於 Gigabit 被動光纖網路下多媒體串流鑑識系統之設計 —以 MSN 即時通訊為例

蘇暉凱*[a]、洪丞緯[b]、吳光閔[b]
國立虎尾科技大學電機工程系[a]
南華大學資訊管理研究所[b]
Email: hksu@nfu.edu.tw*

摘要 — 光纖到府已成為目前逐漸普遍之網路接取服務，GPON (Gigabit PON) 採用點對多點 (point to multi-point；P2MP) 之架構，大量降低光纖使用量以達到節省成本支出。現今即時通訊興起與普及，使用者可在任何時間地點透過即時通訊進行即時性文字或影音會談。然而網路行為是使用者所觸發，透過網路知識多元化與上網速度之提升，駭客行為日漸複雜，故本研究設計 GPON 環境多媒體串流數位鑑識系統，記錄使用者 MSN 即時通訊行為並將相關資訊資料庫中，提供數位鑑識時所需之相關資訊。

一、 前言

隨著資訊時代來臨，網際網路之頻寬日漸增加，而網路資訊科技之應用也漸趨多元，使用者使用網路服務之行為也日漸複雜。透過網路，使用者可開會工作、交易購物、認識朋友與取得多方面知識…等，由於網路知識容易取得之特性，使用者透過網路學習駭客行為攻擊其他使用者之比例日漸提高，故資訊在傳輸時所帶有之風險也日漸增加。許多攻擊行為發生後要追查之時效性有限，使用者電腦之環境亦容易遭到更改或破壞，故本研究設計一多媒體串流鑑識系統，透過見識可還原攻擊行為當下之即時通訊應用狀態。

傳統之資訊安全設備與技術大多以保護與偵測攻擊行為為主，少有提供網路行為紀錄之鑑識系統，故在發生攻擊行為後常難以追查攻擊者之主機與身分。使用即時通訊時，使用者容易受到詐騙或因接收帶有病毒之檔案而導致電腦遭受攻擊，故本論文透過以 MSN 即時通訊為例透過會談分類技術提出一多媒體串流鑑識系統記錄使用者上網行為，透過本系統所設計之 Snooping Agent 元件放置於 GPON ONU 前擷取 MSN 會談封包，並透過 Analyzer Server 元件分析使用者之 ID、狀態、暱稱與好友名單，以 Media Processing Server 元件分析還原出影音串流與檔案傳輸串流並儲存於資料庫中。

當使用者使用即時通訊之影音串流或檔案傳輸服務時遭受到攻擊，在事後可透過鑑識系統所擷取之資訊找出攻擊者之主機與身分，本研究之設計即為提供數位鑑識時所需之相關檔案資訊。

二、 背景

本研究設計之系統建構於 Gigabit 被動光纖網路上，以 MSN 即時通訊應用為例，並將擷取之多媒體串流資訊重組還原儲存於資料庫中，未來可提供數位鑑識時所需之相關網路串流資訊。

