Foxy: the good, the bad, and the ugly

Dr K P Chow & Computer Forensics Research Group
Center for Information Security and Cryptography
University of Hong Kong

Agenda

- Incidents related to Foxy
- What is Foxy?
- Foxy security questions:
  - Why so many personal and confidential documents available on Foxy?
  - Is it possible to trace who shares a copy of a document?
  - Is it possible to trace the *seeder* of a document
  - Once a document is available on Foxy, can it be *removed*?

Incidents that related to Foxy

Case 26/05/2008 : Police confidential information leakage

- On May 26, 2008, police confidential and classified documents discovered by Foxy 天王
- The documents include information on three undercover police officers who have bought illegal substances in a dubious Mong Kok disco and cars used by people suspected of thefts from motor vehicles in Wong Tai Sin
- And more …

Foxy天王再爆三大部門秘料

上週四，入境處十六份監聽黑名單的機密文件在搜尋器FOXY外洩，震動整個港府。翌日特首曾蔭權下令入境處要即時整頓，處長白韞六公開宣布已把所有機密資料劃走，確保不再外洩。不過，同一名爆料人繼續在FOX...

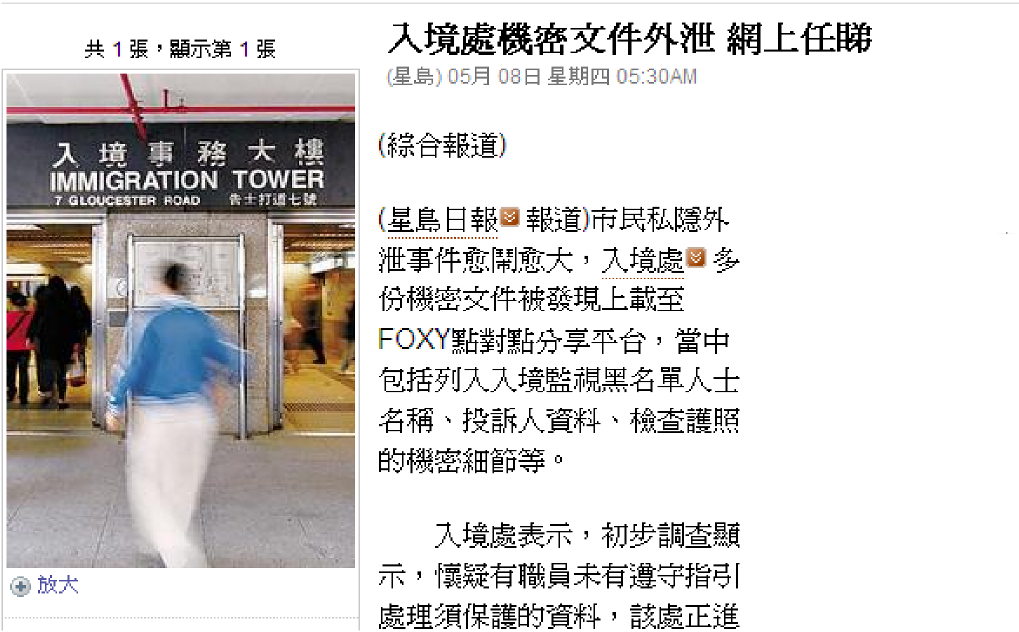
臥底警身份曝光

Foxy又洩密 兩月第二宗

政府部門紛「中招」

Case 08/05/2008 : HK Immigration Department “watchlist” partially leaked onto website

- The PC of the employee in Immigration Department has the Foxy installed
- When he connected to the Internet, the files were distributed without his knowledge



入境處機密文件外泄 網上任睇

(星島) 05月 08日 星期四 05:30AM

(綜合報道)

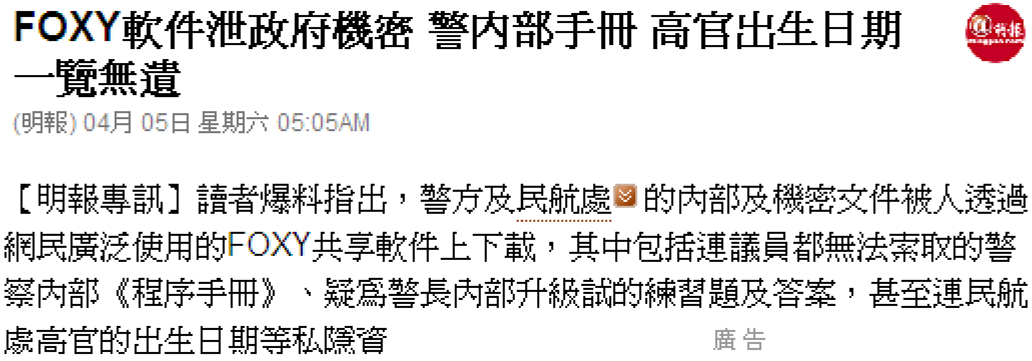
(星島日報報道)市民私隱外泄事件愈鬧愈大，入境處多份機密文件被發現上載至FOXY點對點分享平台，當中包括列入入境監視黑名單人士名稱、投訴人資料、檢查護照的機密細節等。

入境處表示，初步調查顯示，懷疑有職員未有遵守指引處理須保護的資料，該處正進

Case 05/04/2008 : Police internal information leakage

- On Apr 5, 2008, MingPao reported that users can use the keywords “pol”, “fpm” etc to search for internal information of Hong Kong Police

- These information include internal forms, procedures manual, promotion exam questions and answers, even the birthdates of some of the higher authorities.



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) 04月 05日 星期六 05:05AM

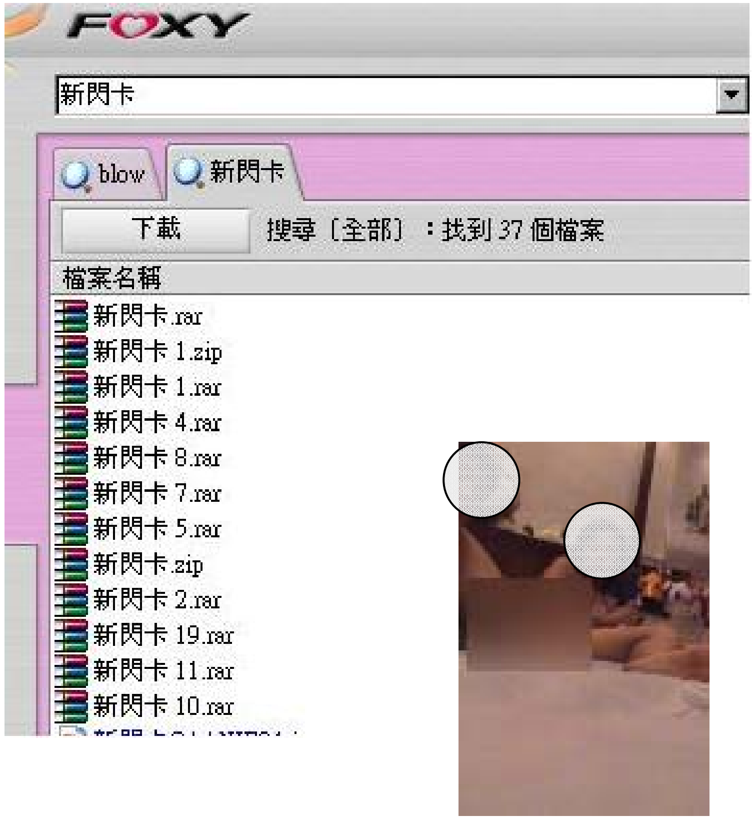
【明報專訊】讀者爆料指出，警方及民航處的內部及機密文件被人透過網民廣泛使用的FOXY共享軟件上下載，其中包括連議員都無法索取的警察內部《程序手冊》、疑爲警長內部升級試的練習題及答案，甚至連民航處高官的出生日期等私隱資

廣告

Case 02/2008 : Edison Chen's scandal photos leakage

- On Feb 2008, Internet users use FOXY to share Edison's scandal photos:
  - Whenever new photos surface on the internet, they pass on the messages using the code: "hurry on bit the fox" and using the keyword "新閃卡"
  - Users share the files with names 新閃卡 by putting those files in their share folder
  - The photos spread rapidly on the Foxy network

- Law enforcement has tried to trace users who share the photos on the Foxy network



