

How to Do File-sharing Without Getting Caught

Ken Takusagawa

ESP Splash!

Saturday, November 21, 2009

<http://mit.edu/kenta/www/one/file-sharing-splash>

Example

Frostwire, a file-sharing application

RIAA Lawsuit

- ▶ They see a file is available on file-sharing.
- ▶ Find the IP address
- ▶ Subpoena the ISP for the customer
- ▶ then...

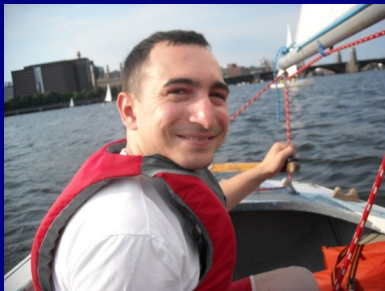
RIAA Lawsuit

- ▶ Pre-lawsuit settlement offer, \$4,000
- ▶ Lawsuit
- ▶ Settlement offers for much more than \$4,000

RIAA Lawsuit

Two cases have gone to trial.

- ▶ Capitol v. Thomas, \$1.92 million in favor of Capitol (2007-July 2009)
- ▶ RIAA v. Tenenbaum, \$675,000 in favor of RIAA (July 2009, Massachusetts)



The law is depressing

- ▶ “Making available” constitutes copyright infringement.
- ▶ Illegal items will be marked with red slides.

The law is depressing

- ▶ Political activism to change the law, later...

How to do file-sharing without getting caught

- ▶ Hide who you are
- ▶ Make it look like it was someone else
- ▶ Thwart being able to prove it was you

How does the Internet work?

- ▶ What is an Internet address (IP address)?
- ▶ How does data navigate the Internet?

The acronym IP

IP

- ▶ Intellectual Property
- ▶ Internet Protocol

Internet Protocol

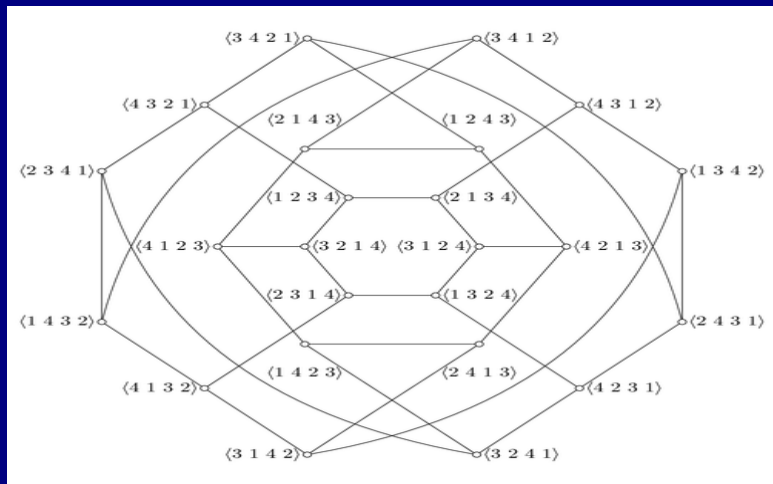
- ▶ RFC 791, a document defining the Internet Protocol
- ▶ How the Internet works is public knowledge, in RFCs

IP Packet

bit offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	Differentiated Services	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160 or 192+	Data				

Bits 96 through 127 are the source address.

Routing network



Routers decide which way to send packets.

