

# SuperFoxy

## Pwning The Chinese P2P Network 潛入知名華人P2P網路

Tsung Pei Kan  
peikan@gmail.com

# About Tsung Pei Kan


- Graduated from Central Police University . He likes to study about Kernel and Reverse Engineering. He is interested in the subject of Computer Forensic. He's working for National Police Agency now. Besides, he is also the docent for Taiwan Network Information Center.
- At the beginning of last year he developed a scanner based on behavioral analysis call "NPASCAN", it can detect and exam the unknown malware very quickly. The most important thing is you can free download from the NPA website.
- **Special skills:**
  - Windows System Programming
  - Malicious Software Analysis
  - Software Reversing
  - Computer Forensics
- **Experience**
  - National Police Agency (NPA)
    - Information Department
  - Criminal Investigation Bureau (CIB)
    - High-Tech Crime Investigation Center
    - Information Department



# About Foxy P2P

- Foxy is a Chinese P2P software which is popular in Taiwan, China, Hong Kong and Macau.
- It is based on the Gnutella and G2 architecture.

## 漢光演習軍機 4度外洩 FOXY網站可搜尋 資訊戰「敗到底」

2007年 04月30日  讚

【王焯華／台北報導】國軍即將在五月展開「漢光二十三號演習」，證機密資料再度外洩，在知名FOXY網站中即可搜尋到，由於該資料「機密（本件屬國家機密亦屬軍事機密，保密至民國一〇五年十一月除密）」等字樣，讓國軍保密問題再度受各界質疑。

### 漢光23號演習7大演習區實兵驗證

資料來源：國防部




Data leaked into Foxy P2P network(TW)

## FOXY搜個資 盜刷信用卡32萬 下載卡號授權碼 買3C品轉賣換現金

2011年 04月10日  讚 210

【蔡進男、劉文淵／綜合報導】FOXY用戶請小心個資外洩，利用FOXY分享軟體，搜尋並盜取被害人存放電腦中的信用卡號、授權碼等資料，再將3C產品低價網拍換現金，警方獲報後，前天前往男子約談，處理伏逮人，發現他不法獲利全購買毒品揮霍殆盡，訊後將他依詐欺罪嫌送辦。

### 維安計劃 FOXY看得到

2008年 05月15日  讚

#### 機密外洩

準總統馬英九五二〇就職，並南下高雄舉辦國宴，國民黨料，扁呂今年及去年兩次高雄行程的道路維安計劃外洩，洞，籲檢修馬在高雄維安計劃，勿讓馬陷遇刺危機。

## 近百人信用卡號、個資又遭Foxy外洩

作者：張維君整理 -05/10/2010

P2P分享軟體Foxy又惹禍。前幾年因為有個人報稅、警方筆錄等資料在Foxy上被因而引起大家注意。日前又有不肖歹徒利用Foxy搜尋到信用卡號、檢核碼及個資冒受害者身分網購盜刷信用卡，警方與多家受害銀行合作後，日前終於將嫌犯逮捕歸案，並依詐欺、妨害電腦使用罪嫌送辦。

## 網路下載軍機 外患罪起訴

〔記者鮑建信、顏宏駿、羅添斌／綜合報導〕國軍軍載？別懷疑，這種離譜的事真的發生在台灣，而軍方也多次了！

### Foxy分享赫見作戰計畫

彰化縣民林建宏一時好奇，自Foxy分享平事檔案，被高雄高分檢依外患罪起訴，檢方犯行，求處徒刑八月，並建議法院宣告緩刑中流出？迄今仍難查明，遑論追究洩

本案當事人、卅歲的林建宏，個性保守，化縣員林鎮住處沉迷網際網路，並在其使用體，以利上網搜尋其他共享資料。

今年三月，林建宏一連三、四天上網搜尋，碰巧有人電腦分享資料夾內，經林建宏多次網搜結果，傳入林的下載蒐集共廿件，其中有部分是尚未解禁的軍事機密，的情報、作戰、防禦等計畫。

## 馬專機駕駛個資 FOXY全都露

2008年 12月01日  讚

### 維安漏洞

國軍剛完成「資通安全講習」，卻發生國軍中堅幹站上的洩密案，包括國防大學政戰學院學生名冊、資料。其中空軍官校名冊中還包括各飛行單位的職軍各作戰飛行聯隊少校飛行官及負責總統專機的專在網路上「全都露」。

## 高雄縣調站搞烏龍 線民資料Foxy外洩

〔記者林慶川、黃敦硯／台北報導〕調查局高雄縣調查站一名組長，涉嫌違反通訊安全規定，將佈建的線民資料存在隨身碟中，不慎遭Foxy網路軟體開放分享後遭人下載；這是調查局成立至今首宗資料外洩事件。

Data leaked into Foxy P2P network(TW)

身碟，確有資料外流，但外傳13位線民那麼多，且外洩的只是一般性對象，未造成重大危害，考量當事人並非故意，調查局最後將這名組長記兩次申誡。



高縣調查站發生線民資料外洩事件。（記者王榮祥攝）



因前男友電腦安裝分享軟體，女子的裸照意外外洩，上網仍可看見。

頭條要聞 > FOXY軟體抓舊愛裸照 男不起訴

 點閱(569)  轉寄(0)  引用(0) 字級:  

## FOXY軟體抓舊愛裸照 男不起訴

2008年 06月07日  讚

【呂志明／台北報導】就讀某私立大學的廖姓學生，拍在電腦裡，兩人分手後女方無意間利用FOXY軟體竟然的裸照，認為是對方故意散布，憤而提出告訴，檢察官該是出在FOXY分享軟體上，將廖男不起訴。

# Data leaked into Foxy network (HK)

- ↑ 台灣蘋果日報即時新聞：侵權爭議 FOXY宣布關站 [↗](#)，2011年10月23日。
- ↑ 高登討論區：侵權爭議 FOXY宣佈關站 [↗](#)，2011年10月23日。
- ↑ 3.0 3.1 Foxy檔案下載桌面全腦任睇 特別版恐藏間諜程式 專家籲勿用 [↗](#)，明報，2008年5月29日。
- ↑ Sandbox [↗](#)
- ↑ 明報：FOXY軟件泄政府機密 警內部手冊 高官出生日期 一覽無遺 [↗](#)
- ↑ 明報：警方機密檔案疑外泄(2008年5月26日) [↗](#)
- ↑ 星島日報：警隊臥底身分「任人睇」 [↗](#)2008年5月27日。
- ↑ 星島日報：入境處機密文件外泄 網上任睇 [↗](#)，2008年5月8日
- ↑ 明報：入境處監視名單外泄 員工違規帶機密文件回家 誤經Foxy上載 [↗](#)，2008年5月8日
- ↑ 蘋果日報：揭秘網民擔心被找麻煩 [↗](#)，2008年5月27日。
- ↑ 星島日報：輪姦片上網 警拘三人 [↗](#)，2008年9月11日
- ↑ 東方日報：Foxy天王踢爆警隊再洩內部文件 [↗](#)，2008年9月30日
- ↑ 星島日報：消防處調查內部資料外洩事件 [↗](#)，2009年2月8日。
- ↑ 星島日報：李少光關注消防員個人資料外洩事件 [↗](#)，2009年2月8日。
- ↑ 星島日報：球員薪酬外泄 南華震驚或報警 [↗](#)，2009年2月15日。
- ↑ 明報：警隊資料再經FOXY外泄 [↗](#)，2009年3月7日。
- ↑ 明報：廉署沒安裝FOXY 指信件外泄報道不確 [↗](#)，2009年4月7日。
- ↑ 星島日報：銀行疑網上泄密 廉署案件曝光 [↗](#)，2009年4月7日。
- ↑ 星島日報：警隊密件又經Foxy外泄 [↗](#)，2009年12月3日。
- ↑ 蘋果日報：Foxy又洩重案組臥底資料 撰寫文件探員 曾獲一哥嘉獎 [↗](#)，2011年4月29日。
- ↑ 蘋果日報：警戰術機密外洩 內地網站流出 圖文並茂講述 [↗](#)，2011年7月19日。
- ↑ 蘋果日報：資料又外洩 警隊武力清場教材曝光 經 FOXY流出 投考者私隱任人睇 [↗](#)，2011年8月9日。
- ↑ 明報：黎智英是泛民大水喉 [↗](#)，2011年10月18日。
- ↑ 星島日報：黎智英是泛民大水喉 [↗](#)，2011年10月23日。
- ↑ 自由時報(台灣)：FOXY涉侵權逾58億 負責人被訴 [↗](#)，2009年4月16日。
- ↑ 蘋果日報：免費下載歌曲電影 涉侵權金額58億 FOXY被台灣起訴 [↗](#)，2009年4月17日。

# Foxy P2P UI

The screenshot displays the Foxy P2P client interface. At the top, there are three steps: 1. 在此欄輸入你要找的歌曲或歌手 (Enter the song or artist you want to find in this field), 2. 選音訊 (Select audio), and 3. 按搜尋 (Click search). The search field contains '蔡小虎' and the audio format is set to '音訊' (Audio). A search button labeled '搜尋' is visible.

Below the search bar, there are tabs for '江蕙' and '蔡小虎'. A red arrow points to the '蔡小虎' tab with the text '將你找的歌首列出' (List the songs you found). Below the tabs, there is a search bar with the text '搜尋 [音訊] : 找到 67 個檔案' (Search [Audio] : Found 67 files). A red arrow points to this search bar with the text '4. 將你要的歌曲用滑鼠按左邊兩下就會跑到下載區去了' (Click the song you want with the mouse twice on the left side, and it will go to the download area).

The main area shows a table of search results with columns: 檔案名稱 (File Name), 大小 (Size), 類型 (Type), 速度 (Speed), 來源 (Source), and 狀態 (Status). The table lists various MP3 files by artists like 蔡小虎, 龍千玉, and 蝴蝶夢.