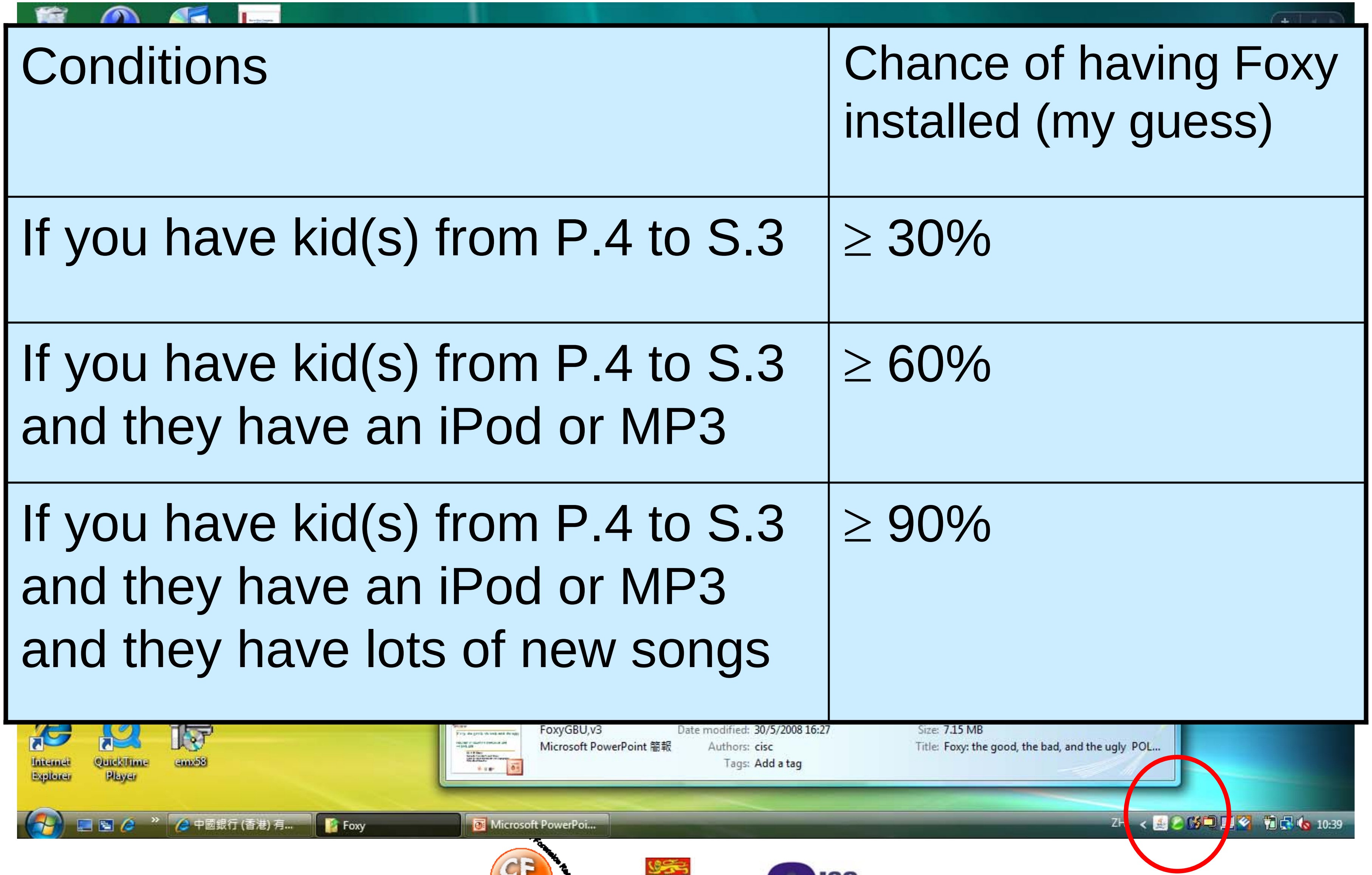
新閃卡

搜尋〔全部〕：找到 37 個檔案

檔案名稱
新閃卡.rar
新閃卡 1.zip
新閃卡 1.rar
新閃卡 4.rar
新閃卡 8.rar
新閃卡 7.rar
新閃卡 5.rar
新閃卡.zip
新閃卡 2.rar
新閃卡 19.rar
新閃卡 11.rar
新閃卡 10.rar

Does your home PC have Foxy installed?

Conditions	Chance of having Foxy installed (my guess)
If you have kid(s) from P.4 to S.3	≥ 30%
If you have kid(s) from P.4 to S.3 and they have an iPod or MP3	≥ 60%
If you have kid(s) from P.4 to S.3 and they have an iPod or MP3 and they have lots of new songs	≥ 90%



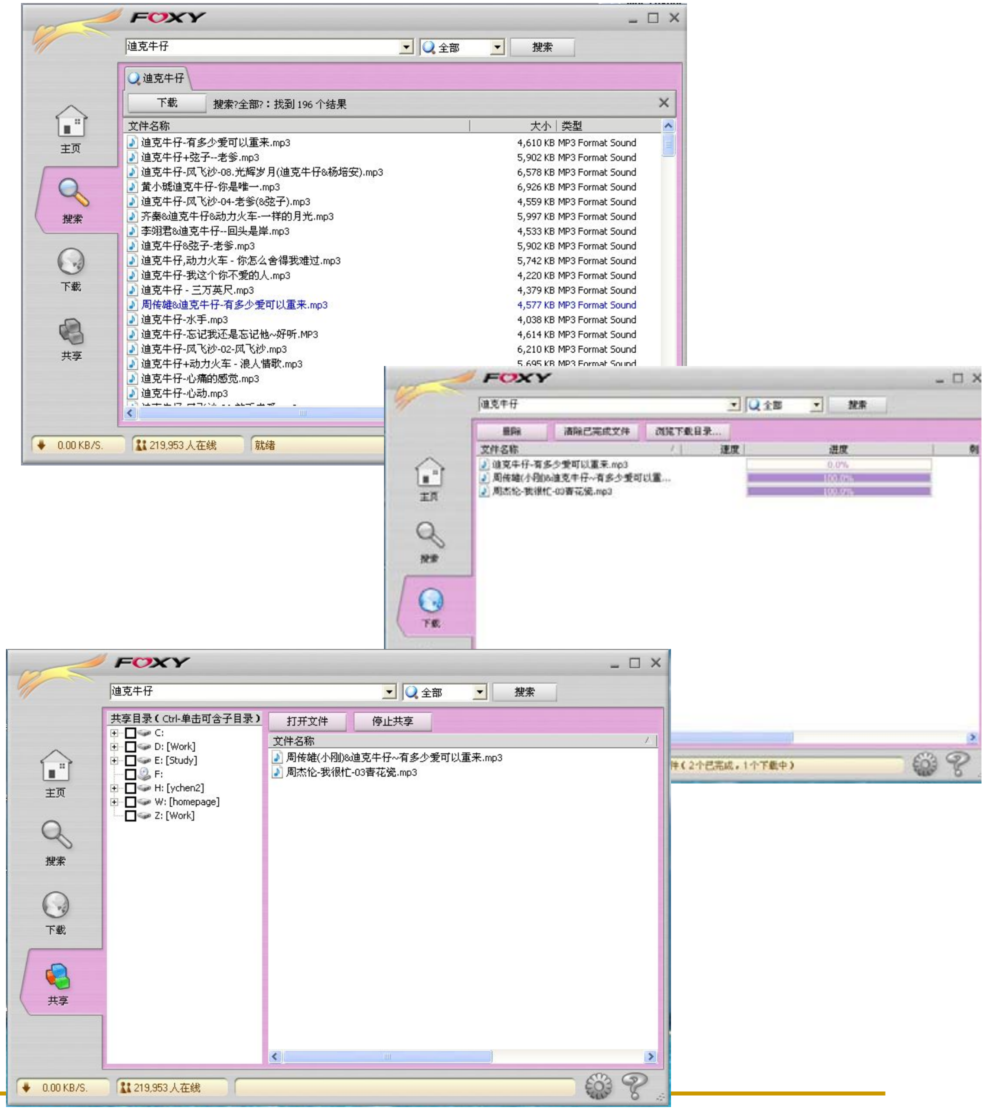
FoxyGBU,v3
Microsoft PowerPoint 簡報
Date modified: 30/5/2008 16:27
Authors: cisc
Tags: Add a tag
Size: 7.15 MB
Title: Foxy: the good, the bad, and the ugly POL...

What is Foxy?

What is Foxy?

- Foxy
  - A Traditional Chinese peer to peer file transfer program
  - Initially published by Foxy Media, Inc.
  - Widely used in Hong Kong, Mainland China and Taiwan
  - Very popular in upper primary schools and secondary schools

- Unlike other P2P programs (such as eMule, BitTorrent), Foxy is
  - Very easy to use
  - Has unlimited download capabilities



迪克牛仔 | 全部

搜索?全部?：找到 196 个结果

文件名称	大小	类型
迪克牛仔-有多少爱可以重来.mp3	4,610 KB	MP3 Format Sound
迪克牛仔+弦子--老爹.mp3	5,902 KB	MP3 Format Sound
迪克牛仔-风飞沙-08.光辉岁月(迪克牛仔&杨培安).mp3	6,578 KB	MP3 Format Sound
黃小琥迪克牛仔-你是唯一.mp3	6,926 KB	MP3 Format Sound
迪克牛仔-风飞沙-04-老爹(&弦子).mp3	4,559 KB	MP3 Format Sound
齐秦&迪克牛仔&动力火车-一样的月光.mp3	5,997 KB	MP3 Format Sound
李翊君&迪克牛仔--回头是岸.mp3	4,533 KB	MP3 Format Sound
迪克牛仔&弦子-老爹.mp3	5,902 KB	MP3 Format Sound
迪克牛仔,动力火车 - 你怎么舍得我难过.mp3	5,742 KB	MP3 Format Sound
迪克牛仔-我这个你不爱的人.mp3	4,220 KB	MP3 Format Sound
迪克牛仔 - 三万英尺.mp3	4,379 KB	MP3 Format Sound
周传雄&迪克牛仔-有多少爱可以重来.mp3	4,577 KB	MP3 Format Sound
迪克牛仔-水手.mp3	4,038 KB	MP3 Format Sound
迪克牛仔-忘记我还是忘记他~好听.MP3	4,614 KB	MP3 Format Sound
迪克牛仔-风飞沙-02-风飞沙.mp3	6,210 KB	MP3 Format Sound
迪克牛仔+动力火车 - 浪人情歌.mp3	5,695 KB	MP3 Format Sound
迪克牛仔-心痛的感觉.mp3		
迪克牛仔-心动.mp3		

0.00 KB/S. | 219,953 人在线 | 就绪

文件名称	速度	進度
迪克牛仔-有多少爱可以重来.mp3		0.0%
周传雄(小刚)&迪克牛仔~有多少爱可以重...		100.0%
周杰伦-我很忙-03青花瓷.mp3		100.0%

件（2个已完成，1个下载中）

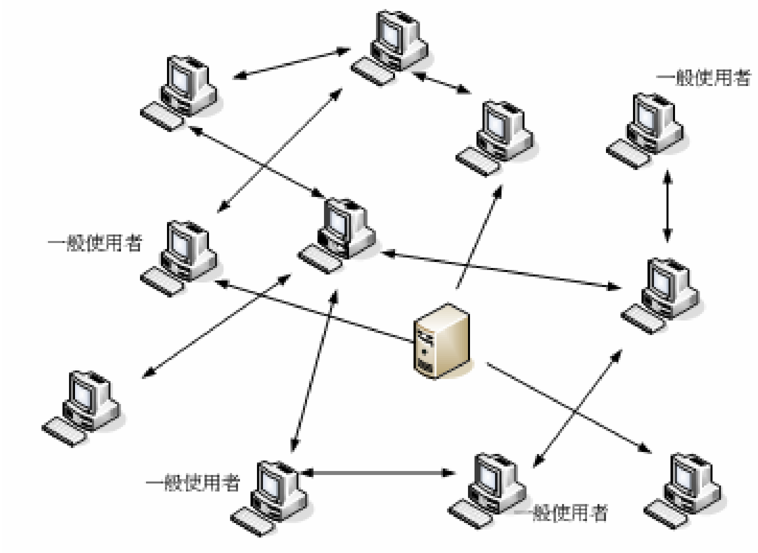
共享目录（Ctrl-单击可含子目录）
- ☐ C:
- ☐ D: [Work]
- ☐ E: [Study]
- ☐ F:
- ☐ H: [ychen2]
- ☐ W: [homepage]
- ☐ Z: [Work]

