

TAKING A LEAK ON THE NETWORK: LITTLE THINGS THAT GIVE AN ATTACKERS IDENTITY AWAY

Adrian Crenshaw



About Adrian

- ▣ I run Irongeek.com
- ▣ I have an interest in InfoSec education
- ▣ I don't know everything - I'm just a geek with time on my hands
- ▣ (ir)Regular on the ISDPodcast
<http://www.isd-podcast.com/>



What information is leaking out about your (or someone else's) box while connected to a network?

- ▣ Outright identification
- ▣ Shrinking of the “anonymity set”
 - An anonymity set is the total number of possible candidates for the identity of an entity. Reducing the anonymity set means that you can narrow down the suspects.



Why this talk?

- ▣ Because Rob told me to come up with something
- ▣ I'm in a privacy class, and intended to use it as a project (but ended up working with I2P instead)
- ▣ Call to research on the topic
- ▣ "The quieter you become the more you can hear." -
- Baba Ram Dass (and since I'm not a shiftless hippy that doesn't bathe, I just think of it as the BackTrack Linux slogan)



Who might this talk interest

- ▣ Pentesters
- ▣ “Pro Bono Pentesters”
- ▣ Attackers
- ▣ IDS and Log Watchers
- ▣ Incident Response, and people who want to test Incident Response



Clean Room Box

- ▣ I advocate making a “Clean Room Box” if you can afford it.
- ▣ Separate boot partition is the 2nd best option
- ▣ “Clean Room VM” May be an option
- ▣ Most of the mitigations I mention can be taken in the Clean Room
- ▣ For legitimate pentesters, this also helps keep customer data separate



Just a few leaks, of many

- ▣ MAC Address left in logs
- ▣ Browser tabs that automatically open
- ▣ Network scans that automatically use the credentials of the logged in user
- ▣ WiFi SSID Probes
- ▣ Host name/NetBIOs name broadcasts
- ▣ Last DHCP lease renew
- ▣ Other apps? (Skype, IM, IRC, etc)



MAC Address left in logs

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cb:37:89
          inet
addr:192.168.127.129  Bcast:192.168.127.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feeb:3789/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:108974 (108.9 KB)  TX bytes:92538 (92.5 KB)
          Interrupt:19 Base address:0x2000
```

Wireless LAN adapter Wireless Network Connection:

```
Connection-specific DNS Suffix  . :
Description . . . . . : Broadcom 802.11n Network Adapter
Physical Address. . . . . : 00-1A-70-3C-A6-3D
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . :
fe80::b1ce:9626:799a:5f41%14(Preferred)
IPv4 Address. . . . . : 192.168.1.13(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 369105520
DHCPv6 Client DUID. . . . . : 00-01-00-01-12-E4-11-A3-00-1A-A0-
8D-BC-BE

DNS Servers . . . . . : 192.168.1.1
NetBIOS over Tcpip. . . . . : Enabled
```



Details

- ▣ In theory MAC addresses are unique (but not really)
- ▣ Can be spoofed, but good luck proving that it was Bob Swim
- ▣ First 6 HEX digits are the vendor's OUI (Organizationally Unique Identifier)
<http://standards.ieee.org/regauth/oui/oui.txt>
- ▣ I wonder if any vendors store this information?



Mitigation

- ▣ Change it if possible:
<http://www.irongeek.com/i.php?page=security/changemac>
- ▣ Linux:
ifconfig eth0 down hw ether 00:00:00:00:00:01
ifconfig eth0 up
- ▣ Windows:
Regedit or some tools
(but some card drivers just say no or require the same OUI)

MadMacs

<http://www.irongeek.com/i.php?page=security/madmacs-mac-spoofers>

Smac

<http://www.klcconsulting.net/smac/>



Related

▣ IPv6 Stateless Address Autoconfiguration

<https://www.defcon.org/images/defcon-15/dc15-presentations/Lindqvist/Whitepaper/dc-15-lindqvist-WP.pdf>

- ▣ This example may be local only, and non-routable, sort of like 169.254.0.0/16 in IPv4

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:cb:37:89
          inet addr:192.168.127.129  Bcast:192.168.127.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe3b:3789/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1102 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:108974 (108.9 KB)  TX bytes:92538 (92.5 KB)
          Interrupt:19 Base address:0x2000
```



Browser tabs that automatically open

- What does it say about you?



Details

- ▣ Just the names of the sites give tons on information
- ▣ Plaintext login information
- ▣ Imagine using Facebook during a pentest?
- ▣ Even if SSL is used, DNS queries give away information about the sites visited
- ▣ Headers (browser type, version, plugins)

Thanks to d4ncingd4n for reminding me to add headers



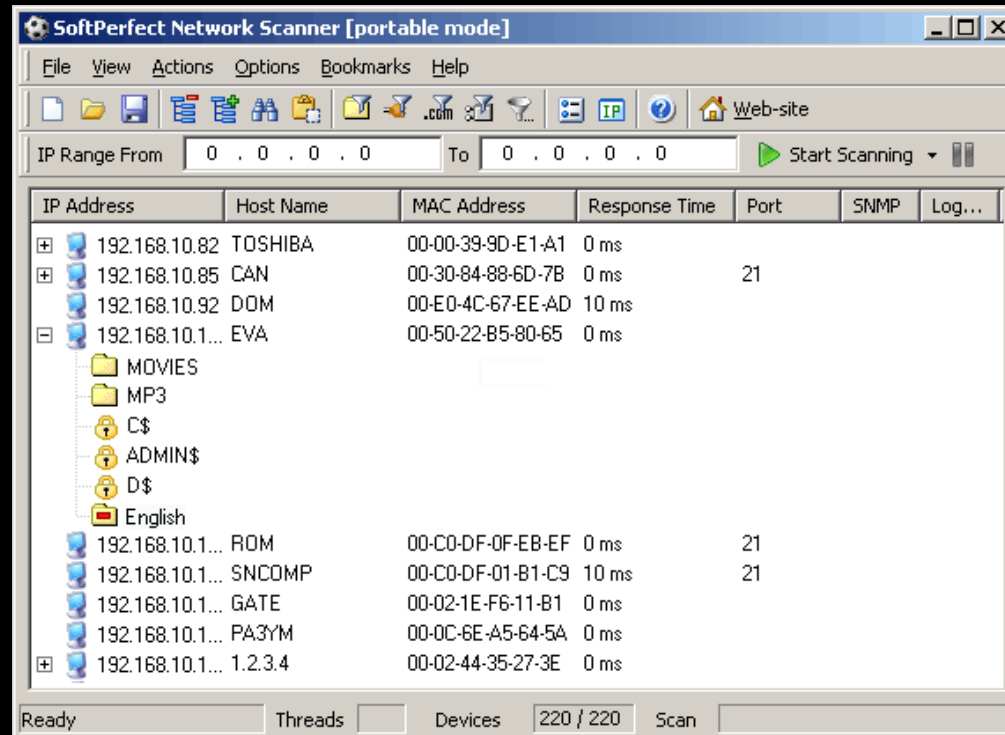
Mitigation

- ▣ Dedicated browser for certain activities
- ▣ Limit plugins
- ▣ Keep changing user agent
(or make sure it's very generic)
- ▣ Don't have the browser do anything automatically
 - Passwords
 - Forms
 - Tabs



