

# SEARCH



## San Diego International Conference on Child & Family Maltreatment

Portable Apps as an Investigative Tool



# What is SEARCH?

- Non-profit based in Sacramento, CA
- Funded to offer assistance to law enforcement throughout the country
- Low-cost (or free) law enforcement training around the U.S.
  - Introduction to Computer Crime
  - Cell Phone Data Recovery
  - Advanced Responders: Search and Seizure of Networks
  - Social Networking Website Investigations
  - Peer-to-Peer



# What is SEARCH?

- Free technical assistance to federal, tribal, state and local LE
- Other resources
  - SEARCH ISP List
  - SEARCH Investigative Toolbar
  - Whitepapers
  - LE conference speakers



# What is SEARCH?

## www.search.org

The screenshot shows the homepage of the SEARCH website. At the top left is the SEARCH logo with the tagline "The online resource for justice and public safety decision makers". Navigation links include HOME, CAREERS, CONTACT US, ABOUT SEARCH, PRODUCTS & SERVICES, PROGRAMS, PUBLICATIONS, and CALENDAR. A search bar is located on the right. The main content area features a "Celebrating 40 Years of Leadership" banner for "JUSTICE, PUBLIC SAFETY AND BEYOND" (1969-2009), a "Register Today! 2011 Winter Membership Meeting" button, and a "SEARCH News" section. A central "In the Spotlight" section highlights "SEARCH Offers High-Tech Crime Investigative Resources" with a "LEARN MORE" button. A "Quick Links" sidebar lists various resources like "CRIMINAL HISTORY RECORDS", "HIGH-TECH INVESTIGATIVE GUIDES", "IDENTITY THEFT", "ISP LIST", "JIEM® TOOL", "PODCASTS", "PUBLIC SAFETY ISSUE BRIEFS", "SEARCH INVESTIGATIVE TOOLBAR", "SEX OFFENDER REGISTRIES", and "SURVEYS". A video player is visible at the bottom of the spotlight section.



# Who We Are

**Lauren Wagner**

High-Tech Crime Training Specialist

lauren@search.org



# Who We Are

**Elizabeth Tow**

High-Tech Crime Training Specialist

elizabeth@search.org



# Portable Apps

<http://portableapps.com/>



- Can be run from USB Thumb Drive on any Windows computer
  - Little evidence of use left on computer hard drive
  - Forensic evidence typically located on thumb drive



# Portable Apps

- Can be an investigative tool
  - If you have no access to an undercover computer
  - If you have to use multiple computers as part of your job
  - If you have no other tools available to capture evidence, portable apps can be used as a **non-forensic** tool



# Portable Apps

- Allow you to configure applications to use on multiple computers
- Programs include:
  - Firefox
  - Exif Viewer
  - Command Prompt
  - MD5 Analyzer
  - Antivirus
  - Chat Program



# Portable Apps

- There is a full portable apps suite
  - <http://portableapps.com/download>
  
- OR you can download programs individually
  - <http://portableapps.com/apps>



# Sidenote - Viewing USB Devices

- You can access the registry to see what USB devices have been plugged into the computer
- Or programs are available that can more easily show what USB devices have been plugged into a computer
  - Helix
  - USBDeview



# Sidenote - USBDeview

- USBDeview is a free download
  - [http://download.cnet.com/USBDeview/3000-2094\\_4-10614190.html?tag=mncol](http://download.cnet.com/USBDeview/3000-2094_4-10614190.html?tag=mncol)
- Run on the computer in question to see list of USB Devices
- **May NOT be FORENSIC!!**

The screenshot shows the USBDeview application window with a menu bar (File, Edit, View, Options, Help) and a toolbar. The main area contains a table with the following data:

Device Name	Description	Device Type	Created Date	Connected
Port_#0001.Hub_#0002	TYM Flash Disk USB Device	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Apple iPod USB Device	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	USB Mass Storage Device	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Memorex TD Classic 003C US...	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Kingston DataTraveler 2.0 USB...	Mass Storage	7/6/2010 4:35:34 PM	No
Port_#0001.Hub_#0002	Kingston DataTraveler 2.0 USB...	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Kingston DataTraveler 2.0 USB...	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Kingston DataTraveler 2.0 USB...	Mass Storage	6/4/2010 4:59:18 PM	No
Port_#0001.Hub_#0002	WDC WD12 00VE-00KWT0 US...	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	Ut163 USB2FlashStorage USB ...	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	USB Device	Mass Storage	5/18/2010 11:12:34...	No
Port_#0001.Hub_#0002	USB Device	Mass Storage	5/18/2010 11:12:34...	No

At the bottom of the window, it shows "96 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net> usb.ids is not loaded".



# Portable Apps

- When you download a portable app, these are just the program files, the programs are not yet installed
  - You have to run the program files and install the programs individually
  - The thumb drives provided already have the apps installed and configured
  - If you want to add a new app to this thumb drive you will need to run the program files and install the programs individually



# Portable Apps Contents

- Audacity: audio editor and recorder
- ClamWin: antivirus
- CommandPrompt: link to a customizable command prompt
- Firefox: web browser
- FoxitReader: PDF reader



# Portable Apps Contents

- IrfanView: photo and image editor
- KVIrc: full-featured IRC chat client
- Lightscreen: screenshot tool
- OpenOffice: word processor, spreadsheet, presentations with Microsoft compatibility



# Portable Apps Contents

- Pidgin: chat with AOL, MSN and Yahoo users
- Skype: instant messaging, video chat and phone calls
- VLC: media player that plays most audio and video formats
- Visualizer Lite for Facebook and MySpace: Mapping tool that creates a visual representation of top friends



# Portable Firefox

- Allows user to run Firefox from USB Thumb Drive  
**[http://portableapps.com/apps/internet/firefox\\_portable](http://portableapps.com/apps/internet/firefox_portable)**
- Can personalize browser and use on various computers
  - Saves browsing history, cache & passwords to the thumb drive
  - Does NOT leave any trace of browsing history on computer



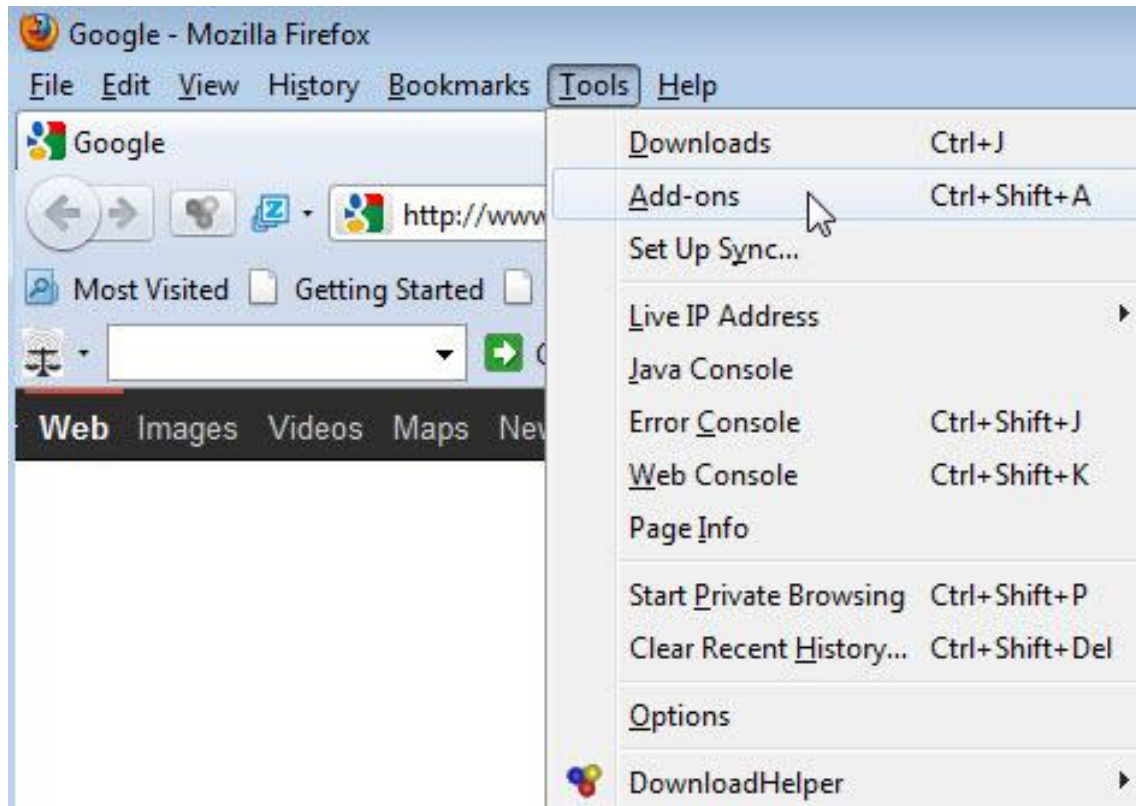
# Firefox Portable

- This firefox can be configured to run any add-ons that you want
- Some of the configuration settings may need to be changed to install the add-ons
  - For example, before the SEARCH Toolbar can be installed the cache in the browser needs to be increased



