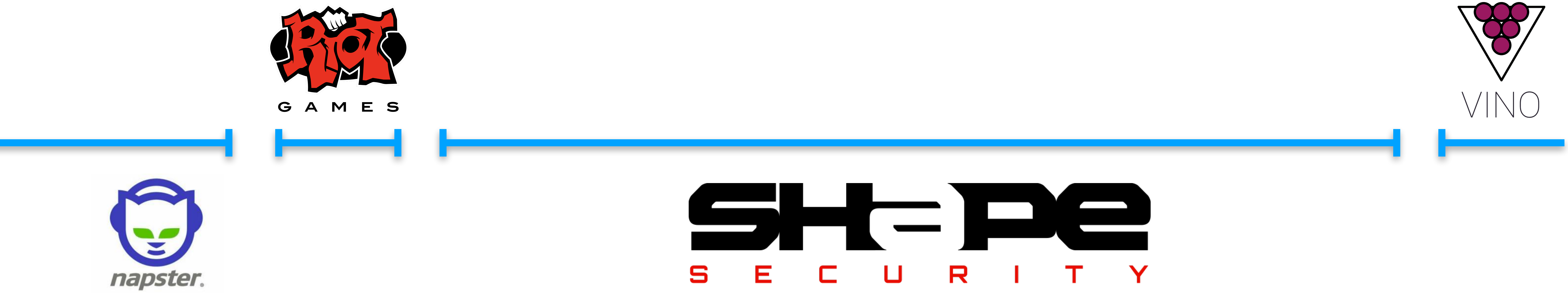
The state of credential stuffing.

Bad bots and the automation war

Jarrod Overson - @jsoverson

Jarrod Overson

Perpetually frustrated maker of things.



What's driving evolution?

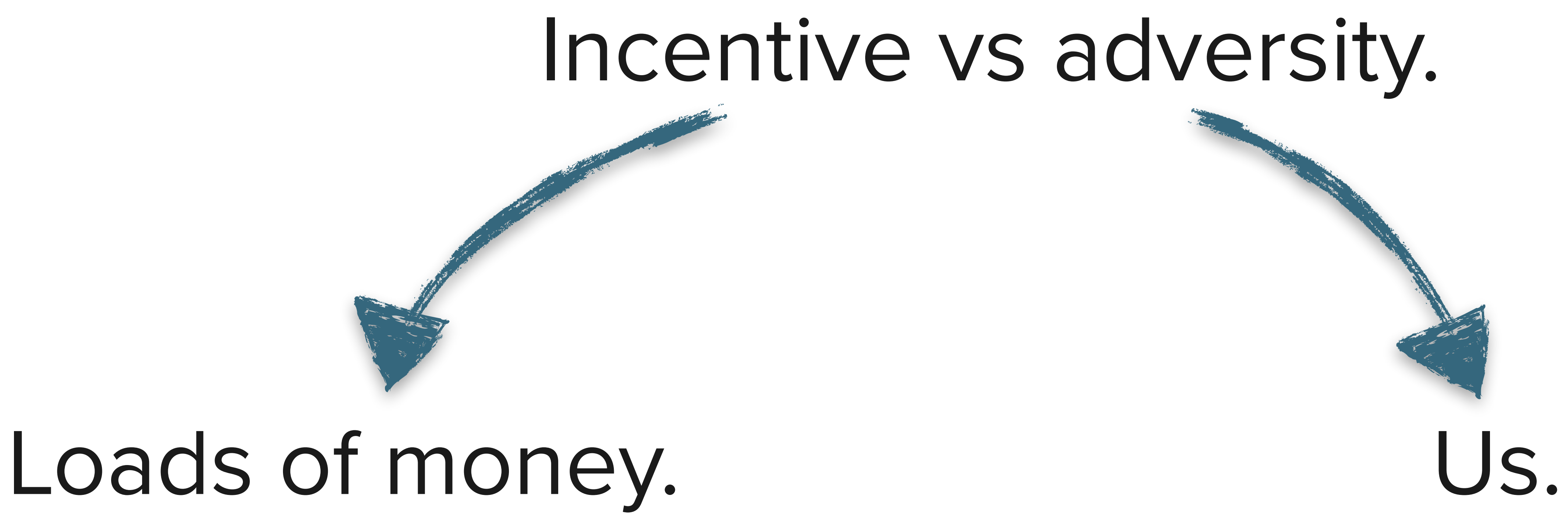
How has automation evolved?

Where do we go from here?

What's driving evolution?

Incentive vs adversity.

What's driving evolution?

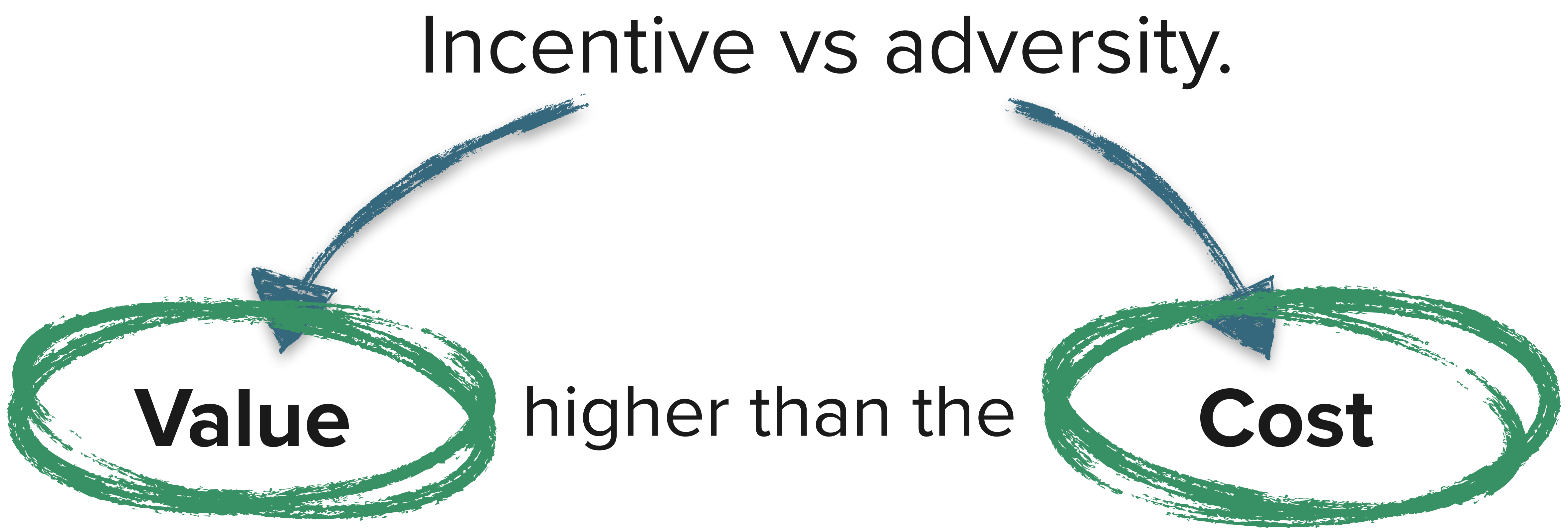


Incentive vs adversity.

