

# Data Seepage

Robert Graham – Founder & CEO

David Maynor – Founder & CTO





## What is Data Seepage?

- Don't Confuse it with Data Leakage.
- Data Leakage is when information you care about is accidentally revealed.
  - This can be due to programming errors, improper handling of sensitive information, or malicious internal threats.

 **NEWS.com**

Search:

[Today on CNET](#)

[Reviews](#)

[News](#)

[Downloads](#)

[Tips & Tricks](#)

[CNET TV](#)

[Today on News](#) | [Business Tech](#) | [Cutting Edge](#) | [Access](#) | [Threats](#) | [Media 2.0](#)

### Google plugs Gmail data leak flaw

By Joris Evers  
Staff Writer, CNET News.com

 **NEWS.com**

Search:

[Today on CNET](#)

[Reviews](#)

[News](#)

[Downloads](#)

[Tips & Tricks](#)

[Today on News](#) | [Business Tech](#) | [Cutting Edge](#) | [Access](#) | [Threats](#)

### Veterans' data swiped in the f

By Greg Sandoval  
Staff Writer, CNET News.com

## What is Data Seepage?

- What is Data Seepage then?
  - Information that is broadcast or available via simple inquiry or spoofing that may not by itself seem critical but become more important as pieces of a larger puzzle.





## What is Data Seepage?

- Think about what your laptop does when it starts up.
  - Programs set to autostart
  - Looking for certain resources like intranet homepage and shared drives
  - Email clients
  - Instant messaging clients



## EEFI

- The military is well aware of this.
- A military intelligence term meaning “essential elements of friendly information”
  - **Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness.**
  - **<http://usmilitary.about.com/od/glossarytermse/g/eefi.htm>**

## EEFI: Example



Him: When can I see you again?

Her: How about next week? My boss, the director of the NSA has a trip he is going on he can't even tell me about. It makes me so mad, how am I suppose to help coordinate things if I don't even know where he is going. He did ask me to buy a lot of suntan lotion though...

Him: Excuse me, I have to make a phone call.....to my sister...about...trees.

Her: Ok hurry back, I am going to order another drink.



Him: The director of the NSA is going somewhere that requires a lot of suntan lotion.

Terrorist: We have gotten word that a major US Intelligence officer will be visiting Baghdad soon. Director of NSA == US Intelligence officer, therefore I deduce that the Director of the NSA will be visiting Iraq next week.

Him: Why did you say "equal equal" outloud? lol

Terrorist: It makes me seem creepier.





## EEFI doesn't apply to you?

- Think of things the movements of your CEO, sales staff, or even engineers can tell a diligent observer about your business.
  - Repeated trips to a competitors headquarters?
  - Sales guys cancelling dates near end of month or end of quarter.
  - Engineers cars in parking lots as a ship date comes and goes.





Him: When can I see you again?

Her: How about next week? My boss, the CEO, is out all next week on some sort of secret trip. Its his third time going to Redmond this month and he hasn't even brought me a present, but I have to be on call at all hours to coordinate a conference call with all the C level execs.

Him: Excuse me, I have to make a phone call.....to my brother...about...a playdate for our dogs...

Her: That's so sweet, Hurry back, I am ordering more drinks.



Him: Hey, something's up with XYZsoft.

Stock Broker: My friend on a project at Microsoft just got reassigned to a different project. He sad the would solve the problem a different way. Microsoft must be buying XYZsoft.

Him: Has anyone told you that for a stock broker you sure look like a terrorist?

Stock Broker: I use to be, taking advantage of your capitalist systems pays better though.

Him: I am strangely comfortable with that.





## More EEFI examples

- The Pentagon ordering a lot of delivery food.
- Warehouses of business shipping items like crazy as end of quarter approaches.
- A small company placing an order for 50 new workstations or placing an order to for more VoIP quality circuits to locations they where they don't have offices.



## Data Seepage...

- So how does this apply to computers?
- You laptop, PDA, even mobile phone will give up information that may not seem important but combined with other info can paint a picture for malicious intruders.



## Data seeps via the network...

- Wifi packets
- DHCP Broadcast
- NetBIOS/SMB Broadcast
- DNS/Bonjour Requests



## Wifi Packets

- Probe Requests
  - <http://www.theta44.org/software/karma.README>
  - <http://www.nmrc.org/pub/advise/20060114.txt>
  - When a wifi enabled laptop starts up it will look for a list of “known networks” or networks it has connected to before.
  - This list can be used to determine where the laptop has been used.



## DHCP ++

- You can offer up an address and pretend to be what ever server you are looking for.
- Look at the Karma project.
  - Respond to WiFi “probe”
  - Respond with DHCP address
  - Respond to ARPs
  - Respond to NetBIOS queries
  - Respond to SMB/DCE-RPC connections
  - Respond to DNS queries
  - Respond to SMTP connections



## NetBIOS/SMB Broadcast

- WKSSVC announcements
- AD activity
- Attempting to connect to shared drives
- Printers





## DNS Requests

- Almost all internet activity requires a DNS lookup
  - **Connecting to intranet sites**
  - **Connecting to mail servers**
  - **Almost any other application starting up**
    - IM apps
    - VoIP apps
    - Games (yes even poker games)



## Other Protocols

- Bonjour
  - Very chatty about who you are
- Skype
  - It always finds a way
- Security tools
  - They are always update hungry
- OS
  - They love the updates as well
- AIM will update you to all you buddies status.
  - This tells an eavesdropper who is on your buddy list.



## What does all this mean?

- Lets look at the information that can be gathered:
  - A machine with the Mac Address of 00-18-f3-57-24BD belongs to John Smith.
  - This laptop has connected to wifi access point at Hartsfield airport, Heathrow, SeaTac, and various T-Mobile spots, and ABCsoft and XYZsoft.
  - John has the AIM name “PrschDude9” and has XYZsoft1 on his buddy list.
  - He uses a popclient to check his personal email and his passwd is porsche911turbo.
  - John works for ABCsoft because his browsers attempts to go to [internal.abcsoft.com](http://internal.abcsoft.com) when it first starts up.
  - It also attempts to connect to [\\internal.abcsoft.com\sales](http://internal.abcsoft.com/sales) and [\\internal.abcsoft.com\public](http://internal.abcsoft.com/public) on start up.
  - He has a myspace account where he had pics of the last company party.