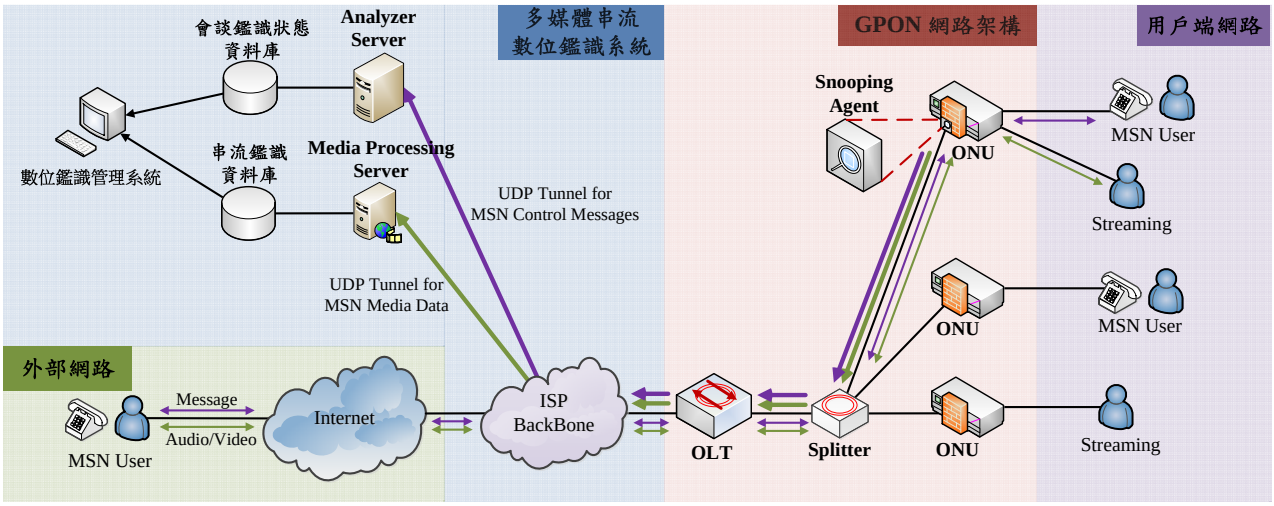
2.1 Gigabit 被動光纖網路

Gigabit 被動光纖網路又稱為 GPON (Gigabit Passive Optical Network)，GPON 之系統設備由局端設備 (Optical Line Terminal, OLT)、遠端設備 (Optical Network Unit, ONU) 與被動式分光器 (Passive Optical Splitter, POS) 組成。傳統之 EPON [1] 之架構為點對點拓樸架構，一條光束最多可經由 OLT 分給 32 台 ONU 使用，其傳輸速率最大可支援上下行 1.25 Gbps 之對稱速率，最大傳輸距離為 20 公里；GPON [2] 之架構提供點對多點拓樸架構，一條光束最多可由 OLT 分給 64 台 ONU 使用，傳輸速率最大可支援上下行 2.5 Gbps 對稱速率，最大傳輸距離為 20 公里。傳統 EPON 之架構容易浪費光纖佈建時之使用量，GPON 架構之應用則可大降低光纖使用量，進而達到節省成本與支出。由於 GPON 為目前唯一可在單一波長下提供 2.5 Gbps 頻寬之技術，具有高頻寬、高效能、傳輸距離遠與支援多種服務 (如：語音 (Voice Communications)、影像 (Video)、視訊會議 (Video Conferencing)、數據 (Data Traffic) 與綜合數位信號傳輸 (Digital Signal Transmission))，GPON 提供 QoS 保證能力，包含分時多工 (Time-Division Multiplexing, TDM)、Data、Video 等保證要求，為目前支援較多服務之網路類型，故更能適應為來 FTTx 之頻寬系統。

2.2 會談串流應用

2.2.1 MSN 即時通訊

MSN 即時通訊 (The Microsoft Networks Messenger)



圖一： 多媒體串流數位鑑識系統架構圖

[3][4] 是由微軟公司於 1995 年開發之即時通訊軟體，初版軟體只提供網路即時通訊之服務 [5]，在軟體更新至 8.0 後改名為 Windows Live Messenger，簡稱 WLM，目前最新版本為 WLM 15。新版除了提供即時通訊之服務外，也提供與其他即時通軟體互通之功能、撥打一般電話、小遊戲與使用其他應用程式…等服務 [6]。MSN 即時通訊之傳輸協定為 MSNP，其運作原理類似於 FTP，透過命令與回應兩種傳輸；但 MSN 即時通訊協與 FTP 傳輸協定之不同點在於 MSNP 之命令及回應是屬於多行 (與 MSN Server 連線時為多行，完成後則恢復為單行)，以及 MSNP 在收到命令時會自行回傳回應。；MSN 交談時將透過三台 Server 傳輸訊息，分別為：Dispatch Server (DS)、Notification Server (NS) 與 Switchboard Server (SB)。其功能分別為：

1) DS：用來指引使用者連接到 NS。
2) NS：提供 MSN 連線，記錄個人資訊與好友名單，並通知使用者之上下線狀態與好友狀態。
3) SB：提供使用者溝通之交換伺服器，透過此伺服器可交換文字訊息、視訊會談服務與檔案傳輸等服務功能。

2.3 多媒體串流

傳統網路影音播放都需先透過下載才能撥放，而此做法需花費時間下載並需有足夠儲存空間。現今多媒體串流服務乃透過影音伺服器傳送影音封包，當使用者欲使用影音服務時，會先從伺服器下載部分影音檔案撥放，使用者可一邊下載一邊撥放，不需等完整影音檔案下載完成才撥放。此串流影音做法之優點，除可避免下載時等待之時間外，亦不會浪費多餘的儲存空間。[7]

2.4 數位鑑識

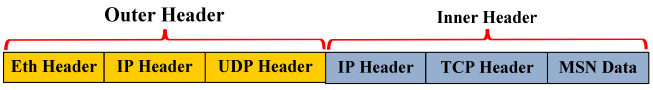
數位鑑識又稱為電腦鑑識，由於資訊科技發達，在高科技資訊化之環境中涉及電腦之犯罪案件多不勝數，鑑識人員已無法利用傳統蒐證方式採集證據，故需透過電腦鑑識技術來輔助振查與還原環境。透過數位行為之紀錄與保存，鑑識人員可利用鑑識工具與系統還原案發當時之環境與系統狀態。[8]