TCP Segment goes inside IP Data

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset	Reserved						C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size																
128	Checksum																Urgent pointer															
160	Options (if Data Offset > 5)																															
...	...																															
160+	Data																															

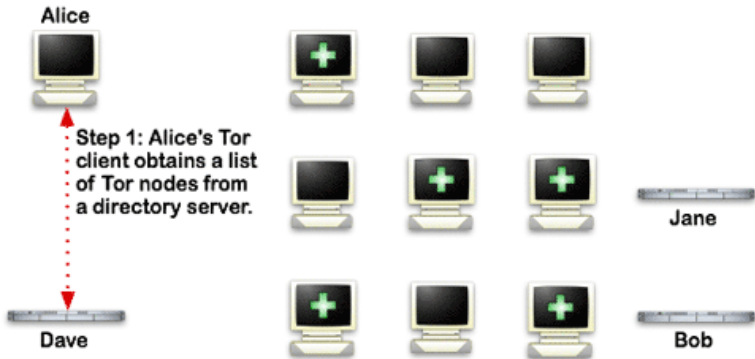
What shall we put in the TCP data? Anything!

Hide who you are: Tor



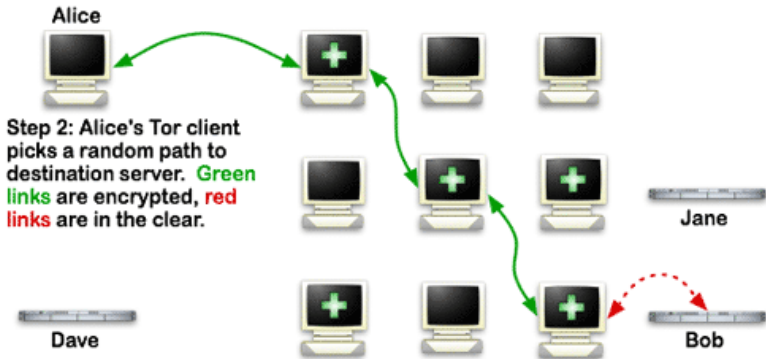
- ▶ Tor: The Onion Router

How Tor Works: 1



How Tor Works: 1

How Tor Works: 2



How Tor Works: 2

How Tor Works: 3



Alice



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, **green links** are encrypted, **red links** are in the clear.



Dave



Jane



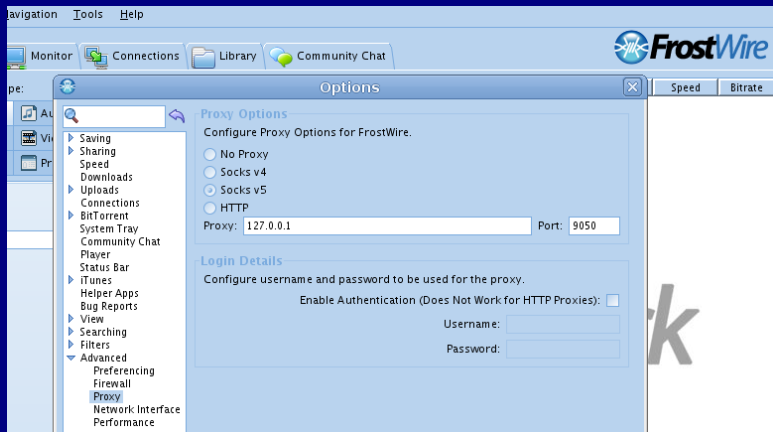
Bob

How Tor Works: 3

Safe harbor in the law

- ▶ The “Transitory Network Communications Safe Harbor” provision of the Online Copyright Infringement Liability Limitation Act, originally meant to protect Internet Service Providers (ISPs).
- ▶ The RIAA will probably try to change this if Tor gets popular.

Configuring FrostWire for Tor



I don't know if this works!

Tor Hidden Services

- ▶ Internet sites inside the Tor network
- ▶ <http://gaddbiwdftapglkq.onion/>

Leaking information

- ▶ Post files on a hidden service, no one can discover the location of the hidden service
- ▶ But post a file with your identifying information, you lose
- ▶ Often legally purchased downloaded music has identifying markers
- ▶ One mistake is all it takes

Hide who you are: Freenet

Freenet

- ▶ Stores a copy of data along the routing path
- ▶ Whom do you initially trust?



