Saving Cyberspace by Reinventing File Sharing

Eijah

v1.0

The Modern Internet

A Price of Convenience

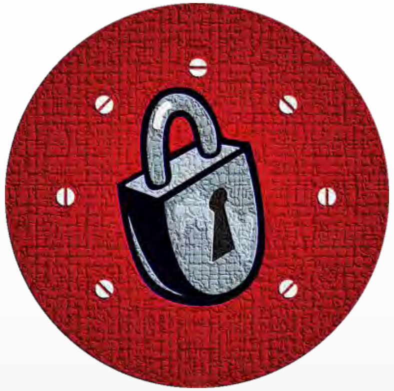
“…One can easily remain free of even the most intense political oppression simply by placing one’s faith and trust in institutions of authority.”
– *Glenn Greenwald*

“When I am afraid, I put my trust in you.”
– *Psalm 56:3*

A State of Change

- The Argument
  - Internet access is a basic human right
  - We have the right to share our content freely
- The Modern Internet
  - The right to share files online has been under assault
  - Governments, corporations and others fear openness
  - Losing our fundamental rights to privacy and personal beliefs
- The Goal
  - Individual privacy rights and freedoms are protected
  - Digital self-expression is commonplace and encouraged

A State of Unity and Distrust



- Corporations and 3rd Parties
    - Ubiquitous and pervasive computing
    - Interoperability through industry standards
    - Data breaches, financial repercussions, erosion of trust, and the bottom line
- Users
    - Division between an individual and his/her data
    - Are we greater than the sum of our personal data?
    - Who owns our information?
- Governments and Enforcers
    - Data aggregation and mining
    - The ease of accountability
    - Unlawful transparency

A State of Recovery

- The Qualifications
  - Experts in our fields
  - An arsenal of tools, experiences, and technologies
  - We choose not to live in a world of illegal surveillance
- The Right to Share
  - Data manifesto
  - A recipe for changing the world
  - The path to limitless file sharing
  - Secure transfer of personal information between all of your devices, from anywhere in the world
  - Understanding our right to share is the first step

A Brief History

From FTP to µTorrent

“The increase of disorder or entropy is what distinguishes the past from the future, giving a direction to time.”
– Stephen Hawking, A Brief History of Time

“Information is power. But like all power, there are those who want to keep it for themselves.”
– Aaron Swartz

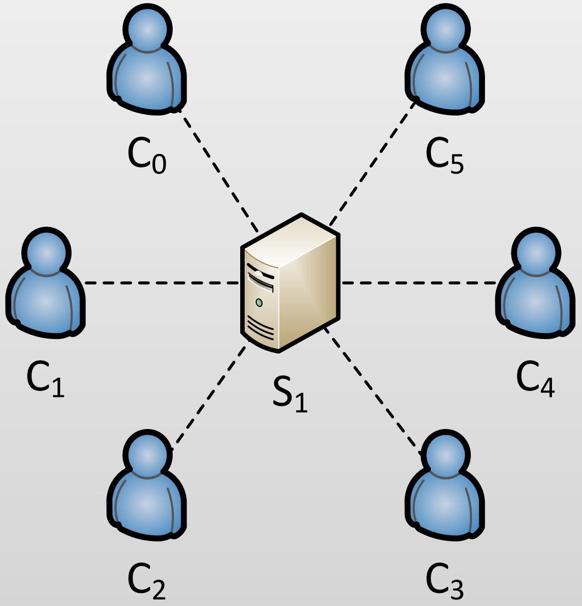
File Sharing Models

- Centralized
  - Client-Server
  - Web-Based
  - File Systems
  - Cloud Computing
  - Streaming
- Decentralized
  - Peer-to-Peer
  - Content Distribution
  - Streaming

Centralized Model

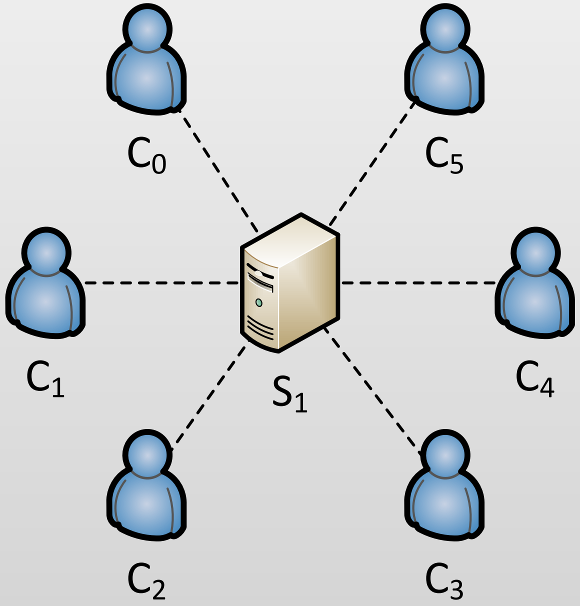
- Client-Server
  - S/FTP
  - Usenet
  - IRC
- Web-Based
  - MediaFire
  - Mega(upload)
  - RapidShare
- File Systems
  - NTFS
  - Samba
  - NFS

- Cloud Computing
  - Microsoft Azure, OneDrive
  - Amazon Web Services
  - Google Drive
  - Dropbox, Box
- Streaming
  - Netflix
  - Amazon Prime
  - HBO Go
  - Revision 3
  - Crackle
  - Hulu (+)
  - Aereo (RIP)



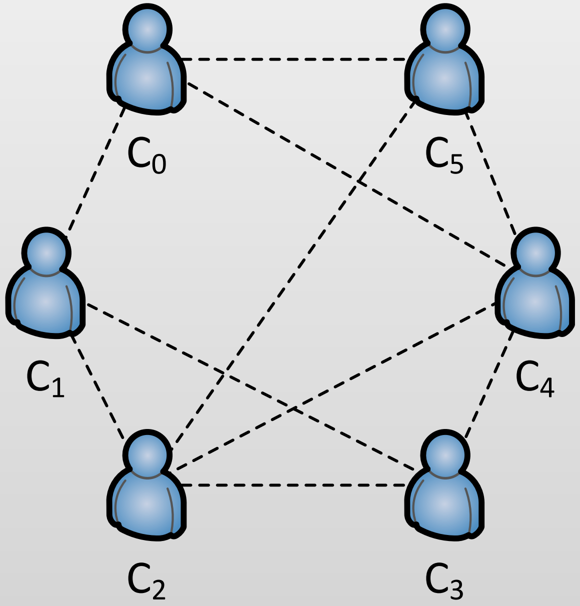
Centralized Model

- Pros
  - Stability
  - Computational capacity
  - Simplified programming model
  - Dedicated hosting benefits
- Cons
  - Proprietary
  - Expensive to configure and run
  - Digital Rights Management (DRM)
  - Identity (IP) and usage transparency
  - Credential-based security
  - Personal liability
  - Auditability



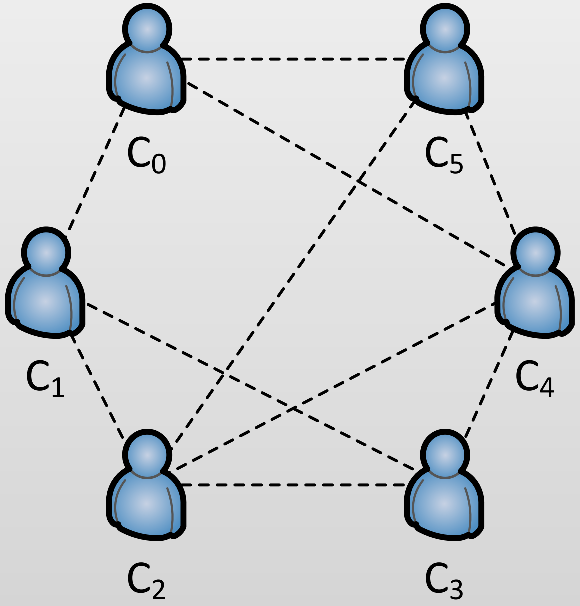
Decentralized Model

- Peer-to-Peer
  - Napster
  - BitTorrent
  - Instant Messenger
  - IRC (DCC)
- Content Distribution
  - Rsync
  - Plex
- Streaming
  - Chromecast
  - DLNA

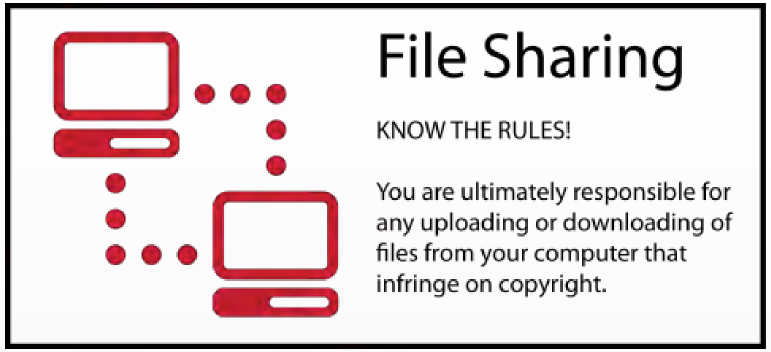


Decentralized Model

- Pros
  - Reliability
  - Fault tolerance
  - Redundancy
  - Scalability
  - Interoperability
  - In perpetuity
- Cons
  - Security
  - Identity (IP) and usage transparency
  - Loss of anonymity
  - Personal liability
  - Auditability



File Sharing Problems



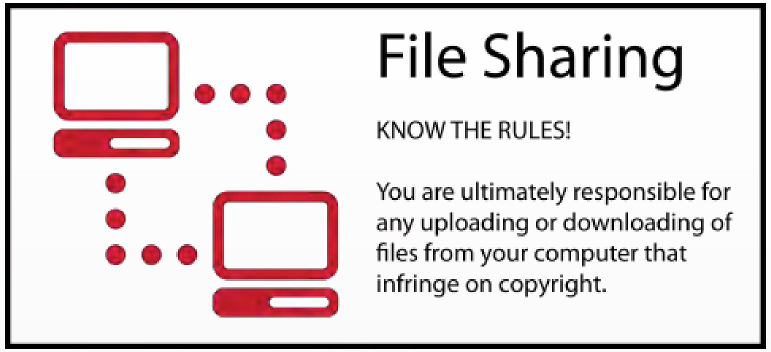
File Sharing

KNOW THE RULES!

