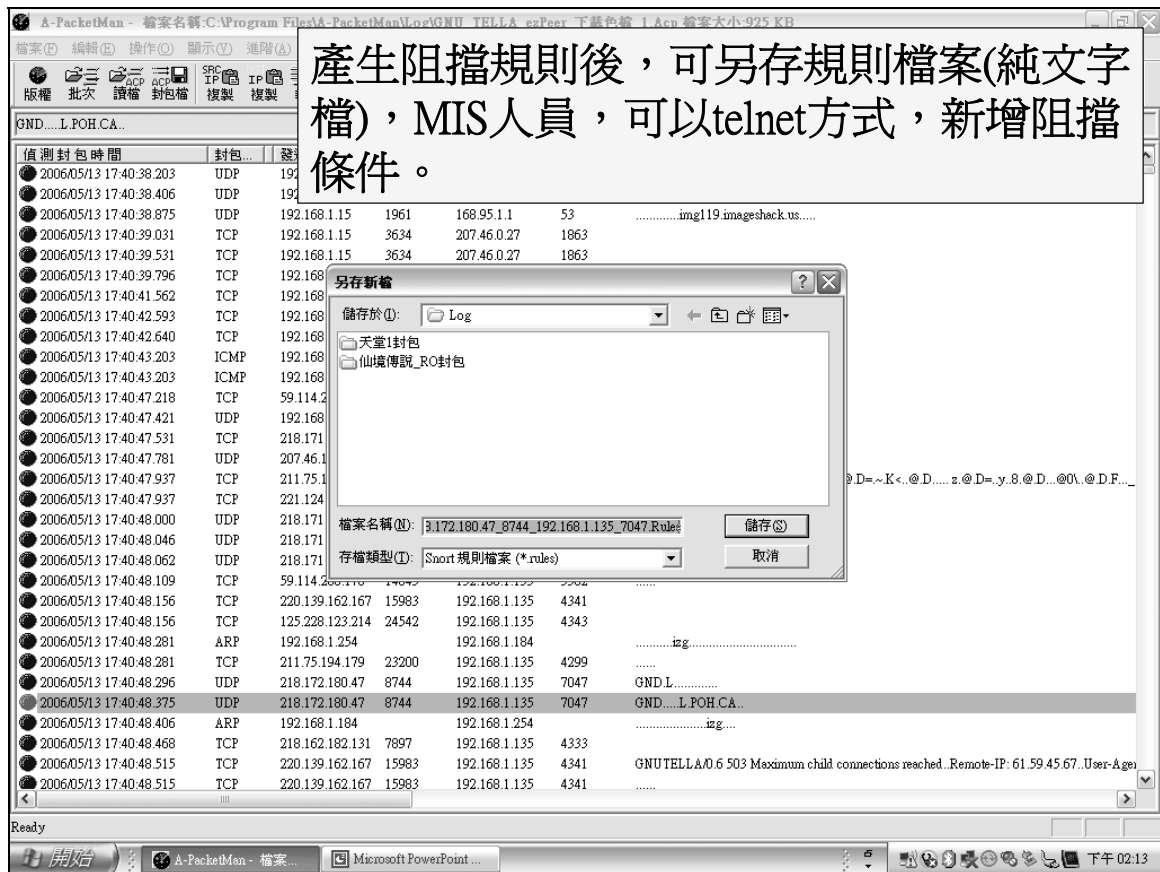




A-PacketMan - 檔案名稱: C:\Program Files\A-PacketMan\Log\GNU_TELLA_ezPeer_下載色包_1.Acp 檔案大小: 925 KB						
P2P通聯記錄分析畫面						
網路封包的通聯記錄已經製作完成，有效記錄 427 個。						
日期-時間	封包類別	發送者 IP 地址	通訊...	接收者 IP 地址	通訊...	封包內容
2006/05/13 17:40:48.000	點對點下載: (未確定)P2P...	218.171.125.189	6906	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:40:48.515	點對點下載: P2P 取得連接...	220.139.162.167	15983	192.168.1.135	4341	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊
2006/05/13 17:40:48.734	點對點下載: (未確定)P2P...	218.175.160.101	23935	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:40:51.312	點對點下載: P2P 正在下載...	218.175.180.185	6158	192.168.1.135	4347	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 C
2006/05/13 17:40:52.656	點對點下載: P2P 取得連接...	218.175.160.101	23935	192.168.1.135	4344	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊
2006/05/13 17:40:52.875	點對點下載: P2P 正在下載...	61.15.84.13	10192	192.168.1.135	4353	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 楊丞琳-遇上愛
2006/05/13 17:40:54.140	點對點下載: P2P 正在下載...	218.175.180.185	6158	192.168.1.135	4347	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 C
2006/05/13 17:40:55.156	點對點下載: P2P 取得連接...	61.30.154.130	17801	192.168.1.135	4300	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊
2006/05/13 17:40:57.359	點對點下載: P2P 傳送自己...	220.131.180.217	18039	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella系列等等, 回應解說: 發送端用
2006/05/13 17:40:58.125	點對點下載: (未確定)P2P...	218.175.160.101	23935	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:41:03.468	點對點下載: P2P 已經完成...	219.68.43.55	4048	192.168.1.135	4372	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [一本道]可愛
2006/05/13 17:41:08.906	點對點下載: P2P 正在下載...	61.216.245.44	22221	192.168.1.135	4360	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3
2006/05/13 17:41:10.546	點對點下載: P2P 變更連接...	211.74.220.204	7884	192.168.1.135	4383	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2
2006/05/13 17:41:11.578	點對點下載: P2P 變更連接...	61.231.250.196	7884	192.168.1.135	4384	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2
2006/05/13 17:41:12.140	點對點下載: P2P 已經完成...	211.75.121.44	5100	192.168.1.135	4381	工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3
2006/05/13 17:41:12.765	點對點下載: P2P 已經完成...	218.184.36.194	5100	192.168.1.135	4374	工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本(B
2006/05/13 17:41:14.140	點對點下載: P2P 變更連接...	218.170.194.5	7884	192.168.1.135	4212	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2
2006/05/13 17:41:16.781	點對點下載: P2P 正在下載...	221.126.138.27	11160	192.168.1.135	4400	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西
2006/05/13 17:41:18.156	點對點下載: P2P 正在下載...	219.71.97.202	9335	192.168.1.135	4387	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西
2006/05/13 17:41:19.734	點對點下載: P2P 變更連接...	59.120.78.236	5100	192.168.1.135	4401	工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2
2006/05/13 17:41:20.250	點對點下載: (未確定)P2P...	218.170.207.55	24579	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:41:20.812	點對點下載: P2P 正在下載...	61.217.89.81	14078	192.168.1.135	4405	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3
2006/05/13 17:41:21.234	點對點下載: P2P 正在下載...	219.71.97.202	9335	192.168.1.135	4387	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西
2006/05/13 17:41:22.562	點對點下載: P2P 正在下載...	218.167.188.251	4626	192.168.1.135	4412	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 C
2006/05/13 17:41:28.140	點對點下載: (未確定)P2P...	125.228.123.214	24542	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:41:29.531	點對點下載: P2P 已經完成...	60.244.60.149	7719	192.168.1.135	4431	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記-2
2006/05/13 17:41:29.578	點對點下載: P2P 已經完成...	125.228.213.170	5100	192.168.1.135	4441	工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本(B
2006/05/13 17:41:30.296	點對點下載: (未確定)P2P...	125.228.123.214	24542	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告
2006/05/13 17:41:31.453	點對點下載: P2P 已經完成...	220.140.18.25	5100	192.168.1.135	4424	工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 C
2006/05/13 17:41:31.578	點對點下載: P2P 已經完成...	61.225.166.208	18643	192.168.1.135	4452	工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3
2006/05/13 17:41:31.781	點對點下載: (未確定)P2P...	218.170.207.55	24579	192.168.1.135	7047	工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告

