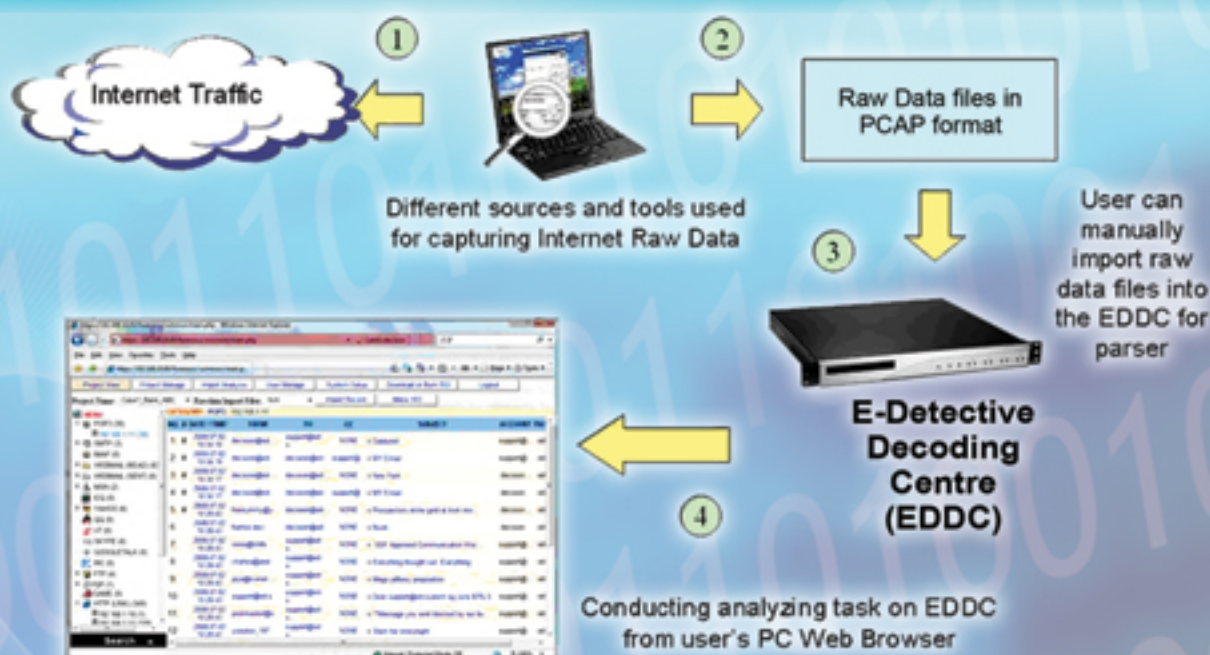




E-Detective Decoding Centre - EDDC

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.eddecision4u.com

Distributor / Partner :



Parser and Reconstruction (Sample Screenshots)

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

The screenshot displays the 'Email' category in the EDDC interface. It shows a list of email items with columns for No., Date/Time, From, To, CC, BCC, Subject, and Message Type. A detailed view of an email is shown, including headers and body text.

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

The screenshot displays the 'IM/Chat' category in the EDDC interface. It shows a list of chat items with columns for No., Date/Time, Screen Name, Participants, and Conversation Count. A detailed view of a chat conversation is shown, including participant names and chat messages.

3. HTTP (Link, Content, Reconstruct)

The screenshot displays the 'HTTP' category in the EDDC interface. It shows a list of HTTP items with columns for No., Date/Time, Account, Password, Action, FTP Server, and File Name. A detailed view of an HTTP content item is shown, including the reconstructed content.

4. FTP

The screenshot displays the 'FTP' category in the EDDC interface. It shows a list of FTP items with columns for No., Date/Time, Account, Password, Action, FTP Server, and File Name. A 'File Download' dialog box is shown, asking if the user wants to open or save the file.

5. P2P

The screenshot displays the 'P2P' category in the EDDC interface. It shows a list of P2P items with columns for No., Date/Time, Tool, Filename, Last Activated, Seed, and Receive Throughput. A detailed view of a P2P item is shown, including the file name and throughput.

Administrative and Management

1. Case Management (Sample Screenshots)

The screenshot displays the 'Case Management' section in the EDDC interface. It shows a table of cases with columns for Case Name and Function. A 'Create New Case' button is visible.

2. User Management

The screenshot displays the 'User Management' section in the EDDC interface. It shows a table of users with columns for User, Authority, Creation Date/Time, and Function. A 'Create New User' button is visible.

3. Full Text Search

The screenshot displays the 'Full Text Search' section in the EDDC interface. It shows a search results table with columns for No., Date/Time, User, Tag Name, File, Date, File Date/Time, and File Source. A search bar and filters are visible.