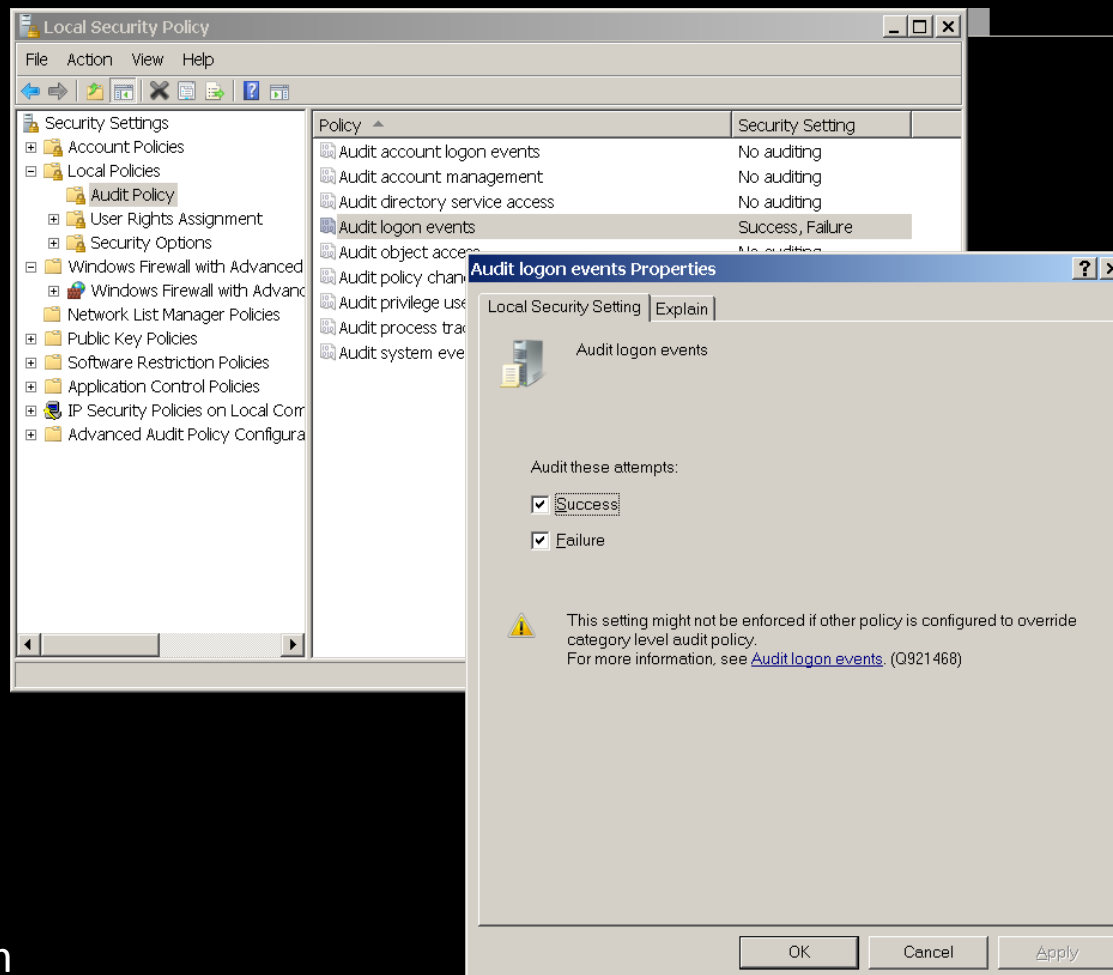
Network scans that automatically use the credentials of the logged in user

- ▣ Watch out for “Use current credentials”



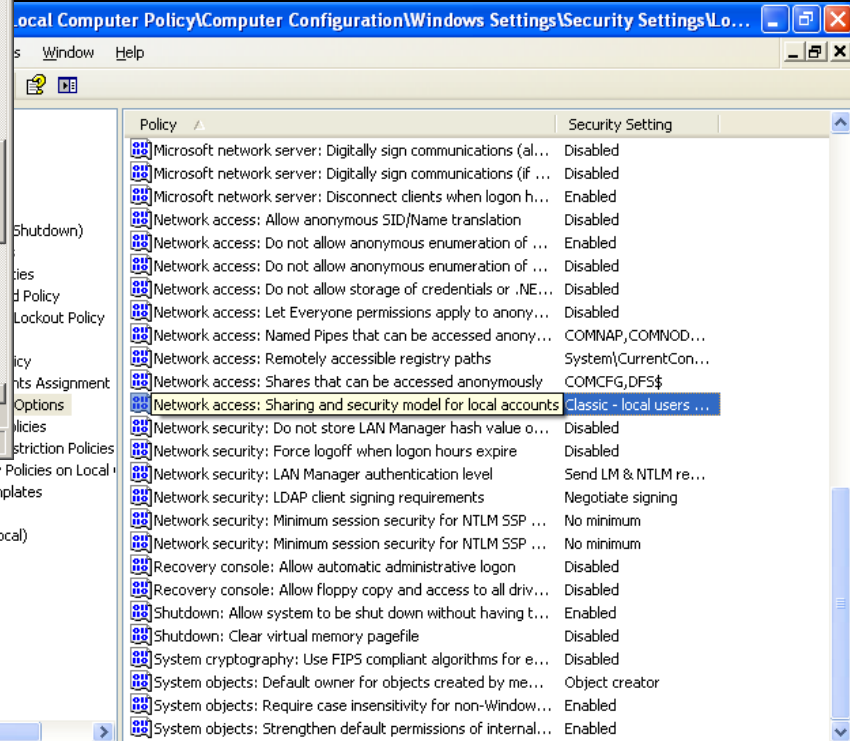
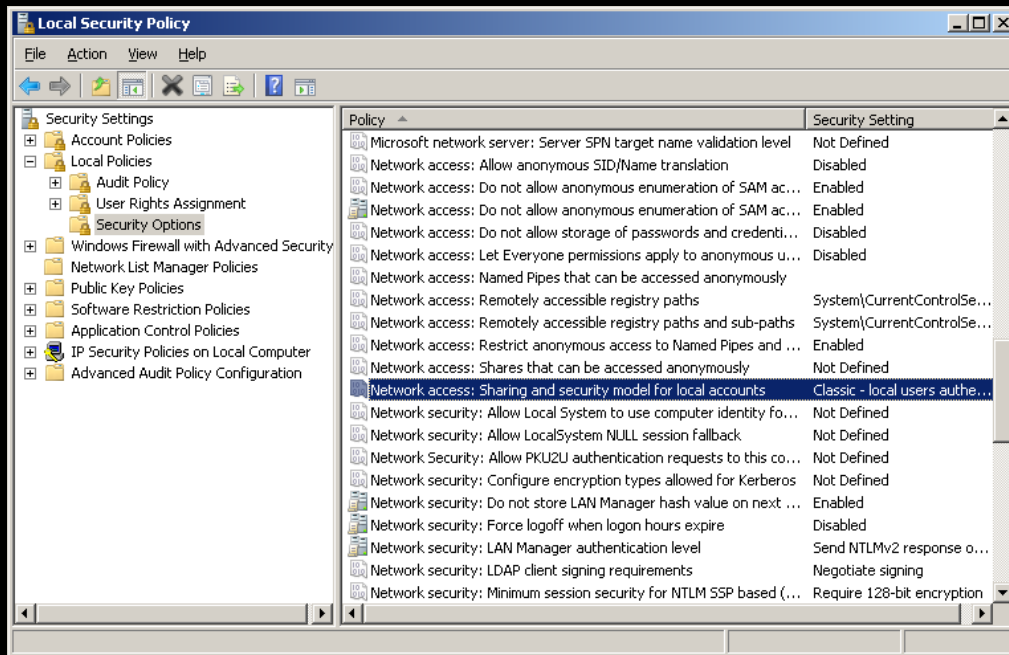
Details