檔案名稱	大小	類型	速度	來源	狀態
蔡小虎-蝴蝶夢-01. 蝴蝶夢vs龍千玉.MP3	6,043 KB	MP3 音訊檔 (mp3)	184 KB/S	7 個來源	
龍千玉+蔡小虎真心只愛你...-真心只愛你-世間路.mp3	3,952 KB	MP3 音訊檔 (mp3)	130 KB/S	6 個來源	
蔡小虎-思相枝-04-意難忘.MP3	3,664 KB	MP3 音訊檔 (mp3)	127 KB/S	5 個來源	
蔡小虎-一生只有你.mp3	4,357 KB	MP3 音訊檔 (mp3)	138 KB/S	5 個來源	
蔡小虎&龍千玉-世間路.mp3	4,138 KB	MP3 音訊檔 (mp3)	199 KB/S	4 個來源	
林珊+蔡小虎-我的選擇猶原是你.mp3	5,306 KB	MP3 音訊檔 (mp3)	180 KB/S	4 個來源	
台語-台語情歌對唱-江蕙-蔡小虎-心痛的戀情-(天地有情-片尾曲)...	3,857 KB	MP3 音訊檔 (mp3)	125 KB/S	4 個來源	
龍千玉-酒後吐真言(蔡小虎).mp3	3,873 KB	MP3 音訊檔 (mp3)	168 KB/S	3 個來源	
龍千玉-阿郎-02. 紅紅的酒-蔡小虎.mp3	6,317 KB	MP3 音訊檔 (mp3)	167 KB/S	3 個來源	
龍千玉&蔡小虎-相逢的酒.mp3	4,414 KB	MP3 音訊檔 (mp3)	205 KB/S	3 個來源	
蝴蝶夢-12. 尚愛也是你-蔡小虎+陳美鳳.mp3	6,054 KB	MP3 音訊檔 (mp3)	220 KB/S	3 個來源	
蝴蝶夢-10. 日出日落-蔡小虎+龍千玉.mp3	6,538 KB	MP3 音訊檔 (mp3)	193 KB/S	3 個來源	
蝴蝶夢-06. 月光河-蔡小虎+龍千玉_1.mp3	6,320 KB	MP3 音訊檔 (mp3)	75 KB/S	3 個來源	
蔡小虎-蝴蝶夢-08-愛你用生命(&黃思婷).mp3	6,633 KB	MP3 音訊檔 (mp3)	326 KB/S	3 個來源	
蔡小虎-陳雷-王識賢-黃乙玲-愛恨罷是你.mp3	3,375 KB	MP3 音訊檔 (mp3)	318 KB/S	3 個來源	
曾心梅&蔡小虎-一生甘願為你錯.MP3	3,739 KB	MP3 音訊檔 (mp3)	170 KB/S	3 個來源	
台語老歌-林珊&蔡小虎-我的選擇猶原是你.MP3	4,243 KB	MP3 音訊檔 (mp3)	187 KB/S	3 個來源	
台語老歌-蔡小虎-愛人醉落去.mp3	3,904 KB	MP3 音訊檔 (mp3)	25 KB/S	3 個來源	
5. 真愛無後悔-陳美鳳+蔡小虎-(真愛無悔)01_1.mp3	5,950 KB	MP3 音訊檔 (mp3)	140 KB/S	3 個來源	
蝴蝶夢-07. 難分難離-蔡小虎+龍千玉.mp3	5,127 KB	MP3 音訊檔 (mp3)	242 KB/S	2 個來源	
蝴蝶夢-03. 对你的這段情--蔡小虎+龍千玉.mp3	6,472 KB	MP3 音訊檔 (mp3)	22 KB/S	2 個來源	
蔡小虎_心所愛的人.mp3	3,977 KB	MP3 音訊檔 (mp3)	376 KB/S	2 個來源	
蔡小虎-蝴蝶夢-11-情牽七千年(黃思婷).mp3	5,738 KB	MP3 音訊檔 (mp3)	19 KB/S	2 個來源	
蔡小虎-蝴蝶夢-09-無奈闕無奈(&龍千玉).mp3	5,931 KB	MP3 音訊檔 (mp3)	242 KB/S	2 個來源	
蔡小虎-蝴蝶夢-05-真愛無後悔(&陳美鳳).mp3	5,950 KB	MP3 音訊檔 (mp3)	317 KB/S	2 個來源	
蔡小虎-蝴蝶夢-04-再會啦!再會(&黃思婷).mp3	5,371 KB	MP3 音訊檔 (mp3)	242 KB/S	2 個來源	
蔡小虎-蝴蝶夢-02-醉到底(&王瑞霞).mp3	5,585 KB	MP3 音訊檔 (mp3)	82 KB/S	2 個來源	
蔡小虎-牽手做陣行(龍千玉 & 蔡小虎).mp3	5,553 KB	MP3 音訊檔 (mp3)	242 KB/S	2 個來源	
蔡小虎-春夏秋冬.mp3	3,776 KB	MP3 音訊檔 (mp3)	80 KB/S	2 個來源	
蔡小虎-思相枝-02-故鄉的地圖.mp3	4,020 KB	MP3 音訊檔 (mp3)	82 KB/S	2 個來源	
蔡小虎-01-愛你無罪.mp3	3,295 KB	MP3 音訊檔 (mp3)	376 KB/S	2 個來源	
蔡小虎-01-一段情一場夢.mp3	3,977 KB	MP3 音訊檔 (mp3)	230 KB/S	2 個來源	
蔡小虎-思相枝-11-浪子情深.mp3	5,220 KB	MP3 音訊檔 (mp3)	48 KB/S	1 個來源	

# Honey P2P UI





# Getchaman



DOWNLOAD



Getchaman是一套完全免费的下载软件，不限下载数量与速度，能够在网络上快速搜寻及下载各种格式的文件。配合内置高速搜索引擎，更可快速搜索各种网络资源，而且支持所有格式的档案传输，是不可或缺的平台。



- ✔ 完美支持电驴、BT等协议
- ✔ 不限速下载，资源占用极小
- ✔ 内置优化磁盘缓存引擎减轻硬盘负担
- ✔ 支持多种文字编码关键字高效率搜索
- ✔ 特别优化界面使用简单快捷

# Foxy = HoneyP2P = Getchaman

- Although they have different UI, these clients join to the same P2P network.
- Do not think that you did not install foxy, so your data will be safe.



adsl

全部

搜尋

adsl

下載

搜尋 [全部] : 找到 472 個檔案

檔案名稱	大小	類型
administrator@adsl.hinet[2].txt	387 Bytes	文字文件
ADSL 帳號密碼.txt	39 Bytes	文字文件
ADSL 帳號密碼.txt	18 Bytes	文字文件
ADSL.txt	38 Bytes	文字文件
ADSL.txt	Bytes	文字文件
ADSL.txt	Bytes	文字文件
ADSL.txt	Bytes	文字文件
adsl.txt	Bytes	文字文件
ADSL.txt	Bytes	文字文件
adsl.txt	Bytes	文字文件