You are ultimately responsible for any uploading or downloading of files from your computer that infringe on copyright.

- Insecure
  - Trust a 3rd party source
  - Reveal your identity via P2P
  - Illegal disconnections
- Complacent
  - Forcing us to seek alternate viewing methods
  - File-sharing is a method by which the industry is forced to evolve
  - Adapt or die
- Expensive
  - The Cloud
  - Dropbox, Box
  - HBO Go

File Sharing Problems



File Sharing

KNOW THE RULES!

You are ultimately responsible for any uploading or downloading of files from your computer that infringe on copyright.

- Inflexible
  - I want my files available everywhere at all times
  - I don't want to force-sync content across all devices
  - Not everybody should be forced to seed
  - Acquisition vs. Aggregation
  - What if I'm offline?
- Inconvenient
  - I don’t want to watch ads
  - I want to watch the show that I am paying for
  - Hulu+ should be more like Netflix
  - People will pay for content if it's convenient and reasonably priced
    - Netflix, Amazon Prime, Crackle, Revision 3

A Recipe for Change

From Lemons to Fruity Juice

“I don’t want to live in a world where there’s no privacy, and therefore no room for intellectual exploration and creativity.”
– Edward Snowden

“People who think they know everything really annoy those of us who know we don't.”
– Bjarne Stroustrup

A Tricky Business

- Conflicting Interests
  - Availability, performance, and ease of use
  - Anonymity and security
- Market Evolution
  - Inadequacy breeds innovation
  - Created a niche market for such products
    - VPN’s and proxies
    - Cloud computing
    - Rapidshare, Mega(upload)
    - Dropbox, Box
    - Plex
- The Next Generation
  - Leverage our over-priced ISP connections
  - File sharing can do better

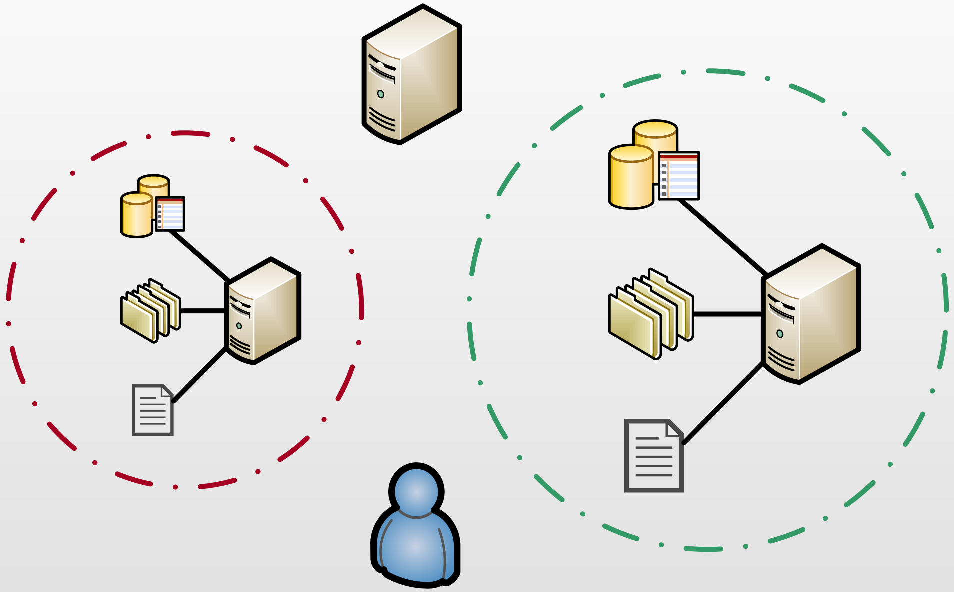
Key Principles of File Sharing

- Authoritative Source
- Stateless Authentication
- Modular Security
- Standard Protocols
- Distributed Endpoints

Authoritative Source

Saving Cyberspace means that we need to reclaim the Authoritative Source

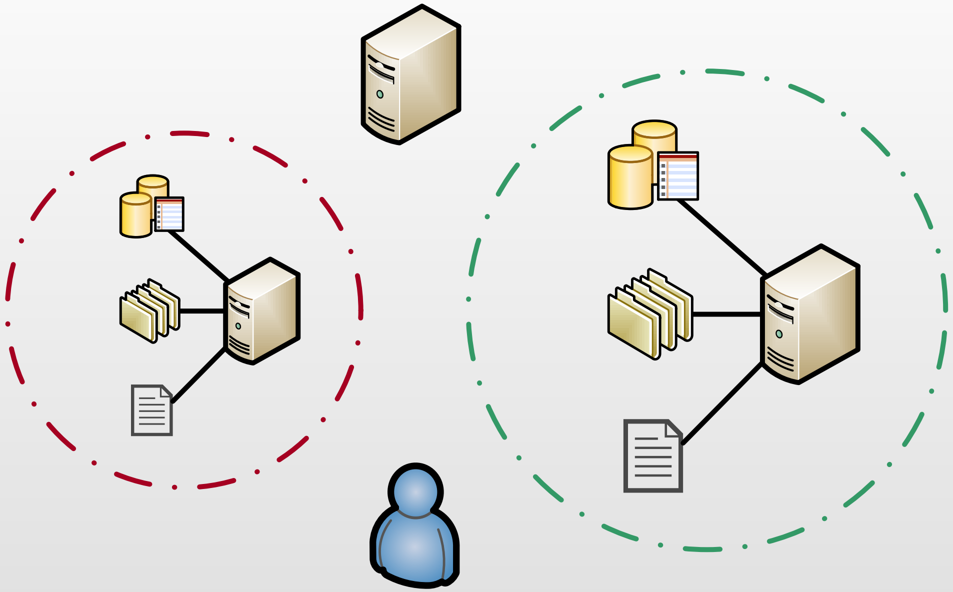
- Overview
  - Primary repository of trusted data
  - Data is the foundation of file sharing
  - First to be secured
  - Last to be compromised
- Too Quick to Trust
  - Models based on trust are flawed
  - Where has trust historically gotten us?
  - Don’t be surprised when trust is betrayed
  - Once it’s gone, it’s gone forever



Authoritative Source

Saving Cyberspace means that we need to reclaim the Authoritative Source

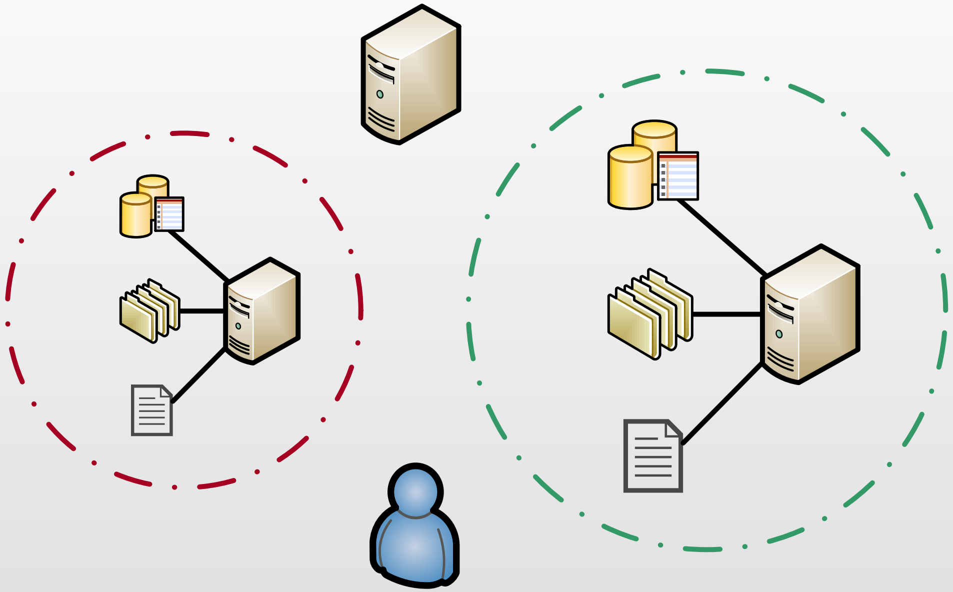
- A Costly Convenience
  - The price of the Modern Internet
  - We've already given away so much
  - Applications fight over control of our data
  - Companies abuse our sensitive data
  - The bottom line seldom favors the customer
- Too Much to Lose
  - The control of our sensitive data
  - The power to protect what's ours
  - The certainty that our data is protected
  - The choice to respond to attacks
  - The ability to remain anonymous



Authoritative Source

Saving Cyberspace means that we need to reclaim the Authoritative Source

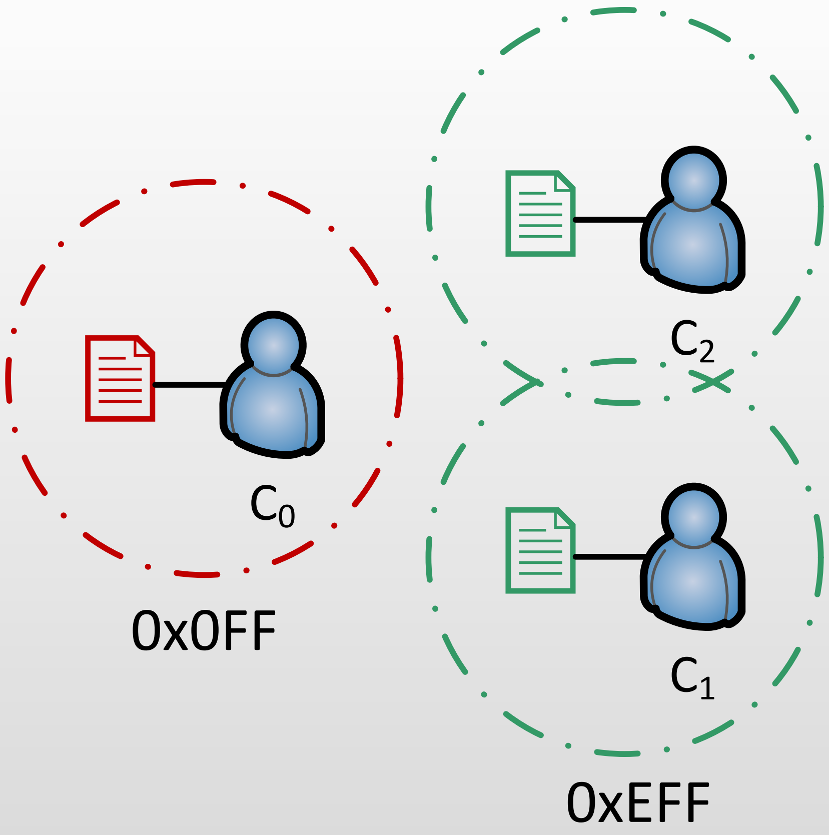
- The Solution
  - Take responsibility
  - Reclaim the Authoritative Source
  - Do what companies continue to fail at
  - Anonymize our file sharing habits
  - Secure our data



