

## Forensics Investigation Toolkit (FIT)



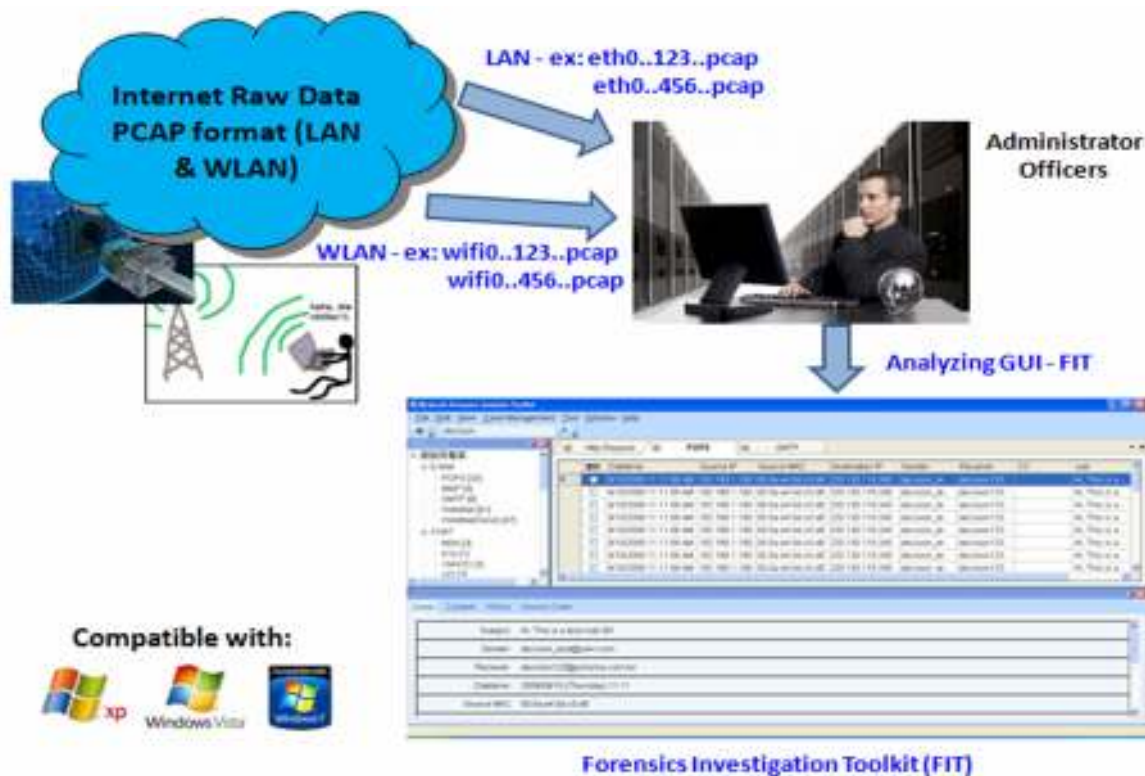
- How do you analyse the raw data (PCAP) files that you have captured from your network?
- Can you understand the encoded content by reading the raw data (PCAP) files using Packet Analyser Tool?
- Can you investigate who is leaking information and what has been leaked out in your organization?

FIT is 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. Developed by Decision Group expert, FIT and E-Detective series of products have now been used extensively by Private and Public organizations, Law Enforcement and Defence Officers and Investigators.

FIT comes with very user friendly Graphical User Interface (GUI) that even allow novice to easily learn and capitalize on the powerful functionality and features of FIT. All protocols and services analysed and reconstructed are displayed in readable format to the users. The GUI much easier to navigate and operate compare with many of the packet analyser tool. 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. Therefore, 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 result.

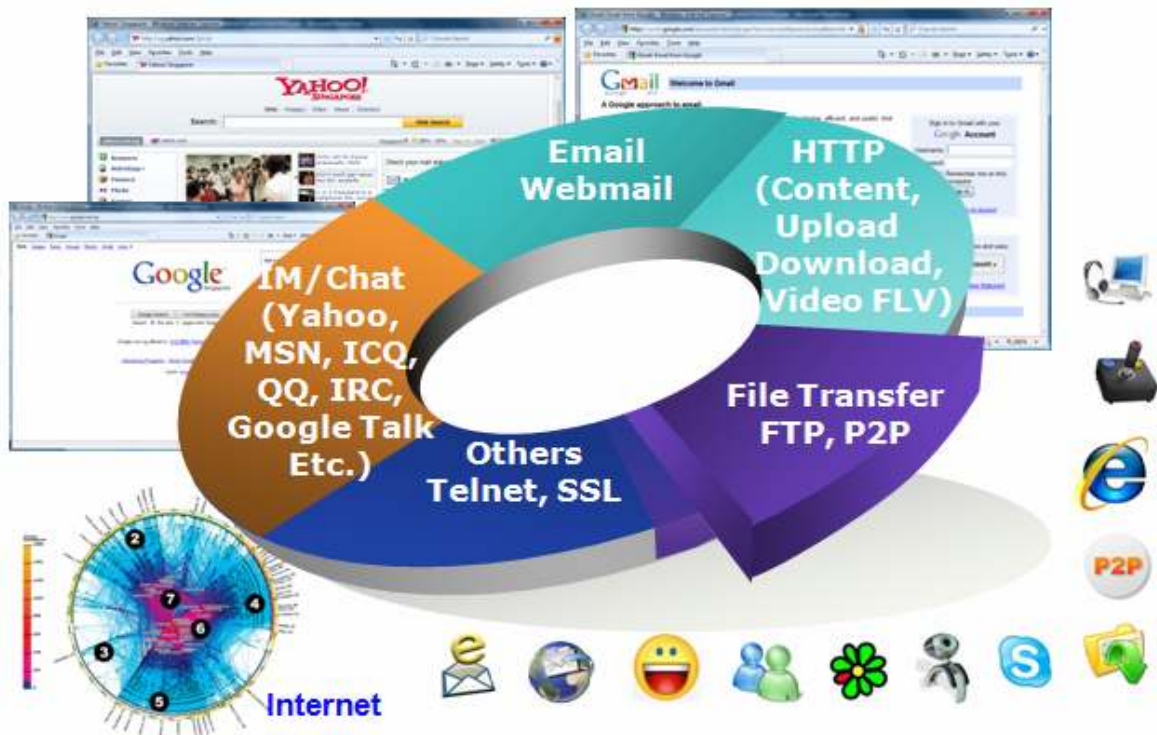
## How It Works?

Raw data files (PCAP) captured from sources like LAN and WLAN can be imported to the FIT accordingly (by selecting the intended case). Imported raw data files will be parsed and the output content will be displayed in intended service categories. Refer to the application diagram below on how the procedures.



## Product Features:

- Application Software Tool (Windows based)
- Case Management
- Support Import of Raw Data Files (PCAP Format)
- Analyse and Reconstruction Various Internet Traffic Types including Email (POP3, SMTP, IMAP), Webmail (Read and Sent), IM/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).
- Detail information includes Date-Time, Source IP, Destination IP, Source MAC etc.
- Search
- WhoIS and Google Map Integration
- Bookmark



*Diagram: Protocol/Services supported by FIT*

## Who Should Use FIT?

- Network Manager and Administrator
- Forensics Investigator
- Risk Analysis and Auditor
- Law Enforcement Officers (Police, Military Intelligence, High Tech Criminal Investigation Agencies etc.)
- Educator

### Some Screenshots of FIT

