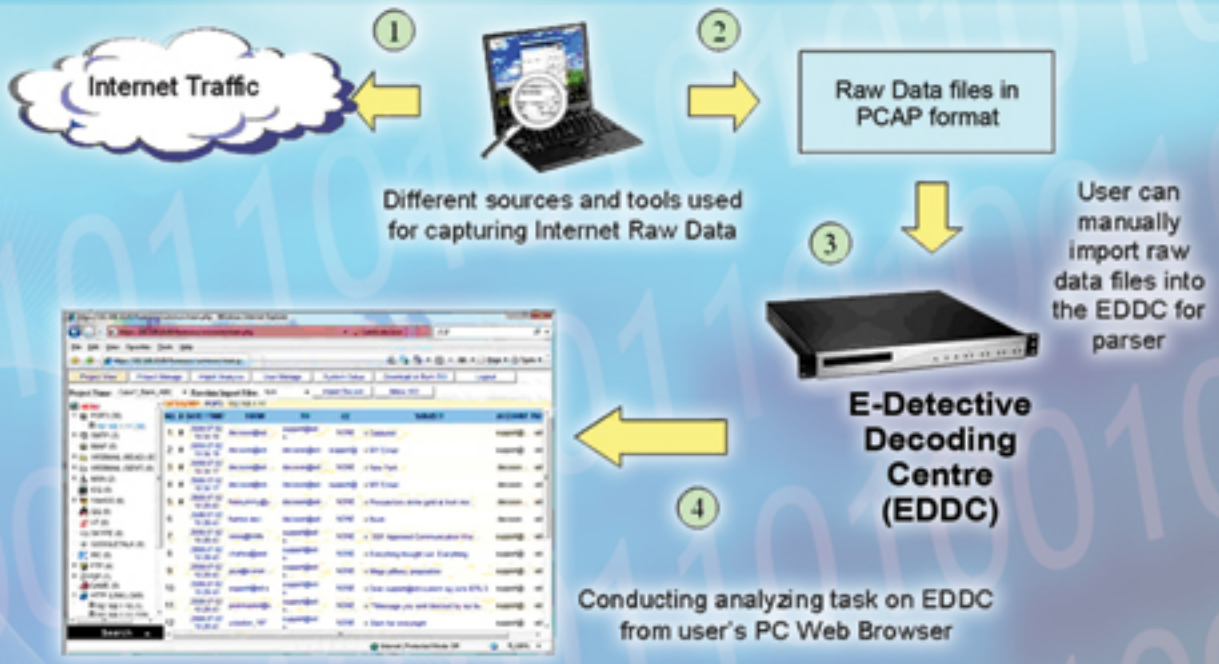
E-DETECTIVE®

E-Detective Decoding Centre - EDDC

Offline Internet Raw Data Reconstruction System



E-Detective Decoding Centre (EDDC) is designed as a Linux based centralized system for offline Internet raw data file parser or reconstruction. It can be used to parse raw data files in PCAP format collected from different sources. Internet raw data packets can be collected from an Ethernet LAN network or a open WLAN network through different packet capturing or sniffing tools such as Wireshark, LinkFerret etc.

EDDC comes with specifically designed features that allow different forensic investigators in an organization to create cases and specify the offline Internet raw data files for decoding and reconstructing on a system. It allows the administrator to create different user accounts and different cases for users or forensic professionals or investigators. The administrator has the flexibility to assign different rights and access levels to different users to manage and access to the reconstructed data on different cases. The users can then import their Internet raw data files collected from different sources into the system to carry out the parser and analysing process.

EDDC allows Internet Content Forensics tasks to be carried out easily and systematically in order to obtain a variety of information and evidence needed from the Internet raw data files collected. EDDC also aims to assist Police Intelligence Services, Military Intelligence Organizations, Intelligence Bureaus, National Security Agencies, Government Intelligence Agencies and all forensics related agencies in conducting Internet Content Forensics geared towards enhancing their investigative effort.