# Add-ons

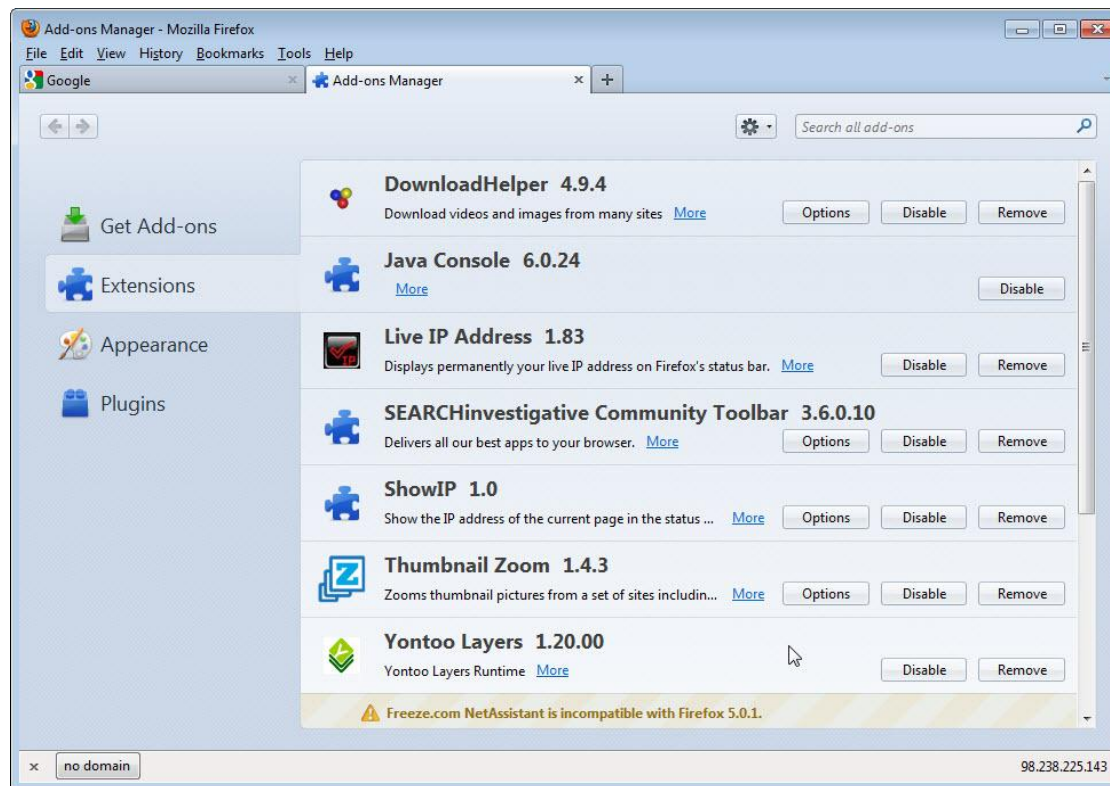
- To download Add-ons select 'Tools' then 'Add-ons'





# Add-ons

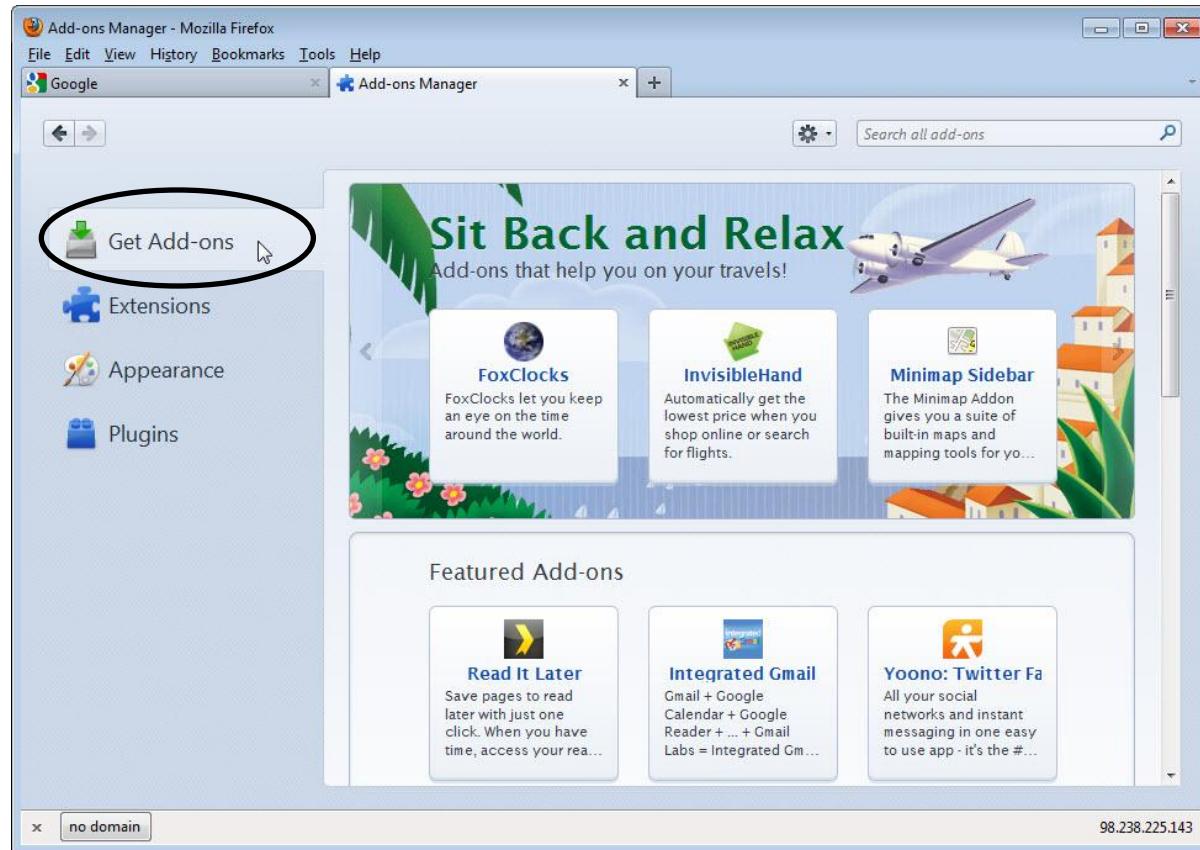
- A new tab with your current Extensions will open
- This is where you your current Extensions





# Add-ons

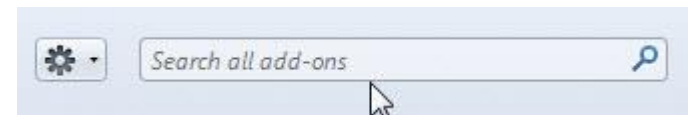
- Select 'Get Add-ons'





# Add-ons

- In the top right corner, type in the add-on you are searching for in the 'Search all add-ons' box and press 'Enter'





# Add-ons

- Choose the desired add-on and select 'Install'



- Once add-on is downloaded, select 'Restart now'





# Add-ons

- See SEARCH white paper for a list of helpful investigative add-ons
  - Linky
  - PrintPDF
  - Video DownloadHelper
  - Download Statusbar
  - Screengrab
  - Live IP Address
  - ShowIP
  - UnMHT
  - Thumbnail Zoom
  - Xmarks