三、 系統架構

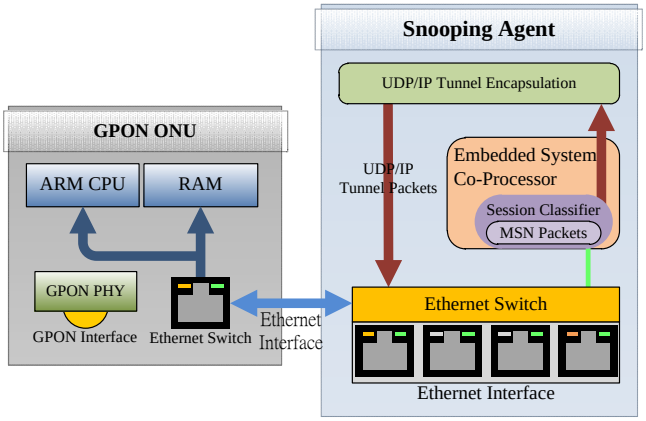
圖一為本論文之系統架構圖，底層為現有之 GPON 網路環境，包含用戶端 ONU 與局端 OLT，中間利用 Splitter 元件串接，本元件所設計之元件，後端部分包含 Analyzer Server、 Media Processing Server 及資料庫與多媒體串流數位鑑識系統。

當外部使用者經由 GPON 網路連接用戶端網路與內部使用者溝通時，鑑識系統可從 ONU 端擷取到使用者所傳遞之控制訊息 (紫色細線資料流) 與影音串流 (綠色細線資料流) 之封包，當系統從 ONU 擷取到 MSN 即時通訊之封包時透過本論文所設計之 Snooping Agent 元件，利用 UDP/IP Tunnel 封裝技術將所擷取之使用者控制資訊傳送到 Analyzer Server (紫色粗線資料流)，並且將會談媒體資料傳送到 Media Processing Server (綠色粗線資料流)。所謂 UDP/IP Tunnel 封裝技術是將原本所擷取之 MSN 封包再封裝 UDP 之標頭與目的地 IP 位址後，封裝成 UDP 封包送往所要到達之目的地，UDP/IP Tunnel 封裝結構如圖二。

當後端多媒體鑑識系統元件收到擷取控制訊息之 Tunnel 封包時，Analyzer Server 將封包解封分析使用者 ID、使用者狀態與暱稱；Media Processing Server 解封後分析出影音與檔案傳輸之封包，重組還原並儲存於資料庫中。在本論文設計之多媒體鑑識系統中可透過一多媒體串流數位鑑識系統呈現出使用者之 ID、狀態與暱稱並顯示其使用 MSN 即時通訊會談之相關內容與資訊，並且提供 MSN 鑑識資料查詢。



圖二： UDP/IP Tunnel 封裝示意圖



圖三： Snooping Agent 元件設計圖

本研究之系統元件設計主要為 Snooping Agent、Analyzer Server、Media Processing Server 與數位鑑識管理系統。

3.1 元件設計

3.1.1 Snooping Agent

本系統之 Snooping Agent 元件可以整合 GPON ONU 設備，擷取使用者資訊與會談服務之封包並傳輸至後端多媒體串流鑑識系統。

本系統設計之 Snooping Agent 元件設計如圖三，當 MSN 即時通訊使用者之封包流過 ONU 時，本元件將配置於 ONU 前端，封包會從 Snooping Agent Ethernet Interface 流入，本元件將過濾及複製一份 MSN 封包，並透過 UDP/IP Tunnel 封裝技術將封包從本元件之 Ethernet Switch 與 GPON ONU 連接之 Ethernet Switch 進入 GPON 網路中傳送至後端多媒體串流鑑識系統。當本元件擷取封包時，將透過會談分類之方式過濾擷取出 MSN 封包並複製一份透過 UDP/IP Tunnel 封裝技術傳輸至後端多媒體串流數位鑑識系統進行會談封包分析，故本元件之設計並不影響正常流量之傳輸。

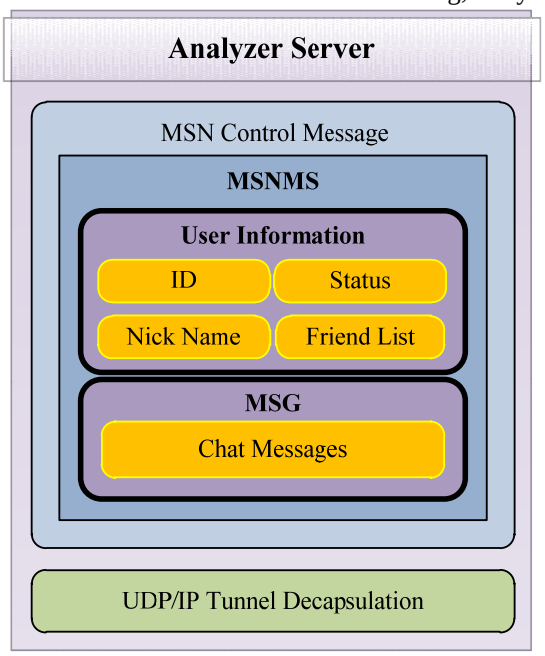
3.1.2 Analyzer server

本研究設計之 Analyzer Server [9] 乃透過一狀態式封包分析器，在不影響正常封包傳輸情況下，根據會談傳輸時所擷取之封包取出會談控制資訊，且加以分析並管理儲存至資料庫中。