**Adsl dial  
Id/Password**



主頁



搜索



下載

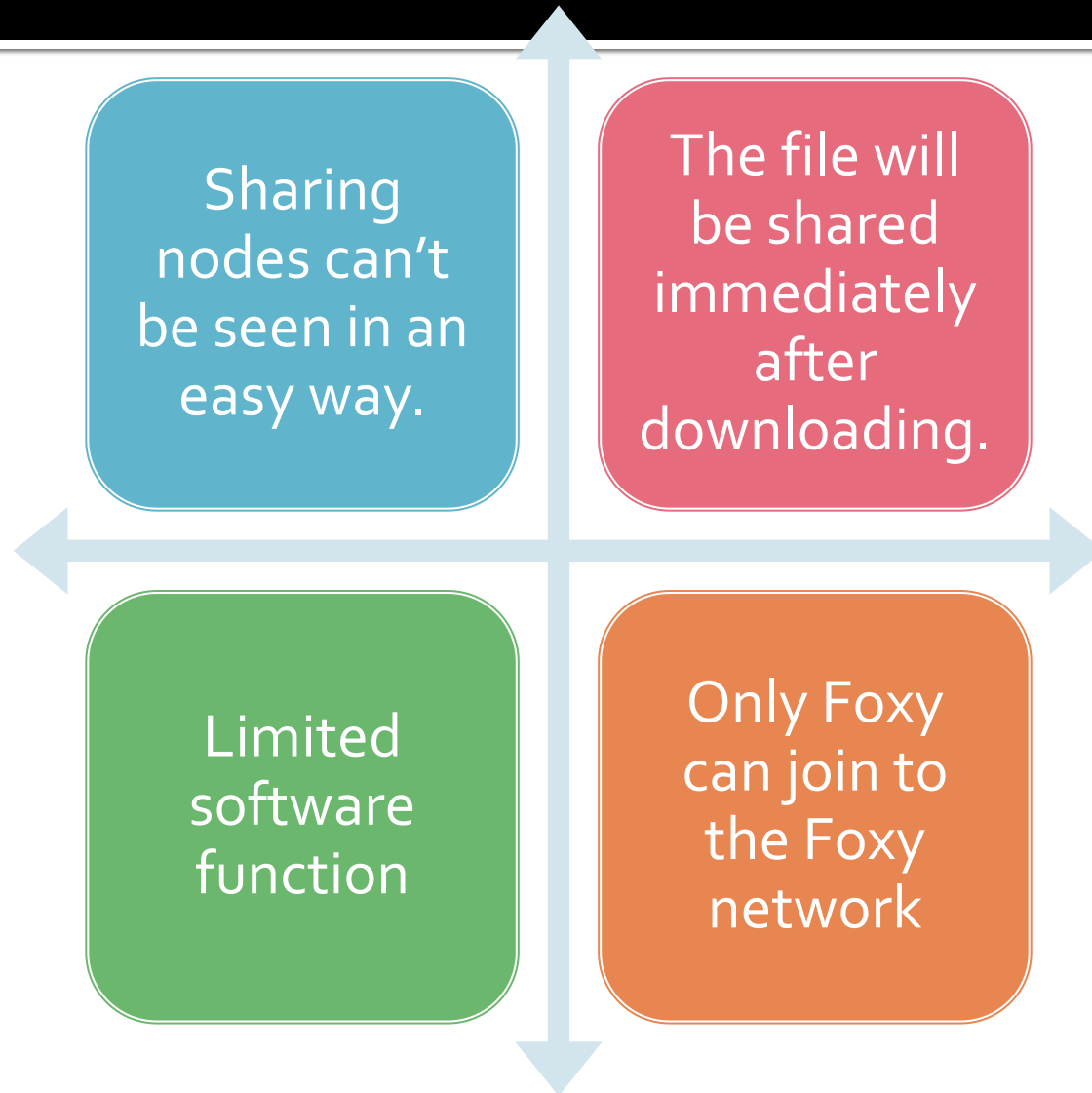


共享



音樂下載

# The challenge of audit Foxy network



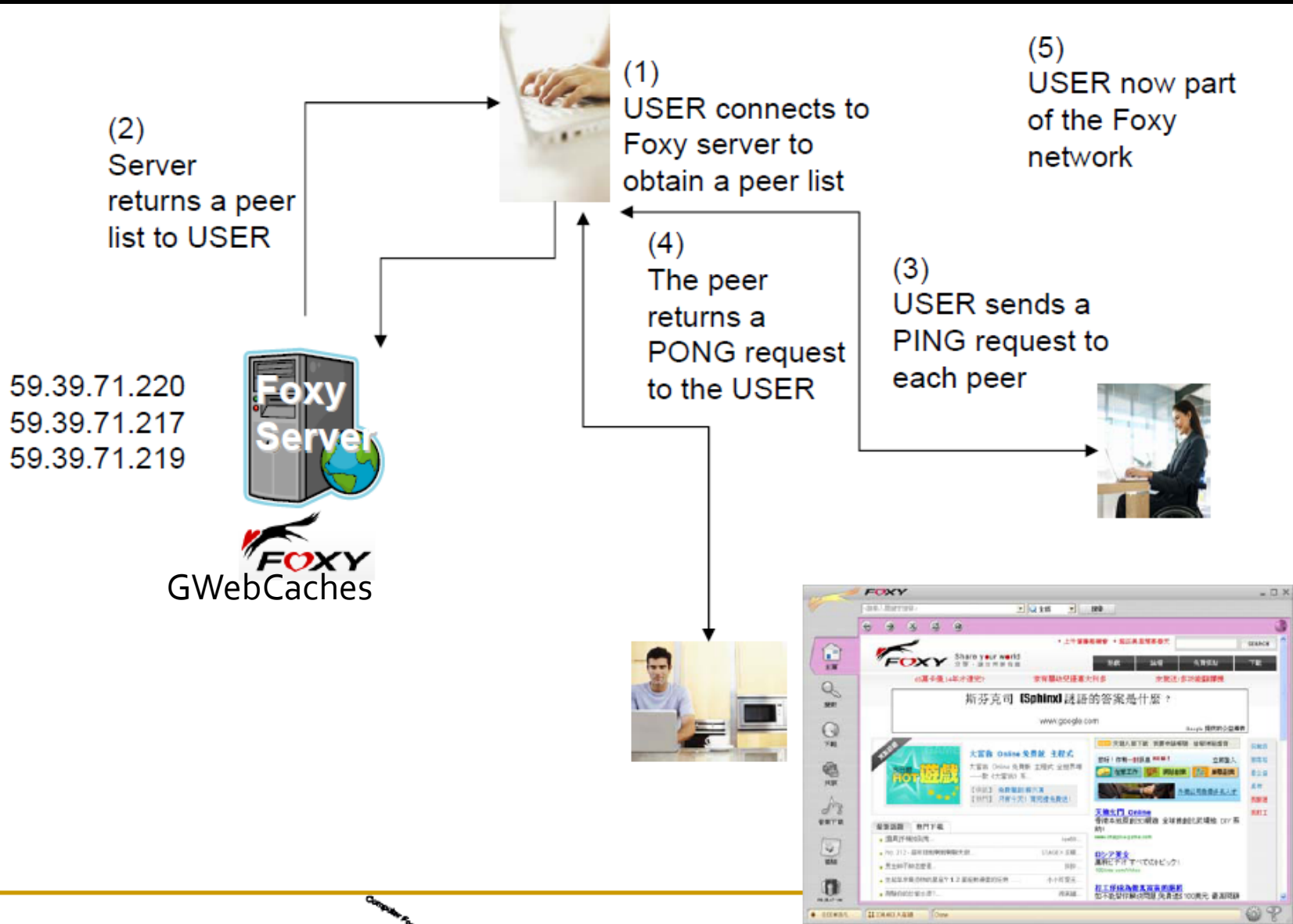
# Foxy P2P network architecture

Connect to Foxy

Search from Foxy

Download from foxy

# How does foxy connect to P2P network



# GWebCache Server (bootstrap)

← → ↻ 🏠 216.18.206.17:2108/gwc/cgi-bin/fc?get=1&net=foxy&cl

🌐 新分頁 🌐 about:blank 📁 Andriod 📁 Security 📁 Forensics 📁 CodeReview 📁

```
H|125.225.136.15:22051|21
H|203.73.34.190:11239|13
H|114.47.250.77:19413|3
H|218.162.102.214:4230|22
H|122.100.72.210:24228|28
H|1.175.1.68:10817|26
H|111.184.172.217:5024|15
H|122.118.188.150:9447|7
H|122.100.248.217:6012|23
H|114.39.12.75:4287|26
H|124.155.190.48:9849|10
H|123.0.239.99:3375|7
H|114.47.170.51:12428|16
H|218.170.102.174:19292|25
H|119.247.98.114:21819|29
H|183.179.113.86:24509|11
H|61.225.23.37:9431|26
H|58.152.26.193:13765|26
H|114.27.209.16:3506|26
H|111.242.40.64:18803|30
```



# Foxy handshak (SYN)

- GNUTELLA CONNECT/o.6
- Listen-IP: 61.57.116.229:24499
- Remote-IP: 203.185.52.200
- User-Agent: Foxy 1.8.6.0
- Accept: application/x-gnutella2
- X-Ultrapeer: False
- Accept-Encoding: deflate
- X-Auth-Challenge: KxElu1Q

# Foxy handshak (SYN+ACK)

- GNUTELLA/0.6 200 OK
- Listen-IP: 203.185.52.200:7952
- Remote-IP: 61.57.116.229
- User-Agent: Foxy 1.9.10.0
- Content-Type: application/x-gnutella2
- Accept: application/x-gnutella2
- X-Ultrapeer: True
- Accept-Encoding: deflate
- X-Auth-Response: RhXb6zC5Yss
- X-Auth-Challenge: 3H5HtDHD
- X-Try-Hubs: 219.78.62.158:10686 2010-10-03T15:37Z,111.249.145.101:18218

# Foxy handshaking (ACK)

- GNUTELLA/o.6 200 OK
- X-Ultrapeer: False
- Content-Type: application/x-gnutella2
- Content-Encoding: deflate
- X-Auth-Response: PLHJxl7zcKU

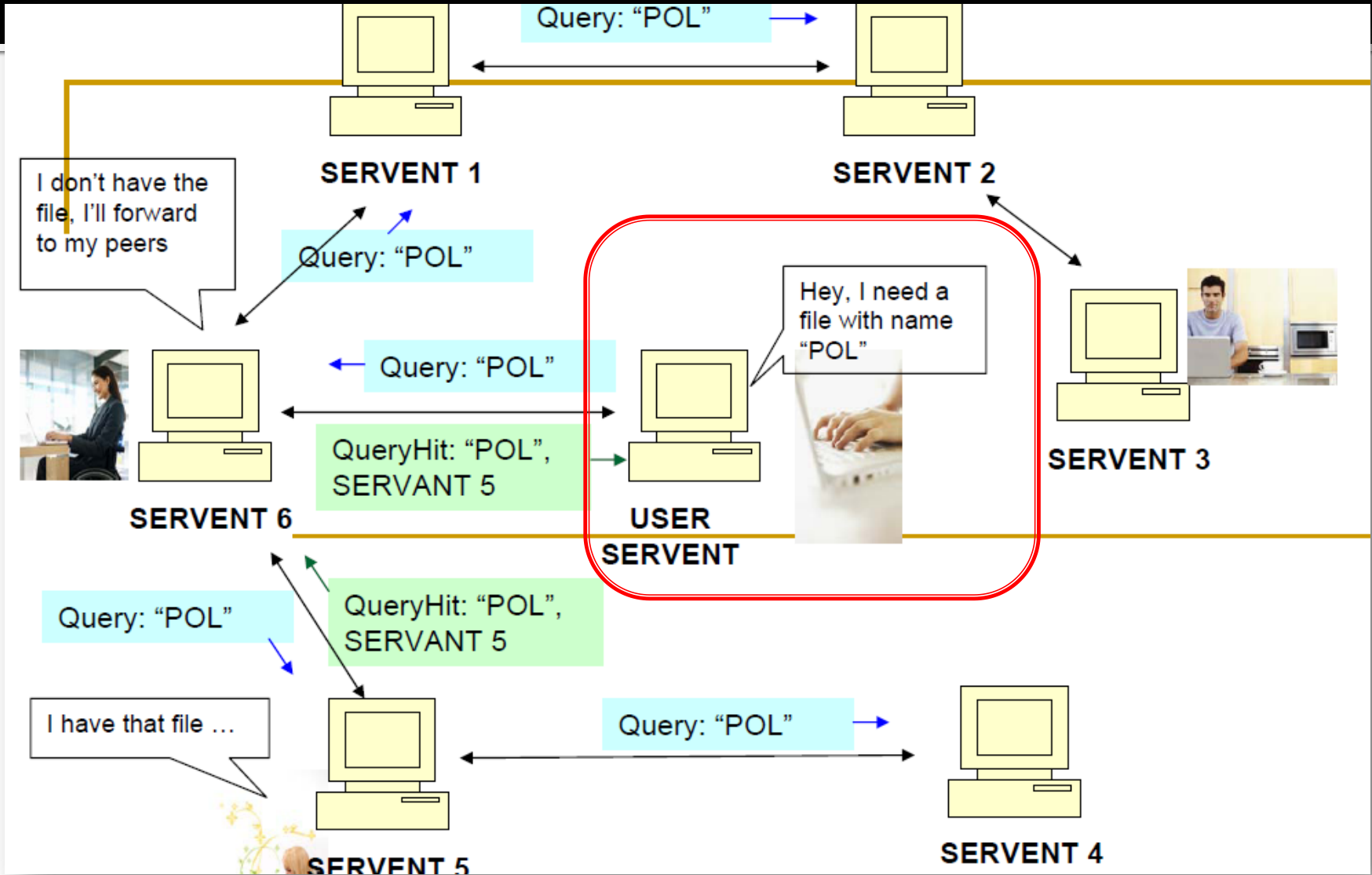
*Using custom Tiny Encryption Algorithm (TEA) and Base64 algorithm.*

