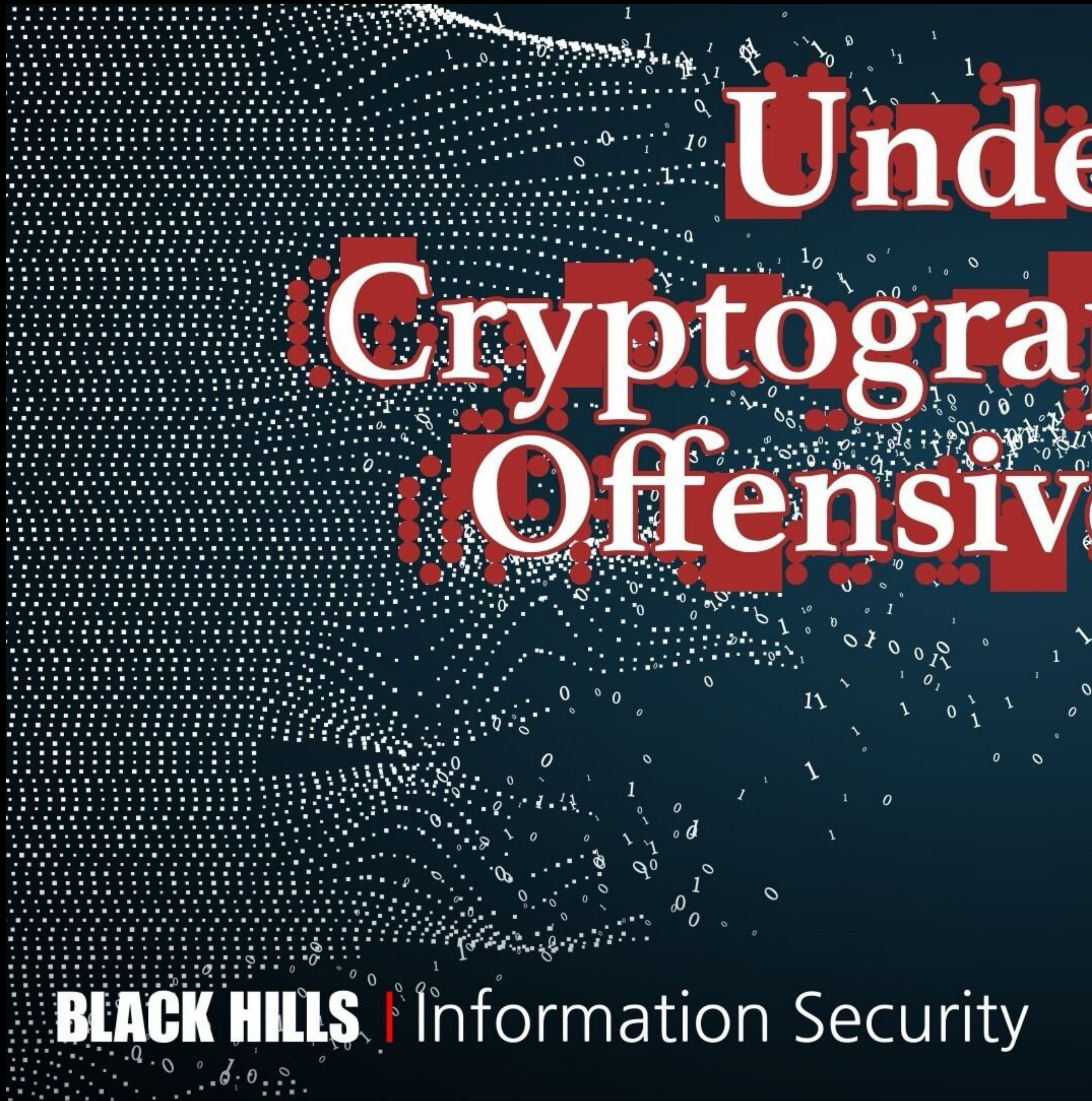


Understanding Cryptography for Offensive Security

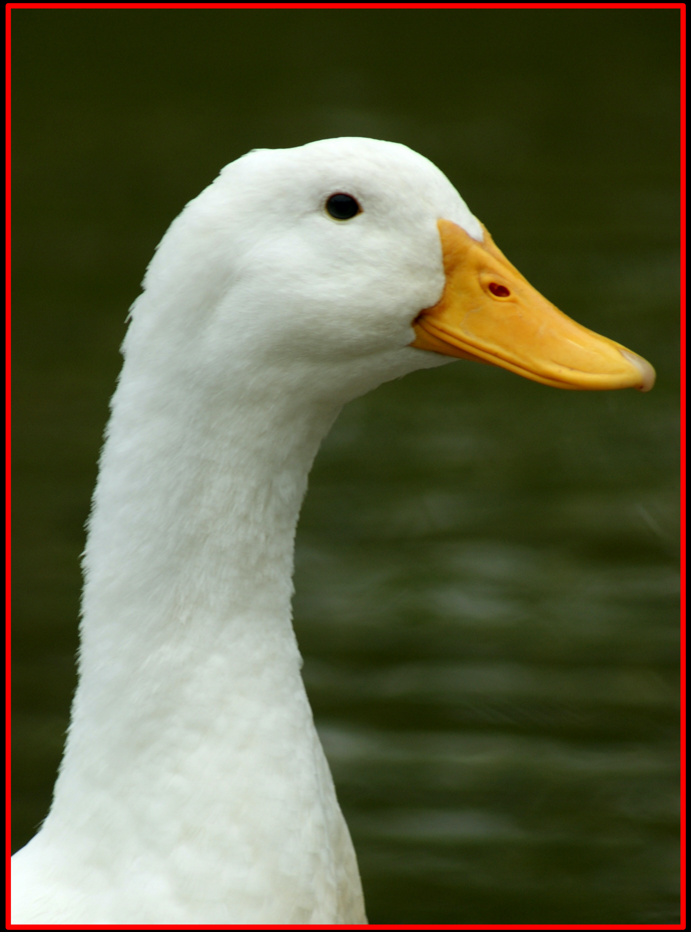
Ayub Yusuf

BLACK HILLS | Information Security

WEBCAST

Ayub Yusuf

- Hacker at BHIS
- GSE, OSCP
- Scared of Bees and Math



@whitecyberduck

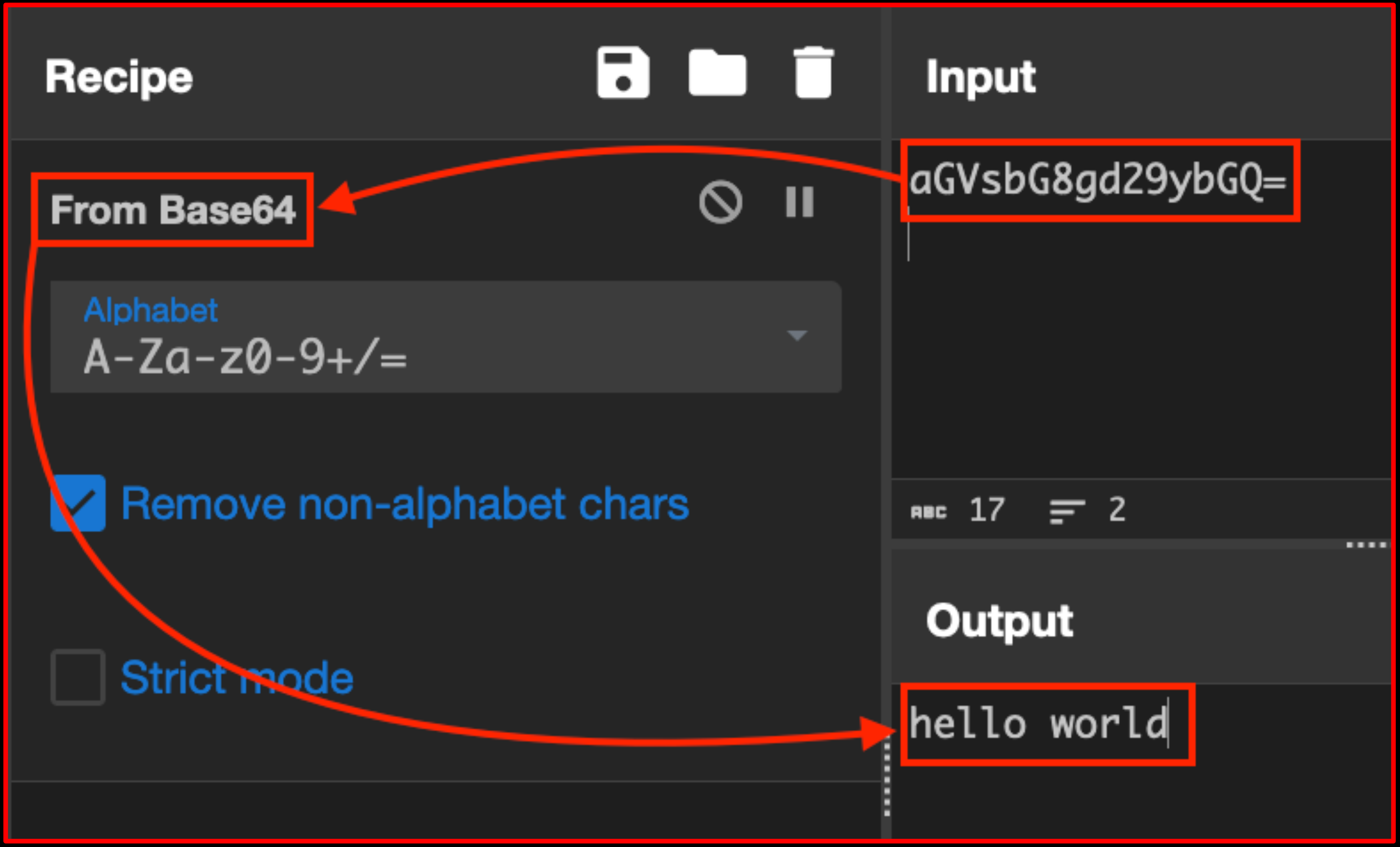
Encoding

Encoding is how we transmit information

Examples

- ASCII
- UTF-8 (most everything)
- UTF-16LE (windows, for some reason)
- base64

aGVsbG8gd29ybGQ=



Recipe

From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