▣ Auditing matters



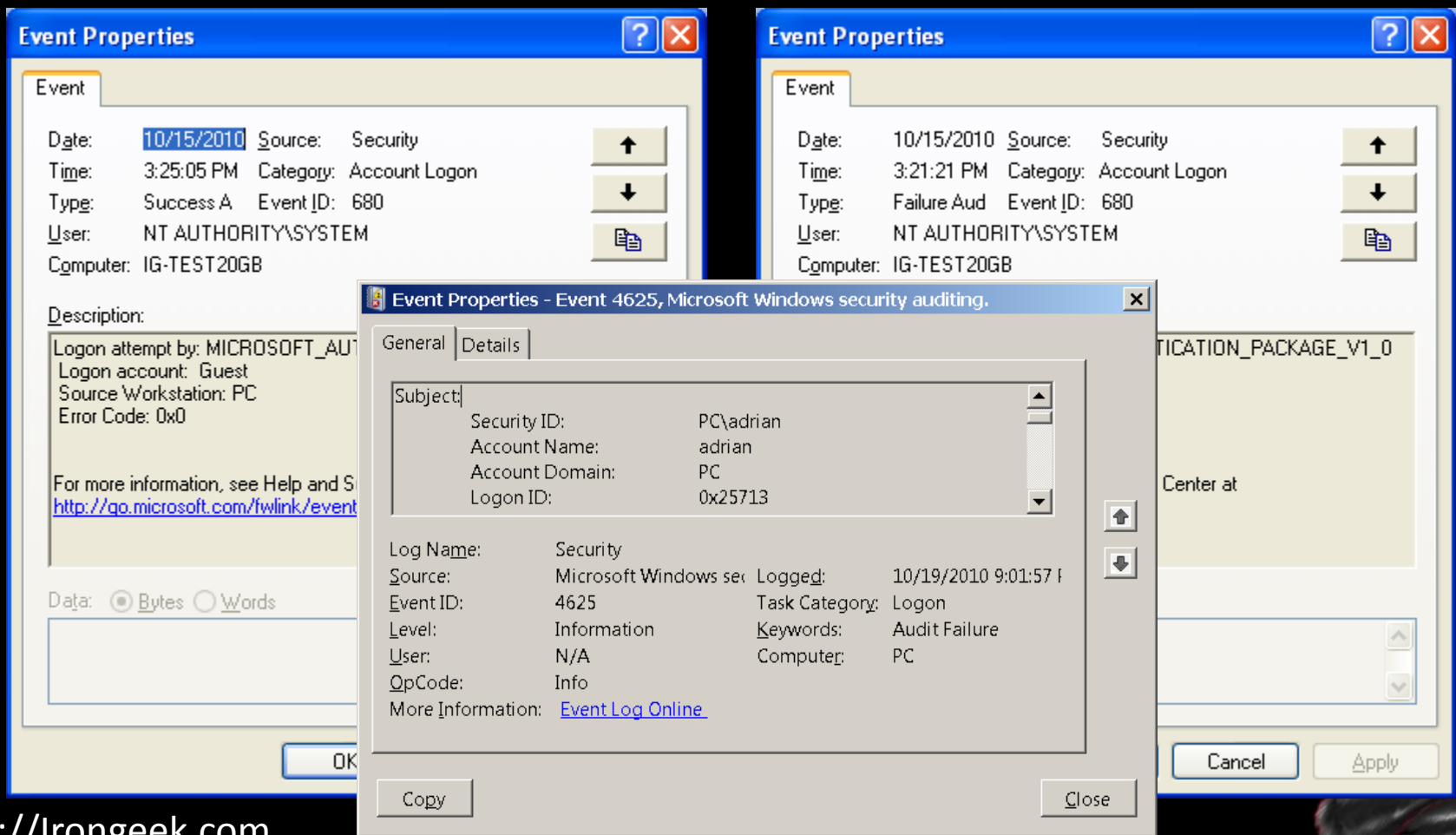
Details

▣ Share type matters



Details

- What shows in the logs depends on share type



Mitigation

- ▣ Use a different account
- ▣ Use a non-specific user name
- ▣ If the tool has an option for “use other credentials”, try using it, keeping in mind “Trust but verify”
- ▣ “Shift+Right-Click ->Run As” works wonders



Related

- ▣ When auditing logins causes security problems
- ▣ A successful login right after a failed one, with a user name that matched your password complexity rules? Hum, let me think here. 😊
- ▣ PEBKAC Attack
<http://www.irongeek.com/i.php?page=security/pebkac-attack-passwords-in-logs>



WiFi SSID Probes

- ▣ SSID probes, not like the alien kind

```
root@bt: ~ - Shell - Konsole
Session Edit View Bookmarks Settings Help
Kismet Sort View Windows
Name T C Ch Pkts Size
- Autogroup Probe P N --- 72 0B
  <Any> P N --- 157 0B
  Belkin Enhanced Wire P N --- 5 0B
  Andy&Mo's A 0 6 17 0B
  Belkin_Enhanced_Wire A N 1 64 2K
No GPS info (GPS not connected)
INFO: Saved data files
INFO: Saved data files
INFO: Saved data files
INFO: Saved data files
INFO: Saved data files
```