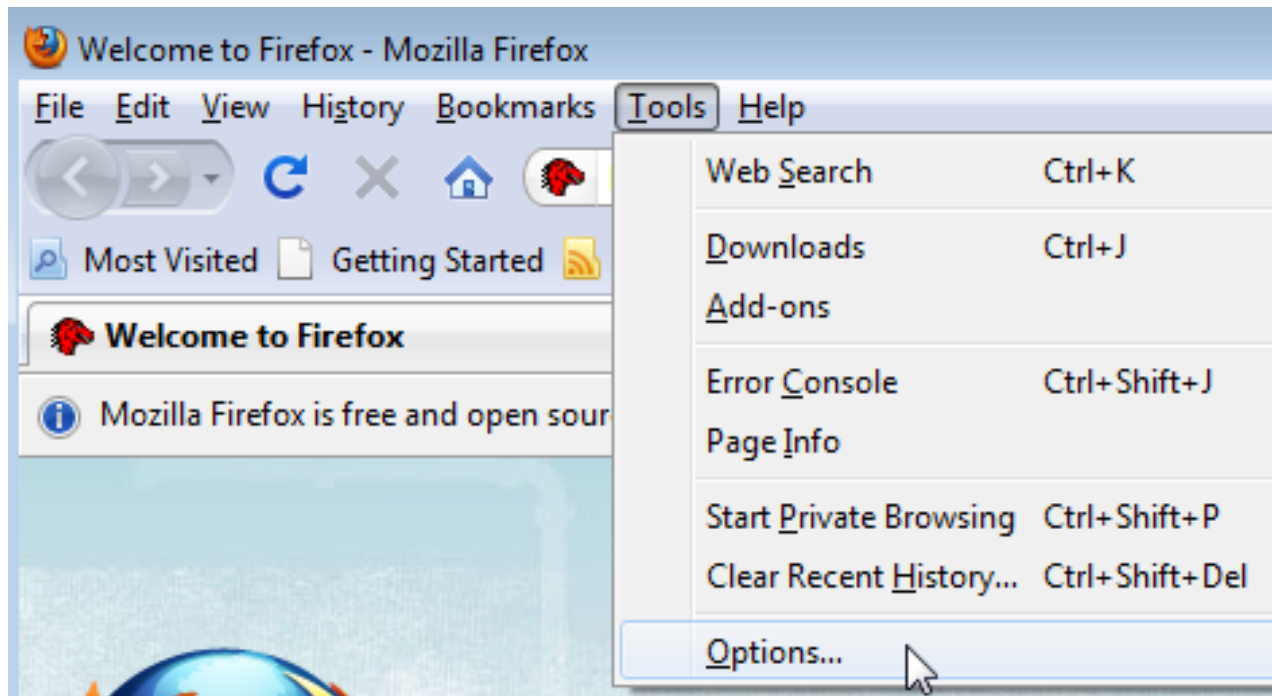
# Firefox Portable Exercise

**Install Firefox Add-on together**



# Firefox Portable

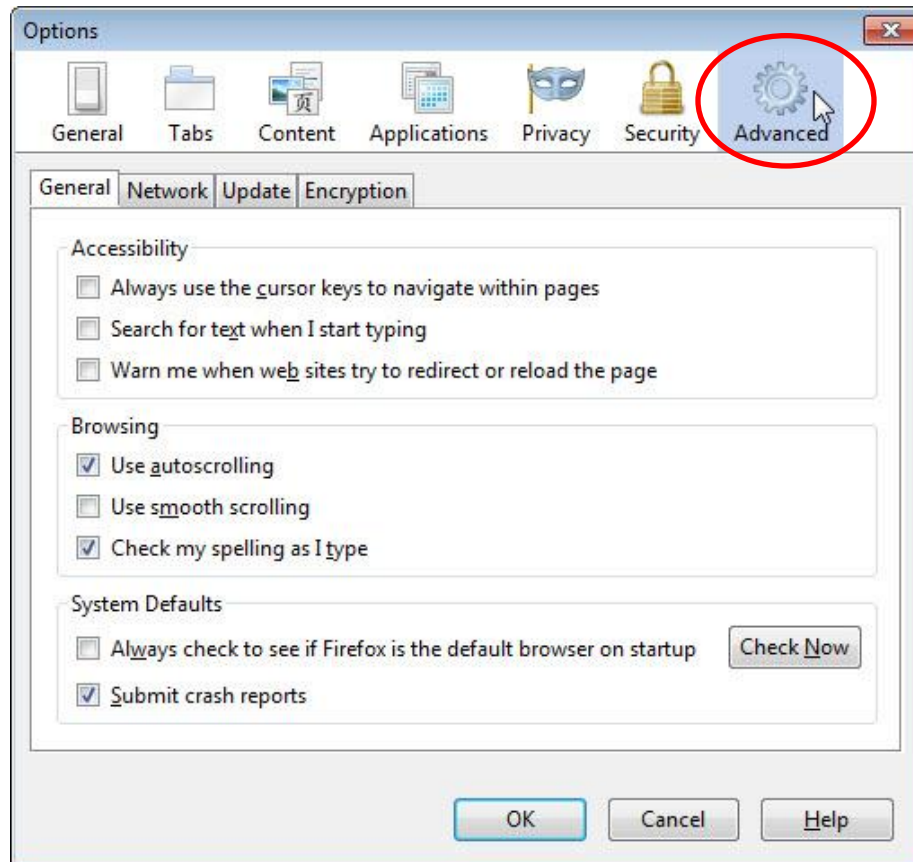
- Go to '**Tools**' and '**Options**'





# Firefox Portable

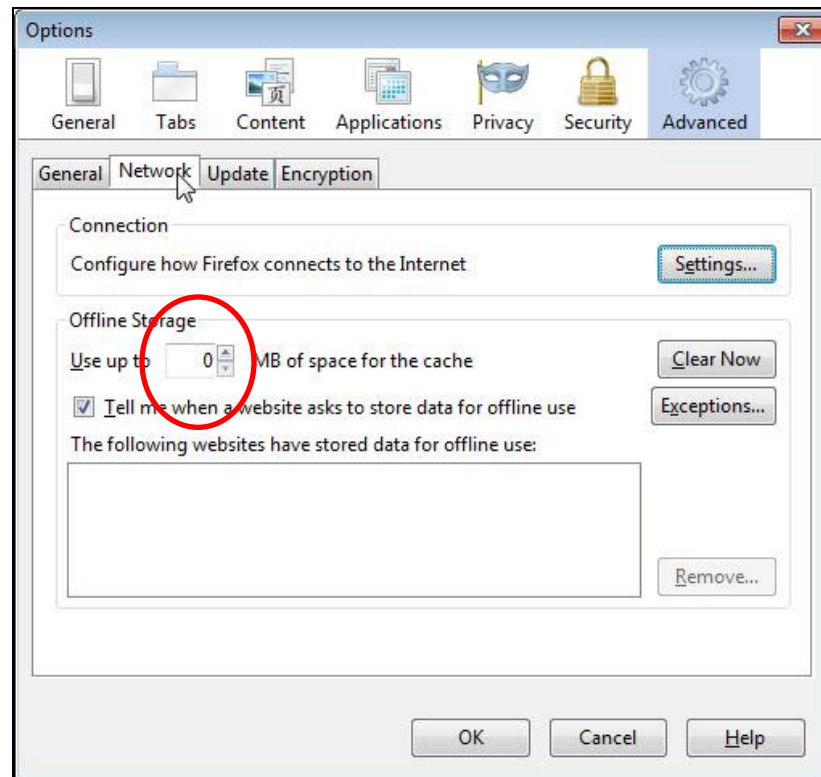
- Click on '**Advanced**'





# Firefox Portable

- Click on '**Network**'
- Increase the cache to 50 MB
- Click '**OK**'





# Sidebar - The SEARCH Toolbar

- Now you can install the SEARCH Toolbar
- The SEARCH Toolbar will assist you in your investigations
- Free download from  
**[www.searchinvestigative.ourtoolbar.com](http://www.searchinvestigative.ourtoolbar.com)**





# IrfanView Portable

- IrfanView is an image viewing and manipulation program
- IrfanView will also allow you to view exif data on images





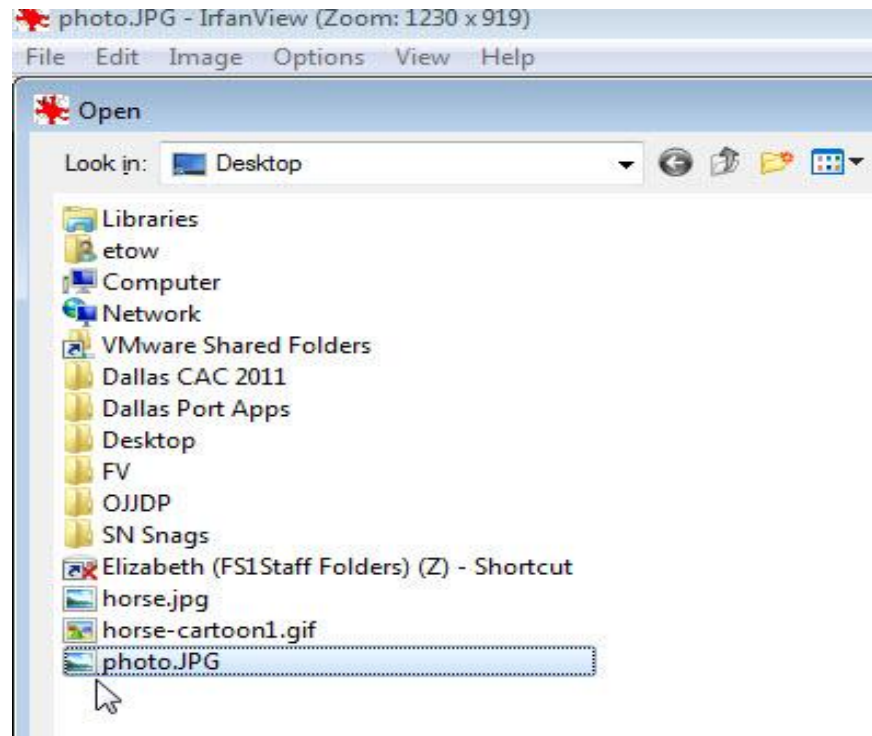
# Viewing Exif

- Exif data is information embedded in photographs by the device taking the picture
- May contain:
  - Make/model of camera
  - Serial number of camera
  - Creation time and date
  - GPS coordinates where photo was taken
- To view exif data you need a specialized viewer; IrfanView is installed on the portable apps thumb drive