## Applying information

- So what can you determine about this if you know ABCsoft and XYZsoft are bitter rivals?
  - **Sounds like a merger or buyout.**
- Since you know Johns pop password you can try it against ABCsoft's webmail client, he might use the same password.
- Social Engineering – “Hey wasn't that a horrible shirt John was wearing at the last company party...run this program to update your accounting software.”
- You know portions of the internal layout of the ABCsoft intranet.
  - **Make trojans and client side exploits more efficient because you have a target to attack.**



# THEORY- CRAFT



## Process of collecting seaped information

- Identity
  - **Tell me everything knowable about the subject**
- Opportunity
  - **What can I do with the subject**
- Baconizing
  - **Create a graph of who contacts whom**
    - Which servers they connect to
    - Who they have in their buddy lists
    - Who they send e-mail to



# WEBSITES

Google - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.google.com/ Go

Wizz RSS 2.1.7 Feed Search Help etc. Options etc. Watch List

**blackhat.test@gmail.com** | [Personalize this page](#) | [My Account](#) | [Sign out](#)

# Google™

Web [Images](#) [Video](#) [News](#) [Maps](#) [more »](#)

Google Search I'm Feeling Lucky

[Advanced Search](#)  
[Preferences](#)  
[Language Tools](#)

[Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2007 Google

Done 0.172s S Adblock



errata  
security

The Worldwide Leader In Sports - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://espn.go.com/

RSS 2.1.7 Feed Search Help etc. Options etc. Watch List Weather

MyESPN Member Services

Welcome, Blackhat | [Sign Out](#)

OFFICIAL SMALL BUSINESS OF  
**NASCAR**  
Courtesy of Office DEPOT

Your company logo could go here

ESPNews  
Search

ESPN.com's Hottest Searches:  
[Bracketology](#) | [Drive to 65](#) | [Power 16](#) |  
[Sports Guy](#) | [Dickie V](#) | [NHL rankings](#)



LINKS FROM: SPORTSCENTER

- Katz: Buckeyes arrive at title right on schedule
- Blount: Martin has to reconsider his schedule
- Stark: Veteran Braves long for October return

ON ESPN Full TV Schedule

SportsCenter

9 p.m. ET: College Hoops  
Florida at Tennessee

Insider ESPN360 Page 2 SportsNation Blogs Video PodCenter Video Games Travel Contests Shop En Español  
Fantasy NFL NBA MLB NHL ESPNU College FB Men's BB Women's BB NASCAR Autos Golf Soccer Tennis Boxing Olympics More +

LIVE SCORING. NOW FREE. SIGN UP FREE

Super Freak

Access to MLB Rumor Central and predictive analysis. All the tools you need to stay ahead! Sign Up Now

Insider | One Step Ahead of the Game

NBA 6 of 10

Find Next Find Previous Highlight all Match case Phrase not found

Make My Yahoo! your home page

**MY YAHOO!** Welcome, **robert\_david\_graham**  
 [ Sign Out ] [ My Account ]

Yahoo! Mail More Yahoo!

**Vanguard**  
 Obtain prospectus.  
 All investments are subject to risk. Vanguard Marketing Corp., Distributor. © 2006 The Vanguard Group, Inc.

All our books share the same plot. Helping to make you a more successful investor.

**TARGET RETIREMENT FUNDS**

Category: **Web** | Images | Video | Local | News | Shopping

Search:

Thu, Mar 1, 01:01 am

[Bad credit? Need\\$? 4 of 5 approved!](#)

+ Add Content | ⇅ Change Layout | 🎨 Change Colors

Select Page:

Message Center

[Check Email](#)

[Launch Messenger](#)

**Welcome to the new My Yahoo!**

It's all about choice -- and giving you more of it. We just made it better. You'll now get the new, improved My Yahoo! We encourage you to explore what's new, edit your page, and indulge yourself. Click "Add Content" and discover lots of cool new stuff for your page.

[See everything that's new in My Yahoo!](#) | [Give us your feedback](#)

Calendar

◀ March 2007 ▶

Su	Mo	Tu	We	Th	Fr	Sa
25	26	27	28	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17

Comics

[Doonesbury](#)