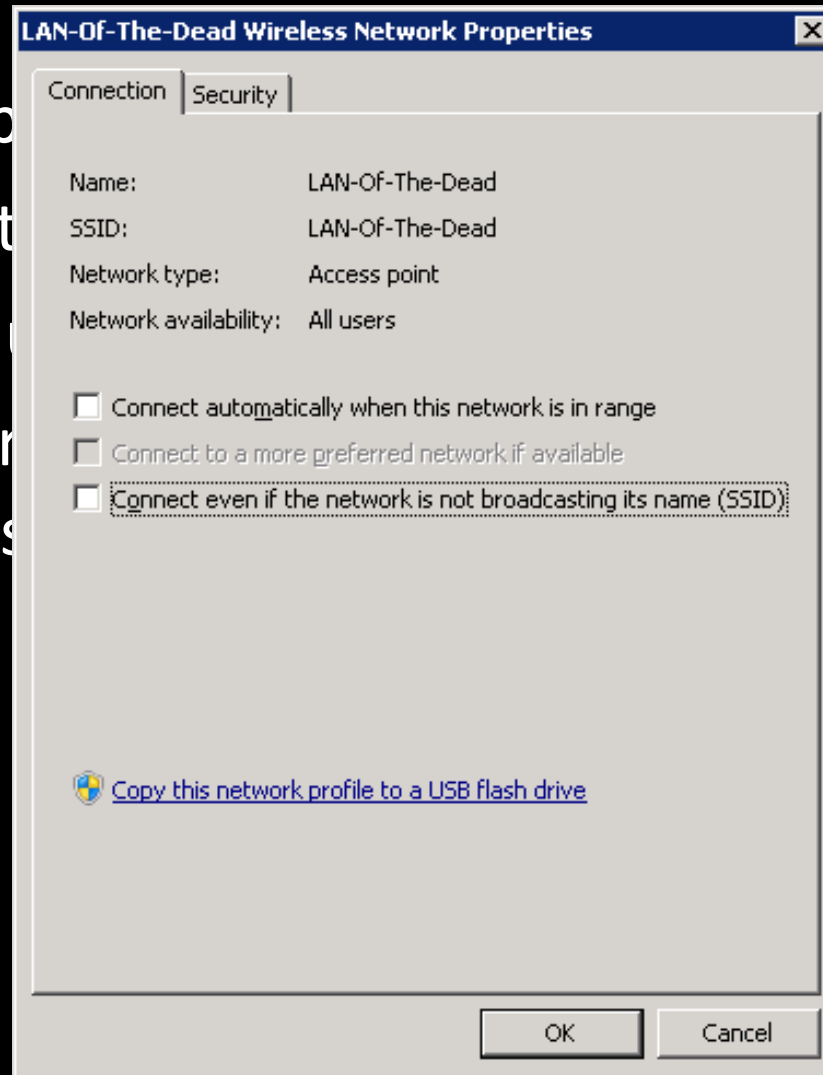
Details

- ▣ Depends on OS and configuration
- ▣ Sometimes probes are sent from a wireless client saying “hey, are you out there?” to a previously used SSID (Wireless Network Name)
- ▣ Network names may be significant (now I know what comics you like, where you go to school, and where you get coffee)
- ▣ Geolocation:
 - Google Street View?
 - Wigle it, just a little bit!
<https://wagle.net/gps/gps/main/query/>



Mitigation

- ▣ Use a sup
- ▣ Clean out
- ▣ Disable a
- ▣ Another r
- to useless



home

profiles

)
SSID is just a bad



Host name/NetBIOs name broadcasts

- What does your name say about you?

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time
ig-test20gb	192.168.1.141		
*	192.168.1.109		
*	192.168.1.139		
BobbysWorld	192.168.1.108		
WET610N	192.168.1.130		
glenn-lappy	192.168.1.110		
PC	192.168.1.134		
cthulhu	192.168.1.103		
*	192.168.1.102		
WebCamRotate	192.168.1.253		

System Properties

Computer Name | Hardware | Advanced | System Protection | Remote

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

Full computer name: skynet

Workgroup: WORKGROUP

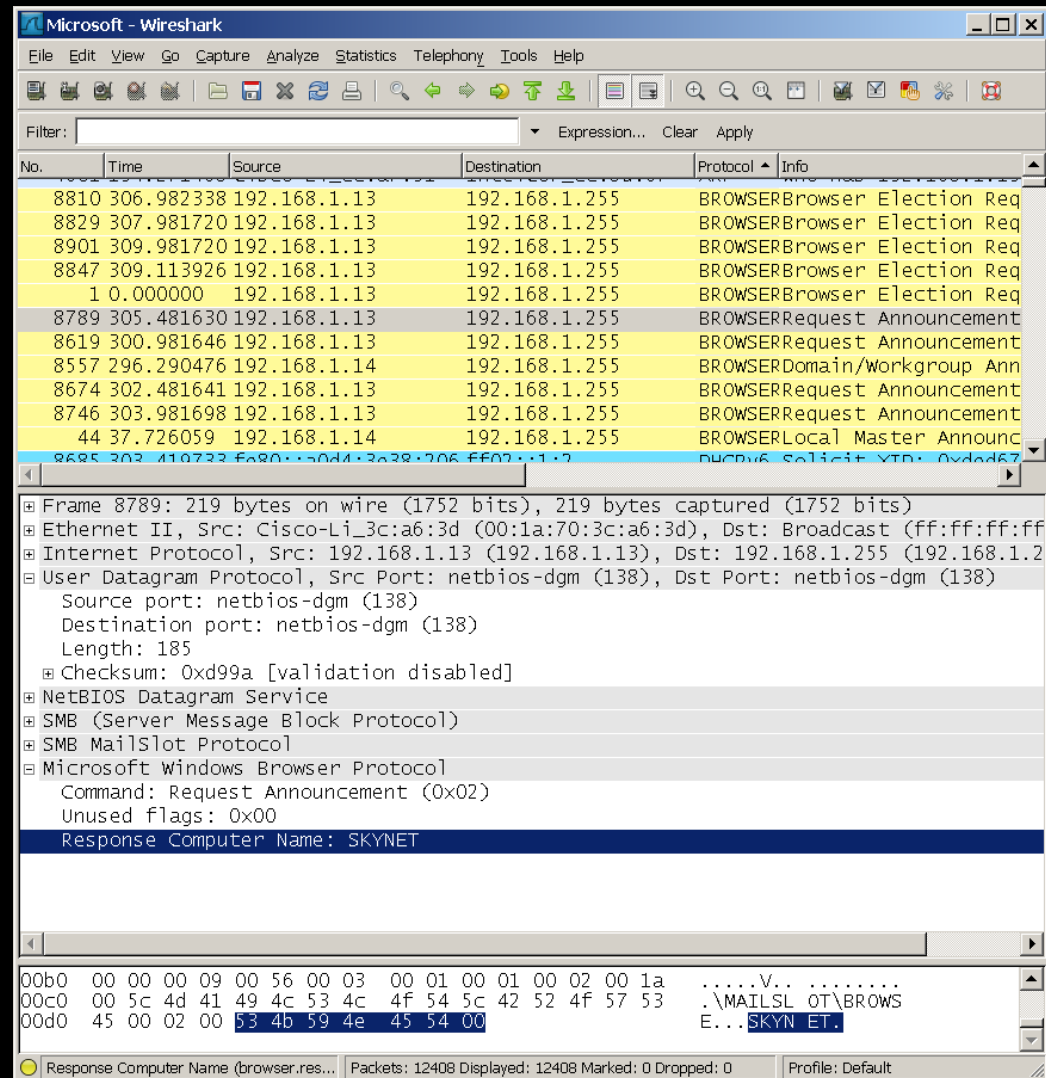
To use a wizard to join a domain or workgroup, click Network ID.