Foxy is a closed Gnutella P2P network

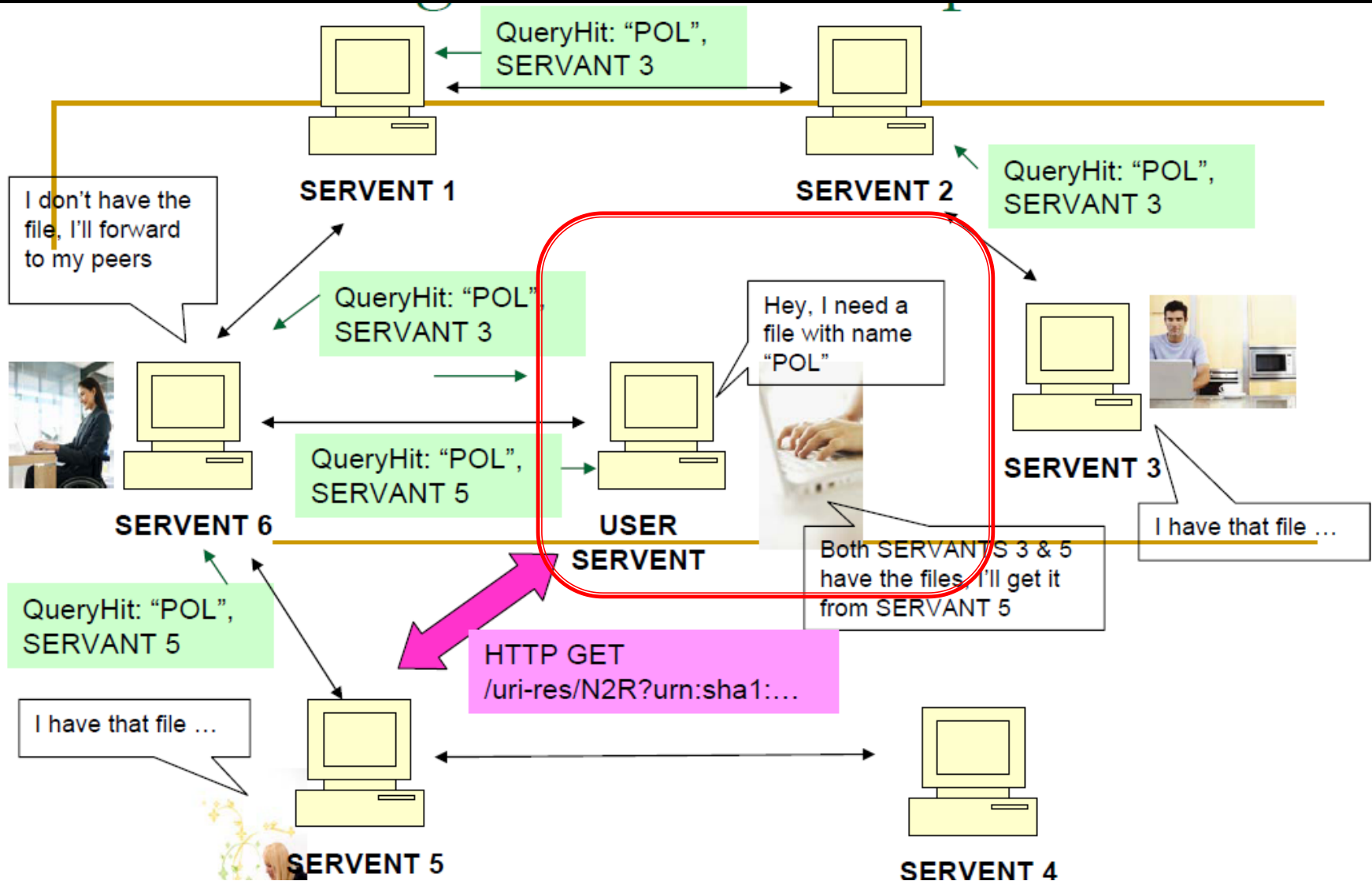
# Use a different key to handshaking

```
de_foxy.cpp x
0 10 20 30 40 50 60 70 80 90 100
222 if ( a2 <= 8 )
223     a2 = 8;
224 v4 = (int)malloc(2 * a2 + 1);
225 if ( v3 < 8 )
226 {
227     *(DWORD *)v4 = 0;
228     *(DWORD *) (v4 + 4) = 0;
229 }
230 memcpy((char *)v4, a1, 4 * (v3 >> 2));
231 v6 = a2;
232 memcpy((char *) (v4 + 4 * (v3 >> 2)), (char *)a1 + 4 * (v3 >> 2), v3 & 3);
233 // sub_49F4EA((const char *)v4, v6, (char *)v4);
234 char key [] = {0x5F,0x85,0x5E,0xBF,0xC9,0x18,0xB9,0x2C,0xE7,0x04,0xE0,0x4E,0xF4,0xD9,0xFF,0x35};
235 // char key[] = {0xEA,0x9F,0x6C,0x7F,0xF9,0xF5,0x99,0x94,0xDF,0x04,0xB5,0x6C,0x89,0x7A,0x30,0x2F};
236 sub_49F4EA((const char *)v4, v6, (char *)v4, (int)&key);
237
238 v7 = a3;
239 // sub_49F4EA(v7, v4, a2);
240 string cc = sub_49F4EA(v7, v4, a2);
241
242 free((char *)v4);
243 // cout <<cc.c_str()<<endl;
244 string s;
245 int n = cc.find_last_of('=');
246
```