NICE T.D. (MAY 10) YO. FINEMAN! (IDIOTS! DO LOOK AT THAT) (YOUR SURF



# PACKETS

# errata security

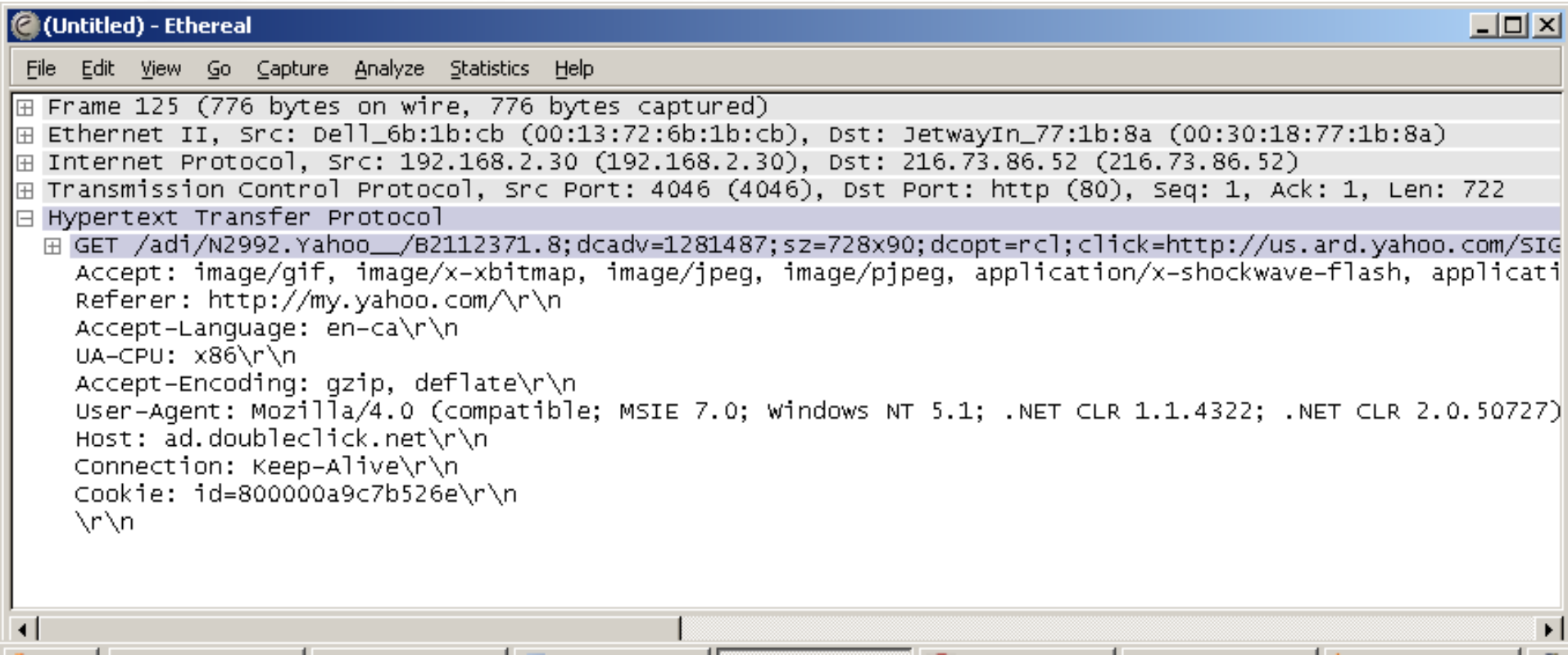
```

65 0.261450 69.94.196.132 224.0.0.251 MDNS Standard query response SRV 0 0 9 david-mayno...
0000 08 01 2c 00 00 15 c7 aa d5 30 00 17 f2 41 31 6d ..... .0...Alm
0010 01 00 5e 00 00 fb e0 06 aa aa 03 00 00 00 08 00 ..^.....
0020 45 18 01 dc 36 19 00 00 ff 11 99 01 45 5e c4 84 E...6... ..E^..
0030 e0 00 00 fb 14 e9 14 e9 01 c8 05 08 00 00 84 00 .....
0040 00 00 00 09 00 00 00 00 2d 44 61 76 69 64 20 4d ..... -David M
0050 61 79 6e 6f 72 e2 80 99 73 20 43 6f 6d 70 75 74 aynor... s Comput
0060 65 72 20 5b 30 30 3a 31 36 3a 63 62 3a 64 32 3a er [00:1 6:cb:d2:
0070 30 37 3a 61 61 5d 0c 5f 77 6f 72 6b 73 74 61 74 07:aa]._ workstat
0080 69 6f 6e 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00 ion._tcp .local..
0090 21 80 01 00 00 00 78 00 21 00 00 00 00 00 09 18 !.....x. !.....
00a0 64 61 76 69 64 2d 6d 61 79 6e 6f 72 73 2d 63 6f david-ma ynors-co
00b0 6d 70 75 74 65 72 2d 33 c0 4c c0 0c 00 10 80 01 mputer-3 .L.....
00c0 00 00 11 94 00 01 00 09 5f 73 65 72 76 69 63 65 ..... _service
00d0 73 07 5f 64 6e 73 2d 73 64 04 5f 75 64 70 c0 4c s._dns-s d._udp.L
00e0 00 0c 00 01 00 00 11 94 00 02 c0 3a c0 3a 00 0c ..... :...:..
00f0 00 01 00 00 11 94 00 02 c0 0c c0 63 00 1c 80 01 ..... C....
0100 00 00 00 78 00 10 fe 80 00 00 00 00 00 00 02 17 ...x....
0110 f2 ff fe 41 31 6d 01 44 01 36 01 31 01 33 01 31 ...Alm.D .6.1.3.1
0120 01 34 01 45 01 46 01 46 01 46 01 32 01 46 01 37 .4.E.F.F .F.2.F.7
0130 01 31 01 32 01 30 01 30 01 30 01 30 01 30 01 30 .1.2.0.0 .0.0.0.0
0140 01 30 01 30 01 30 01 30 01 30 01 30 01 30 01 30 .0.0.0.0 .0.0.0.0
0150 01 38 01 45 01 46 03 69 70 36 04 61 72 70 61 00 .8.E.F.i p6.arpa.
0160 00 0c 80 01 00 00 00 78 00 02 c0 63 c0 63 00 0d .....x ...C.C..
0170 80 01 00 00 00 78 00 50 0a 4d 61 63 42 6f 6f 6b .....x.P .MacBook
0180 31 2c 31 44 4d 61 63 20 4f 53 20 58 20 31 30 2e 1,1DMac OS X 10.
0190 34 2e 38 20 28 38 4c 32 31 32 37 29 2c 20 6d 44 4.8 (8L2 127), mD
01a0 4e 53 52 65 73 70 6f 6e 64 65 72 2d 31 30 38 2e NSRespon der-108.
01b0 32 20 28 41 75 67 20 32 35 20 32 30 30 36 20 31 2 (Aug 2 5 2006 1
01c0 34 3a 35 30 3a 34 38 29 c0 63 00 01 80 01 00 00 4:50:48) .c.....
01d0 00 78 00 04 45 5e c4 84 03 31 33 32 03 31 39 36 .x..E^.. .132.196
01e0 02 39 34 02 36 39 07 69 6e 2d 61 64 64 72 c1 1e .94.69.i n-addr..
01f0 00 0c 80 01 00 00 00 78 00 02 c0 63 .....x ...C

```



```
070213-gatech-balls-ch06a.pcap - Ethereal
File Edit View Go Capture Analyze Statistics Help
Frame 65 (508 bytes on wire, 508 bytes captured)
IEEE 802.11
Logical-Link Control
Internet Protocol, Src: 69.94.196.132 (69.94.196.132), Dst: 224.0.0.251 (224.0.0.251)
User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)
Domain Name System (response)
  Transaction ID: 0x0000
  Flags: 0x8400 (Standard query response, No error)
  Questions: 0
  Answer RRs: 9
  Authority RRs: 0
  Additional RRs: 0
Answers
  David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type SRV, class FLUSH, pr
  David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type TXT, class FLUSH
  _services._dns-sd._udp.local: type PTR, class IN, _workstation._tcp.local
  _workstation._tcp.local: type PTR, class IN, David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._work
  david-maynors-computer-3.local: type AAAA, class FLUSH, addr fe80::217:f2ff:fe41:316d
  D.6.1.3.1.4.E.F.F.2.F.7.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.ip6.arpa: type PTR, class FLUSH, david-ma
  david-maynors-computer-3.local: type HINFO, class FLUSH, CPU MacBook1,1, OS Mac OS X 10.4.8 (8L2127), mDN
  david-maynors-computer-3.local: type A, class FLUSH, addr 69.94.196.132
  132.196.94.69.in-addr.arpa: type PTR, class FLUSH, david-maynors-computer-3.local
```