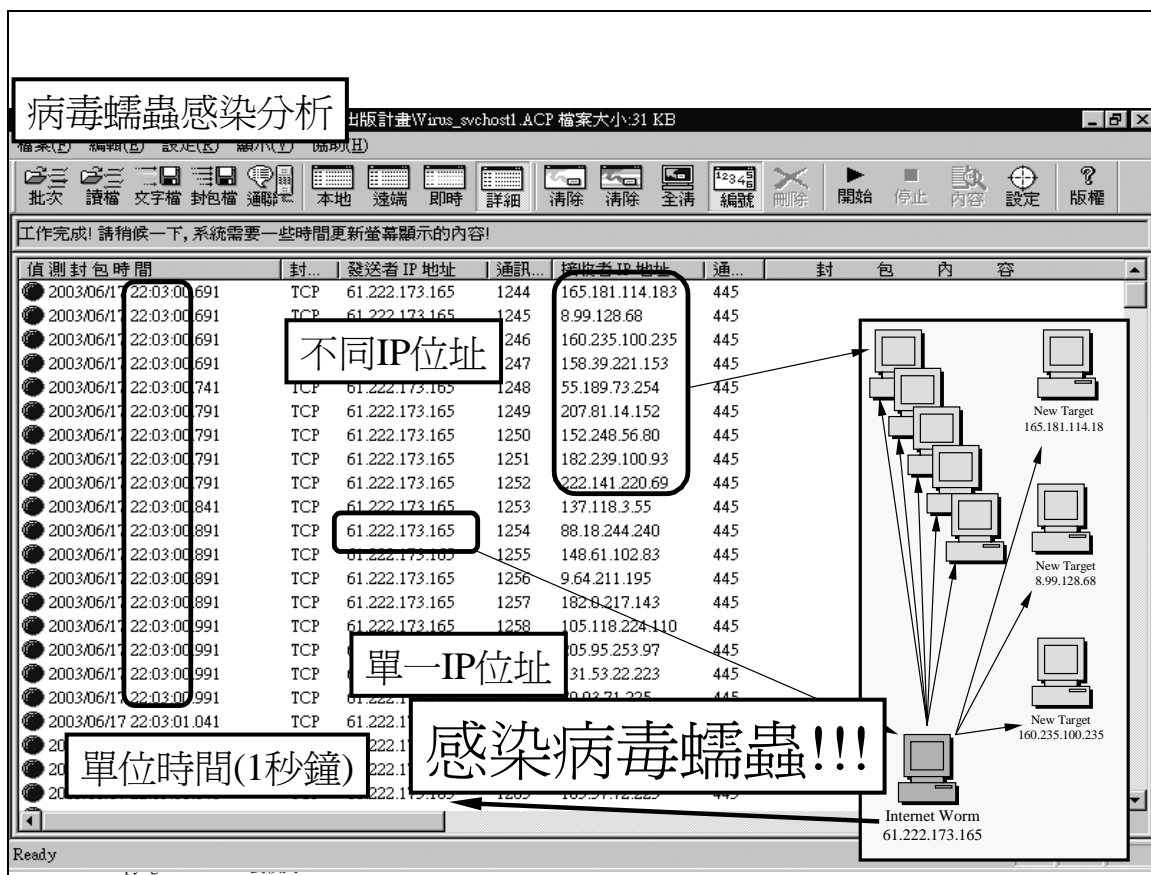
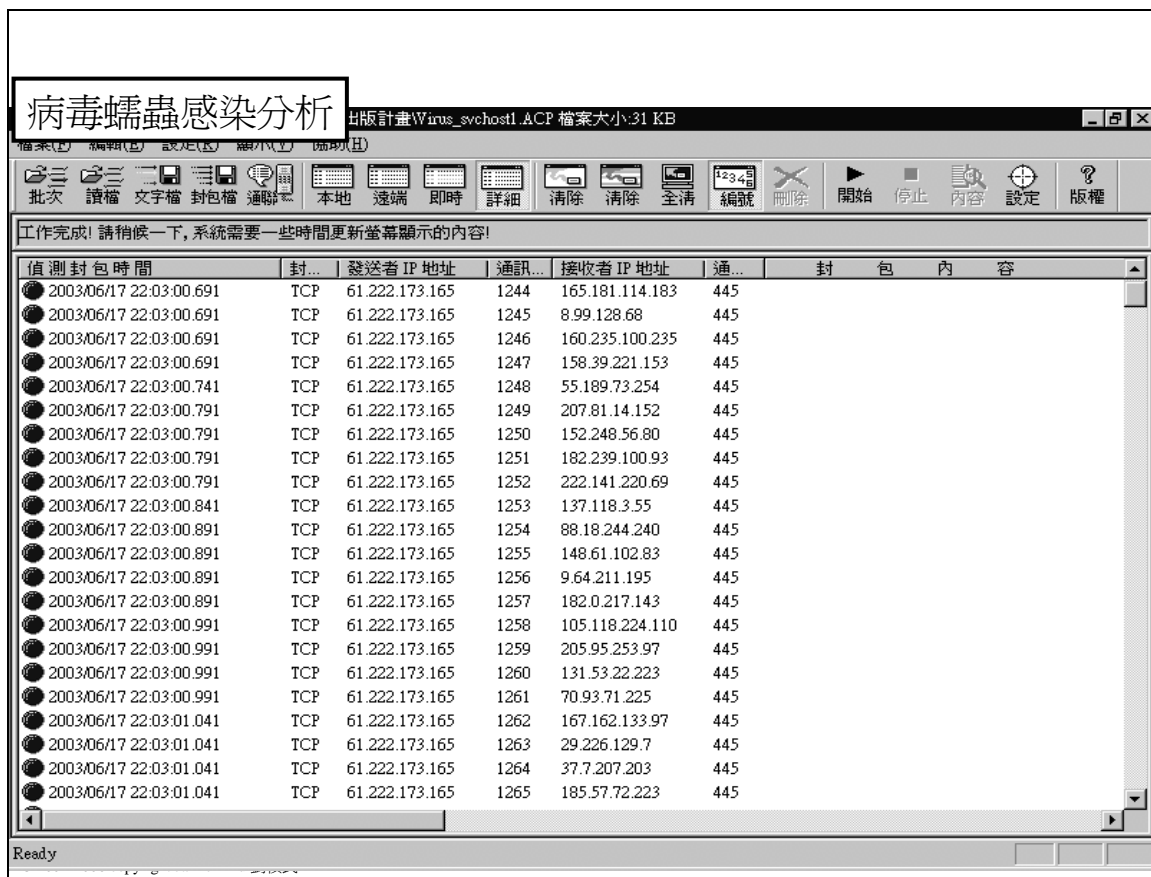
A-PacketMan - 檔案名稱: C:\Program Files\A-PacketMan\Log\GNU_TELLA_ezPeer_下載色包_1.Acp 檔案大小: 925 KB						
可分析該IP位置之異常狀況，並將P2P下載的影音檔案名稱，解譯為中文檔案名稱。						
網路封包的通聯記錄已經製作完成，有效記錄 427 個。						
封包內容						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應解說: P2P用戶回應訊息。 Maximum child connections reached						
工具名稱: Mxie,Foxy,ezPeer,GnuTella系列等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點。						
工具名稱: Mxie,Foxy,ezPeer,GnuTella系列等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點(單查封包未確定，需參考前後封包內容)。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [一本道]可愛小女生隔台臥室被玩弄.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本(破碼版56分鐘)觀月雛乃.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西密碼 1.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西密碼.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點(單查封包未確定，需參考前後封包內容)。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版 1.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: [電影]連文西密碼.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點(單查封包未確定，需參考前後封包內容)。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記-2-驚中-國語發音 2.mpeg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: A影片-日本(破碼版56分鐘)觀月雛乃.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點(單查封包未確定，需參考前後封包內容)。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2 CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 不可能任務3急速搶先版.mvb, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,Foxy,ezPeer,GnuTella等等, 回應解說: 發送端用戶告知其他P2P用戶，自己為P2P下載端點(單查封包未確定，需參考前後封包內容)。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2-冰河世紀CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記-2-驚中-國語發音 2.mpeg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2-冰河世紀CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						
工具名稱: Foxy,ezPeer,GnuTella系列等等, 檔案名稱: 冰原歷險記2-冰河世紀CD1.mpg, 回應解說: P2P用戶下載影片音樂檔案。						
工具名稱: Mxie,ezPeer,GnuTella系列等等, 回應內容: 回應解說: P2P被下載端已經滿載，或是僅有部份檔案可以下載，請與其他IP位址重新下載檔案。						





A-PacketMan 的應用範例

- 病毒蠕蟲感染分析
- 木馬後門通訊分析
- 使用者異常行為分析
- 網路攻擊行為分析
- 資料庫通訊分析



病毒蠕蟲感染分析 (TCP-1025, TCP-1026, TCP-1027, TCP-135, TCP-137)

GET /HTTP/1.1...Accept: image/gif, image/x-bitmap, image/jpeg, image/png, image/pipe; /*.User-Agent: Mozilla/4.0 (compatible; MSIE 5.5; Windows 98).Host: 211.21.41.114

偵測封包時間	封包類別	發送者 IP 地址	通訊...	接收者 IP 地址	通訊...	封包內容
2004/04/27 13:24:31.620	TCP	218.238.208.216	4737	211.21.41.114	80	SEARCH /HTTP/1.1.Host: 211.21.41.114...
2004/04/27 13:24:31.630	TCP	211.21.41.114	80	218.238.208.216	4737	HTTP/1.1 404 Object Not Found..Server: Mic
2004/04/27 13:24:31.640	TCP	211.21.41.114	80	218.238.208.216	4737	
2004/04/27 13:25:34.140	TCP	211.21.41.114	3670	146.246.179.3	80	G
2004/04/27 13:25:34.400	TCP	146.246.179.3	80	211.21.41.114	3670
2004/04/27 13:25:36.513	TCP	211.104.124.148	1369	211.21.41.114	2745	
2004/04/27 13:25:36.513	TCP	211.104.124.148	1375	211.21.41.114	6129	
2004/04/27 13:25:37.284	TCP	211.104.124.148	1375	211.21.41.114	6129	
2004/04/27 13:25:37.294	TCP	211.104.124.148	1369	211.21.41.114	2745	
2004/04/27 13:25:37.955	TCP	211.104.124.148	1375	211.21.41.114	6129	
2004/04/27 13:25:37.955	TCP	211.104.124.148	1369	211.21.41.114	2745	
2004/04/27 13:25:39.427	TCP	211.104.124.148	1371	211.21.41.114	1025	
2004/04/27 13:25:39.678	TCP	211.104.124.148	1371	211.21.41.114	1025
2004/04/27 13:25:49.702	TCP	211.104.124.148	1371	211.21.41.114	1025H.....F.....]
2004/04/27 13:25:49.712	TCP	211.21.41.114	1025	211.104.124.148	1371<.....1025.....
2004/04/27 13:25:50.023	TCP	211.104.124.148	1371	211.21.41.114	1025X.....@.....2\$X..EdI.p.t..^A...
2004/04/27 13:25:50.083	TCP	211.104.124.148	1371	211.21.41.114	1025	...JW...Yo...<...JW...Yg...Yo...<...JWS...Y
2004/04/27 13:25:50.093	TCP	211.21.41.114	1025	211.104.124.148	1371	...#.....
2004/04/27 13:25:50.303	TCP	211.104.124.148	1371	211.21.41.114	1025
2004/04/27 13:25:50.303	TCP	211.21.41.114	1025	211.104.124.148	1371
2004/04/27 13:25:50.553	TCP	211.104.124.148	1371	211.21.41.114	1025
2004/04/27 13:26:04.073	TCP	211.21.41.114	2524	146.246.40.64	80	G
2004/04/27 13:26:51.641	TCP	211.21.41.114	1160	134.252.141.223	80	G
2004/04/27 13:26:51.892	TCP	134.252.141.223	80	211.21.41.114	1160
2004/04/27 13:27:00.267	TCP	211.21.41.114	1267	124.147.12.26	80

木馬後門通訊分析 (IRC聊天室木馬, 屬於BotNet的一種)

PING :TheSlayer.Is.Back.Com..

