Interface Design for Hacking Tools

Greg Conti

original image: http://www.daveyandgoliath.org/

Disclaimer

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.

image: http://www.leavenworth.army.mil/usdb/standard%20products/vtdefault.htm

Outline

- Introduction
- Command Line vs. GUI's
- Task, User, & Technology
- Principles of Design
- GUI Components
- Critique of Tools
- Pointers
- Q&A

image: http://www.uk-anime.net/fanart/large/cloud.jpg by Jim Evans

What is an Interface?

"The point of interaction or communication between a computer and any other entity, such as a printer or human operator."

source: http://dictionary.reference.com/search?q=interface

What is an Interface?

"The way that you accomplish tasks with a product and how it responds – that's the interface."

Command Line vs. GUI

- Flexibility
- Time
- Ease of use
- Best for heavy users

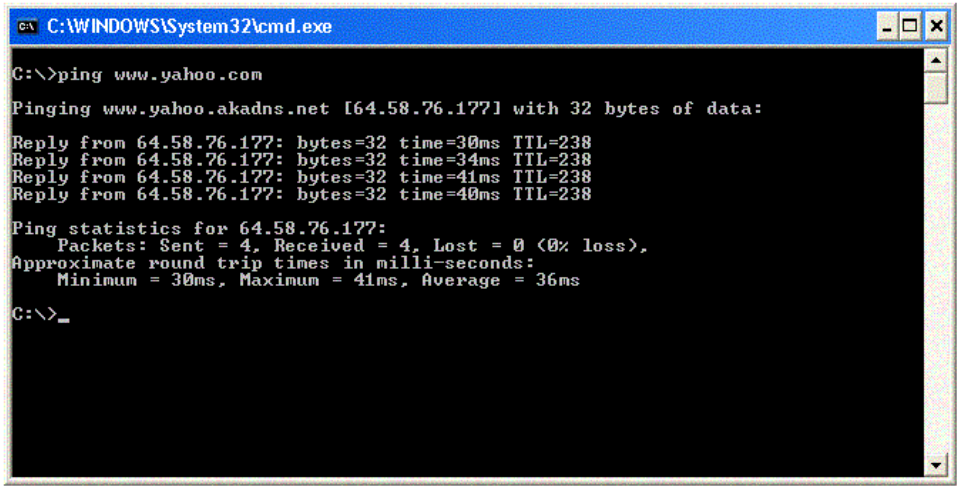


image: http://helpdesk.princeton.edu/images/ping.gif

source: http://www.jpeek.com/talks/svlug_19991103/020.html

Crack in One Line of Perl

```
perl -nle 'setpwent;crypt($_,$c)eq$c&&print"$u $_"while($u,$c)=getpwent'
```

Author: Alec Muffett

Several Lines of Perl Can Crack DVD Encryption

```
#!/usr/bin/perl
# 472-byte qrpff, Keith Winstein and Marc Horowitz <sipb-iap-dvd@mit.edu>
# MPEG 2 PS VOB file -> descrambled output on stdout.
# usage: perl -I <k1>:<k2>:<k3>:<k4>:<k5> qrpff
# where k1..k5 are the title key bytes in least to most-significant order

s''$/=\2048;while(<>){G=29;R=142;if((@a=unqT="C*",_)[20]&48){D=89;_=unqb24,qT,@
b=map{ord qB8,unqb8,qT,_^$a[--D]}@INC;s/...$/1$&/;Q=unqV,qb25,_;H=73;O=$b[4]<<9
|256|$b[3];Q=Q>>8^(P=(E=255)&(Q>>12^Q>>4^Q/8^Q))<<17,O=O>>8^(E&(F=(S=O>>14&7^O)
^S*8^S<<6))<<9,_=(map{U=_%16orE^=R^=110&(S=(unqT,"\xb\ntd\xbz\x14d")[_/16%8]);E
^=(72,@z=(64,72,G^=12*(U-2?0:S&17)),H^=_%64?12:0,@z)[_%8]}(16..271))[_]^((D>>=8
)+=P+(~F&E))for@a[128..$#a]}print+qT,@a}';
```

Authors: Keith Winstein and Marc Horowitz
Original source: http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/qrpff.pl
*Note that code above is not complete

Foundations...

- Tasks
- Users
- Technology

image: www.amazon.com

Understanding Tasks

What tasks are your users trying to accomplish?

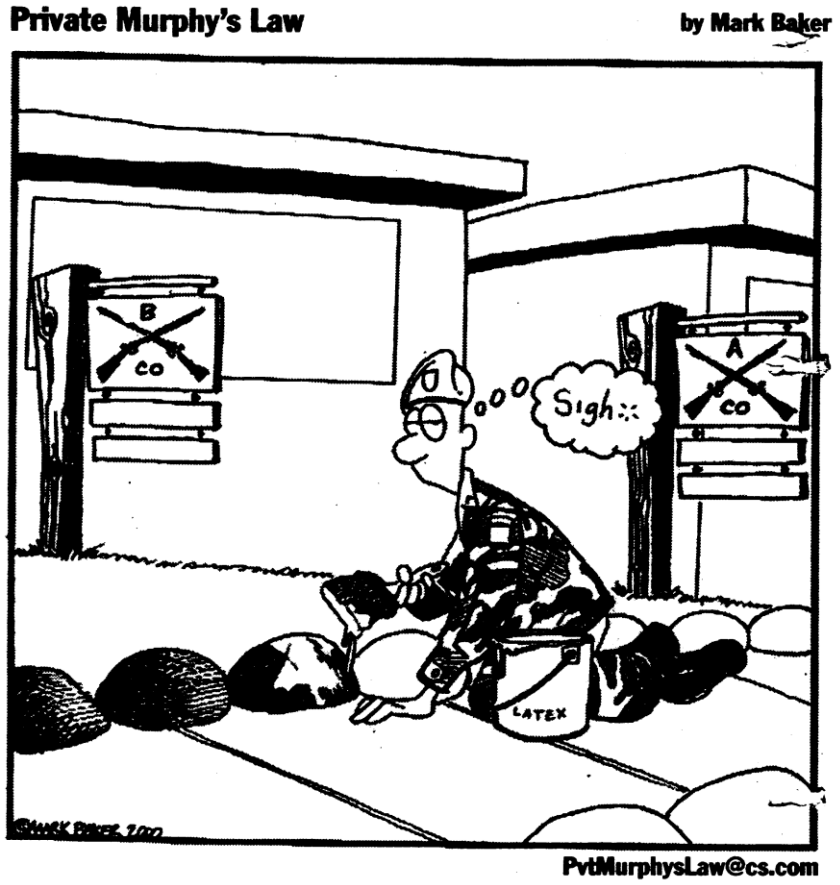


image: http://www.pvtmurphy.com, used with permission

Who are your users?

image: http://www.noderunner.net/~sparks/art/tara.gif by Rachel Blackman, used with permission

Your Users may be Beginners…

"Ok I know i'm very slow, stupid too maybe….I can't see a damn thing execpt the poster's e-mail address …. I am new to computers and am trying to learn what I can so please be gentle."

- alt.2600.hackersz

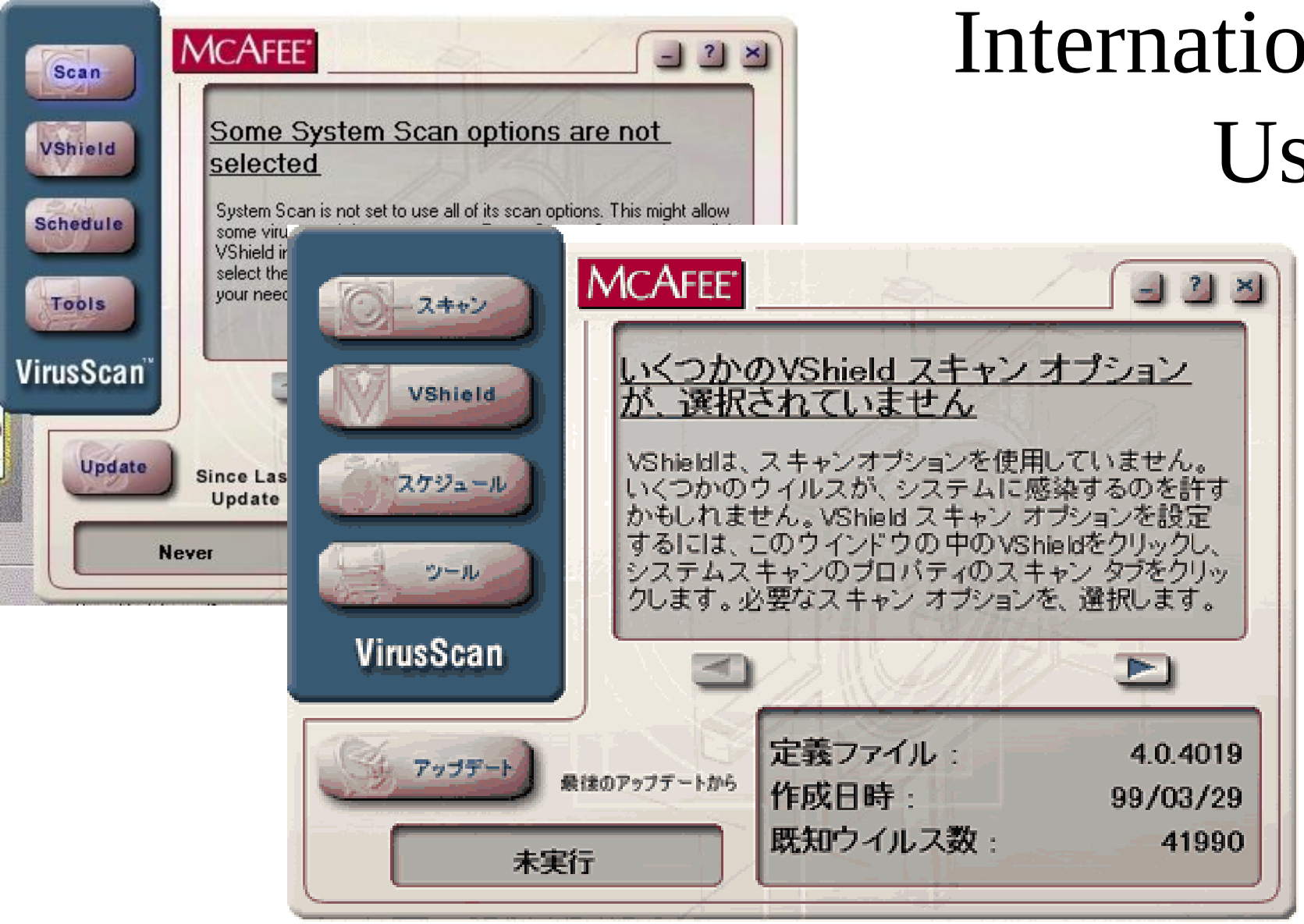
source: alt.2600.hackersz

Advanced…

"From your questions, it seems you are over-simplifying just what a dissassembler can do for you. If you are not an experienced assembly language programmer then the dissassembled file will look like Greek"

- alt.2600.hackersz

International Users



McAfee VirusScan can be found at www.mcafee.com
Image (English): http://www.evergreen.edu/support/how_to/virus/mcafee_update/imageNU2.JPG
Image (Japanese): http://dekiru.impress.co.jp/net/mcafee/img/mcafee.gif

Enabling Technology

Analyze the task and your users first.

The proper technology follows.

image: http://is.cgu.edu/pcmuseum/images/TRS-80%20front.jpg by Dionna Harris and Paul Gray, used with permission

Principles of Design

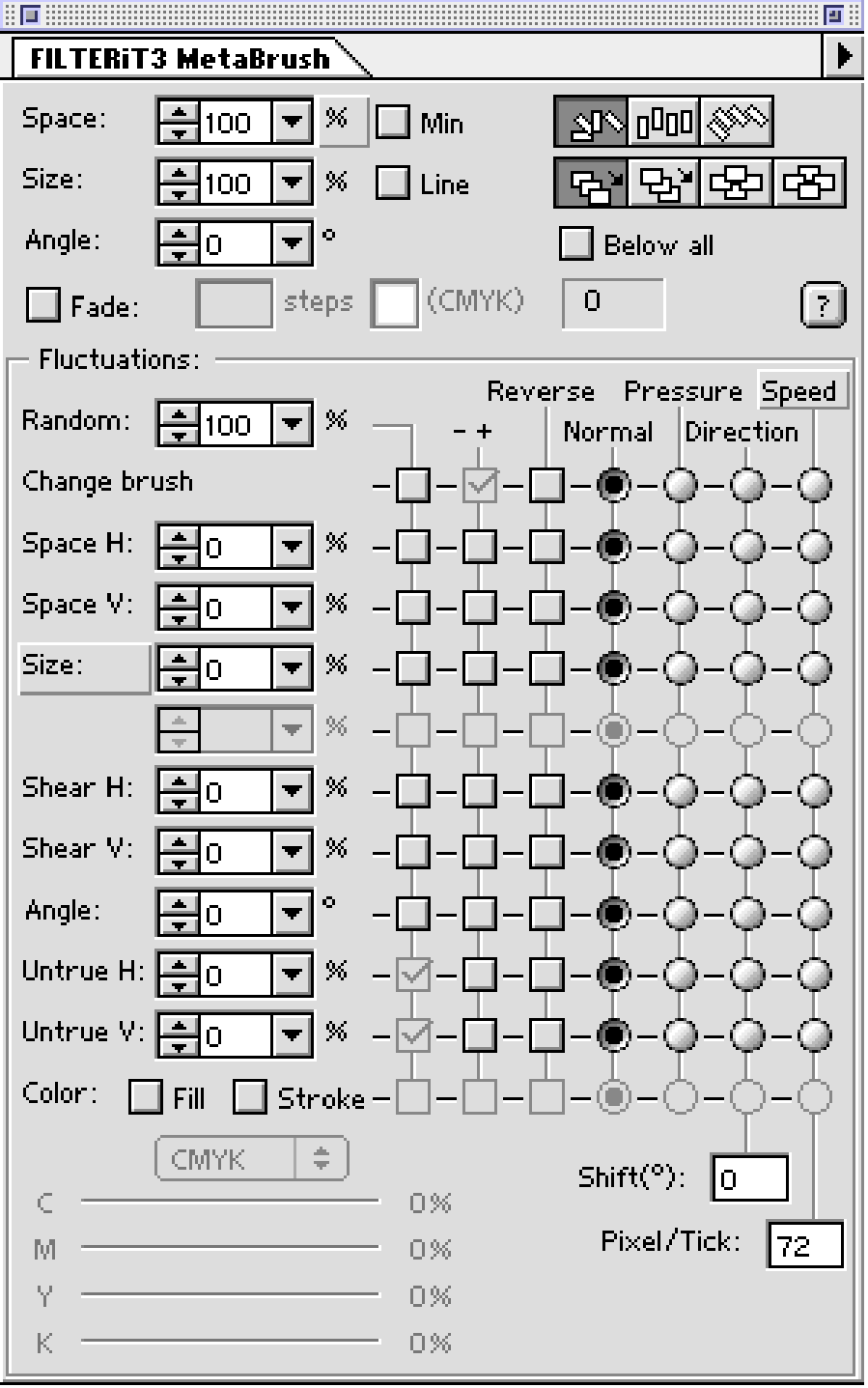
- Cognitive Science
- Design for Clarity
- Navigation
- Color
- Fonts
- Metaphor
- Consistency
- Feedback
- Testing
- Information Display and Visualization

image: http://www.uk-anime.net/gallery/

Cognitive Science

- Fitt's Law
- Invisible structures
- Mental Models
- Modes

image: http://www.uk-anime.net/fanart/large/loughead2.gif by Michelle Loughead



Design for Clarity

- Intuitive
- Allow Exploration
- Always allow a way out
- Consistency

image: http://www.atpm.com/6.07/images/filterit-confusing.gif

Navigation

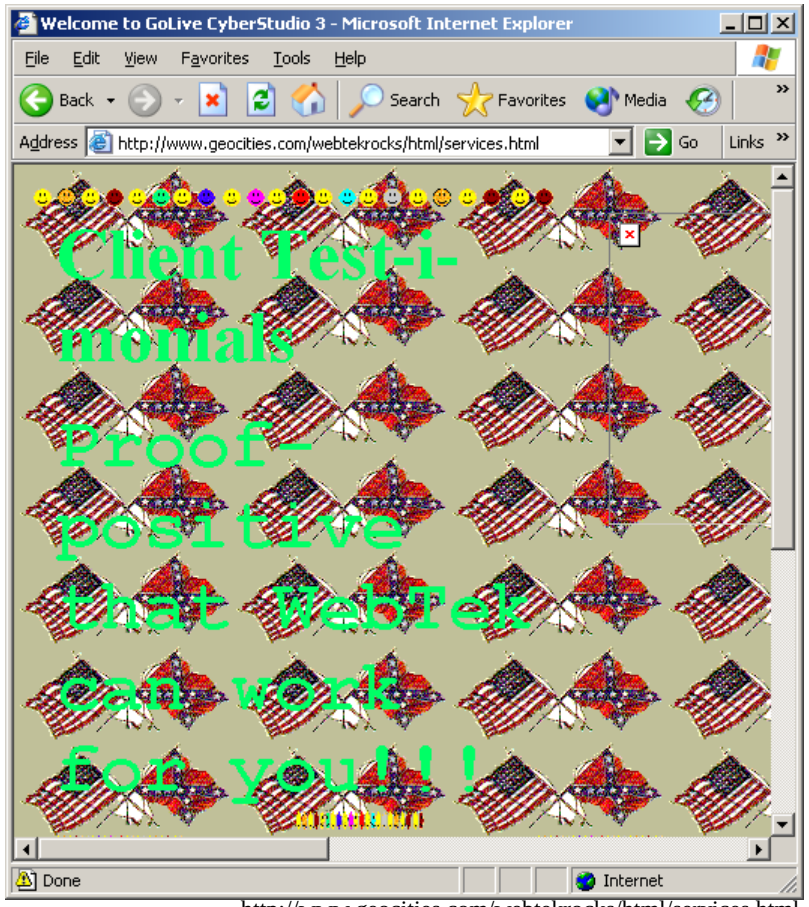
- Beware too many features at top level
- Go where users expect

image source: http://www.dack.com/web/amazon.html by Dack Ragus, used with permission