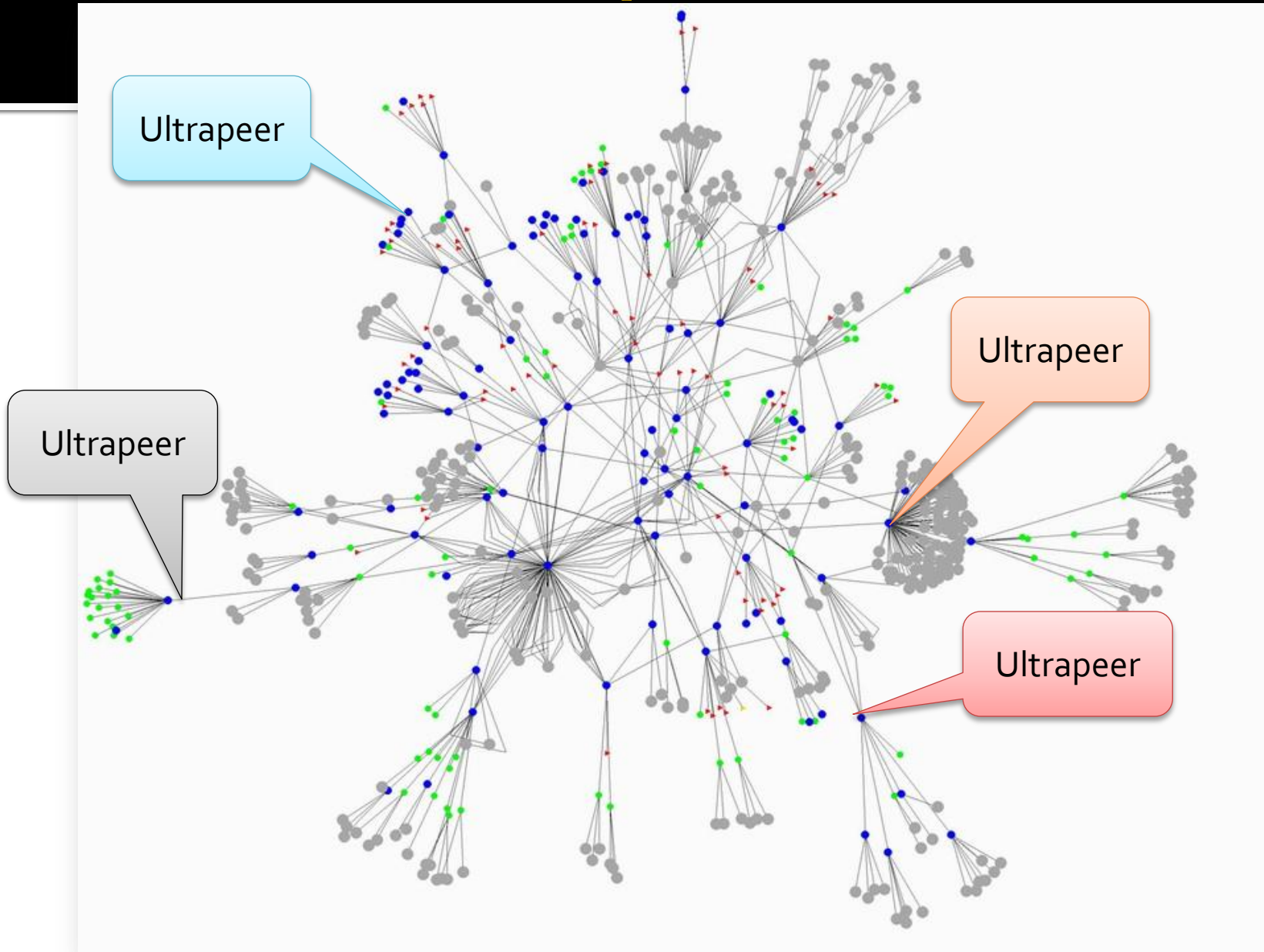
# Search in foxy



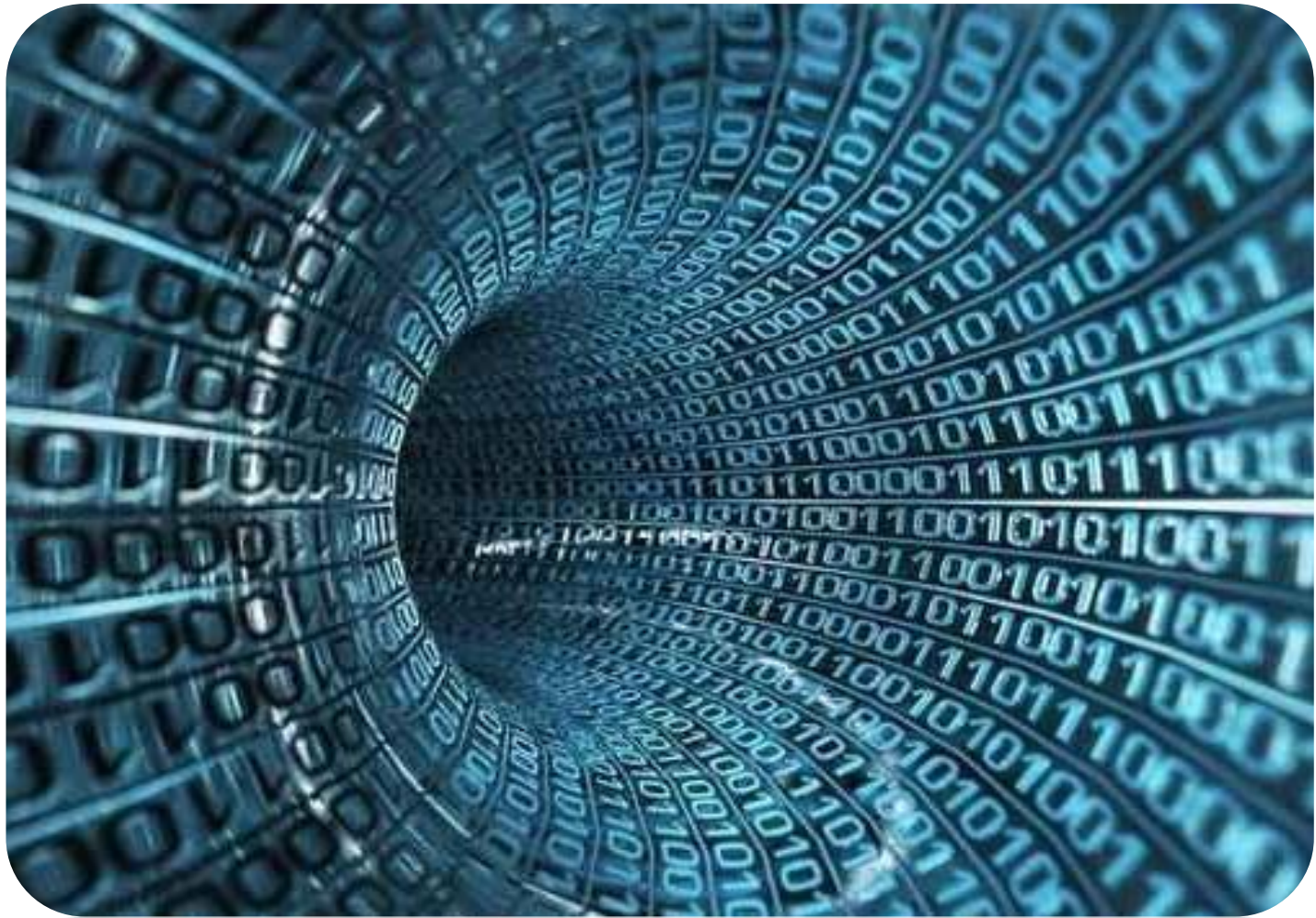
# Download in foxy



# Servent vs. Ultrapeer



# How to audit the FoxyP2P network?





## A MODEL FOR FOXY PEER-TO-PEER NETWORK INVESTIGATIONS

Ricci Jeong, Pierre Lai, Kam-Pui Chow, Frank Law, Michael Kwan and Kenneth Tse

Not very  
efficiency

Abstract In recent years, peer-to-peer (P2P) applications have become the dom-

## 4. Foxy Protocol Analysis

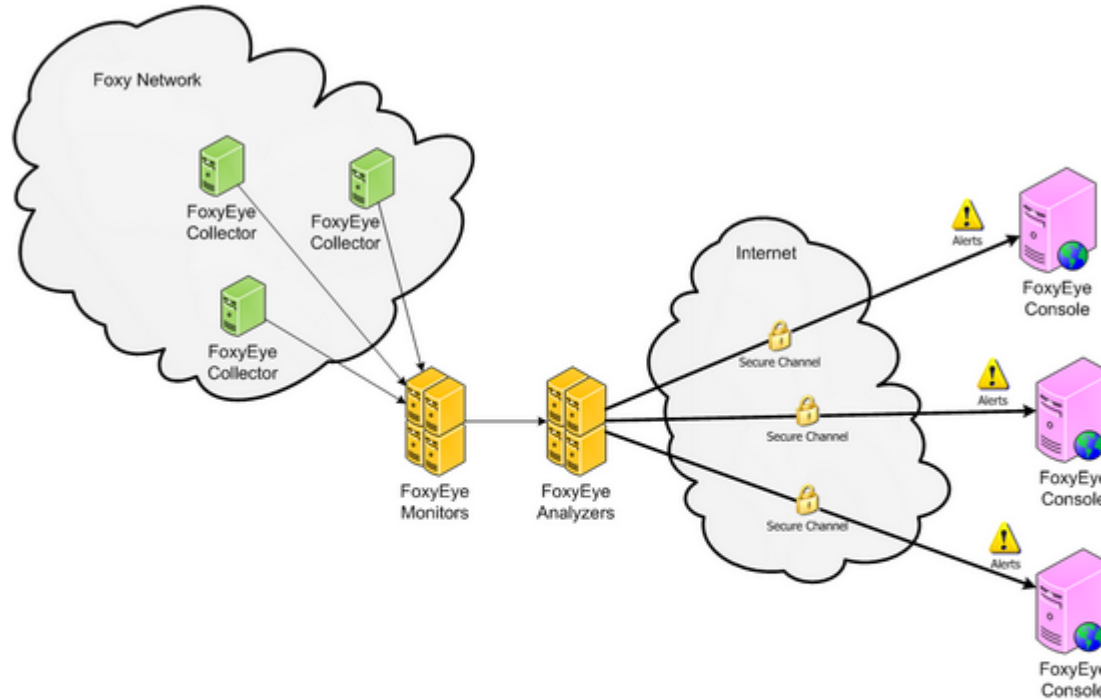
In order to determine and analyze the behavior of the Foxy network, traffic generated and received by several Foxy clients was captured using Wireshark [15], a popular network packet capturing tool. This section describes the experimental results based on the analysis of more than 80 sets of Foxy communication network traffic records involving approximately 3 million packets.

### 4.1 Data Collection

Table 1 lists the five data collections (A through E) used to analyze the Foxy protocol. The collections, which are of varying lengths, were executed over a five-month period. Data collections A and B focus on the search results of popular keywords. Data collection C compares and analyzes the search results of a query between two Foxy clients. Data collections D and E investigate how search queries and results propagate across multiple clients.

# Other products about foxy investigation: FoxyEye, FoxyCollector

## Architecture

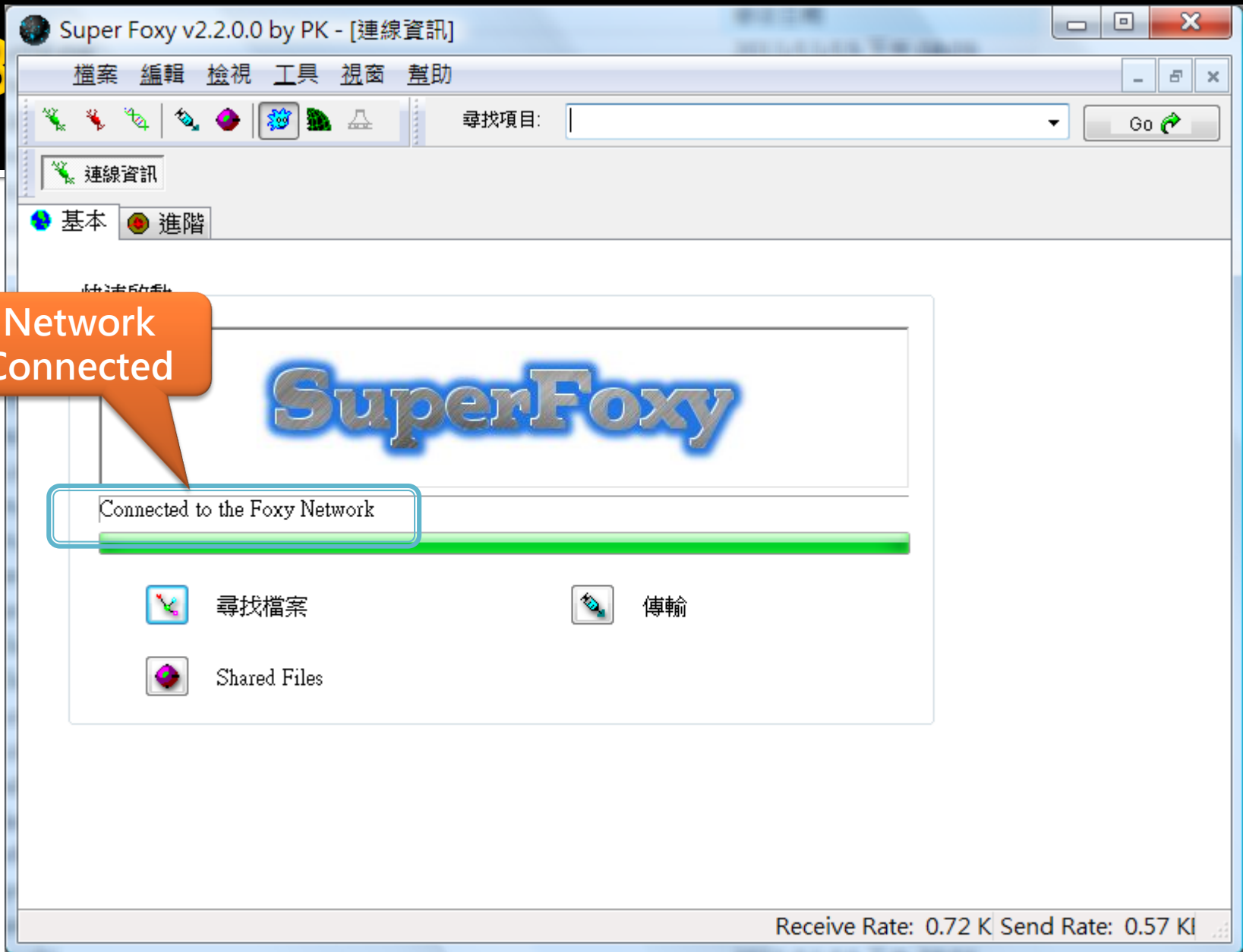


FoxyEYE monitors are effectively silent users that collect information from the FOXY network. Through the means of IP and filename matching, it can determine whether the monitored IP addresses are connected to the network and whether sensitive files are being shared among FOXY users. As a silent user, FoxyEYE collectors listen to the FOXY network without providing any data/information for other FOXY users. The collected information is sent to a local FoxyEYE monitor for keyword/IP scanning. All these matching are done inside the local network to ensure that the keywords/IP that are monitored stay within the network. Using passive scanning techniques, no active searching on the FOXY network is performed. Statistical data in the FoxyEYE solution are computed using FoxyEYE analyzers with the information from the monitors. Lastly, FoxyEYE consoles are installed to the end-user's computers. Such consoles facilitate the raising of alerts when abnormalities arise.

Now...

SWAGGER FOXY

B



Super Foxy v2.2.0.0 by PK - [蒐尋中: 筆錄 - 103 Results]

檔案 編輯 檢視 工具 視窗 幫助

尋找項目: 筆錄

連線資訊 蒐尋中: 筆錄

蒐尋結果 進階

蒐尋模式 159,419 G2 Nodes Searched, Gnutella Unknown

檔案名稱	大小	類型	速度	分散節點
卷48筆錄用.doc	105 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷47筆錄用.doc	150 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷46筆錄用.doc	114 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷45筆錄用.doc	111 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷44筆錄用.doc	122 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷43筆錄用.doc	110 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷42筆錄用.doc	130 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷41筆錄用.doc	115 KB	Microsoft Office Word ...	0 KB/s	1 Host
卷40筆錄用.doc	49 KB	Microsoft Office Word ...	0 KB/s	1 Host
車禍(酒駕)被害人筆錄(空白).lnk	913 Bytes	捷徑	0 KB/s	1 Host
車禍(酒駕)被害人筆錄(空白).LNK	799 Bytes	捷徑	0 KB/s	1 Host
私娼筆錄張鈺樺.LNK	419 Bytes	捷徑	4 KB/s	1 Host
用 Foxy 下載別人的秘密照片、帳號密碼、報稅資料、...	71 KB	HTML 文件	290 KB/s	1 Host
下載別人的秘密照片、帳號密碼、報稅資料、-信件-對...	619 KB	WinRAR 壓縮檔	54 KB/s	1 Host
八關齋戒筆錄二.doc	38 KB	Microsoft Office Word ...	0 KB/s	1 Host
98.02.03林宏達竊盜筆錄.lnk	503 Bytes	捷徑	24 KB/s	1 Host
1員工筆錄-朱麗雲.LNK	1 KB	捷徑	4 KB/s	1 Host
1員工筆錄-朱麗雲.lnk	683 Bytes	捷徑	4 KB/s	1 Host
1001003劉全能夜間-酒調查筆錄.lnk	774 Bytes	捷徑	0 KB/s	1 Host
1000918黃英豐夜間-酒駕-中山路489巷調查筆錄.lnk	824 Bytes	捷徑	0 KB/s	1 Host
1000917許水秀夜間-酒駕-中正路350-5號調查筆錄.lnk	834 Bytes	捷徑	0 KB/s	1 Host
1000522諫靜彤-酒駕-大社所調查筆錄.lnk	611 Bytes	捷徑	0 KB/s	1 Host

下載選取項目 檢視下載項目

Refine Search   Filter Results

Receive Rate: 3.57 K Send Rate: 0.90 KI

Input the search keyword

Sharing  
Nodes

延伸資訊

檔名: 武俠 (甄子丹金城武) [2011香港電影].rmvb

大小: 473,220,618 Bytes

SHA1 雜湊值: 26AUTFSYBZUNMTYOZVXOK5QDZSXOBI0E

Bitprint Hash:

14 主機列表

主機	速度	屬性	客戶端	節點...	IP反解資訊
1.64.176.36	325 KB/s	Stable	Foxy	2	1-64-176-036.static.netvigator.com
27.51.129.32	0 KB/s			0	27-51-129-32.adsl.fetnet.net
60.245.64.96	0 KB/s			0	
61.224.76.32	0 KB/s			0	61-224-76-32.dynamic.hinet.net
113.254.91.9	246 KB/s	Stable	Foxy	2	
115.43.226.28	60 KB/s	Stable	Foxy	2	host-28.226-43-115.dynamic.totalbb.net.tw
119.14.141.248	0 KB/s			0	host-248.141-14-119.dynamic.totalbb.net.tw
122.122.216.1...	0 KB/s			0	122-122-216-191.dynamic.hinet.net
124.114.215.2...	0 KB/s			0	
124.244.108.2...	0 KB/s			0	124244108201.ctinets.com