文件名称
周传雄(小刚)&迪克牛仔~有多少爱可以重来.mp3
周杰伦-我很忙-03青花瓷.mp3

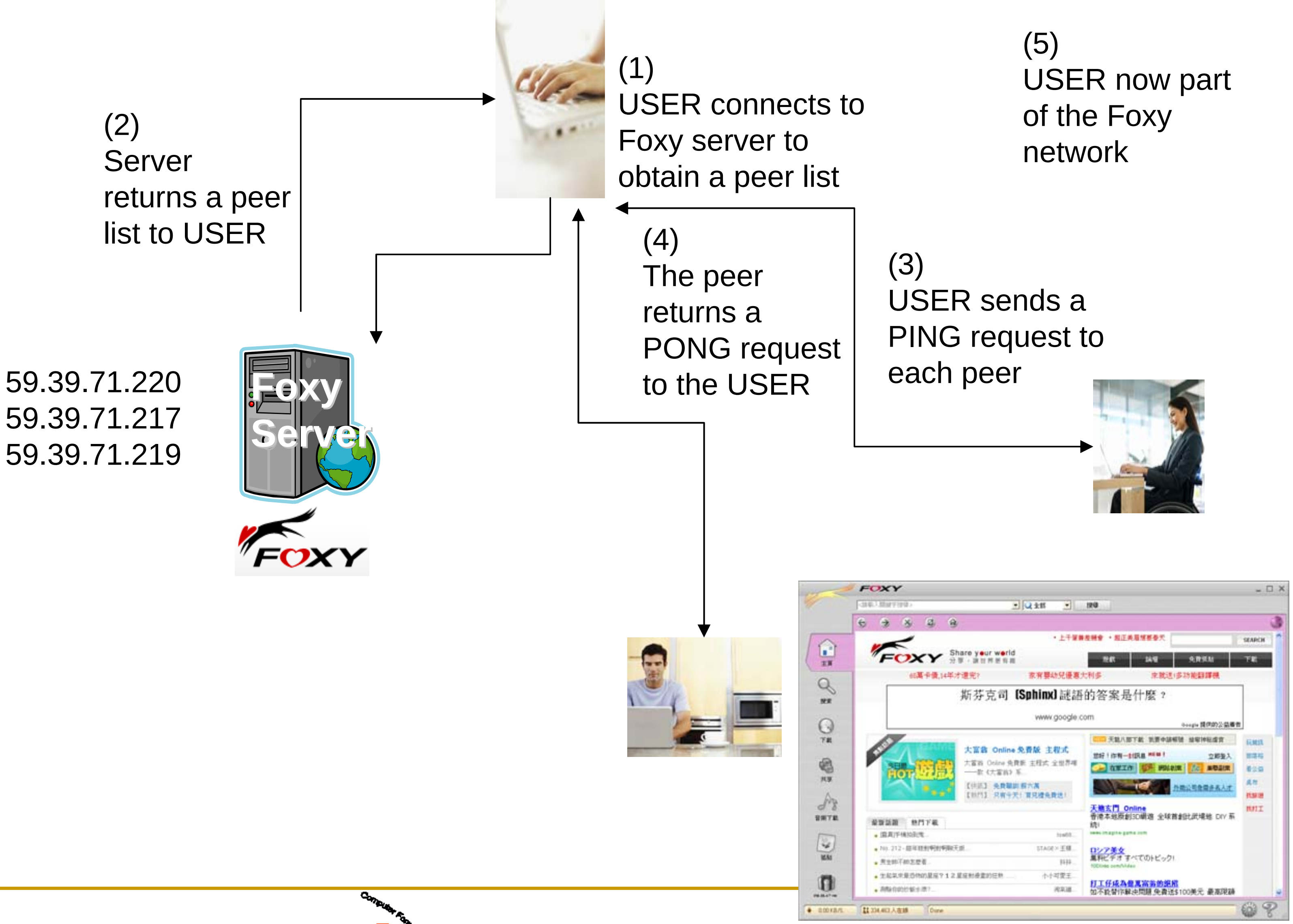
0.00 KB/S. | 219,953 人在线

Foxy Architecture

1. Connecting to the Foxy network
2. Search for files on the Foxy network
   - Based on Gnutella 2 protocol
3. Download file from a peer
   - Based on http download



Connecting to the Foxy network



(1)
USER connects to
Foxy server to
obtain a peer list

(2)
Server
returns a peer
list to USER

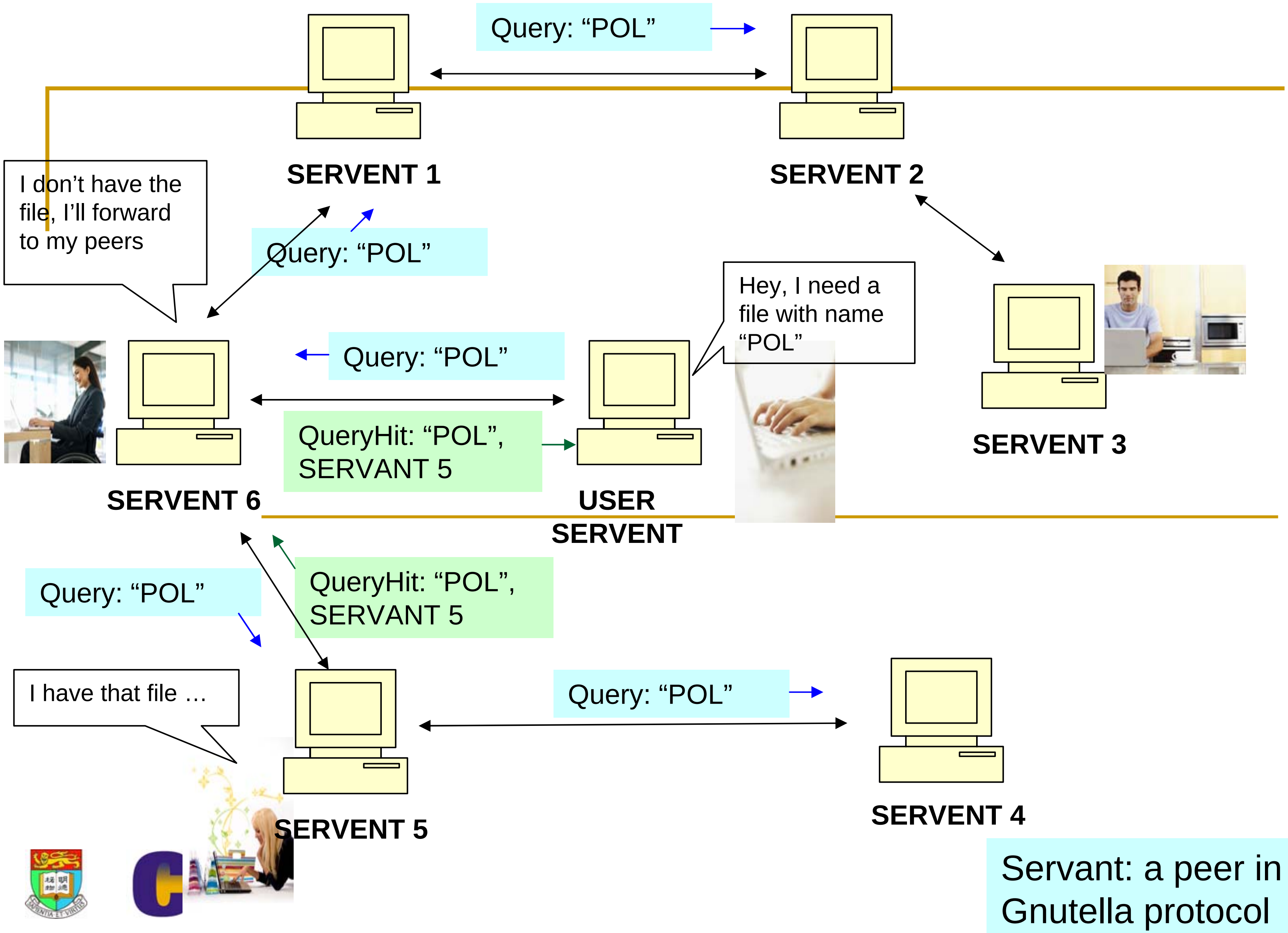
59.39.71.220
59.39.71.217
59.39.71.219

(3)
USER sends a
PING request to
each peer

(4)
The peer
returns a
PONG request
to the USER

(5)
USER now part
of the Foxy
network

Searching Files on the Foxy network



Query: “POL”

SERVENT 1

SERVENT 2

I don’t have the file, I’ll forward to my peers

Query: “POL”

Hey, I need a file with name “POL”

SERVENT 3

Query: “POL”

QueryHit: “POL”, SERVANT 5

SERVENT 6

USER SERVENT

Query: “POL”

QueryHit: “POL”, SERVANT 5

I have that file …

Query: “POL”