Loads of money.

Us.

What's driving evolution?



Incentive vs adversity.

Value higher than the **Cost**

Case study: credential stuffing.

What does it take?

1. Credentials

Total: $0

Case study: credential stuffing.

What does it take?

1. Credentials
2. An account checker

Total: $0 + $0

Case study: credential stuffing.

What does it take?

1. Credentials
2. An account checker
3. Proxies

Total: $0 + $0 + $.0005

Case study: credential stuffing.

What does it take?

1. Credentials
2. An account checker
3. Proxies
4. CAPTCHA bypasses

Total: $0 + $0 + $.0005 + $.001

Case study: credential stuffing.

What does it take?

Total: less than $^2/_{10}$ of one US penny per tested credential.

The break-even rate for accounts worth $1 is 0.2%

Accounts are regularly worth $3 - >$100

At Shape, we saw success rates around 2%

What's driving evolution?

How has automation evolved?

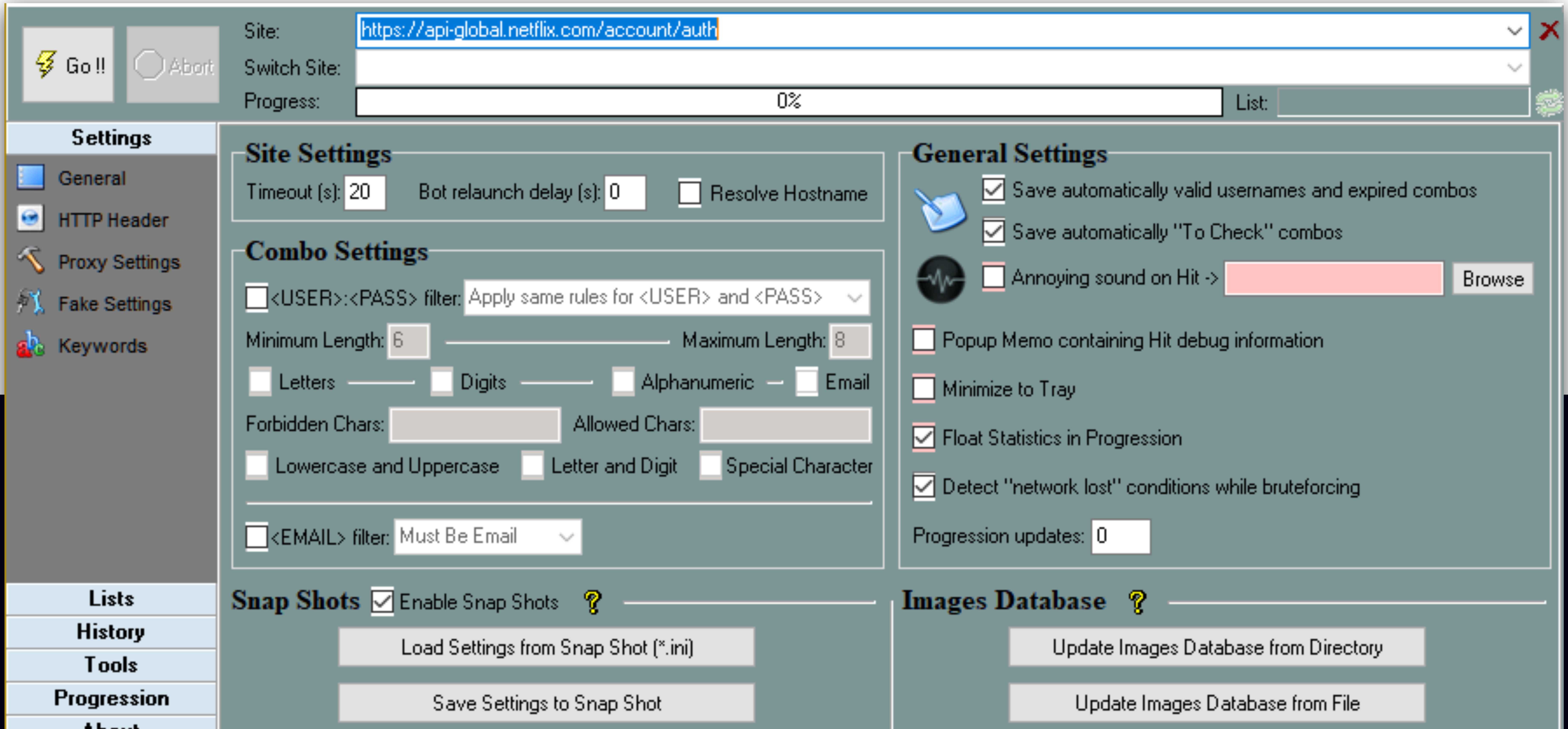
Where do we go from here?

Generation 0: Basic HTTP requests with common tools

```
$
```

SentryMBA

- Performs basic HTTP requests.
- Extensible and highly configurable.
- Tailored towards specific attack use cases.