偵測封包時間	封包...	發送者 IP 地址	通訊...	接收者 IP 地址	通訊...	封包內容
2005/04/02 23:27:41.877	UDP	218.42.208.21	1030	61.222.173.164	137CKAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.....]
2005/04/02 23:31:15.634	ARP	61.222.173.161		61.222.173.164	Y]...=?ad=.....
2005/04/02 23:31:15.634	UDP	61.222.173.164	1044	168.95.1.1	53	iw.....time.windows.com.....
2005/04/02 23:31:15.684	UDP	61.222.173.164	25438	61.222.173.161	1900	M-SEARCH *HTTP/1.1.HOST: 239.255.255.250:1900.MAN: "ssdp:discover".MX: 2.ST: urn
2005/04/02 23:31:16.035	UDP	168.95.1.1	53	61.222.173.164	1044	iw.....time.windows.com.....d.windows.com.....nsl.msft.net.2.....ns2.M.2.....
2005/04/02 23:31:16.085	UDP	61.222.173.164	123	207.46.130.100	1234n.....
2005/04/02 23:31:16.285	UDP	207.46.130.100	123	61.222.173.164	123U+...1M.m...4n...4...g3.4...g3
2005/04/02 23:31:17.286	UDP	61.222.173.164	1044	168.95.1.1	53	2t.....cstrikededi.page.us.....
2005/04/02 23:31:17.387	UDP	61.222.173.164	1052	168.95.1.1	53	bu.....defaced.xuma.nl.....
2005/04/02 23:31:17.437	UDP	168.95.1.1	53	61.222.173.164	1052	bu.....defaced.xuma.nl.....c.H.\xuma.nl.....7...ns2.xumaservers.com.1.....7...nsl.H.
2005/04/02 23:31:17.587	UDP	168.95.1.1	53	61.222.173.164	1044	2t.....cstrikededi.page.us.....#..B.....#..B.....#..k.page.us.....NSO.DNSMAI
2005/04/02 23:31:17.787	TCP	61.222.173.164	1053	72.20.18.92	5734	NICK [MSA]-78430.USER cltq 0 0 [MSA]-78430..
2005/04/02 23:31:18.088	TCP	61.222.173.164	1054	66.197.233.165	30591	NICK [bah]47039428.USER ekvizehocu 0 0 [bah]47039428..
2005/04/02 23:31:18.388	TCP	66.197.233.165	30591	61.222.173.164	1054	irc.black7.net NOTICE AUTH :Looking up the hostname for 61.222.173.164....
2005/04/02 23:31:18.989	TCP	66.197.233.165	30591	61.222.173.164	1054	irc.black7.net NOTICE AUTH :Successfully resolved your IP to 61-222-173-164.HINET-IP.hin
2005/04/02 23:31:23.796	TCP	72.20.18.92	5734	61.222.173.164	1053	TheSlayer.Is.Back.Com.001 [MSA]-78430 :Welcome to the TheSlayer IRC Network [MSA]-78
2005/04/02 23:31:23.796	TCP	72.20.18.92	5734	61.222.173.164	1053	TheSlayer.Is.Back.Com.252 [MSA]-78430 5 :operator(s) online..TheSlayer.Is.Back.Com.253 [
2005/04/02 23:31:23.856	TCP	61.222.173.164	1053	72.20.18.92	5734	USERHOST [MSA]-78430..
2005/04/02 23:31:24.056	TCP	72.20.18.92	5734	61.222.173.164	1053	Is.Back.Com.372 [MSA]-78430 :- re violating code 431.322.12 of the Internet Privacy ...TheSl
2005/04/02 23:31:24.056	TCP	61.222.173.164	1053	72.20.18.92	5734	MODE [MSA]-78430 +i JOIN #woei r00t.USERHOST [MSA]-78430.MODE [MSA]-78430 +i
2005/04/02 23:31:24.357	TCP	72.20.18.92	5734	61.222.173.164	1053	TheSlayer.Is.Back.Com.302 [MSA]-78430 :[MSA]-78430=cltq@61.222.173.164 ..
2005/04/02 23:31:24.757	TCP	72.20.18.92	5734	61.222.173.164	1053	[MSA]-78430:cltq@61.222.173.164 JOIN #woei..TheSlayer.Is.Back.Com.332 [MSA]-78430
2005/04/02 23:31:25.168	UDP	61.222.173.164	1052	168.95.1.1	53	r.....www.ringtone.net.....
2005/04/02 23:31:26.169	UDP	61.222.173.164	1052	168.95.1.1	53	r.....www.ringtone.net.....
2005/04/02 23:31:26.219	UDP	168.95.1.1	53	61.222.173.164	1052	r.....www.ringtone.net.....M..H.n.ringtone.net.....nsl.darknameservers.com.
2005/04/02 23:31:30.726	UDP	168.95.1.1	53	61.222.173.164	1052	r.....www.ringtone.net.....H..n.....nsl.darknameservers.com.....ns2.E.A.
2005/04/02 23:31:32.478	TCP	66.197.233.165	30591	61.222.173.164	1054	irc.black7.net 001 [bah]47039428 :Welcome to the Internet Relay Chat network, [bah]4703942
2005/04/02 23:31:32.528	TCP	61.222.173.164	1054	66.197.233.165	30591	USERHOST [bah]47039428..
2005/04/02 23:31:32.779	TCP	66.197.233.165	30591	61.222.173.164	1054	irc.black7.net 009 [bah]47039428 ASCII :Current character mapping...[bah]47039428!-ekvize
2005/04/02 23:31:32.779	TCP	61.222.173.164	1054	66.197.233.165	30591	MODE [bah]47039428 -x+1 JOIN #news0r## p00p0r.USERHOST [bah]47039428.MODE [
2005/04/02 23:31:33.079	TCP	66.197.233.165	30591	61.222.173.164	1054	irc.black7.net 302 [bah]47039428 :[bah]47039428!-ekvizehocu@UQ99-328-103-239.HINE
2005/04/02 23:31:33.530	TCP	66.197.233.165	30591	61.222.173.164	1054	[bah]47039428!-ekvizehocu@61-222-173-164.HINET-IP.hinet.netMODE [bah]47039428 -x

使用者異常行為分析

檔案(F) 編輯(E) 檢視(V) 設定(S) 網路(N) 幫助(H)

批次 讀檔 文字檔 封包檔 本地 遠端 即時 詳細 清除 清除 全清 編號 刪除 開始 停止 內容 設定 版權

工作完成!

偵測封包時間	封包類別	發送者 IP 地址	通訊端口編號	接收者 IP 地址	通訊...	封包內容
2004/07/01 08:26:50.714	TCP	172.16.103.80	3574	172.74.2.82	1025	
2004/07/01 08:26:50.717	TCP	172.16.14.181	2234	220.134.9.8	6885	...aLE.V.. "R...JR" ...`.....}.....p.....r
2004/07/01 08:26:50.717	TCP	172.16.14.181	2234	220.134.9.8	6885	...Zo`.....I.x3...B.q.P0...\$%.x.TL#;
2004/07/01 08:26:50.724	TCP	213.84.35.17	31371	172.16.18.156	1552	...s.A.N.-q3^4...l.8>Cnd.a.KJ\$g.v
2004/07/01 08:26:50.730	ICMP	172.16.106.27		81.84.34.11		...u.H.....
2004/07/01 08:26:50.732	ICMP	210.69.253.14		172.16.106.27		...E.k.....j.QT"...u.H
2004/07/01 08:26:50.736	TCP	61.231.142.223	2083	172.16.15.245	8150	?...jgf.K.wK.E.Fj6,b.....s.-yA.\$;*;
2004/07/01 08:26:50.737	ICMP	172.16.15.37		61.120.175.54		...SoftEther Keep-Alive Packet
2004/07/01 08:26:50.740	TCP	172.16.15.245	8150	193.167.201.10	4353
2004/07/01 08:26:50.743	TCP	172.16.13.36	4614	172.49.184.165	1025	
2004/07/01 08:26:50.744	TCP	172.16.14.22	1929	69.20.74.193	6667	
2004/07/01 08:26:50.745	TCP	172.16.13.36	4618	172.49.184.165	3410	
2004/07/01 08:26:50.746	TCP	172.16.13.36	4619	172.49.184.165	5554	

Ready NUM

© 2004-2006 copyright Jamien Liu 劉楨民

使用者異常行為分析

檔案(F) 編輯(E) 檢視(V) 設定(S) 網路(N) 幫助(H)

批次 讀檔 文字檔 封包檔 本地 遠端 即時 詳細 清除 清除 全清 編號 刪除 開始 停止 內容 設定 版權

工作完成!

偵測封包時間	封包類別	發送者 IP 地址	通訊端口編號	接收者 IP 地址	通訊...	封包內容
2004/07/01 08:26:50.714	TCP	172.16.103.80	3574	172.74.2.82	1025	
2004/07/01 08:26:50.717	TCP	172.16.14.181	2234	220.134.9.8	6885	...aLE.V.. "R...JR" ...`.....}.....p.....r
2004/07/01 08:26:50.717	TCP	172.16.14.181	2234	220.134.9.8	6885	...Zo`.....I.x3...B.q.P0...\$%.x.TL#;
2004/07/01 08:26:50.724	TCP	213.84.35.17	31371	172.16.18.156	1552	...s.A.N.-q3^4...l.8>Cnd.a.KJ\$g.v
2004/07/01 08:26:50.730	ICMP	172.16.106.27		81.84.34.11		...u.H.....
2004/07/01 08:26:50.732	ICMP	210.69.253.14		172.16.106.27		...E.k.....j.QT"...u.H
2004/07/01 08:26:50.736	TCP	61.231.142.223	2083	172.16.15.245	8150	?...jgf.K.wK.E.Fj6,b.....s.-yA.\$;*;
2004/07/01 08:26:50.737	ICMP	172.16.15.37		61.120.175.54		...SoftEther Keep-Alive Packet
2004/07/01 08:26:50.740	TCP	172.16.15.245	8150	193.167.201.10	4353
2004/07/01 08:26:50.743	TCP	172.16.13.36	4614	172.49.184.165	1025	
2004/07/01 08:26:50.744	TCP	172.16.14.22	1929	69.20.74.193	6667	
2004/07/01 08:26:50.745	TCP	172.16.13.36	4618	172.49.184.165	3410	
2004/07/01 08:26:50.746	TCP	172.16.13.36	4619	172.49.184.165	5554	