平均速度: 45 KB/s

OK

Super Foxy v2.2.0.0 by PK - [傳輸資訊]

檔案 編輯 檢視 工具 視窗 幫助

尋找項目: 筆錄 Go

連線資訊 傳輸資訊 蒐尋中: 筆錄

↓ 下載 ↑ 上傳

顯示  活動中  暫停中  已完成  已停止

File	Status	Size	Completed	Speed	ETA
GRE Account.txt	Completed	0 KB	0 KB		
GRE Argument 題庫單字表---A~Z-無句子.doc	Receiving, 40%	13,37...	5,439 KB	1.42 KB/s	1 hr, 33 min
GRE Argument 題庫單字表.doc	Waiting to Retry in 5	136 KB	0 KB		
GRE Big Book 反義上課講義內單字題.doc	Waiting to Retry in 4	104 KB	0 KB		
GRE 上課講義名詞反義考題合併版.doc	Completed	42 KB	42 KB		
GRE 上課講義形容詞反義考題合併版.doc	Retrying Host 1 of 1	59 KB	0 KB		
GRE 上課講義動詞反義考題合併版.doc	Waiting, more hosts needed	38 KB	0 KB		
GRE 方老師上課講義單字形容詞總合排序表...	Completed	324 KB	324 KB		
GRE 托福 SAT測驗常考的5000英文單字.pdf	Completed	412 KB	412 KB		
卷40筆錄用.doc	Waiting, more hosts needed	49 KB	0 KB		
卷41筆錄用.doc	Waiting, more hosts needed	115 KB	0 KB		
卷42筆錄用.doc	Waiting, more hosts needed	130 KB	0 KB		
卷43筆錄用.doc	Waiting, more hosts needed	110 KB	0 KB		
卷44筆錄用.doc	Waiting, more hosts needed	122 KB	0 KB		
卷45筆錄用.doc	Waiting, more hosts needed	111 KB	0 KB		
卷46筆錄用.doc	Waiting, more hosts needed	114 KB	0 KB		
卷47筆錄用.doc	Waiting, more hosts needed	150 KB	0 KB		
卷48筆錄用.doc	Waiting, more hosts needed	105 KB	0 KB		
卷49筆錄用.doc	Waiting, more hosts needed	132 KB	0 KB		
卷50筆錄用.doc	Waiting, more hosts needed	148 KB	0 KB		
張珮雯-援交30歲_新營分局調查筆錄.doc	Completed	60 KB	60 KB		

移除已選取項目 清除已完成項目 設定 至下載目錄

Receive Rate: 1.56 K Send Rate: 0.15 KI

Downloading

↓ 下載 ↑ 上傳

顯示

活動中  暫停中  已完成  已停止

File	Status	Size	Completed	Speed	ETA
GRE Account.txt	Completed	0 KB	0 KB		
GRE Argument 題庫單字表---A~Z-無句子.doc	Receiving, 40%	13,37...	5,453 KB	1.23 KB/s	1 hr, 47 min
GRE Argument 題庫單字表.doc	Waiting to Retry in 1	136 KB	0 KB		
GRE Big Book 反義上課講義內單字題.doc	Pending, 1 Host Found	104 KB	0 KB		
GRE 上課講義名詞反義考題合併版.doc					
GRE 上課講義形容詞反義考題合併版.doc					
GRE 上課講義動詞反義考題合併版.doc					
GRE 方老師上課講義單字形容詞總合排序表...					
GRE 托福 SAT測驗常考的5000英文單字.pdf	Completed	412 KB	412 KB		
卷40筆錄用.doc	Waiting, more hosts needed	49 KB	0 KB		
卷41筆錄用.doc	Waiting, more hosts needed	115 KB	0 KB		
卷42筆錄用.doc	Waiting, more hosts needed	130 KB	0 KB		
卷43筆錄用.doc	Waiting, more hosts needed	110 KB	0 KB		
卷44筆錄用.doc	Waiting, more hosts needed	122 KB	0 KB		
卷45筆錄用.doc	Waiting, more hosts needed	111 KB	0 KB		
卷46筆錄用.doc	Waiting, more hosts needed	114 KB	0 KB		
卷47筆錄用.doc	Waiting, more hosts needed	150 KB	0 KB		
卷48筆錄用.doc	Waiting, more hosts needed	105 KB	0 KB		
卷49筆錄用.doc	Waiting, more hosts needed	132 KB	0 KB		
卷50筆錄用.doc	Waiting, more hosts needed	148 KB	0 KB		
張珮雯~援交30歲_新營分局調查筆錄.doc	Completed	60 KB	60 KB		

More information

- 開啟
- 重新蒐尋
- 更多資訊
- 開始傳輸
- 停止傳輸
- 移除

移除已選取項目

清除已完成項目

設定

至下載目錄



# Count.

**Receiving**

**File part list**

**各結點傳輸協定**

Extended Info

Name: GRE Argument 題庫單字表-A~Z-無句子.doc  
Size: 13,691,392 bytes

SHA1 Hash:  
TigerTree Hash:

1 Host:

Host	Speed	Status	Client
180.218.122.216:6774	241 KB/s	Receiving	Mxie 9.9.9.9

Handshake:

```
GET /get/2457398/GRE Argument 題庫單字表-A~Z-無句子.doc HTTP/1.1
Host: 180.218.122.216:6774
User-Agent: Foxy 1.9.10.0
Listen-IP: 220.132.129.167:17047
Connection: Keep-Alive
Range: bytes=5600032-5767167
X-Queue: 0.1
X-Features: g2/1.0

HTTP/1.1 206 Partial Content
Server: Mxie 9.9.9.9
Content-type: application/octet-stream
```

Start	Completed	S
0	524,288	524,288
524,288	524,288	524,288
1,048,576	524,288	524,288
1,572,864	524,288	524,288
2,097,152	524,288	524,288
2,621,440	524,288	524,288
3,145,728	524,288	524,288
3,670,016	524,288	524,288
4,194,304	524,288	524,288
4,718,592	524,288	524,288
5,242,880	407,972	524,288
5,767,168	0	524,288
6,291,456	0	524,288
6,815,744	0	524,288
7,340,032	0	524,288
7,864,320	0	524,288
8,388,608	0	524,288
8,912,896	0	524,288
9,437,184	0	524,288
9,961,472	0	524,288
10,485,760	0	524,288

# Exploiting the Security Weaknesses of the Gnutella Protocol

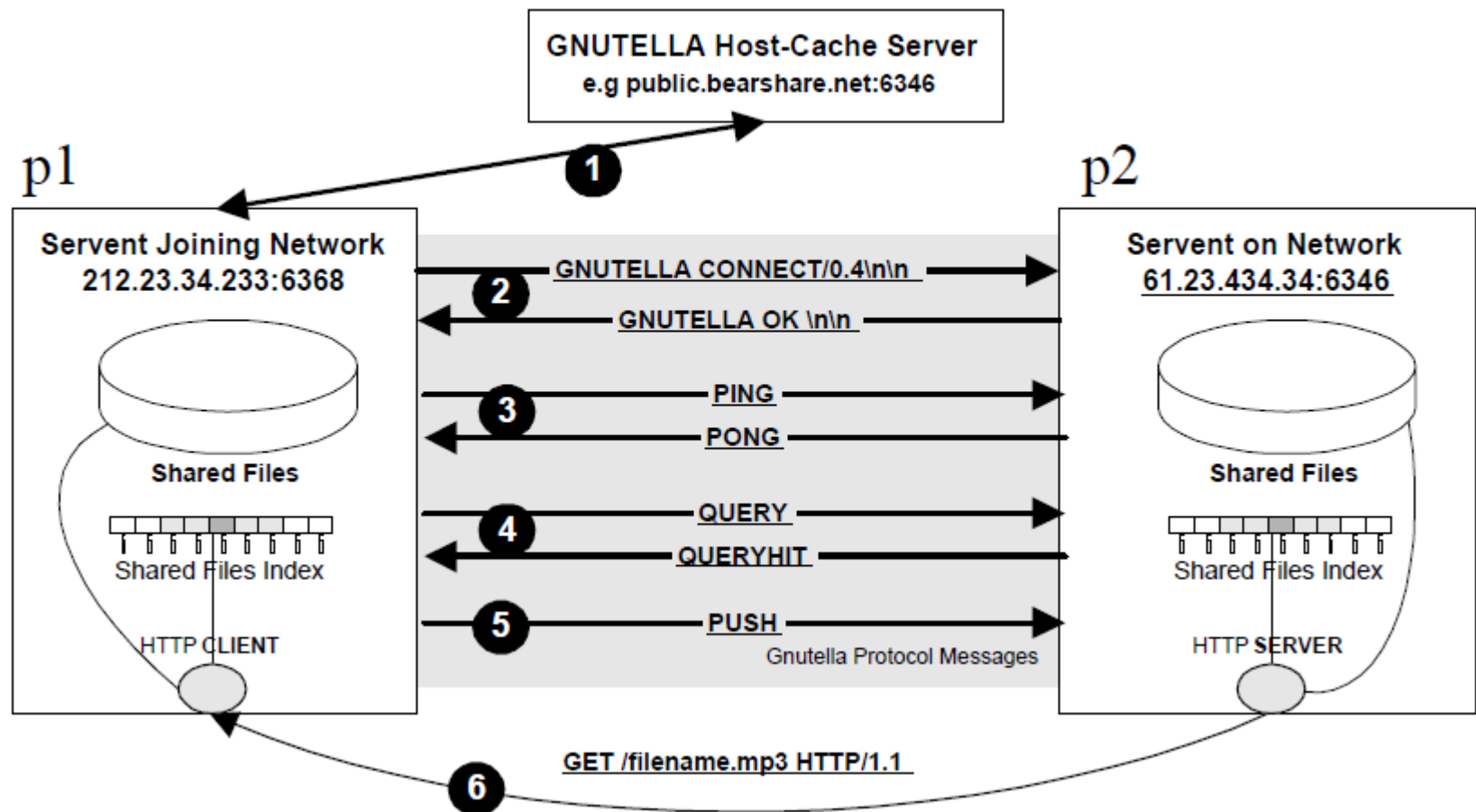
- Gnutella's distributed search protocol allows a set of peers, servers or clients, to perform filename searches over other clients without the need of an intermediate index server.
- The Gnutella network topology is a pure Ad-Hoc topology where clients may join or leave the network at any time without affecting the rest topology in any sense.

# Gnutella's Searching Algorithm

- Recall that using the purely decentralized version, packets are flooded throughout the network.
- If the vo.6 ultrapeer recommendation is implemented, searching is optimized using Query hash tables(QHTs).
  - A QHT is maintained by each node, and describes the content it is sharing.
  - An ultrapeer maintains an aggregate of its leaf's QHTs and its own QHT.
  - Searches are performed by forwarding a query to an ultrapeer, who checks its aggregate QHT for a match.
    - If there is a match, the query is forwarded to the appropriate leaf, otherwise the query is forwarded to neighbouring ultrapeers by “flooding” .