Go !!
Abort
Settings
General
HTTP Header
Proxy Settings
Fake Settings
Keywords
Lists
History
Tools
Progression
Browse
Load Settings from Snap Shot (*.ini)
Save Settings to Snap Shot
Update Images Database from Directory
Update Images Database from File

Site: https://api-global.netflix.com/account/auth

Switch Site:

Progress: 0%

List:

Site Settings

Timeout (s): 20 Bot relaunch delay (s): 0 □ Resolve Hostname

Combo Settings

□ <USER>:<PASS> filter: Apply same rules for <USER> and <PASS>

Minimum Length: 6 Maximum Length: 8

□ Letters □ Digits □ Alphanumeric □ Email

Forbidden Chars: Allowed Chars:

□ Lowercase and Uppercase □ Letter and Digit □ Special Character

□ <EMAIL> filter: Must Be Email

General Settings

☑ Save automatically valid usernames and expired combos

☑ Save automatically "To Check" combos

□ Annoying sound on Hit ->

□ Popup Memo containing Hit debug information

□ Minimize to Tray

☑ Float Statistics in Progression

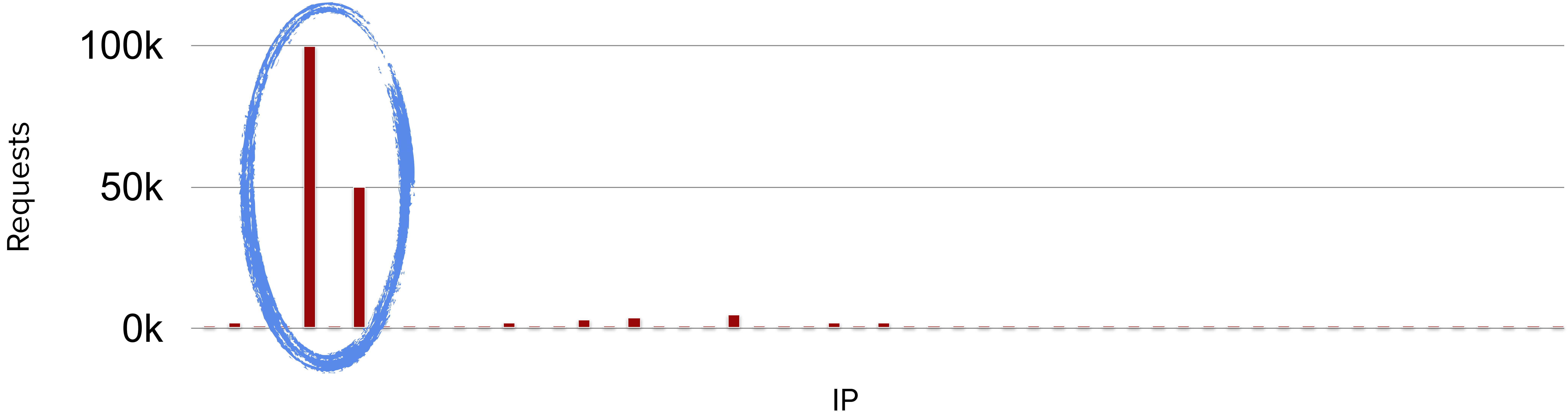
☑ Detect "network lost" conditions while bruteforcing

Progression updates: 0

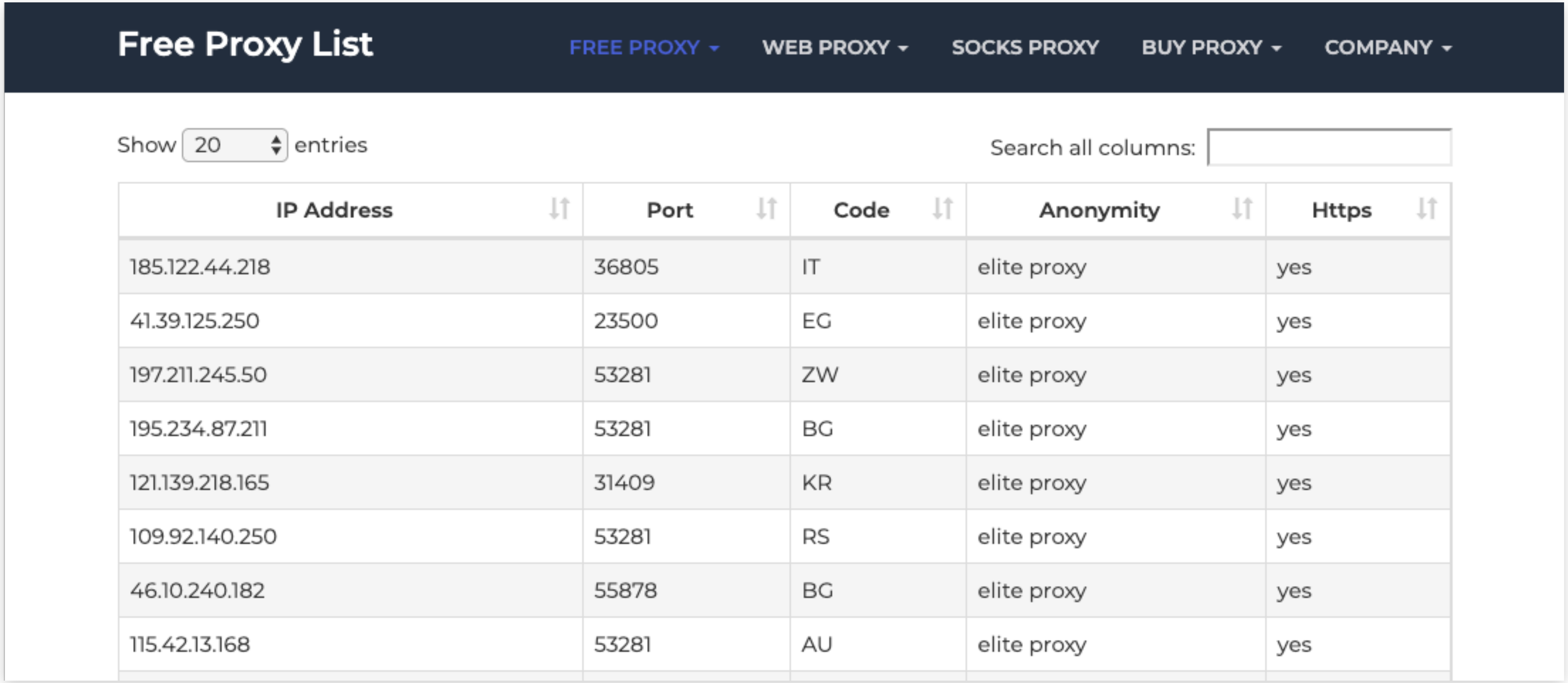
Snap Shots ☑ Enable Snap Shots ?

Images Database ?

Early defense: IP Rate limiting.

