**實驗日期：**

May 4, 2023

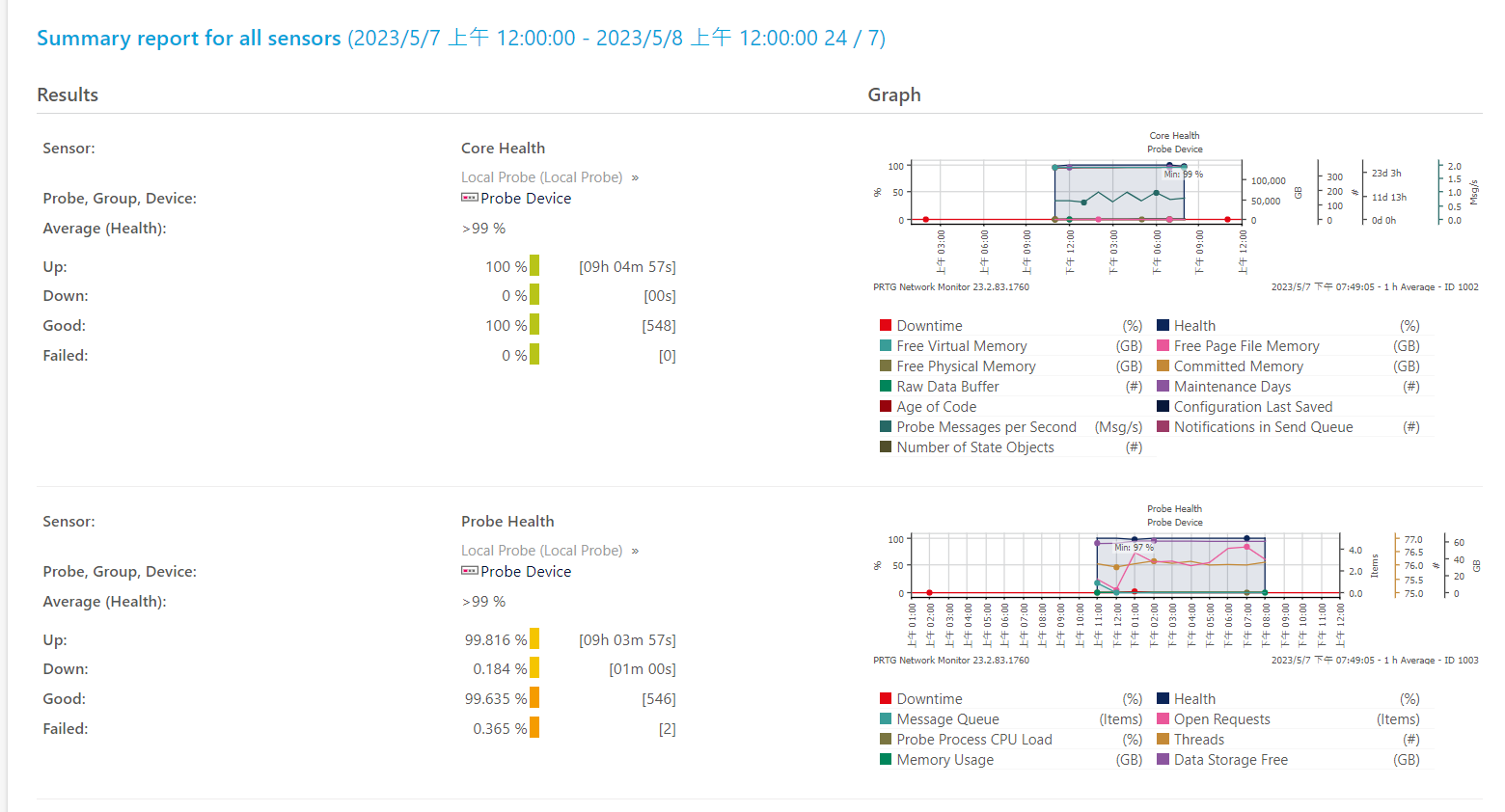
**實驗名稱：**

1. System Analysis: PRTG Traffic Grapher
2. System Analysis: Weblog Expert
3. System Analysis: Ethereal

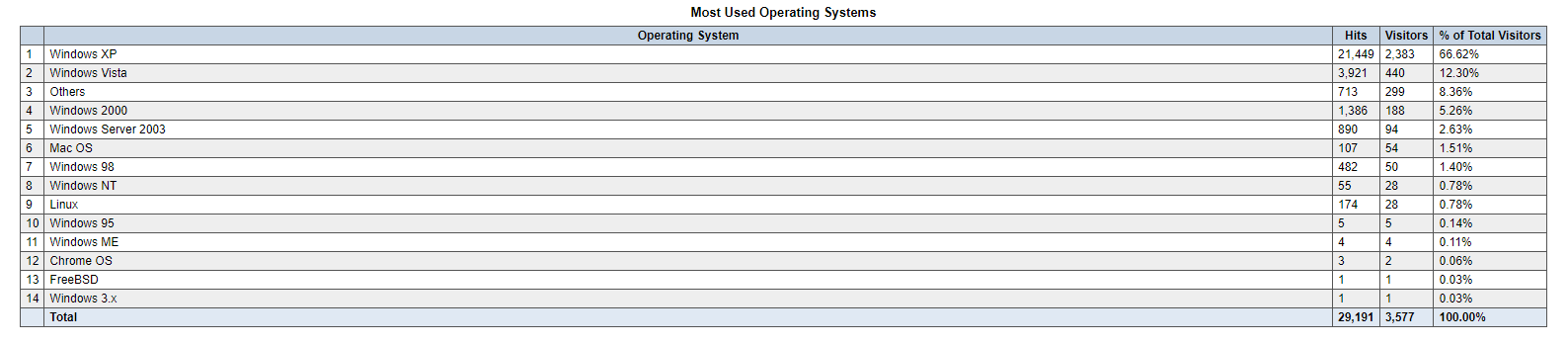
**問題與答案：**

1. 12-1: PRTG Traffic Grapher至少輸出三種以上的圖表，然後說明各個同表的意義。  
   一張含有 圖表 的圖片

   自動產生的描述  
   上圖顯示我的電腦WiFi接收、傳送封包數量變化，由於在偵測期間接上網路線，因此WiFi接收封包數急遽下降的趨勢，後來又將網路線拔掉，所以可以看到圖的後半段曲線出現起伏。  
   一張含有 文字, 光線 的圖片

   自動產生的描述  
   上表顯示我的電腦每分鐘收到和傳出的資料大小、封包數和此裝置運行程度。  
     
   Summary report for all sensors會顯示所有正在運行的sensor的圖表和運行率。
2. 12-2: Weblog Expert至少輸出三種以上的圖表，然後說明各個同表的意義。  
   一張含有 圖表, 資料表 的圖片

   自動產生的描述  
   上圖列出最常使用的瀏覽器，以表格詳細列出各個瀏覽器的點擊數和使用者人數，並以圓餅圖輔助顯示。上圖可知IE為最受歡迎的瀏覽器，其中7.x版本最常被使用，有13003點擊率，1204造訪者，占所有造訪者的32.55%。  
   一張含有 文字 的圖片

   自動產生的描述  