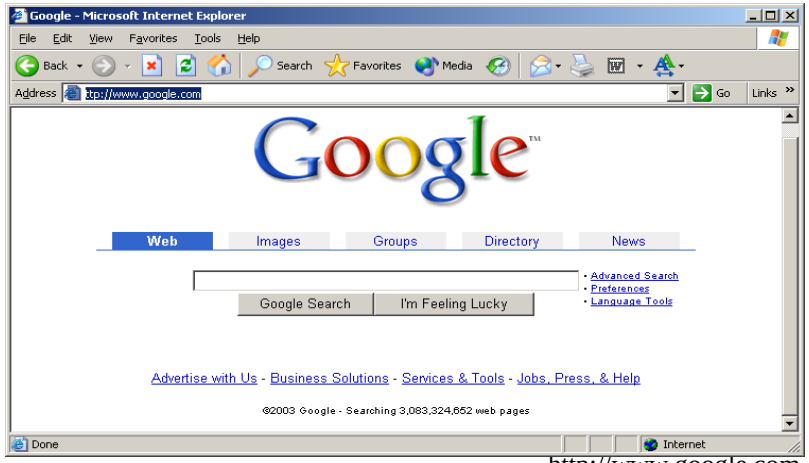
Color

- People need contrast
- Less is more
- Color Blindness
- White or pale backgrounds are preferred
- Use of colors to draw attention

http://www.geocities.com/webtekrocks/



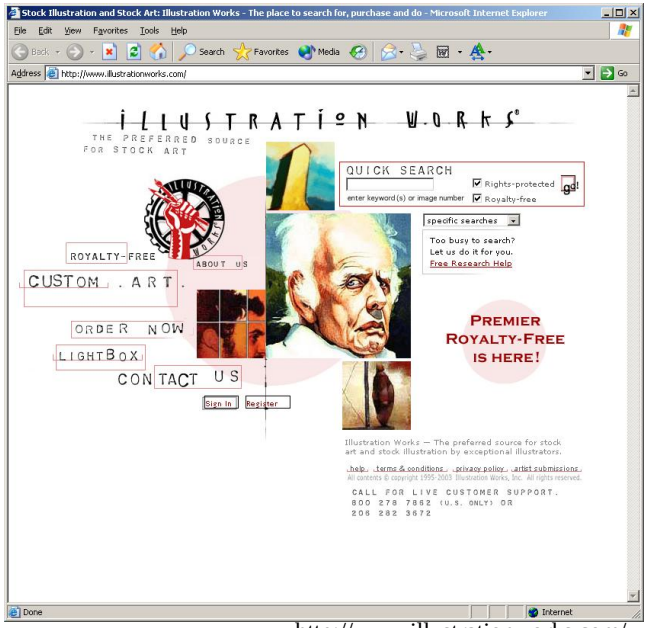
http://www.geocities.com/webtekrocks/html/services.html



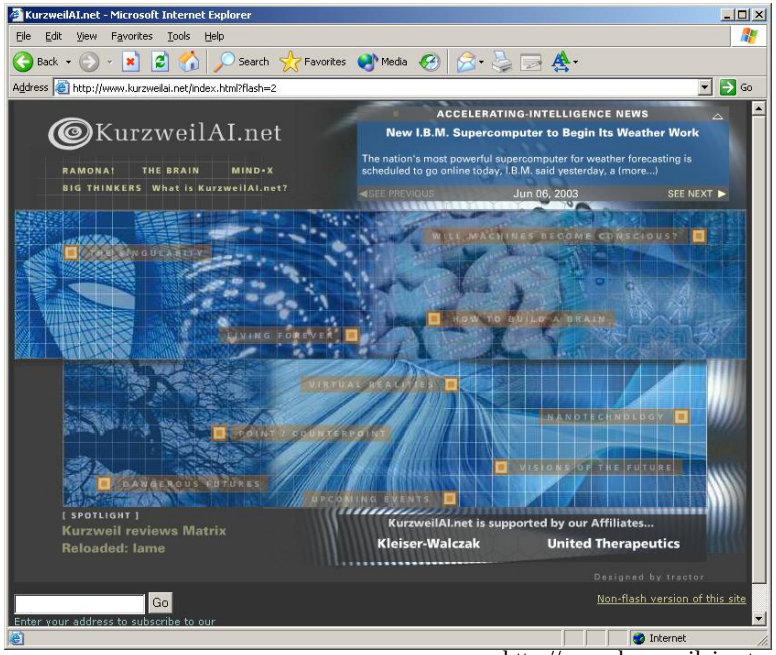
http://www.google.com

http://www.useit.com/

http://www.useit.com/jakob/photos/



http://www.illustrationworks.com/



http://www.kurzweilai.net

http://www.coolhomepages.com/

Fonts

DEFCON / BlackHat
DEFCON / BlackHat
DEFCON / BlackHat

DEFCON / Black Hat
DEFCON / BlackHat
DEFCON / BlackHat
DEFCON / BlackHat

DEFCON / BlackHat

DEFCON/BlackHat

Metaphor

Metaphor use can map easily from people's experience with other concepts

- Don't force it
- Some are overdone…
  - "The Town"
  - "The Library"

images: http://clc.dau.mil/kc/no_login/portal.asp & http://www.albany.edu/jmmh/vol2no1/sanfran-library.jpg

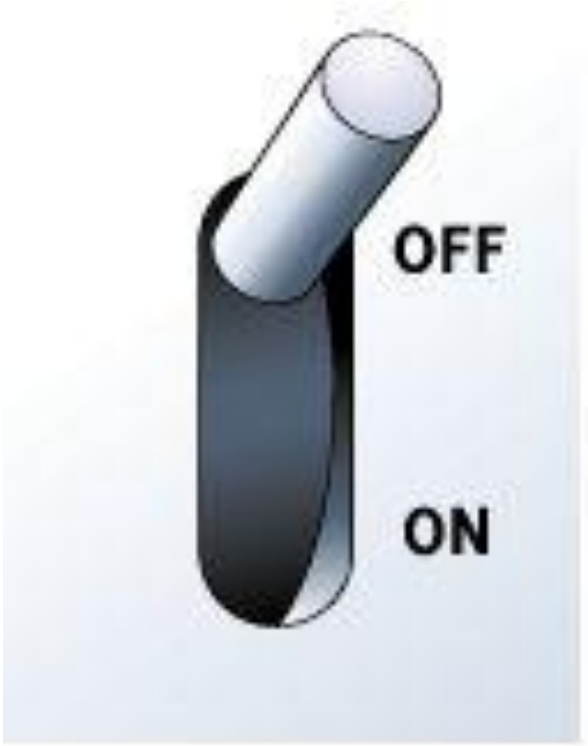
WINAMP can be found at www.winamp.com

images: http://mbc.intnet.mu/radio/internaute/images/winamp.gif & http://www.winamp.com & http://www.axemusic.com/vendors/pioneer/images/ctw208r.gif

Consistency

Build on prior knowledge of other applications

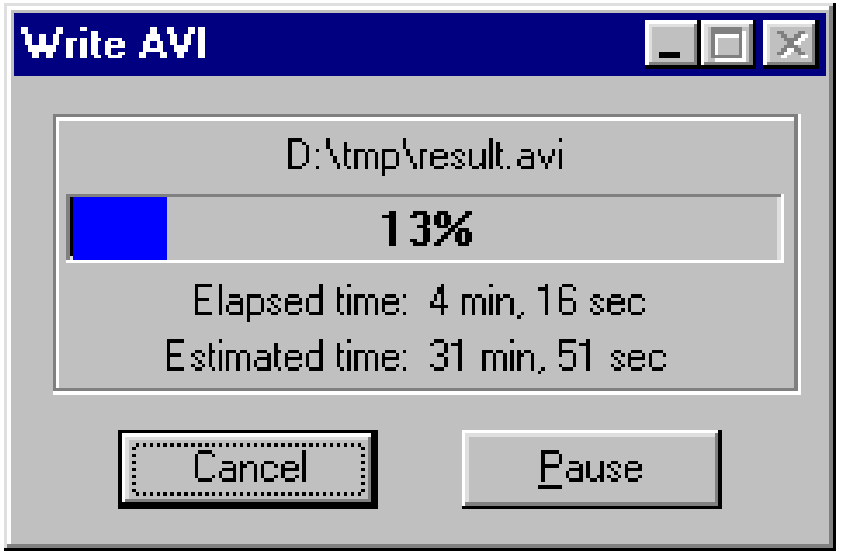
- Placement of controls
- Keyboard shortcuts
- Within program, environment and related tools



http://www.tiresias.org/controls/images/consistency.jpg

Feedback

- Timely feedback
- Busy indicator
- Progress indicator
- Visual and audible



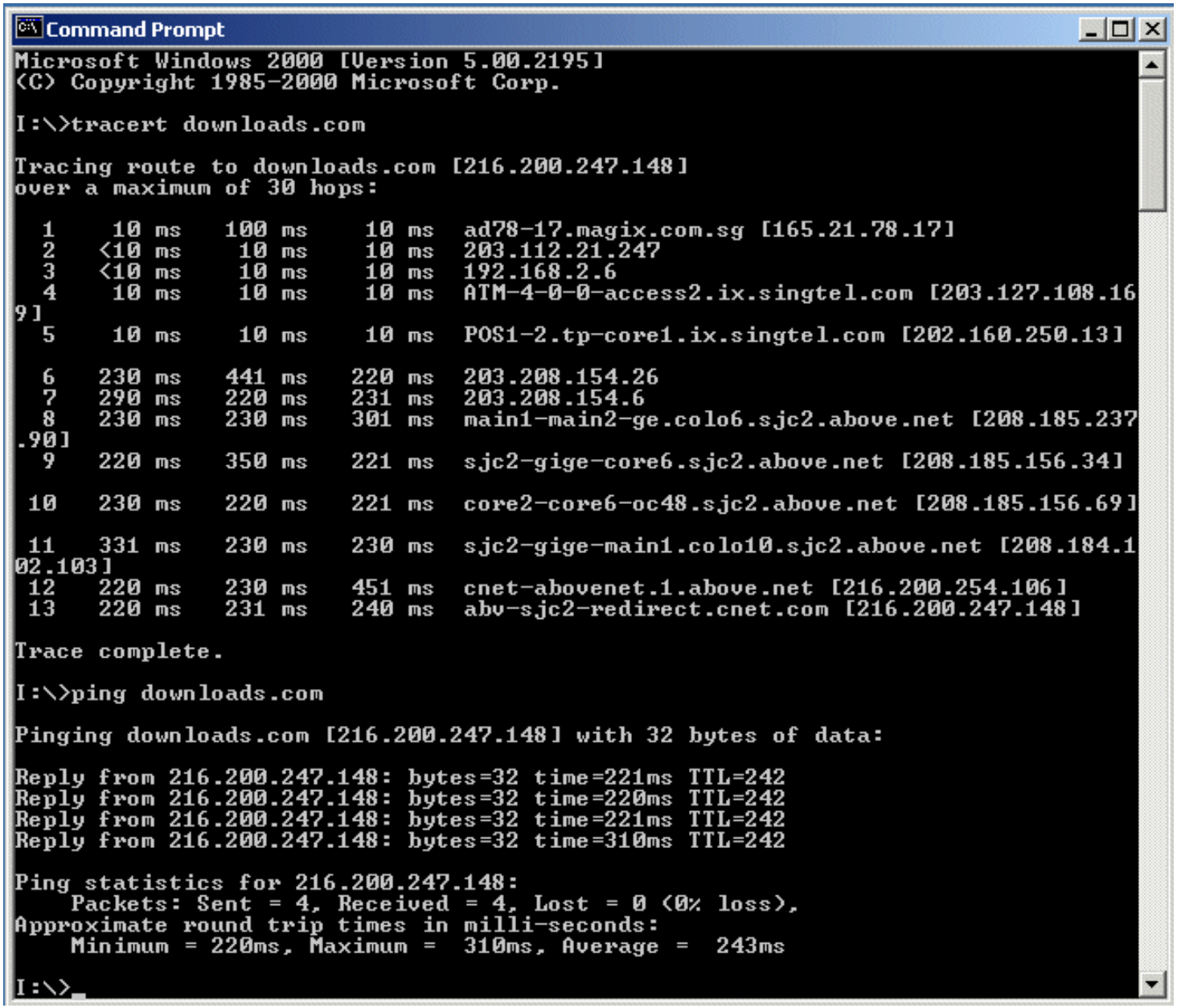
http://www.softlab-nsk.com/ddclipro/images/progress.gif
http://www.dbdomain.com/dba14.htm

Testing

- Try it out on users, get feedback and fix
- You may be surprised
- Allow time to fix your project
- Value of Testing
- Iterative design
- How to conduct testing

image: http://www.uk-anime.net/gallery/images/mac7-4.jpg

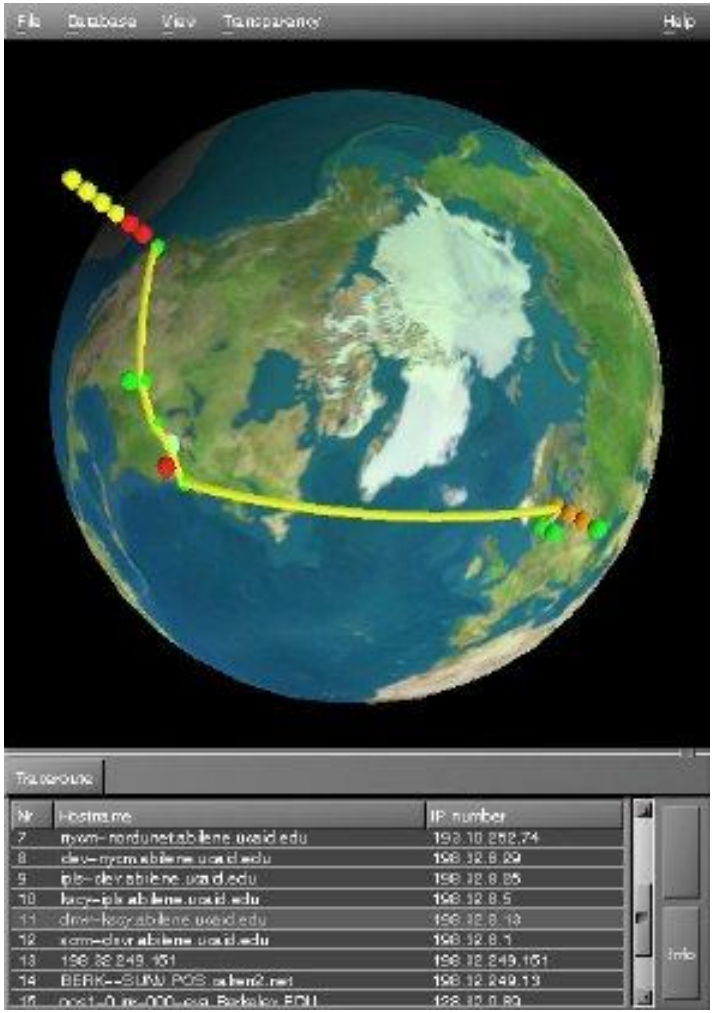
Information Visualization

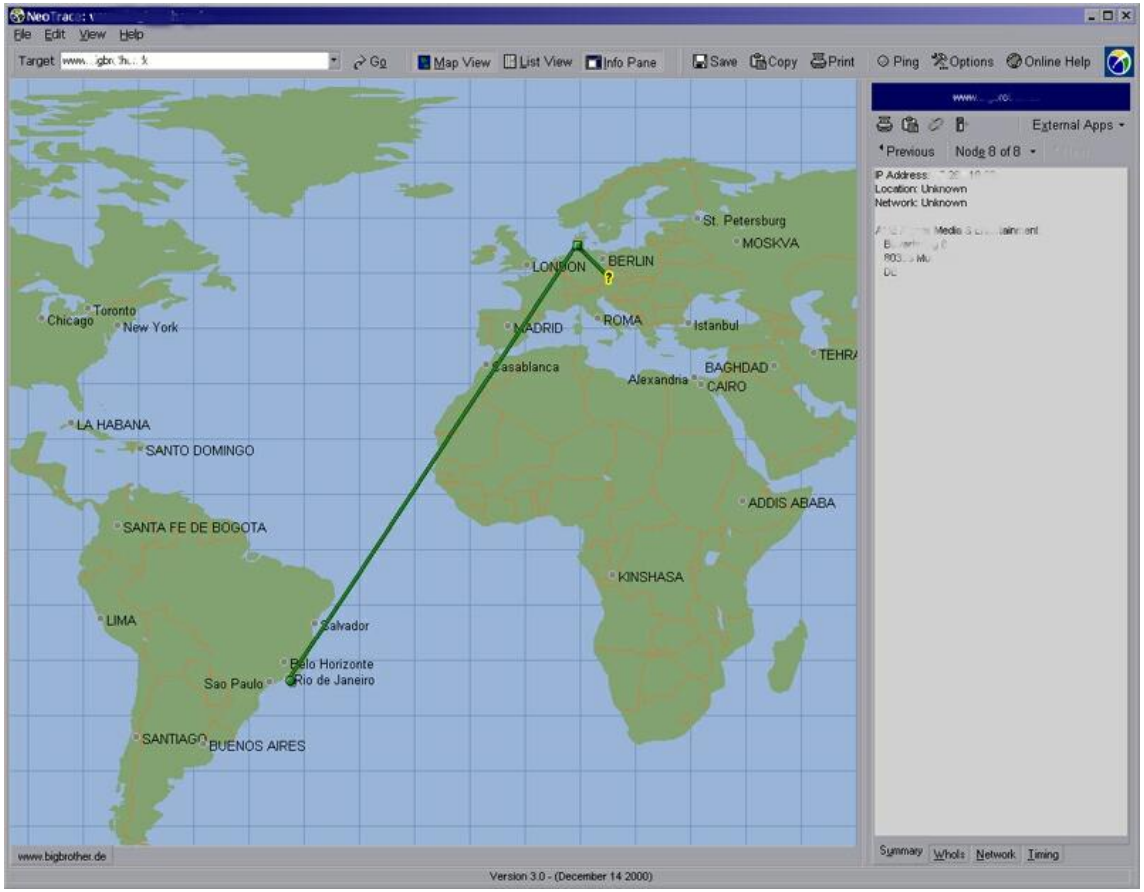


tracert from the command line

http://www.hardware-one.com/reviews/AztechADSLTurbo900/images/Downloads-TraceRT-Ping.gif