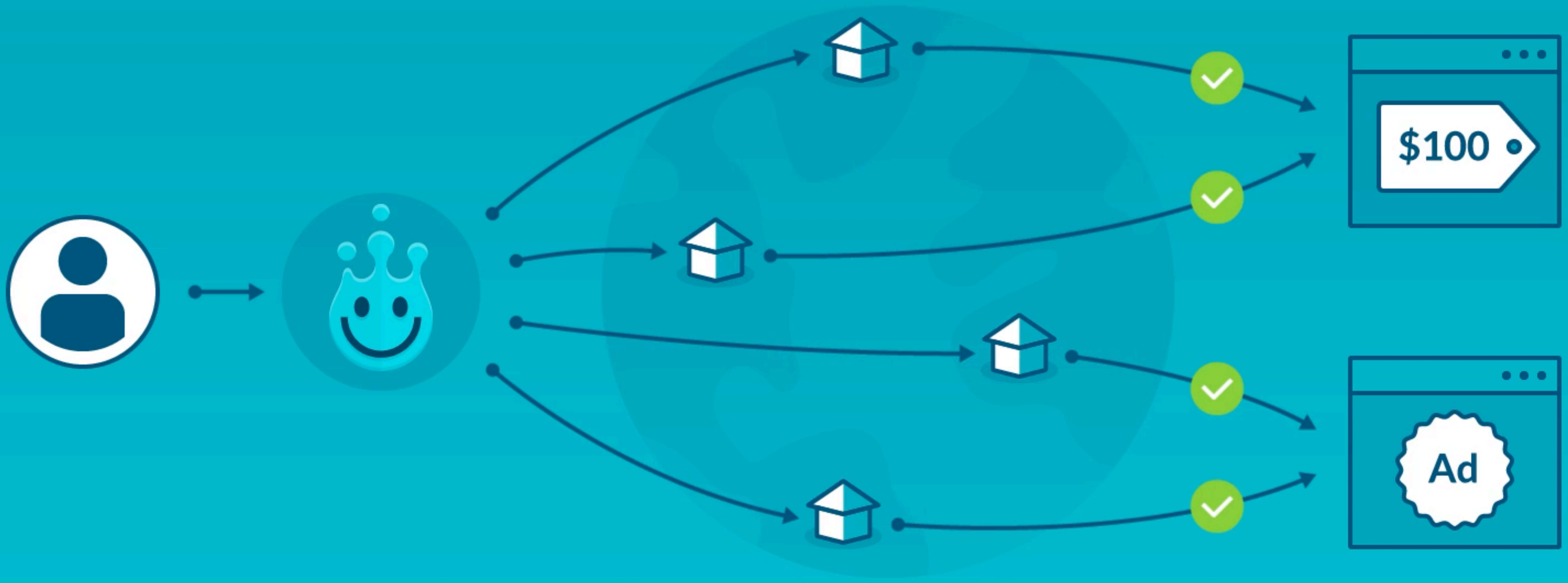


Iteration 1: Rotate through proxies



IP Address	Port	Code	Anonymity	Https
185.122.44.218	36805	IT	elite proxy	yes
41.39.125.250	23500	EG	elite proxy	yes
197.211.245.50	53281	ZW	elite proxy	yes
195.234.87.211	53281	BG	elite proxy	yes
121.139.218.165	31409	KR	elite proxy	yes
109.92.140.250	53281	RS	elite proxy	yes
46.10.240.182	55878	BG	elite proxy	yes
115.42.13.168	53281	AU	elite proxy	yes