本系統之 Analyzer Server 元件設計如圖四，當 Analyzer Server 接收到從 Snooping Agent 所擷取之 MSN 控制資訊封包時，本元件將從 UDP/IP Tunnel 封裝之封包解封出 MSNMS 之封包並分析出使用者之帳號、狀態與暱稱；由於 MSN 即時通訊之文字會談內容並未加密，故本系統可透過 Analyzer Server 元件分析出文字聊天內容，並將所分析之使用者資訊與文字聊天內容儲存於資料庫中。

3.1.3 Media Processing Server

本研究所設計之 Media Processing Server 如圖五，透過 Media Processing Server 可從 Snooping Agent 所擷取之 MSN 即時通訊多媒體串流封包，並透過重組還原成原始影音之檔案並儲存於資料庫中。



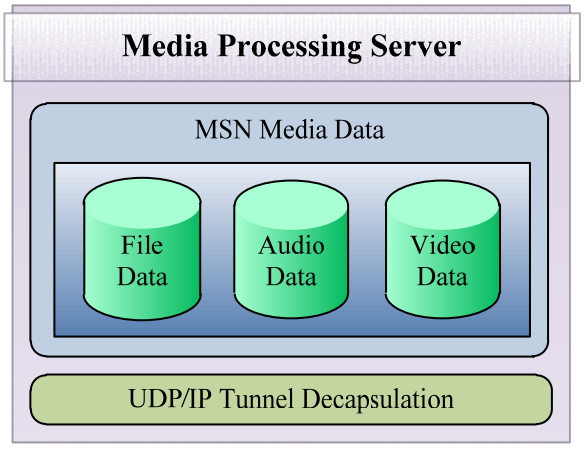
圖四： Analyzer Server 元件設計圖

當 Media Processing Server 收到 Snooping Agent 所擷取之 MSN 多媒體資訊時，本元件會先將 UDP/IP Tunnel 封裝之封包解封出 MSN 多媒體串流封包，並將其中所包含之會談服務資訊重組還原，本元件所還原之內容包括：視訊會談、音訊會談與檔案傳輸，並將所還原之會談內容儲存至資料庫中以便日後數位鑑識時可查看。

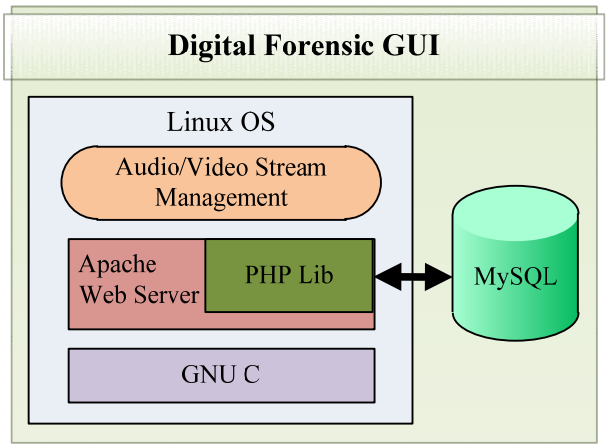
3.1.4 數位鑑識管理系統

本研究透過 Linux、GNU C Lib、Apache HTTPd/PHP 與 MySQL Server…等 open source，設計出一多媒體串流數位鑑識系統，透過本系統可檢視系統所擷取之相關會談影音資訊。

本研究所設計之數位鑑識管理系統元件如圖六。本系統透過 Web Server 連接 MySQL 資料庫，以 PHP 程式語言透過 Web 管理介面，將所需查詢之使用者資訊與會談傳輸資料顯示於鑑識系統之網頁介面。