Ready

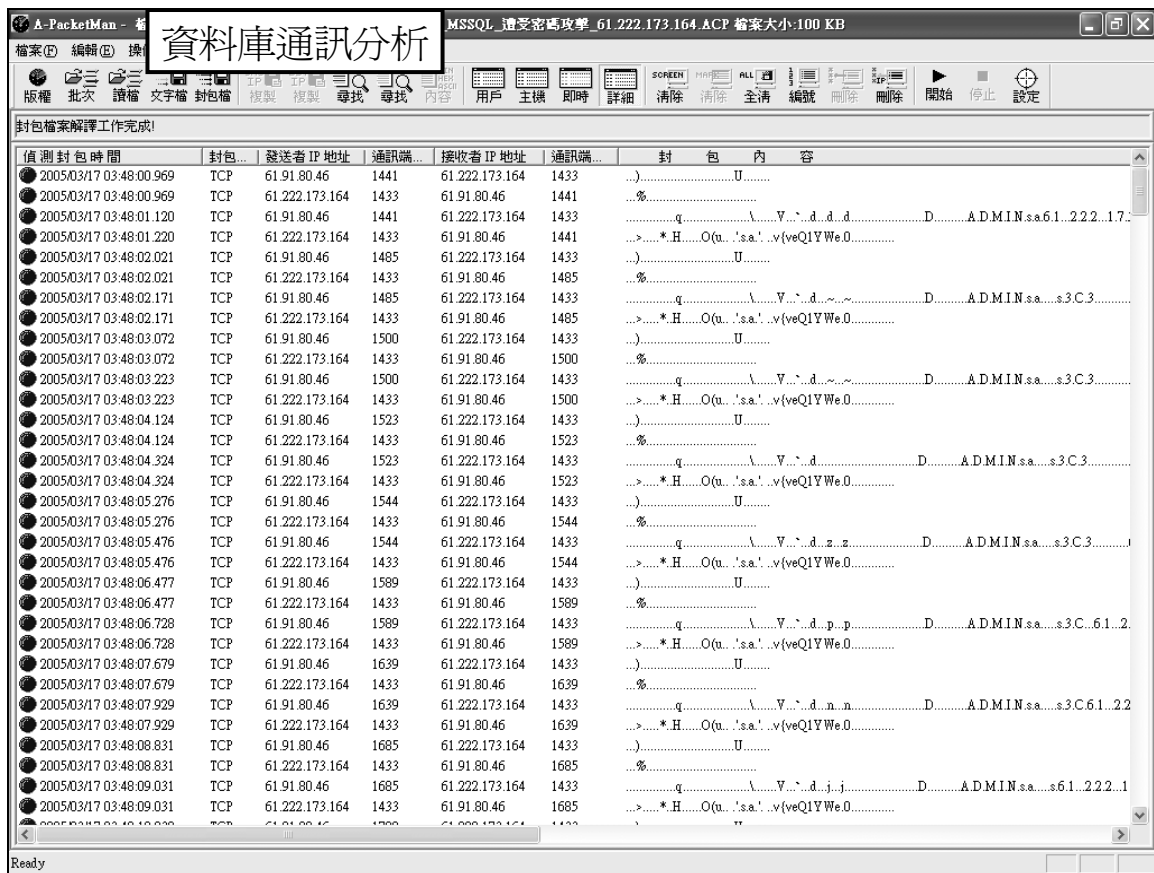
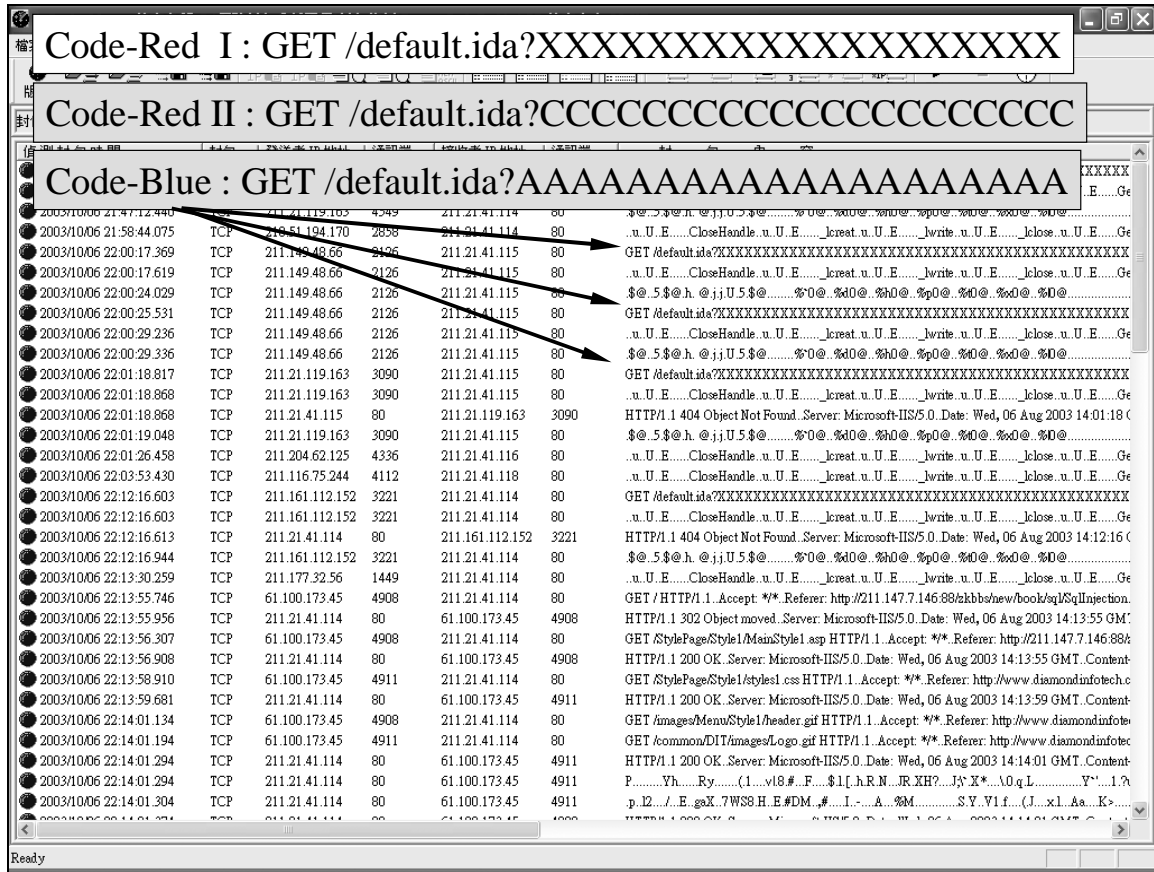
SoftEther 破壞防火牆的防護機制

SoftEther 家用電腦

防火牆 阻擋外來通訊

SoftEther 中繼站

© 2004-2006 copyright Jamien Liu 劉楨民



資料庫通訊分析 MSSQL 遭受密碼攻擊 61.222.173.164.ACP 檔案大小:100 KB

封包檔案解譯工作完成!

偵測封包時間	封包...	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊端...	封包內容
2005/03/17 03:48:00.969	TCP	61.91.80.46	1441	61.222.173.164	1433	...
2005/03/17 03:48:00.969	TCP	61.222.173.164	1433	61.91.80.46	1441	...
2005/03/17 03:48:01.120	TCP	61.91.80.46	1441	61.222.173.164	1433	...
2005/03/17 03:48:01.220	TCP	61.222.173.164	1433	61.91.80.46	1441	...
2005/03/17 03:48:02.021	TCP	61.91.80.46	1485	61.222.173.164	1433	...
2005/03/17 03:48:02.021	TCP	61.222.173.164	1433	61.91.80.46	1485	...
2005/03/17 03:48:02.171	TCP	61.91.80.46	1485	61.222.173.164	1433	...
2005/03/17 03:48:02.171	TCP	61.222.173.164	1433	61.91.80.46	1485	...
2005/03/17 03:48:03.072	TCP	61.91.80.46	1500	61.222.173.164	1433	...
2005/03/17 03:48:03.072	TCP	61.222.173.164	1433	61.91.80.46	1500	...
2005/03/17 03:48:03.223	TCP	61.91.80.46	1500	61.222.173.164	1433	...
2005/03/17 03:48:03.223	TCP	61.222.173.164	1433	61.91.80.46	1500	...
2005/03/17 03:48:04.124	TCP	61.91.80.46	1523	61.222.173.164	1433	...
2005/03/17 03:48:04.124	TCP	61.222.173.164	1433	61.91.80.46	1523	...
2005/03/17 03:48:04.324	TCP	61.91.80.46	1523	61.222.173.164	1433	...

防火牆已經失效!! 並未阻擋 TCP-1433

Hacker 61.91.80.46

Usually, Firewall should block TCP-1433

But we discover firewall fail.
We found TCP-1433 Pass-through it !!

Trying the password of 'sa'

MS-SQL 61.222.173.164

ADMIN.sa...s3C.61.222.173.164

ADMIN.sa...s3C.61.222.173.164

ADMIN.sa...s61.222.173.164

網路封包分析的基本技巧 (The skill of analysis packets)

- 先學習正常封包通訊的情況，瞭解基本通訊，HTTP, SMTP, POP3, SMB/CIFS, DNS, MS-SQL, MySQL等等。
- 分析封包時，先排除已知正常通訊封包。
- 如果已經排除已知正常通訊封包，剩餘無法解釋的通訊封包，可能包括異常與未知通訊封包。
- 分析異常封包的主要原則：
 - 先觀察通訊雙方為內網位址或外網位址?
 - 進一步觀察通訊雙方為單向或雙向通訊?
 - 接著檢查此網路通訊為禁止或開放的網路服務?
 - 傳送內容為明碼資料? 編碼資料? 或加密資料?
 - 是否違反封包行為分析(PBA)的原則?
 - 如果有無法解譯與分析的封包，可以將他從整個檔案萃取出來，方法如後所示。

© 2004-2006 copyright Jamien Liu 劉植民

目標封包萃取歸納技巧 (The skill of analysis packets)

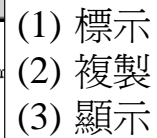
- 標示異常封包為特殊封包(Mark Packets)
 - 根據 IP 位址
 - 根據封包內容
- 複製特殊區段封包(Copy Special Packets)
- 顯示特殊封包視窗(Display Special Packets)
- 儲存封包檔案(Save Special Packets)
- 如果已經確定為禁止通訊的異常封包
 - A-PacketMan企業版，支援阻斷與清除的方式
 - 阻斷方式，產生相關阻斷規則，網管人員確認後，進行防火牆的指令更新。
 - 清除方式，需搭配S-Check程式，至電腦本機清除問題程式。