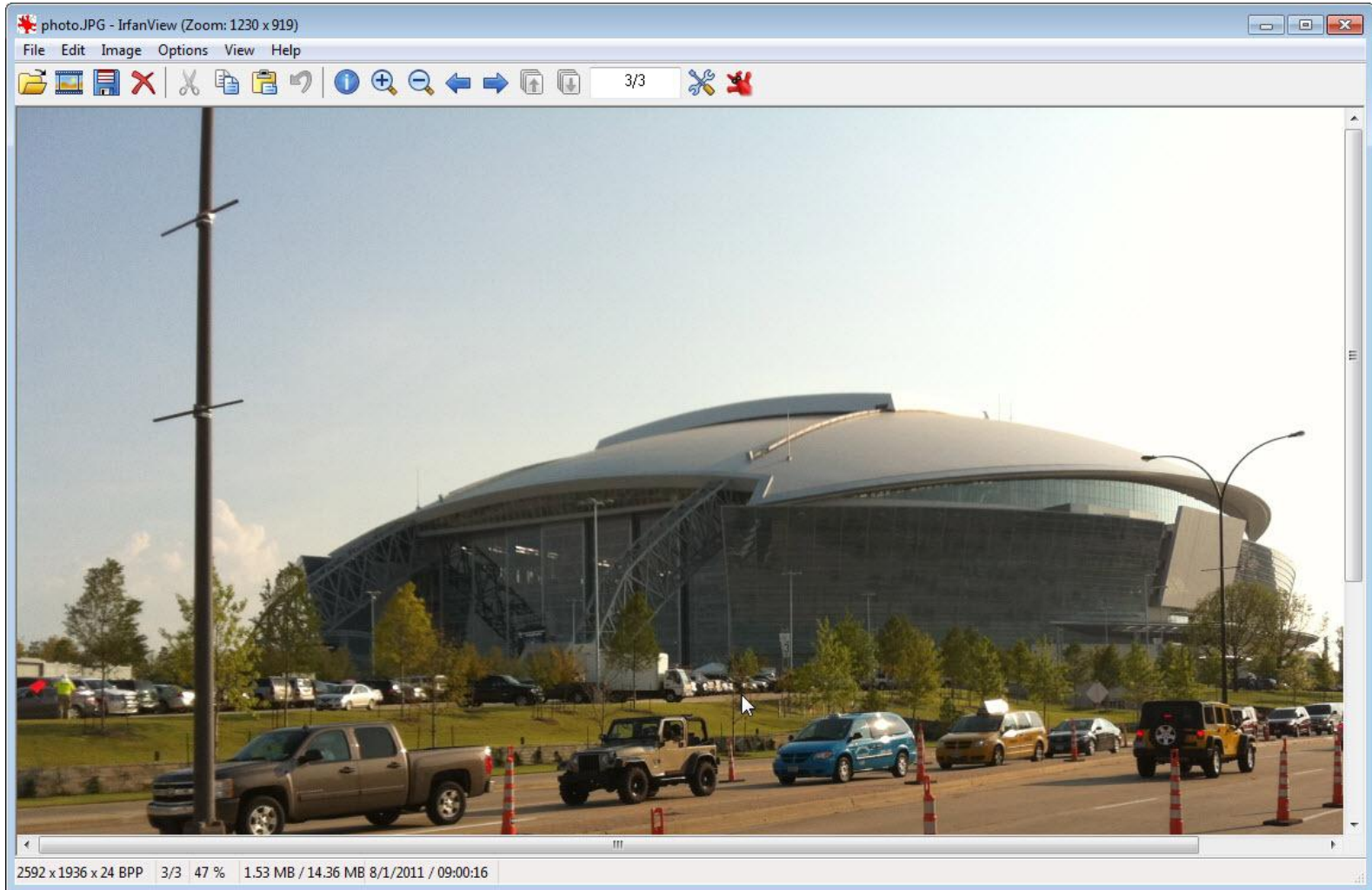
# Viewing Exif

- To view exif data
  - Open IrfanView Portable
  - Open '**File**' and select the image





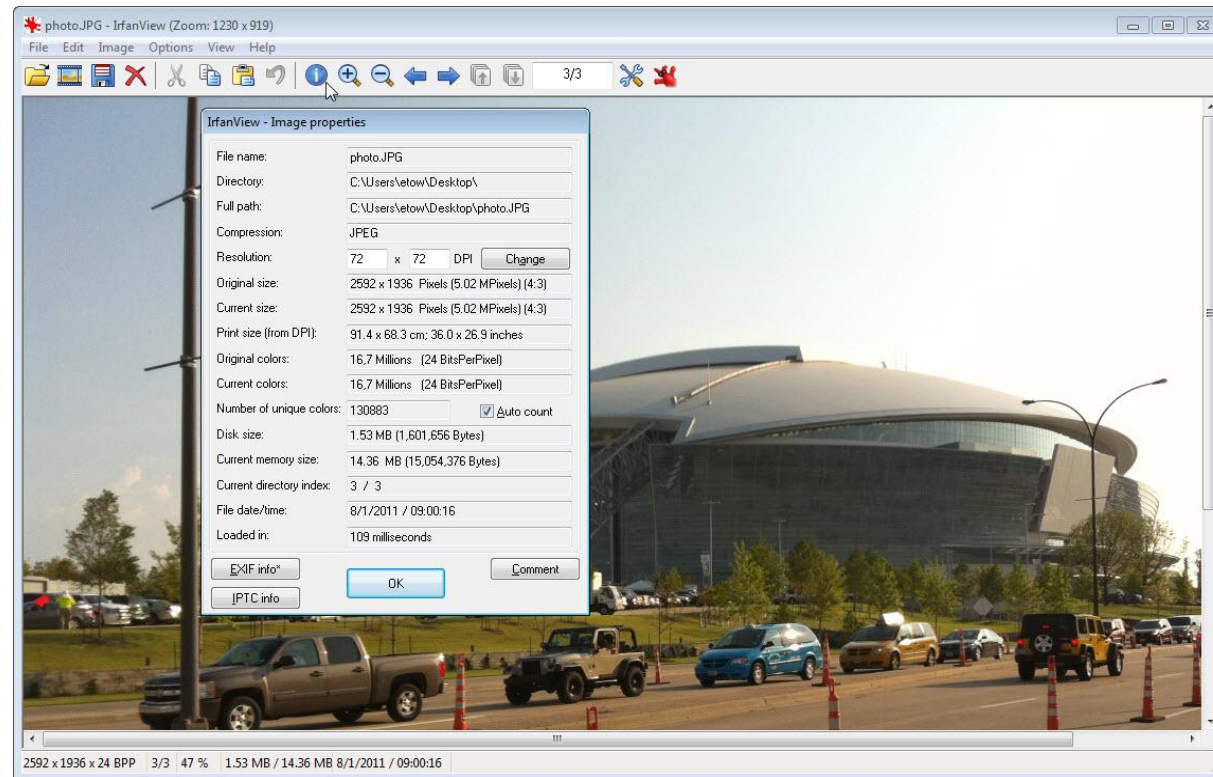
# Viewing Exif





# Viewing Exif

- To view exif data
  - Left click on '**Image Information**'
  - Keyboard shortcut is Ctrl + I



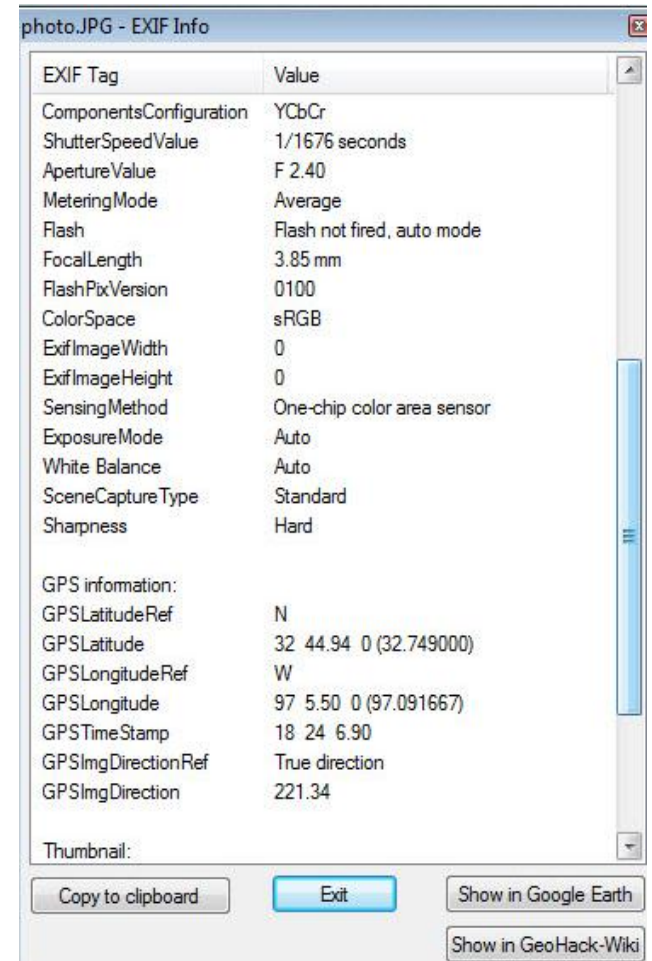


# Viewing Exif

- To view exif data
  - Click '**EXIF info\***'
  - Keyboard shortcut Ctrl + E

To view the picture's longitude and latitude on a map

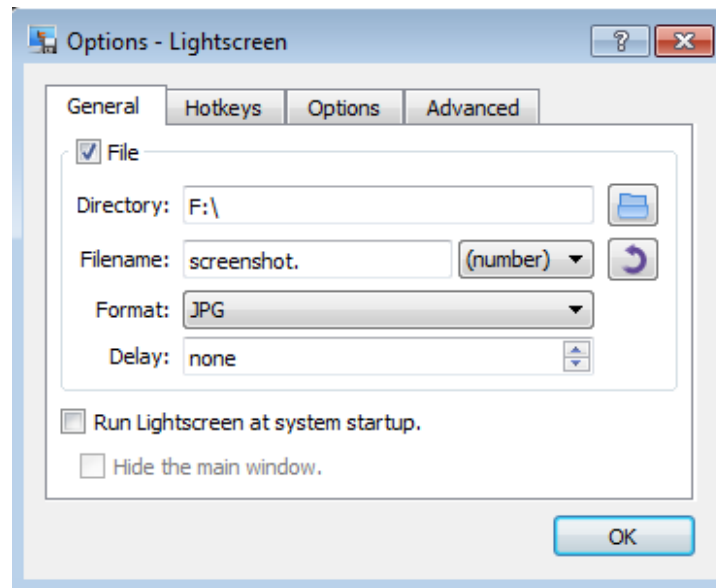
- Click '**Show in GeoHack-Wiki**'





