EDETECTIVE®

FIT Forensics Investigation Toolkit (V2)

Network Packet Forensics Software

on MS Windows®

FIT(V2) is a Windows-Based Content Forensics Toolkit to read and analyse the content of the Internet raw data in PCAP format. FIT(V2) 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(V2) 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(V2). All protocols and services analysed and reconstructed are displayed in readable format to the users. The other uniqueness of the FIT(V2) 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
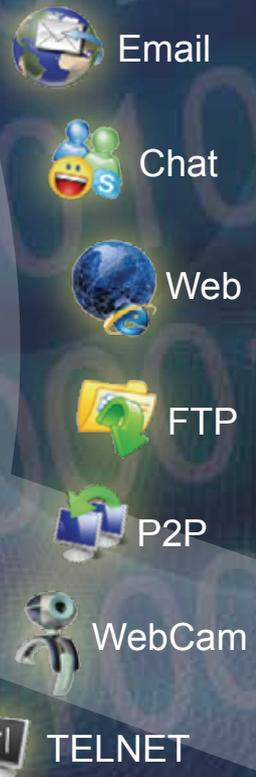
DECISION GROUP
Decision Group Inc (HQ) Taiwan
Decision Computer Pte Ltd Singapore
Decision Computer Juergen Merz e.k. Germany

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
decision@ms1.hinet.net

1 Diagram 1 : How FIT works?
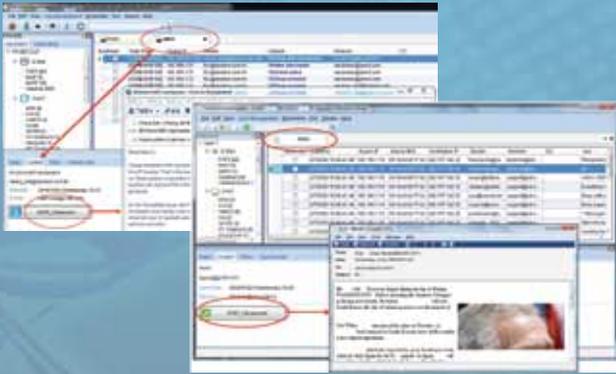
2 Diagram 2 : Email (POP3, SMTP, IMAP) and Webmail Packet Content Reconstruction
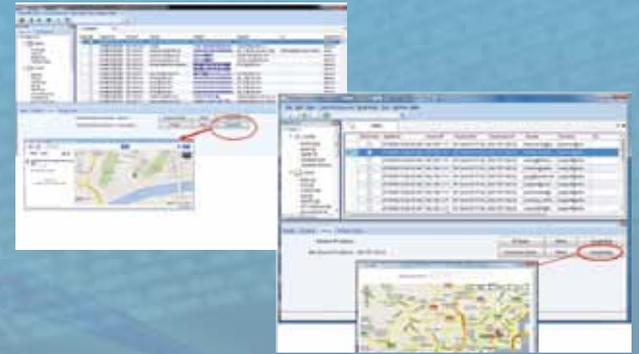
3 Diagram 3 : *WhoIs* Source-Destination Query function and *Google* Map Query function

4 Diagram 4 : Web Browsing (HTTP Content) reconstruction

5 Diagram 5 : Search Function

6 Diagram 6 : Case ManagementT

7 Diagram 7 : Association Analysis

Product Features
(FIT version 2.0):

• Application Software Tool (Windows based)
• Case Management Function
• Support Import of Raw Data Files (in PCAP / CAP Format)
• Detail information includes Date-Time, Source IP, Destination IP, Source MAC etc.
• Search Function (Full Text Search)
• WhoIS and Google Map Integration Functions
• Bookmark Function
• 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, Hangouts(Google Talk), IRC Chat Room, LINE, Fetion, AliWnagWang, FireChat, WiFi Talkie, Serval Mesh), File Transfer (FTP, P2P), Telnet, HTTP (Web Page), Upload/Download, Video Streaming, Request) , Social Network Service (Sina weibo, Sohu weibo, Tencent weibo, 163 weibo, Kaixin, Renren, Q Zone, Linkedin, Odnoklassniki, VK, My World) and Others (TELNET, SSL, SQLLOG).
• Association Analysis
• Support Windows 2000 / XP / VISTA / Windows 7 / Windows 8
• Export analysis data to PDF file
• Provide Sorting Analysis data format

Support more than 140 Network Protocols