Xtraceroute
Neotrace visualization





NeoTrace by NeoWorx is available at http://download.com.com/3000-2172-7139158.html?legacy=cnet
Xtraceroute by Björn Augustsson is available at http://www.dtek.chalmers.se/~d3august/xt/
See also the excellent Atlas of Cyberspaces at http://www.cybergeography.org/atlas/routes.html
images: http://www.dtek.chalmers.se/~d3august/xt/index.html & http://www.lewe.com/img/toptools/neotrace-1.jpg

Network Traffic Dataset

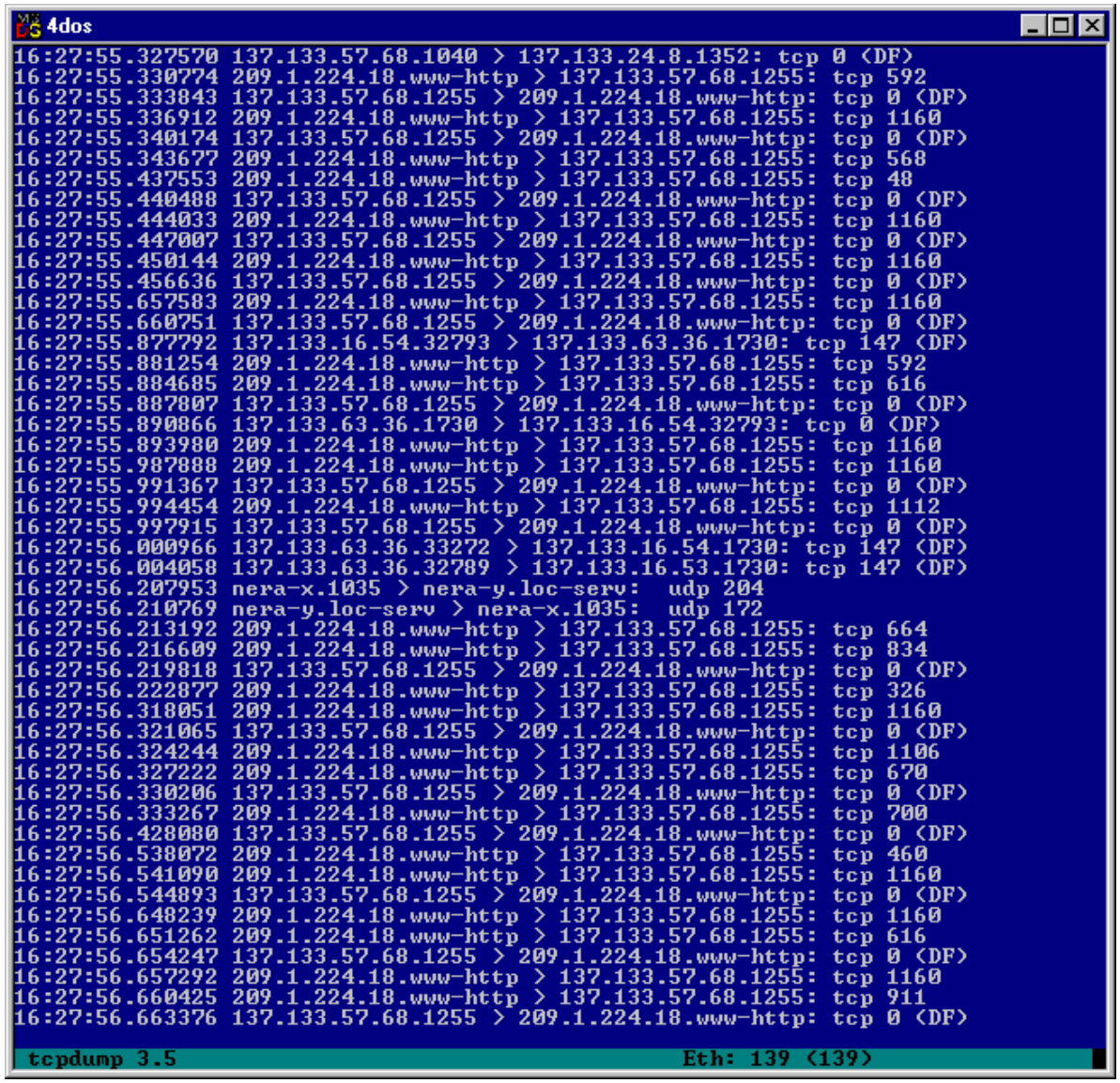
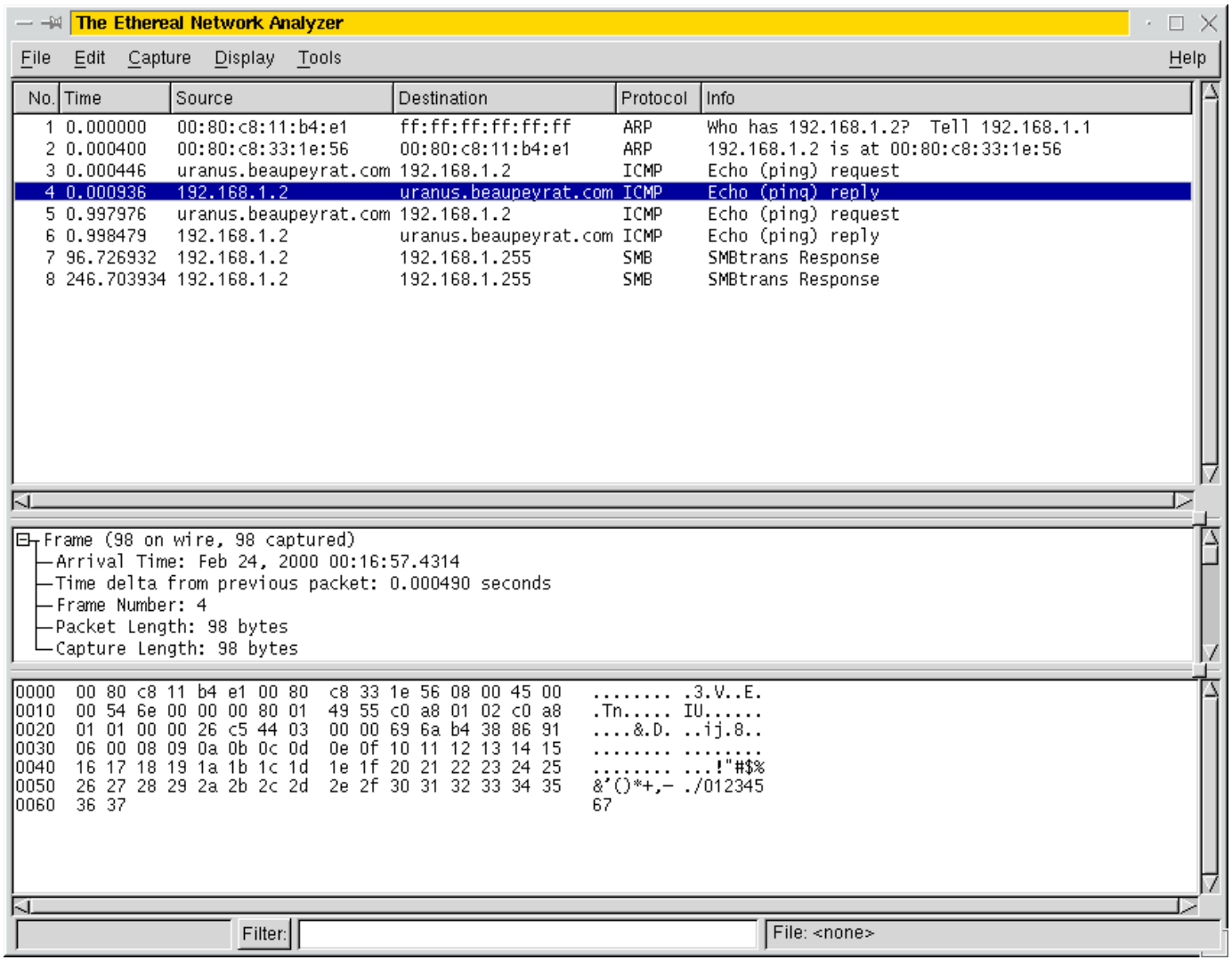


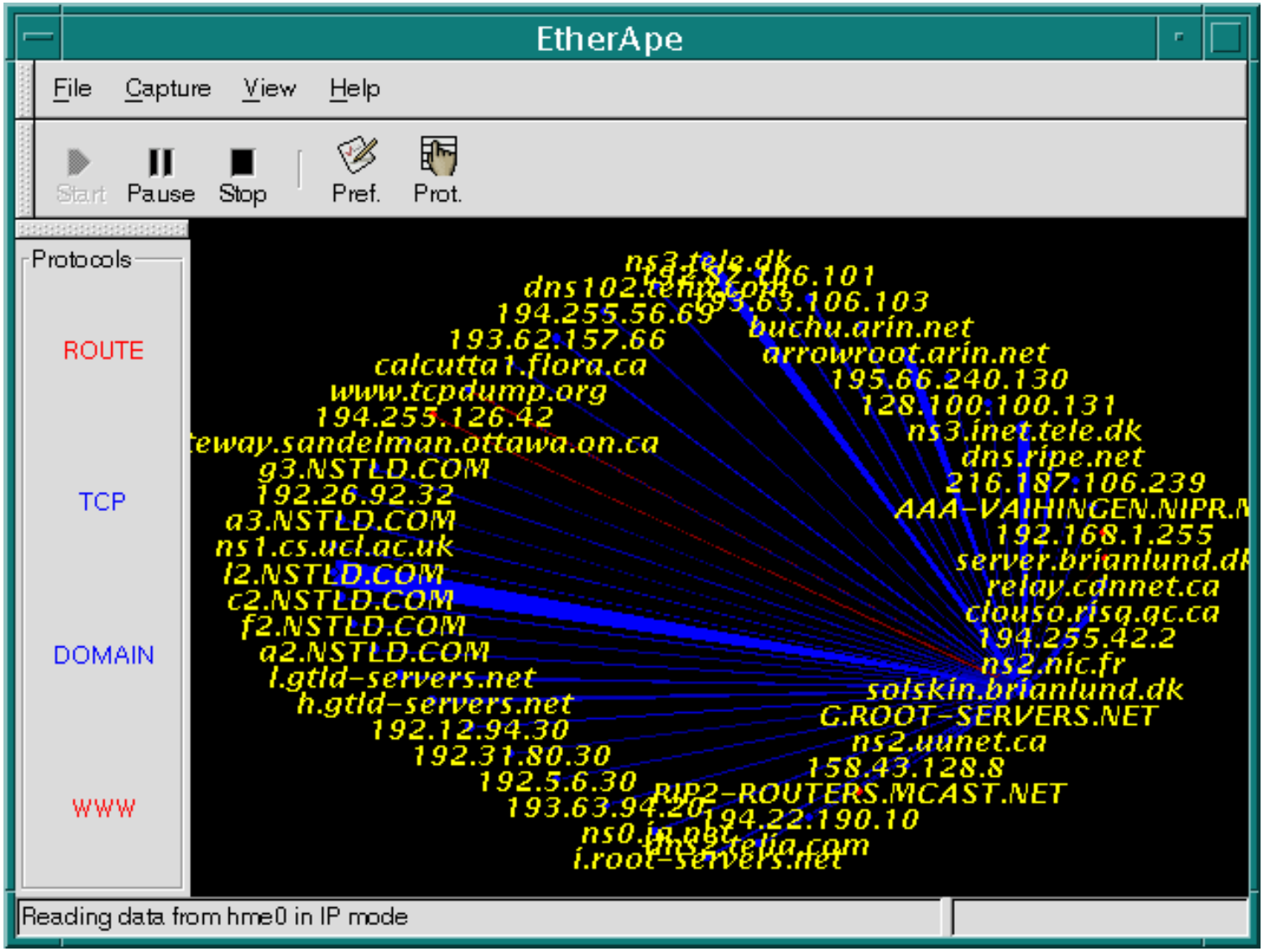
image: http://www.bgnett.no/~giva/pcap/tcpdump.png

Network Traffic Viewed in Ethereal

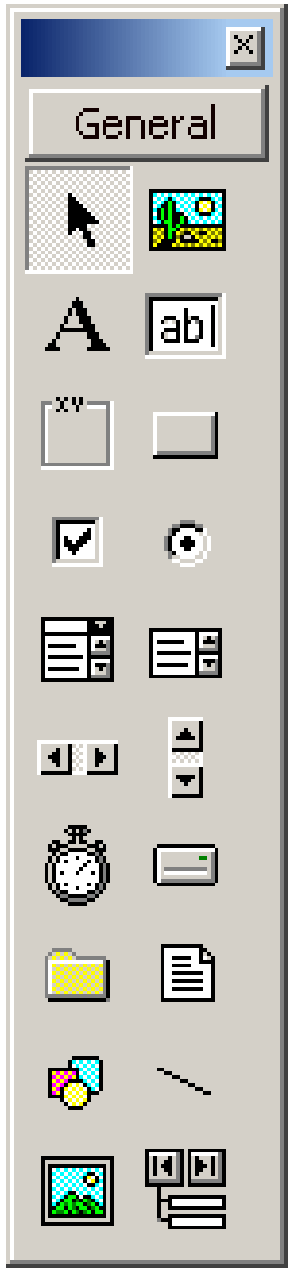


Ethereal by Gerald Combs can be found at http://www.ethereal.com/
image: http://www.linux-france.org/prj/edu/archinet/AMSI/index/images/ethereal.gif

Network Traffic as Viewed in EtherApe



Etherape by Juan Toledo can be found at http://etherape.sourceforge.net/
screenshot: http://www.solaris4you.dk/sniffersSS.html