A screenshot of the Ethereal network traffic capture application. The window title is '(Untitled) - Ethereal'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The main display area shows a list of captured packets. The selected packet is Frame 125 (776 bytes on wire, 776 bytes captured). The protocol stack is Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The Hypertext Transfer Protocol details are expanded, showing a GET request for an advertisement on Yahoo. The request includes headers for Accept, Referer, Accept-Language, UA-CPU, Accept-Encoding, User-Agent, Host, Connection, and Cookie.

```
(Untitled) - Ethereal
File Edit View Go Capture Analyze Statistics Help
[+] Frame 125 (776 bytes on wire, 776 bytes captured)
[+] Ethernet II, Src: Dell_6b:1b:cb (00:13:72:6b:1b:cb), Dst: JetwayIn_77:1b:8a (00:30:18:77:1b:8a)
[+] Internet Protocol, src: 192.168.2.30 (192.168.2.30), Dst: 216.73.86.52 (216.73.86.52)
[+] Transmission Control Protocol, Src Port: 4046 (4046), Dst Port: http (80), Seq: 1, Ack: 1, Len: 722
[+] Hypertext Transfer Protocol
    [+] GET /adi/N2992.Yahoo_/B2112371.8;dcadv=1281487;sz=728x90;dcopt=rc1;click=http://us.ard.yahoo.com/SIG
        Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/javascript, application/xaml+xml, application/vnd.ms-xsl+xml, application/xhtml+xml, application/xml;q=0.9, text/css;q=0.9, text/html;q=0.9
        Referer: http://my.yahoo.com/\r\n
        Accept-Language: en-ca\r\n
        UA-CPU: x86\r\n
        Accept-Encoding: gzip, deflate\r\n
        User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
        Host: ad.doubleclick.net\r\n
        Connection: Keep-Alive\r\n
        Cookie: id=800000a9c7b526e\r\n
        \r\n
```



# DEMOS

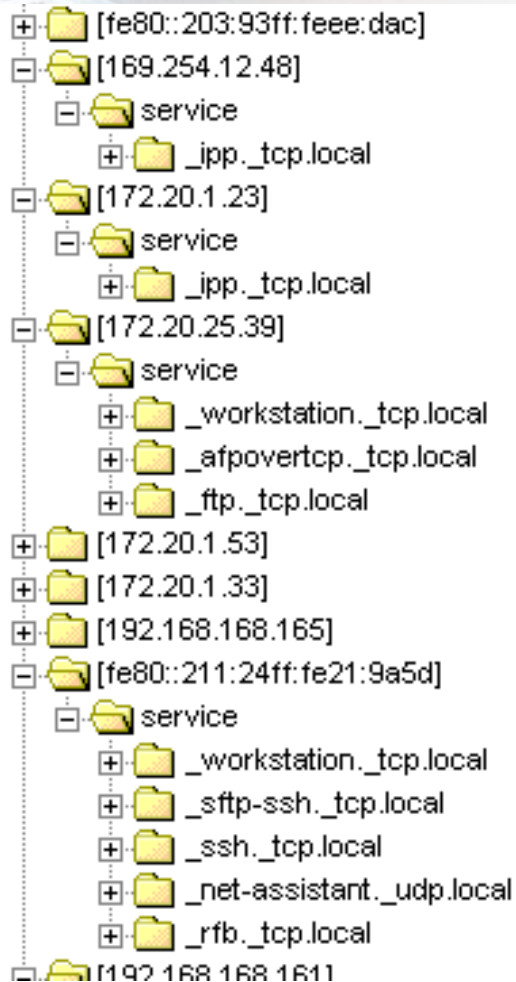


## FERRET – Data seepage monitor

- Like password sniffer, but sniffs more than just passwords
- Like intrusion-detection, but sniffs legitimate operations rather than intrusions
- Protocols: DHCP, SNMP, DNS, HTTP, AIM, MSN-MSGR, Yahoo IM, ...
- Ferret Viewer: allows you to browse the data easier



