

The Unsearchables

Finding Things That Google Doesn't

Me

- Technical Trainer
- TomNomNom online
- I do a bit of bug bounty
- I love a bit of recon
- I've been burnt out
 - Take care of yourselves!



What To Look For

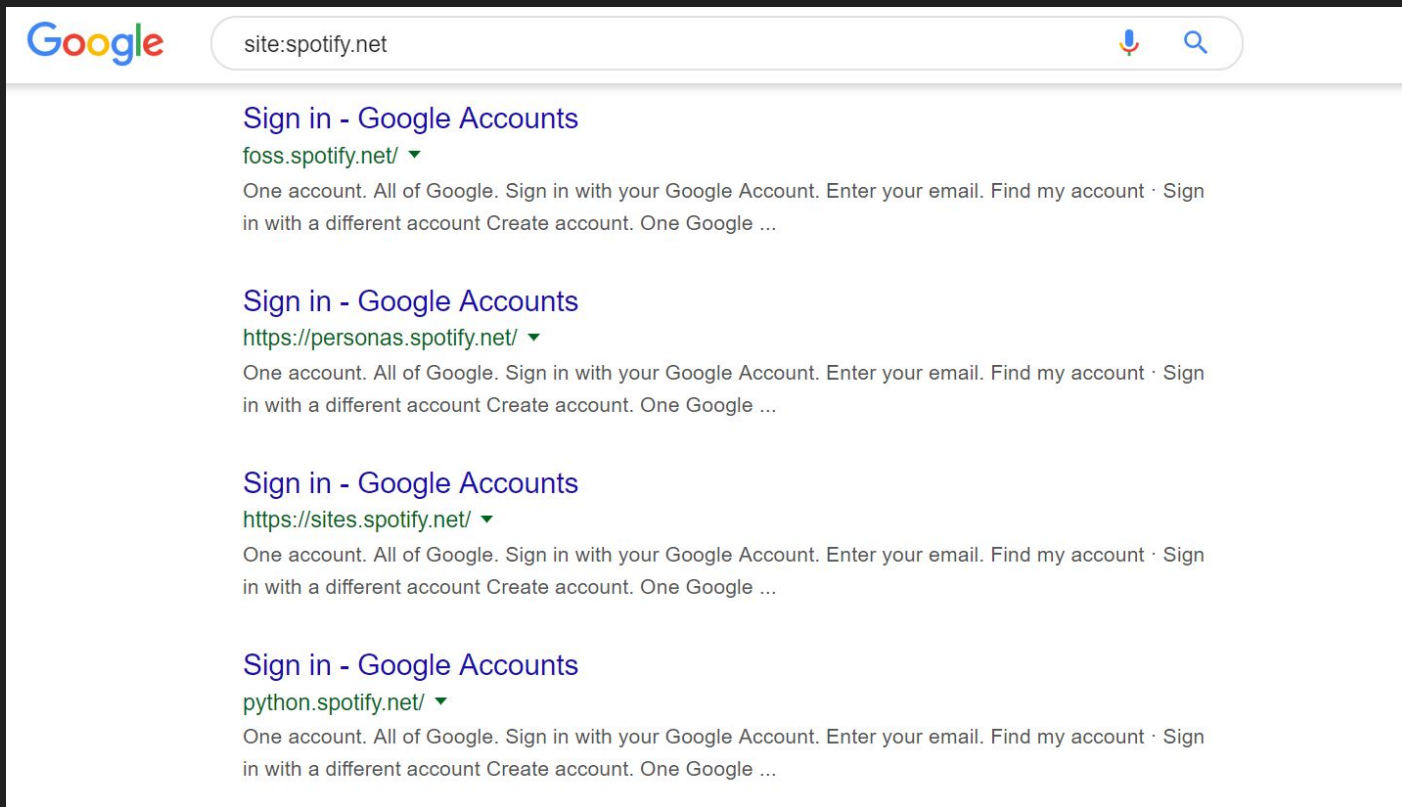
- Credentials
- Internal URLs
- Unknown paths
- Internal documentation
- “Internal Indicators”
- ...anything you probably shouldn't know