Input

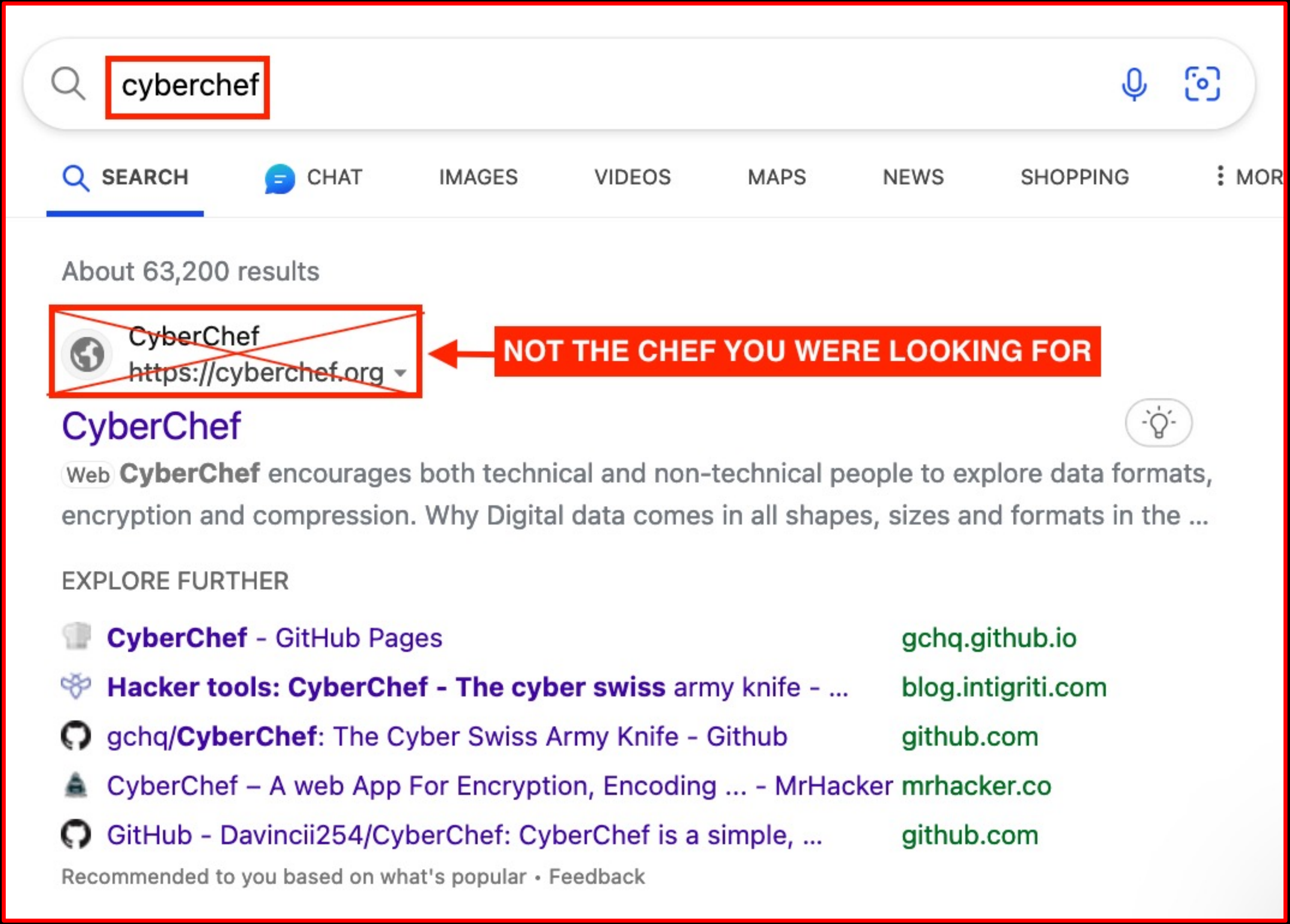
```
aGVsbG8gd29ybGQ=
```

abc 17 ☰ 2

Output

```
hello world
```

https://gchq.github.io/CyberChef/
https://github.com/mattnotmax/cyberchef-recipes



About 63,200 results

~~CyberChef~~
~~https://cyberchef.org~~

NOT THE CHEF YOU WERE LOOKING FOR

CyberChef

Web **CyberChef** encourages both technical and non-technical people to explore data formats, encryption and compression. Why Digital data comes in all shapes, sizes and formats in the ...