To rename this computer or change its domain or workgroup, click Change.



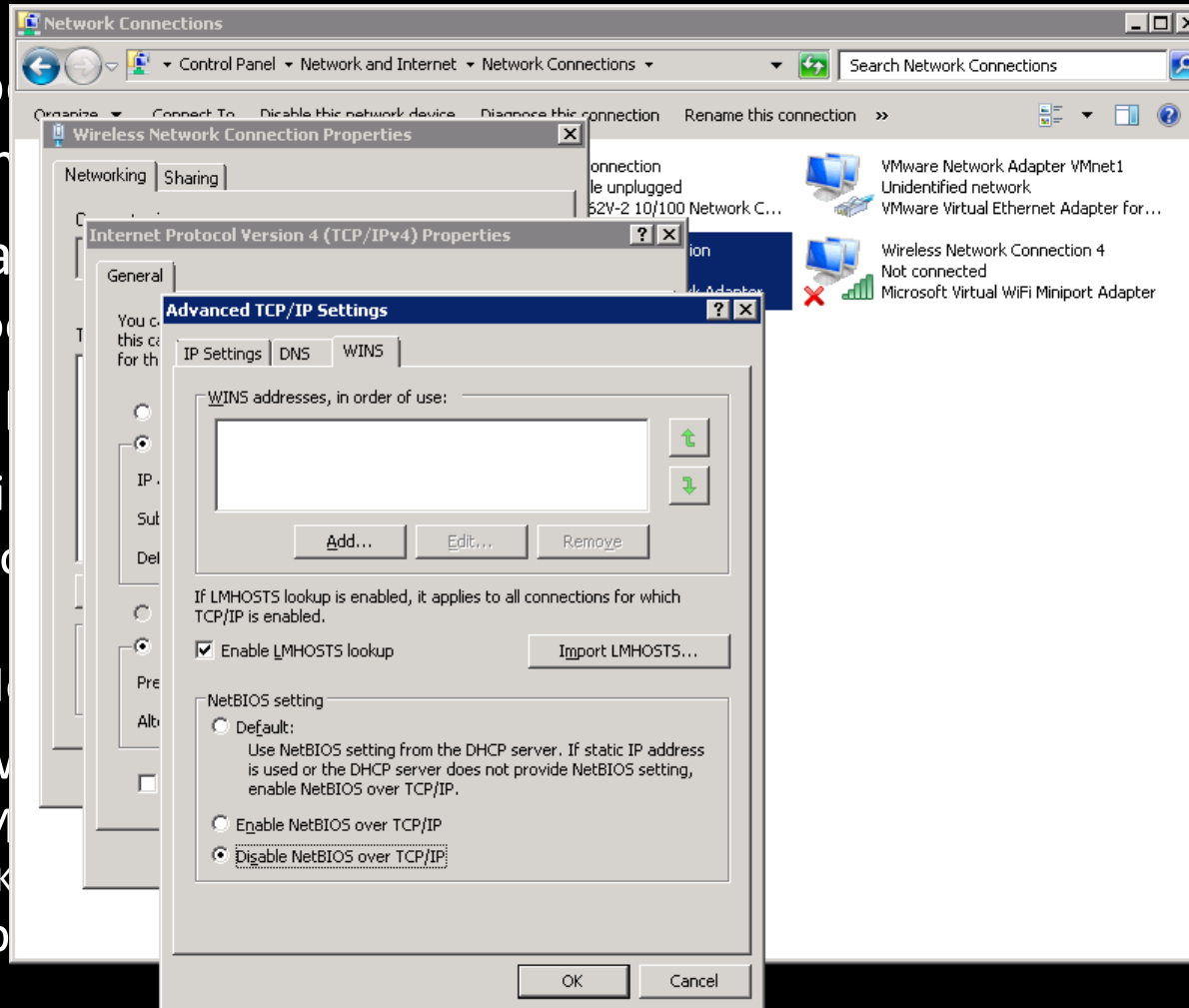
Details

- ❑ DHCP can have a host name option
- ❑ NetBIOs naming traffic says “hey, I’m here”
- ❑ Direct probe may also list name



Mitigation

- Choose a channel name
- Disable NetBIOS (Choose NetBIOS over TCP/IP)
- For Windows XP
 - Link-local Multicast Name Resolution
 - Windows Firewall