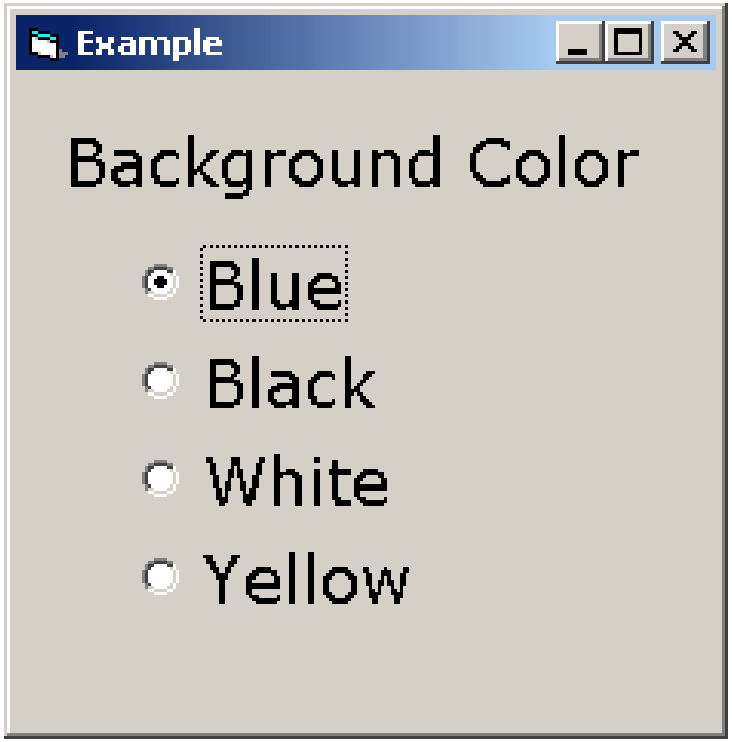
GUI Components

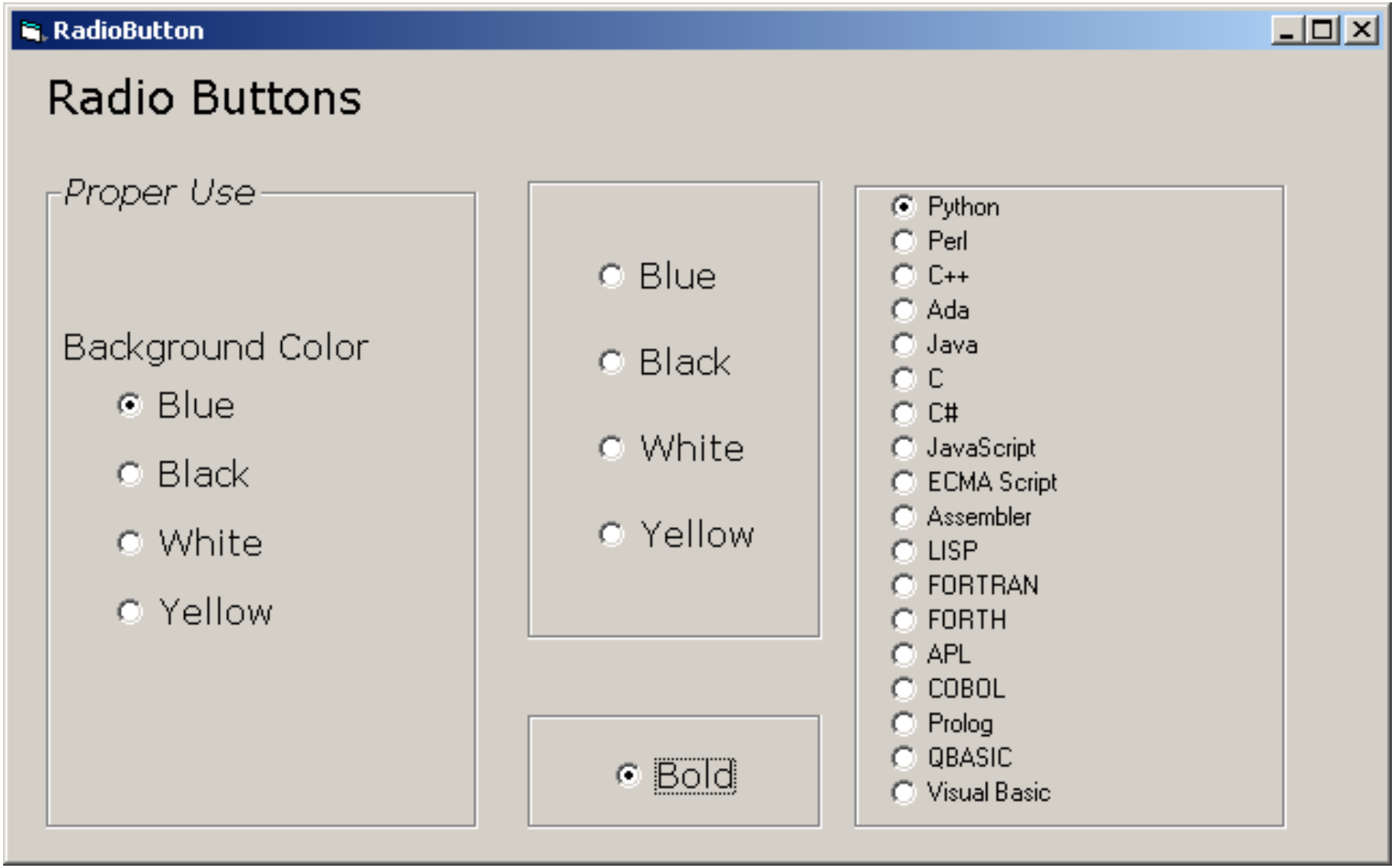
- **Radio Buttons**
- **Check Boxes**
- **Dialog Boxes**
- **Menus**
- **Labels**
- **Text Fields**
- **Toolbars**
- **Forms**
- Splash Screens
- Push Buttons List Boxes
- Spinners
- Sliders
- and more…

image: MS Visual Basic 6.0

Radio Buttons

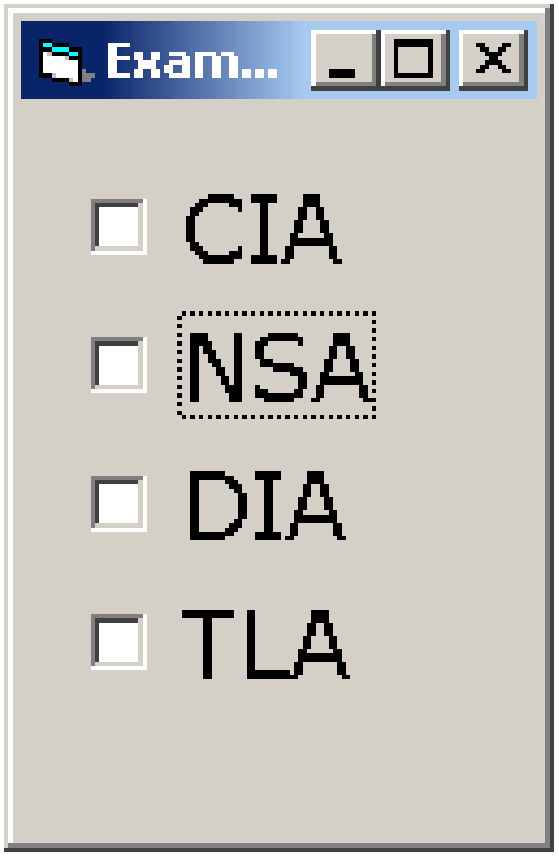
- 1 to Many Control
- Try to limit to 6 items
- Set Default
- Not a check box
- Never use just one

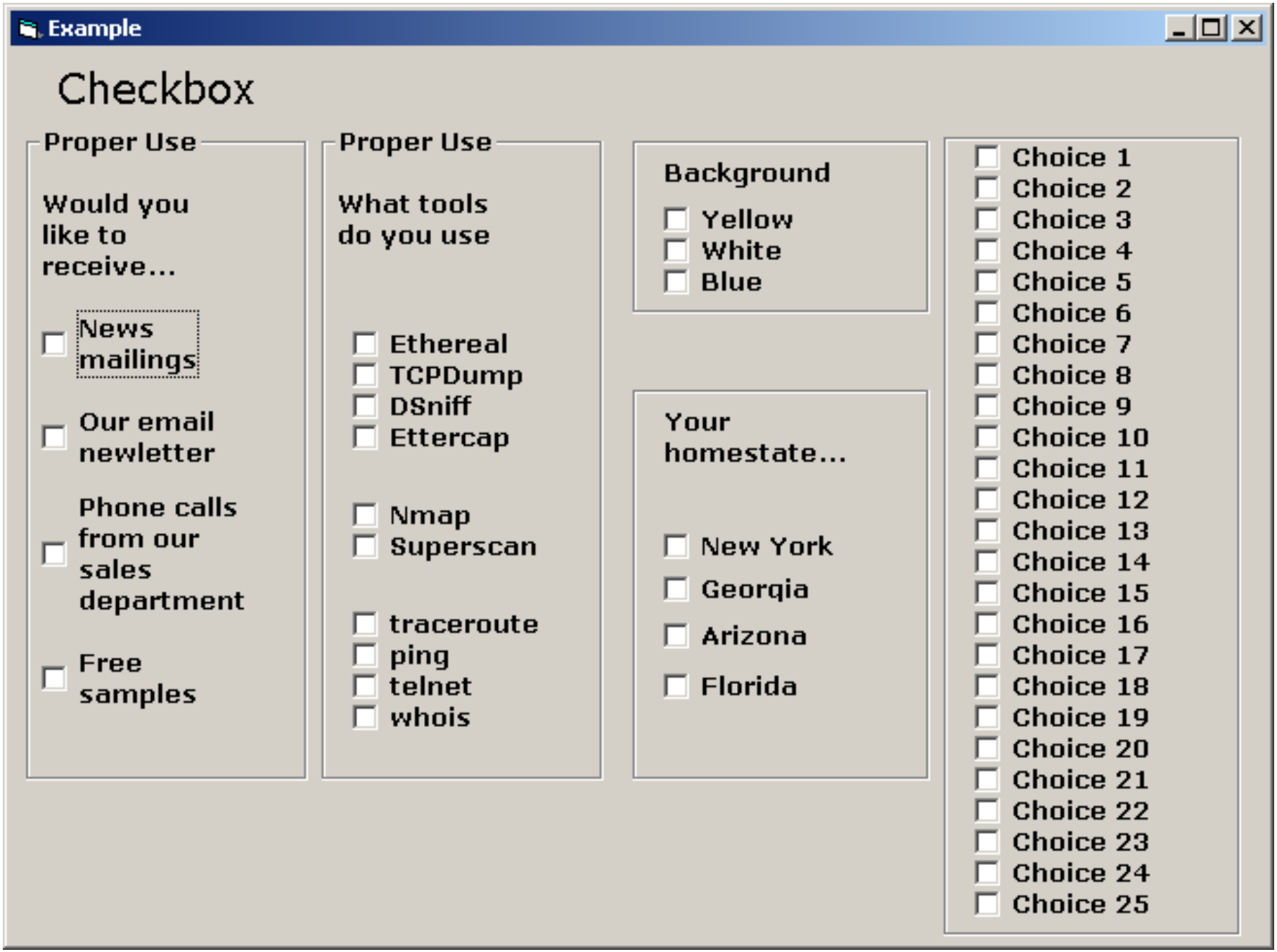



RadioButton
Radio Buttons
Proper Use
Background Color
Blue
Black
White
Yellow
Blue
Black
White
Yellow
Bold
Python
Perl
C++
Ada
Java
C
C#
JavaScript
ECMA Script
Assembler
LISP
FORTRAN
FORTH
APL
COBOL
Prolog
QBASIC
Visual Basic

Check Boxes

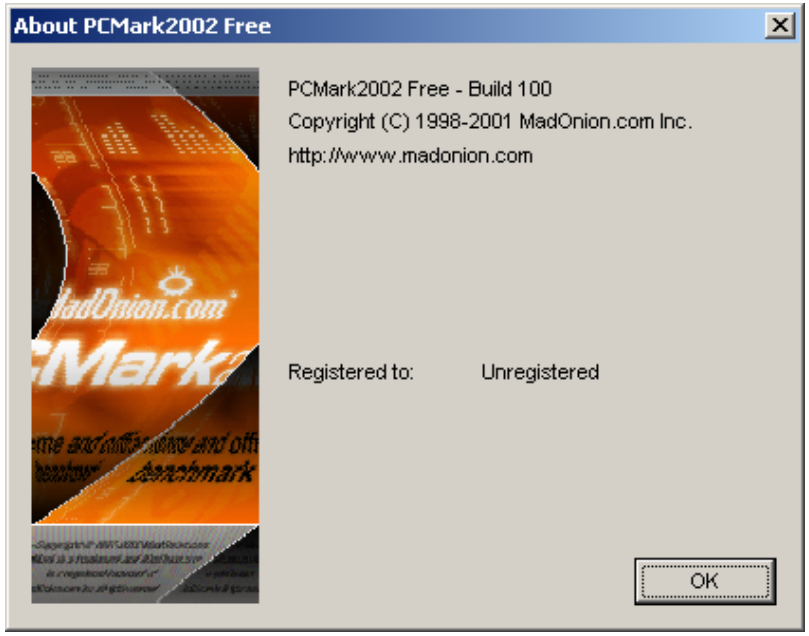
- Used for single on/off settings
- Max 12 per group
- Don’t confuse with radio buttons

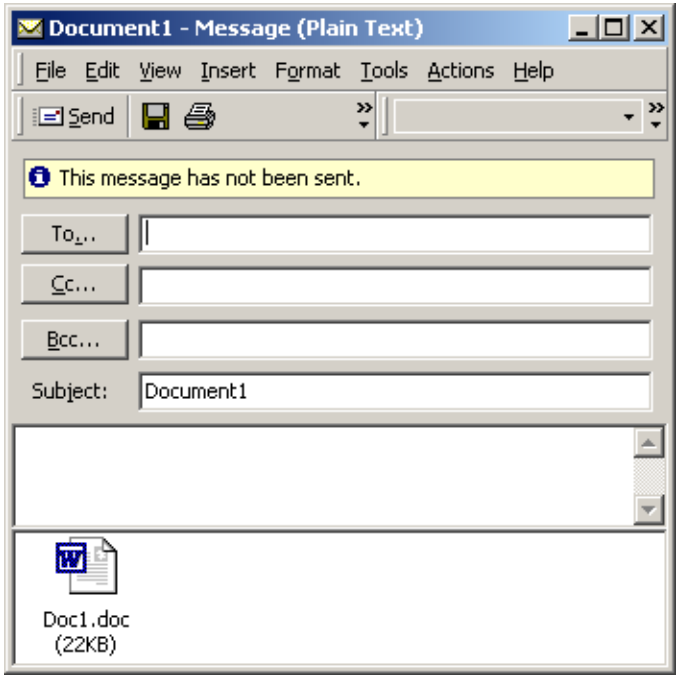


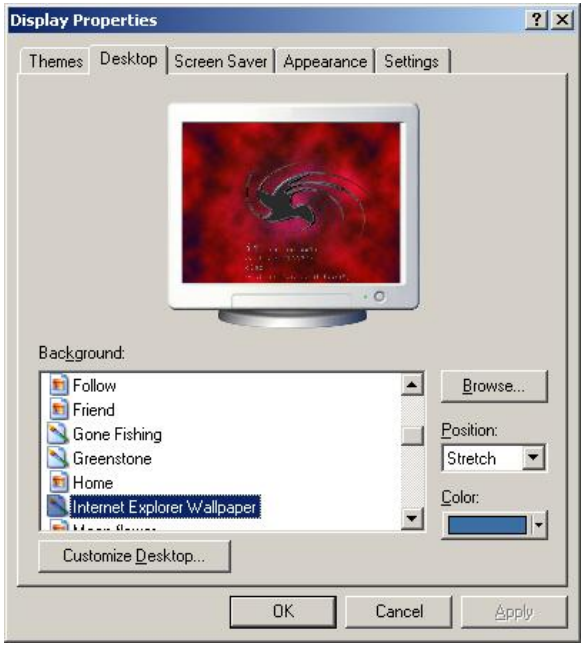

Example
Checkbox
Proper Use
Would you like to receive...
News mailings
Our email newletter
Phone calls from our sales department
Free samples
Proper Use
What tools do you use
Ethereal
TCPDump
DSniff
Ettercap
Nmap
Superscan
traceroute
ping
telnet
whois
Background
Yellow
White
Blue
Your homestate...
New York
Georgia
Arizona
Florida
Choice 1
Choice 2
Choice 3
Choice 4
Choice 5
Choice 6
Choice 7
Choice 8
Choice 9
Choice 10
Choice 11
Choice 12
Choice 13
Choice 14
Choice 15
Choice 16
Choice 17
Choice 18
Choice 19
Choice 20
Choice 21
Choice 22
Choice 23
Choice 24
Choice 25

Dialog Boxes

- Modal (immediate task)
- Modeless (on going task)
- Beware too many levels
- Cancel doesn't cancel



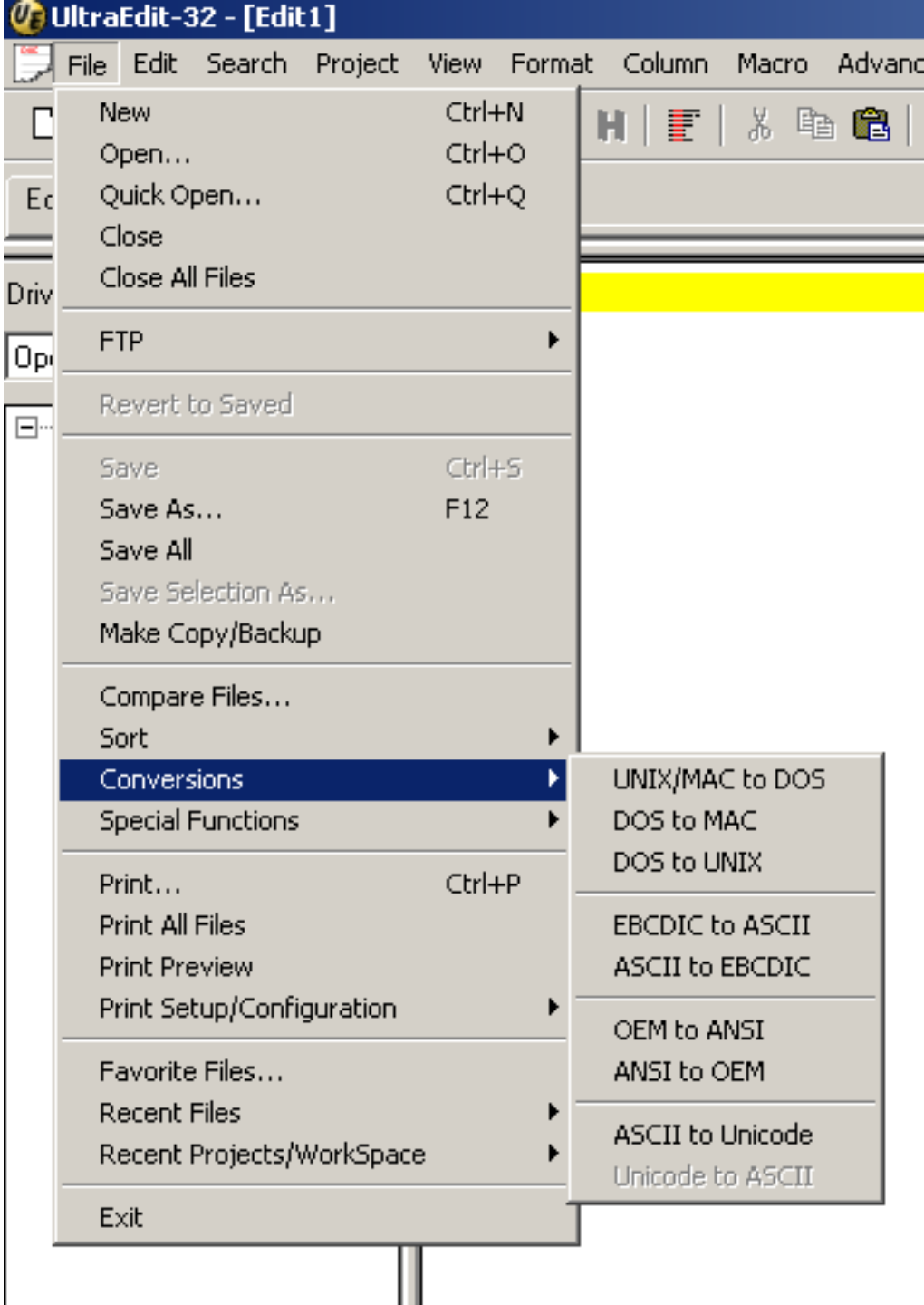




images: PCMark2002, MS Word, Win XP
PCMark2002 by Futuremark Corp can be found at http://futuremark.com/products/pcmark2002/