<http://localhost:8081/MSK%40SSK%40enI8YFo3gj8UVh-Au0HpKMftf6QQAgE/homepage//>

Hide who you are: I2P

I2P (formerly Invisible Internet Project)

- ▶ I2Phex, a file-sharing program
- ▶ Hidden Eepsites: <http://forum.i2p>

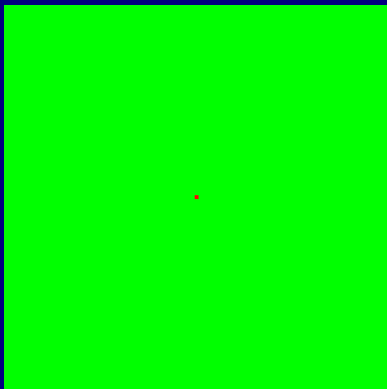
Hide who you are: Perfect Dark

Perfect Dark

- ▶ Another file-sharing program.
- ▶ Originally Japanese.
- ▶ Never trust a security program that's closed source.
- ▶ (It's closed source because it's BETA.)

These programs are slow

- ▶ Imagine the Internet a generation ago: 300 bits per second.
- ▶ Today 3,000,000 bits per second



These programs are new

- ▶ Difficult to use without leaking privacy
- ▶ Tor does not want you doing file-sharing; they worry it will overload the network.
- ▶ Under development. Do you trust \$1.92 million on BETA software?

Hide who you are

- ▶ The RIAA has not broken these cryptographic methods, yet.
- ▶ The RIAA has not tried, yet.
- ▶ They will probably go after the software authors. *MGM v. Grokster*

How to do file-sharing without getting caught

- ▶ Hide who you are
- ▶ Make it look like it was someone else
- ▶ Thwart being able to prove it was you

Make it look like it was someone else

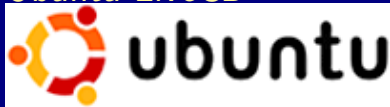
- ▶ Use someone else's computer
- ▶ Use someone else's network

Use someone else's computer, legally

- ▶ What is being logged on the computer?
- ▶ Did you use GMail, Facebook, at the same time?
- ▶ Who saw you? Fingerprints on the keyboard?

Use someone else's computer, legally

Ubuntu LiveCD



USB pen drive possible, too.

Use someone else's computer, illegally

reboot into Ubuntu LiveCD



USB pen drive possible, too.

Break into someone else's computer

- ▶ Install a rootkit
- ▶ Use Tor, etc. to connect to the broken-into computer
- ▶ Follow how computer viruses work

Penalties for computer crime are VERY high

- ▶ Professional computer crime is hard to catch. Spam is illegal, but prevalent.
- ▶ If you get caught, the penalties are EXTREMELY high. They will make an example out of you.
- ▶ It's always the beginners who get caught (that's you).

Demonstration: simple Linux rootkit

```
sudo su  
adduser  
visudo  
sudo aptitude install openssh-server  
ifconfig
```

Legal defense

Look at all these people who could have hacked my computer!



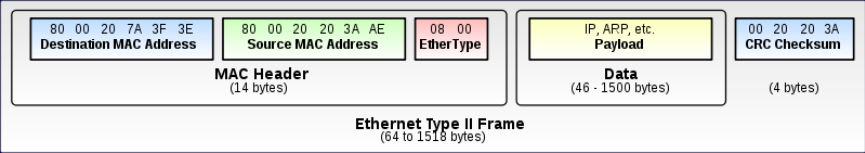
Rent a computer in someone else's name

- ▶ Identity Theft
- ▶ Managed Hosting

Use someone else's network

- ▶ Use your computer on someone else's network.
- ▶ Open wireless

Ethernet frame



Media Access Control (MAC) address

MAC addresses

- ▶ Beware: it is possible for someone to determine the MAC address of who is on their network.
- ▶ Solution: change MAC address

IP Packet

bit offset	0-3	4-7	8-15	16-18	19-31
0	Version	Header length	Differentiated Services	Total Length	
32	Identification			Flags	Fragment Offset
64	Time to Live		Protocol	Header Checksum	
96	Source Address				
128	Destination Address				
160	Options				
160 or 192+	Data				

Bits 96 through 127 are the source address.