Nearly Anything Can Be Useful

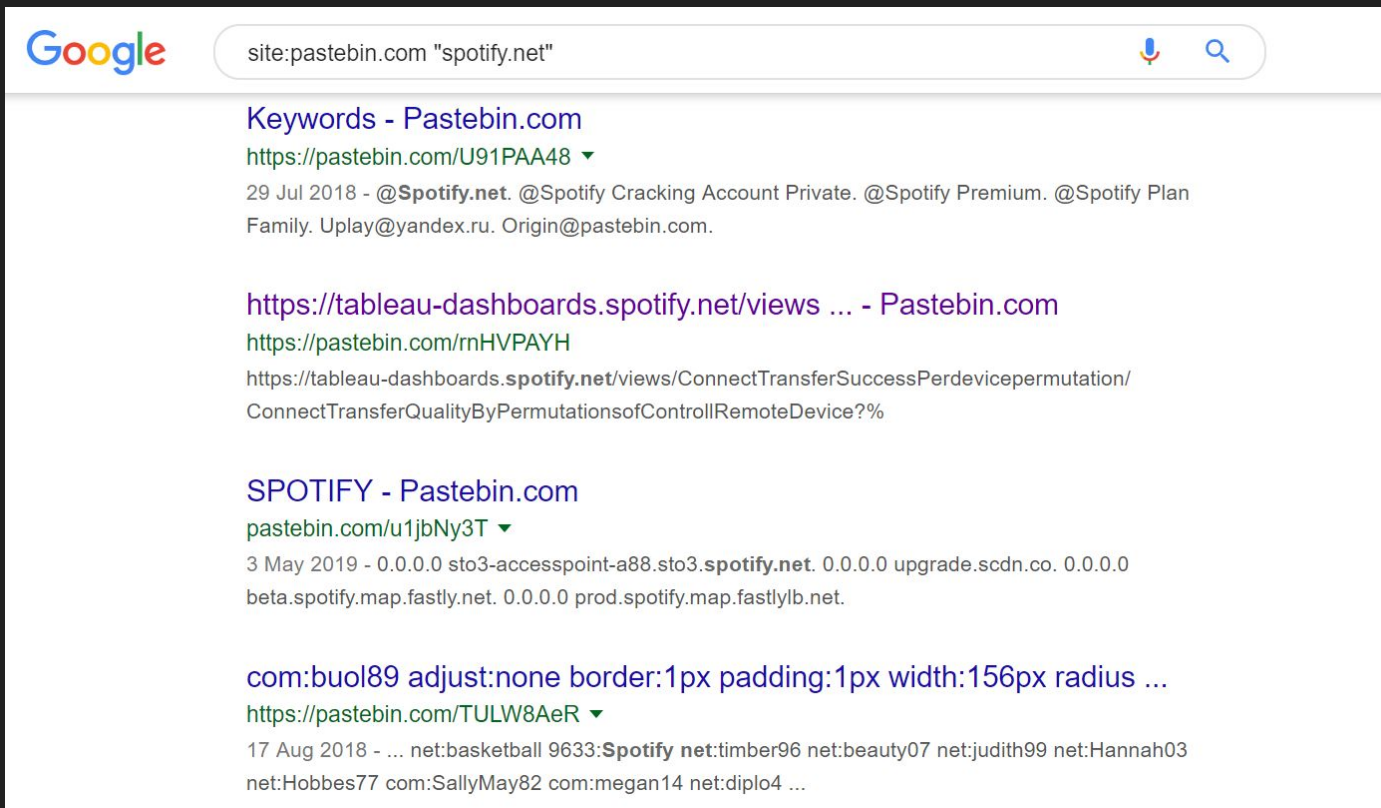
*“Knowledge is
power”*

- Some wise dude, a really long time ago

Things You Can Google For



The Other Things You Can Google For



Google

site:pastebin.com "spotify.net"

Keywords - Pastebin.com
<https://pastebin.com/U91PAA48> ▼
29 Jul 2018 - @**Spotify.net**. @Spotify Cracking Account Private. @Spotify Premium. @Spotify Plan Family. Uplay@yandex.ru. Origin@pastebin.com.

