FED Forensics E-Detecitve
網路封包解譯鑑識系統

網路封包解譯鑑識系統Forensics E-Detective(FED)」適用於專案型或任務型網路封包鑑識，可安裝於輕便型的獨立主機，做為可攜式之網路封包鑑識工具，接收解譯還原online或offline網路封包。

使用者可針對不同任務於系統內建立不同專案，專案皆為各自獨立。不同目標的網路封包各自保留於獨立區域，避免資料互相混雜。

網路封包內容還原是網路鑑識重要一環。FED具備Email、Webmail、FTP 、P2P、Telnet、WebSite、Video Stream、VoIP(Option)、HTTPS(Option)等網路協定解析，力求網路封包內容可視性。

除了具備條件式搜尋功能、使用者可透過日期/時間/IP/Email帳號...等條件查找之外，系統並提供全文檢索功能，利用關鍵字針對已解析的資料進行快速檢索，大幅節省作業時間。

因應不同網路封包來源，系統具備「有線網路封包」、「有線網路之HTTPS / SSL加密網路連線封包(option)」及「離線網路封包」等網路封包擷取處理模式。系統可在Online模式下，利用SnifferMode或是Man-in-the-middle(MITM)方式擷取封包、也可在Offline模式下，匯入原始封包檔後，進行網路封包解析。在任務需求下，系統可保留原始封包檔並匯出。

多樣化網路封包接收模式適用於各種網路環境、不同任務專案各自獨立、不同目標網路資料互不混餚、支援多種網路協定解譯、條件式搜尋/全文檢索可快速查找所需資料...，FED是可攜式網路封包鑑識最佳工具。

定興科技股份有限公司
DECISION GROUP INC.
www.edecision4u.com | www.internet-recorder.com.tw
TEL:(02)2766-5753|FAX:(02)2766-5702|
地址:台北市松山區民生東路五段36巷4弄31號4樓