# Lightscreen Portable

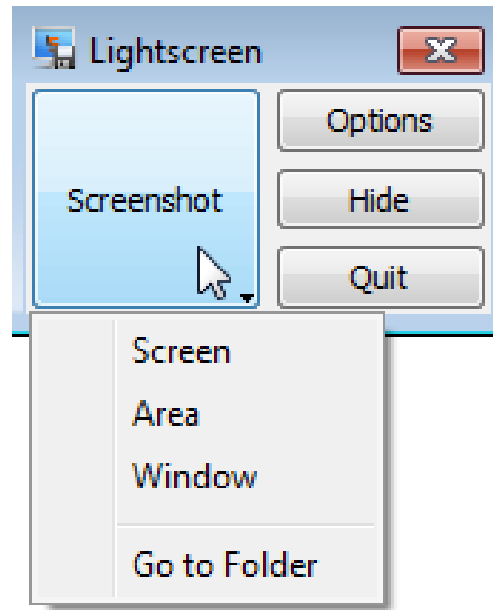
- After Lightscreen is installed, open **LightscreenPortable.exe** from the **LightScreenPortable** folder
- A new window will open to specify output and other configuration options





# Lightscreen Portable

- After settings are set the capture screen will open
- Click '**Screenshot**' to make a capture and select what you want to capture





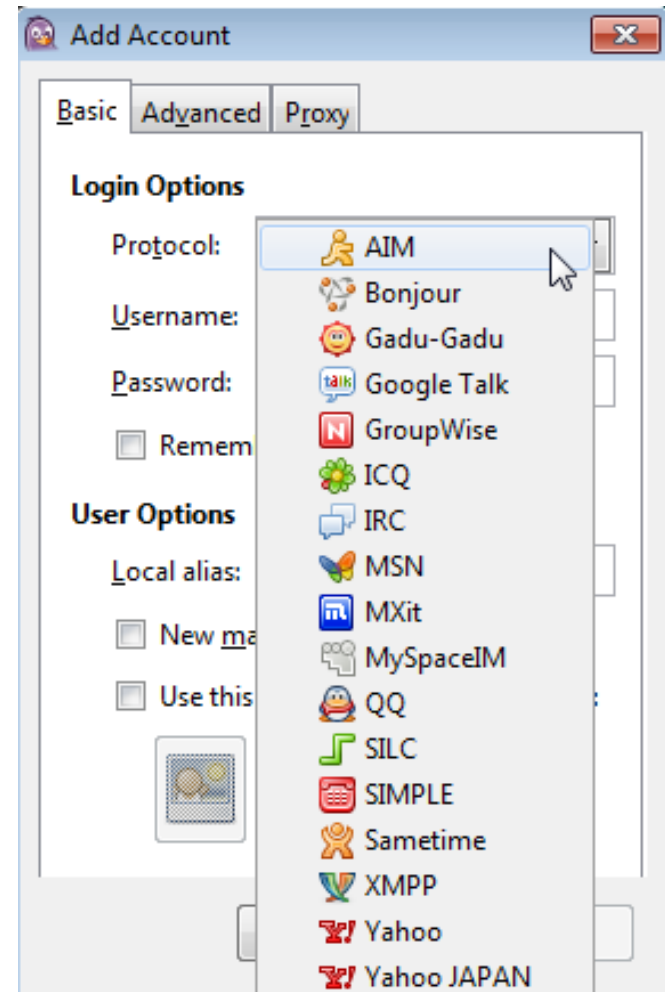
# Chatting with Portable Apps

- Portable Apps has multiple chat programs
- This PPT will show you how to set-up and configure them but will not teach you how to properly conduct undercover chat investigations



# Pidgin Portable

- Pidgin is a chat client that allows you to chat with multiple different accounts at the same time
- Also will allow multiple screen names from a single client





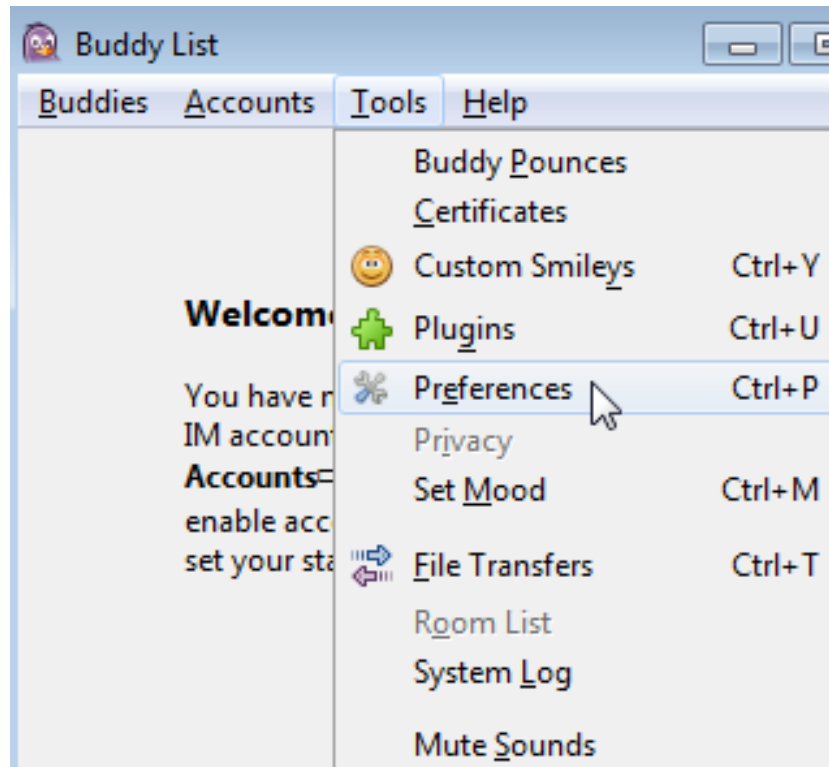
# Pidgin Portable

- Logging is critical
- Make sure that logging is configured before starting any chats
- By default logging is on, but it is always a good idea to double check prior to starting any type of investigative chat



# Pidgin Portable

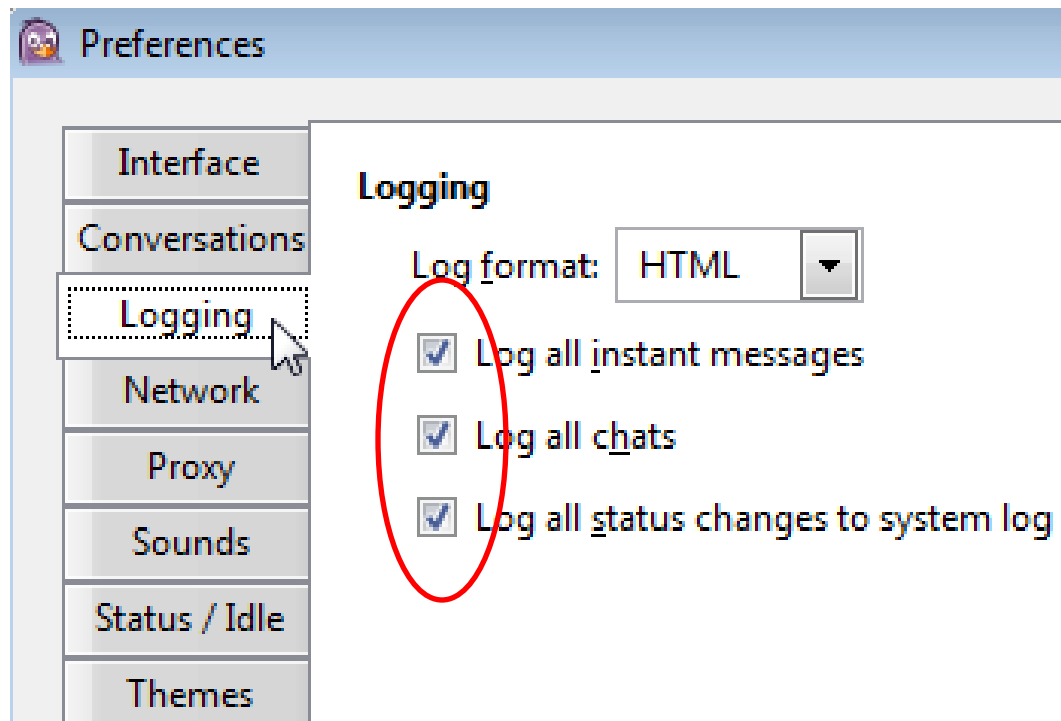
- Click on '**Tools**' then '**Preferences**'