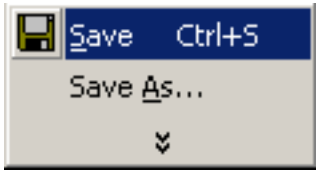
Menus

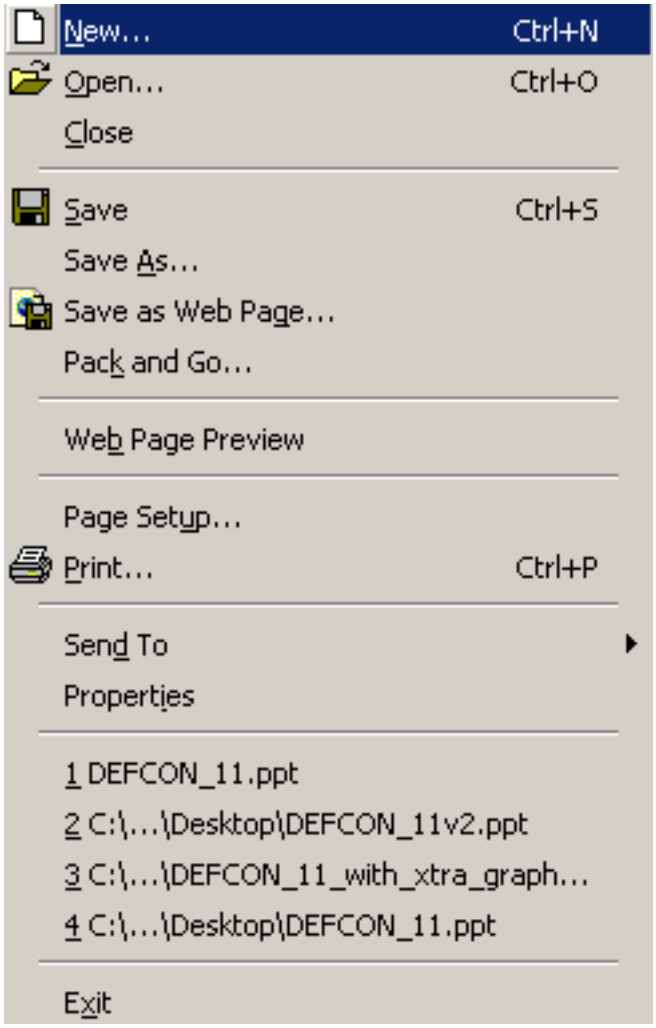
- Menu length
- Confusing menu items
- Keyboard shortcuts



Menus

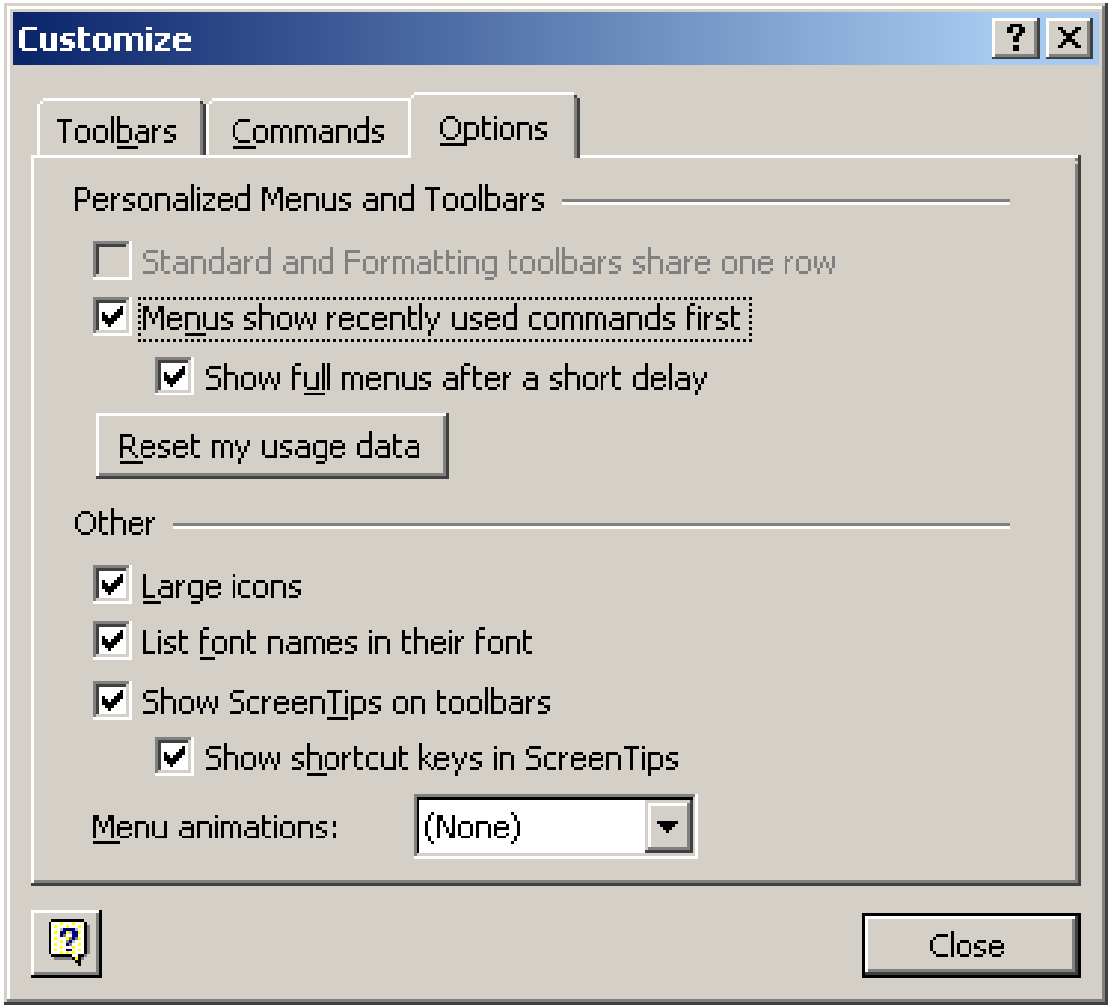
Dynamic interfaces are generally considered bad





Screen capture is from Microsoft PowerPoint 2000

Labels

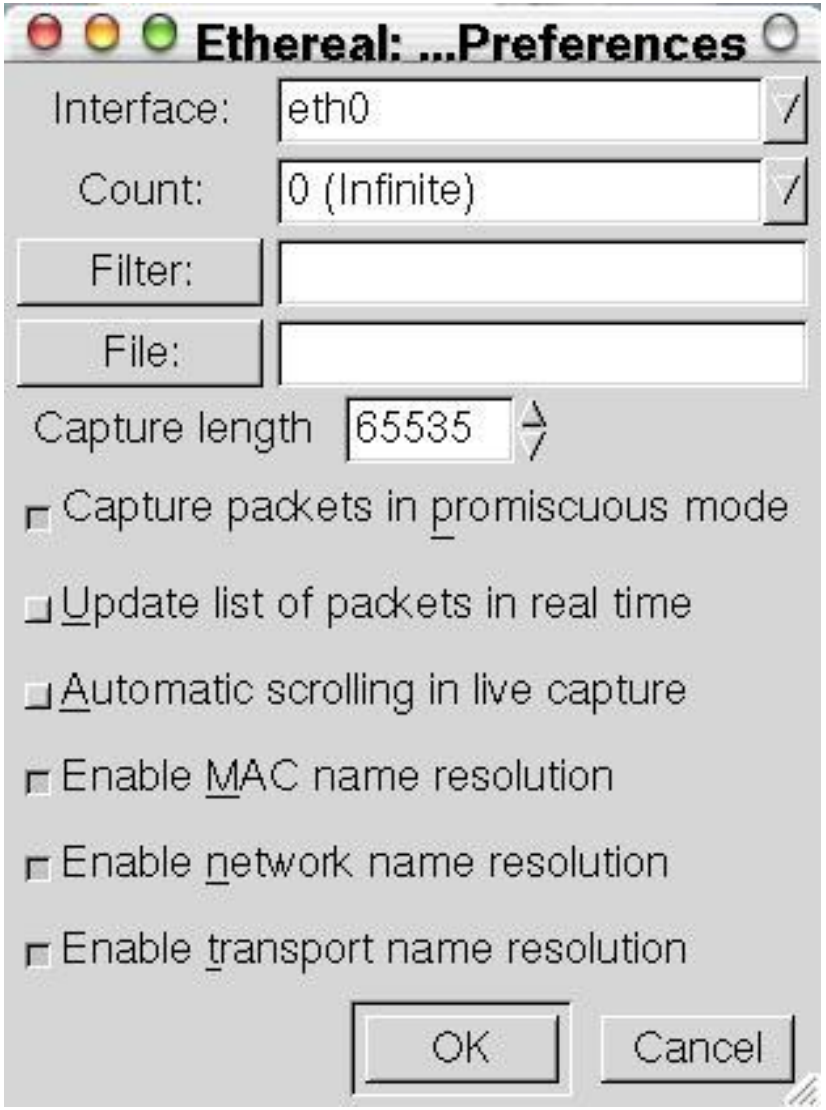


- Keep text clear
- Place labels close to setting
- Consistent terminology, writing
- Avoid ambiguity
- Concepts must be distinct

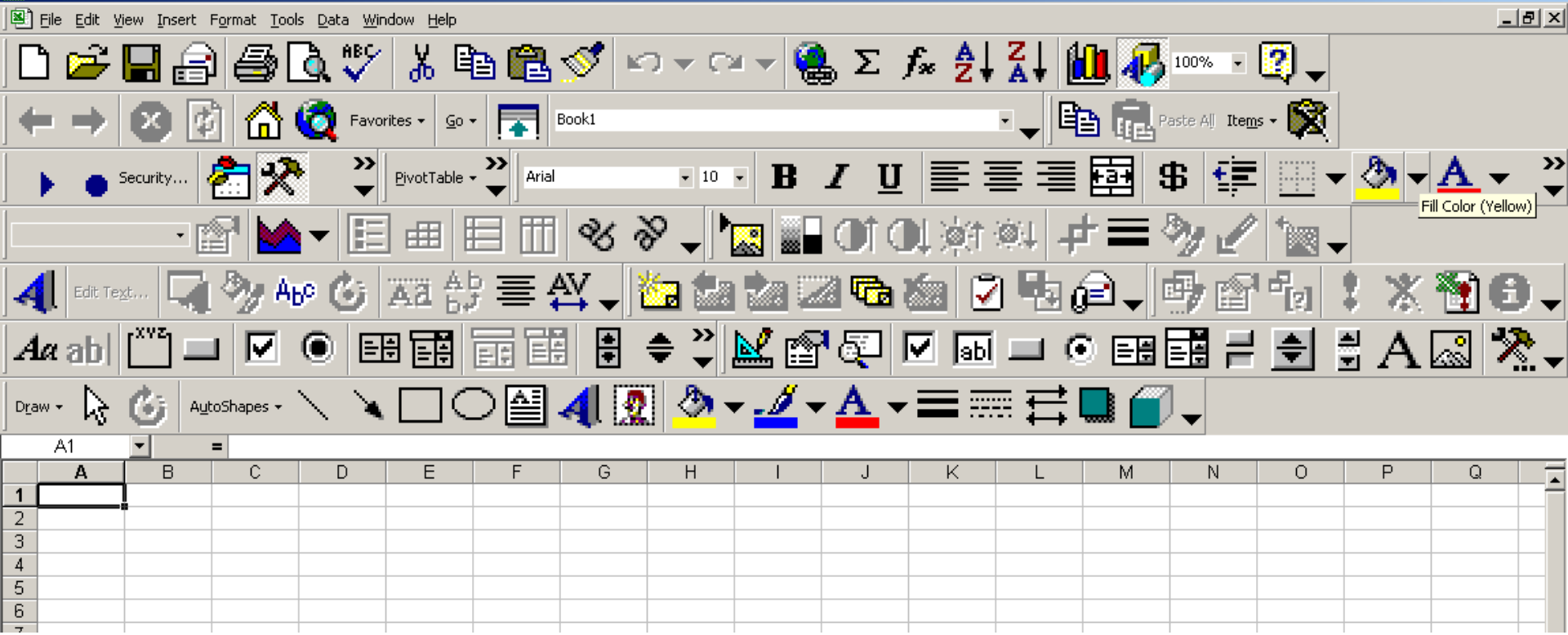
image is from Microsoft Powerpoint 2000

Text Fields

- Defaults
- Make them large enough
- Highlighted current data
- Font size
- Alignment



Ethereal by Gerald Combs can be found at http://www.ethereal.com/
image: http://www.ethereal.com/docs/user-guide/ch03capturestart.html#CH03CAPPREF

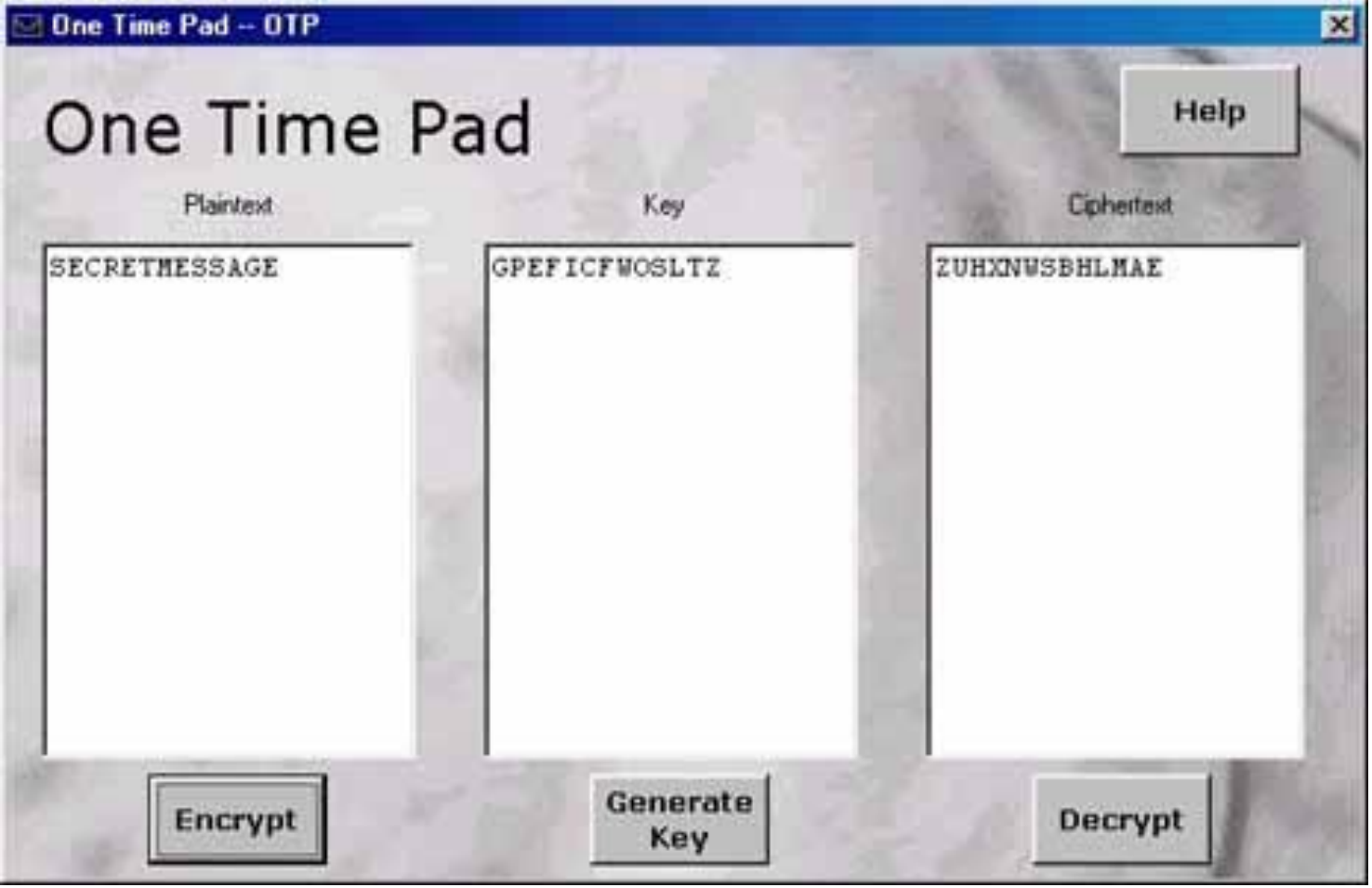


Toolbars/Icons

- Consistency
- Test your images
- Sometimes text just works better
- Don’t Overdo It

image is from Microsoft Excel 2000

Forms and Overall Layout



Four Criteria[1]