TCP Segment goes inside IP Data

Bit offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	Source port																Destination port															
32	Sequence number																															
64	Acknowledgment number																															
96	Data offset	Reserved						C W R	E C E	U R G	A C K	P S H	R S T	S Y N	F I N	Window Size																
128	Checksum																Urgent pointer															
160	Options (if Data Offset > 5)																															
...	...																															
160+	Data																															

What shall we put in the TCP data? Anything!

Break into someone else's wireless network

- ▶ Obtain the wireless password by social engineering
- ▶ Obtain the wireless password by Aircrack-ng

Wireless hacking

- ▶ Try breaking your own wireless
- ▶ Slitaz Aircrack-ng LiveCD

Wireless hacking

There are two types of wireless security

- ▶ WEP: cipher called RC4 broken
- ▶ WPA 1 and 2: not broken, Need to do brute force password search

How to do file-sharing without getting caught

- ▶ Hide who you are
- ▶ Make it look like it was someone else
- ▶ Thwart being able to prove it was you

Thwart being able to prove it was you

- ▶ Keep your own wireless open

Choose your ISP

Choose an ISP which keeps records of IP addresses and customer records as short as possible.
(Cambridge, MA has only three ISPs: Comcast, Verizon, and Speakeasy.)

Encrypt your hard drive

- ▶ Windows: Truecrypt, others...
- ▶ Linux: built-in, encfs
- ▶ Mac: FileVault

How the RIAA might defeat disk encryption

- ▶ Backups
- ▶ iPod
- ▶ Subpoena family and friends to testify against you

Allow virus infection

- ▶ Legal defense: look, there's a rootkit installed!
- ▶ At the moment, I don't recommend this.

History



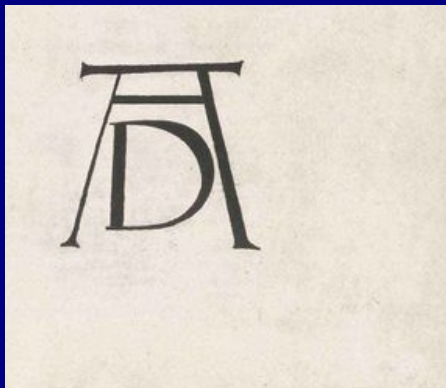
Jewish Sefer Torah, authored by Moses, 500 BCE,
no copyright

History



Raimondi copies Durer, 1500s.

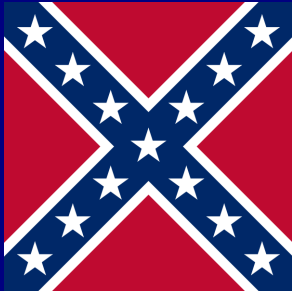
History



Albrecht Durer has a right to his signature, only.

Digression: Federal Law vs. State Law

- ▶ Copyright in the U.S. is a federal law
- ▶ If it were a state law, different states could have different standards.
- ▶ Raimondi skipped town.
- ▶ Why does federal law trump state's rights?



The tradition of derivative works

- ▶ Who wrote Shakespeare's plays? Ovid?
- ▶ Romeo and Juliet, Pyramus and Thisbe
- ▶ Who wrote Shakespeare's plays? They forgot!

Copyright in the modern age

- ▶ The printing press
- ▶ Copying became easier
- ▶ The creator's status becomes elevated
- ▶ Copyright holders become rich and powerful

Political activism

Change the law

Serve on a jury

- ▶ Capitol v. Thomas, \$1.92 million
- ▶ RIAA v. Tenenbaum, \$675,000

These were jury trials.

Jury Nullification



- ▶ Vote your conscience, regardless of the letter of the law.
- ▶ The judicial branch checks and balances the legislative branch of government.