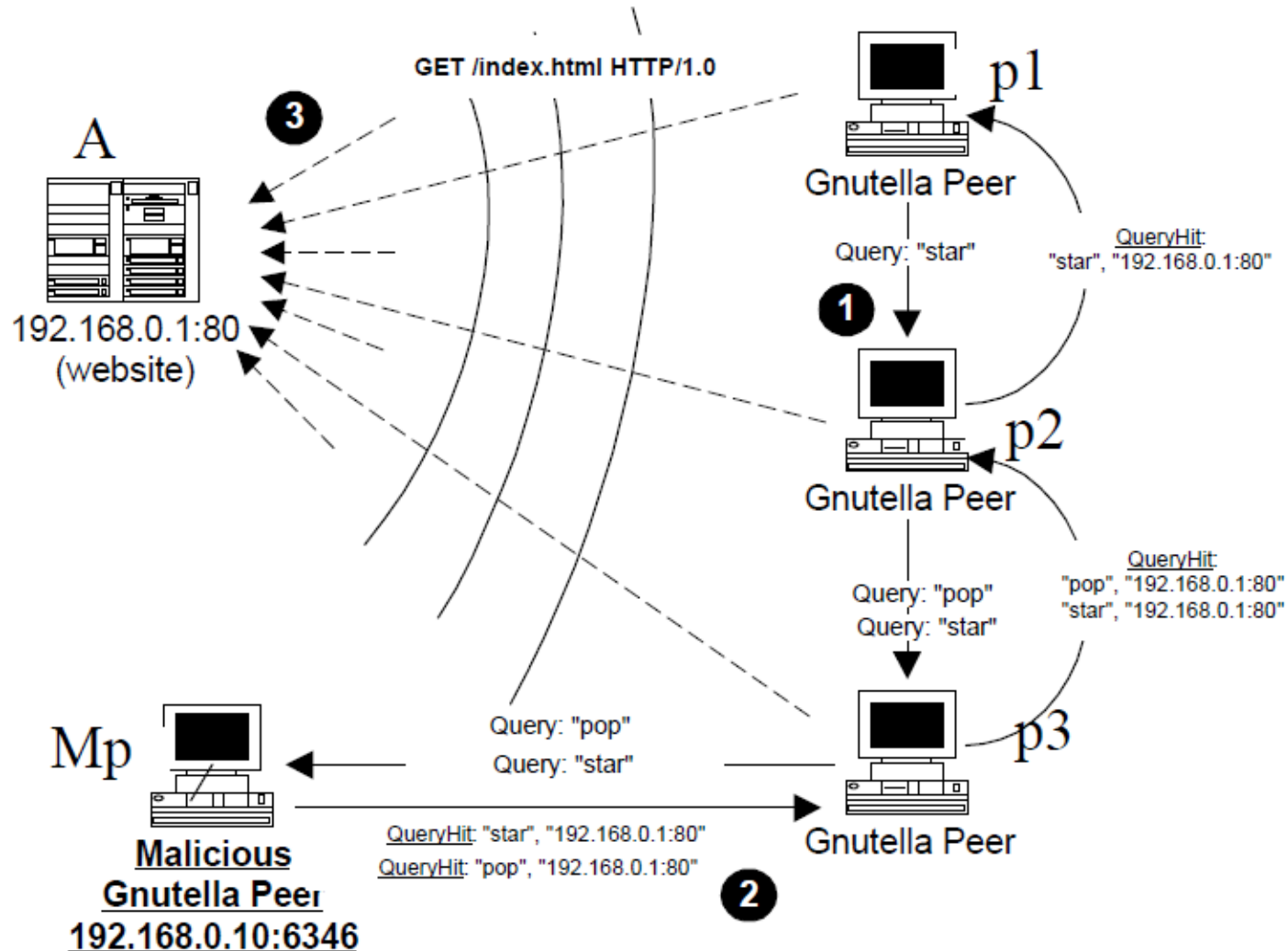
# Gnutella v0.4 Protocol

## The Gnutella v0.4 Protocol

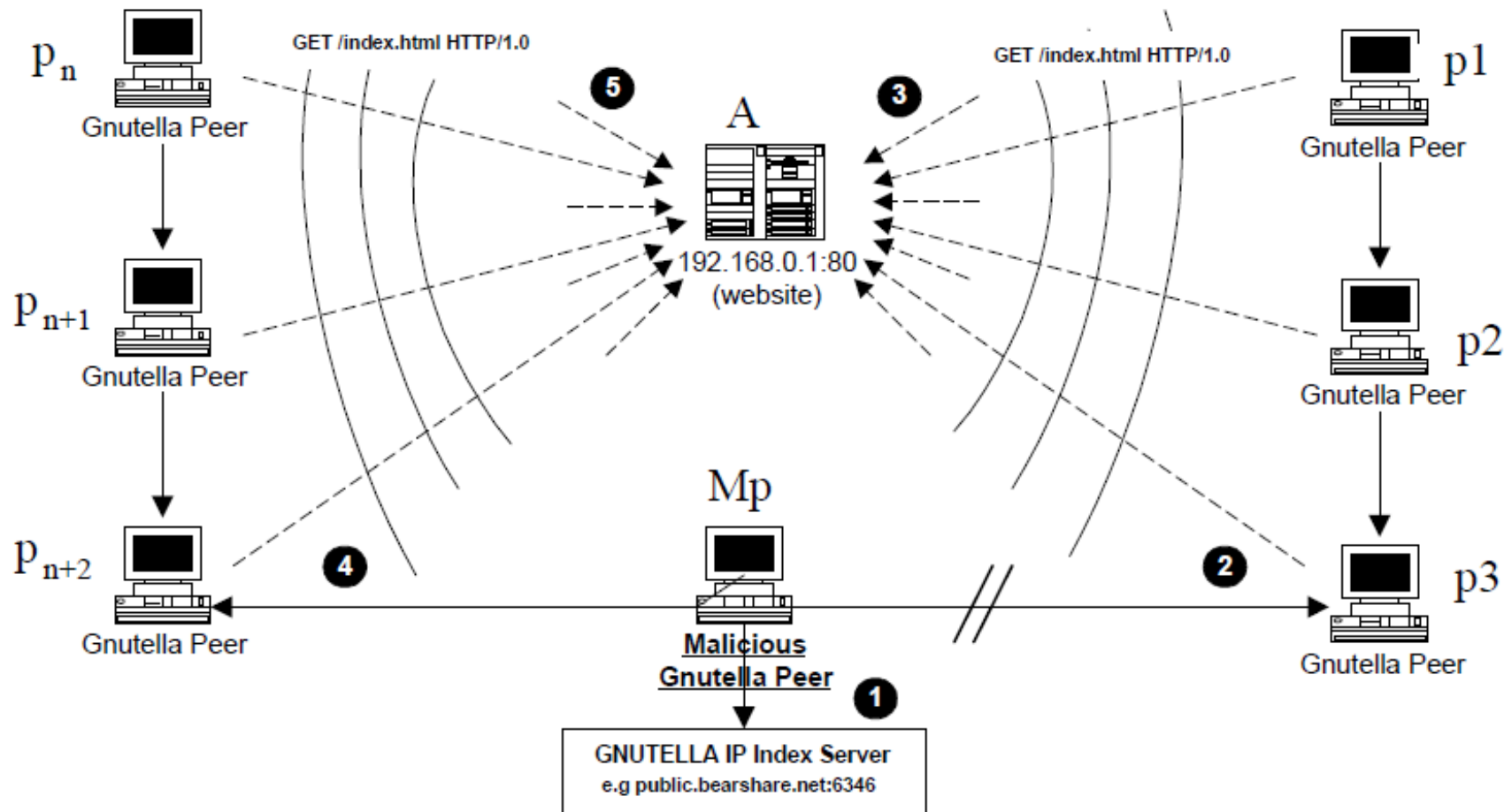


# Performing a Distributed Denial Service on a public webserver

Gnutella Network G



Gnutella Network  $G$



# DDoS Scalability

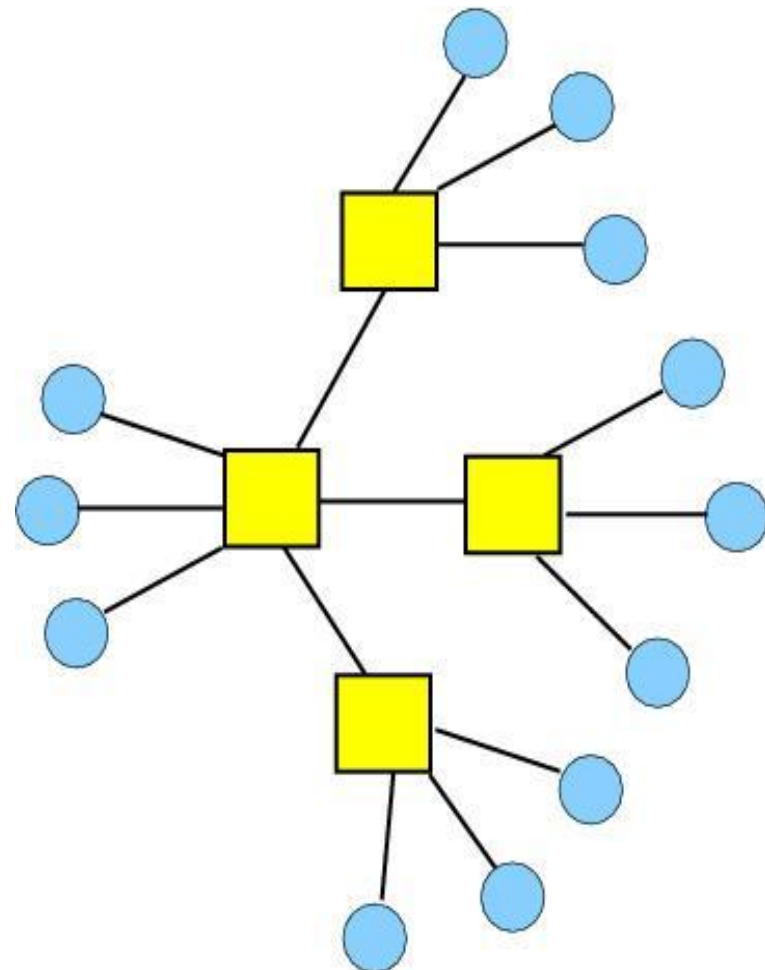
- If we assume that each  $p$  is connecting to averagely 5 other peers (which is usually much higher) and will forward a message only in a depth of 7 (i.e.  $TTL=7$ ), which is also typical for a Gnutella client and assuming that each peer is using message flooding, which means that  $M_p$  fake responses will be sent to all of its peers we will averagely reach 20,480 other  $p$ .
- The reach is determined by  $n$  (# connections to other hosts) and  $TTL$  :

$$\sum_{t=1}^{TTL} (n - 1)^{t-1} \cdot n$$

- Assumption: nodes all have the same  $n$  and  $TTL$ .

# Gnutella2's Network Architecture

- Decentralized, 2-tier.
- This architecture is recommended for Gnutella in vo.6.
- New node enters by connecting to a known hub (almost identical to Gnutella's handshake).
- Hubs typically accept 300-500 leaves, and connect to 5-30 other hubs.
- Leaves typically connect to 3 hubs.