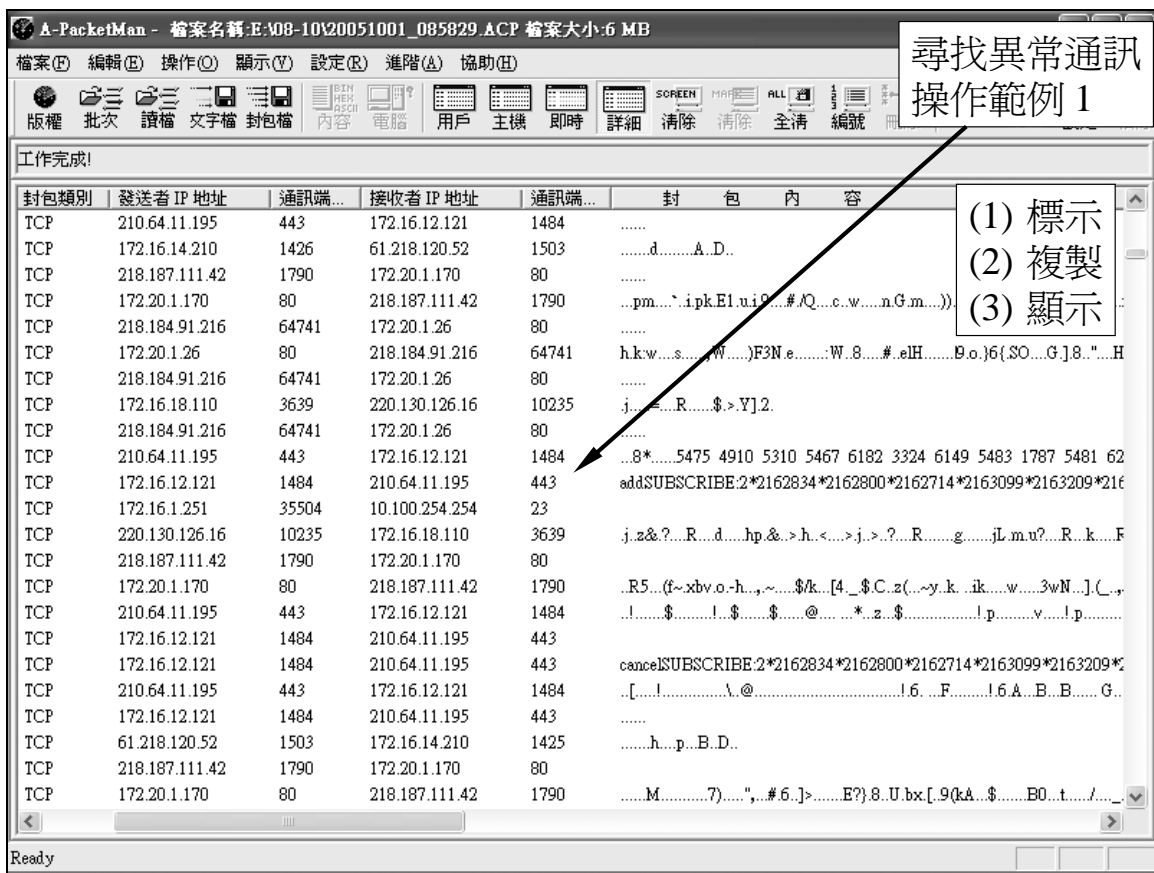
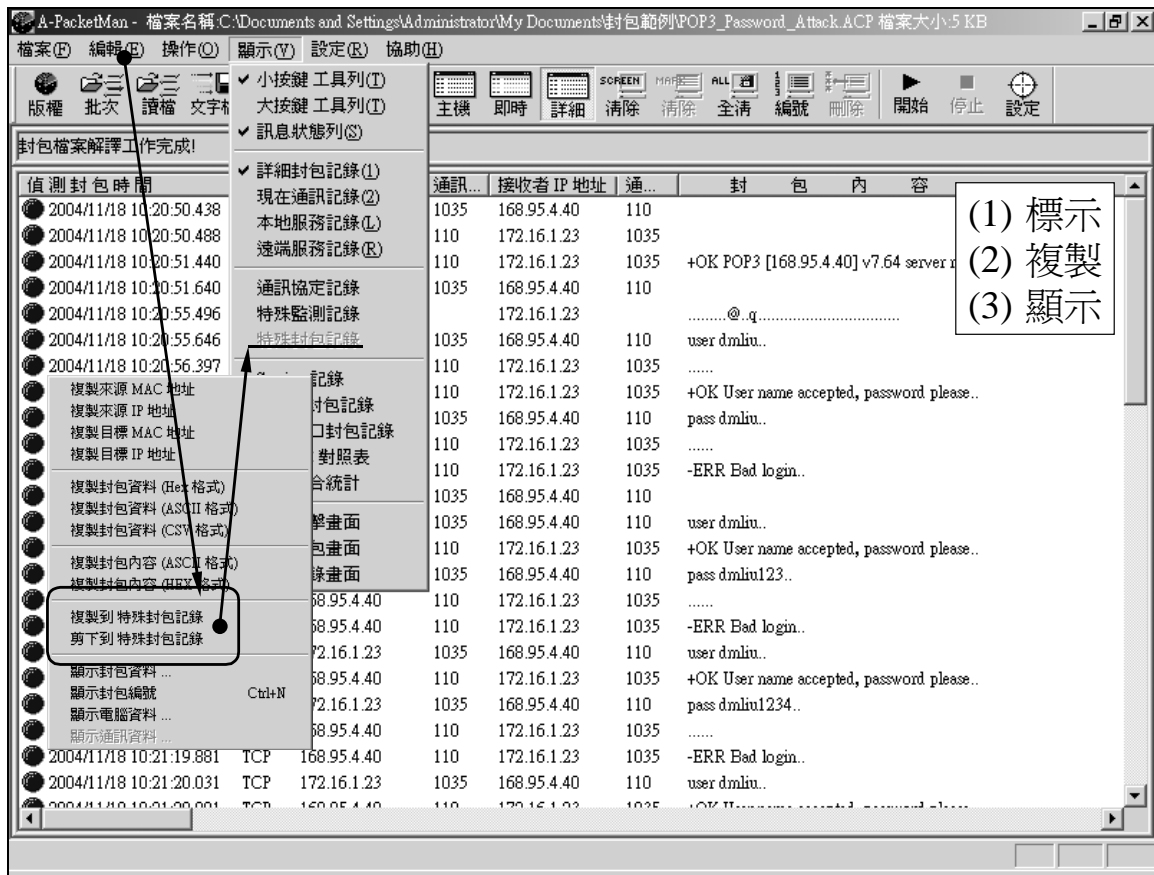
© 2004-2006 copyright Jamien Liu

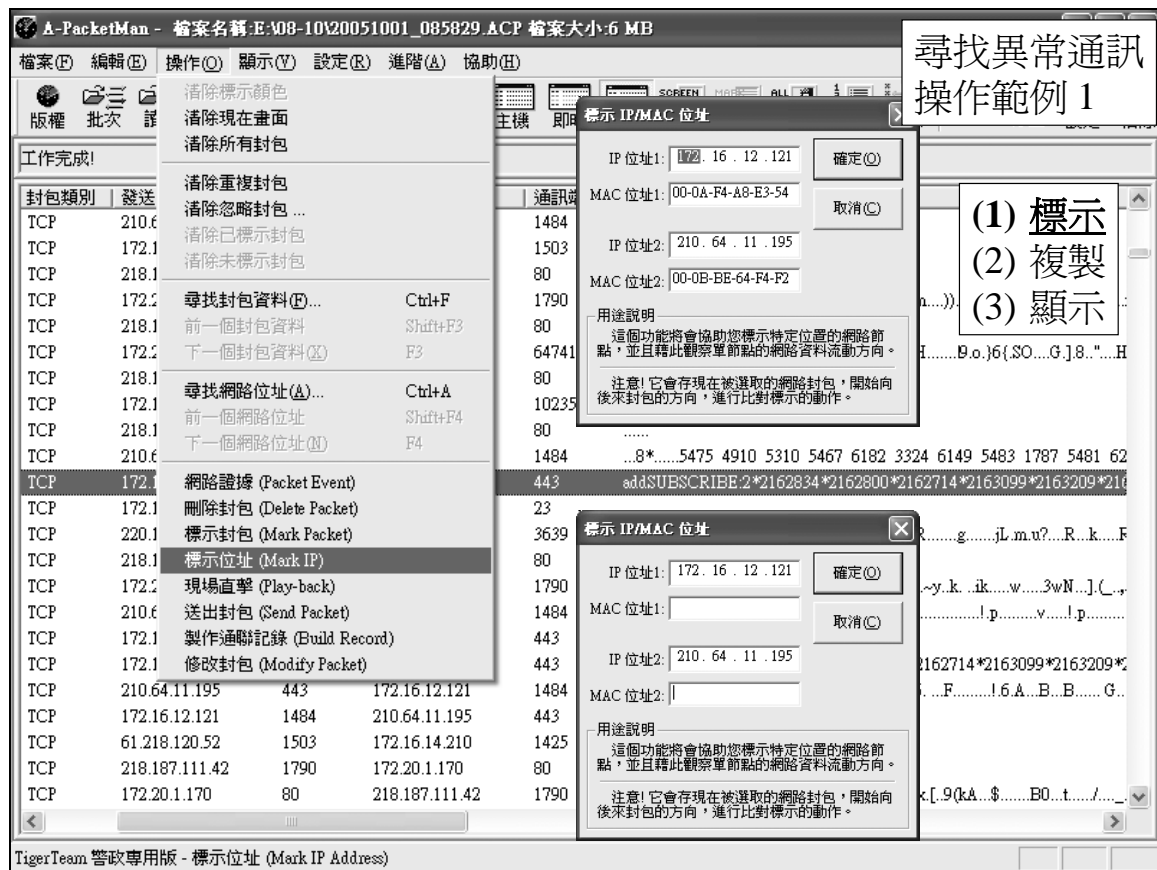
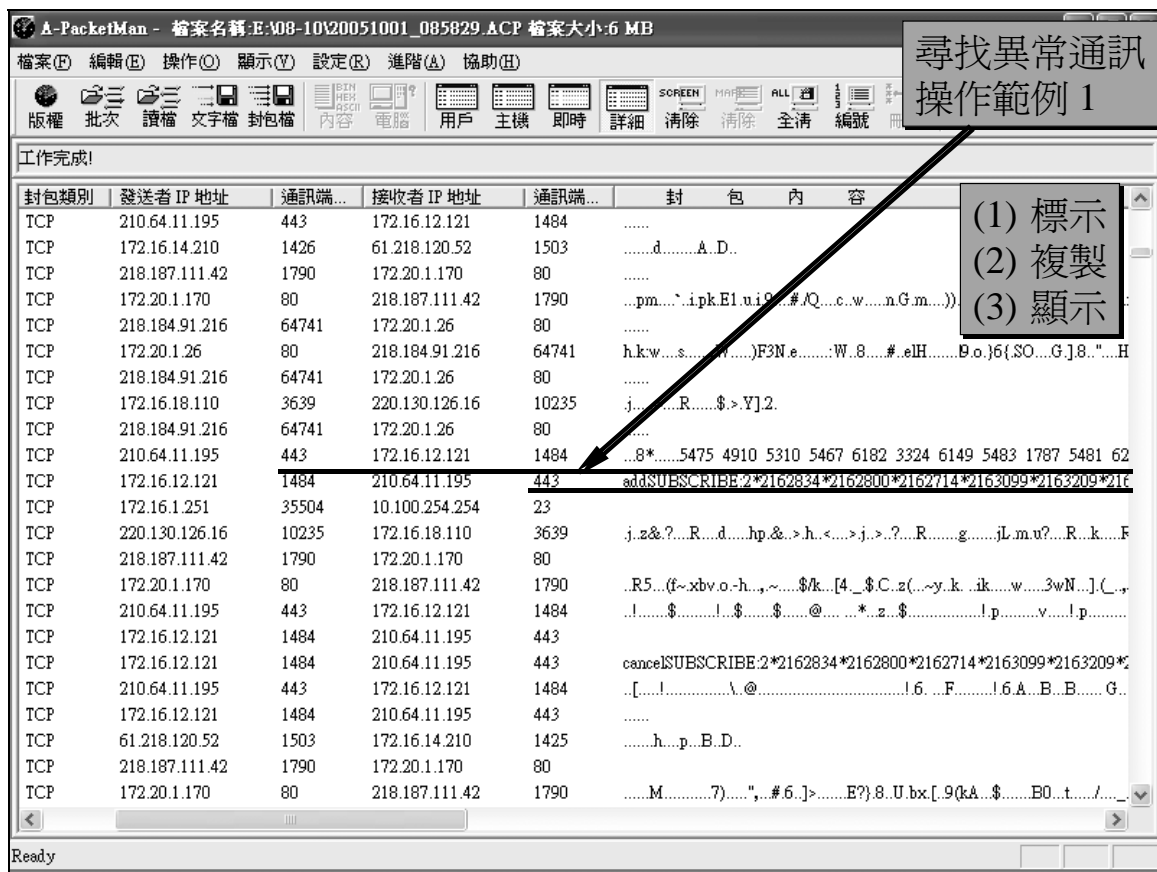
如何尋找特定IP位址或文字內容的封包? (How to search packets by IP address or payload ?)