EXPLORE FURTHER

CyberChef - GitHub Pages	gchq.github.io
Hacker tools: CyberChef - The cyber swiss army knife - ...	blog.intigriti.com
gchq/**CyberChef**: The Cyber Swiss Army Knife - Github	github.com
CyberChef – A web App For Encryption, Encoding ... - MrHacker	mrhacker.co
GitHub - Davincii254/CyberChef: CyberChef is a simple, ...	github.com

Recommended to you based on what's popular • Feedback

https://www.bing.com

Hashing

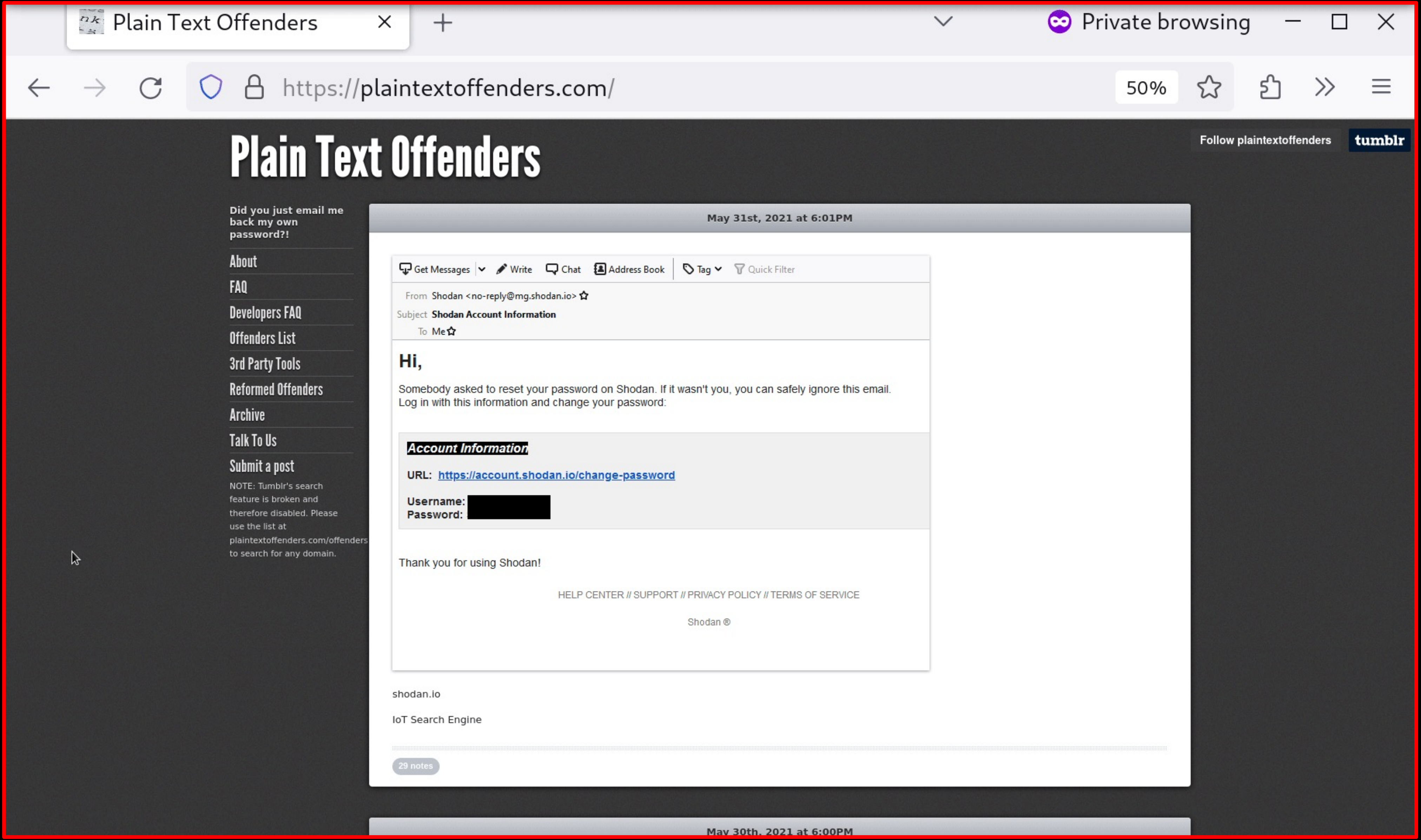
Used to uniquely identify an input.

A good hashing algo

- Is unique and has rare and unpredictable collusions
- Irreversible

Example

- **MD4**
    - NT hashes
- **MD5**
- SHA family



Plain Text Offenders

Did you just email me back my own password?!

- About
- FAQ
- Developers FAQ
- Offenders List
- 3rd Party Tools
- Reformed Offenders
- Archive
- Talk To Us
- Submit a post

NOTE: Tumblr's search feature is broken and therefore disabled. Please use the list at plaintextoffenders.com/offenders to search for any domain.

May 31st, 2021 at 6:01PM

From Shodan <no-reply@mg.shodan.io>
Subject **Shodan Account Information**
To Me

Hi,

Somebody asked to reset your password on Shodan. If it wasn't you, you can safely ignore this email.
Log in with this information and change your password:

Account Information

URL: https://account.shodan.io/change-password

Username: [redacted]
Password:

Thank you for using Shodan!

