EDETECTIVE

FIT Forensics Investigation Toolkit

Network Packet Forensics Software

on MS Windows®

FIT is a Windows-Based Content Forensics Toolkit to read and analyse the content of the Internet raw data in PCAP format. FIT provides security administrative officers, auditors, fraud and forensics investigator as well as lawful enforcement officers the power to perform content analysis and reconstruction on pre-captured Internet raw data from Wired or Wireless networks. FIT comes with very user friendly Graphical User Interface (GUI) that even allows novice to easily learn and capitalize on the powerful functionalities and features of FIT. All protocols and services analysed and reconstructed are displayed in readable format to the users. The other uniqueness of the FIT is the imported raw data files will be immediately parsed and reconstructed. Unlike other packet analyser or reconstruction tool that requires the user to manually reconstruct them session by session. The immediate parsing and reconstruction of the raw data imported allows all the parsed data to be displayed on the intended service categories. That makes the investigator task much easier on viewing the output results.

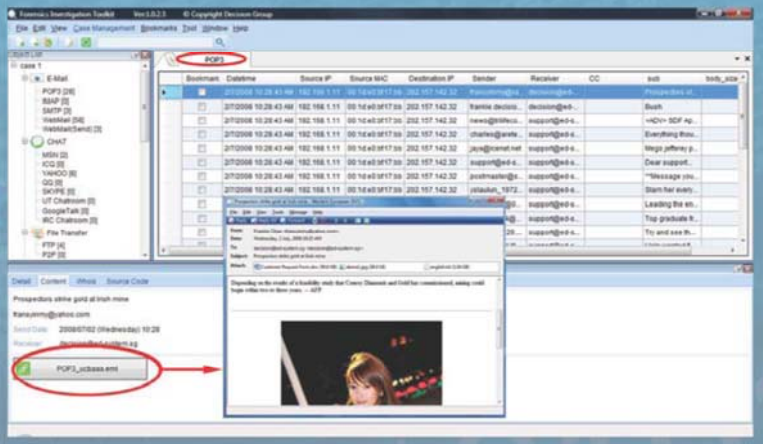
- Email
- Chat
- Web
- FTP
- P2P
- WebCam
- TELNET

DECISION GROUP
Decision Group Inc (HQ) Taiwan
Decision Computer Pte Ltd Singapore
Decision Computer Juergen Merz e.k. Germany
www.edecision4u.com

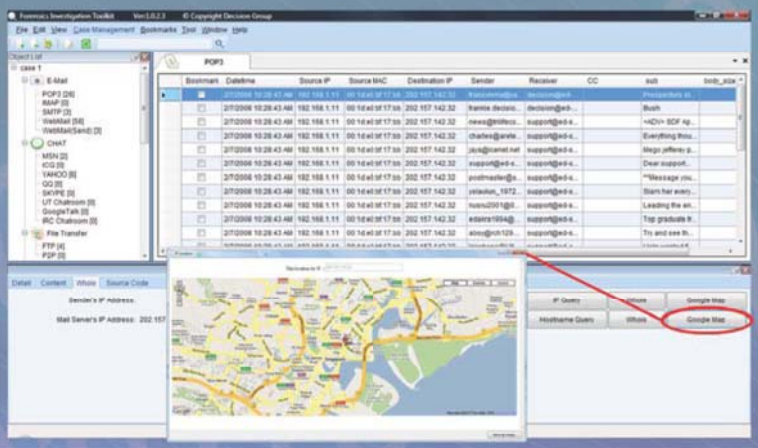
Address : 4/F No.31, Alley 4, Lane 36, Sec. 5, Ming-Sheng East Rd, Taipei, Taiwan ROC.
Phone : +886 227665753 Fax : +886 227665702
Email : decision@decision.com.tw

1 Diagram 1 : How FIT works?

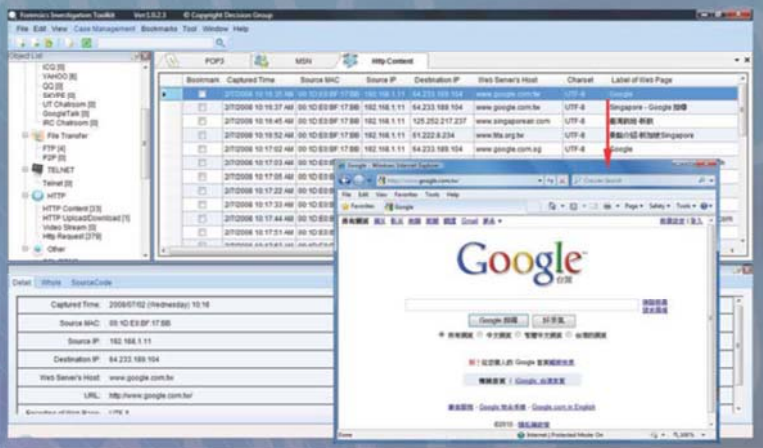
2 Diagram 2 : Email (POP3, SMTP, IMAP) and Webmail Packet Content Reconstruction



3 Diagram 3 : *WhoIs* Source-Destination Query function and *Google* Map Query function

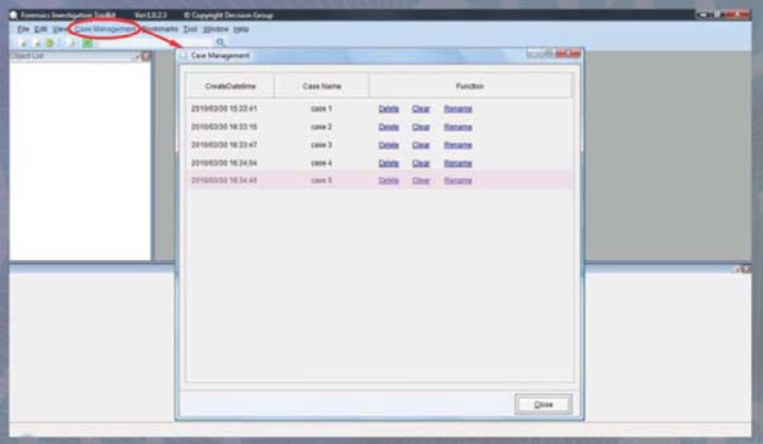


4 Diagram 4 : Web Browsing (HTTP Content) reconstruction



5 Diagram 5 : Search Function

6 Diagram 6 : Case Management



Product Features :

- Application Software Tool (Windows based)
- Case Management Function
- *WhoIs* and *Google* Map Integration Functions
- Support Import of Raw Data Files (in PCAP Format)
- Search Function (Full Text Search)
- Bookmark Function
- Detail information includes Date-Time, Source IP, Destination IP, Source MAC etc.
- Analysing and Reconstruction of various Internet traffic types which includes Email (POP3, SMTP, IMAP), Webmail (Read and Sent), IM or Chat (MSN, ICQ, Yahoo, QQ, Skype Voice Call Log, UT Chat Room, Gtalk, IRC Chat Room), File Transfer (FTP, P2P), Telnet, HTTP (Content, Upload/Download, Video Streaming, Request) and Others (SSL).

Our Representation :

Support more than 140 Network Protocols