Stateless Authentication

Saving Cyberspace means that we will need to redefine authentication

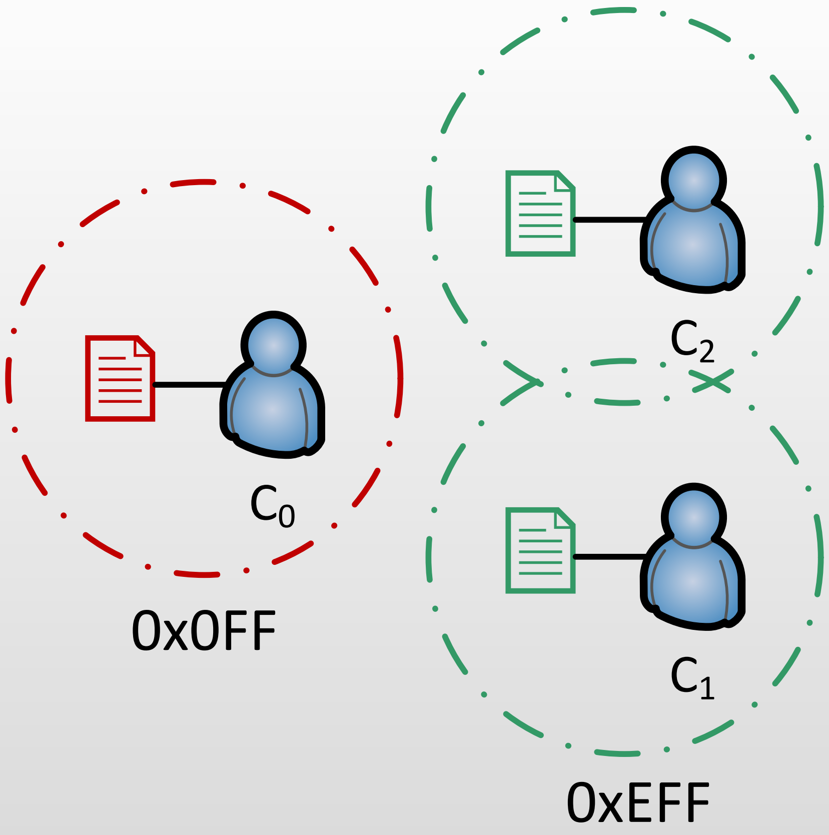
- Overview
  - Form of shared secret authentication
  - Leverages shared assets or other known data
  - Shared secret is obvious to a very specific group
  - Dynamic encryption algorithms
- State-Based Applications
  - What does it mean to authenticate?
  - Inadequate file sharing security models
  - Credentials are antiquated and unnecessary
  - Certificates rely on trusted 3rd parties
  - No registration process or data storage
  - Security only needs to be secure enough



Stateless Authentication

Saving Cyberspace means that we will need to redefine authentication

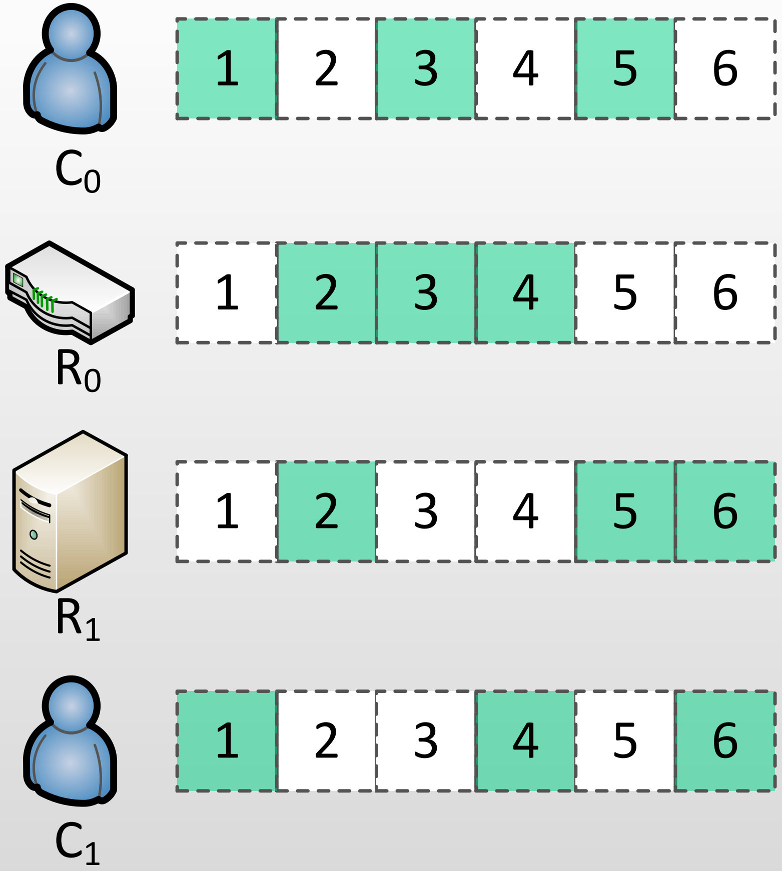
- Data Oversight
  - Who's storing our information?
  - How is our data being used?
  - Who's selling us out to the government?
  - Companies are incapable of protecting our data
- The Solution
  - Shared authentication creates temporary trust
  - Breaches don't reveal any personal information
  - Don't have to worry about identity leakage
  - If you want it done right, do it yourself
  - "Doveryai, no proveryai"



Modular Security

Saving Cyberspace means that we will need to implement a modular approach to security

- Overview
  - Based on Layered Security
  - Division of authority and separation of duties
  - Total is greater than the sum of the parts
  - Inability to store complete secrets
  - Double-blind
- Plausible Deniability
  - Always assume somebody is listening
  - Multiple modules of defense resist penetration
  - What they don’t know won’t hurt you
  - They can’t audit what you don’t have
  - Entire system must be compromised

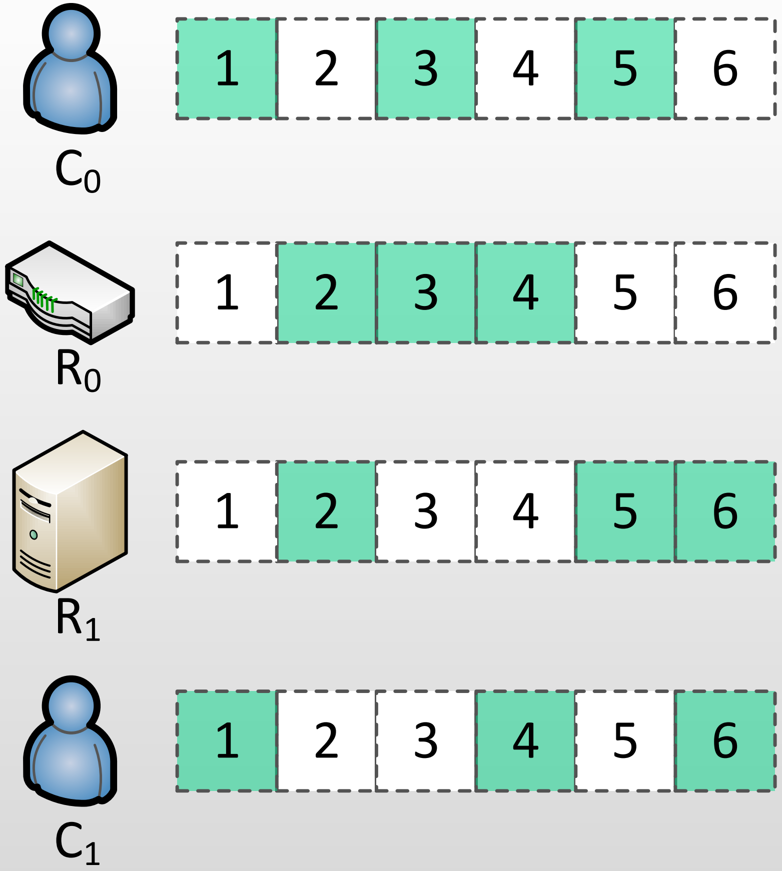


C_0	🟩 1	2	🟩 3	4	🟩 5	6
R_0	1	🟩 2	🟩 3	🟩 4	5	6
R_1	1	🟩 2	3	4	🟩 5	🟩 6
C_1	🟩 1	2	3	🟩 4	5	🟩 6

Modular Security

Saving Cyberspace means that we will need to implement a modular approach to security

- Applications
  - Poor choices in software architecture/design
  - Too many single points of failure
  - Reveal too much information
- The Solution
  - Messages increase strength as they propagate
  - Each module is…
    - Isolated
    - Autonomous
    - Self-sufficient
    - Resistant to attacks