SERVENT 5

SERVENT 4

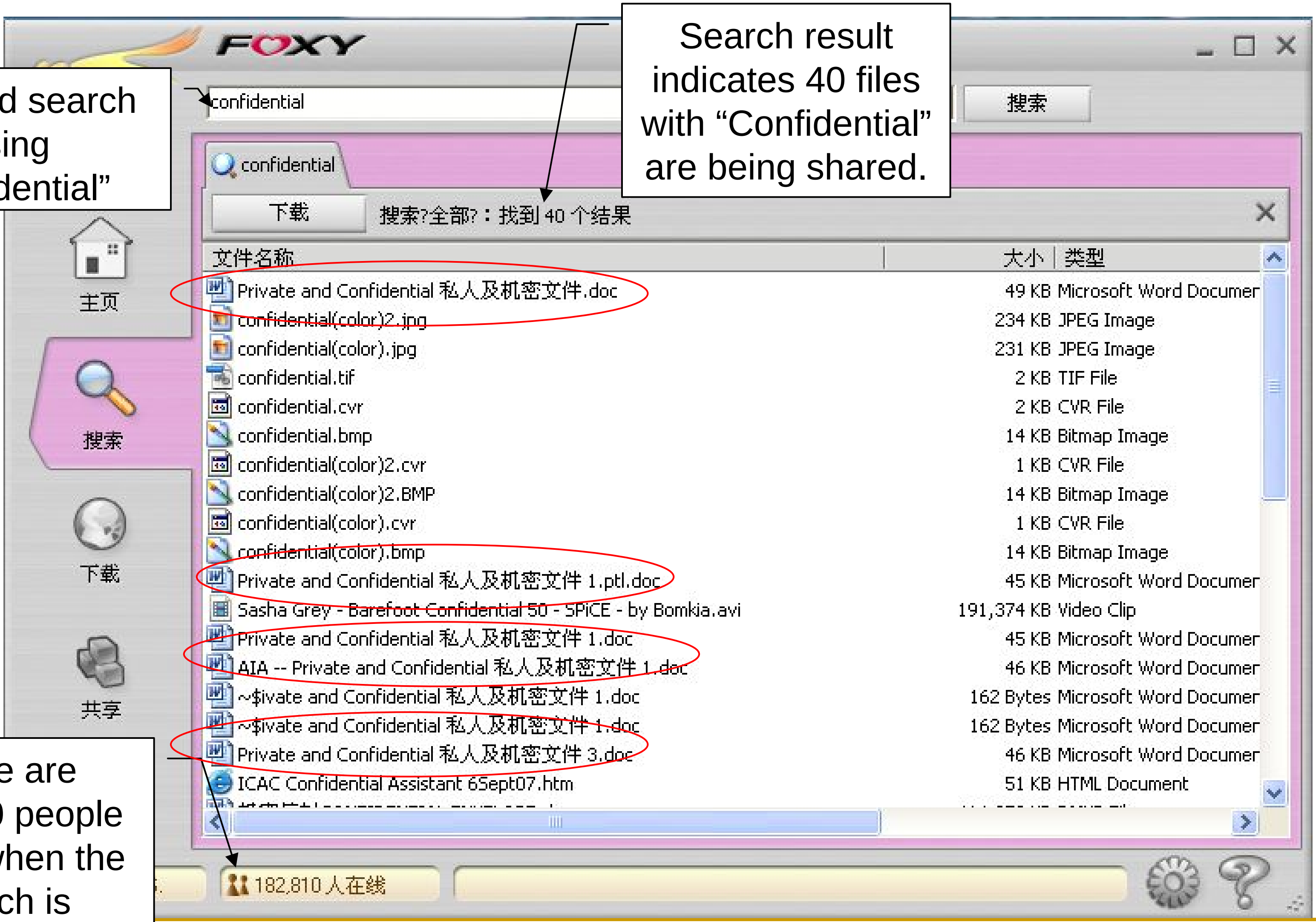
Servant: a peer in the Gnutella protocol

Do a sample keyword search

Keyword search using "confidential"

Search result indicates 40 files with "Confidential" are being shared.

There are 182,810 people online when the search is performed.



confidential

confidential

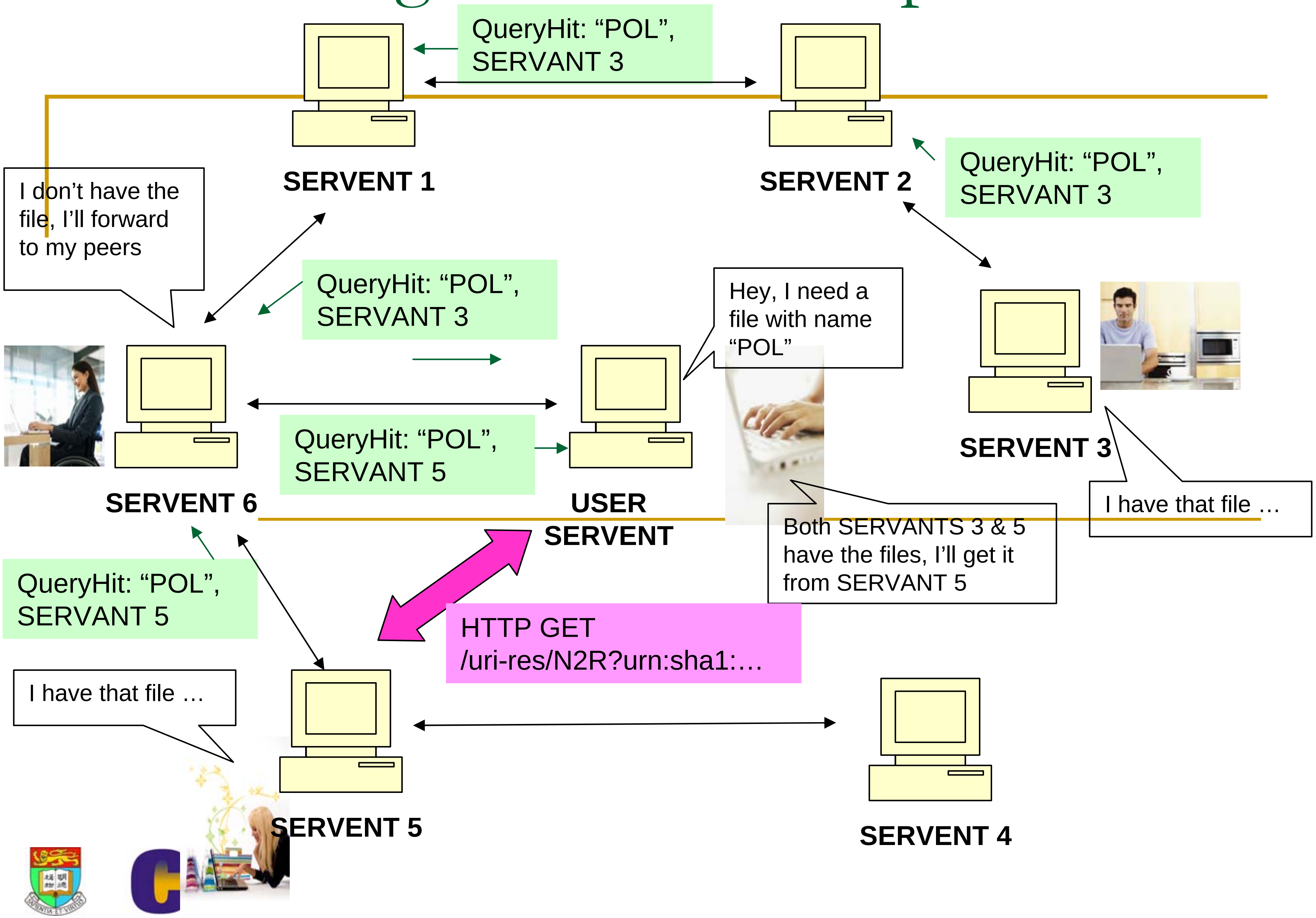
下載

搜索?全部?：找到 40 个结果

文件名称	大小	类型
Private and Confidential 私人及机密文件.doc	49 KB	Microsoft Word Documer
confidential(color)2.jpg	234 KB	JPEG Image
confidential(color).jpg	231 KB	JPEG Image
confidential.tif	2 KB	TIF File
confidential.cvr	2 KB	CVR File
confidential.bmp	14 KB	Bitmap Image
confidential(color)2.cvr	1 KB	CVR File
confidential(color)2.BMP	14 KB	Bitmap Image
confidential(color).cvr	1 KB	CVR File
confidential(color).bmp	14 KB	Bitmap Image
Private and Confidential 私人及机密文件 1.ptl.doc	45 KB	Microsoft Word Documer
Sasha Grey - Barefoot Confidential 50 - SPiCE - by Bomkia.avi	191,374 KB	Video Clip
Private and Confidential 私人及机密文件 1.doc	45 KB	Microsoft Word Documer
AIA -- Private and Confidential 私人及机密文件 1.doc	46 KB	Microsoft Word Documer
~$ivate and Confidential 私人及机密文件 1.doc	162 Bytes	Microsoft Word Documer
~$ivate and Confidential 私人及机密文件 1.doc	162 Bytes	Microsoft Word Documer
Private and Confidential 私人及机密文件 3.doc	46 KB	Microsoft Word Documer
ICAC Confidential Assistant 6Sept07.htm	51 KB	HTML Document

182,810 人在线

Downloading a file from the peer



QueryHit: “POL”, SERVANT 3

SERVENT 1

SERVENT 2

QueryHit: “POL”, SERVANT 3

I don’t have the file, I’ll forward to my peers

QueryHit: “POL”, SERVANT 3

Hey, I need a file with name “POL”