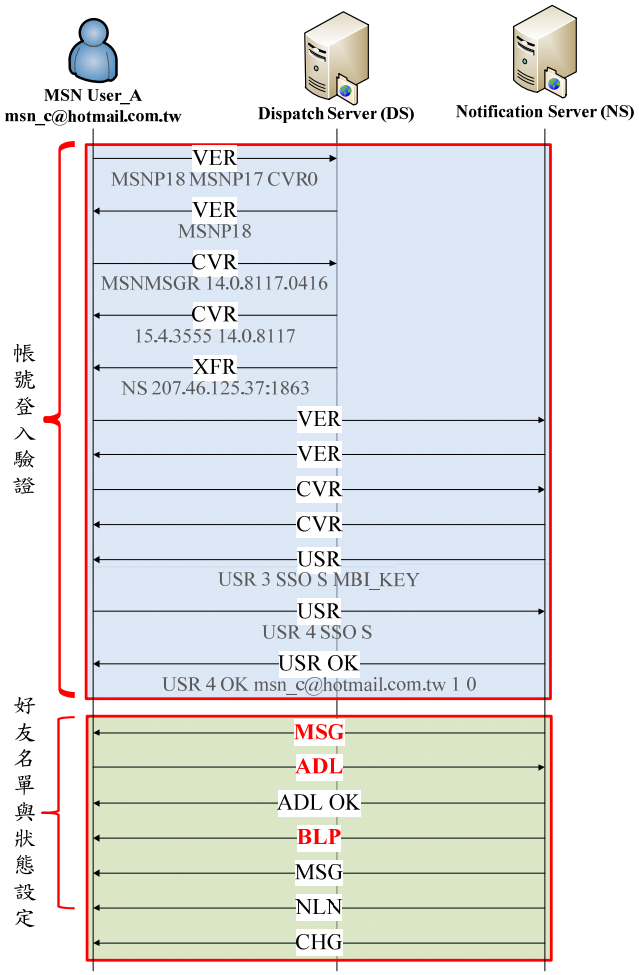


圖五： Media Processing Server 元件設計圖



圖六： 數位鑑識管理系統元件設計圖

當網路管理者需要數位鑑識時，網路管理者可透過本系統提取使用 MSN 即時通訊之使用者資訊，並找出某段時間中使用文字會談、檔案傳輸與視訊影音服務之資訊。



圖七： MSN 即時通訊登入序列圖

四、 案例說明

4.1 MSN 傳輸說明

MSN 即時通訊在連線時將透過三台 Server 建立連線，分別為：Dispatch Server (DS)、MSN Passport Server、Notification Server (NS)與 Switchboard Server (SB)；當 MSN 即時通訊連線時，使用者首先將先連接至 Dispatch Server 要求連接至 Notification Server，此時 MSN Passport Server 將會驗證使用者之帳號密碼，正確後將連接至 Notification Server 建立連線，當兩方連線成功後透過 Switchboard Server 傳輸互動。

4.2 MSN 即時通訊登入

MSN 即時通訊登入連接序列圖如圖七。當 MSN 登入連接時，使用者將連接到 NS，此時使用者須先連接至 DS 要求 NS 之真正 IP 位址。當使用者將登入即時通訊時，使用者會先對 DS 發出 VER 命令要求檢視其通訊協定版本並收到 DS 所回傳之目前使用版本，之後使用者會對 DS 發出 CVR 之命令檢視其軟體版本是否為最新版並會收到 DS 回傳最新版號並詢問是否需要更新，當檢查完成後 DS 便會發送 XFR 命令告知使用者 NS 之 IP 位址。

當使用者連接到 NS 時，伺服器同樣會檢查使用者之通訊協定與軟體版本，檢查完成後會發送 USR 命令 (USR 3 SSO S MBI_KEY) 要求認證使用者之帳號密碼，使用者在收到命令後會回傳 USR 命令 (USR 4 SSO S) 驗證，伺服器在驗證完成後會回傳 USR OK 命令告知使用者驗證完成。

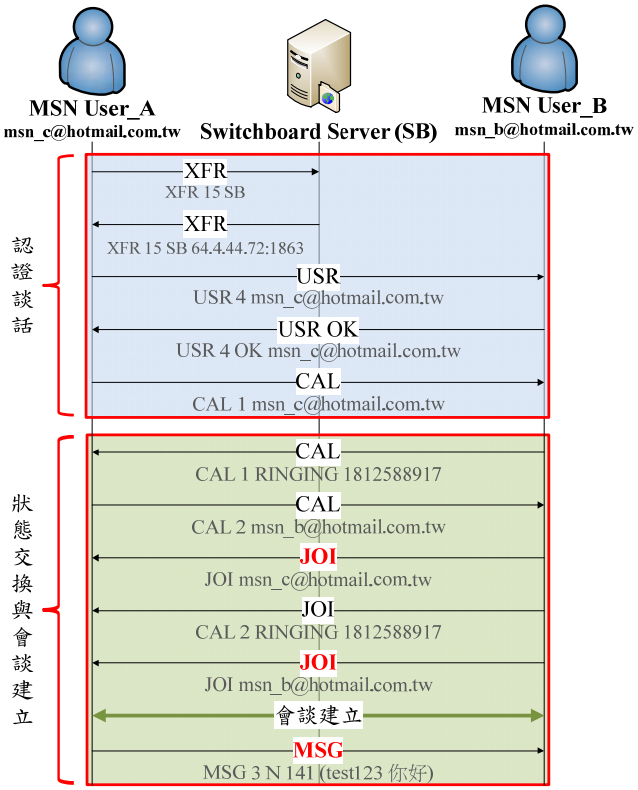
驗證完成後，NS 會發送 MSG 命令初始化使用者資訊，使用者會發送 ADL 命令要求下載好友名單並收到 NS 回傳 ADL OK 命令完成與 BLP 命令之黑名單，最後 NS 會發送 NLN 命令代表使用者上線，並發送 CHG 命令更改使用者之狀態。