- Dominant reading order
- Frequency of use
- Relationship to other controls
- User Expectations

Other Issues

- Resizable
- Background Images
- Logical Grouping
- Line things up

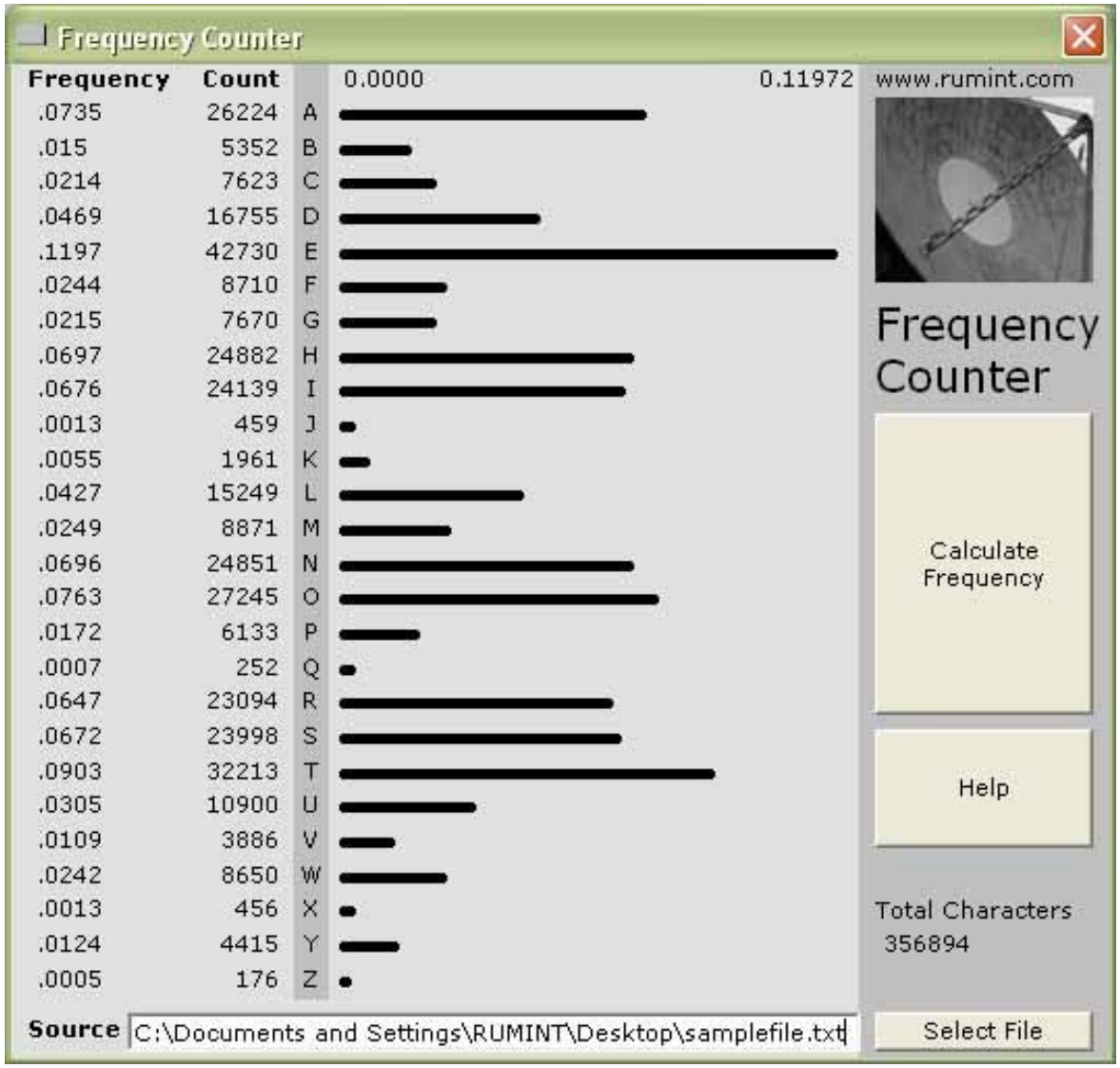
1. GUI Bloopers by Jeff Johnson, p.143
2. OTP can be found at www.rumint.com

Let's Tear Apart My Own Projects

- Frequency Counter
- Advanced Frequency Counter

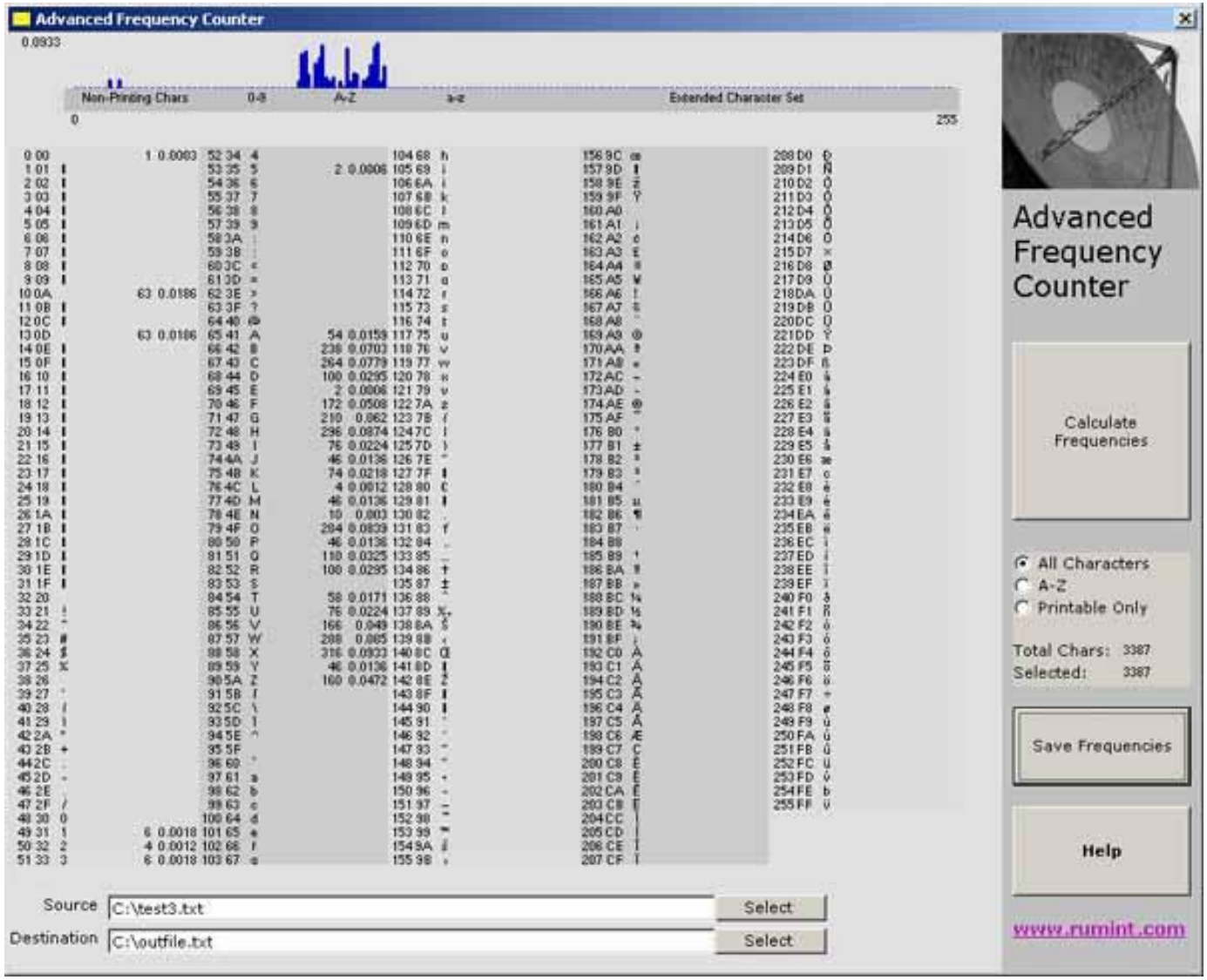
http://www.uk-anime.net/gallery/images/tenchi3.jpg

Frequency Counter



Frequency Counter can be found at www.rumint.com

Advanced Frequency Counter



Advanced Frequency Counter can be found at www.rumint.com

Critique of tools

Image: http://www.misato.co.uk/ by Tracey Knight, used with permission

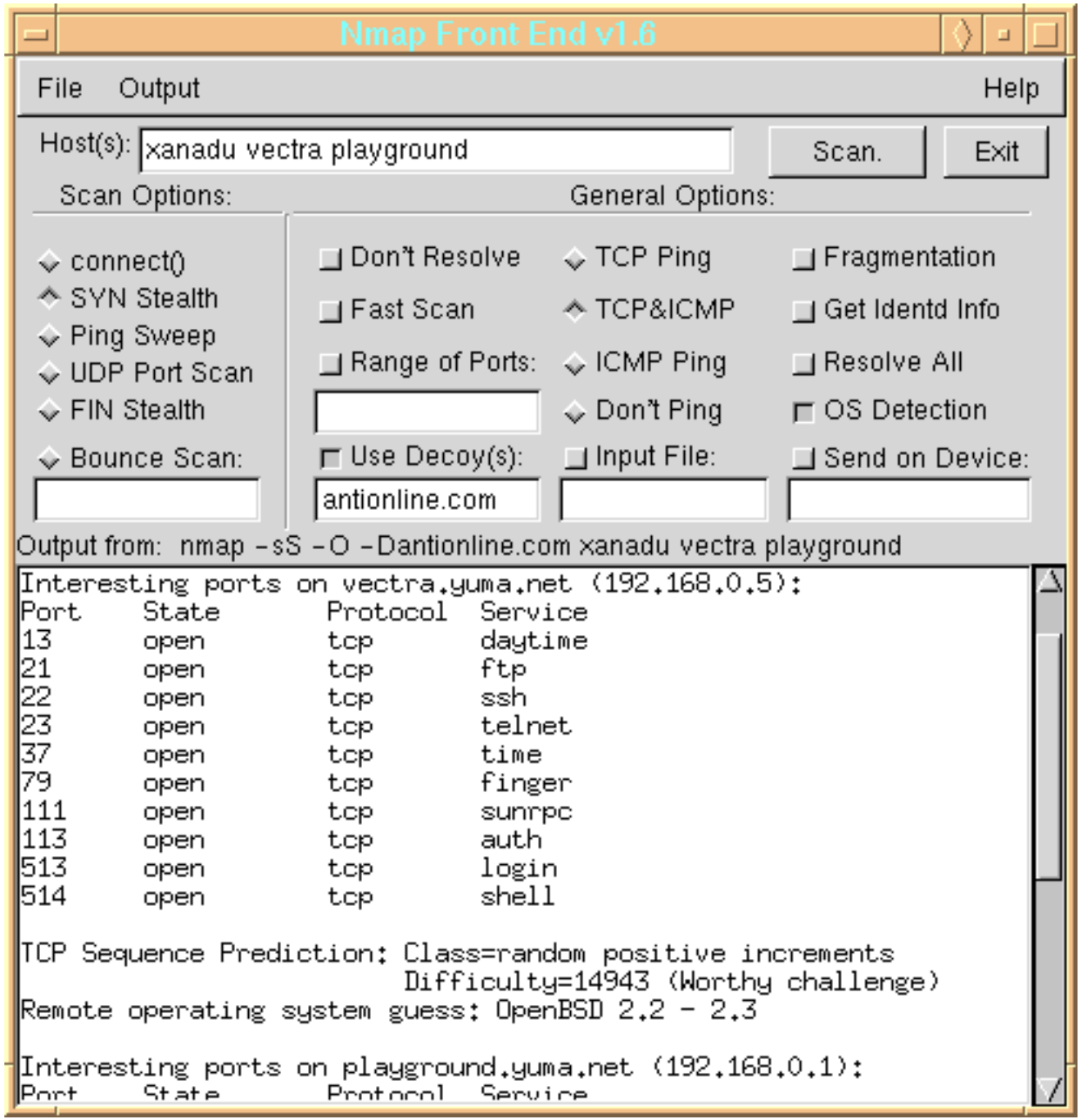
Respect to Authors

Your Kung Fu is Very Good

http://www.uk-anime.net/gallery/images/ranma1.jpg

NetBus

Image source:http://members.tripod.com/~gineco/NET-BUS.
Netbus is by Carl Fredrik Neikter



Nmapwin

Nmap by Fyodor is available at http://www.insecure.org/

The Nmapwin front end by Jens Vogt is available at http://www.nmapwin.org/

SubSeven

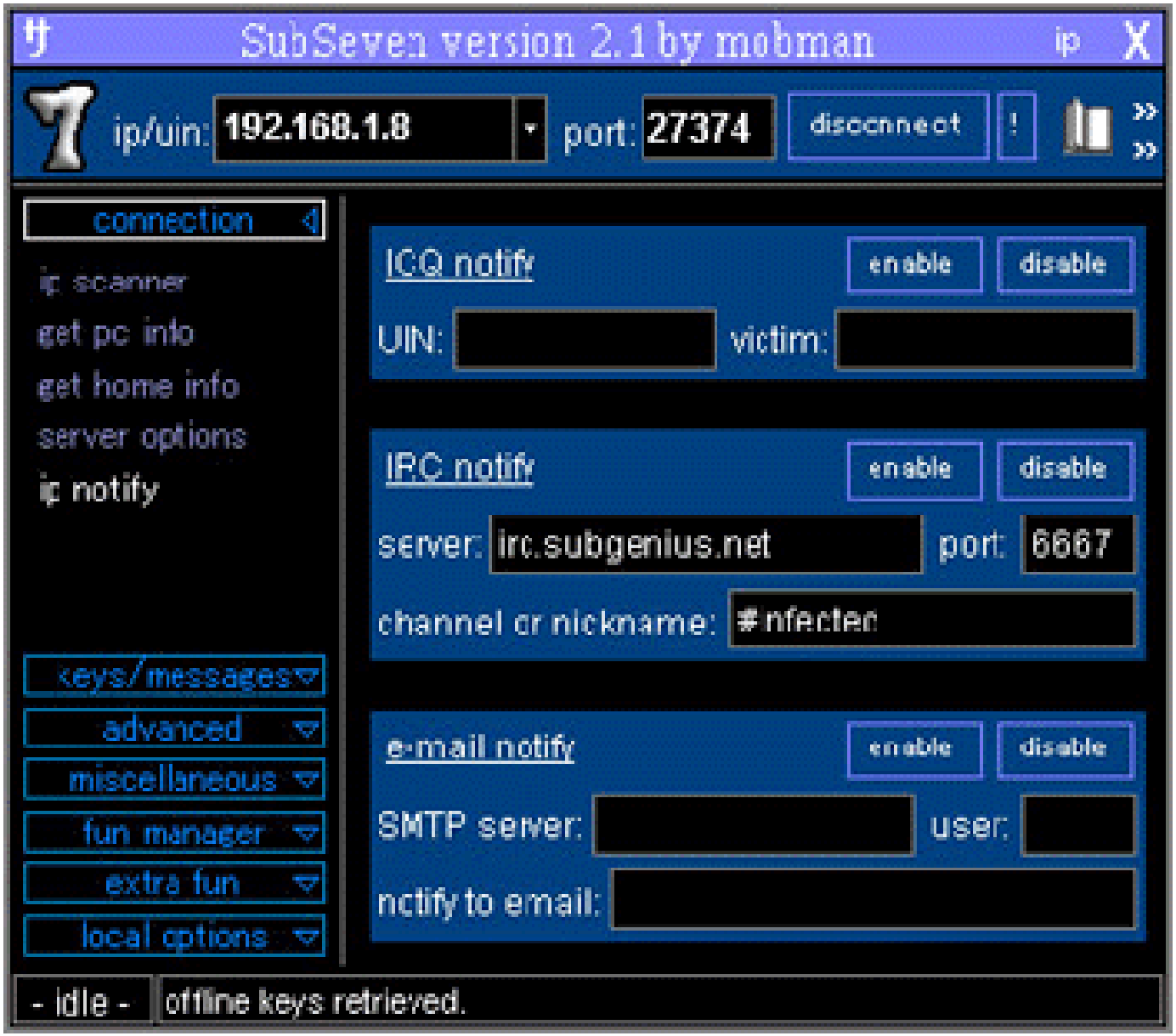
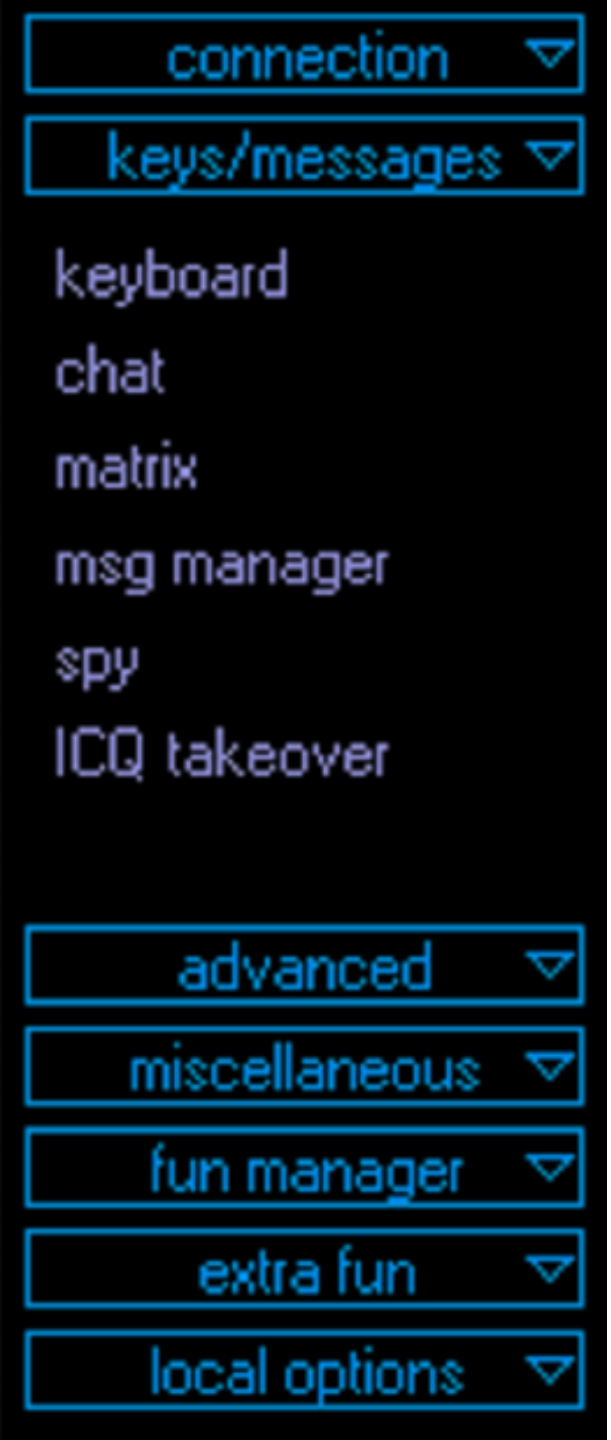


