副本

東吳大學_網路封包鑑識分析工具次測試研究

定興科技有限公司

委託學術研究契約書

網路鑑識分析工具之測試研究

網路鑑識分析工具委託測試研究契約書

立約人定興科技有限公司(以下稱「甲方」)及東吳大學(以下稱「乙方」)。緣甲乙雙方為進行網路鑑識分析工具 Network Forensic Analysis Toolkit 測試研究事宜，特立本契約，並同意條件如下：

第一條：雙方合意

甲方同意委託乙方執行網路鑑識分析工具之測試研究(以下稱「本研究」)，乙方同意承包，從事本研究。

第二條：研究內容

本研究之內容如附件:定興科技有限公司專題測試研究計畫申請書(以下稱「申請書」)。

第三條：研究進度

本研究執行期間自民國九十九年三月十五日起至民國一百年三月十四日止。

第四條：研究進度

一、乙方應依申請書之約定，進行本研究。

二、甲方得視需要要求乙方就本研究之進度提出口頭報告及相關資料，或派人員至乙方了解乙方執行本測試研究之情形。乙方對該人員應提供一切必要之協助。

第五條：成果交付及驗收

一、乙方應於每階段完成後繳交報告予甲方。

二、乙方應依申請書之規定期間繳交期末測試研究成果。

第六條：研究費用

本研究之費用總計新台幣(下同)NT$壹拾柒萬捌仟捌佰貳拾肆元整，其細目如申請書。

第七條：付款辦法

1.本契約生效後支付 30,000 元

2.本契約生效後每隔三個月支付 25,000 元，共 4 期。

3.期末結案後支付 48,824 元

第八條：保密義務

乙方為執行本契約所取得或持有的資訊，非經甲方事先書面同意，不得洩漏或交付予任何第三人或運用於本契約無關之工作。乙方應要求其參與本研究之人員遵守本契約之約定。乙方或其參與本研究之人員違反本條契約約定者，乙方應負責賠償甲方因此所受之損害。

第九條：契約份數

本契約壹式肆份，正本貳份，副本貳份，由乙方執正本壹份，副本壹份，甲方執正本壹份，副本壹份

立合約書人：

甲方：定興科技有限公司
代表人姓名：張侃總經理
電話：02-27665753
地址：台北市民生東路五段 36 巷 4 弄 31 號 4 樓
統一編號：25009669

乙方：東吳大學
代表人姓名：黃鎮台校長
電話：02-23111531
地址：台北市士林區臨溪路 70 號
統一編號：29902605
計畫主持人：連志誠副教授

中 華 民 國 九 十 九 年 三 月 十 五 日

定興科技有限公司專題測試研究計畫書

機構/系所(單位)	東吳大學
本計畫主持人姓名	連志誠
職稱	副教授
本計畫名稱	網路封包鑑識分析工具之測試研究
全程執行期限	自民國九十九年三月十五日起 至民國一百年三月十四日
計畫聯絡人	連志誠副教授
通訊地址	台北市貴陽街一段 56 號
電話號碼	02-23111531 ext.3803
E-Mail	cclien@csim.scu.edu.tw

東吳大學 總幹事
東騎

預期人力

級別或姓名	人數	月數	總計
連志誠	5,000 元/月	12 月	60,000 元
學生 1(待聘)	3,000 元/月	12 月	36,000 元
學生 2(待聘)	3,000 元/月	12 月	36,000 元

經費

項目	金額
人事費	132,000 元
雜費(差旅費、文具、影印、紙、碳粉匣、光碟、、、等)	20,000 元
管理費	26,824 元
總計	178,824 元

本研究功能規格如下：

1 軟體式，安裝在 Windows 環境下使用。

2 有使用者與專案之概念，可依據不同使用者建立不同的專案，同時使用者也可建立不同專案

3 可針對 Email 封包(POP3、SMTP、IMAP、Webmail)、FTP 封包、Instant Message 封包(MSN、ICQ、Yahoo Message、QQ、UT Web Chat)、Website 封包(HTTP & HTTP content & Web site Download or upload)、Telnet 封包等進行解譯還原。

4 E-Mail 記錄：

4.1 POP3、SMTP、IMAP：清單可記錄每封收到 E-Mail 的詳細相關資訊，包括收信日期、時間、寄件者、收件者、副本、主旨、大小和附加檔案，SMTP 含密件副本，並還原郵件內容及附加檔案內容，並可查看信件之原始封包記錄。

4.2 Webmail 記錄：

4.2.1 送出的網頁郵件記錄包含日期、時間、寄件者、收件者、副本、密件副本、主旨、附加檔案、Web Mail Server 名稱。

4.2.2 可記錄利用網頁接收支援的 Web Mail 內容。

4.2.3 可記錄還原 YAHOO MAIL、YAHOO 2.0、GMAIL、HOTMAIL、HINET、SEEDNET、URL、PCHOME、SINA、YAM、GIGA、163.net、mail.tom.com、mail.163.com、sohu.com、INTLJOB、GO2CANADA、MEDIAHUB、PRODATA、WINDOWS LIVE 等 20 種（含）以上之 Web Mail Server。