HELP CENTER // SUPPORT // PRIVACY POLICY // TERMS OF SERVICE

Shodan ®

shodan.io

IoT Search Engine

29 notes

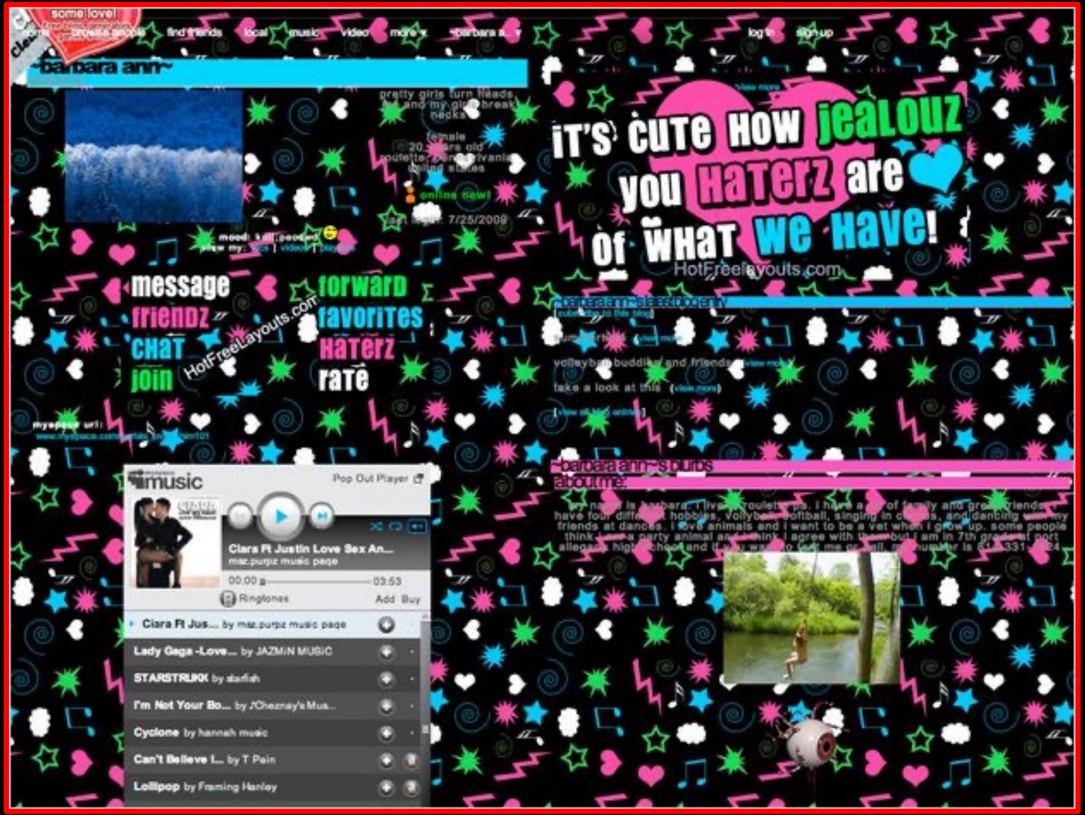
May 30th, 2021 at 6:00PM

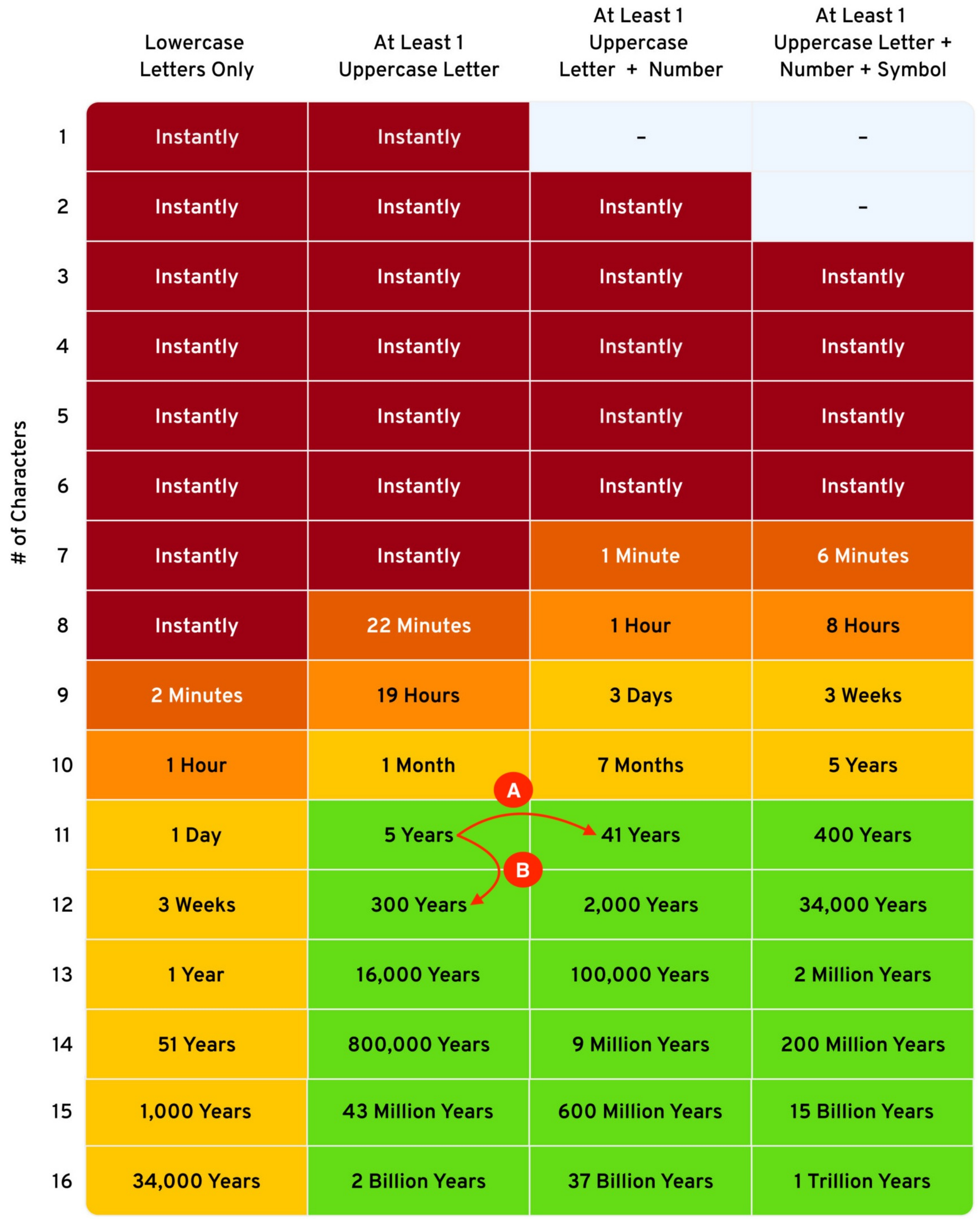
https://plaintextoffenders.com/

Origins of rockyou.txt

rockyou

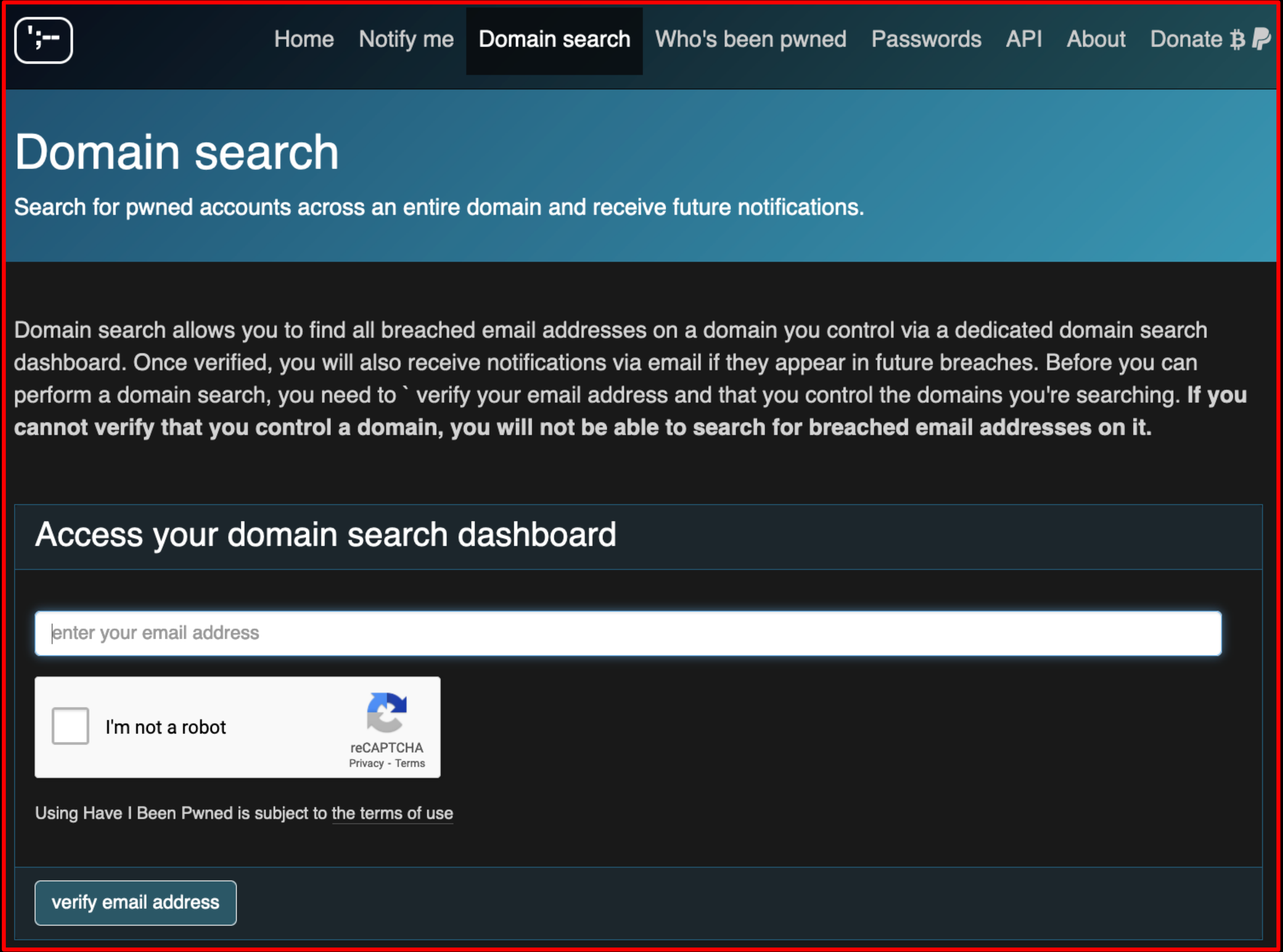
- Developed widgets for MySpace
- In 2009, they suffered a data breach that exposed over 14 million plaintext passwords
- People aren't random generators