[https://tableau-dashboards.spotify.net/views ...](https://tableau-dashboards.spotify.net/views...) - Pastebin.com
<https://pastebin.com/rnHVPAYH>
<https://tableau-dashboards.spotify.net/views/ConnectTransferSuccessPerdevicepermutation/ConnectTransferQualityByPermutationsofControlRemoteDevice?%>

SPOTIFY - Pastebin.com
pastebin.com/u1jbNy3T ▼
3 May 2019 - 0.0.0.0 sto3-accesspoint-a88.sto3.spotify.net. 0.0.0.0 upgrade.scdn.co. 0.0.0.0 beta.spotify.map.fastly.net. 0.0.0.0 prod.spotify.map.fastlylb.net.

[com:buol89 adjust:none border:1px padding:1px width:156px radius ...](https://pastebin.com/TULW8AeR)
<https://pastebin.com/TULW8AeR> ▼
17 Aug 2018 - ... net:basketball 9633:Spotify net:timber96 net:beauty07 net:judith99 net:Hannah03 net:Hobbes77 com:SallyMay82 com:megan14 net:diplo4 ...

Things Google Doesn't Find (:

The screenshot shows a Yandex search interface. The search bar contains the query 'site:spotify.net' and a yellow 'Search' button. Below the search bar are navigation links: Web, Images, Video, News, Translate, Disk, Mail, and Ad. The 'Web' link is underlined. The search results section shows '10 results found' and lists four results, each with a globe icon, a title, a green lock icon, and a URL.

Yandex Search

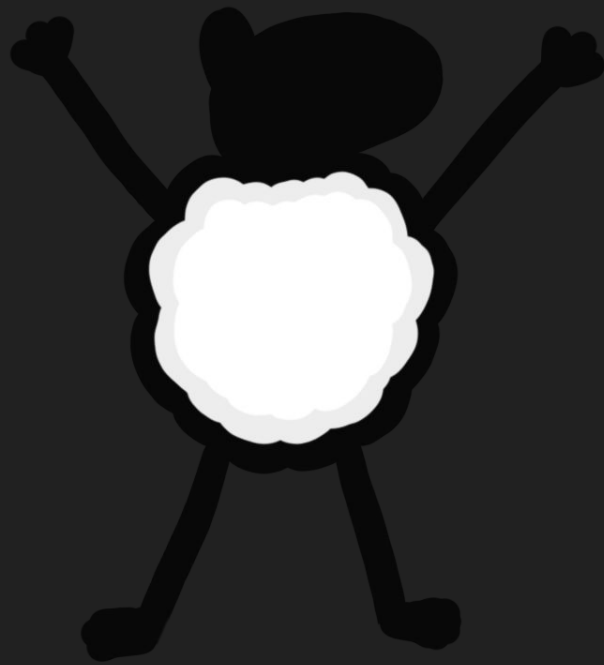
Web Images Video News Translate Disk Mail Ad

10 results found

- [Please Login](#)
🔒 [vpn.spotify.net](#) > remote/login?lang=en ▼
Please Login. Use FTM Push. FortiToken clock drift detected. Please input the next code...
- [vpn.spotify.net](#)
🔒 [vpn.spotify.net](#) ▼
- [resetpassword.spotify.net](#)
🔒 [resetpassword.spotify.net](#) ▼
The site owner hides the web page description.
- [Login | Redash](#)
🔒 [the-keys-dashboard.spotify.net](#) ▼

