

HACKING VIDEO TUTORIAL TIPS: GETTING THE POINT ACROSS WITH SCREENCASTING COMPUTER VIDEOS

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

Sometimes my presentations are like this.



And sometimes my presentations are like this.



Qualifications

- ▣ I've been doing this for awhile
- ▣ I have a lot of time on my hands
- ▣ Do a Google search for Hacking Videos



How I got started with all this

- ▣ I found CamStudio
- ▣ Tools like Cain have a hard to describe interface
- ▣ Slacked off for awhile.....
- ▣ Saw “The Broken” and got back into it (Jeer if you feel like it)



Why videos?

- ▣ Too many fuckers using GUIs
- ▣ Easier to show visually what to do in a GUI than it is to write about it in text
- ▣ Vista rant time (Click Start? What Start?)
- ▣ Some hackers/managers are too lazy to read
- ▣ Some concepts are easier to understand when illustrated visually



TOOLS

Apps I use to make my Hacking Illustrated
videos



CamStudio

<http://www.irongeek.com/i.php?page=CamStudioOSS/camstudio>

<http://camstudio.org/>

- ▣ Captures video of Windows desktop
- ▣ Can make SWF and AVI output
- ▣ Can do sound
- ▣ Webcam picture-in-picture

Tips:

- ▣ Use 5 frames per sec
- ▣ CamStudio lossless codec is great for screen captures

Alternatives:

- ▣ Wink
<http://www.debugmode.com/wink/>
- ▣ iShowU
<http://store.shinywhitebox.com/home/home.html>



<http://Irongeek.com>

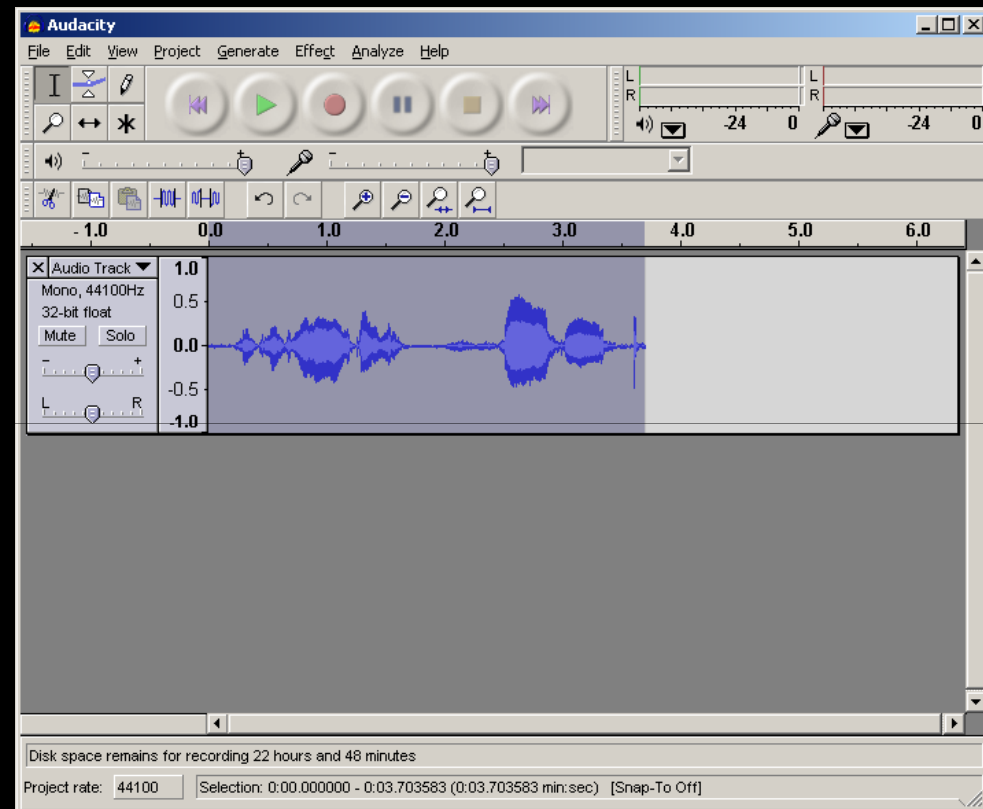
Audacity

<http://audacity.sourceforge.net/>

- Record and edit audio with ease

Tips:

- Great noise removal
- Save as WAV so as to avoid double lossy compression



VNC

<http://en.wikipedia.org/wiki/Vnc>

- ▣ Remote GUI program supported by about every platform you can imagine

Tips:

- ▣ Use when you can't use a VM, the Nokia n810 for example

Alternatives:

- ▣ MyMobiler for Windows Mobile
<http://www.mymobiler.com>
- ▣ RDP



VMWare

<http://www.vmware.com/products/player/>

<http://vmxbuilder.com/>

☐ Hot OS in OS Action!

Tips:

- ☐ USB host support works well for some USB devices
- ☐ WiFi USB is hit or miss RALINK chip sets are pretty good

Alternatives:

- ☐ VirtualBox
<http://www.virtualbox.org/>
- ☐ Many others

<http://Irongeek.com>

```
BT4-Beta VMware Player  Devices  [ - ] [ x ]

<< back | track 龍
<< back | track 龍

* Setting kernel variables (/etc/sysctl.d/10-network-security.conf)... [ OK ]
* Setting kernel variables (/etc/sysctl.d/10-process-security.conf)... [ OK ]
* Setting kernel variables (/etc/sysctl.d/wine.sysctl.conf)... [ OK ]
* Activating swap... [ OK ]
* Starting early crypto disks... [ OK ]
* Starting remaining crypto disks... [ OK ]
* Checking file systems... [ OK ]
fsck 1.41.3 (12-Oct-2008)
* Mounting local filesystems... [ OK ]
* Activating swapfile swap... [ OK ]
* Skipping firewall: ufw (not enabled)... [ OK ]
* Setting up console font and keymap... [ OK ]
* Loading ACPI modules... [ OK ]
* Starting ACPI services... [ OK ]
* Starting system log daemon... [ OK ]
* Doing Wacom setup... [ OK ]
* Starting kernel log daemon... [ OK ]
* Starting system message bus dbus [ OK ]
Checking acpi hot plug done
Starting VMware Tools services in the virtual machine:
Switching to guest configuration: done
Guest memory manager: done
Guest vmxnet fast network device: done
VM communication interface: done
VM communication interface socket family: done
Blocking file system: done
Guest operating system daemon: done
Virtual Printing daemon: done
* Starting Hardware abstraction layer hald [ OK ]

BackTrack 4 Beta bt tty1
bt login:

"The quieter you become, the more you are able to hear."

To direct input to this virtual machine, press Ctrl+G. [ vmware ]
```



