

報道関係各位

株式会社イー・ポスト

パケットデータ可視化・解析FIT^{*1}

「AFIT-PC」を販売開始

～オンライン／オフラインでパケットデータ可視化・解析可能なノート PC タイプ製品～

^{*1} Forensic Investigation Tool

メールサーバソフト開発・販売会社の株式会社イー・ポスト(本社:東京都新宿区、代表取締役:今西和也 <http://www.e-postinc.jp> TEL:03-5272-5386)は、このたび、Windows ノート PC タイプのパケットデータ可視化解析製品「AFIT-PC」(開発元:台湾デシジョングループ社)を、2012年4月16日より販売を開始いたしますのでご案内申し上げます。

本製品は、Wireshark 等の LAN アナライザと一緒に使うことで、ネットワークの利用状況の解析を行ったり、コンテンツの再現・復元したりすることができます。また、ノート PC タイプですので、現場などにも持ち込んで利用できるのも、機動性、携帯性に優れた製品です。

価格は、

「AFIT-PC」が、43 万円 (税別)

※ ノートPCにインストール済みで直ぐに利用可。

※ ソフトウェアのみの提供も可能です。お問合せください。

当社では、年間 30 本の販売を目標としております。

【背景】

スマホの企業利用の拡大、P2P アプリケーションの利用の広がりなどネットワーク利用環境が大きく変わり、ネットワークスペシャリストの業務範囲が情報セキュリティ分野まで広がってきています。

もはや、従来の LAN アナライザだけでは、対応が難しくなってきたといえるでしょう。

- ・ネットワーク・アプリケーションの管理・運用、
- ・メールデータ等のアーカイブ、
- ・ネットワークユーザの行動監視と把握、
- ・企業情報・個人情報の漏洩対策

などの業務内容が負担を増してきています。

本製品は、Windows (Win2000/XP/VISTA/Win7) で動作するオフラインのパケットデータの可視化・解析ツールです。パケット可視化から、「誰が」「いつ」「どこから」「何をした」等、ネットワークユーザの行動監視することができます。

データ採取には FIT のパケットキャプチャ機能または Wireshark や TCPdump などのパケットキャプチャ機能を利用するか、既存の PCAP ファイルを FIT に入力することでパケットデータの入力が出来ます。Wireshark 等の LAN アナライザと一緒に使うことで、ネットワークの利用状況の迅速な解析やコンテンツの再現を実現できます。

主な用途として、以下のようなシーンが考えられます。

- ・社内の情報セキュリティ現状の報告書作成のため、急遽パケット可視化ツールを使いたい・・・。
- ・たくさんある Sniffer や Wireshark を活用して、オフラインで情報セキュリティ状況の調査を行いたい・・・。
- ・アクセス違反などの問題が発生したようで、調査を早急に始めなければならない・・・。
- ・支店で離職者が出る..情報漏洩などが発生しないように、メールや WEB アクセス、ファイル送信のチェックを実施したい・・・。
- ・本格的なフォレンジック装置(NetData Saver)を導入するまで、社内ネットワークの利用状況調査を行い、導入するポイントを選択したい・・・。