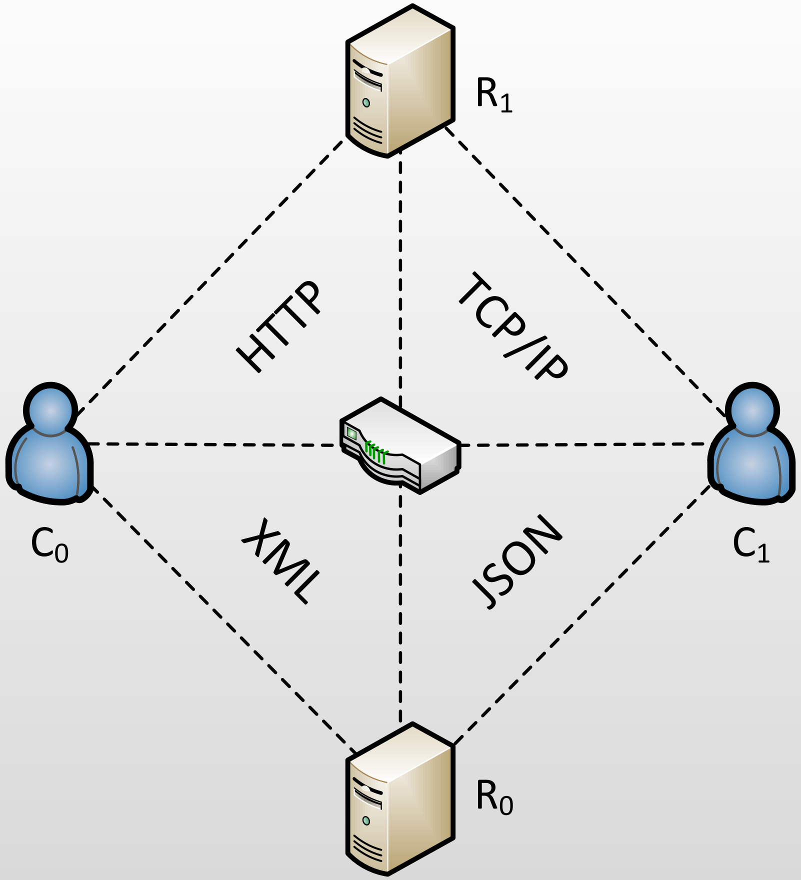


C_0	🟩 1	2	🟩 3	4	🟩 5	6
R_0	1	🟩 2	🟩 3	🟩 4	5	6
R_1	1	🟩 2	3	4	🟩 5	🟩 6
C_1	🟩 1	2	3	🟩 4	5	🟩 6

Standard Protocols

Saving Cyberspace means that we need to adhere to a standard set of pre-existing transfer protocols

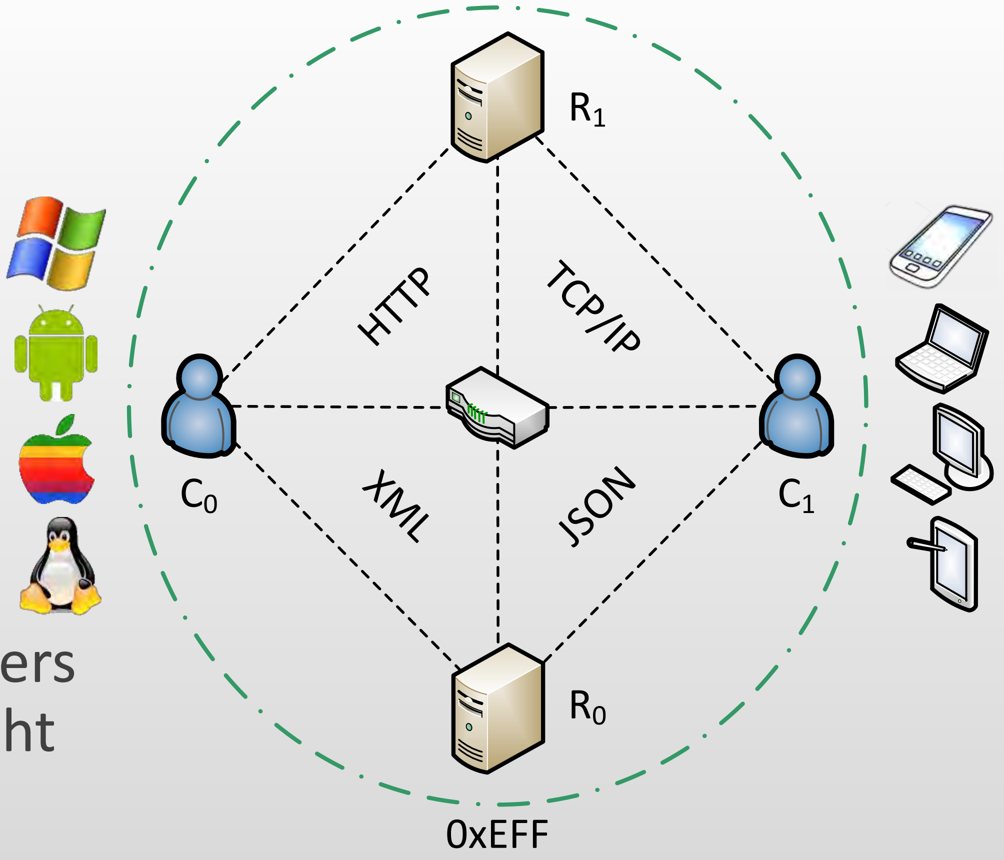
- Overview
  - Creating a file sharing application is science
  - Creating a message protocol is art and wizardry
- Benefits
  - Interoperability
  - Undetectable means we’re essentially invisible
  - Designing a good protocol is hard work
  - A transport protocol is just a means to an end
  - More concerned with the exchange of data
- The Solution
  - Use pre-existing protocols and standards
  - HTTP, XML, JSON, etc.



Distributed Endpoints

Saving Cyberspace means that we will need to support a more flexible and distributed model for file sharing

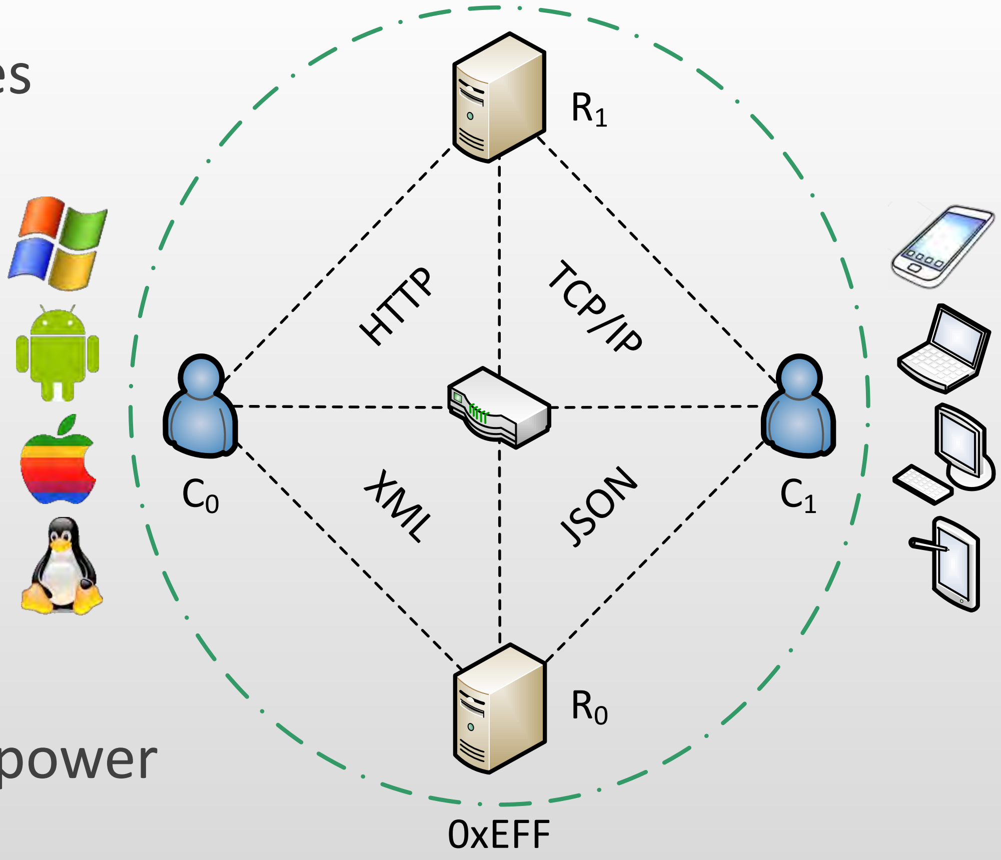
- Overview
  - Hybrid model
  - Transformational network
- Centralized Model is Evil
  - Activities monitored or logged?
  - What happens if the server goes down?
  - Ability to share files shouldn’t depend on others
  - Never trust 3rd parties, corporations, or others that comply with data retention and copyright laws



Distributed Endpoints

Saving Cyberspace means that we will need to support a more flexible and distributed model for file sharing

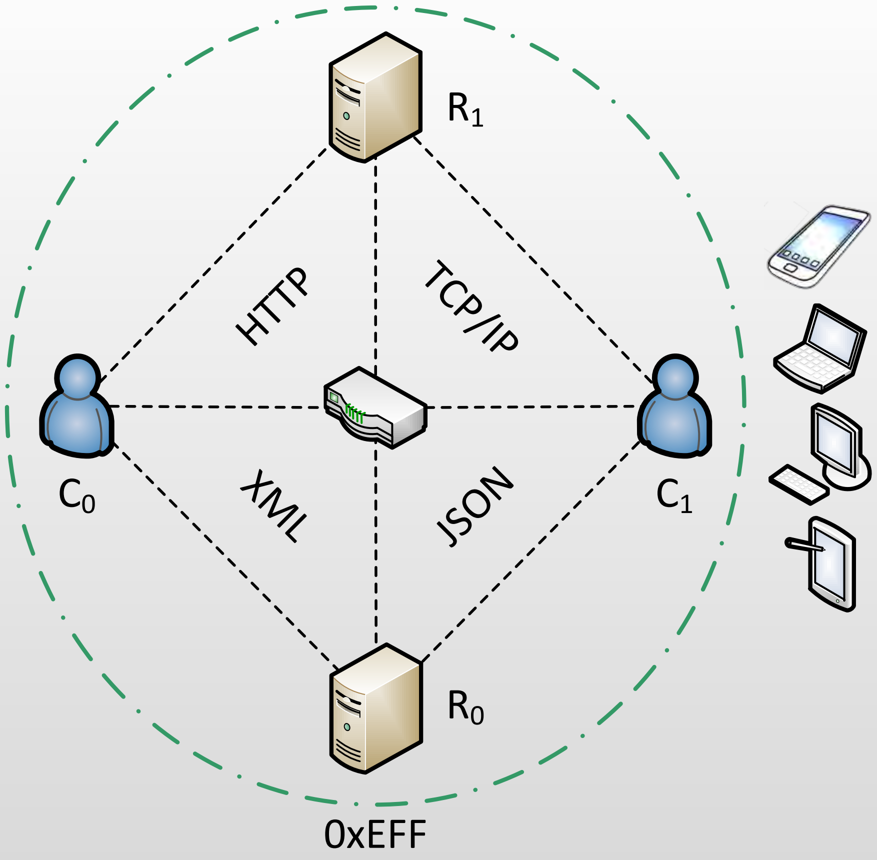
- Decentralized Model is Evil
  - Created a market for IP concealment services
  - Danger of incoming connections
  - IP address as a personal identifier
  - Not suitable for low-power devices
  - Inequality for all
- Device Agnostic
  - Workstations, Servers, and Laptops
  - Windows, Linux, Mac, Android, and iOS.
  - Tablets, Phones, embedded, and other low-power consumption devices