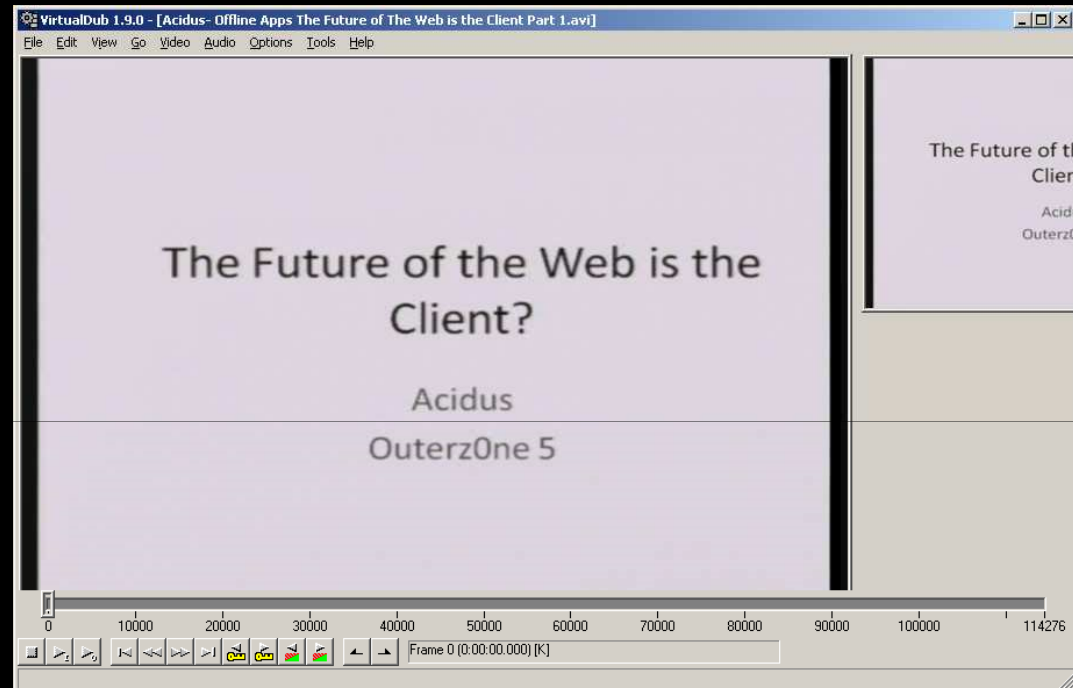
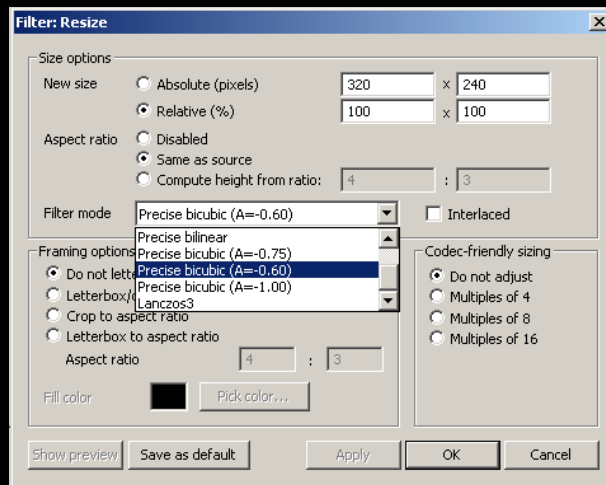
VirtualDub

<http://www.virtualdub.org/>

- ❑ Simple linear video editor

Tips:

- ❑ Add and remove frames to sync videos with sound
- ❑ When you resize, use Bicubic 0.60 or Lanczos3