Thank You For Listening To My Talk

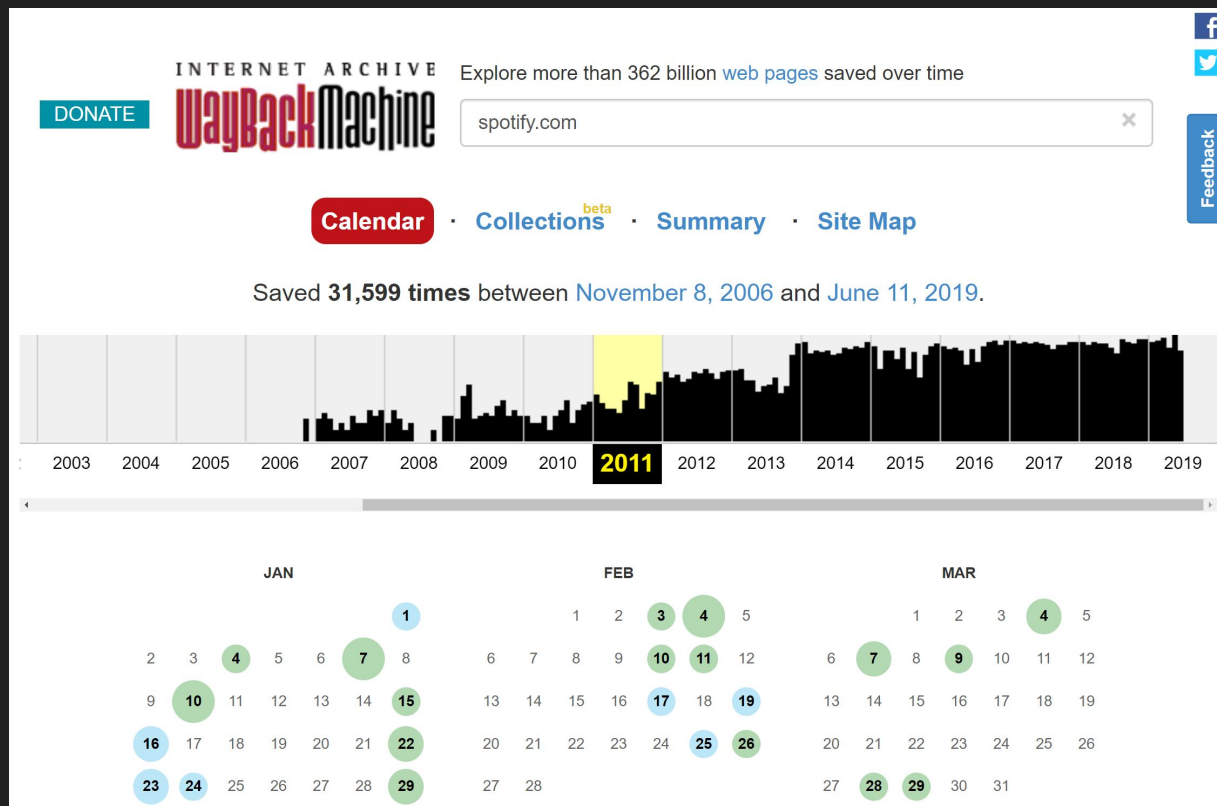
- Questions?
- Hugs?