Luminati — Residential proxy network



Every country and every city in the world

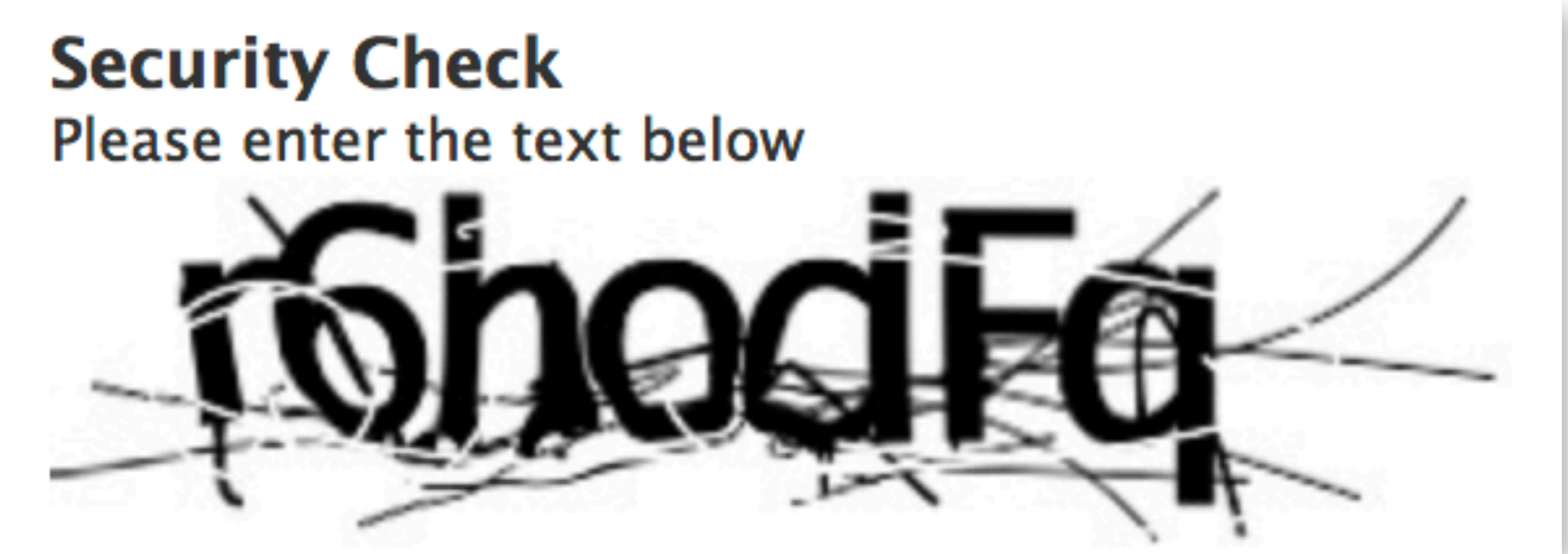
hola!VPN

Unblock any website

Used by over **190 million** people worldwide

Click to install Hola VPN
Start ▶

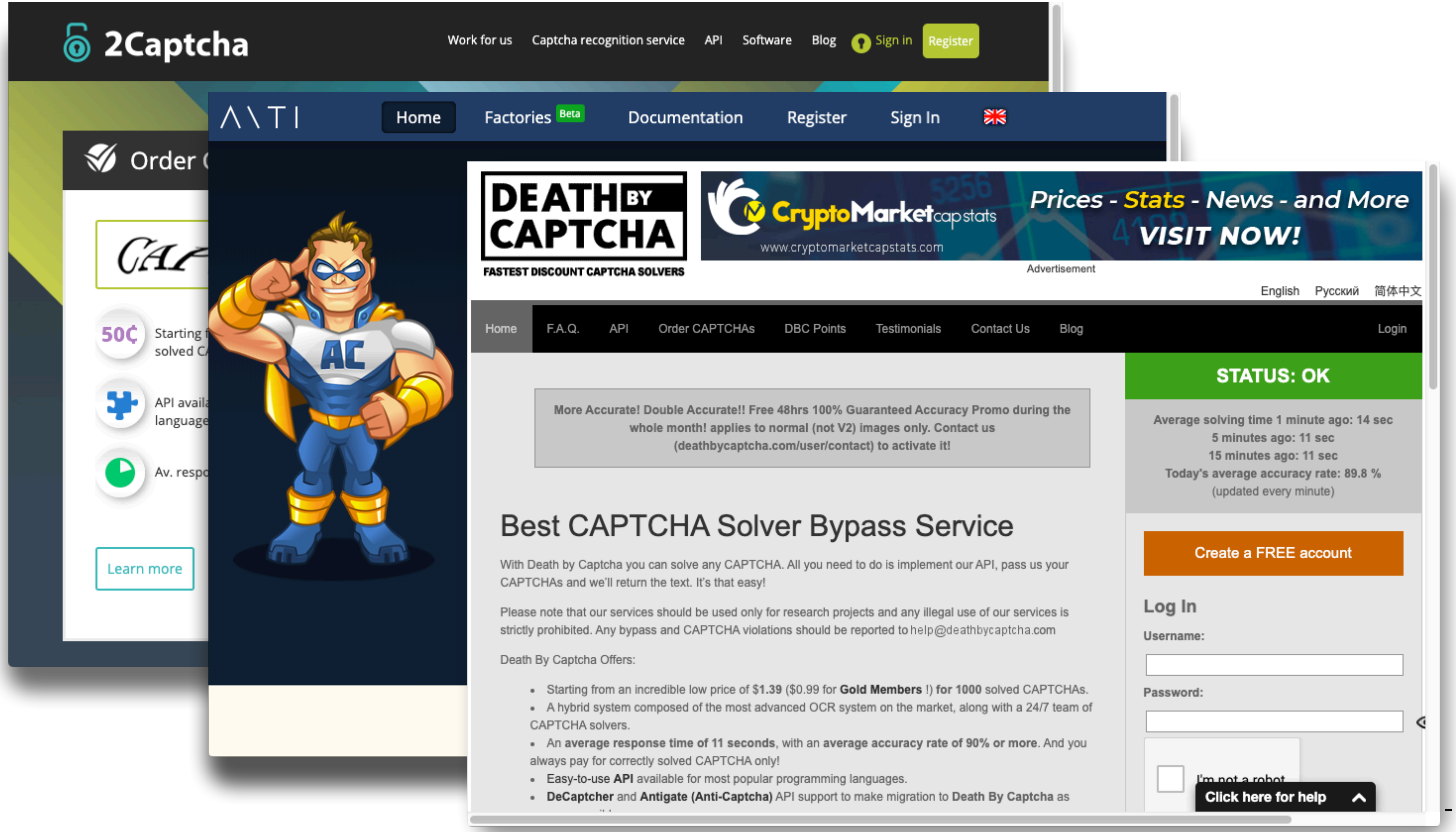
Defense: Text-based CAPTCHAs



Security Check

Please enter the text below

Iteration 2: CAPTCHA Solvers



More Accurate! Double Accurate!! Free 48hrs 100% Guaranteed Accuracy Promo during the whole month! applies to normal (not V2) images only. Contact us (deathbycaptcha.com/user/contact) to activate it!

STATUS: OK

Average solving time 1 minute ago: 14 sec
5 minutes ago: 11 sec
15 minutes ago: 11 sec
Today's average accuracy rate: 89.8 %
(updated every minute)

Best CAPTCHA Solver Bypass Service

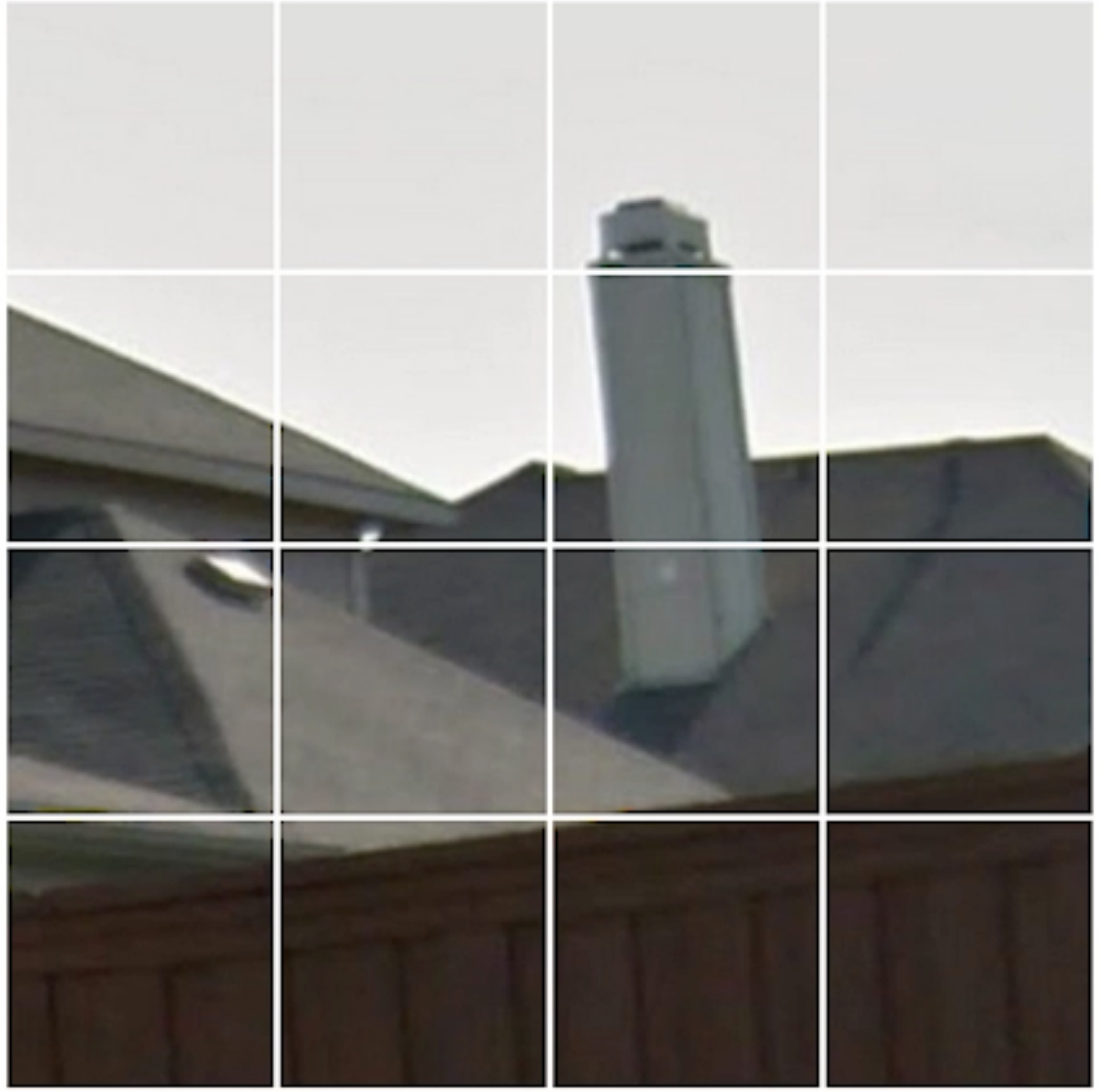
With Death by Captcha you can solve any CAPTCHA. All you need to do is implement our API, pass us your CAPTCHAs and we'll return the text. It's that easy!