Image source:http://www.zdnet.co.jp/help/howto/security/j04/images/sub7.gif
SubSeven is by mobman. The official site is http://www.subseven.ws/



SubSeven

- Connection
- Keys / messages
- Advanced
- Miscellaneous
- Fun manager
- Extra fun
- Local Options

Original image:www.trojaner-info.de
SubSeven is by mobman. The official site is http://www.subseven.ws/

SuperScan

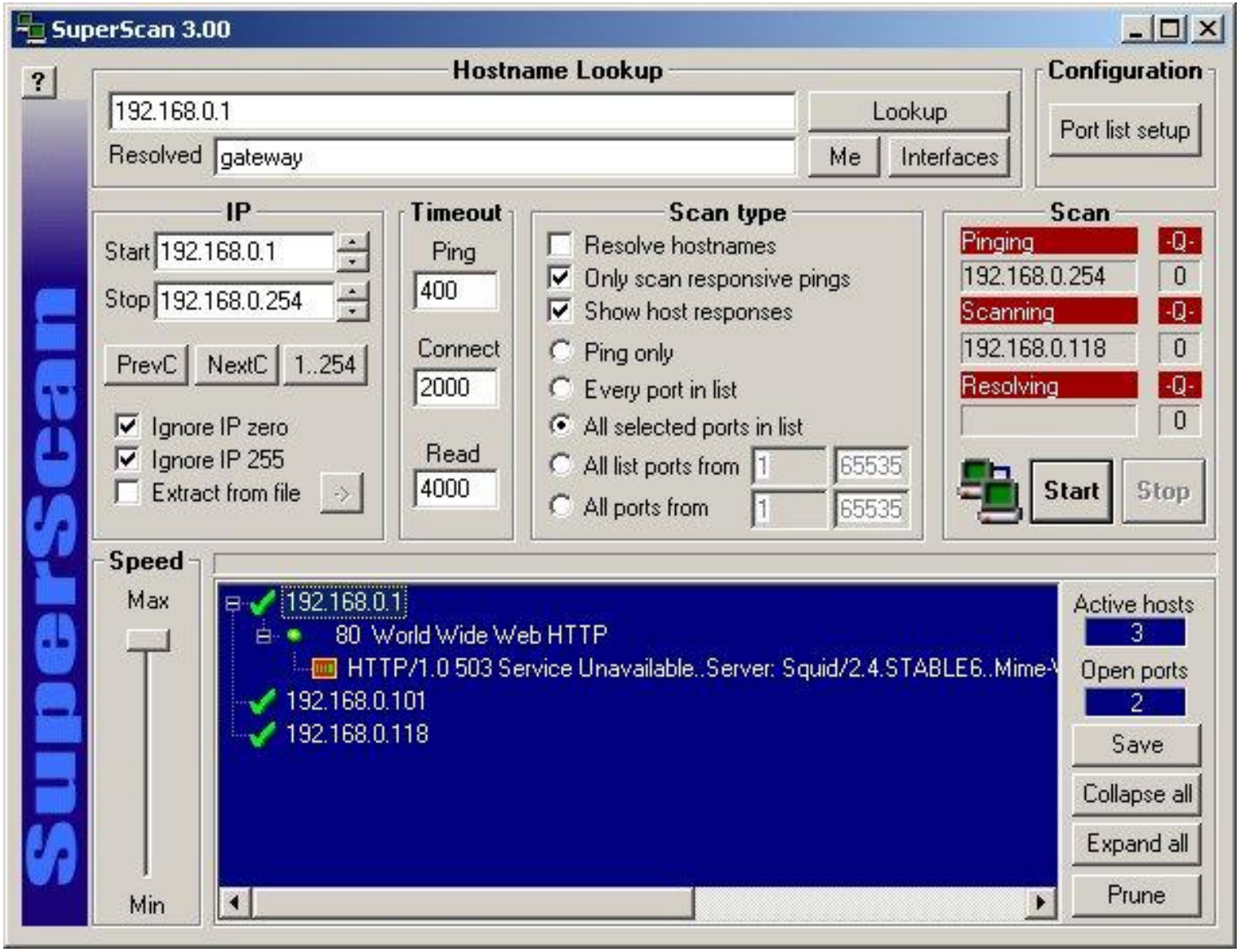
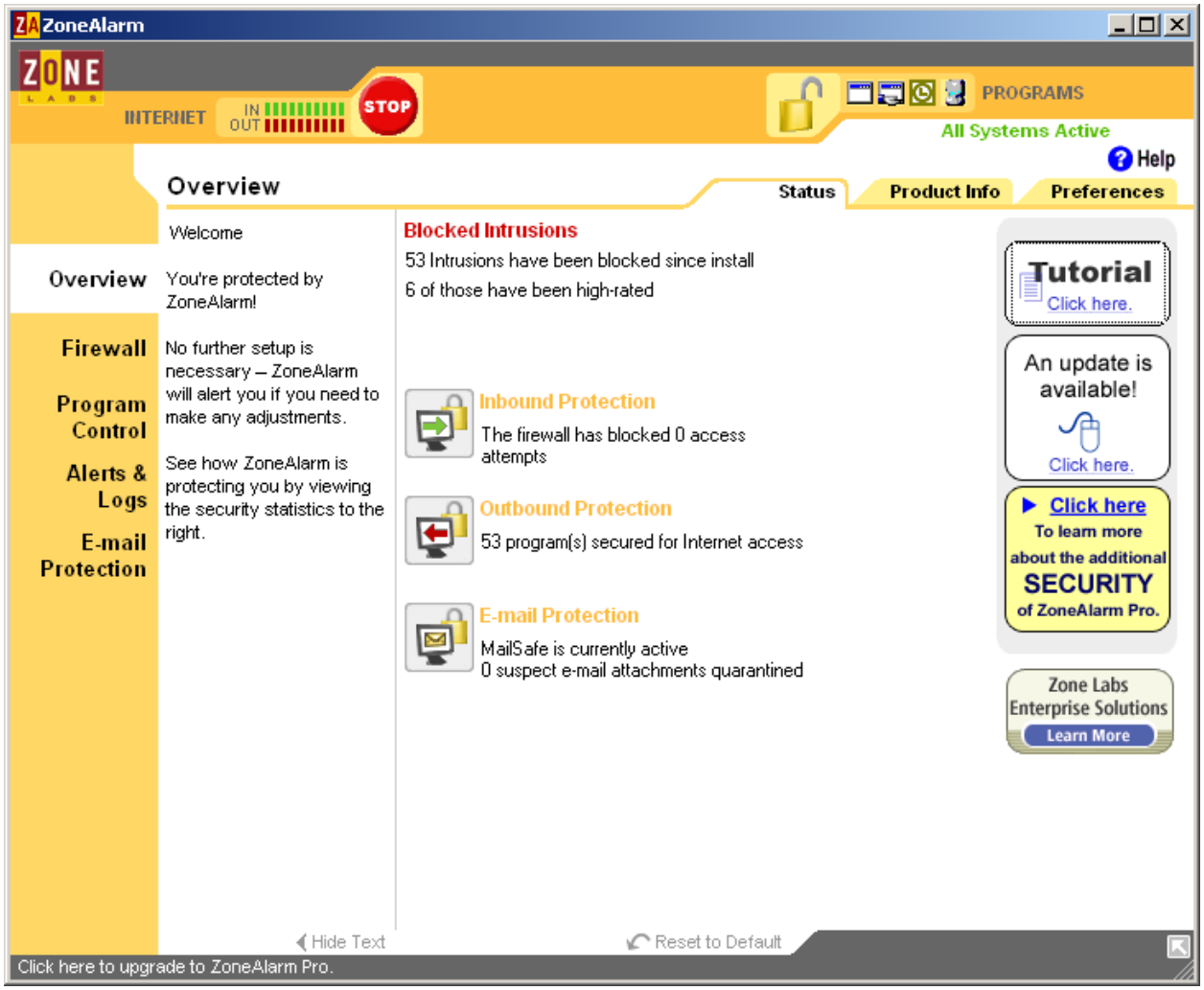


image: http://www.computec.ch/

SuperScan is by Foundstone Corp and can be found at www.foundstone.com

Zone Alarm



Zone Alarm is by ZoneLabs and can be found at http://www.zonelabs.com/

PGP

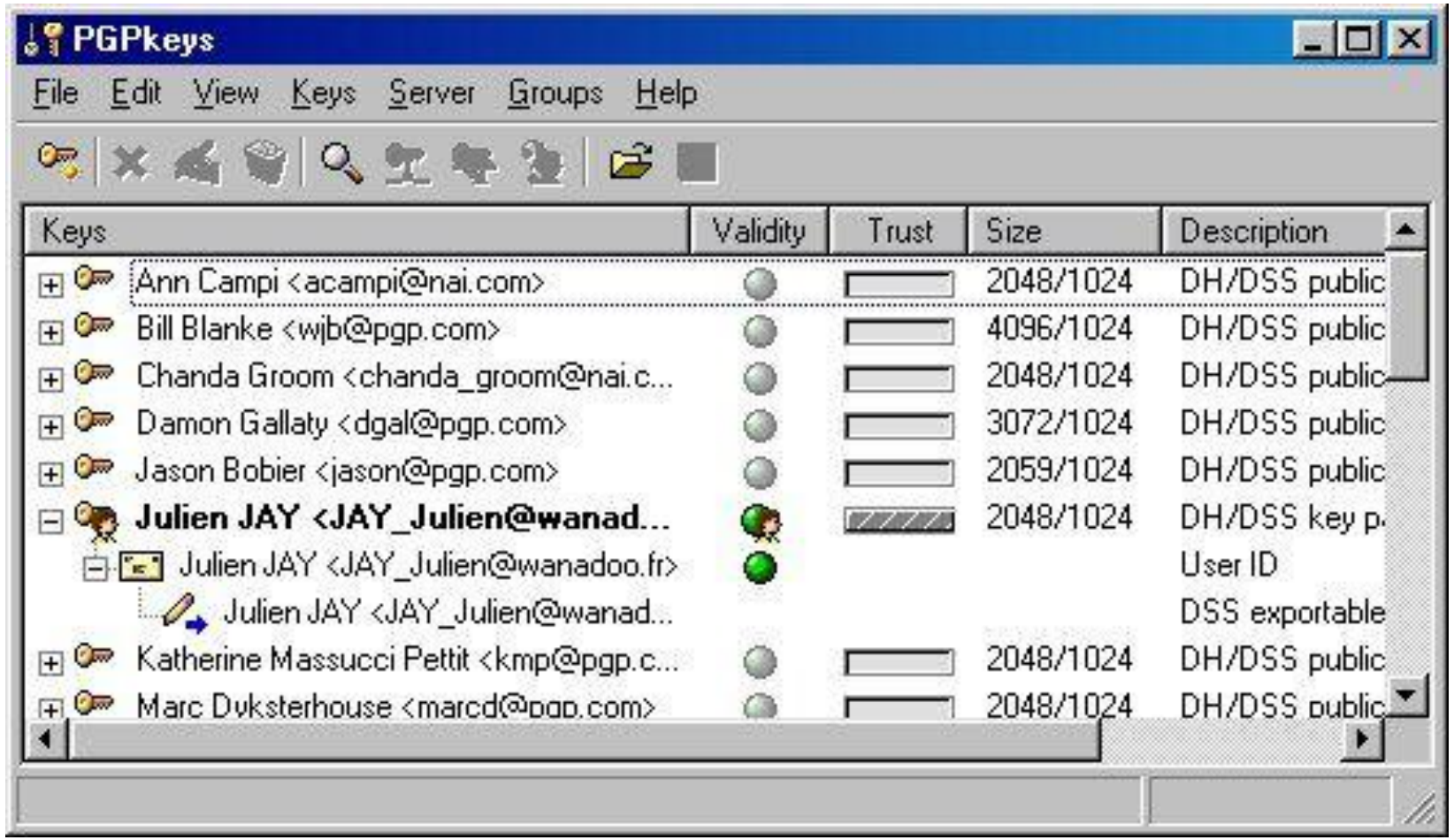
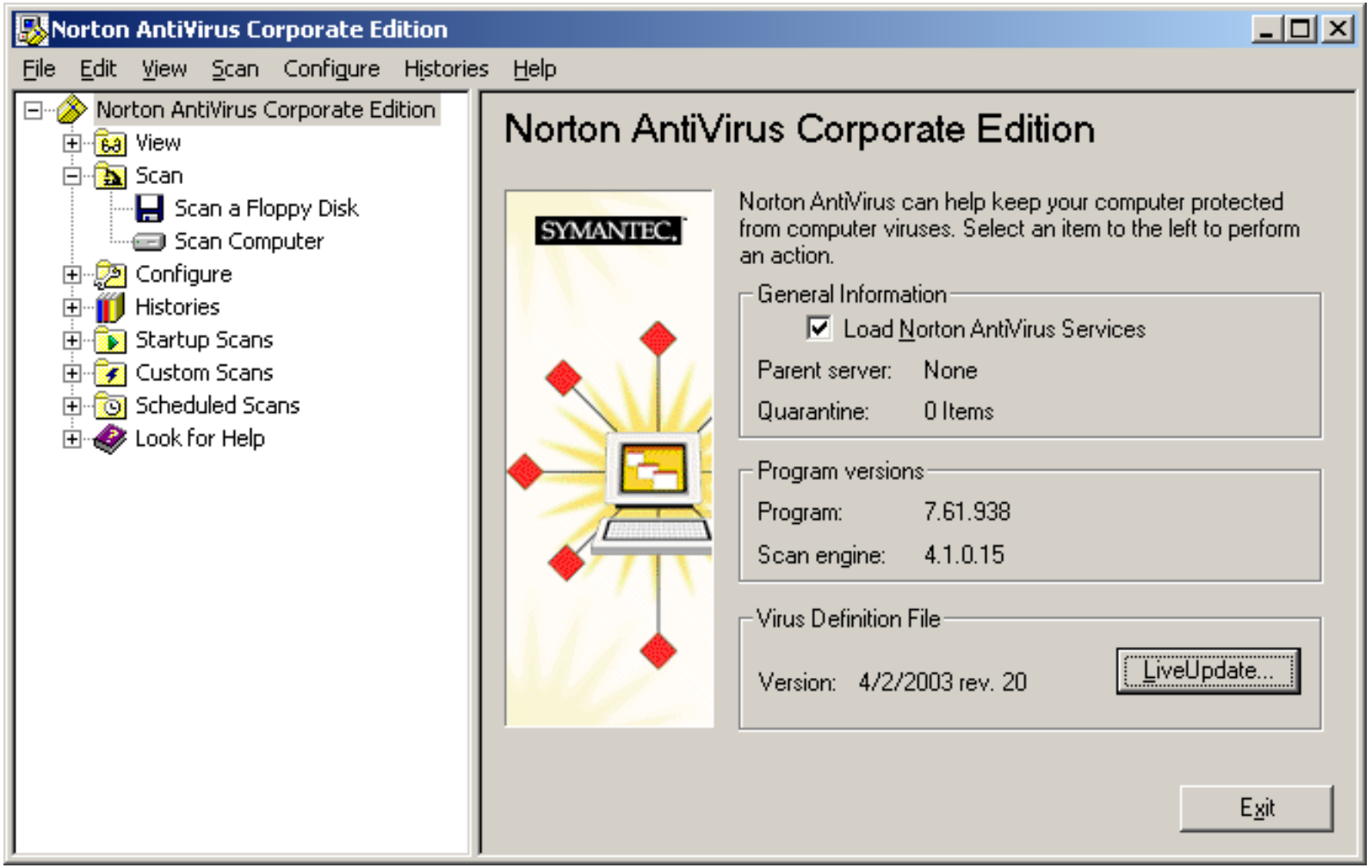


image: http://www.activewin.com/reviews/software/utils/v/vscan5d/images/PGP.jpg
PGP by PGP Corporation and can be found at http://www.pgp.com/