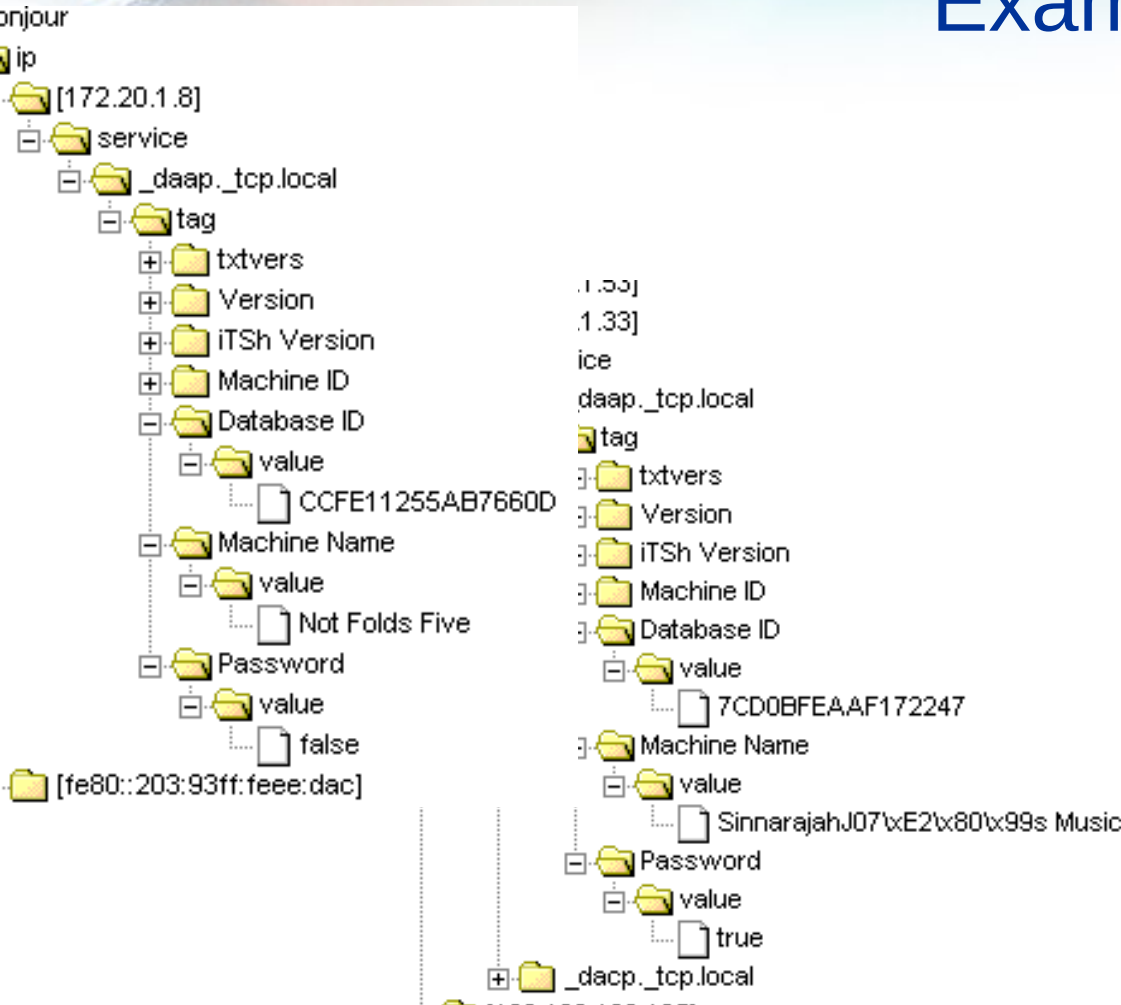
## Example: Bonjour



- Lists services on a machine
- Tells you which ones you can attack



## Example: iTunes server

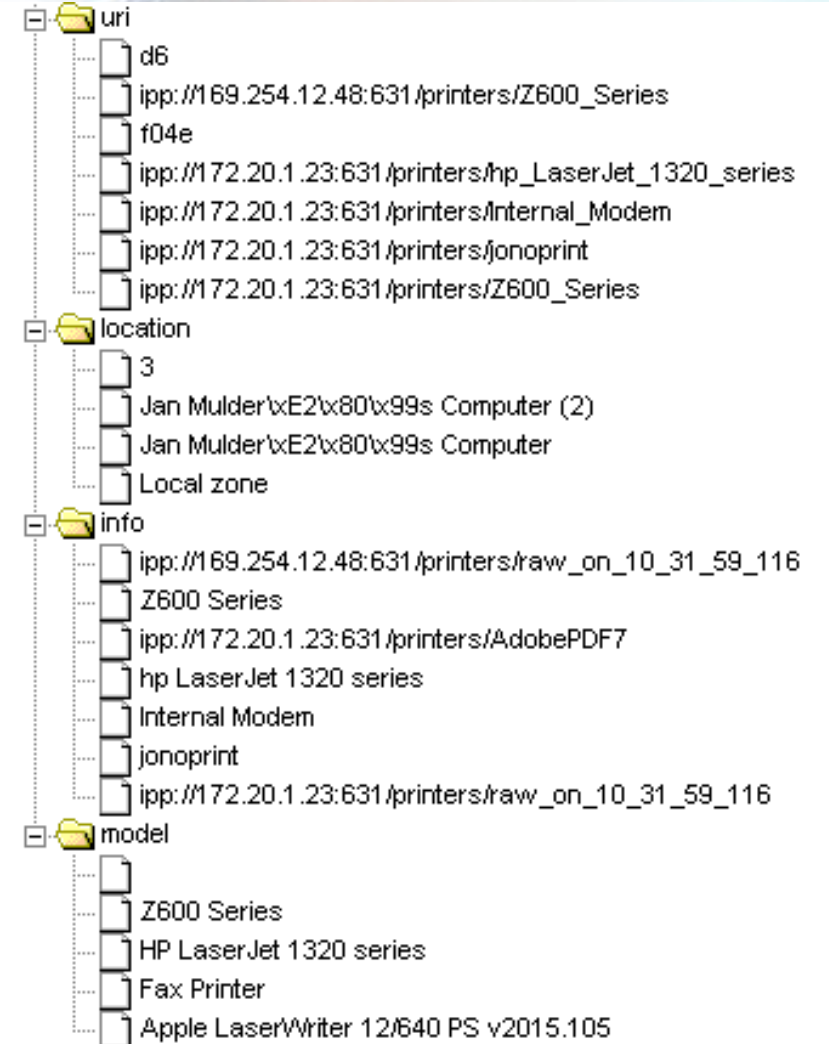


- iTunes uses Bonjour to advertise it's existence
- This tells you that you can connect to that iTunes server and download all the music with no password



## Example: CUPS

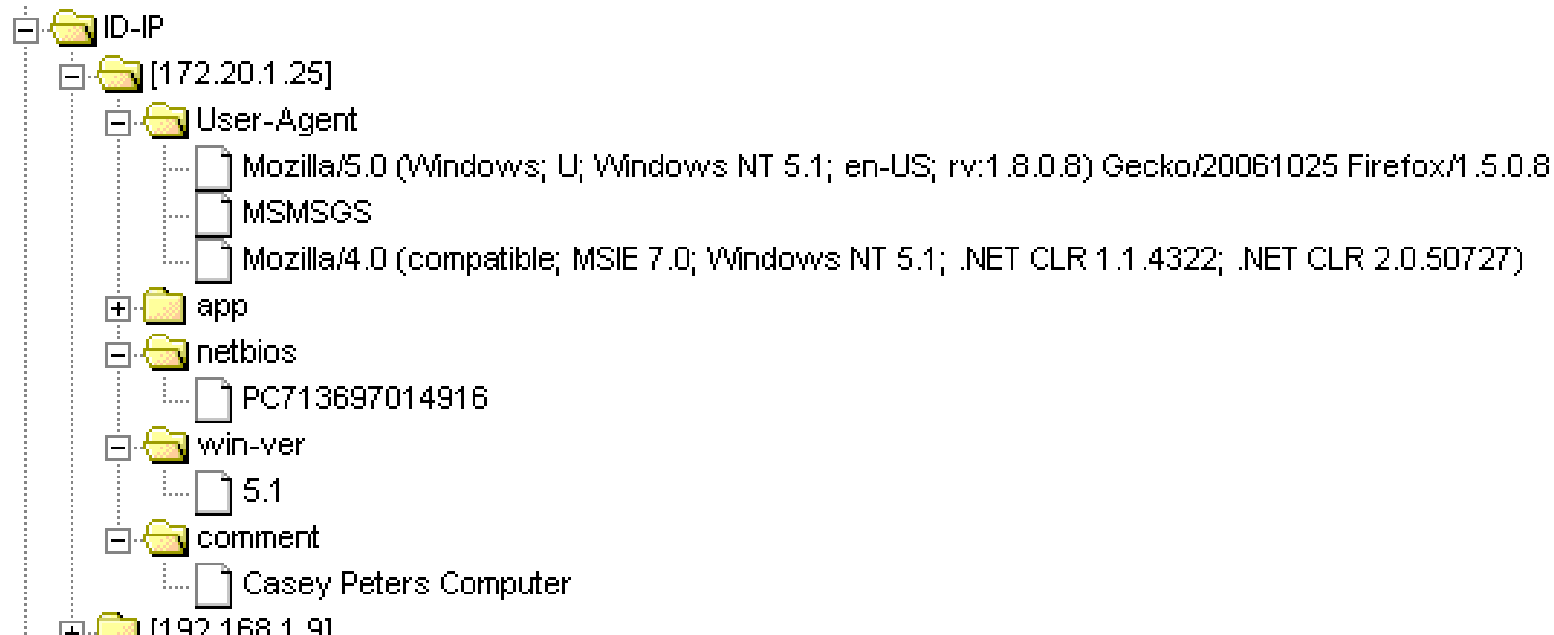
- Tells you about printers available
- Tells you about drivers that may have bugs
  - **Printer driver bugs are common, which is why Microsoft moved them to user-mode drivers**
- Tells you about vulnerable printers
- Maps out the network