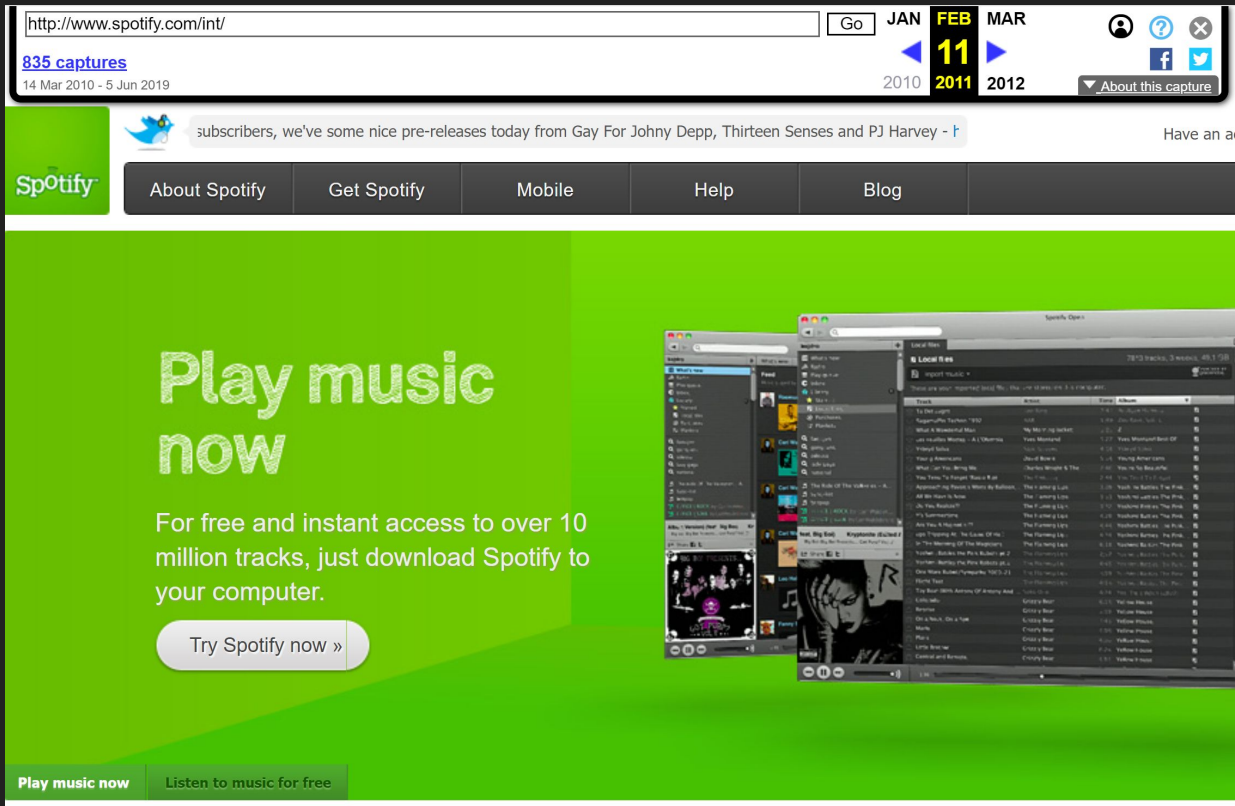
Other Search Engines

- Yandex
- DuckDuckGo / Bing
- Censys
- Shodan
- Zoomeye
- PublicWWW
- Many more...
- ...They're all worth a shot.

Look Into The Past



How To Feel Old: Step 1



Old URLs




```
tom@scan:~/recon/spotify (master)> echo spotify.net | waybackurls | tee -a urls
http://spotify.net/
http://spotify.net/about/what
http://spotify.net/AdrianaMedia
http://spotify.net/Auth0/AdrianaMedia
http://spotify.net/favicon.ico
https://spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fspotify.net%2FAdrianaMedia&
https://spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fspotify.net%2FAuth0%2FAdria
https://spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fspotify.net%2Frobots.txt&Id
http://spotify.net/robots.txt
http://abtesting.spotify.net/
https://abtesting.spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fabtesting.spotify
http://accessibility.spotify.net/
https://accessibility.spotify.net/mellon/login?ReturnTo=https%3A%2F%2Faccessibility
http://act.spotify.net/
https://act.spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fact.spotify.net%2F&IdP=
http://act-dev.spotify.net/
https://act-dev.spotify.net/mellon/login?ReturnTo=https%3A%2F%2Fact%2Ddev.spotify.n
http://adops.spotify.net/
```

No Googles Allowed

```
tom@scan:~/recon/spotify (master)> meg -c 200 -s 200 /robots.txt
tom@scan:~/recon/spotify (master)> grep -hri disallow out/ | awk '{print $NF}'
/webmail/
/shared/webmail/
/webmail/
/shared/webmail/
/
/local/
/download/
/embed-podcast/
/embed/
/
pages
/wp-admin/
/wp-login.php
```

You Get The Gist

GitHub Gist [All gists](#) [Back to GitHub](#)


Search Search

Languages


Text	14
JavaScript	5
HTML	4
Markdown	3
JSON	2
Ruby	2
Shell	2
CSS	1
Python	1
XML	1

[Cheat sheet](#)