當本系統需擷取使用者資訊時，可透過使用者登入之流程，擷取 MSG 命令中之資訊並利用 Analyzer Server 分析出使用者之個人資料，擷取 ADL 命令並利用 Analyzer Server 可分析出使用者之好友名單，擷取 BLP 命令並利用 Analyzer Server 可分析出使用者之黑名單。

4.3 MSN 文字交談

MSN 即時通訊之文字會談序列圖如圖八。在使用文字會談服務時，使用者所傳輸之訊息會先將文字內容傳送到 SB，再由 SB 送至對方。其詳細說明如下。

當使用者欲透過 MSN 即時通訊使用文字會談時，使用者 A 會先與 SB 建立聊天連線，使用者 A 透過 XFR 命令 (XFR 15 SB) 由 SB 通知使用者轉向指定之 NS 並使用 USR 命令 (USR 4 msn_c@hotmail.com.tw) 認證使用者身份。當驗證完成後，使用者 A 將發送 CAL 命令 (CAL 1 msn_c@hotmail.com.tw) 於使用者 B，當使用者 B 收到後則會回傳 CAL 命令 (CAL 1 RINGING 2074159497) 封包，此時代表會談將要建立。最後，當使用者 B 傳送 JOI 命令至使用者 A 時，代表兩方將加入會談，此時會談即建立。當使用者發出訊息時將會接收



圖八： MSN 即時通訊文字交談序列圖

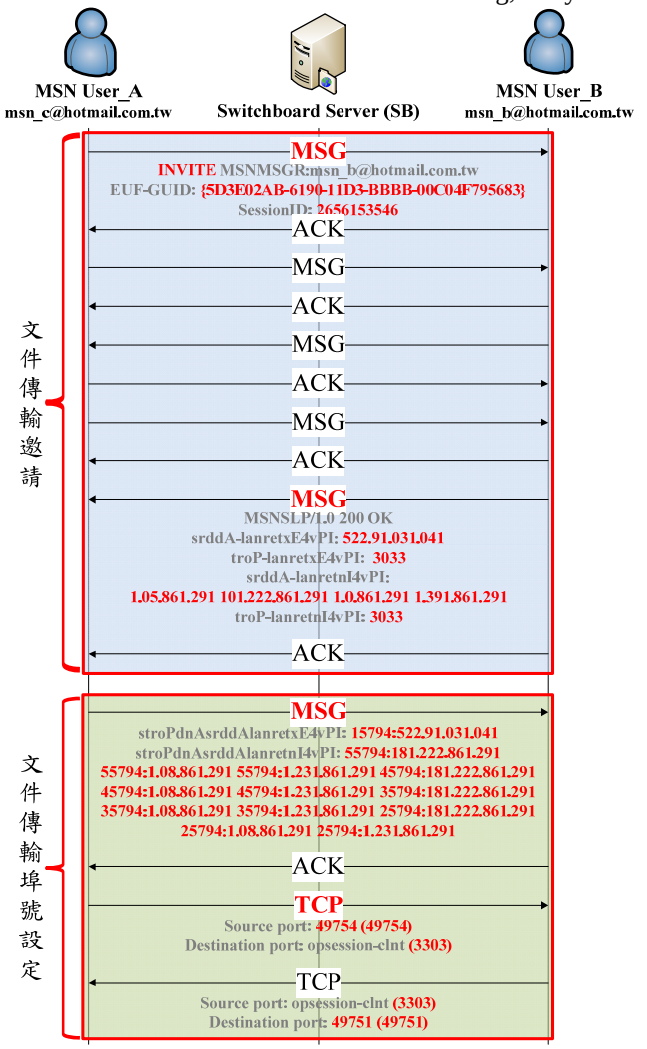
到 MSG 命令 (MSG 3 N 141 (test123 你好)) 帶有其文字交談之內容。

當本系統欲擷取使用者文字聊天訊息時，系統可透過擷取會談建立時之 JOI 命令，本系統之 Analyzer Server 可分析出使用者文字交談之對象 ID，透過擷取 MSG 命令本系統之 Analyzer Server 可分析出使用者之文字聊天內容。