~barbara ann~
iT'S CUTE HOW jeaLOUZ you HATERZ are Of WHAT we Have!
HotFreeLayouts.com
message
friendz
chat
join
forward
favorites
haterz
rate
HotFreeLayouts.com
music
Pop Out Player
Ciara Ft Justin Love Sex An...
Ciara Ft Jus... by maz.purpz music page
Lady Gaga -Love... by JAZMIN MUSIC
STARSTRUKK by starfish
I'm Not Your Bo... by J'Chezney's Mus...
Cyclone by hannah music
Can't Believe I... by T Pain
Lollipop by Framing Hanley



# of Characters	Lowercase Letters Only	At Least 1 Uppercase Letter	At Least 1 Uppercase Letter + Number	At Least 1 Uppercase Letter + Number + Symbol
1	Instantly	Instantly	–	–
2	Instantly	Instantly	Instantly	–
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 Minute	6 Minutes
8	Instantly	22 Minutes	1 Hour	8 Hours
9	2 Minutes	19 Hours	3 Days	3 Weeks
10	1 Hour	1 Month	7 Months	5 Years
11	1 Day	5 Years	41 Years	400 Years
12	3 Weeks	300 Years	2,000 Years	34,000 Years
13	1 Year	16,000 Years	100,000 Years	2 Million Years
14	51 Years	800,000 Years	9 Million Years	200 Million Years
15	1,000 Years	43 Million Years	600 Million Years	15 Billion Years
16	34,000 Years	2 Billion Years	37 Billion Years	1 Trillion Years

Source:
https://www.security.org/



Domain search

Search for pwned accounts across an entire domain and receive future notifications.

Domain search allows you to find all breached email addresses on a domain you control via a dedicated domain search dashboard. Once verified, you will also receive notifications via email if they appear in future breaches. Before you can perform a domain search, you need to ` verify your email address and that you control the domains you're searching. **If you cannot verify that you control a domain, you will not be able to search for breached email addresses on it.**

Access your domain search dashboard

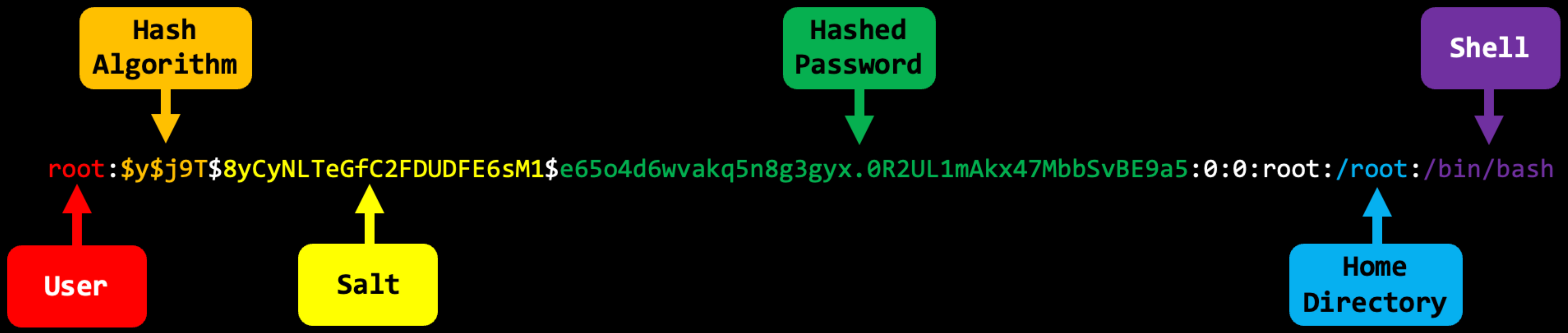
enter your email address

□ I'm not a robot

Using Have I Been Pwned is subject to the terms of use

https://haveibeenpwned.com/DomainSearch

Linux Hashing



Hash Algorithm

Hashed Password

Shell

```
root:$y$j9T$8yCyNLTeGfC2FDUDFE6sM1$e65o4d6wvakq5n8g3gyx.0R2UL1mAkx47MbbSvBE9a5:0:0:root:/root:/bin/bash
```

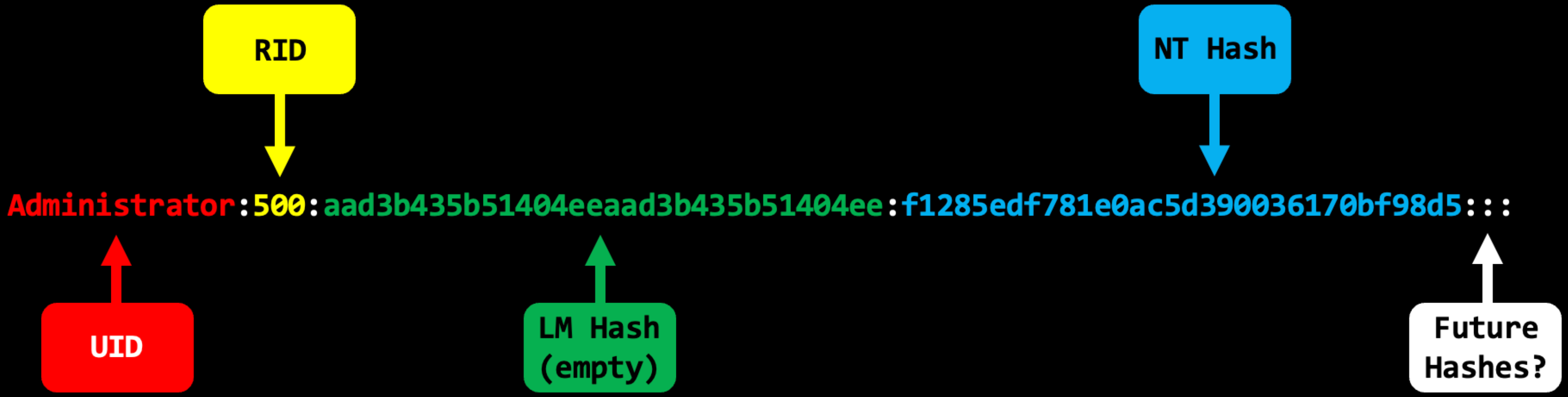
User

Salt

Home Directory

ID	Method	Hashcat (-m {#})	John the Ripper (--format={name})
$1$	MD5	500	md5crypt
$2*$	Blowfish	3200	bcrypt
$5$	SHA-256	7400	sha256crypt
$6$	SHA-512	1800	sha512crypt
$y$	yescript	N/a	crypt