SERVENT 3

SERVENT 6

QueryHit: “POL”, SERVANT 5

USER SERVENT

Both SERVANTS 3 & 5 have the files, I’ll get it from SERVANT 5

I have that file …

QueryHit: “POL”, SERVANT 5

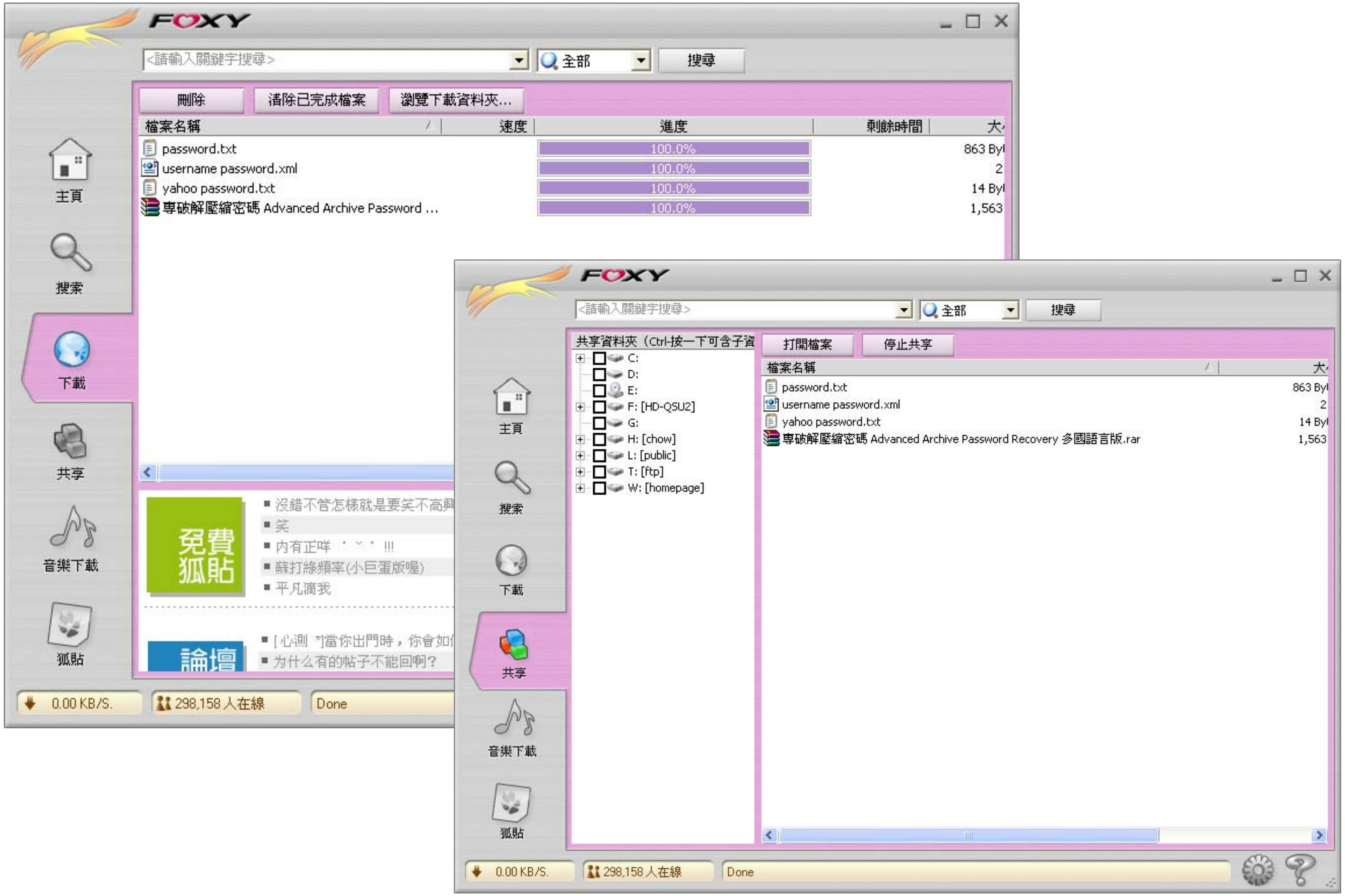
HTTP GET /uri-res/N2R?urn:sha1:…

I have that file …

SERVENT 5

SERVENT 4

Sample download



檔案名稱	速度	進度	剩餘時間	大
password.txt		100.0%		863 Byt
username password.xml		100.0%		2
yahoo password.txt		100.0%		14 Byt
專破解壓縮密碼 Advanced Archive Password ...		100.0%		1,563

- 沒錯不管怎樣就是要笑不高興
- 笑
- 內有正咩 ˙ˇ˙ !!!
- 蘇打綠頻率(小巨蛋版喔)
- 平凡滴我
- [心測 *]當你出門時，你會如何
- 为什么有的帖子不能回啊?

0.00 KB/S. 298,158 人在線 Done

共享資料夾（Ctrl-按一下可含子資

- C:
- D:
- E:
- F: [HD-QSU2]
- G:
- H: [chow]
- L: [public]
- T: [ftp]
- W: [homepage]

檔案名稱	大
password.txt	863 Byt
username password.xml	2
yahoo password.txt	14 Byt
專破解壓縮密碼 Advanced Archive Password Recovery 多國語言版.rar	1,563

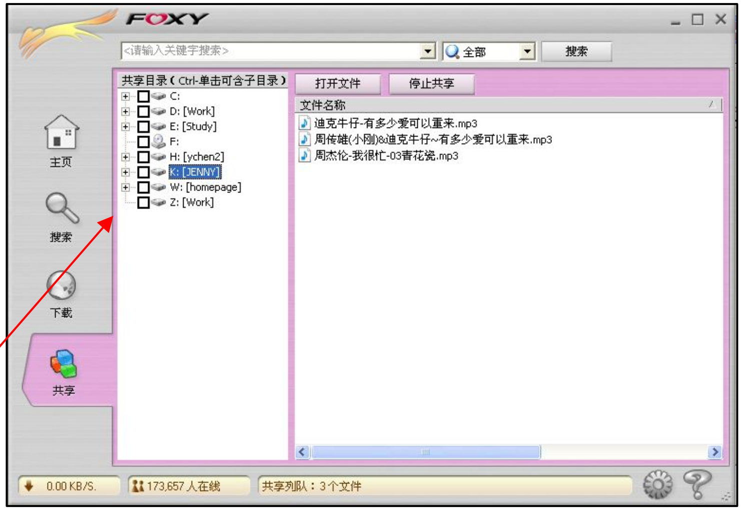
0.00 KB/S. 298,158 人在線 Done

Some Foxy Features

- Default installation starts Foxy automatically after user login

- Foxy allows upload/download of files using the “shared” folder
  - Default “shared” folder is “\Program Files\Foxy\Download”
  - Any other folder can be shared

- Foxy “shared” folder”:
  - All files in the “shared” folder(s) are shared with all other peers in the Foxy network
  - Once the initial setting has been set, all subsequent uses will use this setting as basis

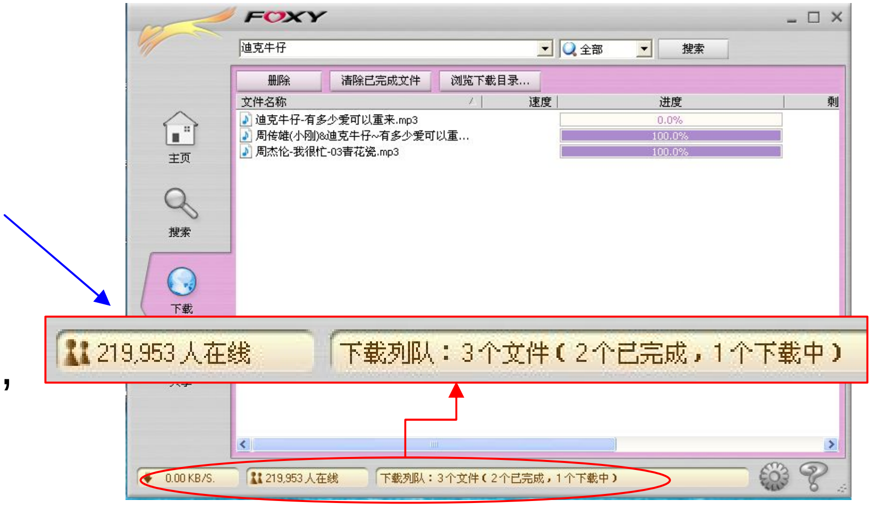


共享目录（Ctrl-单击可含子目录）

- C:
- D: [Work]
- E: [Study]
- F:
- H: [ychen2]
- K: [JENNY]
- W: [homepage]
- Z: [Work]

迪克牛仔-有多少爱可以重来.mp3
周传雄(小刚)&迪克牛仔~有多少爱可以重来.mp3
周杰伦-我很忙-03青花瓷.mp3

0.00 KB/S.　173,657 人在线　共享列队：3个文件



文件名称	速度	进度	剩
迪克牛仔-有多少爱可以重来.mp3		0.0%	
周传雄(小刚)&迪克牛仔~有多少爱可以重...		100.0%	
周杰伦-我很忙-03青花瓷.mp3		100.0%	

219,953 人在线　下载列队：3个文件（2个已完成，1个下载中）

0.00 KB/S.　219,953 人在线　下载列队：3个文件（2个已完成，1个下载中）

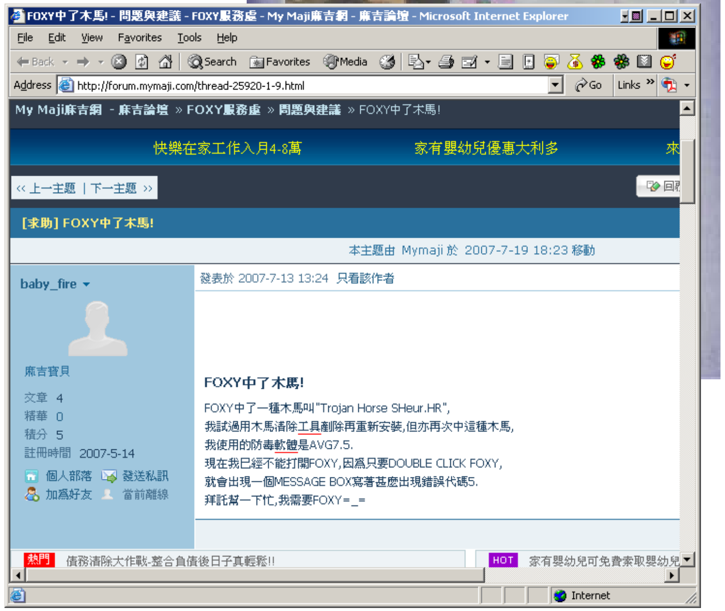
Foxy Security Analysis

Speculations on Foxy Security

- User mistake: user copies confidential documents to the shared folder
- Misconfigured file sharing: user shares a folder that contains confidential documents
- Foxy security vulnerabilities due to program bugs
- Hackers insert backdoor (mark “C:” as shared folder) into Foxy and then distribute the hacked version
- Misconfigured file sharing inherited from previous users

FOXY「分享」檔案測試

1 當有FOXY的電腦用者插入USB後，直接將有關資料透過FOXY分享：


FOXY中了木馬! - 問題與建議 - FOXY服務處 - My Maji麻吉網 - 麻吉論壇 - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address
Go Links
Internet

http://forum.mymaji.com/thread-25920-1-9.html

My Maji麻吉網 - 麻吉論壇 » FOXY服務處 » 問題與建議 » FOXY中了木馬!

快樂在家工作入月4-8萬　家有嬰幼兒優惠大利多

<< 上一主題 | 下一主題 >>

[求助] FOXY中了木馬!

本主題由 Mymaji 於 2007-7-19 18:23 移動

baby_fire

麻吉寶貝

文章 4
精華 0
積分 5
註冊時間 2007-5-14

個人部落　發送私訊
加爲好友　當前離線

發表於 2007-7-13 13:24　只看該作者

FOXY中了木馬!