urer's

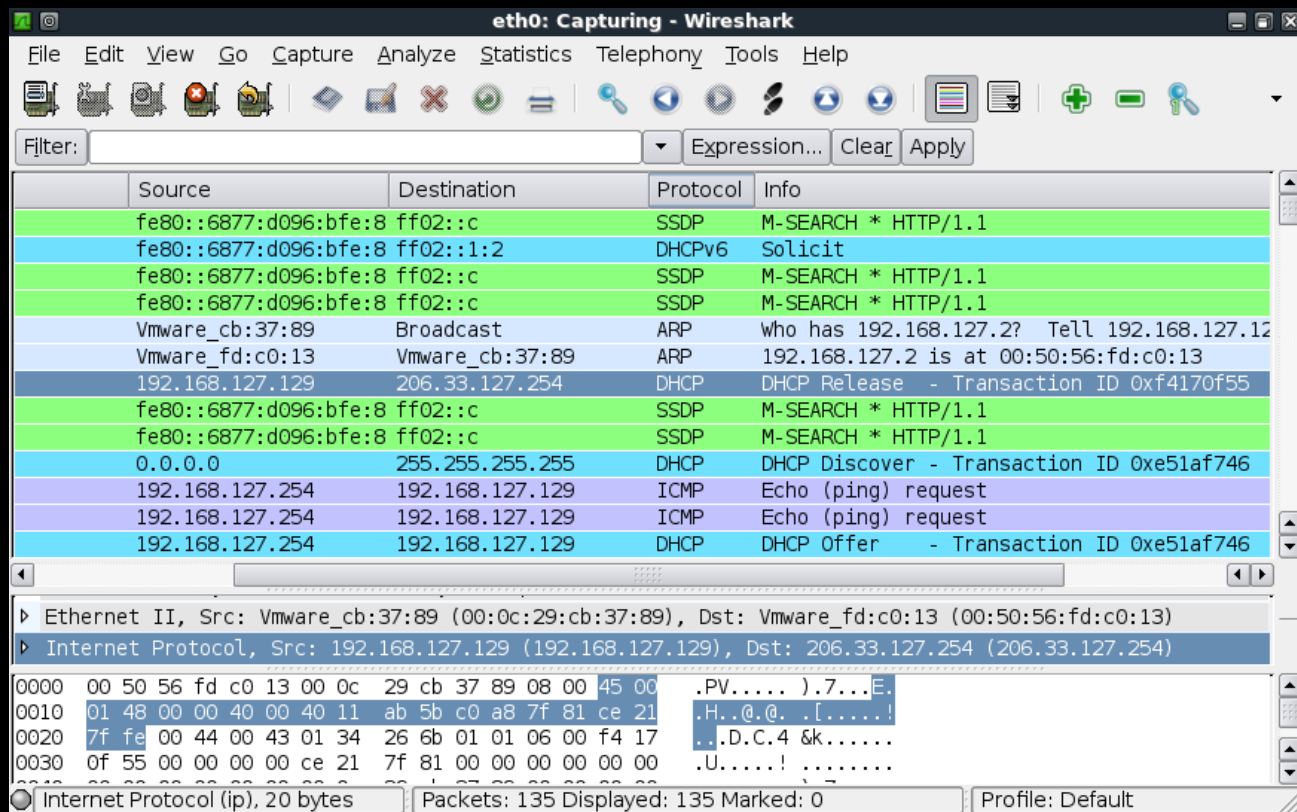
ny opinion)

ptions



Last DHCP lease renew

- What other networks have you been on?

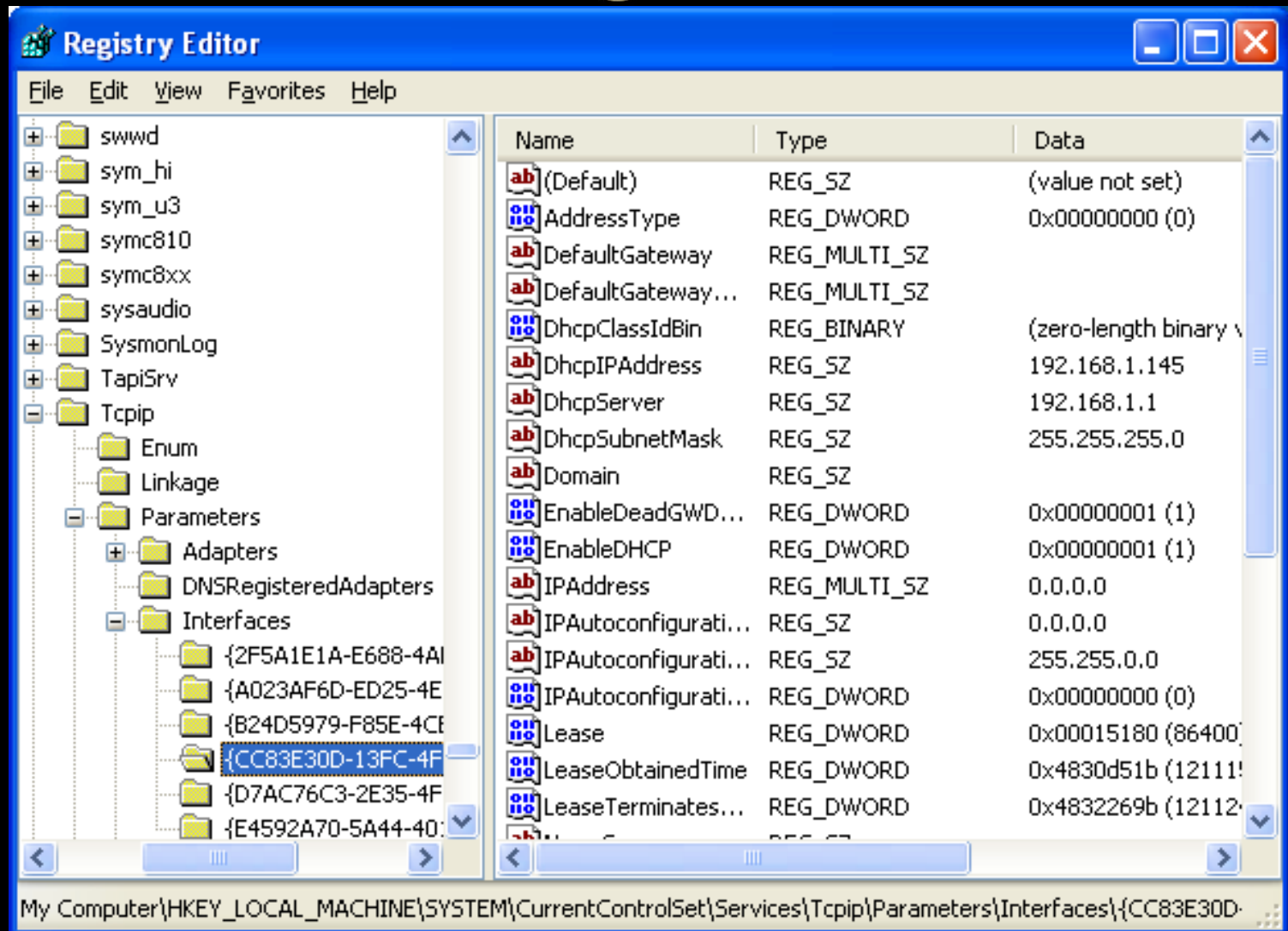


Details

- ▣ Sometimes DHCP info gets sent when you move from network to network
- ▣ If the last DHCP server handed out a non routable (like 192.168.*.*) it may not be a big issue
- ▣ Find who owns the IP
<http://serversniff.net/asreport.php>
- ▣ IP+Network Owner+Host Name+Google = identity?