DECISION GROUP
Address : 4/F No.31, Alley 4, Lane 36, Sec. 5, Ming-Sheng East Rd, Taipei Taiwan ROC
Phone : +886 2 27665753 Fax : +886 2 27665702
Email : decision@decision.com.tw ; decision@ms1.hinet.net
URL : www.decision.com.tw ; www.edecision4u.com

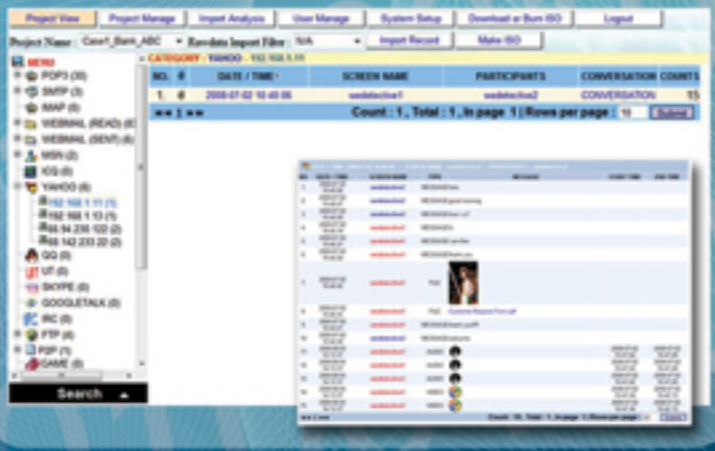
Distributor / Partner :

E-Detective Decoding Centre

Parser and Reconstruction (Sample Screenshots)

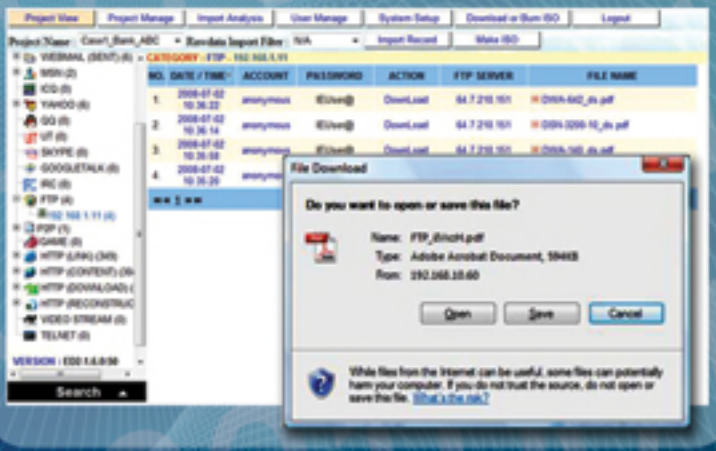
1. Email (POP3, SMTP, IMAP, Webmail)

2. IM/Chat (Yahoo, MSN, ICQ, IRC etc.)

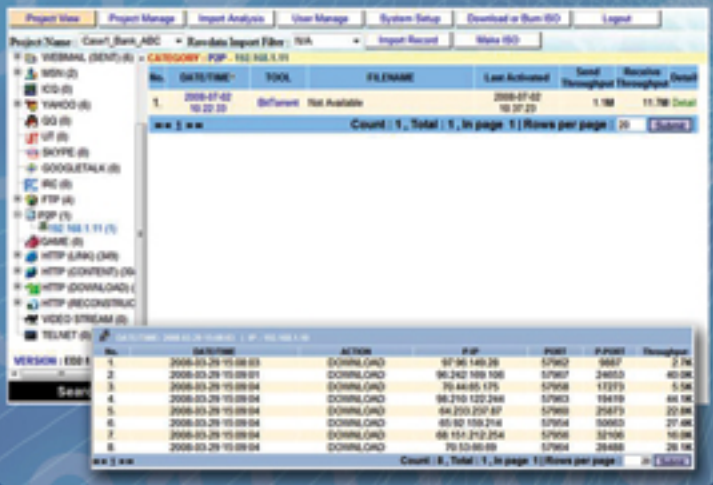


3. HTTP (Link, Content, Reconstruct)

4. FTP



5. P2P



Administrative and Management

1. Case Management (Sample Screenshots)

2. User Management

3. Full Text Search

Note : Internet protocols decoded by EDDC includes Email (POP3, SMTP, IMAP), Webmail (Yahoo Mail, Windows Live Hotmail, Gmail etc.), IM/Chat (Yahoo, ICQ, AOL, MSN, IRC, Google Talk TW, QQ, Skype Voice Call Session Log), File Transfer (FTP, P2P), HTTP (Link, Content, Reconstruct, Upload/Download, Video Stream), Online Game and Telnet.