FOXY中了一種木馬叫"Trojan Horse SHeur.HR",
我試過用木馬清除工具刪除再重新安裝,但亦再次中這種木馬,
我使用的防毒軟體是AVG7.5.
現在我已經不能打開FOXY,因爲只要DOUBLE CLICK FOXY,
就會出現一個MESSAGE BOX寫著甚麼出現錯誤代碼5.
拜託幫一下忙,我需要FOXY=_=

熱門 債務清除大作戰-整合負債後日子真輕鬆!!　HOT 家有嬰幼兒可免費索取嬰幼兒

Foxy Security Assessment

User mistake: user copies confidential documents to the shared folder	Very unlikely since so many incidents
Misconfigured file sharing: user shares a folder that contains confidential documents	Possible but unlikely
Foxy security vulnerabilities due to program bugs	Foxy Media officially denied
Hackers insert backdoor (mark “C:” as shared folder) into Foxy and then distribute the hacked version	Possible, need to find such hacked version (poisoned default configuration)
Misconfigured file sharing inherited from previous users	Likely if no other reason can be found (inherited configuration)

Should I remove Foxy?

- Naïve approach: YES
- Our team’s approach:
  - Identify the cause of the problem
  - Find the root of the problem
  - Fix the root of the problem

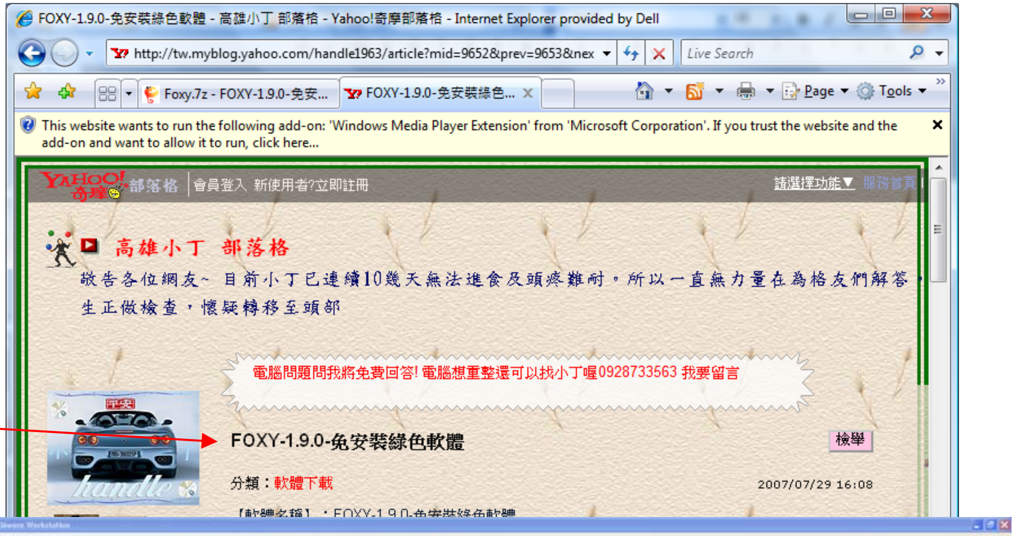
Otherwise, after remove Foxy, some “Yxof” will appear

What is the cause of the problem?

Foxy 綠色版

- Foxy 綠色版: no installation is required
- The distribution of Foxy 綠色版 may consists of default configurations in directory “Conf”
  - ❑ Settings.cfg
  - ❑ Foxy.cfg
  - ❑ Servers.cfg
  - ❑ …

- ❑ Settings.cfg stores the last “shared folders list”
- ❑ What will happen if Settings.cfg is poisoned?



FOXY-1.9.0-免安裝綠色軟體 - 高雄小丁 部落格 - Yahoo!奇摩部落格 - Internet Explorer provided by Dell

http://tw.myblog.yahoo.com/handle1963/article?mid=9652&prev=9653&nex

This website wants to run the following add-on: 'Windows Media Player Extension' from 'Microsoft Corporation'. If you trust the website and the add-on and want to allow it to run, click here...

高雄小丁 部落格

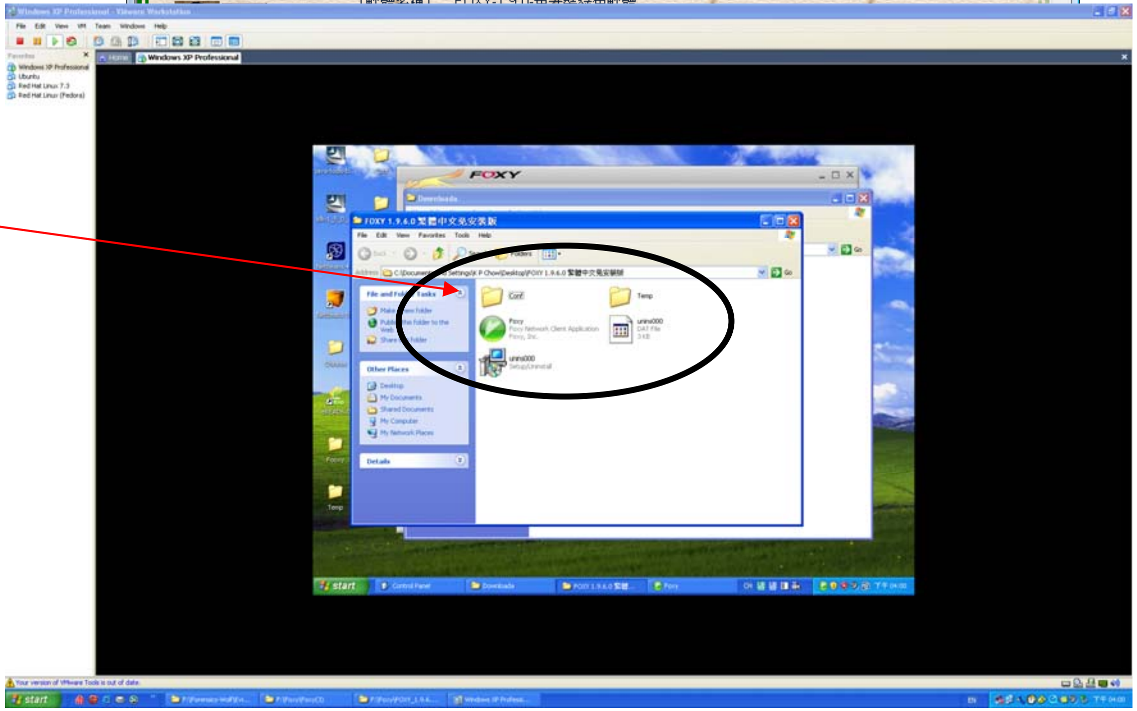
敬告各位網友~ 目前小丁已連續10幾天無法進食及頭疼難耐。所以一直無力量在為格友們解答，生正做檢查，懷疑轉移至頭部