Please note that our services should be used only for research projects and any illegal use of our services is strictly prohibited. Any bypass and CAPTCHA violations should be reported to help@deathbycaptcha.com

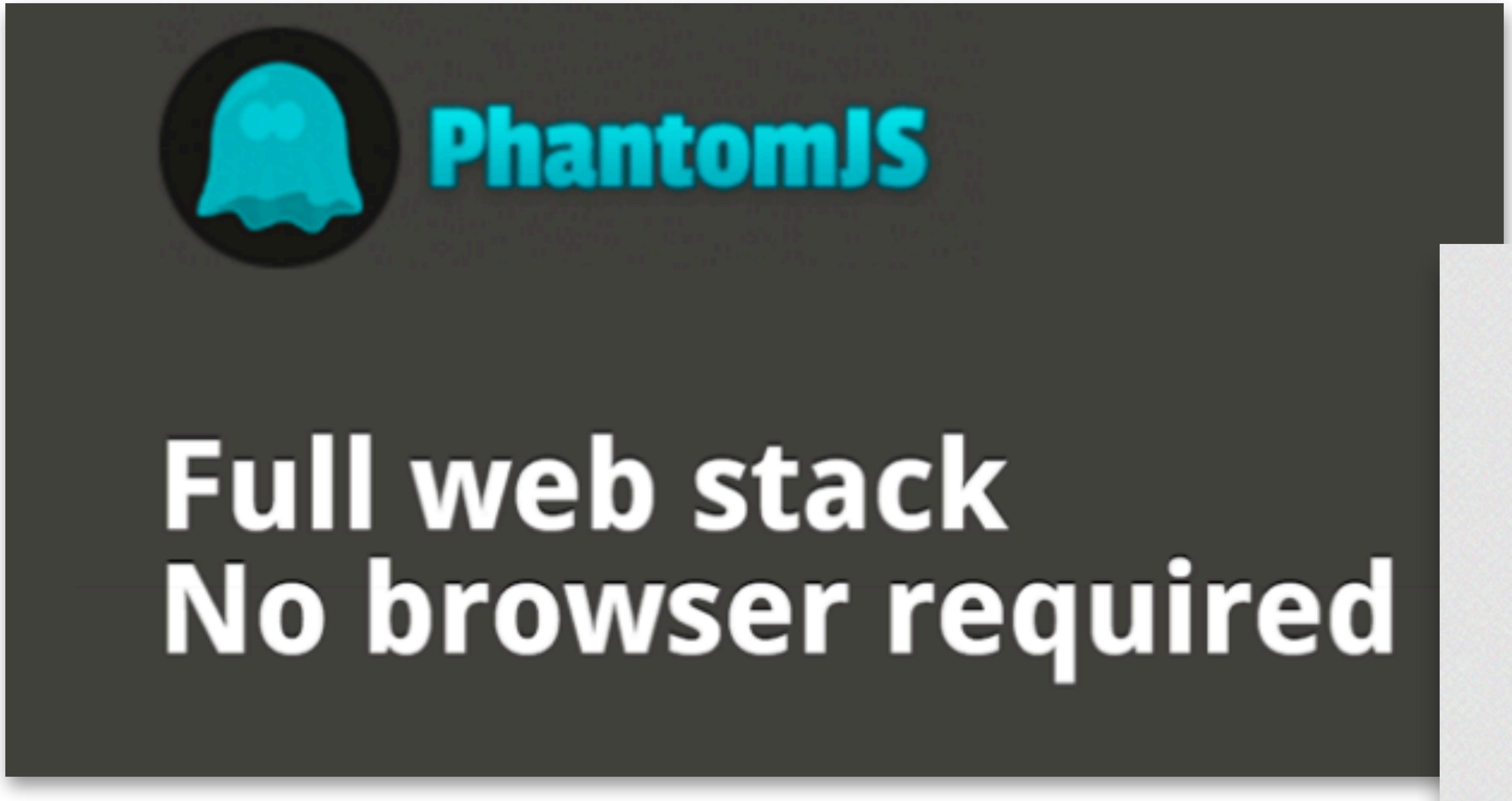
Death By Captcha Offers:

- Starting from an incredible low price of $1.39 ($0.99 for **Gold Members** !) **for 1000** solved CAPTCHAs.
- A hybrid system composed of the most advanced OCR system on the market, along with a 24/7 team of CAPTCHA solvers.
- An **average response time of 11 seconds**, with an **average accuracy rate of 90% or more**. And you always pay for correctly solved CAPTCHA only!
- Easy-to-use **API** available for most popular programming languages.
- **DeCaptcher** and **Antigate (Anti-Captcha)** API support to make migration to **Death By Captcha** as