Distributed Endpoints

Saving Cyberspace means that we will need to support a more flexible and distributed model for file sharing

- Personal Network
  - Pervasive and ubiquitous
  - Can be used by individuals, families, or millions
  - The world in the palm of your hand
- The Solution
  - Best of both worlds, worst of neither
  - No direct communication, no fixed servers
  - Based on network routing technologies
  - Autonomy and segregation of duties
  - Division of authority



demonsaw

Believe in the Right to Share

“If you want to achieve something, you build the basis for it.”
– *Noam Chomsky*

“The only way to keep a secret is to never have one.”
– *Julian Assange*

The Missing Link

- Dilemma
  - Do we really need another file-sharing app?
  - Casual Dropbox user with an addiction to torrents
  - Not happy with the current state of file sharing apps
    - Share with friends, family, and/or strangers
    - Access to all my content from anywhere in the world
    - Fine-grained control

- Current Offerings
  - Why doesn't a solution for me not already exist?
  - It might, depending on your specific needs
  - If not, what is your willingness to compromise and/or assume risk?
  - With the right minds, this should be an easy problem to solve

Demonsaw

- Free
  - No ads
- Anonymous
  - No logging
  - No registration
  - No data retention
  - No loss of control
- Secure
  - No P2P
  - No centralized servers
  - Everything is encrypted
  - Undetectable by companies, governments, and 3rd parties

Demonsaw

- Simple
  - Share, Search, Browse, Transfer
  - Use at home, work, or while traveling
- Scalable
  - Share files with yourself
  - Share files with family and friends
  - Share files with hundreds of your closest friends
- Multi-Platform/Device
  - Windows, Linux, Mac
  - Android, iOS
  - Web
- Demo

Architecture

- Overview
  - A file sharing system should be flexible
  - There is no such thing as fair
  - Cater to individual needs
- Design
  - Entity Component System (ECS)
  - Faster, more flexible, and easier to extend
- Content
  - Separate messages and data
  - Unable to deduce what type of content exchange is occurring
  - Need-to-know basis

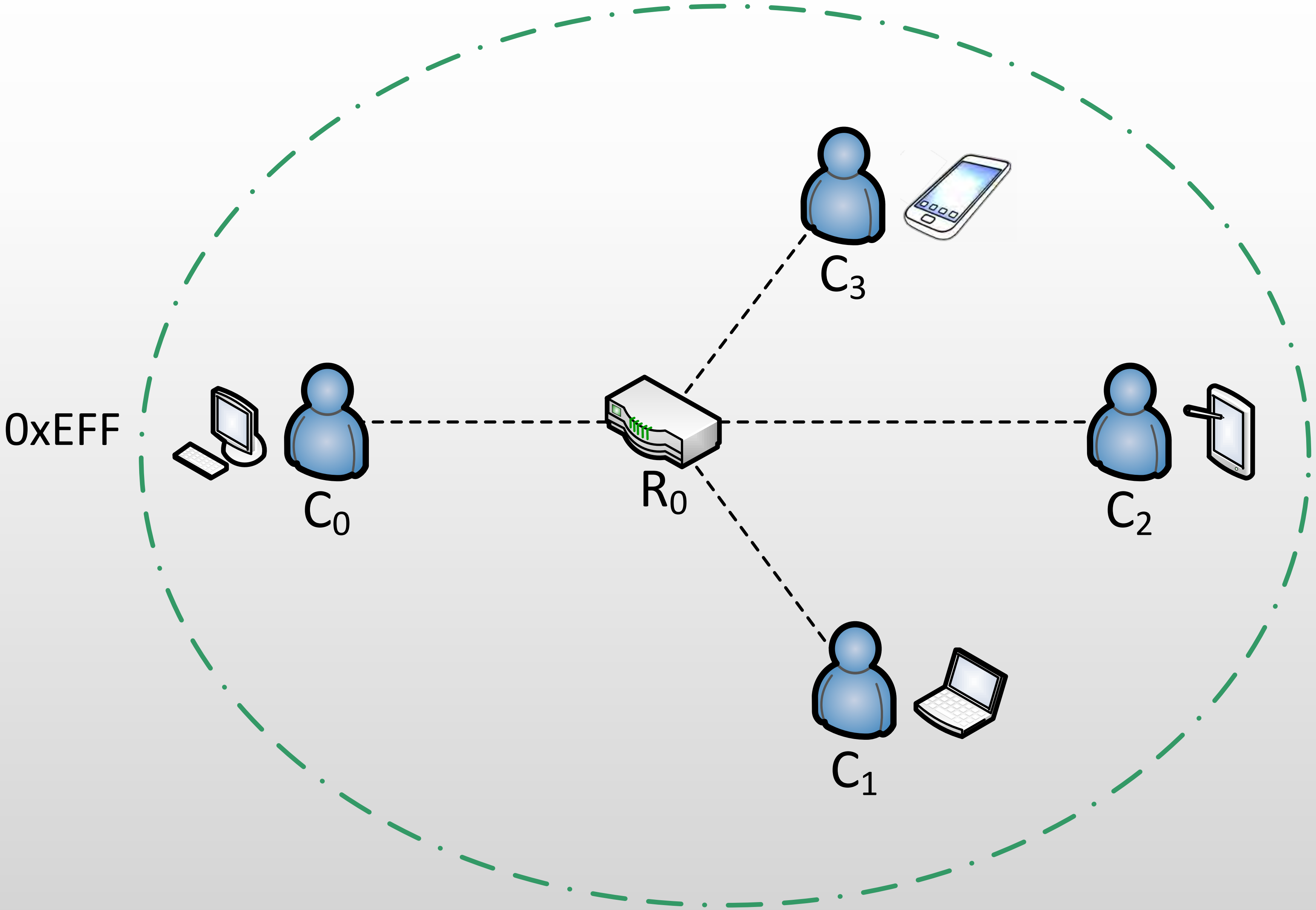
Architecture

- Encryption
  - Messages and data are always encrypted
  - Leverage work on encryption standards and secure message exchange
  - Mutating, Automatic, Isolated, Data-Driven, and Stateless
  - Authentication, authorization
  - Diffie Hellman, AES, etc.
- Client
  - Share files
  - Transfer files

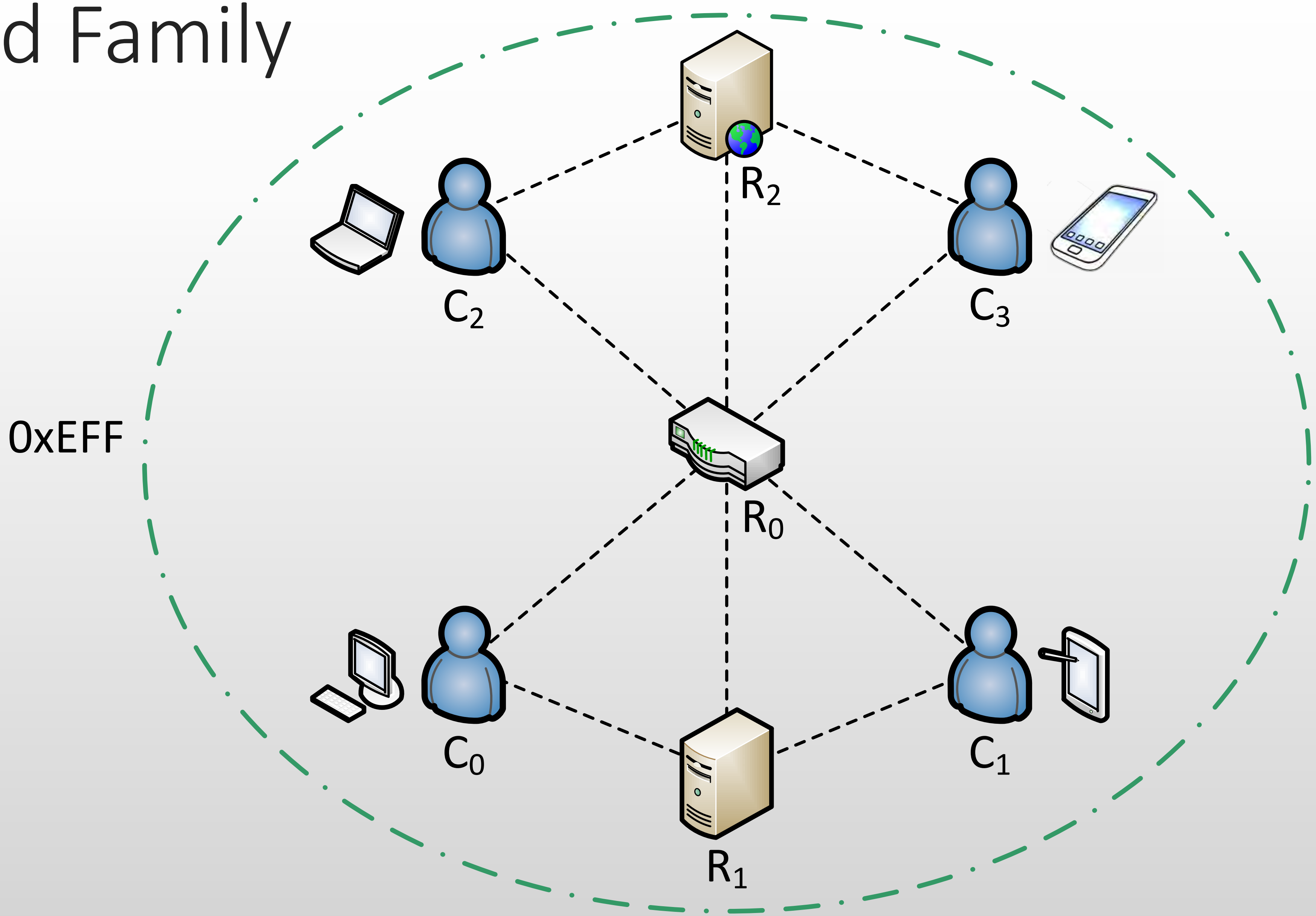
Architecture

- Router
  - Group clients
  - Control program flow
  - Relay messages and/or data chunks
- Proxy
  - Interface with external content sources
  - Acquisition vs. aggregation