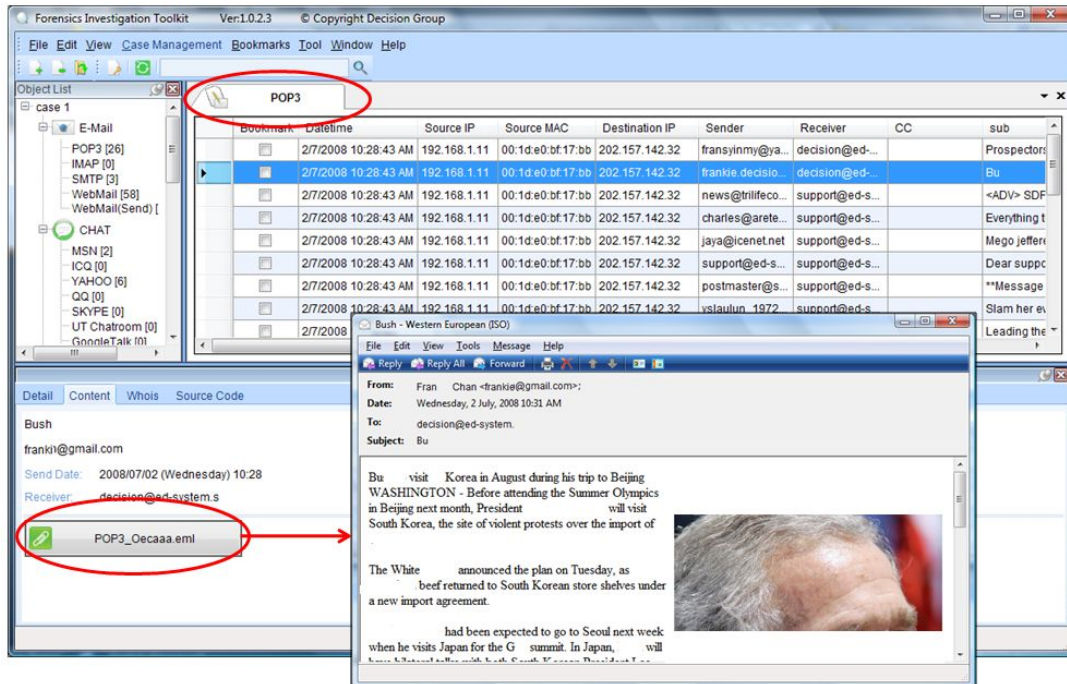
【主な機能・特長】

- ケース・マネジメント機能（監査/検索などの順番や方法の管理）
- パケットデータ・ファイル(PCAP フォーマット)のインポート。オフラインでの利用が可能。
- 30 種類の様々なインターネット・トラフィックデータの分析
 - ・メール(POP3、SMTP、IMAP)、Webmail
 - ・IM チャット(MSN、ICQ、YHOO、QQ、スカイプ音声会話ログ、UT チャットルーム
Gtalk IRC チャットルーム、WhatsApp)
 - ・ファイル転送(FTP、P2P)
 - ・HTTP(SSL)(コンテンツ アップロード/ダウンロード)
 - ・ビデオ・ストリーミング、リクエスト)
- 詳細情報
 - ・日付 時間 ソース IP ソース MAC
 - ・ディスティネーション IP 等
- サーチ機能(全文検索)
- Whois とグーグル地図組込機能
- ブックマーク機能
- 日本語、英語、中国語に対応

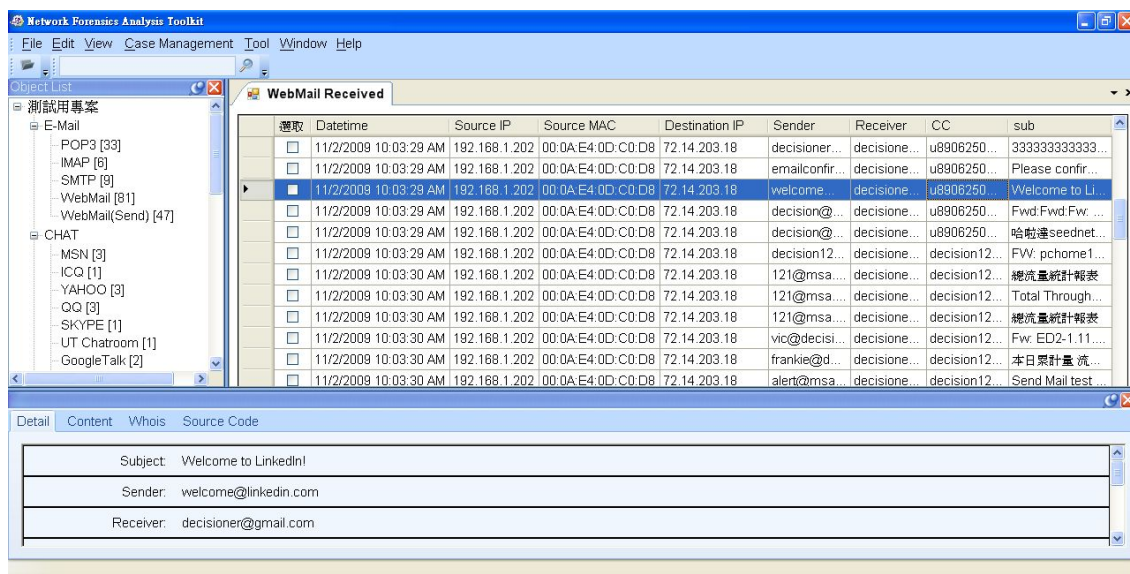
中国企業とのビジネスが多くなる中で、中国圏での豊富な実績をもっているので安心いただけます。

- ノート PC の機動性を生かして、調査現場などの場所に持っていくことができます。

【画面例】「POP3」



【画面例】「IM/チャット -Skype, MSN, QQ, GTalk etc...」



【画面例】「FTP プロトコル」

The screenshot shows the Network Forensics Analysis Toolkit interface. The 'Object List' on the left shows 'FTP [4]' selected. The main window displays a table of FTP sessions and a detailed view of a specific session.