43 gist results Sort: Best match ▾






 [rculbertson](#) / [gist:03d370d42fbe554cf7cb](#) 1 file 0 forks 0 comments 0 stars
Created 5 years ago

```
1 2014-07-24T17:05:28.993+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
2 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
3 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
4 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
5 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
6 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
7 2014-07-24T17:05:28.995+00:00 awsuse1-heliosmaster-a4.shared.cloud.spotify.net helios[17
```

 [Tarrasch](#) / [gist:830e0a22ee4af120fc86](#) 1 file 0 forks 0 comments 0 stars
Created 4 years ago

```
1 ~/spotify/repos/gcp-migrate various-improvements
2 > git remote -v
3 origin git@ghe.spotify.net:arash/gcp-migrate.git (fetch)
4 origin git@ghe.spotify.net:arash/gcp-migrate.git (push)
```

Searching GitHub

 "spotify.net"  Pull requests Issues Marketplace Explore   

Repositories 8

Code 851+

Commits 772

Issues 18

Packages 0

Marketplace 0

Topics 0

Wikis 0

Users 0

Languages

C# 275

JSON 40

Text 36

Shell 34


HTML 33

Markdown 29


Python 28

JavaScript 27

Java 24

Showing 795 available code results 

Sort: Best match ▾

 bogdad/gcprocessing – rring.txt

Showing the top four matches Last indexed on 8 Jul 2018

6

8839064868652493482

7


ash2-pubsub2cassandra-a1.ash2.spotify.net rac1 Up Normal 367.98 GB 1.04%

-9223372036854775808

8

ash2-pubsub2cassandra-a1863.ash2.spotify.net rac1 Up Normal 203.53 GB 1.04%

-8839064868652493483

 irisSchaffer/my-reason-react-app – yarn.lock

Showing the top four matches Last indexed 26 days ago

5

"@babel/code-frame@^7.0.0":

6

version "7.0.0"


7

resolved "https://artifactory.spotify.net/artifactory/api/npm/virtual-npm/@babel/code-frame/-/code-frame-7.0.0.tgz#06e2ab19bdb53538559aabb5ba59729482800f8"

...

13

resolved "https://artifactory.spotify.net/artifactory/api/npm/virtual-npm/@babel/core/-/core-7.4.4.tgz#84055750b05fcd50f9915a826b44fa347a825250"

 jeekl/dotfiles – jumphost

Showing the top four matches Last indexed on 26 Jun 2018

3

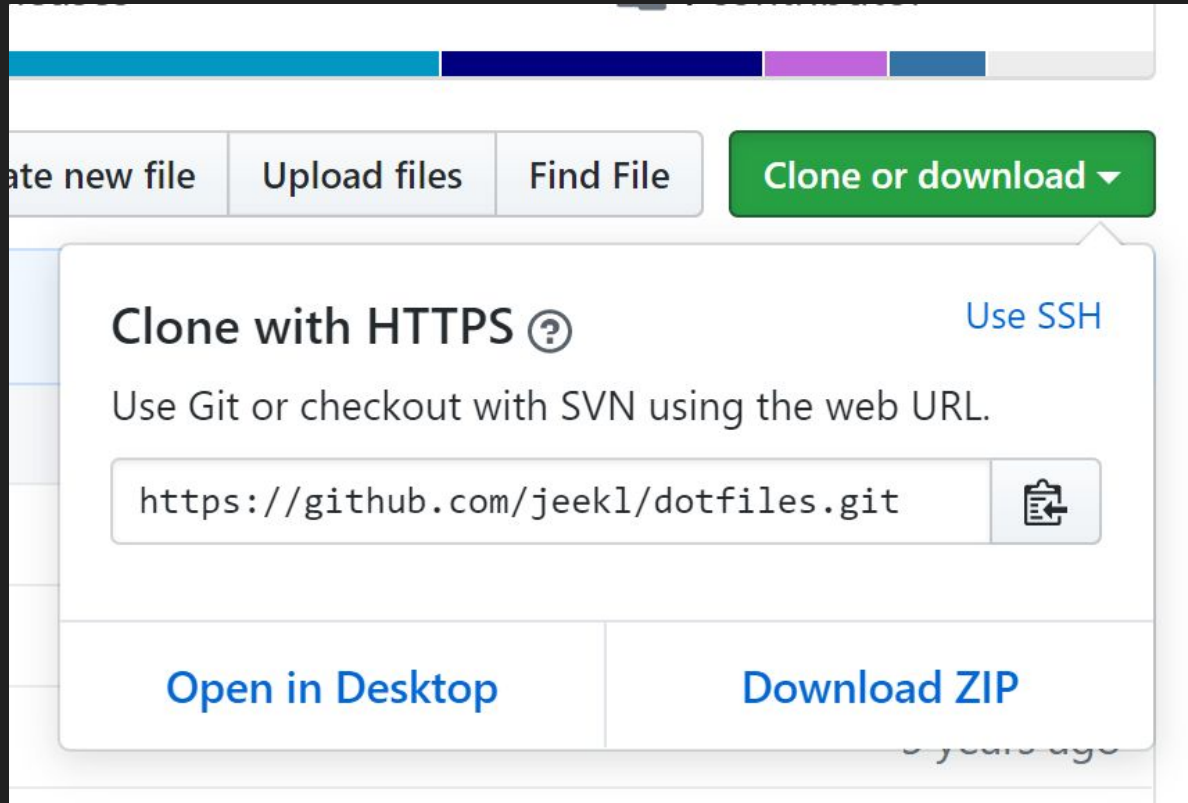
require 'optparse'