Mitigation

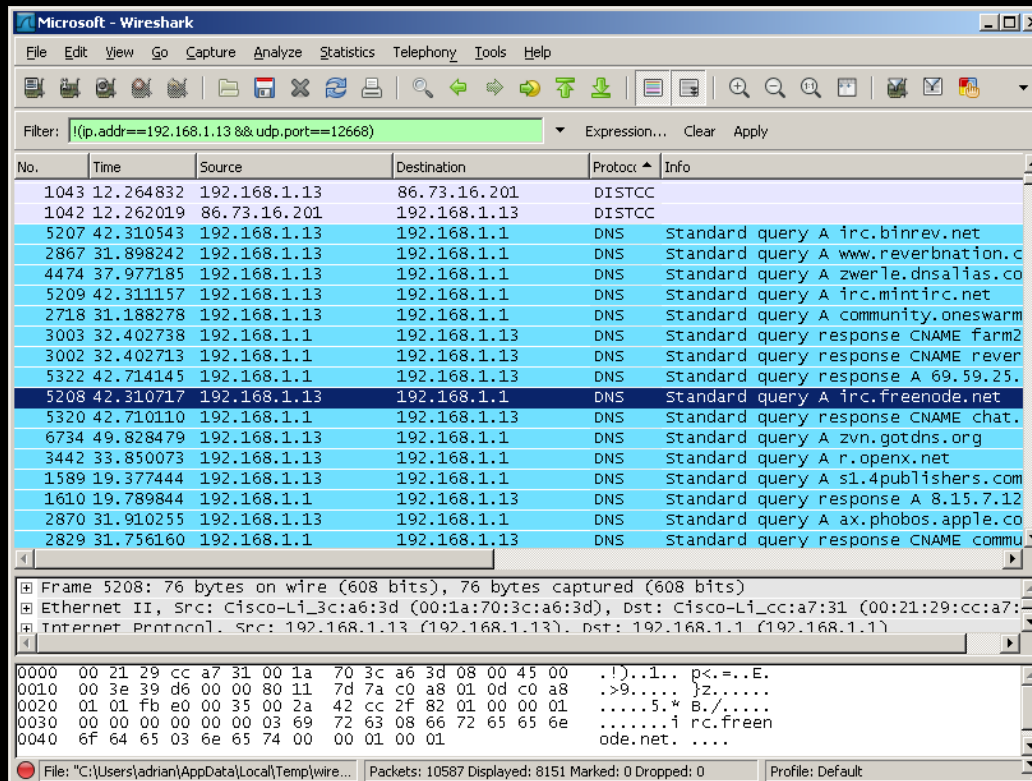


ers\I



Other apps? (Skype, IM, IRC, etc)

- ▣ Test your apps (in my case Pidgin)
- ▣ What servers does it contact, and what does it send?



Microsoft - Wireshark

Filter: `!(p.addr==192.168.1.13 && udp.port==12668)`

No.	Time	Source	Destination	Protocol	Info
1043	12.264832	192.168.1.13	86.73.16.201	DISTCC	
1042	12.262019	86.73.16.201	192.168.1.13	DISTCC	
5207	42.310543	192.168.1.13	192.168.1.1	DNS	Standard query A irc.binrev.net
2867	31.898242	192.168.1.13	192.168.1.1	DNS	Standard query A www.reverbnation.c
4474	37.977185	192.168.1.13	192.168.1.1	DNS	Standard query A zwerle.dnsalias.co
5209	42.311157	192.168.1.13	192.168.1.1	DNS	Standard query A irc.mintirc.net
2718	31.188278	192.168.1.13	192.168.1.1	DNS	Standard query A community.oneswarm
3003	32.402738	192.168.1.1	192.168.1.13	DNS	Standard query response CNAME farm2
3002	32.402713	192.168.1.1	192.168.1.13	DNS	Standard query response CNAME rever
5322	42.714145	192.168.1.1	192.168.1.13	DNS	Standard query response A 69.59.25.
5208	42.310717	192.168.1.13	192.168.1.1	DNS	Standard query A irc.freenode.net
5320	42.710110	192.168.1.1	192.168.1.13	DNS	Standard query response CNAME chat.
6734	49.828479	192.168.1.13	192.168.1.1	DNS	Standard query A zvn.gotdns.org
3442	33.850073	192.168.1.13	192.168.1.1	DNS	Standard query A r.openx.net
1589	19.377444	192.168.1.13	192.168.1.1	DNS	Standard query A sl.4publishers.com
1610	19.789844	192.168.1.1	192.168.1.13	DNS	Standard query response A 8.15.7.12
2870	31.910255	192.168.1.13	192.168.1.1	DNS	Standard query A ax.phobos.apple.co
2829	31.756160	192.168.1.1	192.168.1.13	DNS	Standard query response CNAME commu

Frame 5208: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)

Ethernet II, Src: Cisco-Li_3c:a6:3d (00:1a:70:3c:a6:3d), Dst: Cisco-Li_cc:a7:31 (00:21:29:cc:a7:31)

Internet Protocol. Src: 192.168.1.13 (192.168.1.13). Dst: 192.168.1.1 (192.168.1.1)

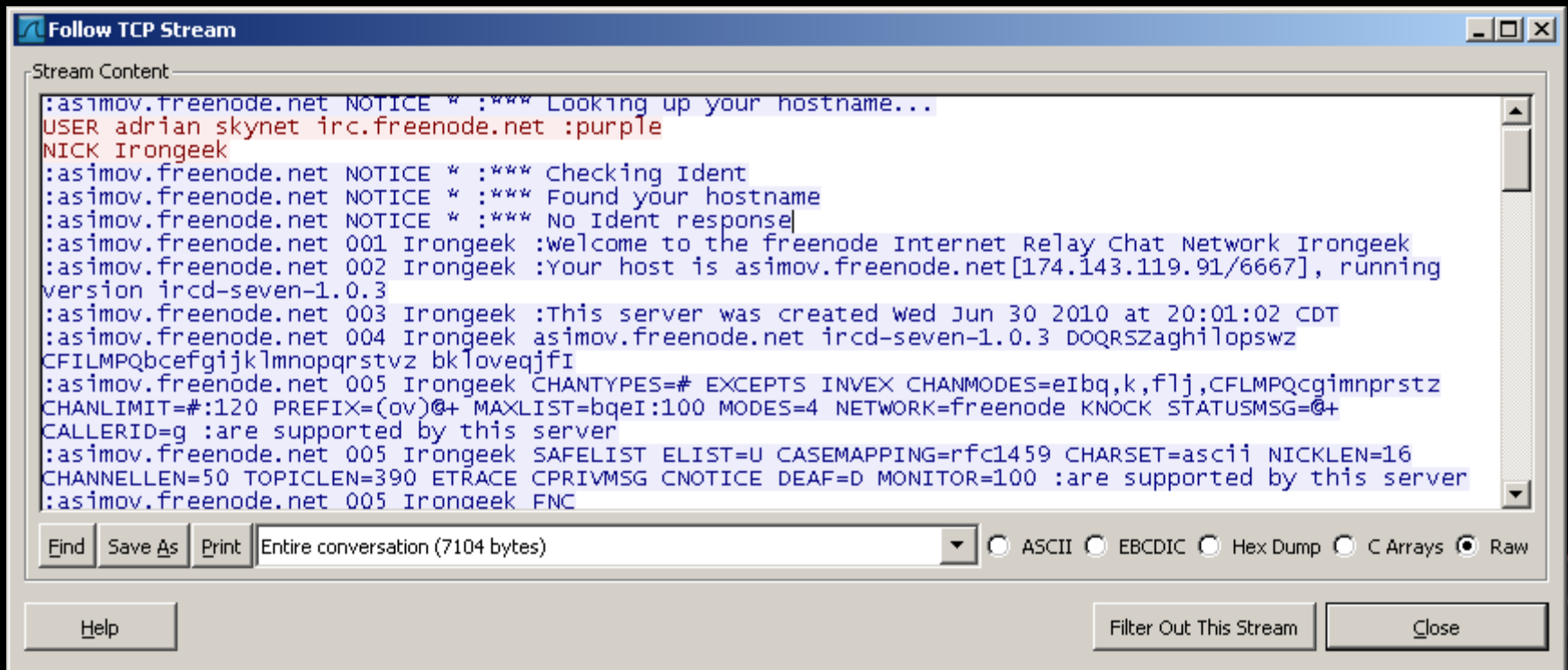
```
0000  00 21 29 cc a7 31 00 1a 70 3c a6 3d 08 00 45 00  ..!)..1.. p<..=.E.
0010  00 3e 39 d6 00 00 80 11 7d 7a c0 a8 01 0d c0 a8  .>9..... }z.....
0020  01 01 fb e0 00 35 00 2a 42 cc 2f 82 01 00 00 01  ....5.* B./.....
0030  00 00 00 00 00 00 03 69 72 63 08 66 72 65 65 6e  .......i rc.freen
0040  6f 64 65 03 6e 65 74 00 00 01 00 01             .....ode.net. ....
```