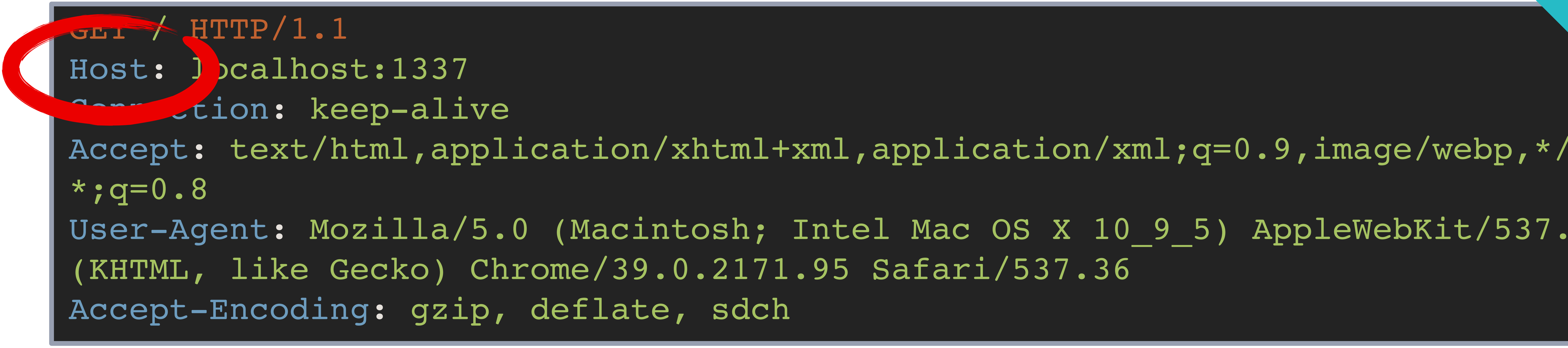
Defense: Dynamic sites and JavaScript heavy defenses.



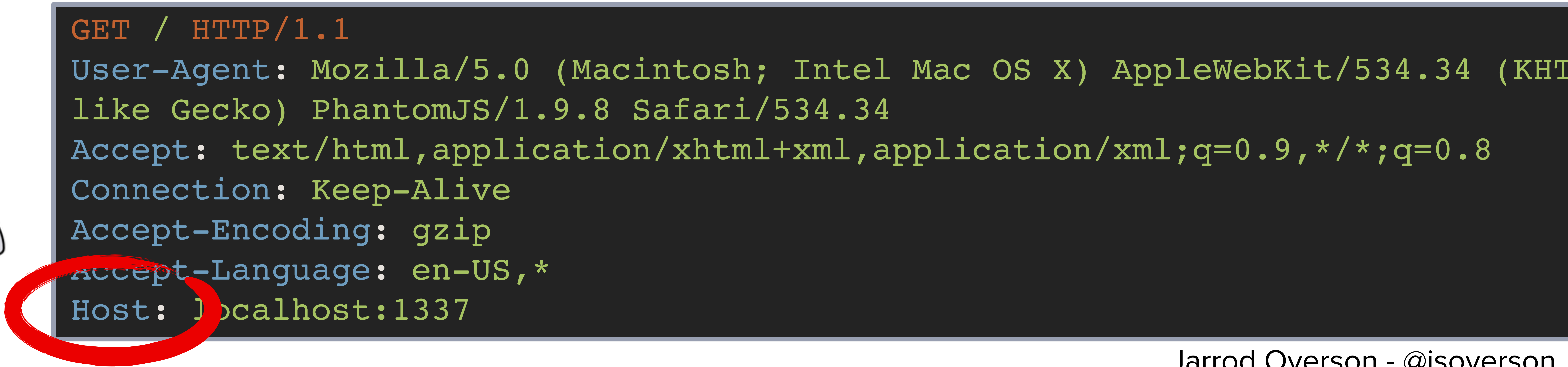
Iteration 3: Scriptable WebViews



Defense: Header Fingerprinting & Environment Checks



```
GET / HTTP/1.1
Host: localhost:1337
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/
*;q=0.8
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.
(KHTML, like Gecko) Chrome/39.0.2171.95 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
```



```
GET / HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X) AppleWebKit/534.34 (KHT
like Gecko) PhantomJS/1.9.8 Safari/534.34
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Connection: Keep-Alive
Accept-Encoding: gzip
Accept-Language: en-US,*
Host: localhost:1337
```

Modern Era

Iteration 4: Scriptable Consumer Browsers

Playwright & Puppeteer

Playwright and puppeteer are automation drivers for modern browsers.

Defense: Browser Fingerprinting

Browser Fingerprinting

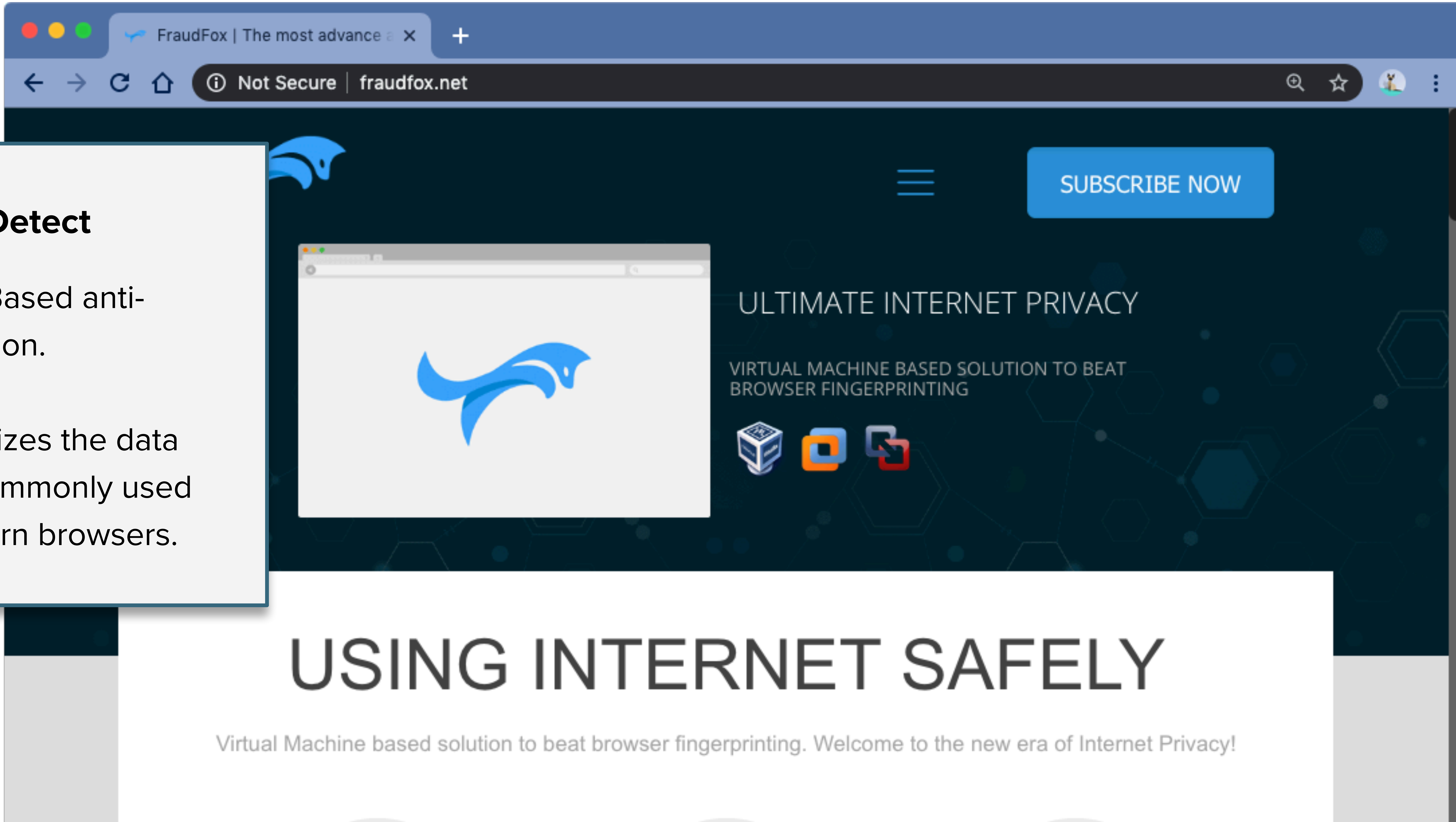
Collecting data points like screen size, fonts, and plugins can produce an effective fingerprint.