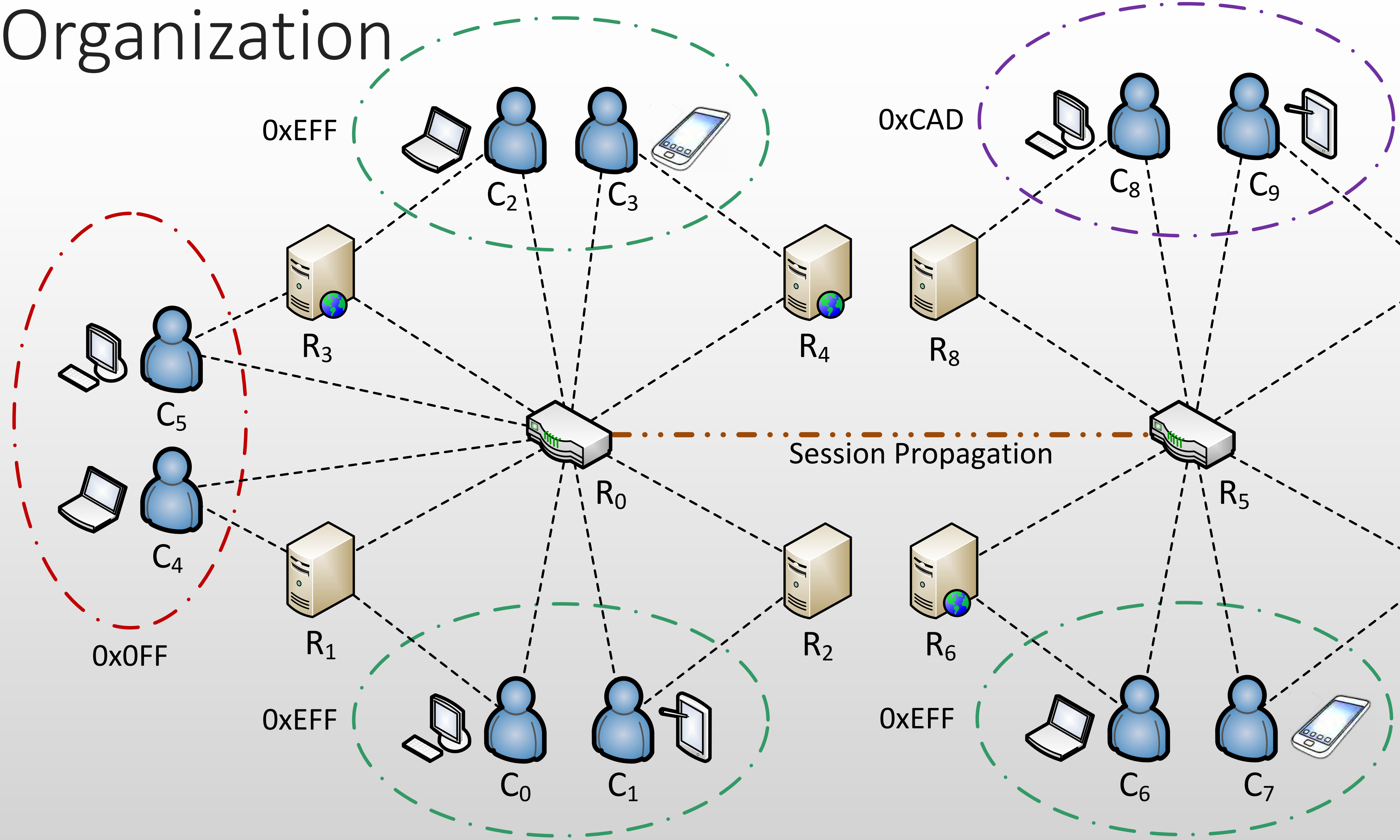
Individual



Friends and Family



Organization



Summary

The Path Forward

“Only a life lived for others is a life worthwhile.”
– *Albert Einstein*

“And one more thing.”
– *Steve Jobs*

Changing the World

- Self-Empowerment
  - We possess a tremendous amount of talent
  - We're good at what we do and we enjoy what we're good at
  - Our skills are used to find vulnerabilities and exposing weaknesses
  - Create something new and beautiful that has the power to change the world
- Enacting Change
  - Demonsaw is a tool
  - Allows us to deviate from the antiquated and insecure model of file-sharing
  - It gives us a new way to share our content without fear of retribution
  - It is my hope that Demonsaw will enact change in content distribution
  - Go forth and share…

Thank you

[Web]

[Email]

[Twitter]

[Facebook]

Eijah

demonsaw

Appendix

Standing on the Shoulders of Giants

“Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same.”
– Ronald Reagan

“Then Jesus asked him, What is your name? My name is Legion, he replied, for we are many.”
– Mark 5:9

References

- Wikipedia
  - http://en.wikipedia.org/wiki/File_sharing
  - http://en.wikipedia.org/wiki/Client_server
  - http://en.wikipedia.org/wiki/Peer_to_peer
- Images
  - http://studentaffairs.duke.edu/sites/default/files/u7/dos_RIAA.png
  - https://www.flickr.com/photos/hughelectronic/sets/72157603862426534
  - http://www.timeshighereducation.co.uk/news/academy-and-business-aim-to-reforge-language-supply-chain/2007785.article
- Network Models
  - http://www.ianswer4u.com/2011/05/client-server-network-advantages-and.html#axzz3681DuDJP
  - http://www.ianswer4u.com/2011/05/peer-to-peer-network-p2p-advantages-and.html#axzz3681DuDJP
  - http://www.cmswire.com/cms/document-management/the-business-benefits-of-hybrid-online-file-sharing-024182.php
  - http://www.workshare.com/workshare/esg-report-the-demand-for-hybrid-online-file-sharing-solutions

Quotes

“When I am afraid, I put my trust in you.”
– Psalm 56:3

“If you want to achieve something, you build the basis for it.”
– Noam Chomsky

“Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same.”
– Ronald Reagan

“The increase of disorder or entropy is what distinguishes the past from the future, giving a direction to time.”
– Stephen Hawking, A Brief History of Time

“Information is power. But like all power, there are those who want to keep it for themselves.”
– Aaron Swartz

“I don’t want to live in a world where there’s no privacy, and therefore no room for intellectual exploration and creativity.”
– Edward Snowden

“People who think they know everything really annoy those of us who know we don't.”
– Bjarne Stroustrup

“If life gives you lemons, make some kind of fruity juice.”
– Conan O’Brien

Quotes

"The only way to keep a secret is to never have one."
 – Julian Assange

"You can now be a master of your own destiny."
 – Sean Parker

"Only a life lived for others is a life worthwhile."
 – Albert Einstein

"And one more thing."
 – Steve Jobs

"Non-conformity is the only real passion worth being ruled by."
 – Julian Assange

"…One can easily remain free of even the most intense political oppression simply by placing one's faith and trust in institutions of authority."
 – Glenn Greenwald

"When the man with the *demon saw* Jesus a long way off, he ran and worshiped Him."
 – Mark 5:6

"Then Jesus asked him, What is your name? My name is Legion, he replied, for we are many."
 – Mark 5:9

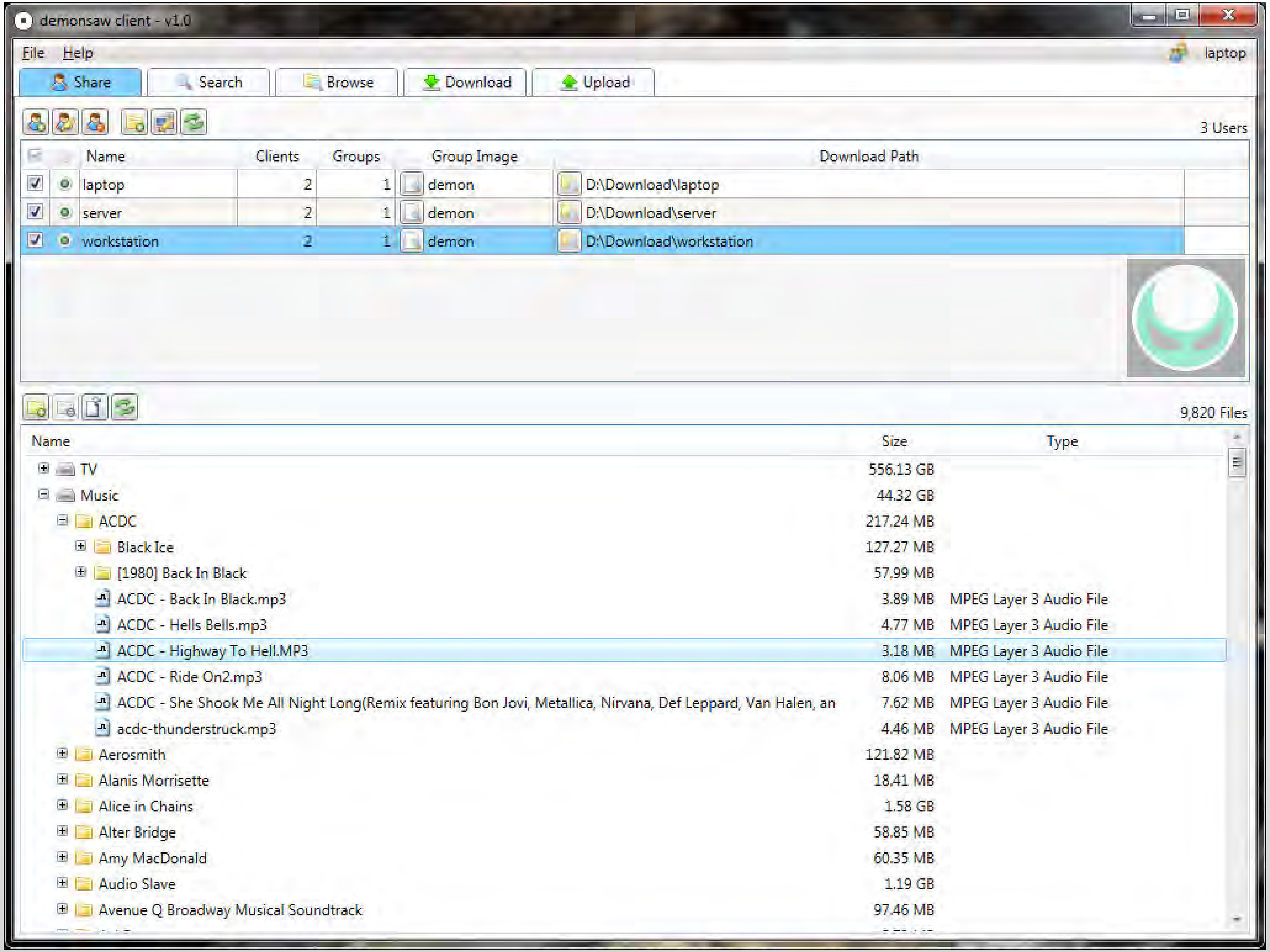
Demo

Demonsaw 1.0 (alpha)