(How to search packets by IP address or payload ?)







A-PacketMan - 檔案名稱: E:\08-10\20051001_085829.ACP 檔案大小: 6 MB

檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)

版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號

工作完成!

封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊端...	封 包 內 容
TCP	210.64.11.195	443	172.16.12.121	1484
TCP	172.16.14.210	1426	61.218.120.52	1503d.....A.D..
TCP	218.187.111.42	1790	172.20.1.170	80
TCP	172.20.1.170	80	218.187.111.42	1790	...pm....`ipkE1.ui9...#AQ...c.w...nG.m...))
TCP	218.184.91.216	64741	172.20.1.26	80
TCP	172.20.1.26	80	218.184.91.216	64741	h.k.w...s...,W...)F3Ne.....W.8...#eLH...9.o)6{SO...G.j}8..."H
TCP	218.184.91.216	64741	172.20.1.26	80
TCP	172.16.18.110	3639	220.130.126.16	10235	j.....=...R.....\$.>Y]2.
TCP	218.184.91.216	64741	172.20.1.26	80
TCP	210.64.11.195	443	172.16.12.121	1484	...8*.....5475 4910 5310 5467 6182 3324 6149 5483 1787 5481 62
TCP	172.16.12.121	1484	210.64.11.195	443	addSUBSCRIBE/2*2162834*2162800*2162714*2163099*2163209*216
TCP	172.16.1.251	35504	10.100.254.254	23
TCP	220.130.126.16	10235	172.16.18.110	3639	j.z&?...R...d...hp&.>h.<...>j...>?...R.....g...jL.m.u?...R..k...F
TCP	218.187.111.42	1790	172.20.1.170	80
TCP	172.20.1.170	80	218.187.111.42	1790	..R5...(f~xbv.o~h...~\$%k...[4_\$.C.z(...~y.k..ik...w...3wN...](...~
TCP	210.64.11.195	443	172.16.12.121	1484	..!.....\$......!\$......\$.....@.....*..z..\$......!p.....v.....!p.....
TCP	172.16.12.121	1484	210.64.11.195	443
TCP	172.16.12.121	1484	210.64.11.195	443	cancelSUBSCRIBE/2*2162834*2162800*2162714*2163099*2163209*
TCP	210.64.11.195	443	172.16.12.121	1484	..[.....!.....\.....@.....!6...F.....!6.A...B...B...G...
TCP	172.16.12.121	1484	210.64.11.195	443
TCP	61.218.120.52	1503	172.16.14.210	1425h...p...B.D..
TCP	218.187.111.42	1790	172.20.1.170	80
TCP	172.20.1.170	80	218.187.111.42	1790M.....7).....",...#6..]>.....E?}8.U.bx[.9(kA...\$.B0.t.../.....

Ready

尋找異常通訊
操作範例 1

(1) 標示
(2) 複製
(3) 顯示

A-PacketMan - 檔案名稱: E:\08-10\20051001_085829.ACP 檔案大小: 6 MB

檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)

版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號

工作完成!

複製來源 MAC 地址
複製來源 IP 地址
複製目標 MAC 地址
複製目標 IP 地址

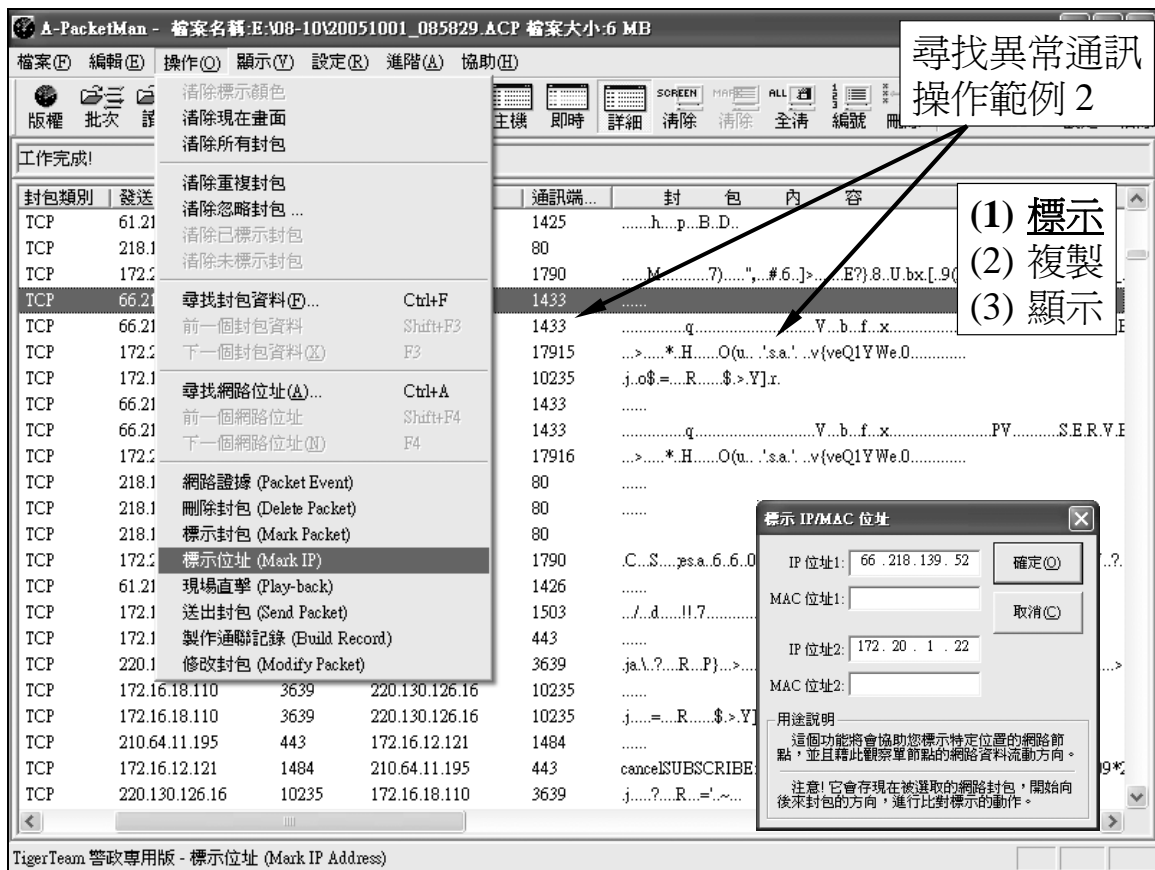
複製封包資料 (Hex 格式)
複製封包資料 (ASCII 格式)
複製封包資料 (CSV 格式)
複製封包內容 (ASCII 格式)
複製封包內容 (HEX 格式)
複製到 特殊封包記錄
剪下到 特殊封包記錄
顯示封包資料 ...
顯示封包編號 Ctrl+N
顯示電腦資料 ...
顯示通訊資料 ...
✓ 顯示封包解說 Ctrl+T