<http://Irongeek.com>

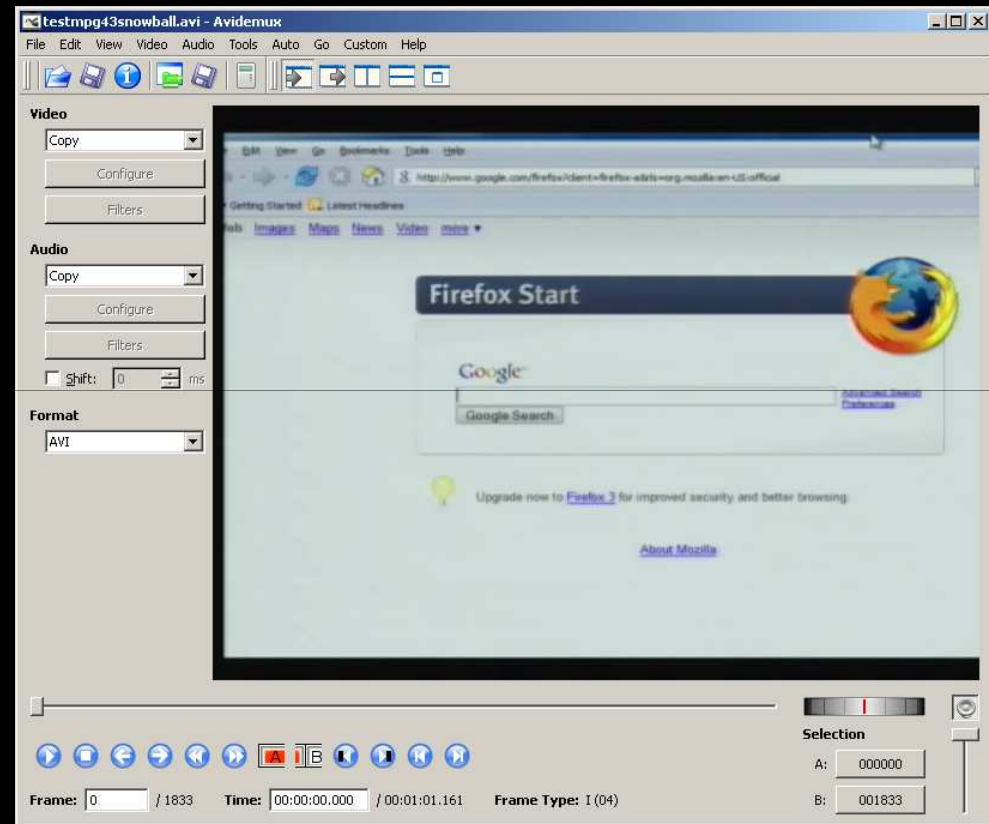
AVIDemux

<http://avidemux.berlios.de/index.html>

- ❑ Convert between just about any video formats

Tips:

- ❑ Use when VirtualDub barfs on your input
- ❑ VirtualDub is mostly for AVIs, AVIDemux works with a lot more media formats