4.4 MSN 檔案傳輸

MSN 即時通訊之檔案傳輸序列圖如圖九。當使用者 A 欲透過 MSN 即時通訊傳輸檔案時，使用者 A 會發送 MSG 命令 (INVITE) 夾帶 EUF-GUID 訊息 (5D3E02AB-6190-11D3-BBBB-00C04F795683) 邀請使用者 B 進行檔案傳輸服務，使用者 B 會回傳 ACK 命令表示確定，此時使用者 A 會發送 MSG 命令要求建立 P2P 連線，當使用者 B 收到時則會回傳 ACK 並發送 MSG 確定來源與目的之使用者帳號，當使用者 A 收到時會回傳 ACK 與 MSG 命令夾帶來源與目的之使用者帳號，當使用者 B 收到時會發送 MSG 命令夾帶 IP 位址與埠號，使用者 A 收到命令後會回傳 MSG 命令夾帶 IP 位址與埠號，此時觀察 TCP 可發現使用者 A 用來傳輸檔案之埠號為 49754，而使用者 B 用來接收檔案之埠號為 3303，當埠號設定完成後，MSN 即時通訊將會透過 HTTP 傳輸檔案。

當本系統欲擷取使用者之檔案傳輸資訊時，系統可擷取 MSG 命令中之 EUF-GUID 之資訊，如其內容為 {5D3E02AB-6190-11D3-BBBB-00C04F795683} 時，即代

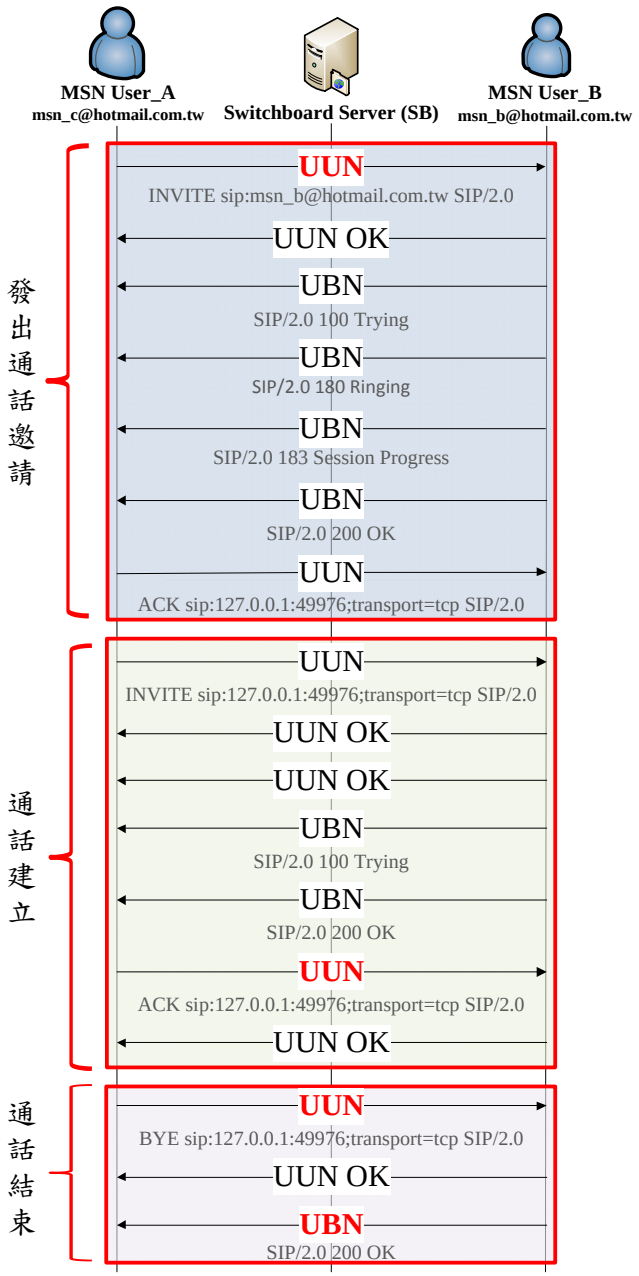


圖九： MSN 即時通訊檔案傳輸序列圖

表使用者提出檔案傳輸之邀請，此時系統可從後方使用者 B 發送之 MSG 命令中擷取出使用者 B 將要接收之埠號，在使用者 A 所傳輸之 MSG 命令中可擷取到發送之埠號，在後方之 TCP 命令中可擷取發現使用者用來傳輸之正確埠號。由於 MSN 即時通訊每次傳輸之埠號並不相同，故本系統需擷取所有可能傳輸之埠號並監聽，當收到 TCP 封包確定欲使用之埠號時，本系統便可針對此兩個埠號所傳輸之 HTTP 封包擷取，並將不需要之封包捨棄，將所擷取之封包傳送至 Media Processing Server 分析並還原成原本傳輸之檔案儲存於資料庫中。