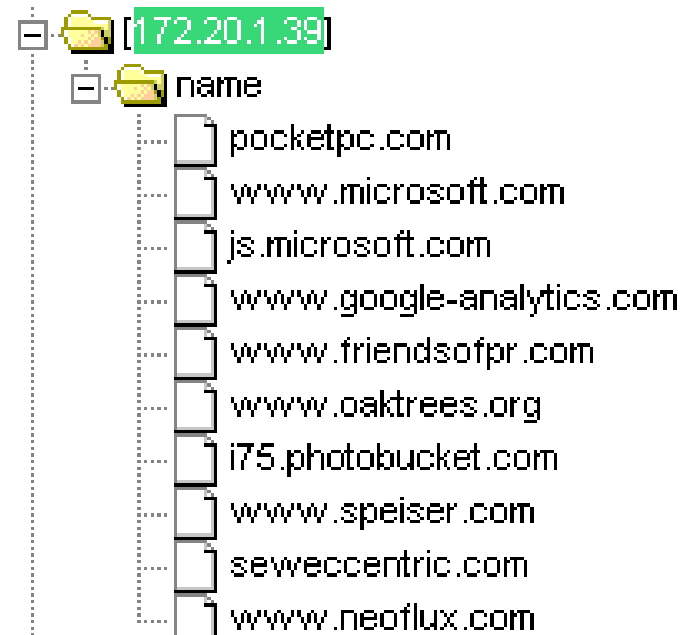
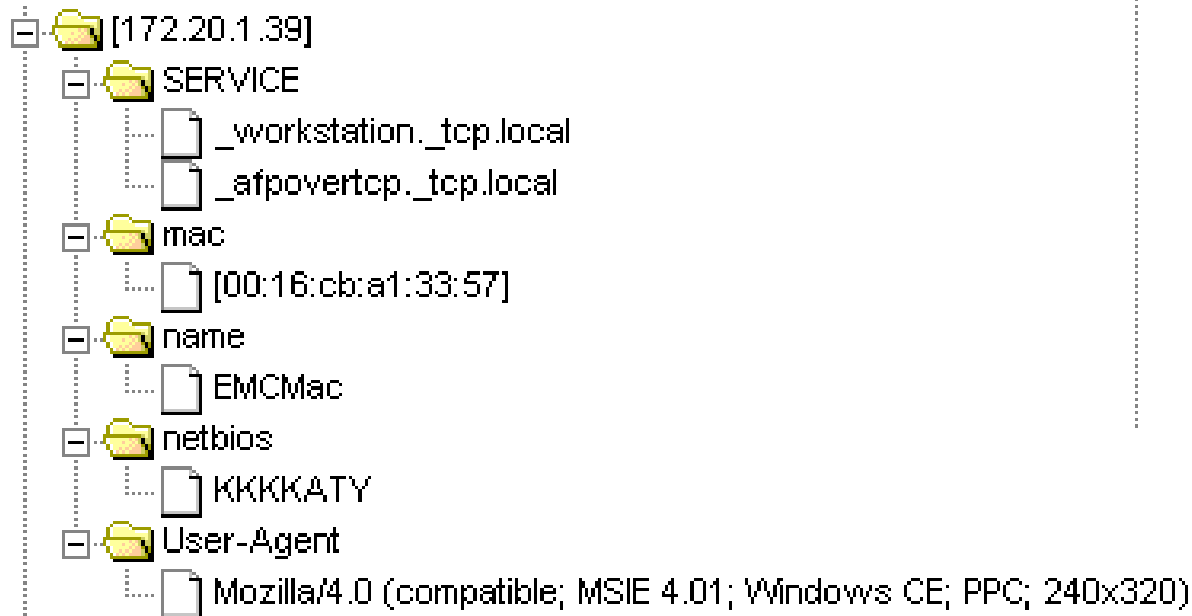
## Example: ID

- Tells you about the system, pulling interesting identification info from various protocols





## Example: ID (more)





## Example: ID (more)

- [-] [172.20.1.12]
  - [-] User-Agent
    - [-] Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.0.8) Gecko/20061025 Firefox/1.5.0.8
    - [-] Windows-Update-Agent
    - [-] Mozilla/4.0 (compatible; MSIE 6.0; Win32)
    - [-] Mozilla/4.0 (compatible; MSIE 6.0; MS Web Services Client Protocol 1.1.4322.2032)
    - [-] Microsoft BITS/6.6
    - [-] Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; CH2M; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
  - [-] netbios
    - [-] PDX31020038
  - [-] win-ver
    - [-] 5.1
  - [-] comment
    - [-] NWR/PDX Ra [REDACTED], Andrew (503) 23 [REDACTED] 0 x4112
  - [-] name
    - [-] pdx310200 [REDACTED] m.com