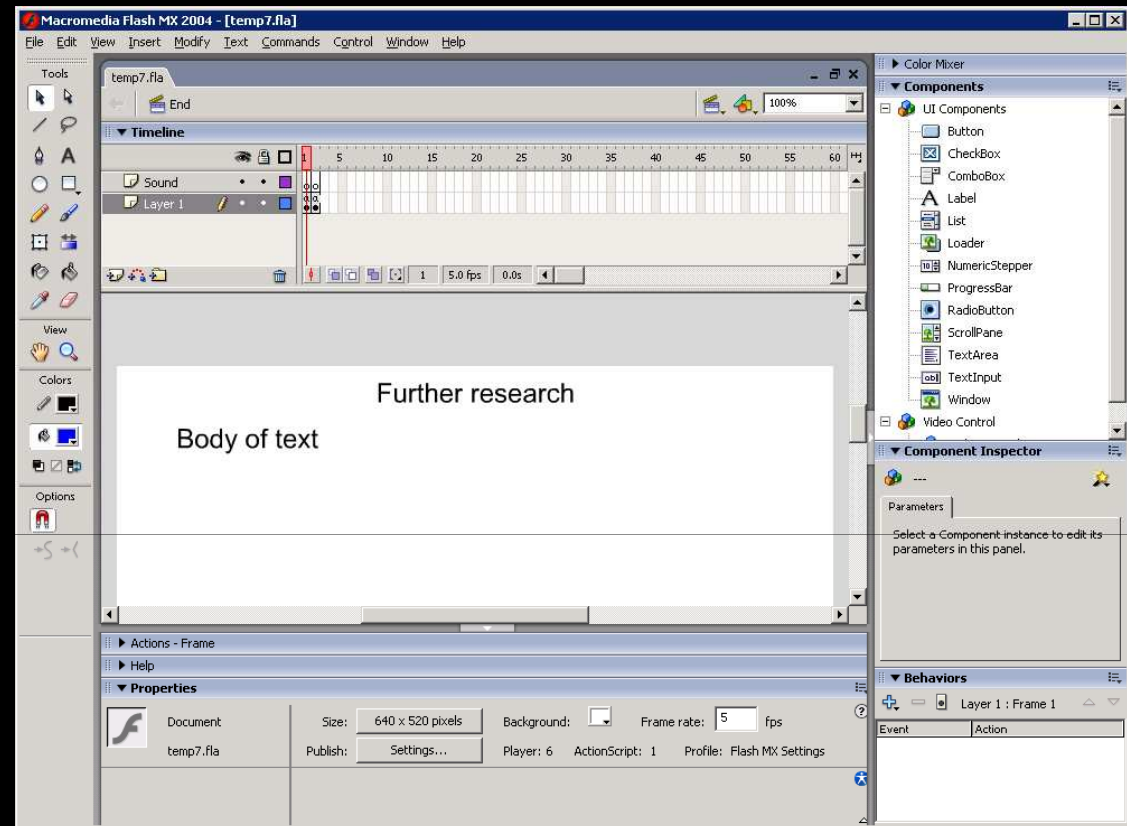
<http://Irongeek.com>

Flash MX 2004

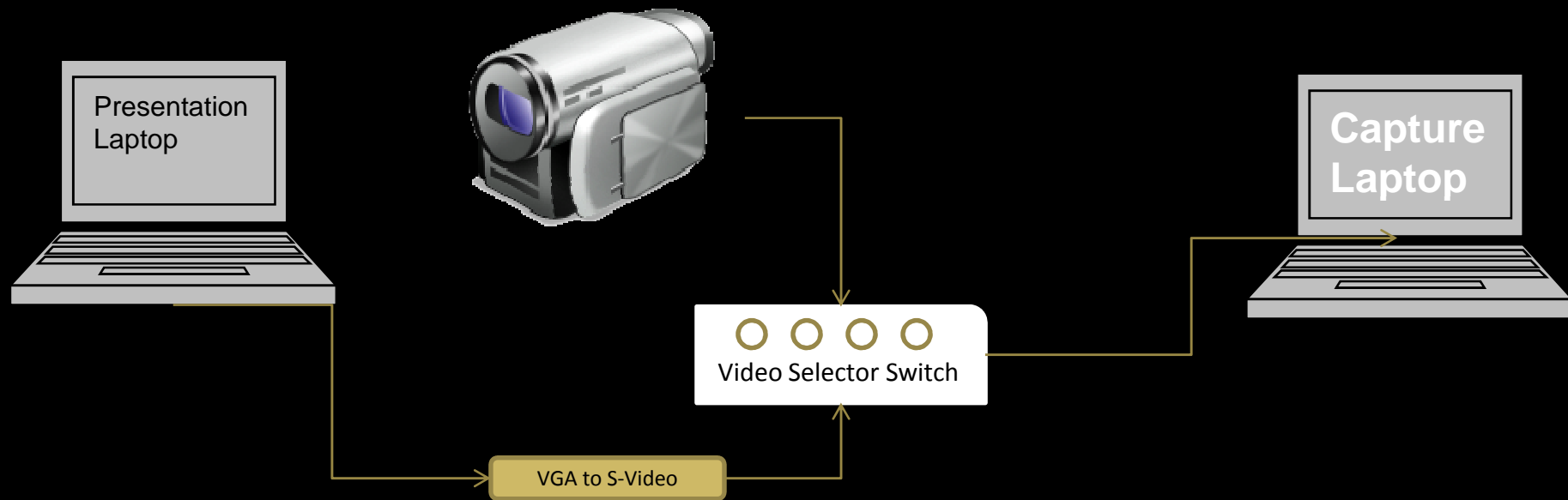
- ❑ Great animation tool whose output is supported by most clients

Tips:

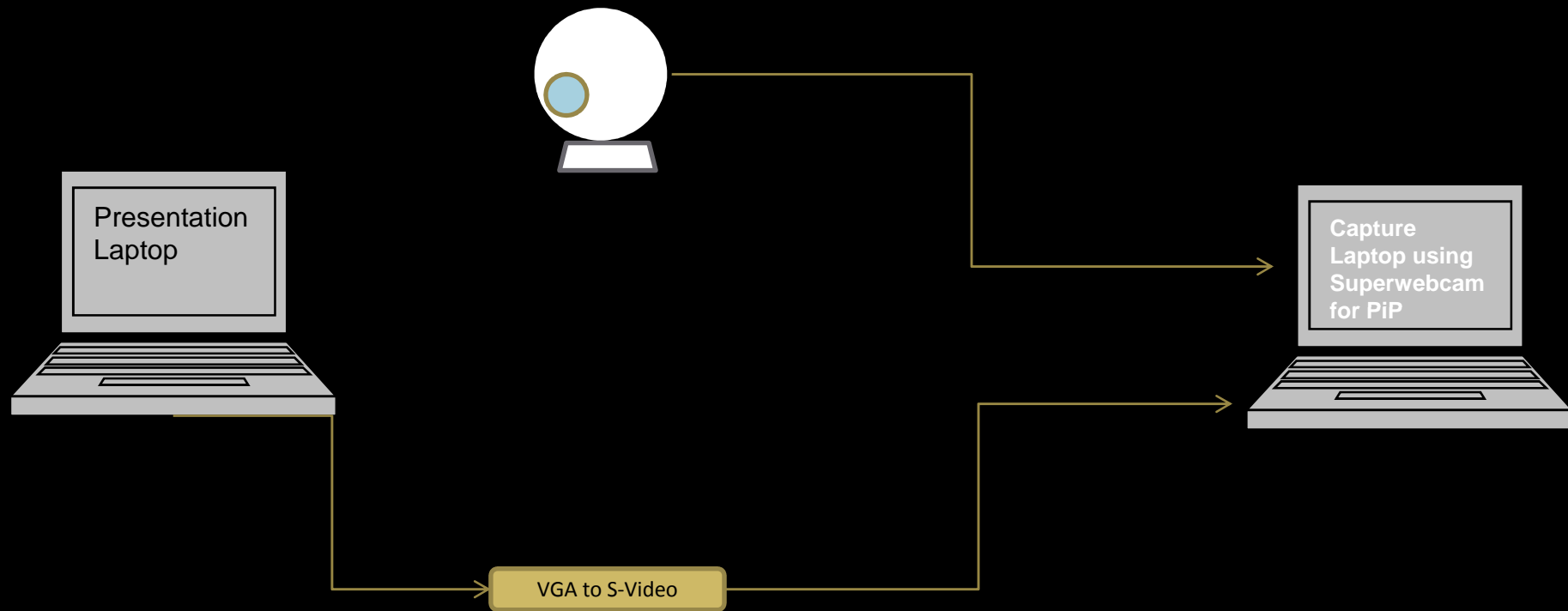
- ❑ I started to use it since it allows you to embed links. Even if someone rips off my content, at least I get links back to my site.
- ❑ Stop whining about your BSD on ARM CPU not supporting it.



Live Class Captures



Superwebcam Method



<http://www.superwebcam.com/>

<http://Irongeek.com>



Places to host your videos

http://en.wikipedia.org/wiki/Comparison_of_video_services

▣ YouTube

<http://www.youtube.com/>

▣ Vimeo

<http://www.vimeo.com/>

▣ BlipTV

<http://blip.tv/>



Tips

- ▣ Write notes before you begin
- ▣ Practice the series of steps before recording (well, I thought that worked)
- ▣ Consider if you want to record live, or add the audio after you record the video
- ▣ Concentrate on the audio
- ▣ Avoid my pet peeves

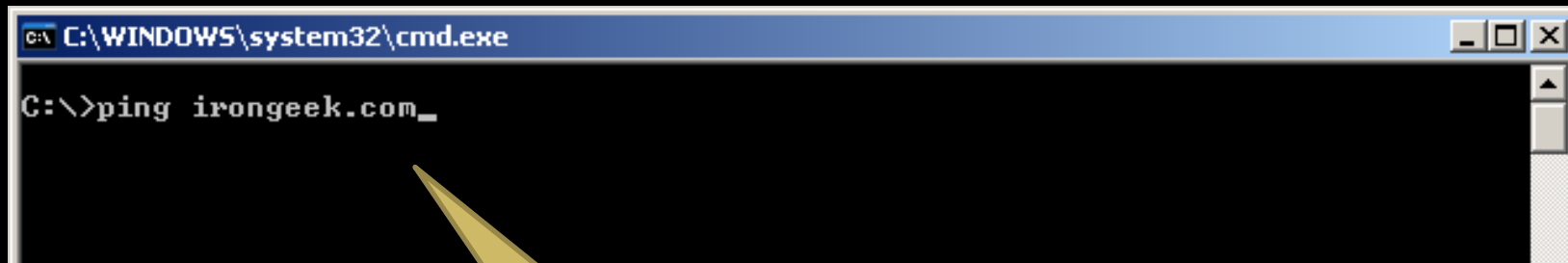


PET PEEVES

I've got more of these than tips



Narrate it!!! It's a video, not an article damn it!