# Pidgin Portable

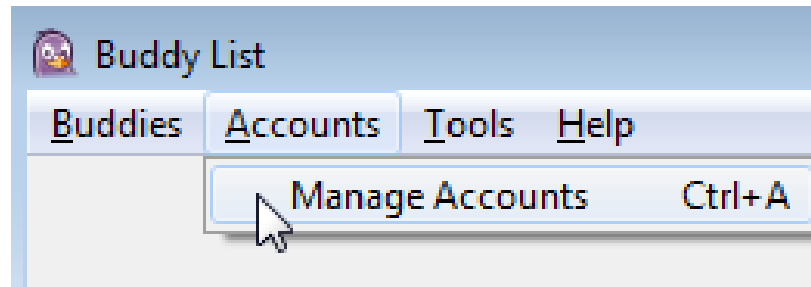
- Click on '**Logging**'
- Make sure all 3 boxes are checked





# Pidgin Portable

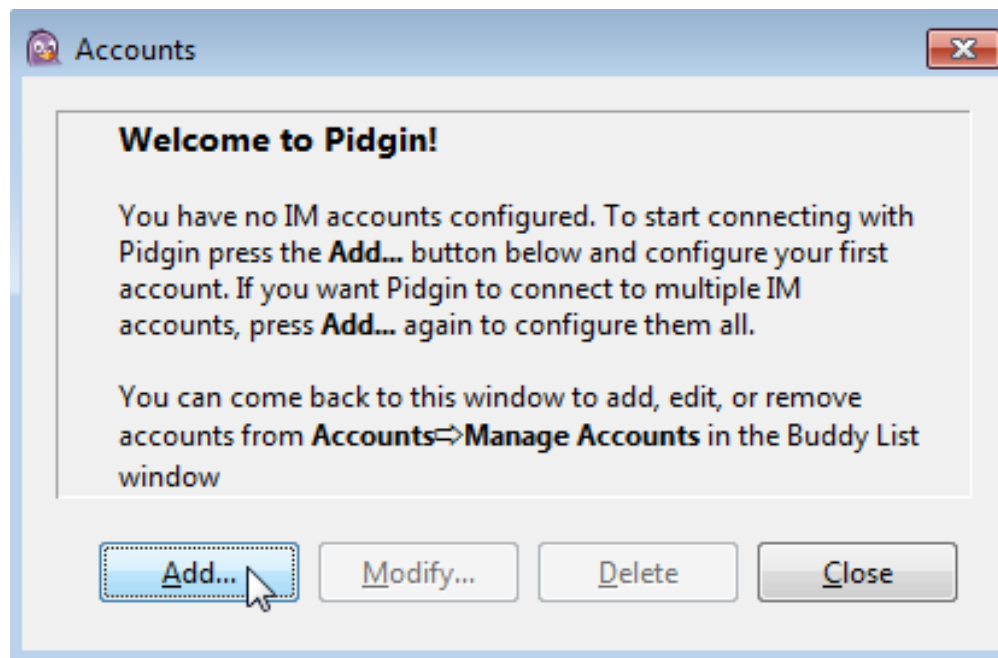
- Add accounts by going to '**Accounts**' then '**Manage Accounts**'





# Pidgin Portable

- Click on '**Add**'





# Pidgin Portable

- Enter account information

**Add Account**

Basic | Advanced | Proxy

**Login Options**

Protocol: Yahoo

Username: Yahoo ID...

Password:


Remember password

**User Options**

Local alias:

New mail notifications

Use this buddy icon for this account:

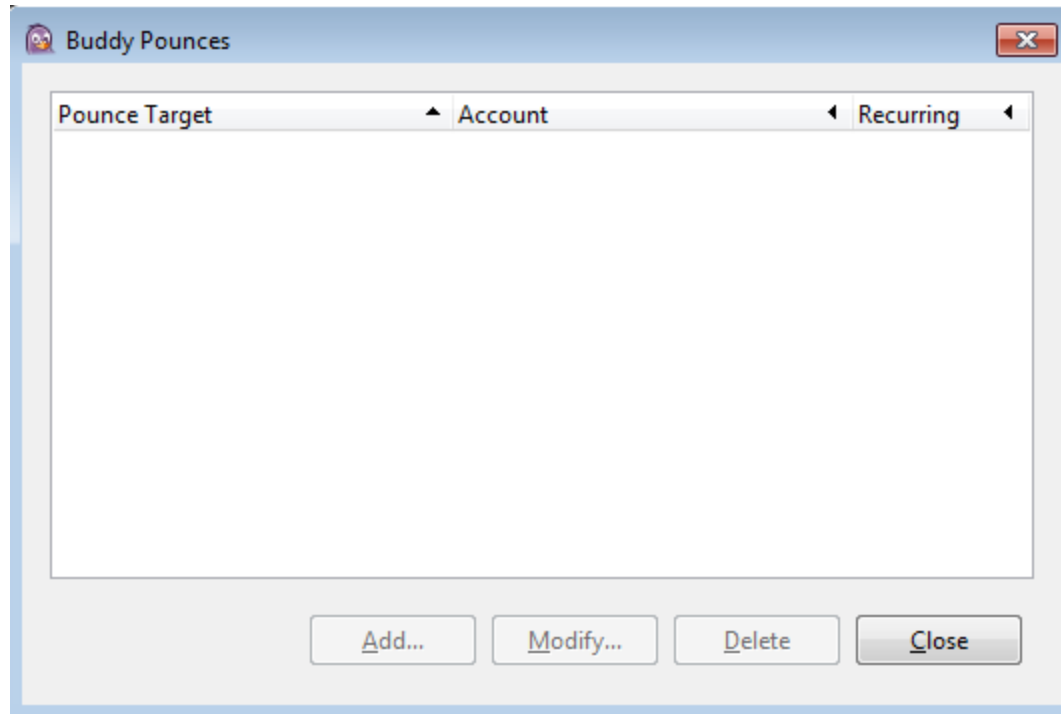
 Remove

Cancel Add



# Buddy Pounce

- Also allows you the ability to “pounce”
- Good for keeping track of suspects online chat behavior





# Buddy Pounce Options

**Add Buddy Pounce**

**Pounce on Whom**

Account:  ▼

Buddy name:

**Pounce When Buddy...**

Sends a message    Goes away    Is no longer idle    Stops typing

Signs on    Returns from away    Starts typing

Signs off    Becomes idle    Pauses while typing

**Action**

Open an IM window

Pop up a notification

Send a message

Font    Insert    Smile!    Attention!

Execute a command

Play a sound

**Options**

Pounce only when my status is not Available

Recurring



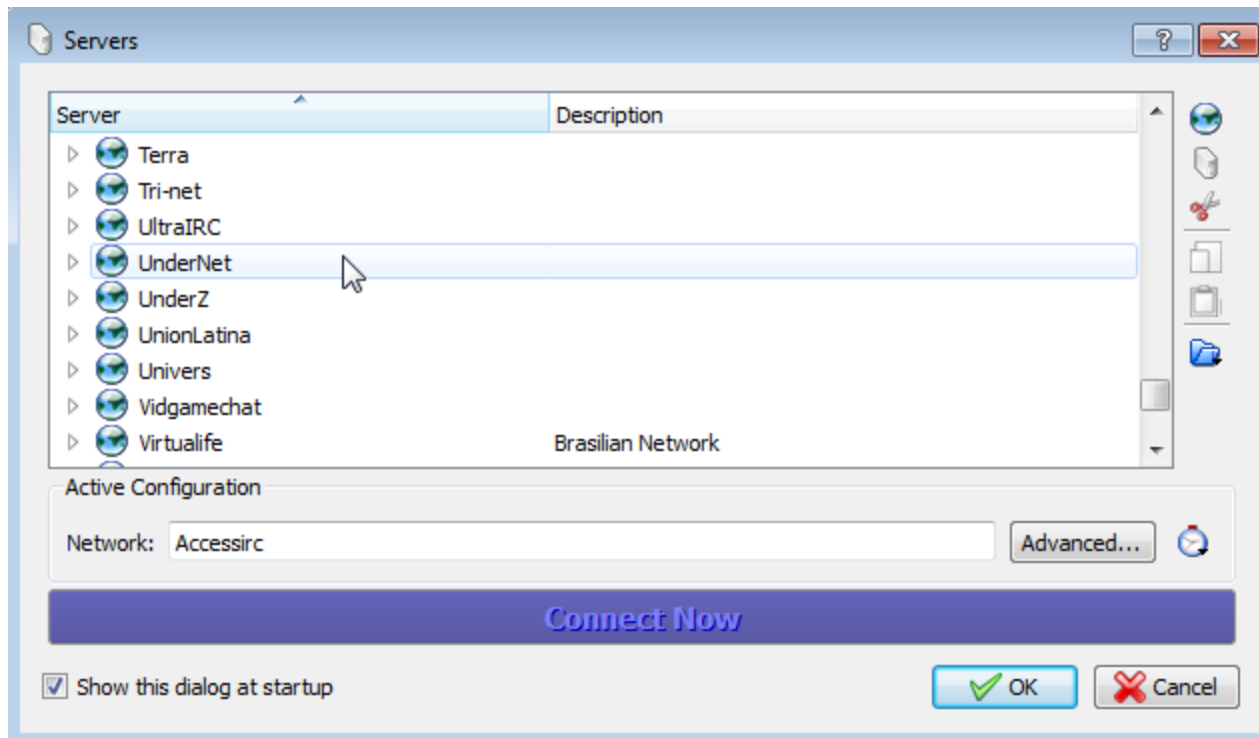
# KVIrc Portable

- Portable IRC client
- This PPT will show you how to set-up and configure them but will not teach you how to properly conduct undercover chat investigations