4

5

jumphosts = ['ash-jumphost-a1.ash.spotify.net',

Searching History



Dumping Git Objects

```
tom@scan:~/recon/spotify/repos/dotfiles (master)> cat $(which ghdump)
#!/bin/bash

{
    find .git/objects/pack/ -name "*.idx" | while read i; do
        git show-index < "$i" | awk '{print $2}';
    done;

    find .git/objects/ -type f |
        grep -v '/pack/' |
        awk -F'/' '{print $(NF-1)$NF}';
} | while read o; do
    git cat-file -p $o | awk "{print \"$o: \" \"$0  }";
done
tom@scan:~/recon/spotify/repos/dotfiles (master)> ghdump > all-objects
```


<3 grep -a

```
tom@scan:~/recon/spotify/repos/dotfiles (master)> grep -Hnia spotify all-objects
all-objects:183:0286a153da6b9902fdcb9f5cb5722fbc20e4551b:          email = jeekl@spotify.com
all-objects:242:0286a153da6b9902fdcb9f5cb5722fbc20e4551b:          host = ghe.spotify.net
all-objects:10422:145c541ae81d2f01ea41ea95a6597dc89c1739: committer Jeff Eklund <jeekl@spotify.com> 1381911686 +0200
all-objects:14788:17ff8007fe358f55efdd202c5bed51f57913afe5: jumphosts = ['ash-jumphost-a1.ash.spotify.net',
all-objects:14789:17ff8007fe358f55efdd202c5bed51f57913afe5:             'ash1-jumphost-b1.ash.spotify.net',
all-objects:14790:17ff8007fe358f55efdd202c5bed51f57913afe5:             'ash2-jumphost-a1.ash2.spotify.net',
all-objects:14791:17ff8007fe358f55efdd202c5bed51f57913afe5:             'ash2-jumphost-b1.ash2.spotify.net',
all-objects:14792:17ff8007fe358f55efdd202c5bed51f57913afe5:             'lon-jumphost-a1.lon.spotify.net',
all-objects:14793:17ff8007fe358f55efdd202c5bed51f57913afe5:             'lon1-jumphost-b1.lon.spotify.net',
all-objects:14794:17ff8007fe358f55efdd202c5bed51f57913afe5:             'lon3-jumphost-a1.lon3.spotify.net',
all-objects:14795:17ff8007fe358f55efdd202c5bed51f57913afe5:             'lon3-jumphost-b1.lon3.spotify.net',
all-objects:14796:17ff8007fe358f55efdd202c5bed51f57913afe5:             'sjc1-jumphost-a1.sjc1.spotify.net',
all-objects:14797:17ff8007fe358f55efdd202c5bed51f57913afe5:             'sjc1-jumphost-b1.sjc1.spotify.net',
all-objects:14798:17ff8007fe358f55efdd202c5bed51f57913afe5:             'sto-jumphost-a1.sto.spotify.net']
all-objects:14800:17ff8007fe358f55efdd202c5bed51f57913afe5: opsjumphosts = ['laxmi.sto.spotify.net',
all-objects:14801:17ff8007fe358f55efdd202c5bed51f57913afe5:                 'ash1-jumphost-b1.ash.spotify.net',
all-objects:14802:17ff8007fe358f55efdd202c5bed51f57913afe5:                 'lon1-jumphost-b1.lon.spotify.net',
all-objects:14803:17ff8007fe358f55efdd202c5bed51f57913afe5:                 'lon3-jumphost-b1.lon3.spotify.net',
all-objects:14804:17ff8007fe358f55efdd202c5bed51f57913afe5:                 'sjc1-jumphost-b1.sjc1.spotify.net']
```