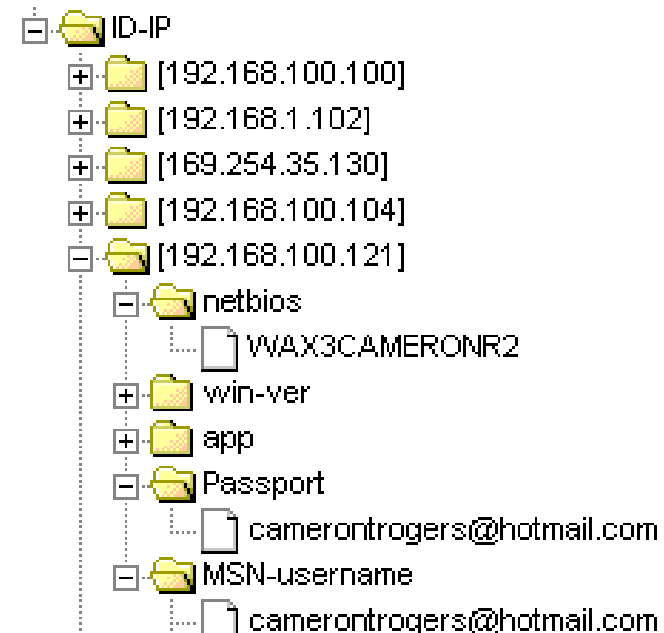
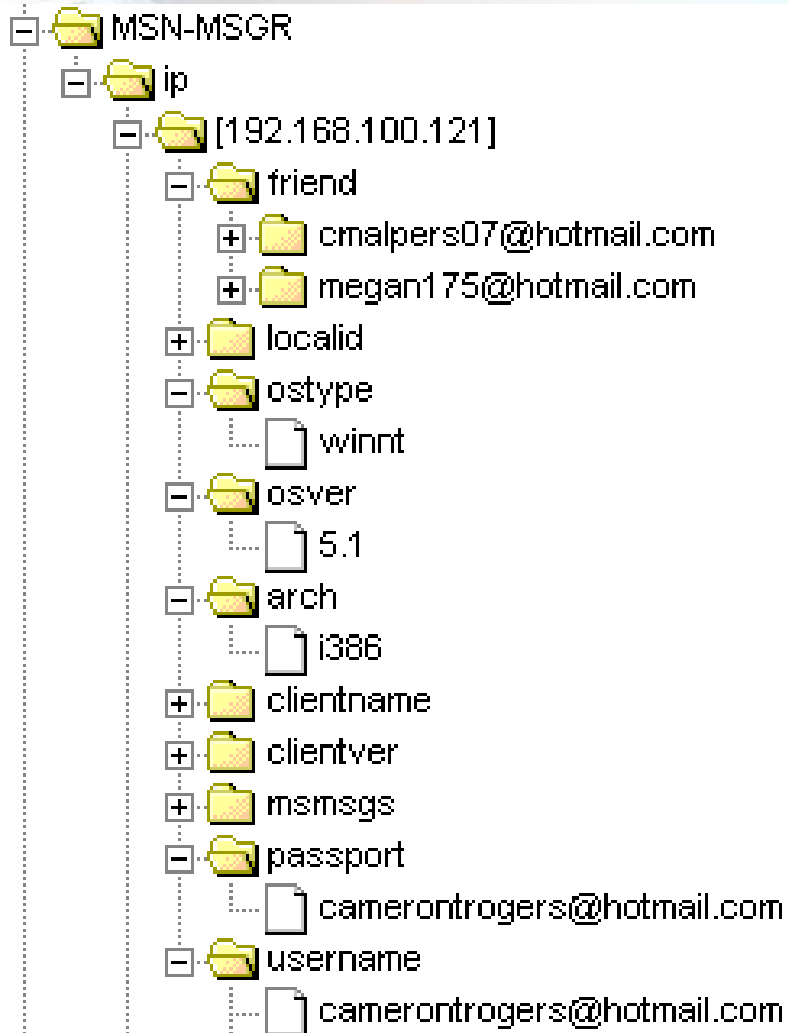
## Example: ID (more)

- [-] [172.20.1.13]
  - [-] netbios
    - ..... NDC\_EMAD
  - [-] win-ver
    - ..... 5.1
  - [-] comment
    - ..... EMAD\_
  - [-] User-Agent
    - ..... Microsoft-WebDAV-MiniRedir/5.1.2600
    - ..... Mozilla/4.0 (compatible; Win32)
    - ..... Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; InfoPath.1)
    - ..... Mozilla/4.0 (compatible; MSIE 6.0; Win32)
    - ..... Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)
    - ..... Industry Update Control
    - ..... Microsoft SUS Client/2.0
    - ..... Microsoft WU Client/2.0
  - [-] name
    - ..... VONGDEUANE-L-N.screen.com



## Example: MSN-MSGR

- Builds 'friends' list
- Grabs user of machine





- SSID
  - (broadcast)
  - NETGEAR
  - Wireless
  - stayonline
  - concourse
  - guestwifi
  - Internet
  - STSN\_Conf
  - ATL-WIFI
  - PBIA\_WIFI
  - NH&AWirele\$\$
  - primnet-916
  - ROC Airport1
  - atlantabread
  - hhonors\_Conf
  - hhonors
  - securedemail\_Home
  - tmobile
  - comfortinn
  - ROC Airport2
  - tsunami
  - mimecom
  - SJ
  - Connexion1
  - 04Z412566951
  - KudoBeans/ANYWHERE
  - Hilton
  - binz network
  - Stjartrosen
  - securedemail