選択	Captured Time	Source MAC	Source IP	Destination IP	FTP Server's Host	Transferred File	Transferred File Size
☒	6/15/2009 3:21:21 PM	00:0e:a6:39:47:43	192.168.1.33	192.168.1.249	192.168.1.249	DiagnosticCD_ED2-1-10-2.iso	16197612
☐	6/15/2009 3:24:46 PM	00:0e:a6:39:47:43	192.168.1.33	192.168.1.249	192.168.1.249	DiagnosticCD_ED2-1-10-2.iso	15695696
☐	6/15/2009 3:21:21 PM	00:0e:a6:39:47:43	192.168.1.33	192.168.1.249	192.168.1.249	DiagnosticCD_ED2-1-10-2.iso	16197612
☐	6/15/2009 3:24:46 PM	00:0e:a6:39:47:43	192.168.1.33	192.168.1.249	192.168.1.249	DiagnosticCD_ED2-1-10-2.iso	15695696

Detail	Whois
Captured Time: 2009/06/15 (Monday) 15:21	
Source MAC: 00:0e:a6:39:47:43	
Source IP: 192.168.1.33	
Destination IP: 192.168.1.249	
FTP Server's Host: 192.168.1.249	
FTP Login Account: flyy	
FTP Login Password: 203154	

【画面例】「P2P」

Network Forensics Analysis Toolkit

File Edit View Case Management Tool Window Help

Object List

IRC Chatroom [1]

File Transfer

FTP [4]

P2P [6]

TELNET

Telnet [1]

HTTP

HTTP Content [590]

HTTP Unlabeled/Download

P2P

選択 Captured Time Source MAC Source IP Destination IP Last Activated Time P2P Tool Transferred File

☐ 9/10/2009 11:25:45 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 9/10/2009 11:26:14 AM Foxy 1.9.8.0 Foxy 1.9.9.TC.Setup[1]

☒ 9/10/2009 11:26:04 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 9/10/2009 11:26:37 AM Foxy 1.9.8.0 碧昂絲-beyonce-bday-C

☐ 9/10/2009 11:26:40 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 9/10/2009 11:27:14 AM Foxy 1.9.8.0 Jay-Z, Rihanna, Kanye

☐ 9/10/2009 11:26:58 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 9/10/2009 11:26:58 AM BitTorrent Not Available

☐ 10/30/2009 11:04:00 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 10/30/2009 11:04:00 AM Foxy 1.9.8.0 Jay-Z ft. Rihanna & Kar

☐ 10/30/2009 11:04:00 AM 00:0a:e4:0d:c0:d8 192.168.1.190 0.0.0.0 10/30/2009 11:04:00 AM Foxy 1.9.8.0 Foxy 1.9.9.TC.Setup.ex

Message Detail Whois

Captured Time Up/Down Bytes Source Port Destination IP Destination Port

☒ 9/10/2009 11:26:04 AM 0 469 1366 114.47.227.199 8445

9/10/2009 11:26:07 AM 0 451 1371 114.27.213.1 9219

9/10/2009 11:26:10 AM 0 460 1377 122.117.162.4 7587

9/10/2009 11:26:13 AM 0 477 1420 114.43.239.7 10369

9/10/2009 11:26:16 AM 0 524745 1407 118.171.133.157 6939

9/10/2009 11:26:23 AM 0 33294 1390 122.127.178.99 7759

9/10/2009 11:26:23 AM 0 1697104 1393 118.169.66.230 10583

9/10/2009 11:26:28 AM 0 77480 1388 114.137.5.63 13935

9/10/2009 11:26:37 AM 0 2722776 1367 114.40.146.6 6210

【製品の概要】

●商品名:「AFIT-PC」(エーフィットピーシー)

●価格(税別)

「AFIT-PC」(JANコード:4562159043605)

¥430,000.-



画面は、ハメコミ合成です。

※PC:Dell Inspiron N5110 または同等品。

※AFIT 以外のインストールされるソフトウェア: mySQL, winpcap, .NET フレームワーク

※初年度保守、購入後 3 ヶ月の初期サポート(電話対応)が含まれます。

※2 年目以降の保守費は年額 50,000 円(税別)です。

※ ソフトウェアのみの提供も承ります。お問合せください。

【発売開始】

2012年4月16日

【販売目標】

30 セット/年

【開発元】デシジョングループ(Decision Group)について

1986 年創立。RS232/422/425 カード、計測機器、FA機器製造の台湾における代表的企業となる。2000 年からインターネットコンテンツ監視、フォレンジック分析ソリューションの設計開発を開始。40 名以上の修士号、博士号を持つ技術者が開発に従事している。2009 年には台湾政府および経済産業省から顕著な開発に対して表彰を受けた。

【会社概要】

- 社名：株式会社イー・ポスト
- 住所：東京都新宿区高田馬場 1-33-14 サンフラワービル 〒169-0075

TEL:03-5272-5386 FAX:03-5286-2610

- 設立：2000年7月19日
- 資本金：1000万円
- 代表者：今西和也
- 業務内容：

・コンピュータソフトウェアの開発、販売

・コンピュータネットワークの企画、開発、設計及びコンサルティング

・デジタル情報技術の開発

・各前号に附帯する一切の事業

文中、製品名、会社名等は、各社の商標及び登録商標です。

記事掲載時のお問い合わせ及び、弊社製品に関する情報や質問は

株式会社イー・ポスト 木下まで

東京都新宿区高田馬場 1-33-14 サンフラワービル 〒169-0075

TEL:03-5272-5386 FAX:03-5286-2610

E-mail: info@e-postinc.jp

ホームページ: <http://www.e-postinc.jp/>