電腦問題問我將免費回答! 電腦想重整還可以找小丁喔0928733563 我要留言

FOXY-1.9.0-免安裝綠色軟體

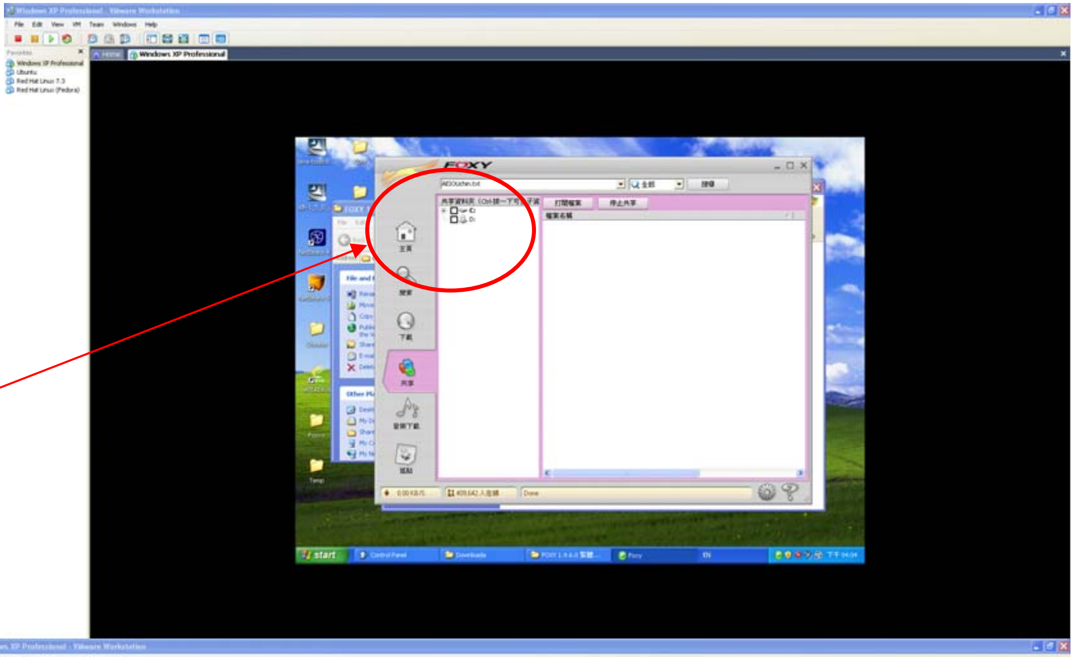
分類：軟體下載

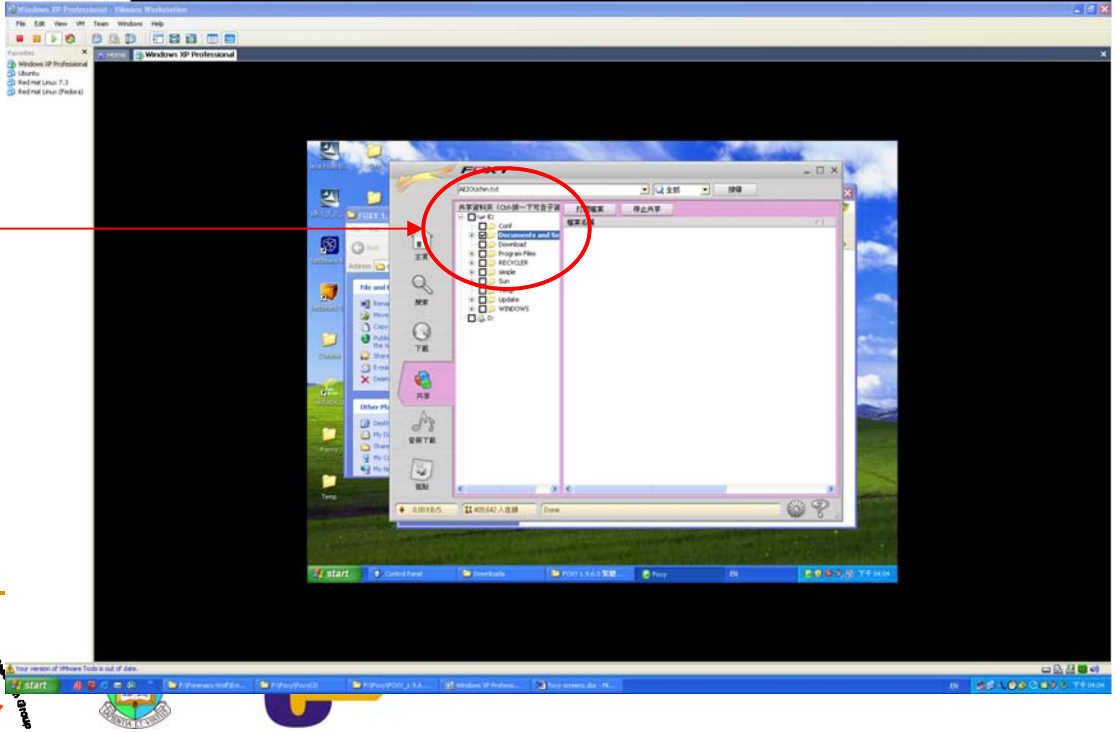
2007/07/29 16:08



Poisoned Default Configuration

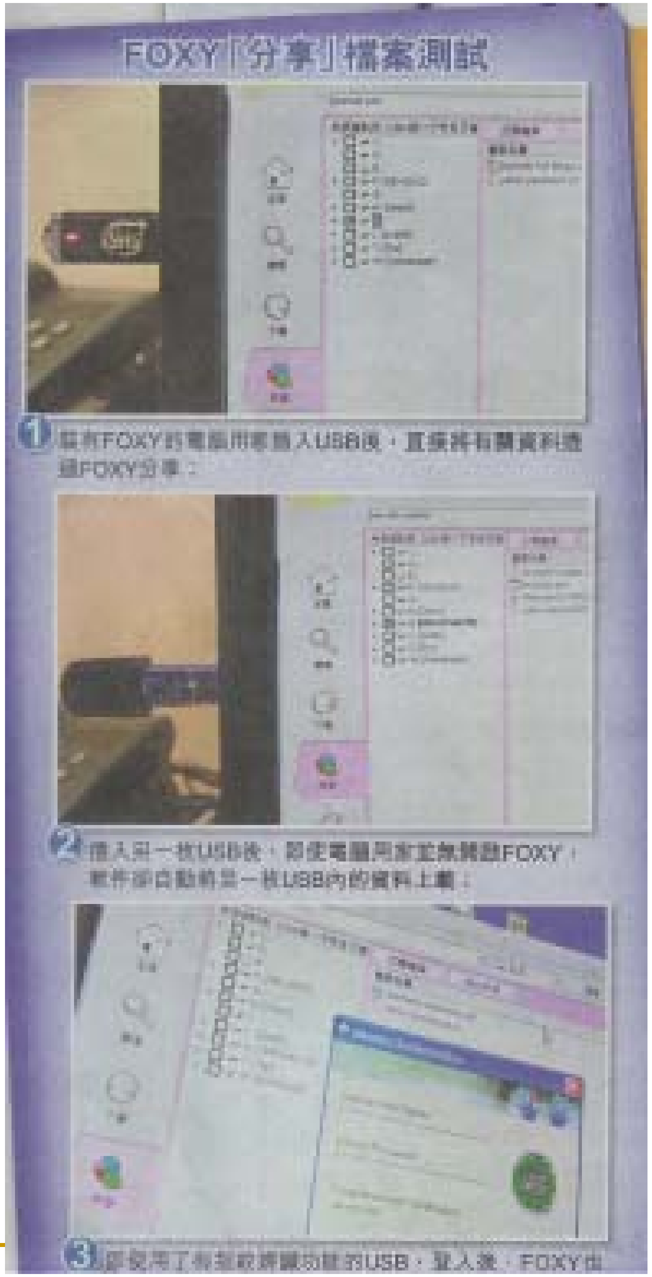
1. In another PC with Foxy running, I set the "C:\Documents and Settings" to be shared
2. I then copy the Settings.cfg into the Conf directory of the Foxy 綠色版
3. When I start the Foxy 綠色版, the C: is not shared, while the "C:\Documents and Settings" is shared
4. Anyone downloads the Foxy 綠色版 together with the configuration Conf\Settings.cfg will have "C:\Documents and Settings" is shared





Inherited Misconfigured File Sharing Setting

- Consider the scenario that a home PC is shared by the *kid* and the *father*
  - The *kid* shares a song in his USB thumbdrive “F:” to his classmates
  - The *father* then uses the PC with the Foxy is running with he shared folder “F:”
  - The *father* inserts his USB thumbdrive which contains confidential documents, also labeled “F:”
  - All documents in “F:” are now shared
  - Foxy 天王 is able to find *father*’s confidential documents



FOXY「分享」檔案測試

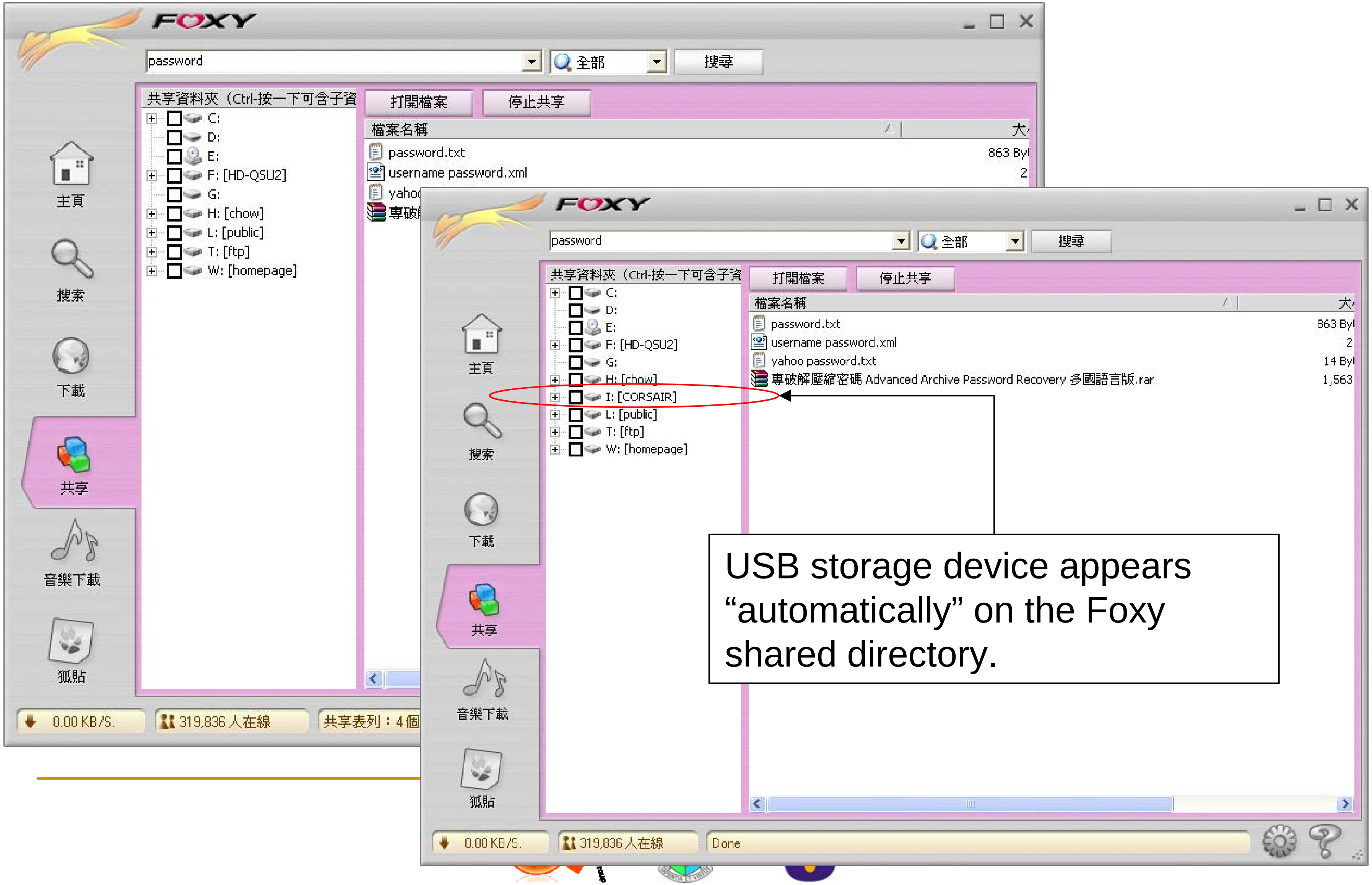
1 當有FOXY的電腦用家插入USB後，直接將有關資料透過FOXY分享；

2 插入另一枚USB後，即使電腦用家並無開啟FOXY，軟件卻自動將另一枚USB內的資料上載；

3 即使用了有加密保護功能的USB，登入後，FOXY仍

From Hongkong Economic Times (13 May 2008)

Files can be shared when plug in a USB storage device



C:
D:
E:
F: [HD-QSU2]
G:
H: [chow]
L: [public]
T: [ftp]
W: [homepage]

password.txt 863 Byl
username password.xml 2
yaho
專破

0.00 KB/S. 319,836 人在線 共享表列：4 個

C:
D:
E:
F: [HD-QSU2]
G:
H: [chow]
I: [CORSAIR]
L: [public]
T: [ftp]
W: [homepage]

password.txt 863 Byl
username password.xml 2
yahoo password.txt 14 Byl
專破解壓縮密碼 Advanced Archive Password Recovery 多國語言版.rar 1,563

0.00 KB/S. 319,836 人在線 Done

USB storage device appears “automatically” on the Foxy shared directory.

What is the root of the problem?

- Microsoft Windows?
- Foxy?

- 2 fundamental principles of computer security are violated:
  - Principle of least privilege
  - Principle of compartmentalization

Any simple fixes?