Donate to political action

Electronic Frontier Foundation



Run for office

- ▶ Senate (30 years)
- ▶ Representative (25 years)
- ▶ City councillor (no age limit)

Lawrence Lessig, *Free Culture, How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* as a political platform.

Teach

Teach privately.

This class's slides are online.

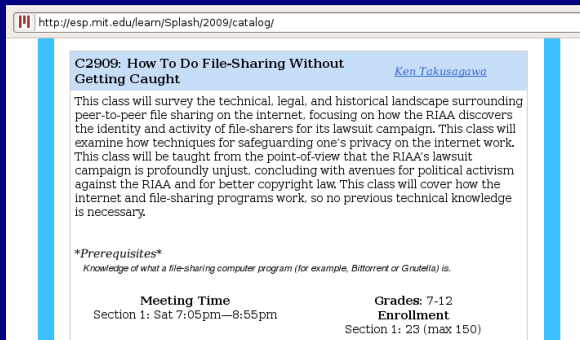
<http://mit.edu/kenta/www/one/file-sharing-splash>

Civil disobedience through dissemination of
knowledge.

Teach

Teach publicly!

- ▶ People know it's been taught.
- ▶ But be prepared for resistance.



http://esp.mit.edu/learn/Splash/2009/catalog/

C2909: How To Do File-Sharing Without Getting Caught *Ken Takusagawa*

This class will survey the technical, legal, and historical landscape surrounding peer-to-peer file sharing on the internet, focusing on how the RIAA discovers the identity and activity of file-sharers for its lawsuit campaign. This class will examine how techniques for safeguarding one's privacy on the internet work. This class will be taught from the point-of-view that the RIAA's lawsuit campaign is profoundly unjust, concluding with avenues for political activism against the RIAA and for better copyright law. This class will cover how the internet and file-sharing programs work, so no previous technical knowledge is necessary.

Prerequisites
Knowledge of what a file-sharing computer program (for example, BitTorrent or Gnutella) is.

Meeting Time Section 1: Sat 7:05pm—8:55pm	Grades: 7-12 Enrollment Section 1: 23 (max 150)
---	---

Original class description

This class will survey the technical, legal, and political landscape surrounding peer-to-peer file sharing on the internet. The class will mainly focus on the technical aspects of how the RIAA discovers the identity of file-sharers for its lawsuit campaign, and countermeasures that you the file-sharer can take to avoid being discovered or avoid being sued. Before getting into the technical details of countermeasures, this class will cover how the internet works, so no previous knowledge of how the internet or computers work is necessary.

Hi Ken,

In the interests of time, here are the changes we want in plain terms:

- Delete from your description any references which imply that students should be engaging in this activity. (eg, "you the file-sharer")
- Delete from your description any mention of "avoiding getting sued" or other references which imply that students can engage in risky behavior without suffering potentially devastating consequences.

More generally, please treat your students and this subject with appropriate respect.*

We do not wish to discourage you from examining the controversy surrounding recent rulings and the question of copyright and illegal file-sharing, nor even from explaining technical countermeasures that safeguard one's privacy. However, you may not encourage fundamentally unsafe behavior through our programs.

If you agree to these changes, let us know and we'll try to find an open classroom.

Attributions

Jury Box: <http://flickr.com/photos/22691745@N00/387561128>

How Tor Works: <http://www.torproject.org/overview.html>

Internet packet: <http://en.wikipedia.org/wiki/IPv4>

TCP Segment: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Network: <http://www.texample.net/tikz/examples/pancake-network/>

Torah: Willy Horsch, <http://tinyurl.com/yfkg5e5>

Joel Tenenbaum: http://en.wikipedia.org/wiki/File:Joel_Tenenbaum.jpg

Visual Aids

- ▶ Cat5 cable
- ▶ Router
- ▶ Torah
- ▶ Ubuntu LiveCD
- ▶ Camera for class photo

This work is licensed under the Creative Commons Attribution-Share Alike 3.0 United States License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/us/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.



Break

The key to fascism is to not let people talk.