Windows Hashing



```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f1285edf781e0ac5d390036170bf98d5:::
```

Method	Hashcat (-m {#})	John the Ripper (--format={name})
LM	3000	LM
NT	1000	NT
NetNTMLv1	5500	netntlm
NetNTLMv2	5600	netntlmv2
Kerberos 5 AS-REQ	18200	krb5asrep
Kerberos RC4	13100	krb5tgs

Encryption

Two types

- Asymmetric
- Symmetric

Foundational Problem

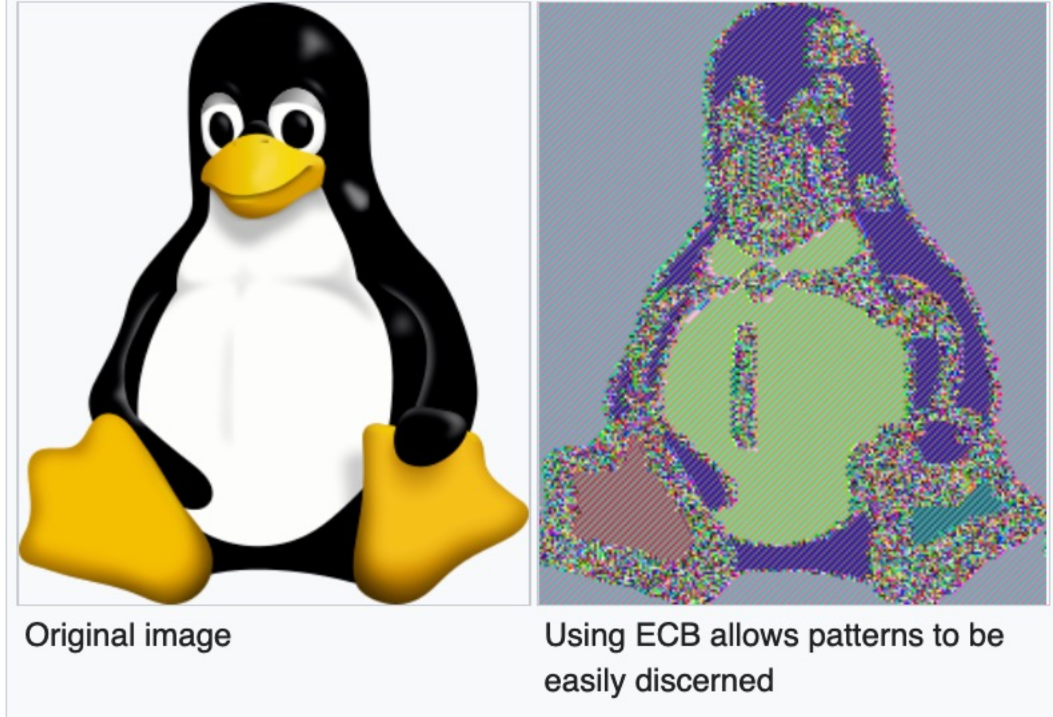
- Key management

Examples

- DES
- AES
- RSA

Block Cipher Modes

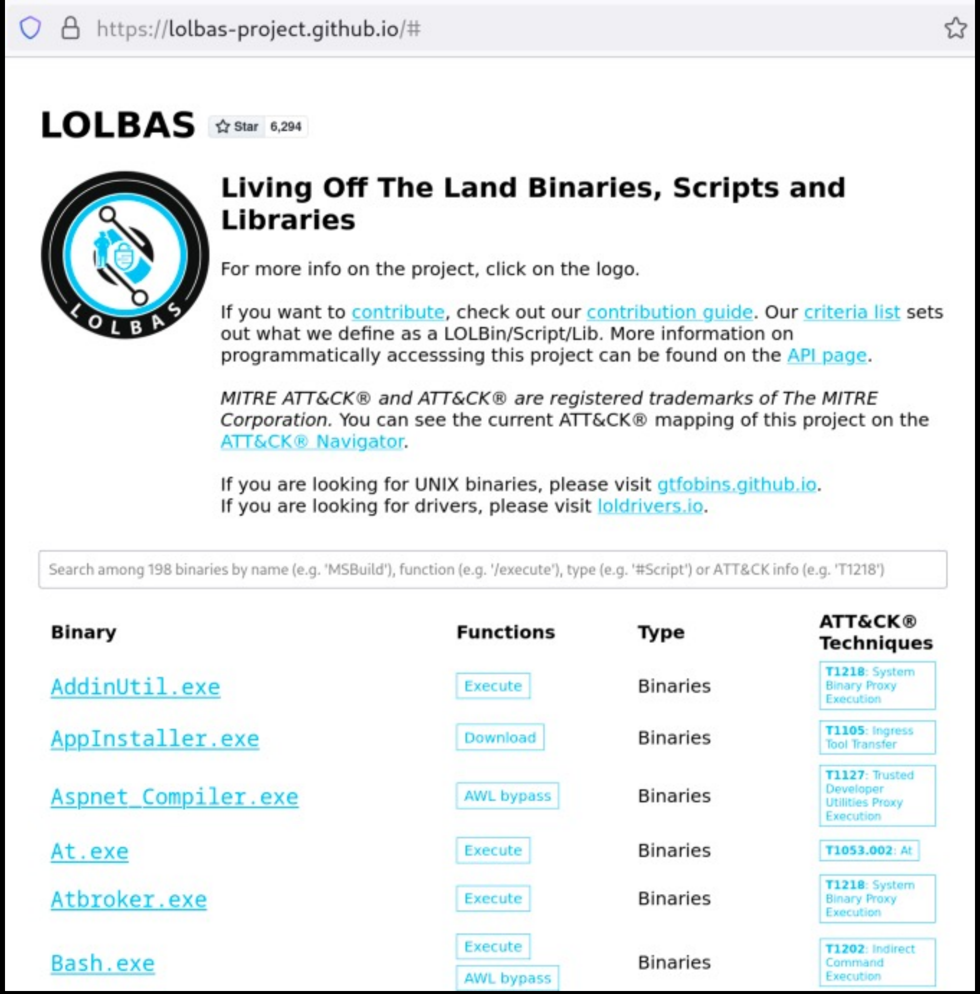
- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Galois/Counter Mode (GCM)



Original image

Using ECB allows patterns to be easily discerned

Digital Signature



LOLBAS

Living Off The Land Binaries, Scripts and Libraries

For more info on the project, click on the logo.

If you want to contribute, check out our contribution guide. Our criteria list sets out what we define as a LOLBin/Script/Lib. More information on programmatically accesssing this project can be found on the API page.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation. You can see the current ATT&CK® mapping of this project on the ATT&CK® Navigator.