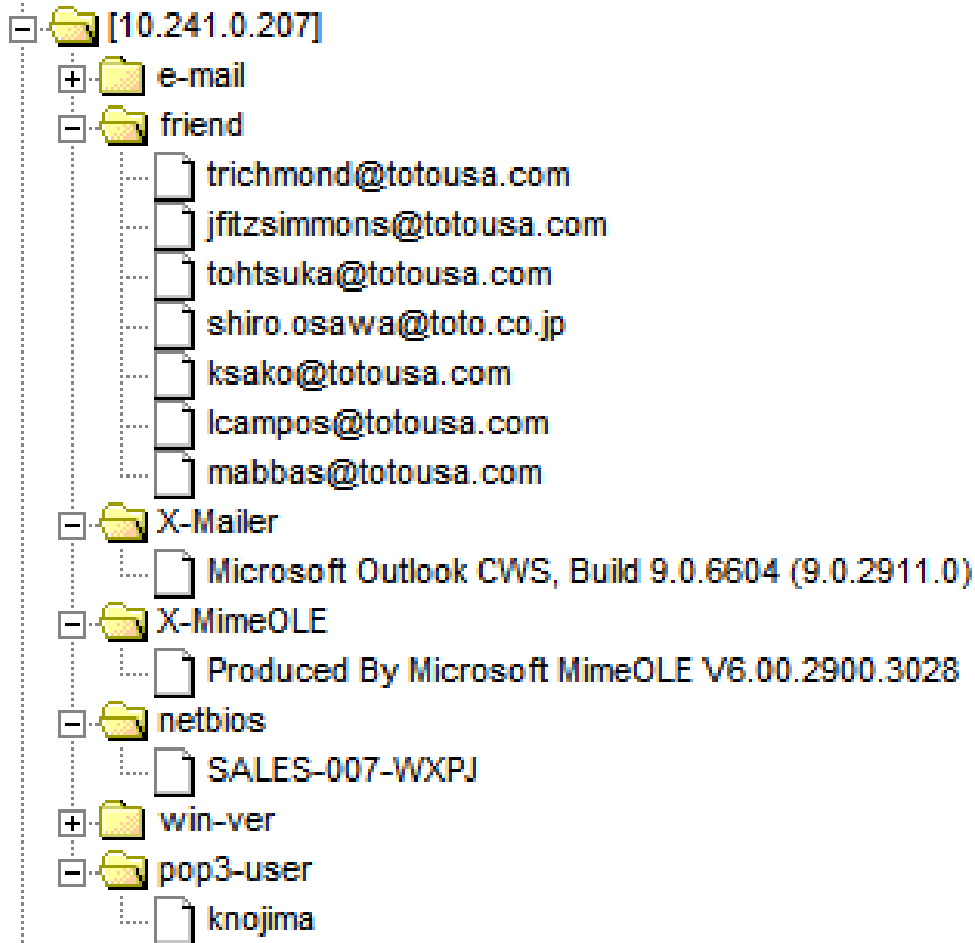


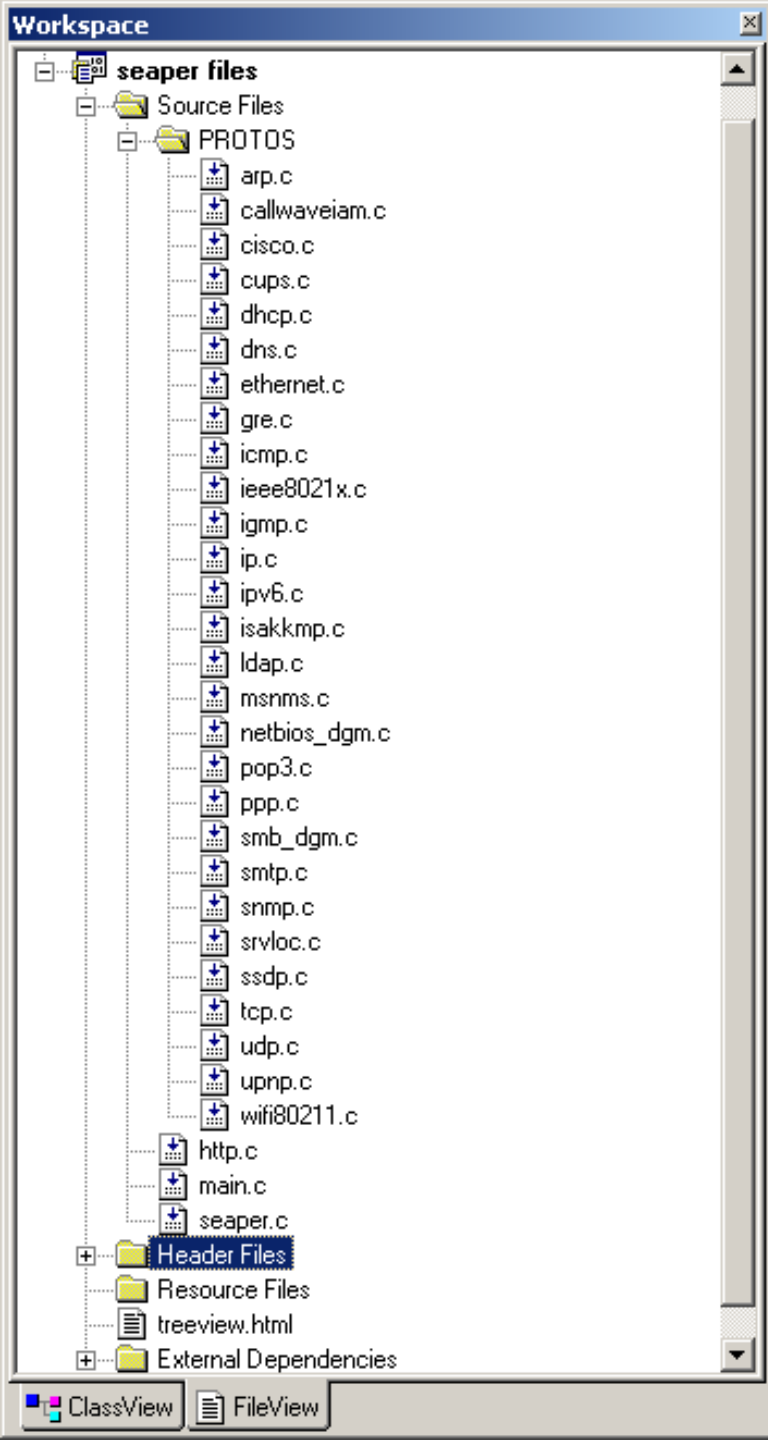
## Example: WiFi probes

- A list of every place the person has been

## Example: e-mail

- Finding the 6-degrees of Kevin Bacon





- Current build of the software

```
C:\WINDOWS\system32\cmd.exe
SNIFFING: \\.\airpcap00
LINKTYPE: 105
TEST="SAP", ethertype=0
Traffic seen
TEST="IEEE802.11", parm=0
TEST="IEEE802.11", parm=1
TEST="IEEE802.11", parm=3
TEST="IEEE802.11", parm=5
TEST="IEEE802.11", parm=42
proto="WiFi", op="unknownparm", macaddr=[00:11:21:e0:98:00], wifi.tag=42, wifi.u
TEST="IEEE802.11", parm=50
TEST="IEEE802.11", parm=133
proto="WiFi", op="unknownparm", macaddr=[00:11:21:e0:98:00], wifi.tag=133, wifi.
ckHat\x00\x00\x00\x00\x00\x00\x00\x00\x12\x00\x00%"
TEST="IEEE802.11", parm=221
TEST="IEEE802.11", oui=16534
proto="WiFi", op="vendor", vendor.name="Aironet", vendor.oui=0x4096, vendor.data
00\x00aC\x00\x00"
proto="WiFi", op="beacon", macaddr=[00:11:21:e0:98:00], SSID="BlackHat", maxrate
proto="WiFi", op="probe", macaddr=[00:09:5b:94:cb:09], SSID="BlackHat"
proto="WiFi", op="probe-response", macaddr=[00:11:21:e0:98:00], SSID="BlackHat",
proto="WiFi", op="probe", macaddr=[00:09:5b:94:cb:09], SSID="(broadcast)"
proto="WiFi", op="unknownparm", macaddr=[00:11:21:e0:98:00], wifi.tag=133, wifi.
ckHat\x00\x00\x00\x00\x00\x00\x00\x00\x12\x00\x00%"
TEST="UDP", src=5353
TEST="UDP", dst=5353
ID-IP=[10.0.1.108], name="macosx.local"
Bonjour="macosx.local", OS="Mac OS X 10.3.9 (7W98), mDNSResponder-58.8.1 (Jan 31
Bonjour="macosx.local", CPU="PowerBook5,6"
TEST="UDP", src=50488
TEST="UDP", dst=192
proto="WiFi", op="probe", macaddr=[00:17:f2:43:a1:9b], SSID="wrightplace"
TEST="UDP", src=50489
proto="WiFi", op="unknownparm", macaddr=[00:11:21:e0:98:00], wifi.tag=133, wifi.
ckHat\x00\x00\x00\x00\x00\x00\x00\x00\x12\x00\x00%"
^C
C:\errata1\src\Ferret\Debug>
```



# CONCLUSION



## How to protect?

- Personal firewalls?
  - Don't allow any traffic unless you are on a trusted network.
  - Users will just blindly click through them
- Corporate Polices...
  - Do these ever really work?
- The best solution for this is to be aware of the danger.
  - Everyone really doesn't need to work from a coffee shop.