   Summary以表格的形式統合不管任何瀏覽器的點擊數、頁面觀看數、造訪者還有頻寬等資訊。  
     
   上表顯示造訪者使用的作業系統排名，大部分造訪者使用的作業系統為Windows，其中從Windows XP造訪網頁者佔最多數，有21449個點擊，2383為造訪者使用Windows XP，占全部使用者的66.62%。
3. 12-3: Ethereal根據驗收的畫面，說明各封包內容的意義。

|  |
| --- |
|  |
|  |

粉色底為送出的封包資訊，黑色底為收到的封包資訊。上圖紅框中送出的封包將TTL設為1，目的地為140.112.30.26，而收到的封包傳送端為163.25.101.254，接收端為本地IP 192.168.68.186，對應到命令提示字元介面的第一個路由正好是回傳封包的傳送端163.25.101.254；橘框將TTL設為2，收到由192.168.101.49回傳的封包，是第二個路由，以此類推。直到第13個路由時不再收到(Time to live exceed in transmit)的訊息表示尋找路線結束。  
  
由上述觀察可知，tracert是利用ICMP protocol傳輸，並且送出的封包目的地為140.112.30.26，因此在filter中下icmp &&ip.dst==140.112.30.26可以過路出所有用於tracert的封包。

**討論：**

這次實驗12-1安裝的應用很有趣，他可以監測電腦上各種不同的裝置，就連C槽、D槽和虛擬機的狀態都會顯示出來，還有一些防毒軟體回報給我的警告訊息也寫得一清二楚，在使用這個app唯一遭遇到的困難就是密碼設置了…我剛設置完就登入不了，只好卸載重來導致中間有資料斷層，好險在卸載時它不會自動把之前收集的資料也刪除，必須手動刪除，因此還保留了一些監測的資料。

**補充資料：  
無**