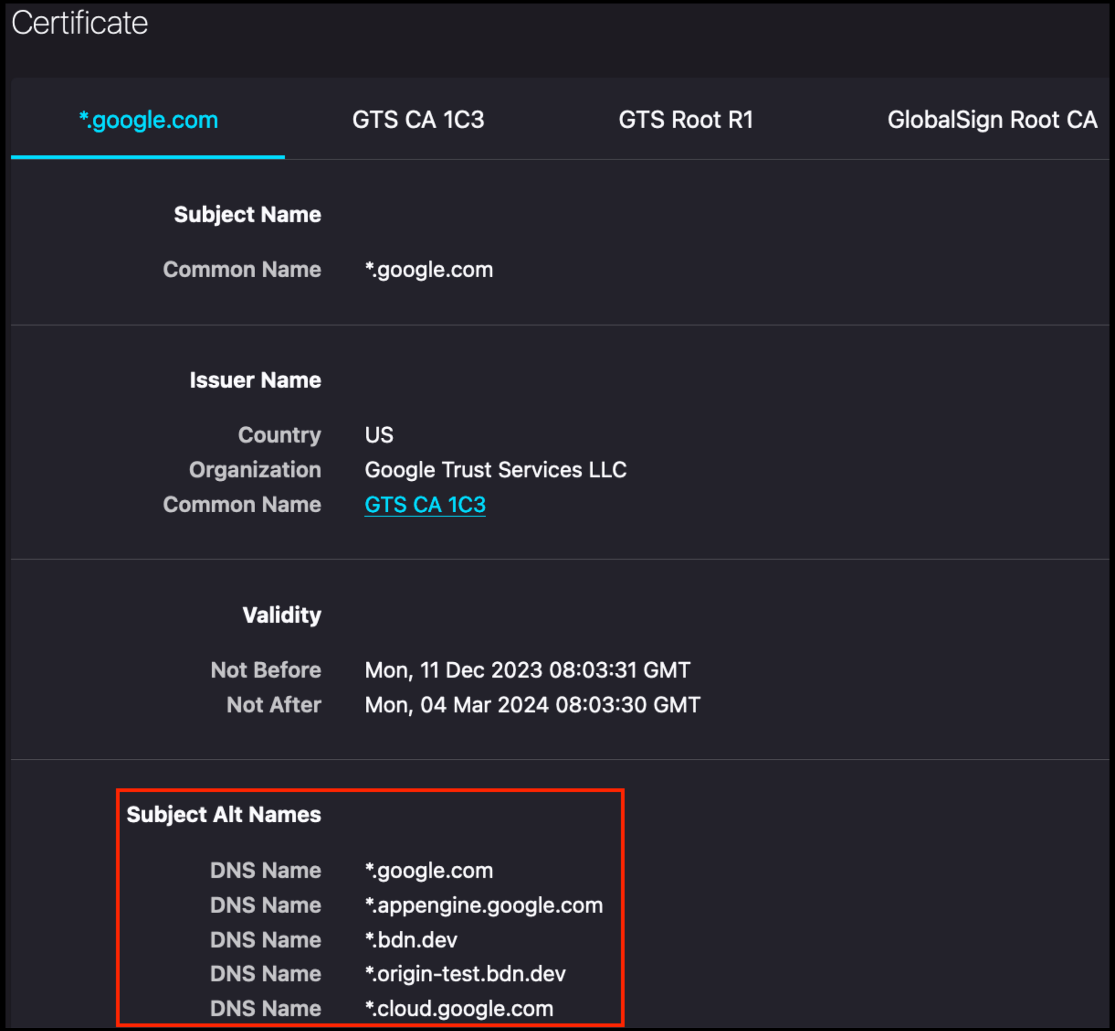
If you are looking for UNIX binaries, please visit gtfobins.github.io.
If you are looking for drivers, please visit loldrivers.io.

Search among 198 binaries by name (e.g. 'MSBuild'), function (e.g. '/execute'), type (e.g. '#Script') or ATT&CK info (e.g. 'T1218')

Binary	Functions	Type	ATT&CK® Techniques
AddinUtil.exe	Execute	Binaries	T1218: System Binary Proxy Execution
AppInstaller.exe	Download	Binaries	T1105: Ingress Tool Transfer
Aspnet_Compiler.exe	AWL bypass	Binaries	T1127: Trusted Developer Utilities Proxy Execution
At.exe	Execute	Binaries	T1053.002: At
Atbroker.exe	Execute	Binaries	T1218: System Binary Proxy Execution
Bash.exe	Execute AWL bypass	Binaries	T1202: Indirect Command Execution

https://lolbas-project.github.io/#

Certificates



Certificate

Subject Name

Common Name *.google.com

Issuer Name

Country US
Organization Google Trust Services LLC
Common Name GTS CA 1C3

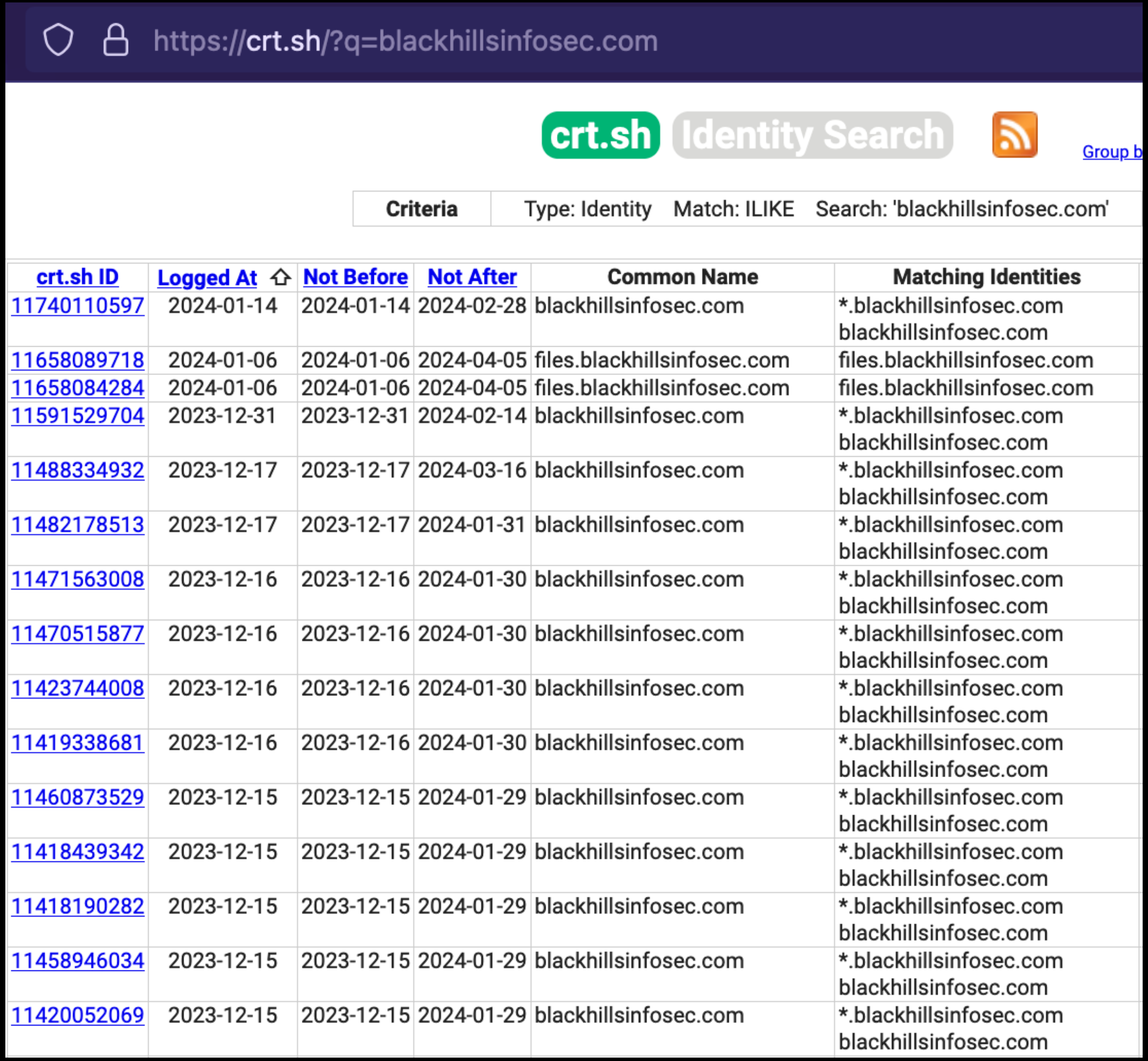
Validity

Not Before Mon, 11 Dec 2023 08:03:31 GMT
Not After Mon, 04 Mar 2024 08:03:30 GMT

Subject Alt Names

DNS Name *.google.com
DNS Name *.appengine.google.com
DNS Name *.bdn.dev
DNS Name *.origin-test.bdn.dev
DNS Name *.cloud.google.com