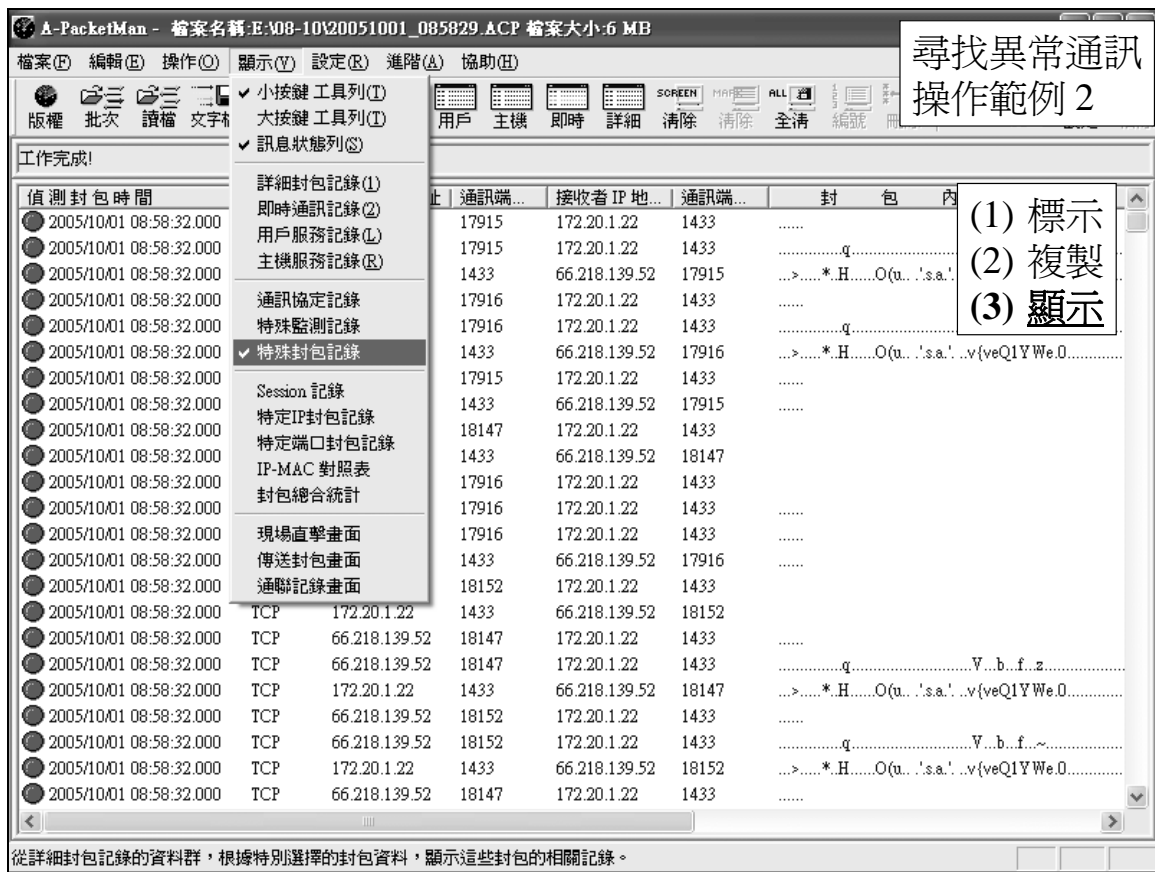
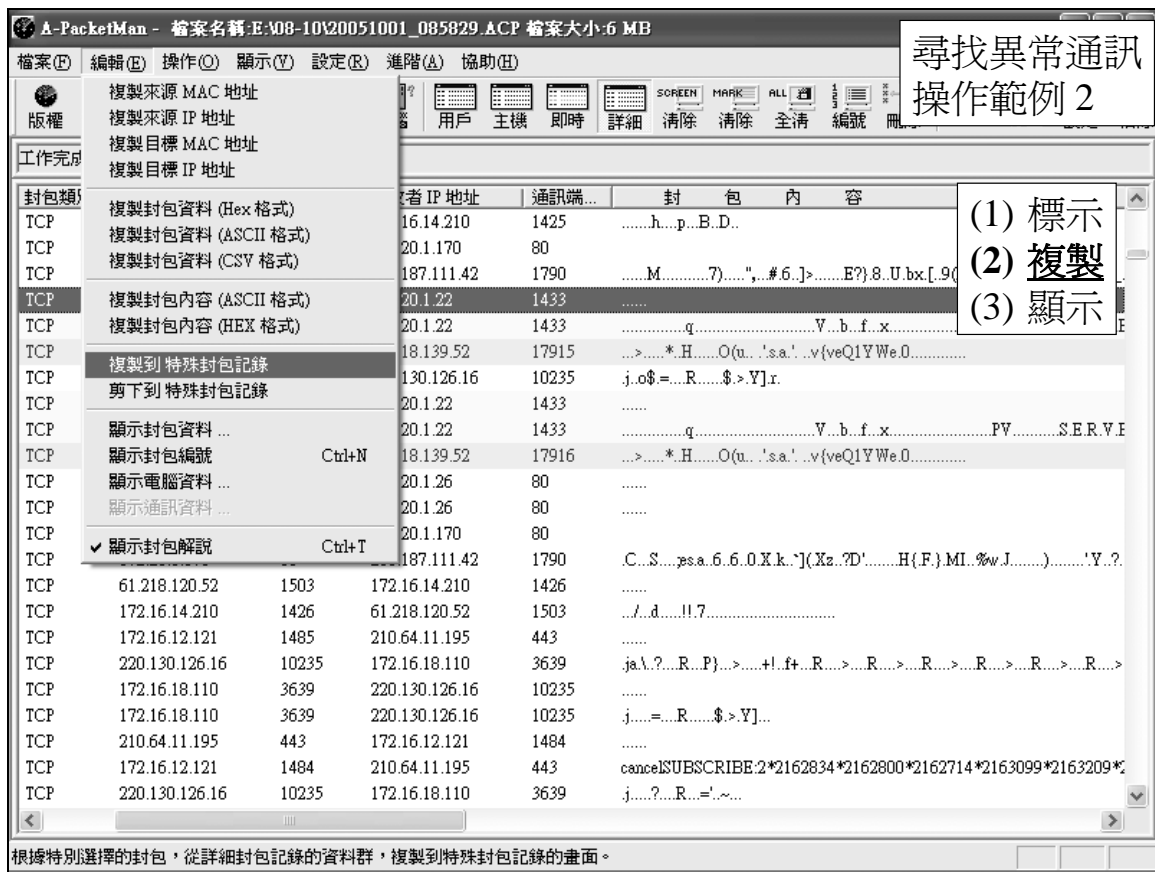
封包類別	發送者 IP 地址	通訊端...	接收者 IP 地址	通訊端...	封 包 內 容
TCP	172.16.12.121	1484
TCP	18.120.52	1503d.....A.D..
TCP	20.1.170	80
TCP	187.111.42	1790	...pm....`ipkE1.ui9...#AQ...c.w...nG.m...))
TCP	20.1.26	80
TCP	184.91.216	64741	h.k.w...s...,W...)F3Ne.....W.8...#eLH...9.o)6{SO...G.j}8..."H
TCP	20.1.26	80
TCP	130.126.16	10235	j.....=...R.....\$.>Y]2.
TCP	20.1.26	80
TCP	16.12.121	1484	...8*.....5475 4910 5310 5467 6182 3324 6149 5483 1787 5481 62
TCP	64.11.195	443	addSUBSCRIBE/2*2162834*2162800*2162714*2163099*2163209*216
TCP	10.100.254.254	23
TCP	16.18.110	3639	j.z&?...R...d...hp&.>h.<...>j...>?...R.....g...jL.m.u?...R..k...F
TCP	20.1.170	80
TCP	172.20.1.170	80	218.187.111.42	1790	..R5...(f~xbv.o~h...~\$%k...[4_\$.C.z(...~y.k..ik...w...3wN...](...~
TCP	210.64.11.195	443	172.16.12.121	1484	..!.....\$......!\$......\$.....@.....*..z..\$......!p.....v.....!p.....
TCP	172.16.12.121	1484	210.64.11.195	443
TCP	172.16.12.121	1484	210.64.11.195	443	cancelSUBSCRIBE/2*2162834*2162800*2162714*2163099*2163209*
TCP	210.64.11.195	443	172.16.12.121	1484	..[.....!.....\.....@.....!6...F.....!6.A...B...B...G...
TCP	172.16.12.121	1484	210.64.11.195	443
TCP	61.218.120.52	1503	172.16.14.210	1425h...p...B.D..
TCP	218.187.111.42	1790	172.20.1.170	80
TCP	172.20.1.170	80	218.187.111.42	1790M.....7).....",...#6..]>.....E?}8.U.bx[.9(kA...\$.B0.t.../.....