4.3 信件轉送：提供過濾 E-Mail 的功能，可以依照需求設定一些條件，系統會記錄符合條件的 E-Mail，並複製一份給您所指定的人員。

5 FTP 記錄：可記錄日期、時間、使用者電腦的 IP、使用者名稱、密碼、上傳或下載的檔案內容。

6 P2P 記錄：可記錄日期、時間、使用者電腦的 IP(含 MAC 資訊)、使用者名稱、使用的 P2P 工具軟體、下載的檔案名稱、最後下載的時間、送出及收入的流量、並詳細記錄所聯結的 IP、傳輸的動作(上傳或下載)、雙方使用的 port 以及各連結傳輸的流量，並主動透過系統連結 Whois 反查詢 IP 或 hostname。

7 Telnet 記錄：各類 Telnet 連線登入或登出行為記錄及原文播放式呈現。

8 Instant Message 記錄：

8.1 可記錄日期、時間、使用者代號、IP(含 MAC 資訊)、對談者和對談內容及附加檔案。

8.2 可記錄 MSN、Web MSN、ICQ、Yahoo Message、Google Talk、QQ、IRC 及 UT 網路聊天室等即時通訊訊息。

8.3 提供匯出指定 Instant Message 聊天內容的功能，以日期為期間條件匯出所有聊天的內容。(Excel 格式)

8.4 可還原 Yahoo Messenger 之影像及語音內容及來源、目的網址解析。

8.5 提供 Skype 使用記錄，可記錄日期、時間、使用者代號、對談者代號、對談者 IP(含 Domain Name 資訊)、對談時間，並可選購 Skype agent 取得 Client Skype 使用內容。

8.6 MSN、Yahoo messenger 提供使用者所有的好友名單。

9 WebSite 記錄：

9.1 記錄使用者瀏覽過的網址和網頁的內容，包括日期、時間、使用者 IP（或使用者名稱含 MAC 資訊）和網址，並可記錄透過網頁上傳及下載之檔案內容。

9.2 提供網頁還原功能，能夠組織並還原使用者瀏覽網頁的實際網頁畫面。

9.3 提供影音串流記錄：可記錄日期、時間、使用者電腦的IP(含 MAC 資訊)、使用者名稱、下載主機名稱及 URL、下載影片檔名、內容及大小，並可播放下載之影片內容。

9.4 提供ICAP Server接收ICAP Client傳輸的網頁封包並加以還原

9.5 可選購 HTTPS 解譯模組，解譯還原 HTTPS 網頁封包

10 提供連線遊戲記錄，包含遊戲橘子楓之谷、遊戲橘子跑跑卡丁車、遊戲橘子爆爆王、遊戲橘子瑪琦、華義熱血江湖、中華網龍黃易群俠傳、中華網龍新蜀山劍俠、因思銳暗黑、BLIZZARD 魔獸世界、網伊 YNK 洛汗、EST 黑色陰謀、koei 大航海時代等八十種(含)以上。

大學章

11 提供全文檢索功能，可輸入關鍵字，在所有的網路服務下尋找相關資料，也可單獨在各網路服務下輸入搜尋條件尋找。

吳東騎

12 提供條件式搜尋功能，可設定日期及時間範圍、使用者 IP、Email 帳號、MSN 帳號等各種相關資訊尋找記錄內容。

13 提供側錄檔案清單搜尋功能，可將需尋找的檔案匯入系統，系統會自動將檔案內容相同，無論檔案名稱是否相同或遭竄改的檔案尋找出來，並可經由檔案追查到使用的服務、日期時間及使用者。

Address : 4/F NO. 31, ALLEY 4, LANE 36, SEC. 5, MING-SHEN EAST ROAD, TAIPEI 105, TAIWAN. R.O.C
TEL : +886-2-2766-5753/ 2769-5496 FAX : +886-2-2766-5702/ 2756-9591 URL: www.decision.com.tw
URL: www.edecision4u.com Email: decision@ms1.hinet.net decision@decision.com.tw

14 系統提供附加檔案資訊列表，透過列表資料查看檔案寄送及接收資訊。

15 提供帳號清單，記錄所有進出使用的帳號，並可以 IP 查詢所有協定使用過的帳號。

16 提供查詢書籤功能，設定書籤可記錄查詢當下的結果，也可將書籤的結果匯出成 ISO 檔案以供查詢。

17 提供未知封包連線記錄分析，可將 UDP、TCP 等連線將日期時間與來源及目的 IP、通信埠、MAC、封包大小、封包數量，可直接排序過濾，也可依照日期時間與來源及目的 IP、通信埠、MAC、封包大小、封包數量等欄位過濾分析及進階的條件式過濾分析。

18 系統控制功能：

18.1 系統使用者帳戶管理，可設定使用者帳號、密碼、群組、權限，透過權限設定分層管理。

18.2 中文操作介面及結果顯示均能支援繁體中文及英文格式。

大學 章 鑒