“Non-conformity is the only real passion worth being ruled by.”
– *Julian Assange*

“You can now be a master of your own destiny.”
– *Sean Parker*

Share



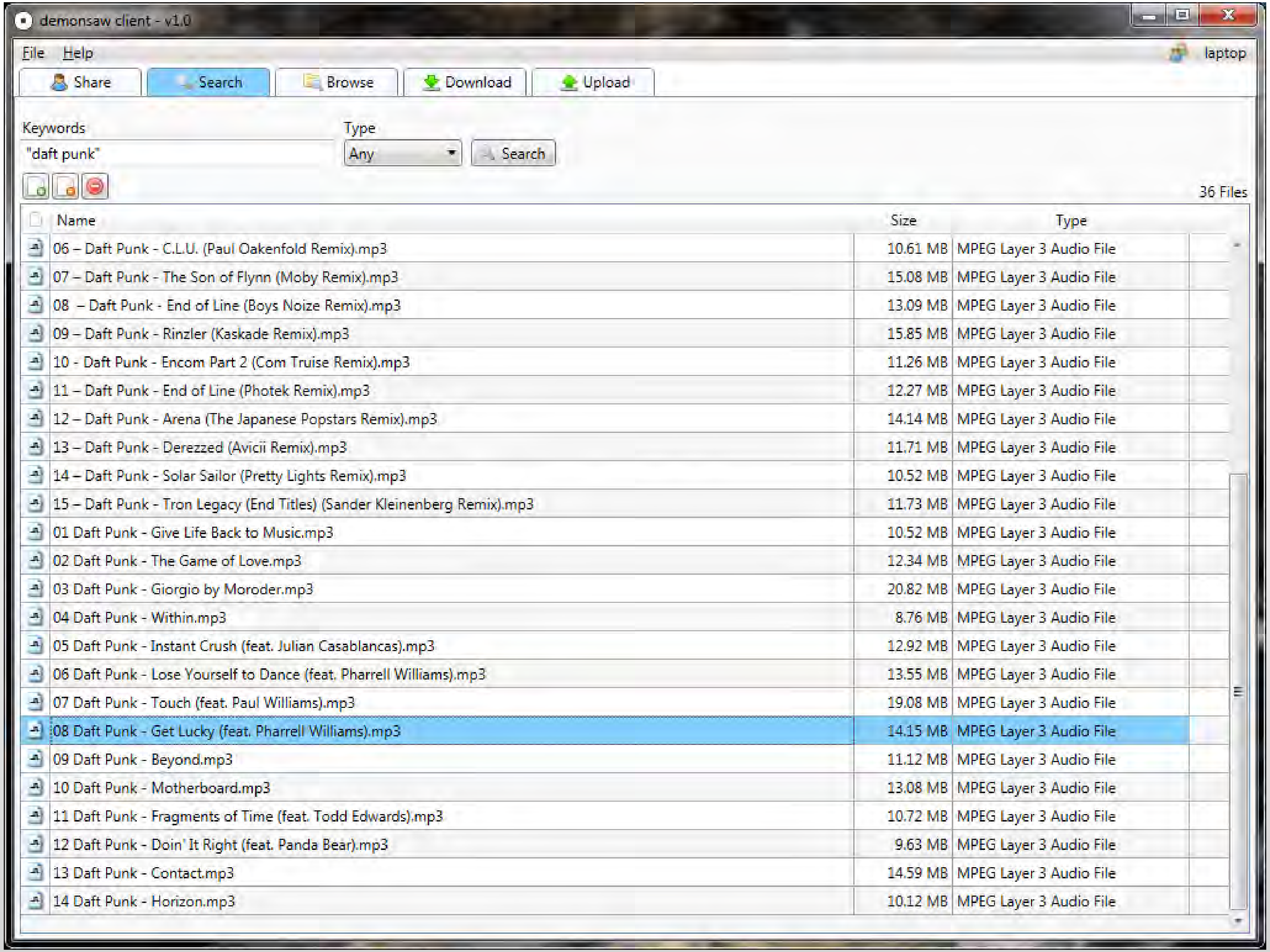
3 Users

☐		Name	Clients	Groups	Group Image	Download Path
☑	●	laptop	2	1	demon	D:\Download\laptop
☑	●	server	2	1	demon	D:\Download\server
☑	●	workstation	2	1	demon	D:\Download\workstation

9,820 Files

Name	Size	Type
⊞ TV	556.13 GB	
⊟ Music	44.32 GB	
⊟ ACDC	217.24 MB	
⊞ Black Ice	127.27 MB	
⊞ [1980] Back In Black	57.99 MB	
ACDC - Back In Black.mp3	3.89 MB	MPEG Layer 3 Audio File
ACDC - Hells Bells.mp3	4.77 MB	MPEG Layer 3 Audio File
ACDC - Highway To Hell.MP3	3.18 MB	MPEG Layer 3 Audio File
ACDC - Ride On2.mp3	8.06 MB	MPEG Layer 3 Audio File
ACDC - She Shook Me All Night Long(Remix featuring Bon Jovi, Metallica, Nirvana, Def Leppard, Van Halen, an	7.62 MB	MPEG Layer 3 Audio File
acdc-thunderstruck.mp3	4.46 MB	MPEG Layer 3 Audio File
⊞ Aerosmith	121.82 MB	
⊞ Alanis Morrisette	18.41 MB	
⊞ Alice in Chains	1.58 GB	
⊞ Alter Bridge	58.85 MB	
⊞ Amy MacDonald	60.35 MB	
⊞ Audio Slave	1.19 GB	
⊞ Avenue Q Broadway Musical Soundtrack	97.46 MB	

Search



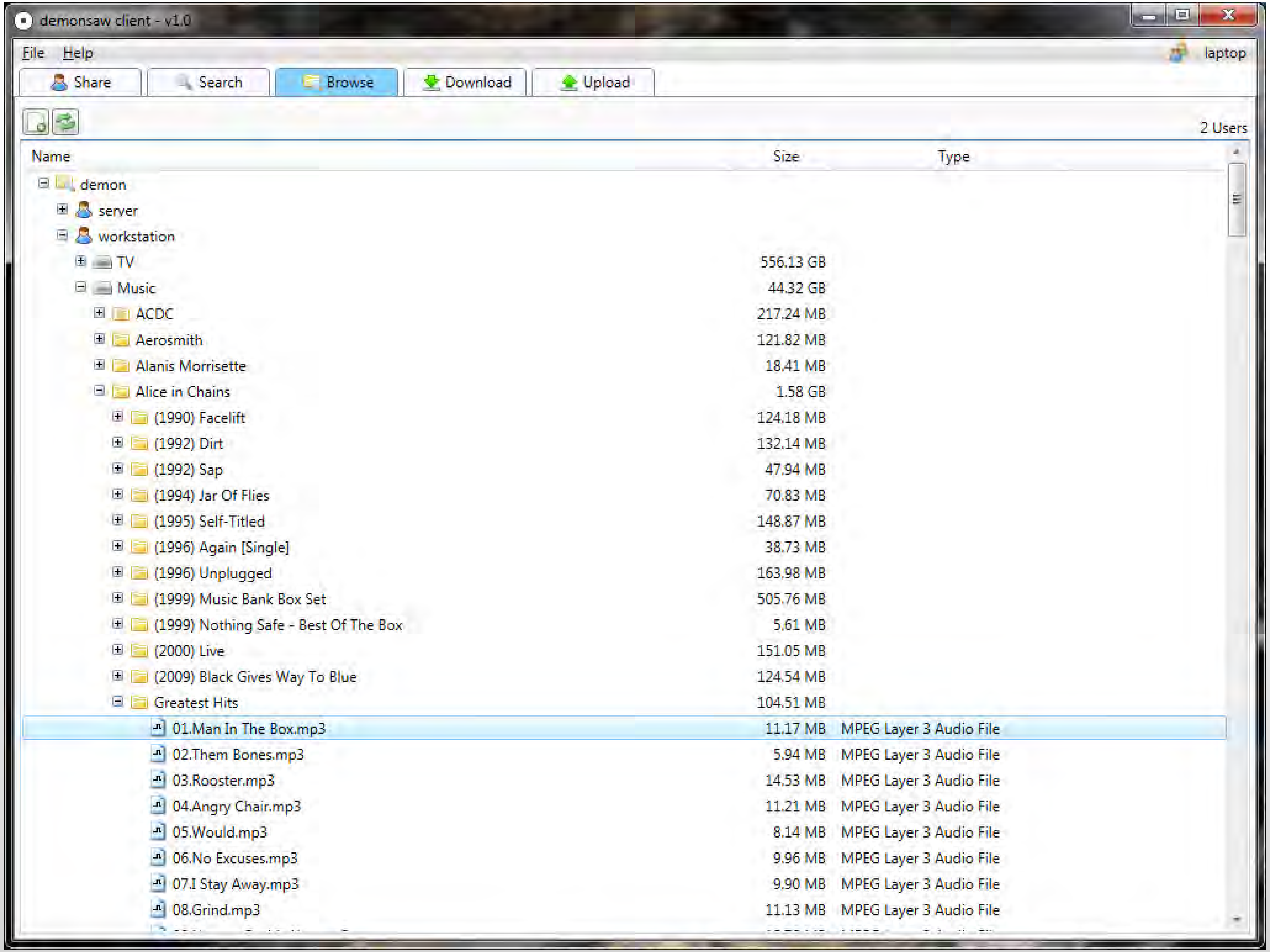
Keywords: "daft punk"