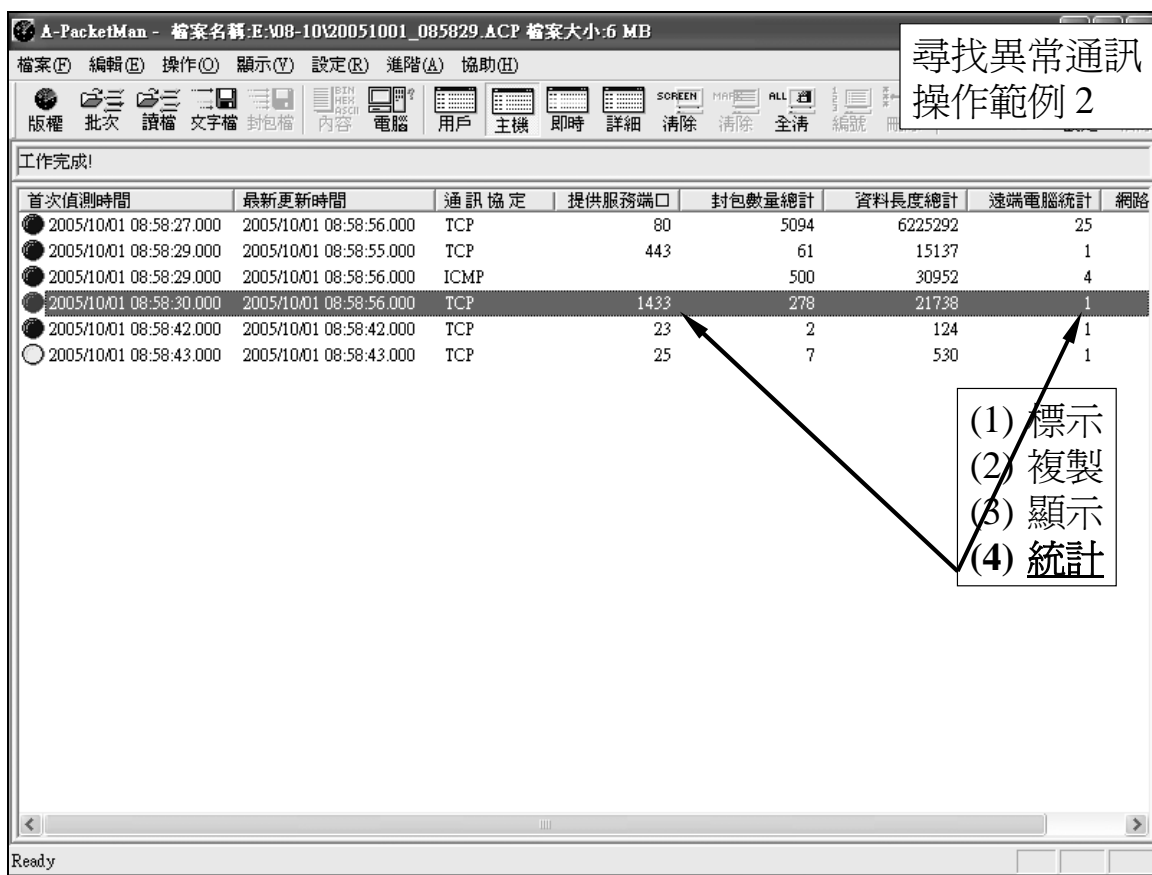
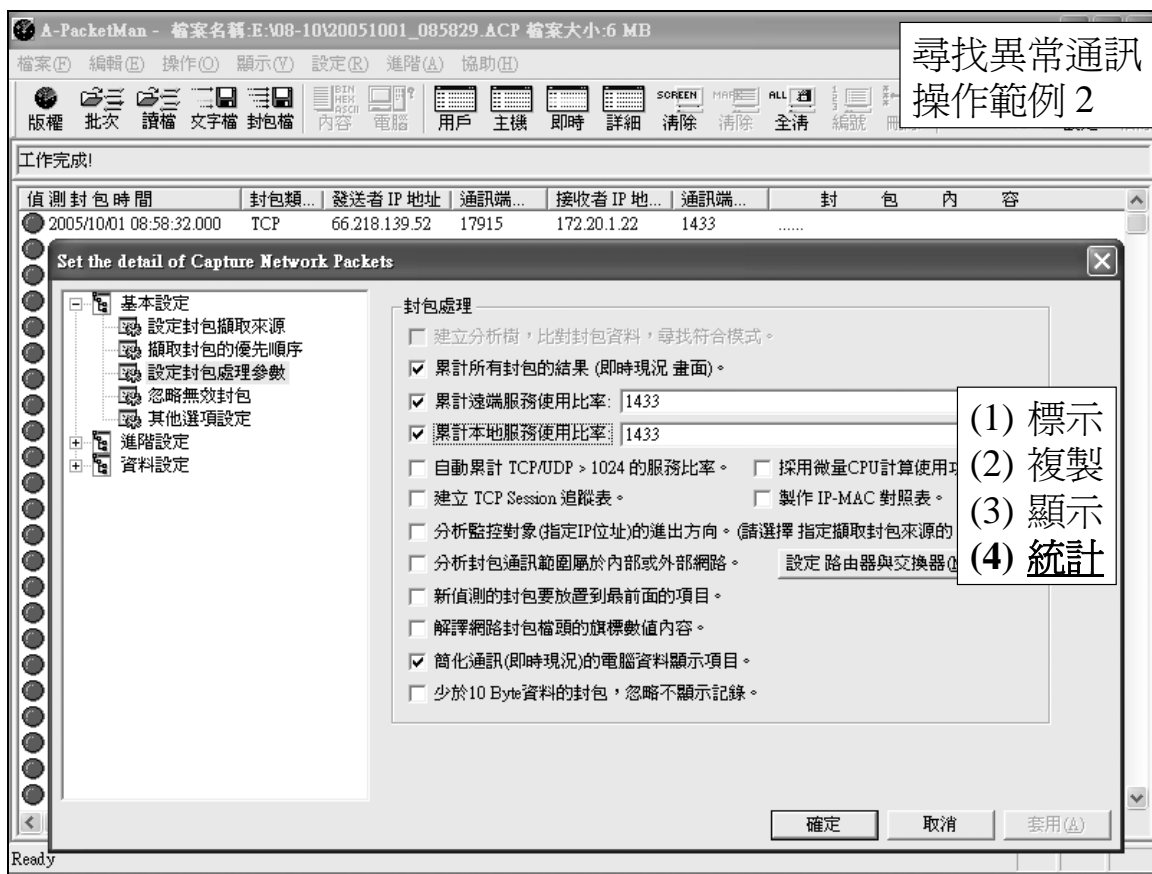
根據特別選擇的封包，從詳細封包記錄的資料群，複製到特殊封包記錄的畫面。

尋找異常通訊
操作範例 1

(1) 標示
(2) 複製
(3) 顯示







A-PacketMan - 檔案名稱:E:\08-10\20051001_085829.ACP 檔案大小:6 MB

檔案(F) 編輯(E) 操作(O) 顯示(V) 設定(R) 進階(A) 協助(H)

版權 批次 讀檔 文字檔 封包檔 內容 電腦 用戶 主機 即時 詳細 清除 清除 全清 編號

工作完成!

首次偵測時間	最新更新時間	通訊協定	使用服務端口	封包數量總計	資料長度總計	遠端電腦...	網路
2005/10/01 08:58:29.000	2005/10/01 08:58:56.000	TCP	80	2714	437740	48	
2005/10/01 08:58:29.000	2005/10/01 08:58:56.000	TCP	其他服務	723	174414	17	
2005/10/01 08:58:29.000	2005/10/01 08:58:56.000	ICMP		500	30952	4	
2005/10/01 08:58:30.000	2005/10/01 08:58:52.000	UDP	其他服務	12	1359	4	
2005/10/01 08:58:30.000	2005/10/01 08:58:56.000	TCP	443	38	4304	1	
2005/10/01 08:58:30.000	2005/10/01 08:58:56.000	TCP	1433	457	44482	2	
2005/10/01 08:58:32.000	2005/10/01 08:58:53.000	TCP	23	7	476	1	
2005/10/01 08:58:43.000	2005/10/01 08:58:43.000	TCP	25	5	317	1	

顯示詳細資料

連結主機清單: 2 hosts

詳細主機資料:

主機 IP 位址

- 205.200.12.32
- 66.218.139.52

(1) 標示
(2) 複製
(3) 顯示
(4) 統計

複製IP位址(C)

Ready

S-Check - 年度授權版 2005.01

系統(S) 編輯(E) 操作(O) 檢視(V) 說明(H)

版權 自動快照 自動比對 Registry Service 目錄清單 程序清單 模組清單 網路清單 網方清單 Event 清單 網站記錄 指令畫面 儲存螢幕 儲存記錄 寄送記錄 寄送螢幕

執行指令: Go! 常用指令: 問道 IP 位址 新波科技 臺灣網址

處理完成。紅色文字(紅燈)代表高度異常資料, 藍色文字(黃燈)代表特別注意資料, 黑色文字(綠燈)代表些微異常資料, 灰色文字(灰燈)代表正常無誤

程序代碼	程序路徑	網路通訊能力	通訊埠
3812	D:\Ap\SecuServer\A-PacketMan.exe	俱備TCP/IP通訊能力	
1120	D:\Ap\S-Check\S-Check.exe	俱備TCP/IP通訊能力	
1332	C:\Program Files\Common Files\RealUpdate_OB\realsched.exe	俱備TCP/IP通訊能力	
716	C:\WINNT\System32\WBEM\WinMgmt.exe	未使用TCP/IP通訊模組	
792	C:\WINNT\System32\svchost.exe	俱備TCP/IP通訊能力	
852	C:\WINNT\System32\inetinfo.exe	俱備TCP/IP通訊能力	TCP:1027,25,80,443 UDP:1028,3456
1152	C:\WINNT\Explorer.EXE	俱備TCP/IP通訊能力	
1164	C:\WINNT\Mixer.exe	未使用TCP/IP通訊模組	
1288	C:\WINNT\System32\intermat.exe	未使用TCP/IP通訊模組	
1248	C:\Program Files\Navnt\Navapw32.exe	未使用TCP/IP通訊模組	
1404	C:\PROGRA~1\Navnt\alertsvc.exe	俱備TCP/IP通訊能力	TCP:1030 UDP:1031
600	C:\WINNT\System32\svchost.exe	俱備TCP/IP通訊能力	
1296	C:\WINNT\System32\Taskmgr.exe	俱備TCP/IP通訊能力	
3304	C:\WINNT\System32\conime.exe	未使用TCP/IP通訊模組	
656	C:\WINNT\System32\MSTask.exe	俱備TCP/IP通訊能力	TCP:1026
144	C:\WINNT\System32\smss.exe	未使用TCP/IP通訊模組	
168	(Unknow)	未使用TCP/IP通訊模組	
188	C:\WINNT\System32\winlogon.exe	俱備TCP/IP通訊能力	
216	C:\WINNT\System32\services.exe	俱備TCP/IP通訊能力	
228	C:\WINNT\System32\lsass.exe	俱備TCP/IP通訊能力	UDP:500,4500
412	C:\WINNT\System32\svchost.exe	俱備TCP/IP通訊能力	TCP:135 UDP:135

【紅色文字-紅燈】=>高度異常資料, 【藍色文字-黃燈】=>注意資料, 【黑色文字-綠燈】=>些微異常資料, 【灰色文字-灰燈】正常無誤

如何進一步學習封包 分析技巧與累積經驗?

- 異常網路封包的危害判斷準則
 - 先排除所有已知的標準通訊協定, HTTP/SMTP/POP3/DNS/CIFS/MSN...
 - 內網或外網 (通訊雙方的IP位址是否為Internet位址?)
 - 禁止或開放 (這類網路服務是否可以執行?)
 - 單向或雙向 (通訊雙方有無互相傳送資料?)
- 異常通訊的蒐證與分析步驟
 - 標示 (標示位址或是標示封包內容)
 - 複製 (將已經標示顏色的封包, 複製到 特殊封包視窗)
 - 顯示 (切換顯示畫面為 特殊封包視窗)
 - 統計 (option, 如果要進一步瞭解攻擊來源或是受害對象)
- Q&A
- 學員論壇
 - <http://forum.AntiHacker.com.tw>
 - <http://forum.DiamondInfoTech.com.tw>

即時封包鑑識工具 對於網路管理人員的益處

- 瞭解DMZ主機的運作情況
- 掌握防火牆的設定現況
- 監測使用者異常網路行為
- 偵測病毒蠕蟲感染程度
- 分析可疑木馬後門程式的通訊
- 避免GSN或ISP通知異常, 事先掌握情況
- 直接將異常(未知攻擊)通訊, 轉換成為已知規則, 輸出為Firewall, IDS, IDP/IPS的規則
 - 產生 Snort, FortiGate, IpTable 的偵測阻擋規則