4.5 MSN 視訊影音會談

MSN 即時通訊之視訊影音會談序列圖如圖十，當使用者 A 欲使用視訊會談服務時，使用者 A 會發出 UUN 命令 (INVITE sip:msn_b@hotmail.com.tw SIP/2.0) 邀請使用者 B，使用者 B 收到時會回傳 UUN OK 命令並發送 UBN 命令 (SIP/2.0 100 Trying) 代表嘗試撥號，在撥號時會發送 UBN 命令 (SIP/2.0 180 Ringing) 代表正在響鈴，之後使用者 B 會發送 UBN 命令 (SIP/2.0 183 Session Progress) 確定目前之會談狀況，當使用者 B



圖十： MSN 即時通訊視訊影音會談序列圖

發送 UBN 命令其中包含 SIP 200 OK 時則代表會談建立，此時使用者 A 會發送 UUN 命令夾帶 ACK 命令代表確認，此時通話邀請即完成。

當邀請完成後，使用者 A 會發出 UUN 命令 (INVITE) 邀請使用者 B 建立通話，當使用者 B 收到邀請時會回傳 UUN OK 命令並發送 UBN 命令 (SIP/2.0 100 Trying)代表嘗試連線中，當使用者 B 發送 UBN 命令內容為 SIP 200 OK 時即代表通話建立，此時使用者 A 會發送 UUN 命令 (ACK) 確定，此時通話即開始。

當使用者 A 欲結束視訊會談時，使用者 A 會發送 UUN 命令 (BYE sip:127.0.0.1:49976;transport=tcp SIP/2.0) 代表結束通話，使用者 B 收到後會回傳 UUN OK 命令與 UBN 命令 (SIP/2.0 200 OK)，此時即代表通話結束。

當本系統欲擷取視訊影音會談服務內容時，系統可由使用者 A 所發送之 UUN 命令中，內容為 INVITE 之訊息擷取出欲邀請通話對象之 ID (使用者 B)，當系統監聽到使用者 B 發送 UUN 命令內容包含 ACK 時，即代表會談將開始，此時系統便可開始擷取視訊影音會談之封包，系統可將擷取之封包傳輸至後端 Media Processing Server 分析還原出視訊影音會談之內容並儲存於資料庫中。

五、 結論

本論文以 Gigabit 被動光纖網路為底層架構，設計一多媒體串流數位鑑識系統，透過擷取 MSN 會談傳輸資訊，分析並儲存於資料庫中。透過使用者資訊對應儲存於資料庫中之影音與傳輸之檔案資訊，以 Web 網頁介面呈現出數位鑑識時所需之相關資訊。

本論文系統之設計以不影響封包傳輸品質為前提，利用本論文設計之多媒體串流數位鑑識系統，以本論文設計之 Snooping Agent 擷取 MSN 即時通訊之會談傳輸封包，利用 UDP/IP Tunnel 封裝技術將封包封裝成 UDP 封包傳輸至後端多媒體串流數位鑑識系統，透過本論文設計之 Analyzer Server 將封包解封後分析出 MSN 控制訊息與文字訊息並儲存於資料庫中；透過本論文設計之 Media Processing Server 將封包解封後分析出 MSN 會談服務之視訊資料、音訊資料與檔案傳輸資料，並還原儲存於資料庫中。當需要數位鑑識時，網路管理者可透過本系統之數位鑑識管理系統找出使用者 MSN 即時通訊之個人資訊與會談封包資料。

鑑識系統所呈現之資訊，可使用於預測攻擊或設計網路安全機制時之參考數據，未來更可結合 SIP 網路電話，應用於更廣泛之多媒體串流應用，並優化其效能，使系統可應用於更多元之多媒體串流應用。

參考文獻

[1] G. Kramer, G. Pesavento, “Ethernet Passive Optical Network (EPON): Building a Next-Generation Optical Access Network,” in IEEE Communication Magazine, pp.66-73, February 2002.

[2] Gigabit-capable passive opticalnetworks (GPON): General Characteristics, Recommendation ITU-T G.984.1, 2008.

[3] MSN Messenger Protocol, http://www.hypothetic.org/docs/msn/.

[4] MSN Messenger Protocol, http://msnpiki.msnfanatic.com/index.php/MSNC:MSNSLP.

[5] Wikipedia – MSN, http://zh.wikipedia.org/wiki/MSN

[6] Wikipedia – Windows Live Messenger , http://zh.wikipedia.org/wiki/Windows_Live_Messenger

[7] 資策會網路多媒體研究所, "產業資訊交流串流影音波放棄最新發展趨勢," 電腦視覺監控產學研聯盟電子報, 第三期, 2005 年 5 月. http://140.113.87.114/cvrc/edm/vol_3/inf2.htm

[8] 黃嘉宏, 詹前隆, 王旭正, "電腦鑑識工具應用於犯罪偵查之研究," 中央警察大學通識教育中心研討會, May 2008.

[9] 胡勝雄, “於 Gigabit 被動光纖網路下 MSN/SIP 會談鑑識系統之設計與實作,” 國立虎尾科技大學電機工程研究所碩士論文, 2011 年七月.