Type: Any

36 Files

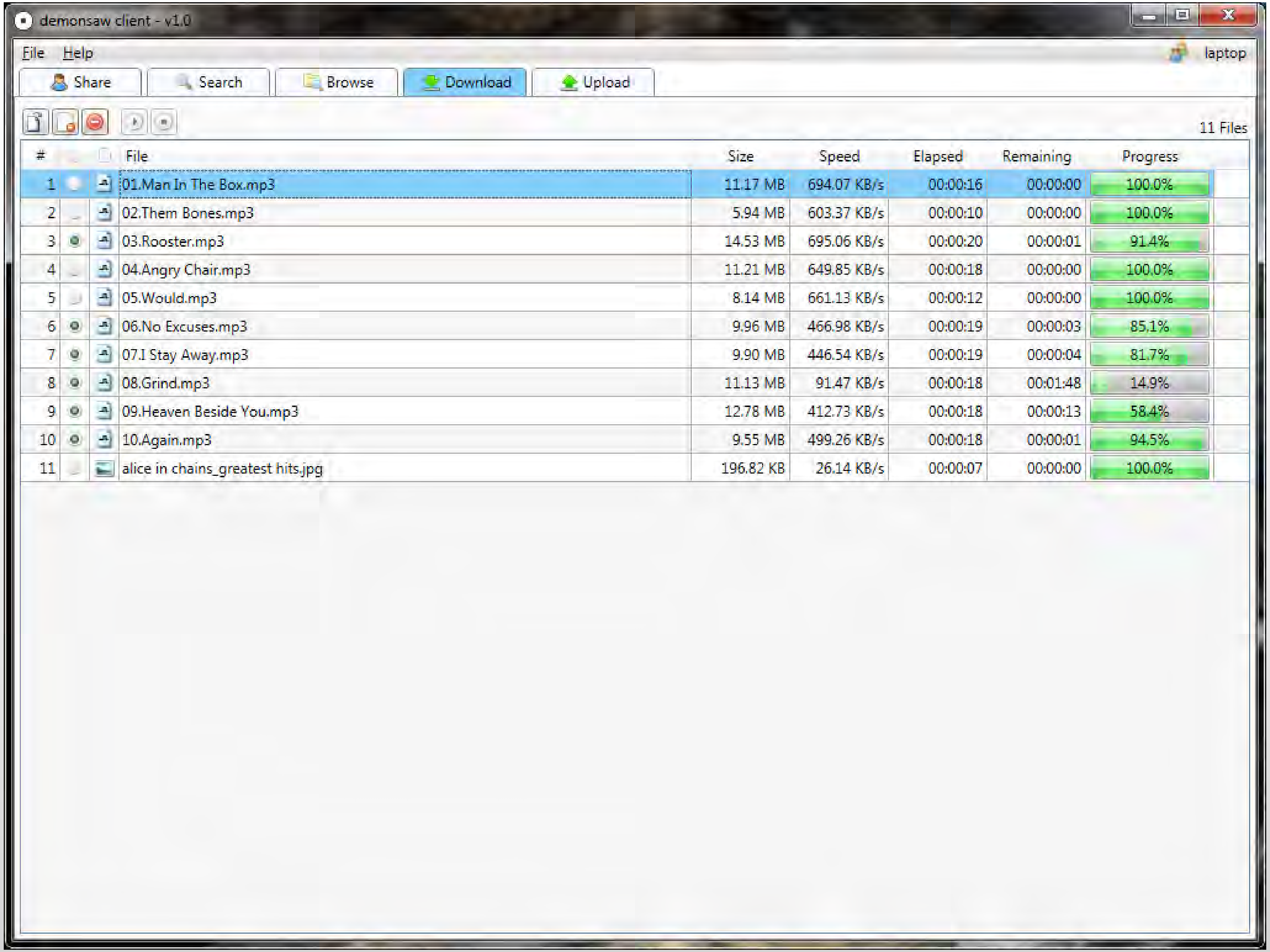
Name	Size	Type
06 – Daft Punk - C.L.U. (Paul Oakenfold Remix).mp3	10.61 MB	MPEG Layer 3 Audio File
07 – Daft Punk - The Son of Flynn (Moby Remix).mp3	15.08 MB	MPEG Layer 3 Audio File
08 – Daft Punk - End of Line (Boys Noize Remix).mp3	13.09 MB	MPEG Layer 3 Audio File
09 – Daft Punk - Rinzler (Kaskade Remix).mp3	15.85 MB	MPEG Layer 3 Audio File
10 - Daft Punk - Encom Part 2 (Com Truise Remix).mp3	11.26 MB	MPEG Layer 3 Audio File
11 – Daft Punk - End of Line (Photek Remix).mp3	12.27 MB	MPEG Layer 3 Audio File
12 – Daft Punk - Arena (The Japanese Popstars Remix).mp3	14.14 MB	MPEG Layer 3 Audio File
13 – Daft Punk - Derezzed (Avicii Remix).mp3	11.71 MB	MPEG Layer 3 Audio File
14 – Daft Punk - Solar Sailor (Pretty Lights Remix).mp3	10.52 MB	MPEG Layer 3 Audio File
15 – Daft Punk - Tron Legacy (End Titles) (Sander Kleinenberg Remix).mp3	11.73 MB	MPEG Layer 3 Audio File
01 Daft Punk - Give Life Back to Music.mp3	10.52 MB	MPEG Layer 3 Audio File
02 Daft Punk - The Game of Love.mp3	12.34 MB	MPEG Layer 3 Audio File
03 Daft Punk - Giorgio by Moroder.mp3	20.82 MB	MPEG Layer 3 Audio File
04 Daft Punk - Within.mp3	8.76 MB	MPEG Layer 3 Audio File
05 Daft Punk - Instant Crush (feat. Julian Casablancas).mp3	12.92 MB	MPEG Layer 3 Audio File
06 Daft Punk - Lose Yourself to Dance (feat. Pharrell Williams).mp3	13.55 MB	MPEG Layer 3 Audio File
07 Daft Punk - Touch (feat. Paul Williams).mp3	19.08 MB	MPEG Layer 3 Audio File
08 Daft Punk - Get Lucky (feat. Pharrell Williams).mp3	14.15 MB	MPEG Layer 3 Audio File
09 Daft Punk - Beyond.mp3	11.12 MB	MPEG Layer 3 Audio File
10 Daft Punk - Motherboard.mp3	13.08 MB	MPEG Layer 3 Audio File
11 Daft Punk - Fragments of Time (feat. Todd Edwards).mp3	10.72 MB	MPEG Layer 3 Audio File
12 Daft Punk - Doin' It Right (feat. Panda Bear).mp3	9.63 MB	MPEG Layer 3 Audio File
13 Daft Punk - Contact.mp3	14.59 MB	MPEG Layer 3 Audio File
14 Daft Punk - Horizon.mp3	10.12 MB	MPEG Layer 3 Audio File

Browse



Name	Size	Type
demon		
server		
workstation		
TV	556.13 GB	
Music	44.32 GB	
ACDC	217.24 MB	
Aerosmith	121.82 MB	
Alanis Morrisette	18.41 MB	
Alice in Chains	1.58 GB	
(1990) Facelift	124.18 MB	
(1992) Dirt	132.14 MB	
(1992) Sap	47.94 MB	
(1994) Jar Of Flies	70.83 MB	
(1995) Self-Titled	148.87 MB	
(1996) Again [Single]	38.73 MB	
(1996) Unplugged	163.98 MB	
(1999) Music Bank Box Set	505.76 MB	
(1999) Nothing Safe - Best Of The Box	5.61 MB	
(2000) Live	151.05 MB	
(2009) Black Gives Way To Blue	124.54 MB	
Greatest Hits	104.51 MB	
01.Man In The Box.mp3	11.17 MB	MPEG Layer 3 Audio File
02.Them Bones.mp3	5.94 MB	MPEG Layer 3 Audio File
03.Rooster.mp3	14.53 MB	MPEG Layer 3 Audio File
04.Angry Chair.mp3	11.21 MB	MPEG Layer 3 Audio File
05.Would.mp3	8.14 MB	MPEG Layer 3 Audio File
06.No Excuses.mp3	9.96 MB	MPEG Layer 3 Audio File
07.I Stay Away.mp3	9.90 MB	MPEG Layer 3 Audio File
08.Grind.mp3	11.13 MB	MPEG Layer 3 Audio File

Transfer



#			File	Size	Speed	Elapsed	Remaining	Progress
1			01.Man In The Box.mp3	11.17 MB	694.07 KB/s	00:00:16	00:00:00	100.0%
2			02.Them Bones.mp3	5.94 MB	603.37 KB/s	00:00:10	00:00:00	100.0%
3	●		03.Rooster.mp3	14.53 MB	695.06 KB/s	00:00:20	00:00:01	91.4%
4			04.Angry Chair.mp3	11.21 MB	649.85 KB/s	00:00:18	00:00:00	100.0%
5			05.Would.mp3	8.14 MB	661.13 KB/s	00:00:12	00:00:00	100.0%
6	●		06.No Excuses.mp3	9.96 MB	466.98 KB/s	00:00:19	00:00:03	85.1%
7	●		07.I Stay Away.mp3	9.90 MB	446.54 KB/s	00:00:19	00:00:04	81.7%
8	●		08.Grind.mp3	11.13 MB	91.47 KB/s	00:00:18	00:01:48	14.9%
9	●		09.Heaven Beside You.mp3	12.78 MB	412.73 KB/s	00:00:18	00:00:13	58.4%
10	●		10.Again.mp3	9.55 MB	499.26 KB/s	00:00:18	00:00:01	94.5%
11			alice in chains_greatest hits.jpg	196.82 KB	26.14 KB/s	00:00:07	00:00:00	100.0%