- Microsoft Windows XP and Vista
  - Separate user accounts for different users
  - No user account should have administrator right (except user *administrator*)
  - User “son” running Foxy is unable to share documents in user “father”

- Foxy is now running with user “son” privilege
- Documents in user “father” and user “son” are in different compartments
- Other P2P file sharing tools with similar features are **unable** to share confidential files accidentally

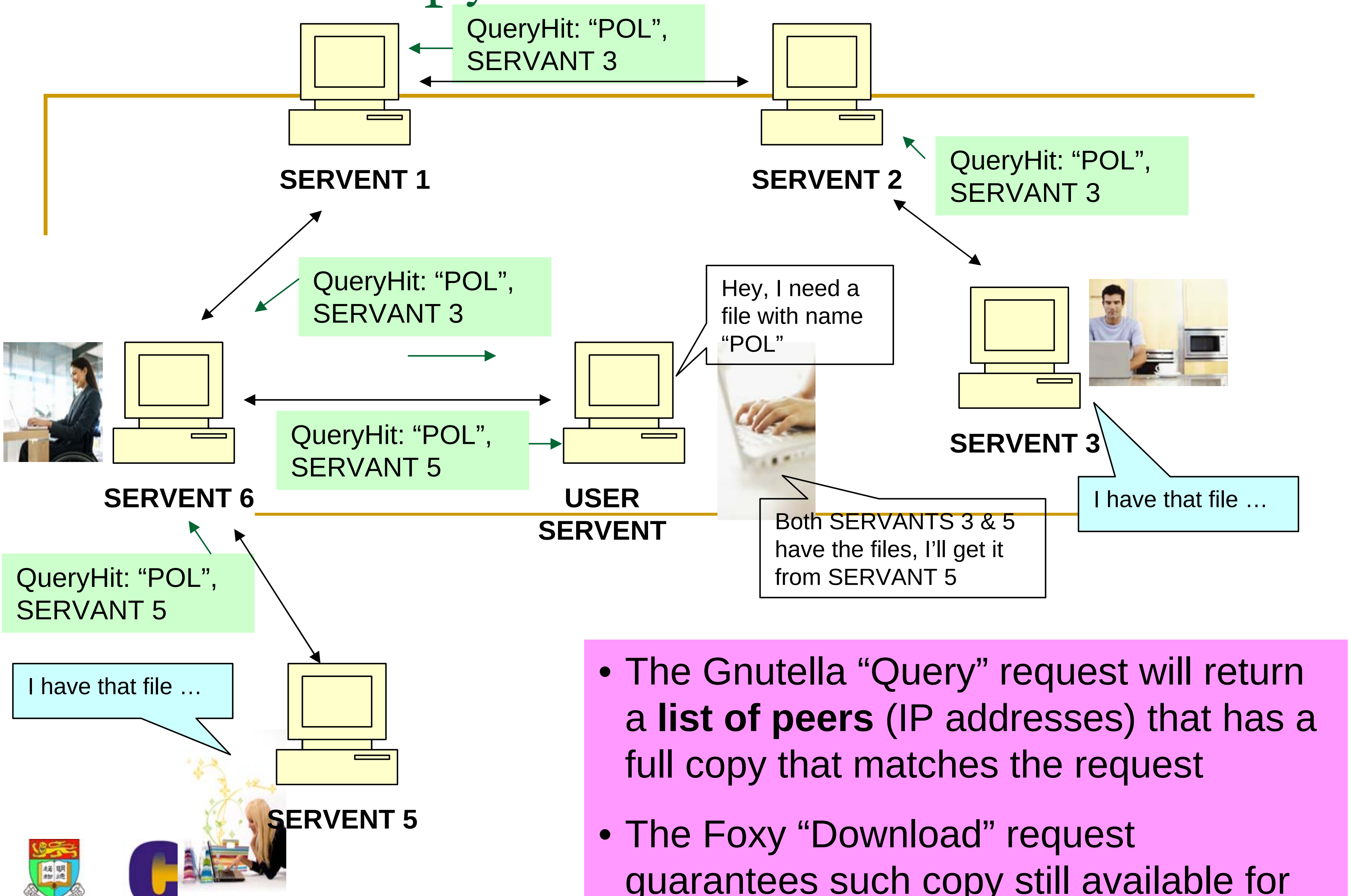
Some advices

- Your home PC:
  - Separate user accounts for different users
  - Download Foxy from the official web site www.gofoxy.net
  - When using Foxy, limit the shared folder to the default, and check the default setting
- USB storage device:
  - Do not plug-in your USB storage device to any *untrusted* PC
  - If it is absolutely necessary, before plug-in the USB storage device, make sure no Foxy or other malicious software is running
- The best protection: encrypt the confidential information and decrypt it only when necessary

Tracing on the Foxy network

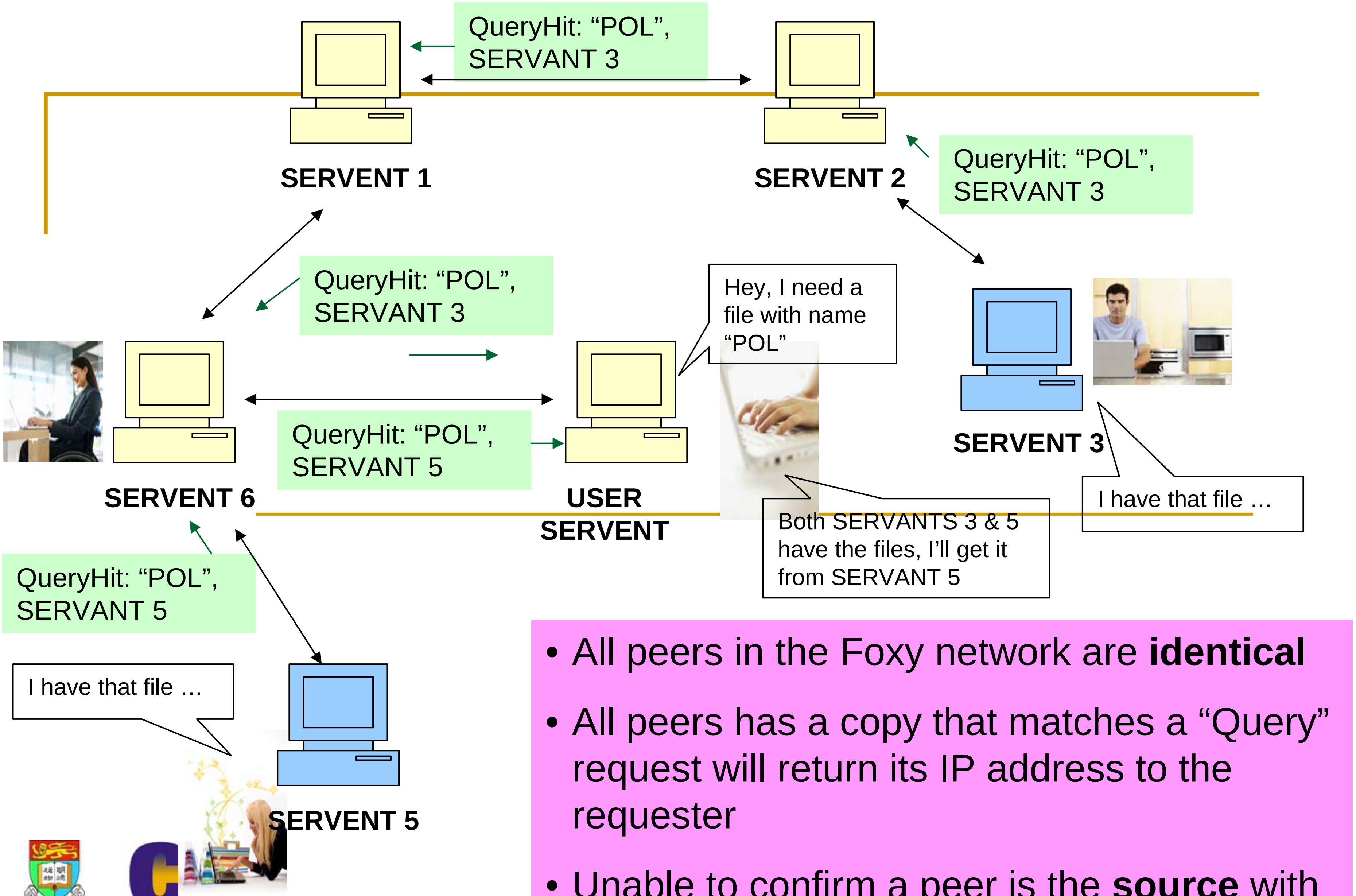
- Is it possible to trace who shares a copy of a document?
- Is it possible to trace the *seeder* of a document
- Once a document is available on Foxy, can it be *removed*?

Who has a copy?


QueryHit: "POL", SERVANT 3
SERVENT 1
SERVENT 2
QueryHit: "POL", SERVANT 3
QueryHit: "POL", SERVANT 3
Hey, I need a file with name "POL"
SERVENT 3
SERVENT 6
QueryHit: "POL", SERVANT 5
USER SERVENT
Both SERVANTS 3 & 5 have the files, I'll get it from SERVANT 5
I have that file …
QueryHit: "POL", SERVANT 5
I have that file …
SERVENT 5

- The Gnutella "Query" request will return a **list of peers** (IP addresses) that has a full copy that matches the request
- The Foxy "Download" request guarantees such copy still available for download

Who is the source?


QueryHit: "POL", SERVANT 3
SERVENT 1
SERVENT 2
QueryHit: "POL", SERVANT 3
QueryHit: "POL", SERVANT 3
Hey, I need a file with name "POL"
SERVENT 3
I have that file …
SERVENT 6
QueryHit: "POL", SERVANT 5
USER SERVENT
Both SERVANTS 3 & 5 have the files, I'll get it from SERVANT 5
QueryHit: "POL", SERVANT 5
I have that file …
SERVENT 5

- All peers in the Foxy network are **identical**
- All peers has a copy that matches a "Query" request will return its IP address to the requester
- Unable to confirm a peer is the **source** with information in the Foxy network

Can a document be removed from the Foxy network by the seeder?

- In Google, function available to remove a document from Google's database and cache (in the IPCC case)
- Does similar function available in Foxy? **NO**
    - Once a document starts sharing and propagating in the Foxy network, it is impossible to recall the document nor stop the propagation
    - How about share a different document with identical name?
        - Both the new and the old files exist in the Foxy network

Conclusion

- Foxy
  - The good: very easy to use P2P software
  - The bad: able to share any files without leaving a "trace"
  - The ugly: accidentally share folders to all peers

- My opinion
  - Good technology should be promoted
  - More user education

Reference

- K.P. Chow, R. Ieong, M. Kwan, P. Lai, F. Law, H. Tse, K. Tse, Security Analysis of the Foxy Peer-to-Peer File Sharing Tool
- http://i.cs.hku.hk/~cisc/forensics/papers/Foxy.pdf

Q & A