Viewing Objects

```
tom@scan:~/recon/spotify/repos/dotfiles (master)> git cat-file -p 0286a153da6b9902fdcb9f5cb5722fbc20e4551b
[user]
    name = Jeff Eklund
    email = jeekl@spotify.com
[core]
    excludesfile = ~/.gitignore
[push]
    default = current
[github]
    user = jeekl
[color]
    diff = auto
    status = auto
    branch = auto
    interactive = auto
    pager = yes
```


Docker Images

 **docker hub**


Search for great content (e.g., mysql)


ExploreSign InPricing


Get Started




spotify [Edit profile](#)

 Community Organization


 Spotify

 <http://labs.spotify.com/>

 Joined July 30, 2013

Repositories

Displaying 25 of 26 repositories



spotify/docker-gc

By [spotify](#) • Updated 5 days ago

10M+ Downloads79 Stars

Garbage collection of Docker containers and images

Container

Overriding The Entrypoint

```
tom@scan:~> sudo docker run -it --entrypoint bash spotify/helios-test-container:1
root@85a8a171caf6:/# ls
bin  boot  dev  etc  home  lib  lib64  media  mnt  openjdk-11-sha256sum.txt  openjdk-11_lin
root@85a8a171caf6:/# vim openjdk-11-sha256sum.txt
bash: vim: command not found
root@85a8a171caf6:/# :(
bash: syntax error near unexpected token `newline'
root@85a8a171caf6:/# _
```


Container Filesystem Access From The Host

```
tom@scan:~> sudo docker inspect 85a8a171caf6 | gron | grep -i pid
json[0].HostConfig.PidMode = "";
json[0].HostConfig.PidsLimit = 0;
json[0].State.Pid = 13130;
tom@scan:~> sudo -i
root@scan:~# cd /proc/13130/root/
root@scan:/proc/13130/root# ls
bin    dev    home   lib64  mnt                openjdk-11_linux-
boot  etc    lib     media  openjdk-11-sha256sum.txt  opt
root@scan:/proc/13130/root# grep -Hnria spotify
var/lib/apt/lists/archive.ubuntu.com_ubuntu_dists_bionic_universe_s
var/lib/apt/lists/archive.ubuntu.com_ubuntu_dists_bionic_universe_s
o[] [] [] [] [] ;T[] [] [] 494aacfcba9d98013c3b16904e8a65d9 19g]Beos_[] [] [] [] 074c0722
var/lib/apt/lists/archive.ubuntu.com_ubuntu_dists_bionic_universe_b
spotify,#5[] 5g[] [] q (>= 2.u9ython (<< 2.8[] C:any& q6.6-7~)[] js-sphinxd
var/lib/apt/lists/archive.ubuntu.com_ubuntu_dists_bionic_universe_b
```

Where Else Can We Look?

- Give me your ideas!
- Ask me your questions!
- I love questions...
- Go on... Please. I'd really appreciate it.