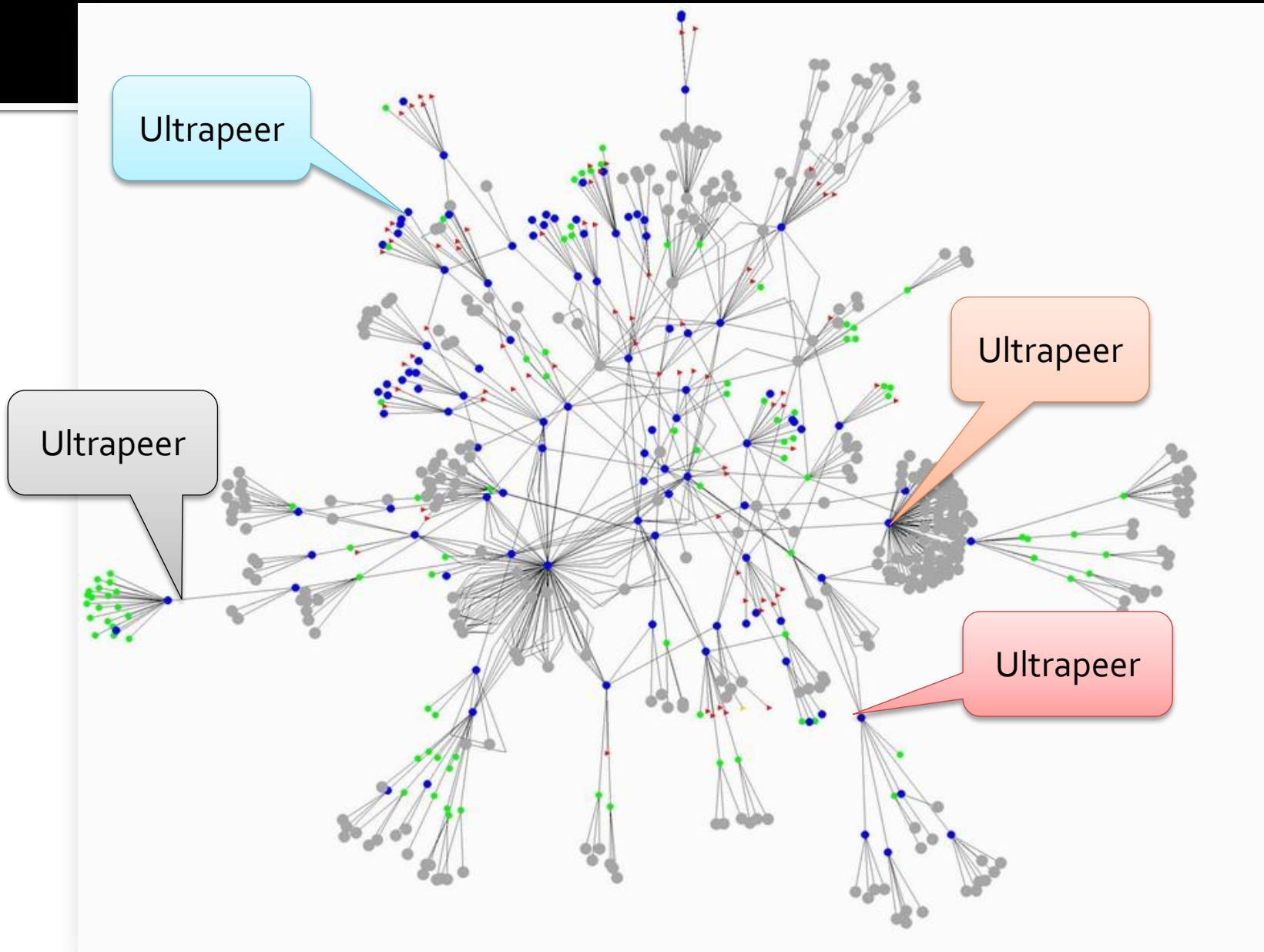




# Gnutella2's Searching Algorithm

- Ultrapeers are called “hubs” .
- Uses a QHT like Gnutella, but if a hub cannot match a query to its aggregate QHT, it checks a set of caches:
  - Each hub maintains a cached copy of each neighbouring hub's aggregate QHT.
  - Upon a search miss, a hub will try to match the query against its cached copies of its neighbours QHTs.
  - If the query matches, it will forward the query once, and the node that receives the query processes it and directly sends the result back to the client.
  - If no match is made, the searching client will continue at another untried hub.

# Maximizing the Number of Polluted Peers



連線資訊

基本

進階

已知結點:

Node	Status
Cache at 90.12 %	
122.120.65.157:4019	G2 Local: 503 Maximum...
60.249.198.33:24349	G2 Local: 503 Maximum...
123.205.183.23:6178	G2 Local: 503 Maximum...
168.70.45.155:2986	G2 Remote: 503 Maximu...
59.149.237.212:10009	G2 Local: 503 Maximum...
118.160.24.38:22399	G2 Remote: 503 Maximu...
118.160.89.241:19287	G2 Remote: 503 Maximu...
180.176.110.235:21697	連線中...
114.27.196.230:5680	G2 Remote: Closed
218.253.252.102:12495	連線中...

Add Node:

Address: Port: 

新增

移除

已連線結點:

Node	Type	Bandwidth	Efficiency
118.170.22.182:21707	Ultrapeer	1.47 KB/s	81.85 %
123.194.240.216:12765	Ultrapeer	1.02 KB/s	80.84 %
114.47.206.223:6106	Ultrapeer	1.47 KB/s	73.98 %
59.104.217.246:18899	Ultrapeer	1.82 KB/s	61.55 %
59.104.24.133:11065	Ultrapeer	1.17 KB/s	64.87 %
218.166.105.2:7900	Ultrapeer	1.45 KB/s	67.20 %
111.249.58.132:8554	Ultrapeer	1.44 KB/s	75.62 %
123.110.13.52:10238	Ultrapeer	0.79 KB/s	67.35 %
223.142.195.225:3138	Ultrapeer	1.63 KB/s	58.96 %
61.228.144.6:23641	Ultrapeer	1.70 KB/s	63.62 %
118.233.166.96:2883	Ultrapeer	1.51 KB/s	68.71 %
114.46.169.98:5052	Ultrapeer	1.61 KB/s	65.95 %
114.36.189.250:3751	Ultrapeer	1.75 KB/s	65.78 %
61.57.152.82:11668	Ultrapeer	1.66 KB/s	64.36 %
118.167.241.184:23486	Ultrapeer	1.65 KB/s	52.46 %
125.229.244.72:12746	Ultrapeer	1.46 KB/s	64.78 %
221.127.155.191:24859	Ultrapeer	1.21 KB/s	43.21 %
59.115.150.91:2526	Ultrapeer	1.48 KB/s	55.20 %
220.141.156.231:8144	Ultrapeer	1.45 KB/s	48.00 %
112.119.62.122:12030	Ultrapeer	1.53 KB/s	57.87 %
61.62.96.44:2603	Ultrapeer	1.48 KB/s	51.13 %
115.43.95.230:6867	Ultrapeer	0.97 KB/s	59.34 %
125.231.169.20:2651	Ultrapeer	1.49 KB/s	55.70 %
112.119.21.184:2873	Ultrapeer	1.49 KB/s	57.52 %
61.231.74.215:19241	Ultrapeer	1.56 KB/s	60.26 %
119.247.50.44:21309	Ultrapeer	1.49 KB/s	56.54 %
118.168.91.87:4953	Ultrapeer	1.47 KB/s	54.56 %

Display

 Gnutella G2

# Launch DDoS attacks

```
pk@inspector: ~  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 0.0.0.0:111             0.0.0.0:*              LISTEN  
tcp        0      0 0.0.0.0:80              0.0.0.0:*              LISTEN  
tcp        0      0 0.0.0.0:59064           0.0.0.0:*              LISTEN  
tcp        0      0 0.0.0.0:25              0.0.0.0:*              LISTEN  
tcp        0      0 0.0.0.0:443             0.0.0.0:*              LISTEN  
tcp        0      0 172.16.1.27:443        218.174.65.199:3796    SYN_RECV  
tcp        0      0 172.16.1.27:443        180.218.110.204:1299   SYN_RECV  
tcp        0      0 172.16.1.27:443        180.218.110.204:1062   SYN_RECV  
tcp        0 41 172.16.1.27:443        114.39.26.70:1681     ESTABLISHED  
tcp        0      0 172.16.1.27:443        118.168.223.207:2531   ESTABLISHED  
tcp        0      0 172.16.1.27:443        114.39.26.70:1362     ESTABLISHED  
tcp        0 41 172.16.1.27:443        219.70.217.188:59612  ESTABLISHED  
tcp        0      0 172.16.1.27:443        113.196.145.180:2318   FIN_WAIT2  
tcp        0      0 172.16.1.27:443        118.168.223.207:2672   ESTABLISHED  
tcp        0      0 172.16.1.27:443        61.224.207.89:62587   FIN_WAIT2  
tcp        0      1 172.16.1.27:443        118.168.223.207:2456   FIN_WAIT1  
tcp        0      0 172.16.1.27:443        219.80.135.46:3838    FIN_WAIT2  
tcp        0      0 172.16.1.27:443        118.168.223.207:2579   ESTABLISHED  
tcp        0 41 172.16.1.27:443        98.230.50.246:3715    ESTABLISHED  
tcp        0      1 172.16.1.27:443        42.98.203.38:2944     FIN_WAIT1  
tcp        0      0 172.16.1.27:443        223.139.208.141:3780   ESTABLISHED  
tcp        0      0 172.16.1.27:443        1.169.125.186:59590    ESTABLISHED  
tcp        0      1 172.16.1.27:443        118.160.43.47:58443    FIN_WAIT1  
tcp        0      1 172.16.1.27:443        61.231.66.87:4428     FIN_WAIT1  
tcp        0      0 172.16.1.27:443        118.165.219.192:19327  ESTABLISHED  
tcp        0      0 172.16.1.27:443        220.129.39.252:4520    ESTABLISHED  
tcp        0      1 172.16.1.27:443        1.169.125.186:61530    FIN_WAIT1
```

# Reference

- <http://evchk.wikia.com/wiki/Foxy>
- [http://www.cs.hku.hk/cisc/event/20080827\\_FoxyPCO/FoxyPCO\\_20080827.pdf](http://www.cs.hku.hk/cisc/event/20080827_FoxyPCO/FoxyPCO_20080827.pdf)
- [http://en.wikipedia.org/wiki/Foxy\\_\(P2P\)](http://en.wikipedia.org/wiki/Foxy_(P2P))
- <http://alumni.cs.ucr.edu/~csyiazti/courses/cs260-2/project/gnutella.pdf>
- [http://limewire.negatis.com/index.php?title=Dynamic\\_Querying](http://limewire.negatis.com/index.php?title=Dynamic_Querying)
- <http://crawler.trillinux.org/status.html>
- [www.scs.carleton.ca/~kranakis/523-course/Thorpe.ppt](http://www.scs.carleton.ca/~kranakis/523-course/Thorpe.ppt)
- <http://gnucleus.cvs.sourceforge.net/viewvc/gnucleus/>

# Q/A



Thank You

If you have any questions, please contact me at

[peikan@gmail.com](mailto:peikan@gmail.com)