File: "C:\Users\adrian\AppData\Local\Temp\wire... | Packets: 10587 Displayed: 8151 Marked: 0 Dropped: 0 | Profile: Default



Details

- ❑ DNS shows info, even if the connection is encrypted
- ❑ Unencrypted, the protocol may give a ton of stuff away to a sniffer



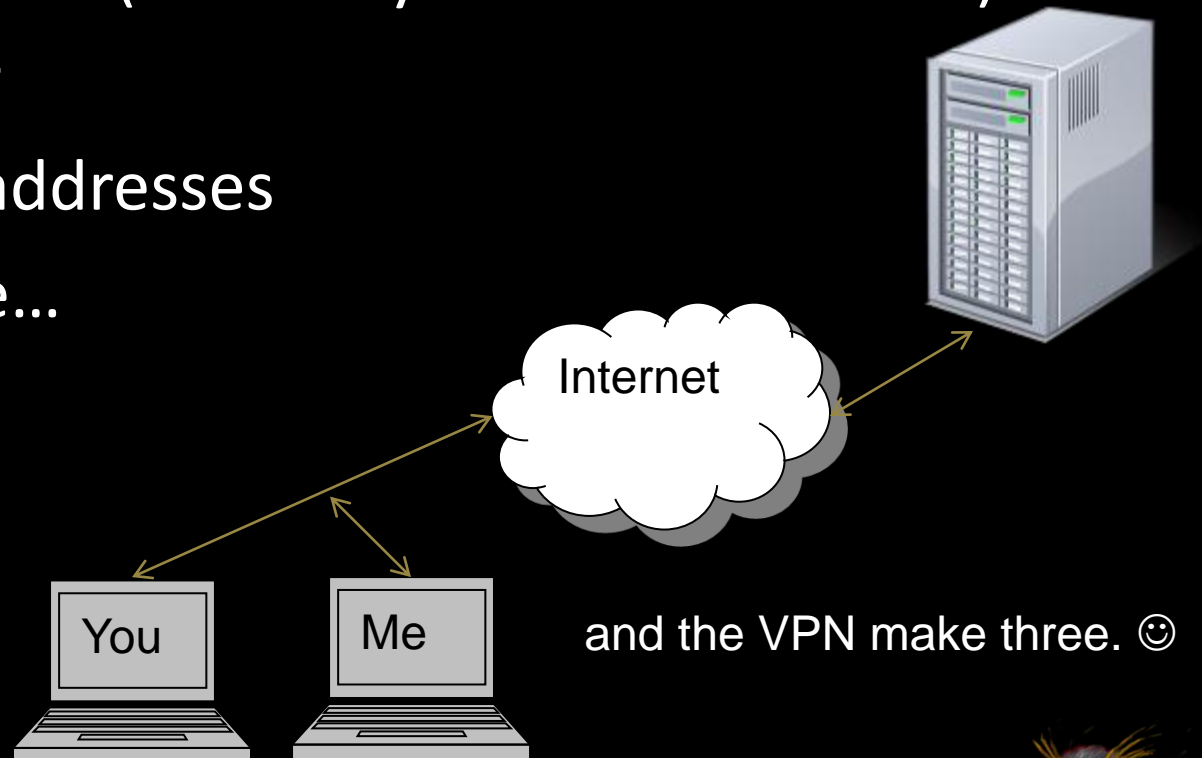
Mitigation

- ▣ Awareness
- ▣ Don't use those apps when you want to stay low profile
- ▣ Sniff to see what your apps give away



More thing that need looking into

- ▣ VPN follow home (fun to try at a hacker con ☺)
- ▣ UPnP/Bonjour
- ▣ Phone home addresses
- ▣ So much more...



- ▣ Thanks to d4ncingd4n, Bill Swearingen, Jim Halfpenny and Michael Dickey for suggestions



Clean Room PC/VM

- ▣ Simply stated:
An attacker should not use the same box for normal use, as for attack.
- ▣ Harden up the box as best as you can using what tips have been given
- ▣ Full Clean Room PC > Clean Room Boot Partition > Clean Room VM
- ▣ Make yourself some dual boot systems!!!



Great tools

- ▣ Wireshark
<http://www.wireshark.org/>
- ▣ NetworkMiner
<http://networkminer.sourceforge.net/>
- ▣ BackTrack Linux
<http://www.backtrack-linux.org/>



Events

- ▣ **DerbyCon 2011, Louisville Ky**
<http://derbycon.com/>
- ▣ **Louisville Infosec**
<http://www.louisvilleinfosec.com/>
- ▣ **Skydogcon/Hack3rcon/Phreaknic/Notacon/Outerz0ne**
<http://www.skydogcon.com/>
<http://www.hack3rcon.org/>
<http://phreaknic.info>
<http://notacon.org/>
<http://www.outerz0ne.org/>



QUESTIONS?

42