Norton Antivirus



Norton Antivirus by Symantec Corp can be found at http://www.symantec.com/

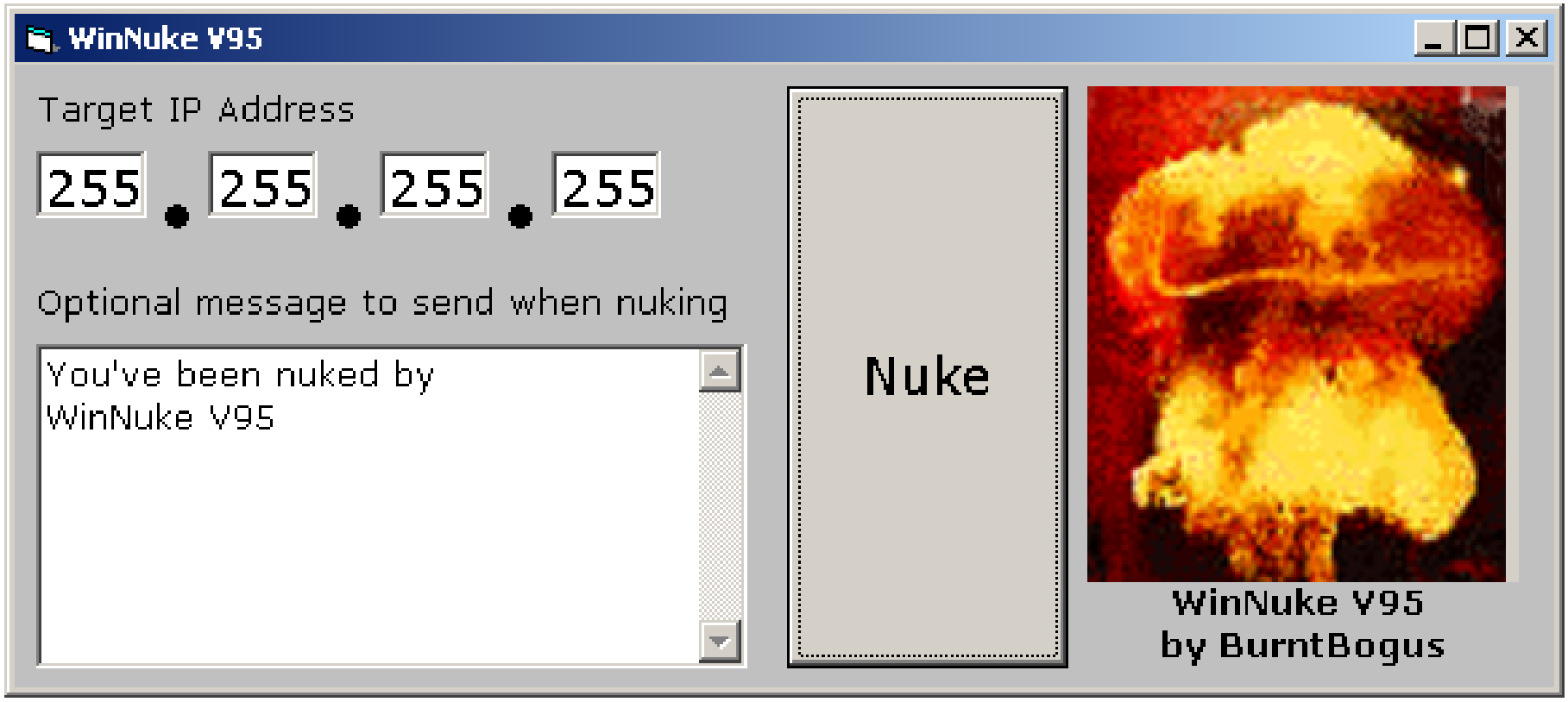
Example Redesigns

image: http://www.noderunner.net/~sparks/art/render/nasako-gym-anime.gif by Rachel Blackman, used with permission

Win Nuke V95

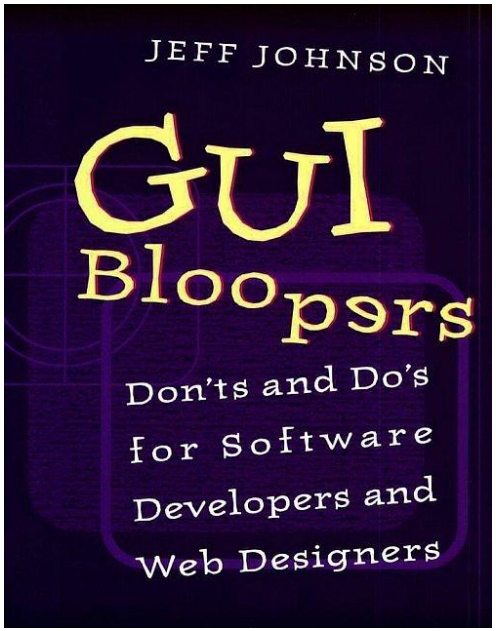
image: http://www.computec.ch/
WinNuke V95 is by BurntBogus and its location changes

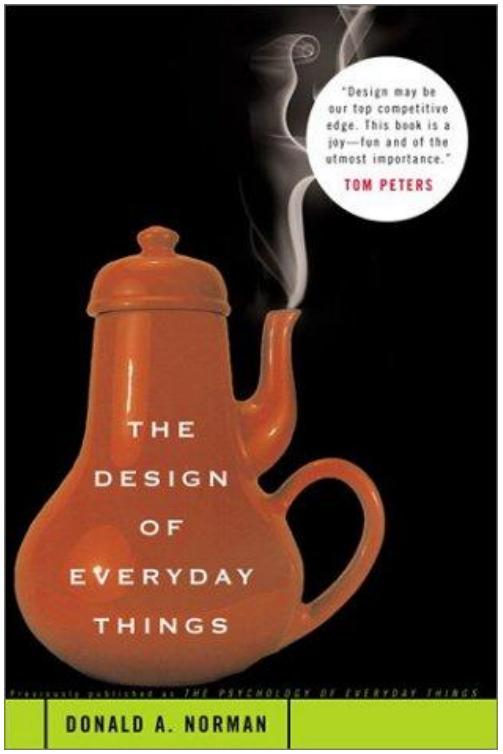
WinNuke 95 Redesign

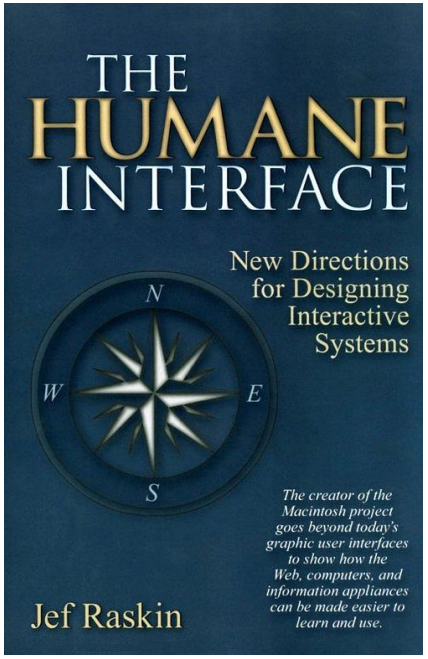


More Information

Big Picture







GUI Bloopers by Jeff Johnson

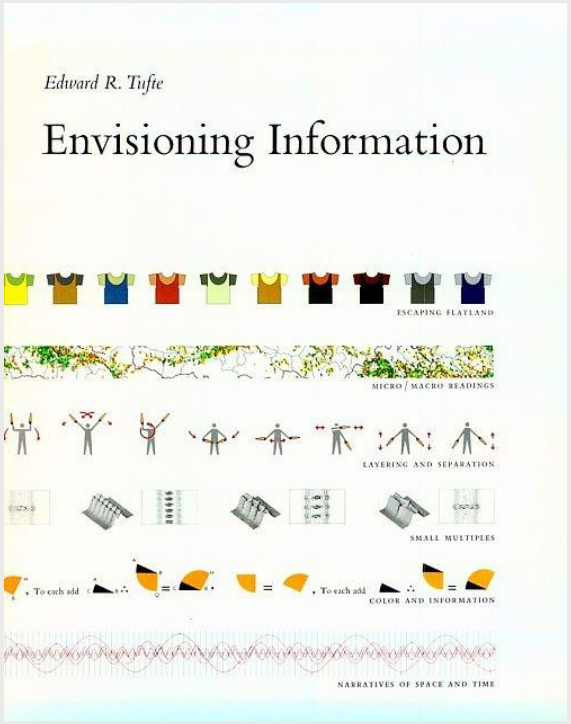
The Design of Everyday Things by Donald Norman

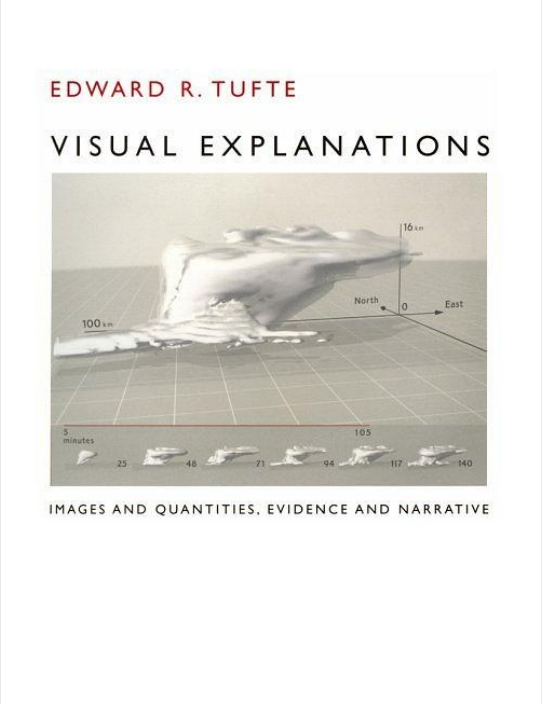
The Humane Interface by Jef Raskin

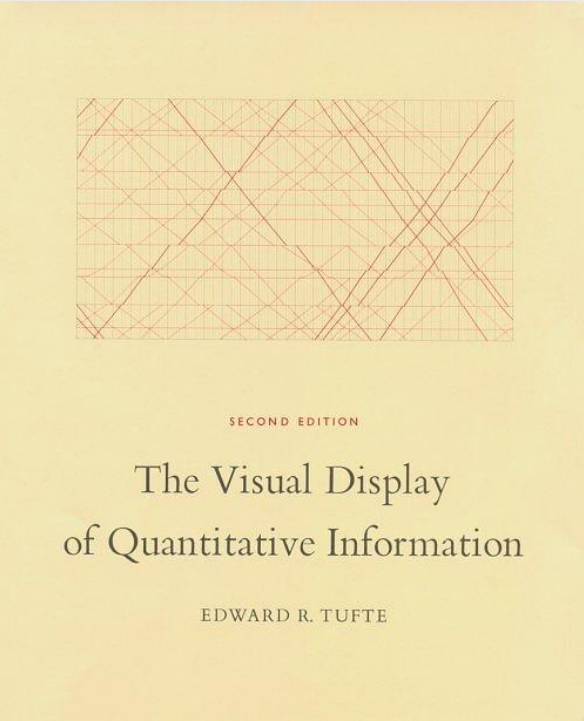
images: www.amazon.com

More Information

Information Visualization







Envisioning Information by Tufte

The Visual Display of Quantitative Information by Tufte

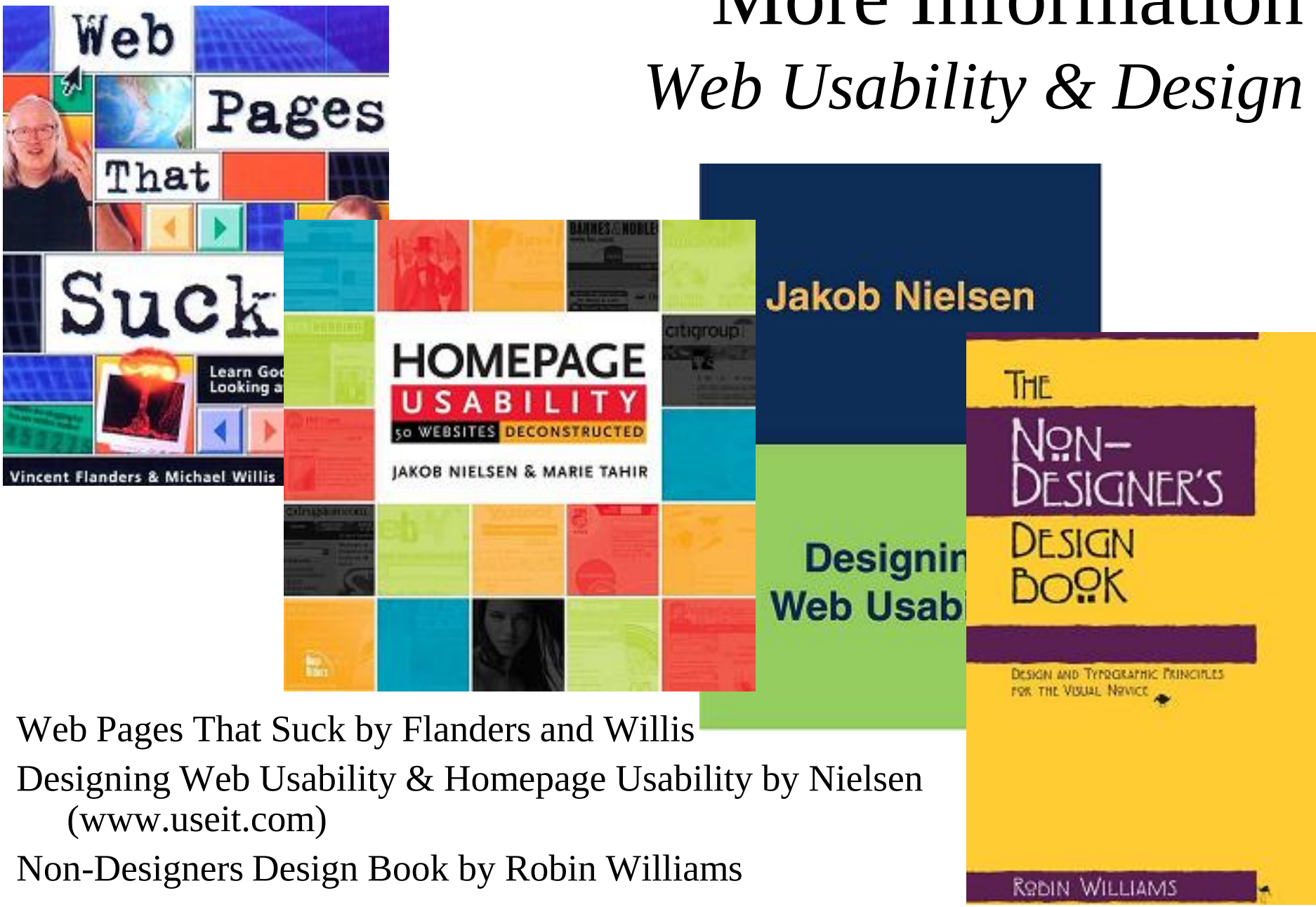
Visual Explanations by Tufte

See also the Tufte road show, details at www.edwardtufte.com

images: www.amazon.com

More Information

Web Usability & Design

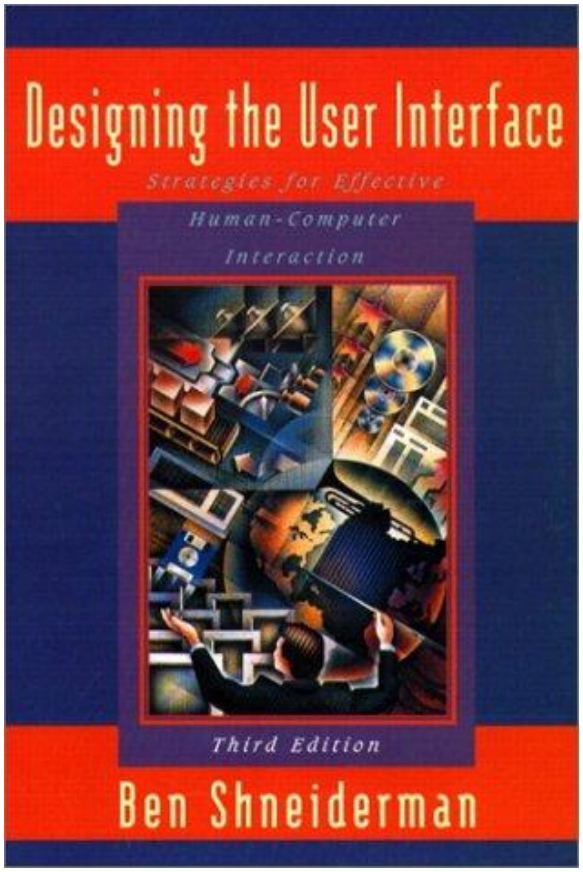


Web Pages That Suck by Flanders and Willis

Designing Web Usability & Homepage Usability by Nielsen (www.useit.com)

Non-Designers Design Book by Robin Williams

images: www.amazon.com



Deep Knowledge…

Designing the User Interface by Ben Shneiderman

Association for Computing Machinery
Special Interest Group for Computer Human Interaction (SIGCHI)
www.acm.org/sigchi

CHI image: http://sigchi.org/chi2004/
Book image: www.amazon.com

There are 10 types of people who understand interface design: those that do and those that don’t…

Your Questions???

http://www.microsoft.com/presspass/events/officexp/images/launch02.jpg