# KVirc Portable

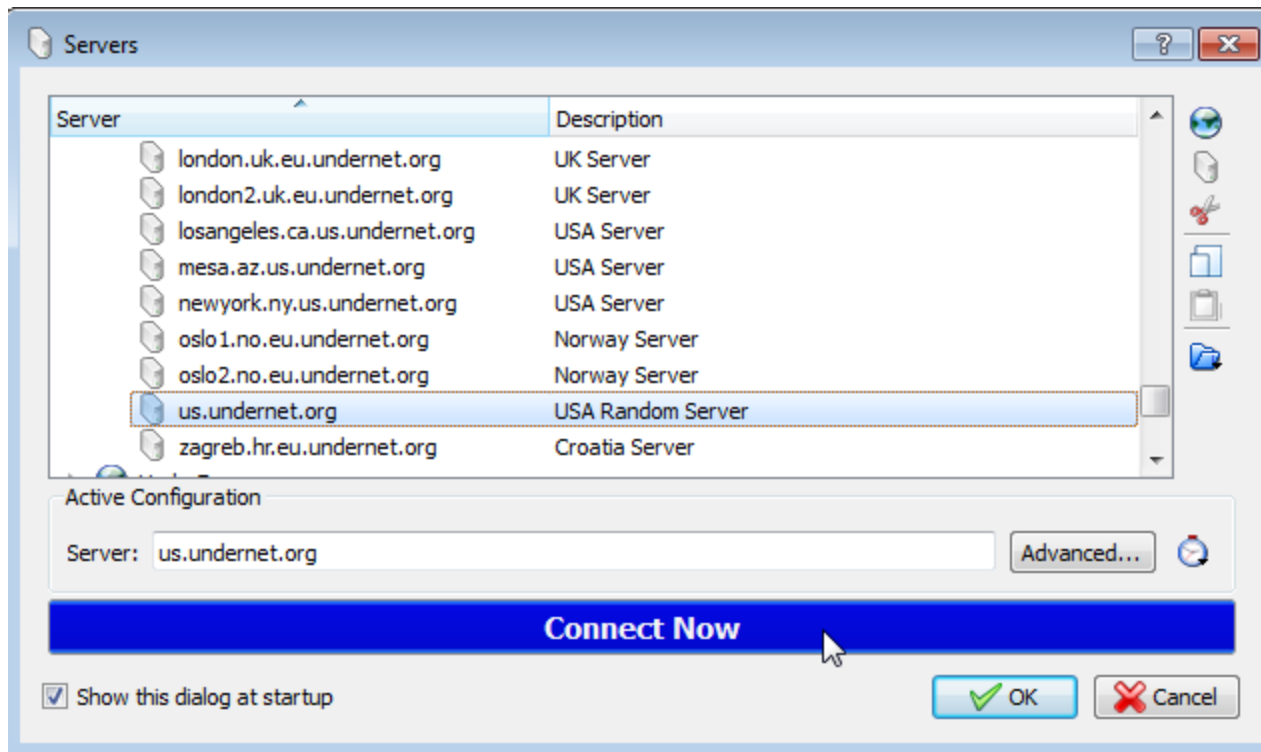
- Connect to UnderNet





# KVirc Portable

- Connect to USA Random Server





# KVirc Portable

- Enter account information

Server Details

irc://losangeles.ca.us.undernet.org:6667

Description: USA Server

Identity Connection Join Channels On Connect On Login Advanced

Properties

Username: cheerluv13

Password:

Nickname: cheerluv13

Real name:

User Mode

Use default user mode

Invisible (+)

Server notices (+s)

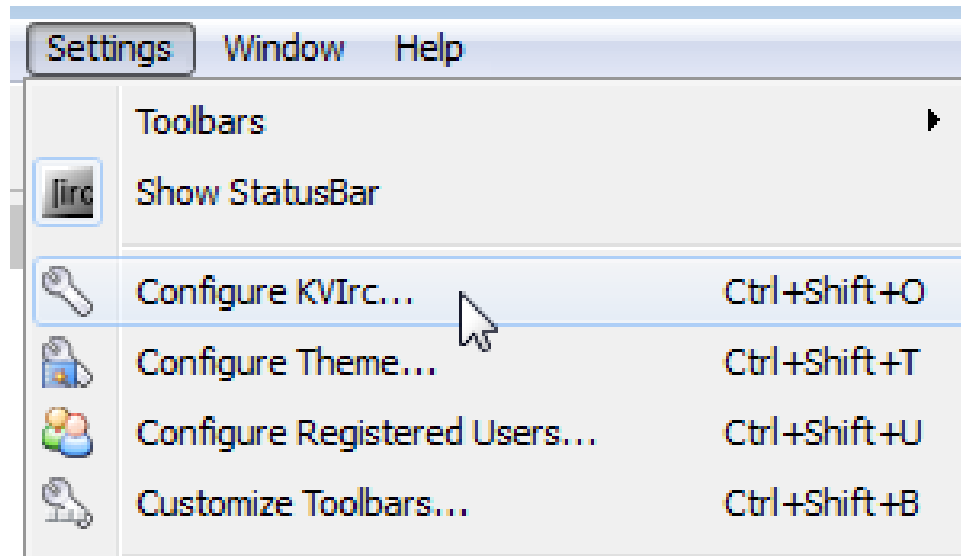
Wallops (+w)