crt.sh



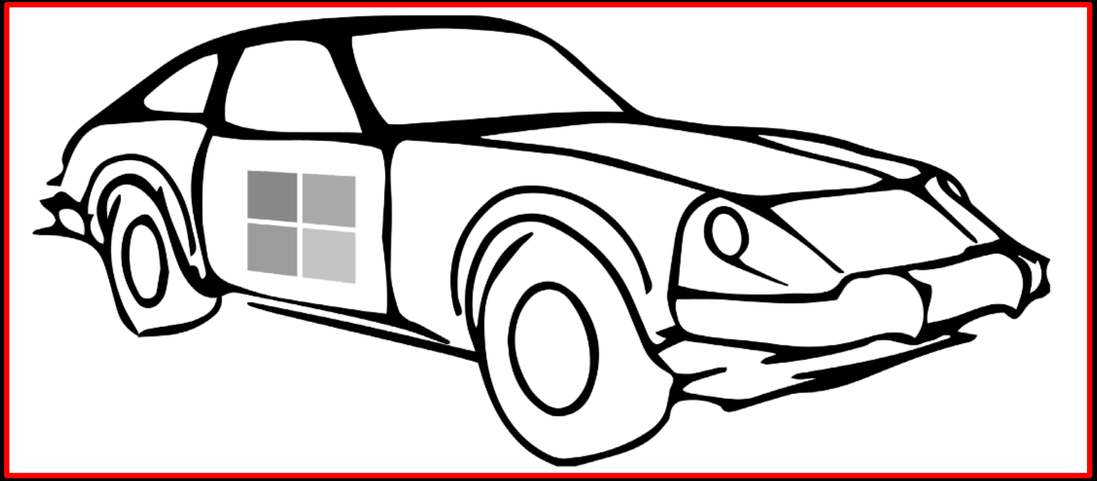
https://crt.sh/?q=blackhillsinfosec.com

Criteria	Type: Identity Match: ILIKE Search: 'blackhillsinfosec.com'

crt.sh ID	Logged At ⇧	Not Before	Not After	Common Name	Matching Identities
11740110597	2024-01-14	2024-01-14	2024-02-28	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11658089718	2024-01-06	2024-01-06	2024-04-05	files.blackhillsinfosec.com	files.blackhillsinfosec.com
11658084284	2024-01-06	2024-01-06	2024-04-05	files.blackhillsinfosec.com	files.blackhillsinfosec.com
11591529704	2023-12-31	2023-12-31	2024-02-14	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11488334932	2023-12-17	2023-12-17	2024-03-16	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11482178513	2023-12-17	2023-12-17	2024-01-31	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11471563008	2023-12-16	2023-12-16	2024-01-30	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11470515877	2023-12-16	2023-12-16	2024-01-30	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11423744008	2023-12-16	2023-12-16	2024-01-30	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11419338681	2023-12-16	2023-12-16	2024-01-30	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11460873529	2023-12-15	2023-12-15	2024-01-29	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11418439342	2023-12-15	2023-12-15	2024-01-29	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11418190282	2023-12-15	2023-12-15	2024-01-29	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11458946034	2023-12-15	2023-12-15	2024-01-29	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com
11420052069	2023-12-15	2023-12-15	2024-01-29	blackhillsinfosec.com	*.blackhillsinfosec.com blackhillsinfosec.com

Active Directory Certificate Services

- In 2021, Certified Pre-Owned paper described eight escalation paths.
- Currently, there are 11 and counting…
- Most dangerous one: ESC1
  - Client Authentication: **True**
  - Enabled: **True**
  - Enrollee Supplies Subject: **True**
  - Requires Management Approval: **False**
  - Authorized Signatures Required: **0**

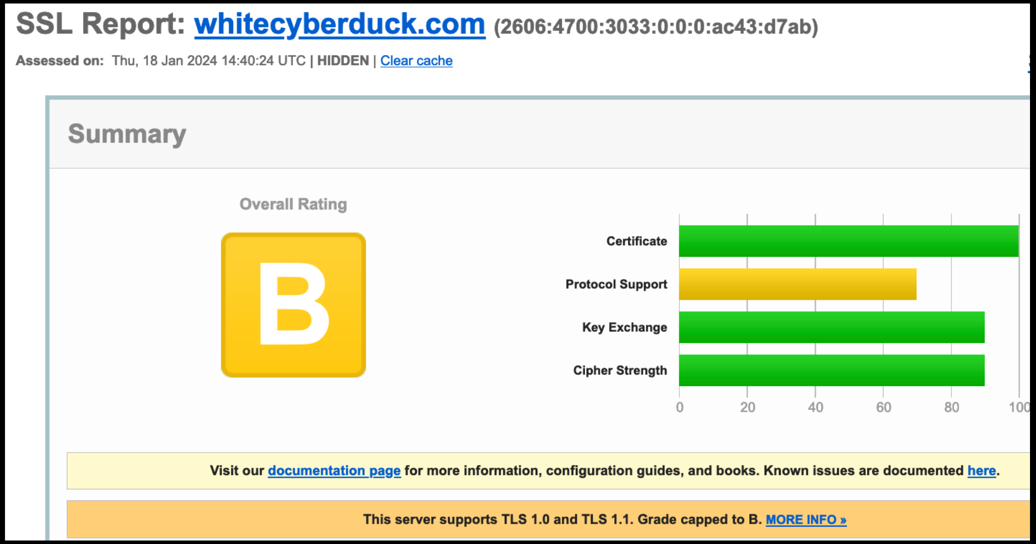


https://specterops.io/wp-content/uploads/sites/3/2022/06/Certified_Pre-Owned.pdf

https://www.blackhillsinfosec.com/abusing-active-directory-certificate-services-part-one/

SSL/TLS

Version	Status
SSLv2	Depreciated in 2011
SSLv3	Depreciated in 2015
TLS 1.0	Depreciated in 2021
TLS 1.1	Depreciated in 2021
TLS 1.2	Active since 2008
TLS 1.3	Active since 2018



SSL Report: whitecyberduck.com (2606:4700:3033:0:0:0:ac43:d7ab)

Assessed on: Thu, 18 Jan 2024 14:40:24 UTC | HIDDEN | Clear cache

Summary

Overall Rating

B

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.0 and TLS 1.1. Grade capped to B. MORE INFO »

https://www.ssllabs.com/ssltest/
https://github.com/drwetter/testssl.sh
https://www.blackhillsinfosec.com/testssl-sh-assessing-ssltls-configurations-at-scale/

Thank you!

Conclusion

- Protect your keys
  - Long (15+) and unique passwords are the best way to protect yourself online
  - Monitor breach data
- Use the best cryptography available with proper configuration
  - TLS 1.2+
  - Avoid weak hashing: MD5 or SHA1
  - Avoid weak encryption: DES
  - Avoid weak modes: ECB or CBC
- One more thing… **tryhackme.com/jr/pineappleonpizza**