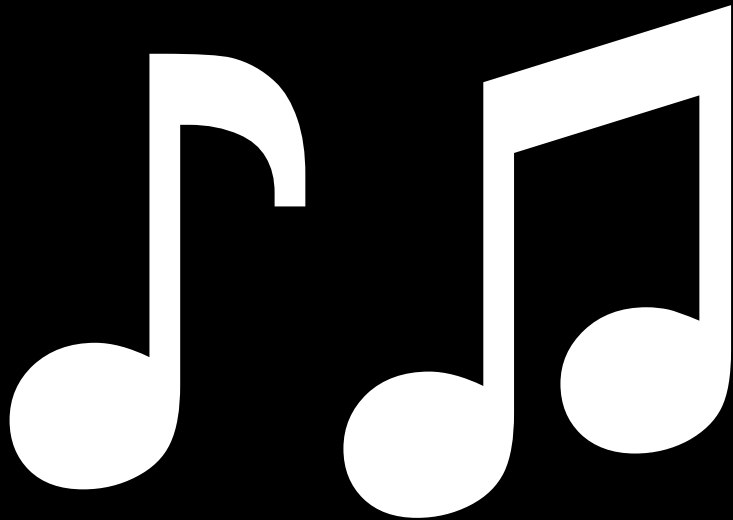


```
C:\WINDOWS\system32\cmd.exe
C:\>ping irongeek.com_
```

Ping is this nifty command that sends and ICMP echo message to a host and hopes to get a reply back. Unfortunately, sometimes folks block all ICMP traffic, which causes this to not always give valid results. Now I could have explained all of this to you my saying it in the audio of this video, but I don't like the way my voice sounds or I'm just lazy so I'll type it all out and hope you can read it in the 1.5 seconds that it stays on the screen.

Commercial music

- ▣ MAF(R)IAA?
- ▣ Stop with the fscking techno!!!



High video resolution (file size and readability)

The screenshot displays the Oxid IT web interface. The main content area shows a table of network devices with the following data:

| Status | IP address | MAC address | Packets -> | <- Packets | MAC address | IP address |
|--------|-------------|--------------|------------|------------|--------------|-------------|
| Idle | 10.10.10.10 | 000C2954ED9C | | | 000C2906F099 | 10.10.10.60 |
| Idle | 10.10.10.10 | 000C2954ED9C | | | 000C29C46748 | 10.10.10.20 |
| Idle | 10.10.10.50 | 000C2903AB8C | | | 000C2906F099 | 10.10.10.60 |
| Idle | 10.10.10.20 | 000C29C46748 | | | 000C2903AB8C | 10.10.10.50 |
| Idle | 10.10.10.10 | 000C2954ED9C | | | 000C2903AB8C | 10.10.10.50 |
| Idle | 10.10.10.20 | 000C29C46748 | | | 000C2906F099 | 10.10.10.60 |

The interface includes a sidebar with navigation options like 'APR', 'APR-Cert', 'APR-DNS', 'APR-SSH-1 (0)', 'APR-HTTPS (0)', 'APR-RDP (0)', 'APR-FTPS (0)', 'APR-POP3S (0)', 'APR-IMAPS (0)', and 'APR-LDAPS (0)'. The bottom status bar shows 'Configuration / Routed Packets' and a taskbar with icons for 'Hosts', 'APR', 'Routing', 'Passwords', and 'VoIP'. The browser address bar shows 'http://www.oxid.it'.



Explain the whys, not just the hows

- ▣ Fine, you can h@x0r the Gibson, but why does this work?
- ▣ People should learn why an attack/defense works so that when something goes wrong when “just typing in commands” they have some idea as to why.



Events

- ▣ Free ISSA classes
- ▣ ISSA Meeting
<http://issa-kentuckiana.org/>
- ▣ Louisville Infosec
<http://www.louisvilleinfosec.com/>
- ▣ Phreaknic/Notacon/Outerz0ne
<http://phreaknic.info>
<http://notacon.org/>
<http://www.outerz0ne.org/>



Thanks

▣ Binrev

<http://www.binrev.com/>

▣ Pauidotcom

<http://pauidotcom.com/>

▣ Infonomicon

<http://nomicon.info/>



QUESTIONS?

42