OK Cancel



# KVirc Portable

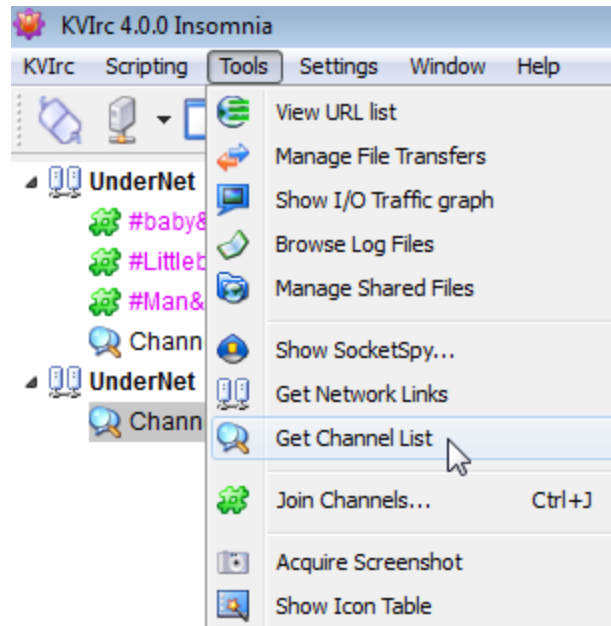
- Configure KVirc settings





# KVirc Portable

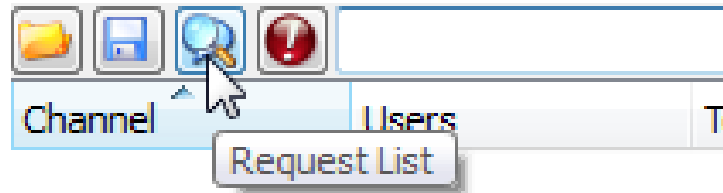
- Get the channel list





# KVIrc Portable

- Click on '**Request List**' to get the full channel list





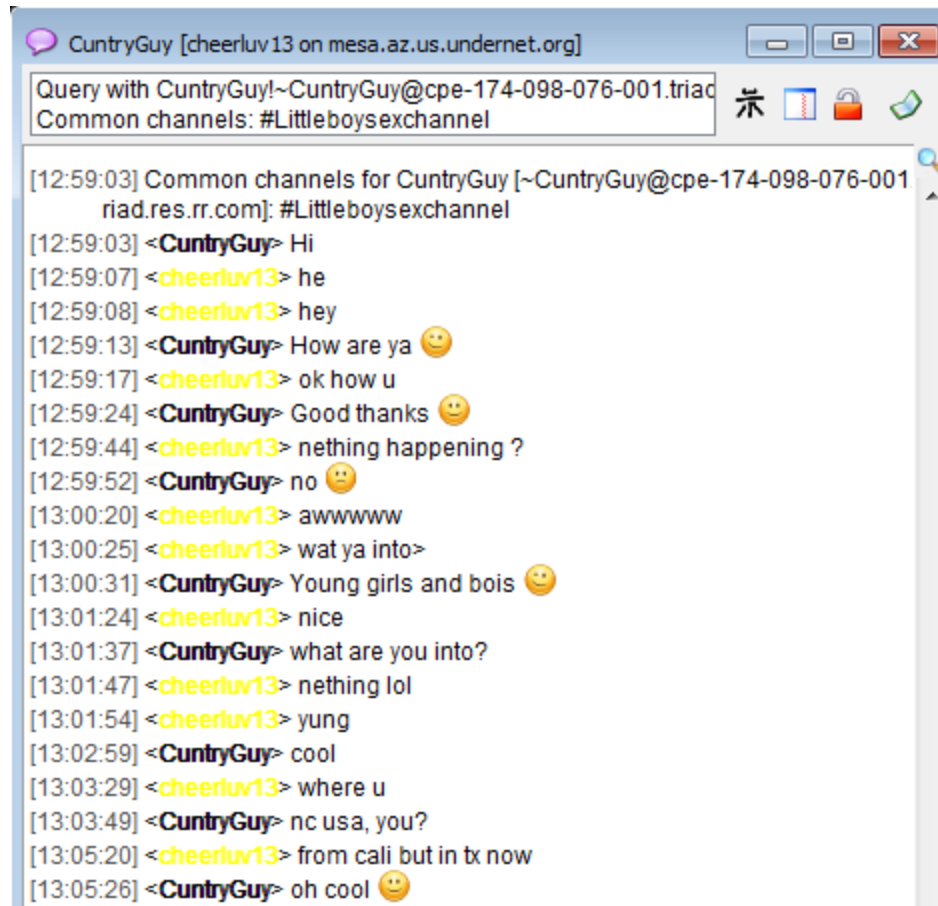
# KVirc Portable

Channel List [IRC Context 2] Connected to Montreal.QC.CA.Undernet.org (UnderNet)

Channel	Users	Topic
#!!!!pedosnuffs	2	
#!Pedotoiletsex	1	
#0!!!!!!!!pedor	97	
#00000pedo	1	
#animalsex	4	Free and open chat   No pedos!!   <a href="http://www.zoophile.net">http://www.zoophile.net</a>
#Nudism	39	NO familysex/incest/pedo/animal/rape type co-channels and no under 18 nicks
#Boysexroleplay	23	Welcome to your play time planet in our pedo galaxy ! Relax and roleplay :-)
#pedophilia	8	\\elcome ;) ( <a href="http://motherless.com/">http://motherless.com/</a> )
#baby&toddlerlo	45	Your naughty nursery fantasy chat ! For more planets in our pedo galaxy go to #Man&Boy4Chat_Uncensored
#Man&Boy4Chat	36	BOYS & BL's WELCOME TO YOUR FANTASY SEX CHAT IN OUR PEDO GALAXY ! For another pedo planet, click on
#masturbation	75	Enjoy Yourself. 16+, NO incest, kiddie/pedo or animal co-channeling, No URL's, 1 hour between repeats, English Only,Be Respectful.
#Littleboysexcha	49	Welcome to fantasy sex chat ! BL's find boys undies are always 1/2 off ! Join our pedo galaxy.
#femslavesex&C	3	18+BDSM Exotic Life Style Room of Domination & submission:SS&C Leads To Great Fun And Trivia:No Trolling,Pedo,Familysex or Sr
#NudeBeach	13	Welcome to Nude Beach! For Nudists, naturists, and interested folks! No Pedos,Force, BDSM channels- 16+.
#boylovers_into	36	Welcome Boylovers into Boylovers ! Wherever you go, here you are ! Please put your pedo cock in the upright and locked position
#toiletsex	18	Urination, Defecation, conversation, recreation... Don't be a Pedo, poser, dogsexer, loser, Romanian with scars or just annoying
#Honkey_Tonk_f	2	
#I_AM_A_REAL_	8	
#sexforlove	15	All lang only, NO pedo/cam/pics ads.NO vulgarity. Enjoy yourself! ( <a href="http://www.youporn.com">www.youporn.com</a> )
#bifemsex	49	18+ english in the channel please no cut/paste/urls no trolling or repeating no incest/pedo channels allowed gentlemen welcome
#familysex	66	English&16+ only,NO pedo/cam/pics ads.NO vulgarity.Be Polite. Enjoy yourself! For complete rules, please visit our website: <a href="http://www.youporn.com">http://www.youporn.com</a>
#pedophilia.	1	
#snuffsex	29	No pedo co-chaneling! Snuff FANTASY only-no limit, no real. Adult only-18+.



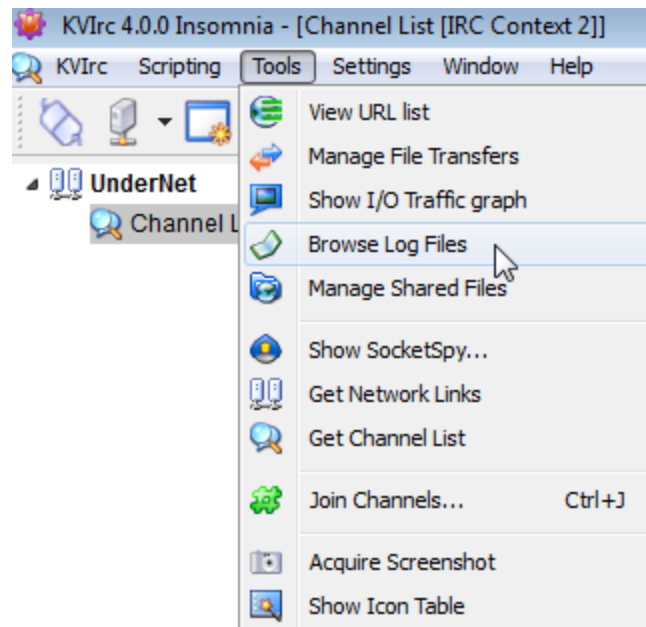
# KVIrc Portable





# KVirc Portable Logs

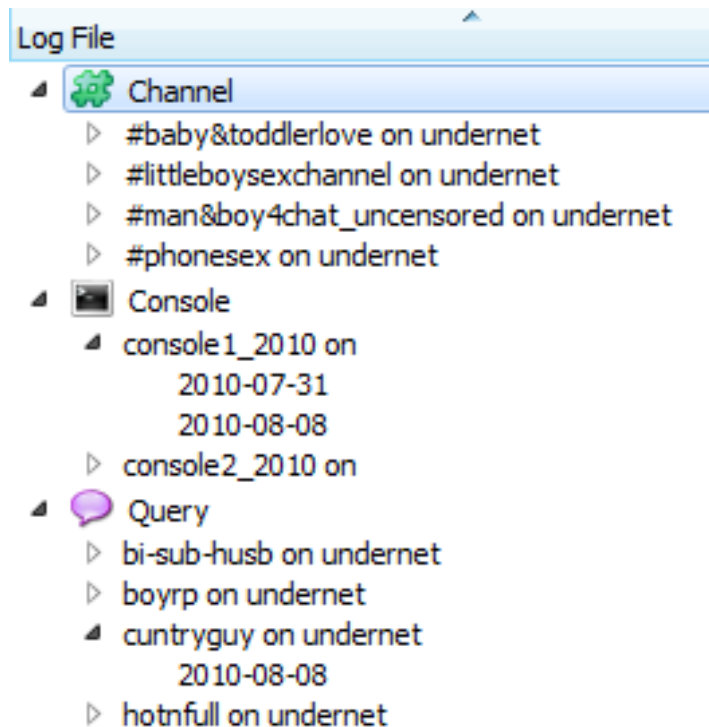
- Click on '**Tools**' then '**Browse Log Files**' to view logs





# KVIrc Portable Logs

- Logs do not display until the chat is closed
- Logs need to be refreshed for newest data





# KVIrc Portable

- Console log – showing WHOIS information

```
[13:00:33] CuntryGuy is CuntryGuy!~CuntryGuy@cpe-174-098-076-001.triad.res.rr.com
[13:00:33] CuntryGuy's real name: Drew
[13:00:33] CuntryGuy's channels: #Boysroleplay, #Littleboysexchannel, #gaydads4sons, #0!!!!!!!Kids'R'us, #0!!!!!!!Itlgirlsexchat, #0!!!!!!!younggirlsex, #0!!!!
!dad&daughtersex, #0!!!!!!!girlswhosuckcock
[13:00:33] CuntryGuy's server: *.undernet.org - The Undernet Underworld
[13:00:33] cuntryguy WHOIS info from mesa.az.us.undernet.org
[13:02:31] Looking up host cpe-174-098-076-001.triad.res.rr.com...
[13:02:31] DNS Lookup result for query "cpe-174-098-076-001.triad.res.rr.com"
[13:02:31] Hostname 1: cpe-174-098-076-001.triad.res.rr.com
[13:02:31] IP address 1: 174.98.76.1
[13:03:01] CTCP PING request from hotNfull [~nick9@251-221-137-216.mtaonline.net] (PING 1281297807), replied
```



# Questions



# Thank you

**lauren@search.org**

**elizabeth@search.org**