Iteration 5: Randomizing Fingerprint Data Sources

FraudFox & AntiDetect

FraudFox is a VM-Based anti-fingerprinting solution.

AntiDetect randomizes the data sources that are commonly used to fingerprint modern browsers.



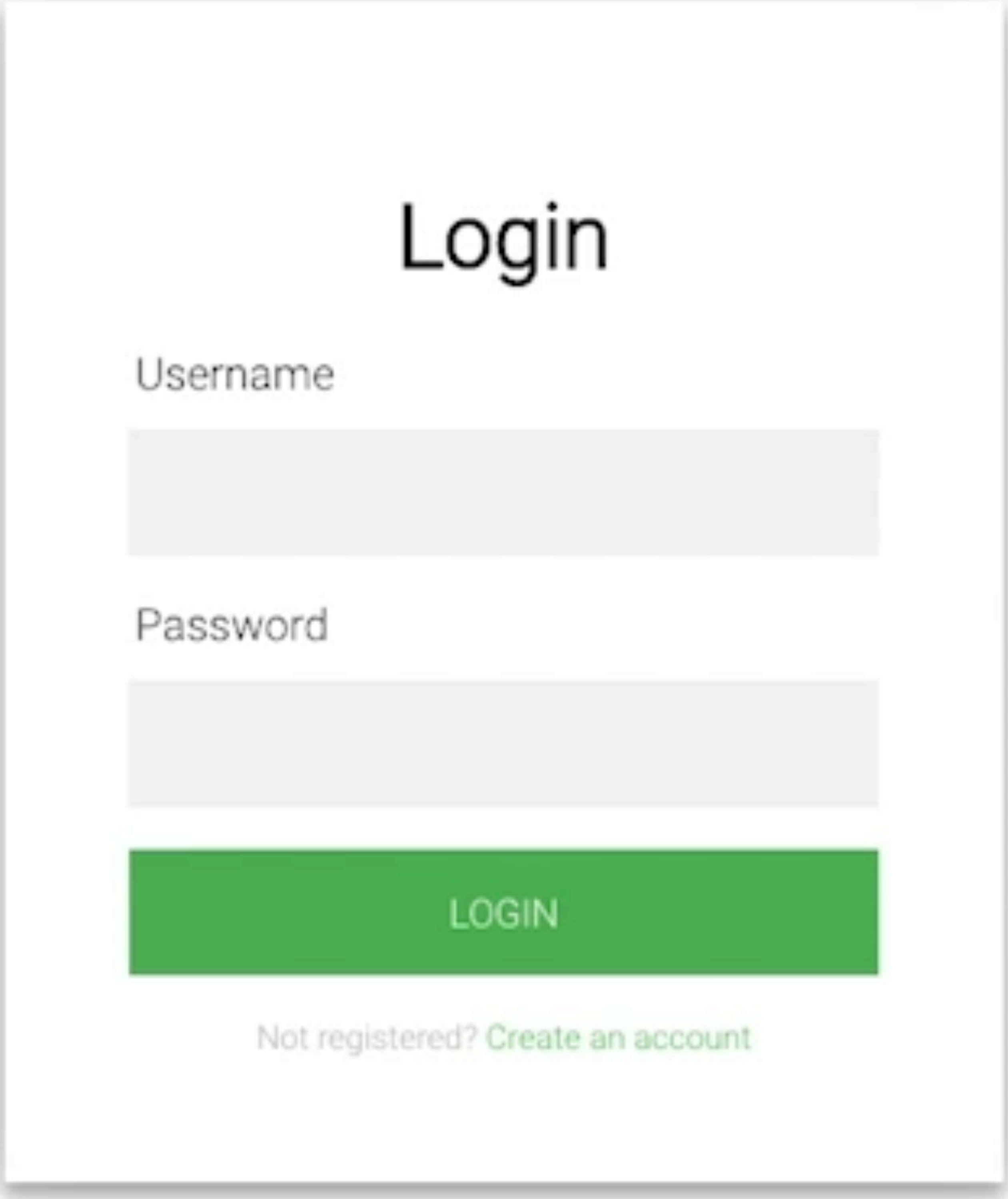
ULTIMATE INTERNET PRIVACY

VIRTUAL MACHINE BASED SOLUTION TO BEAT BROWSER FINGERPRINTING

USING INTERNET SAFELY

Virtual Machine based solution to beat browser fingerprinting. Welcome to the new era of Internet Privacy!

Defense: Behavior Analysis for Negative Traits



Login

Username

Password

LOGIN

Not registered? Create an account

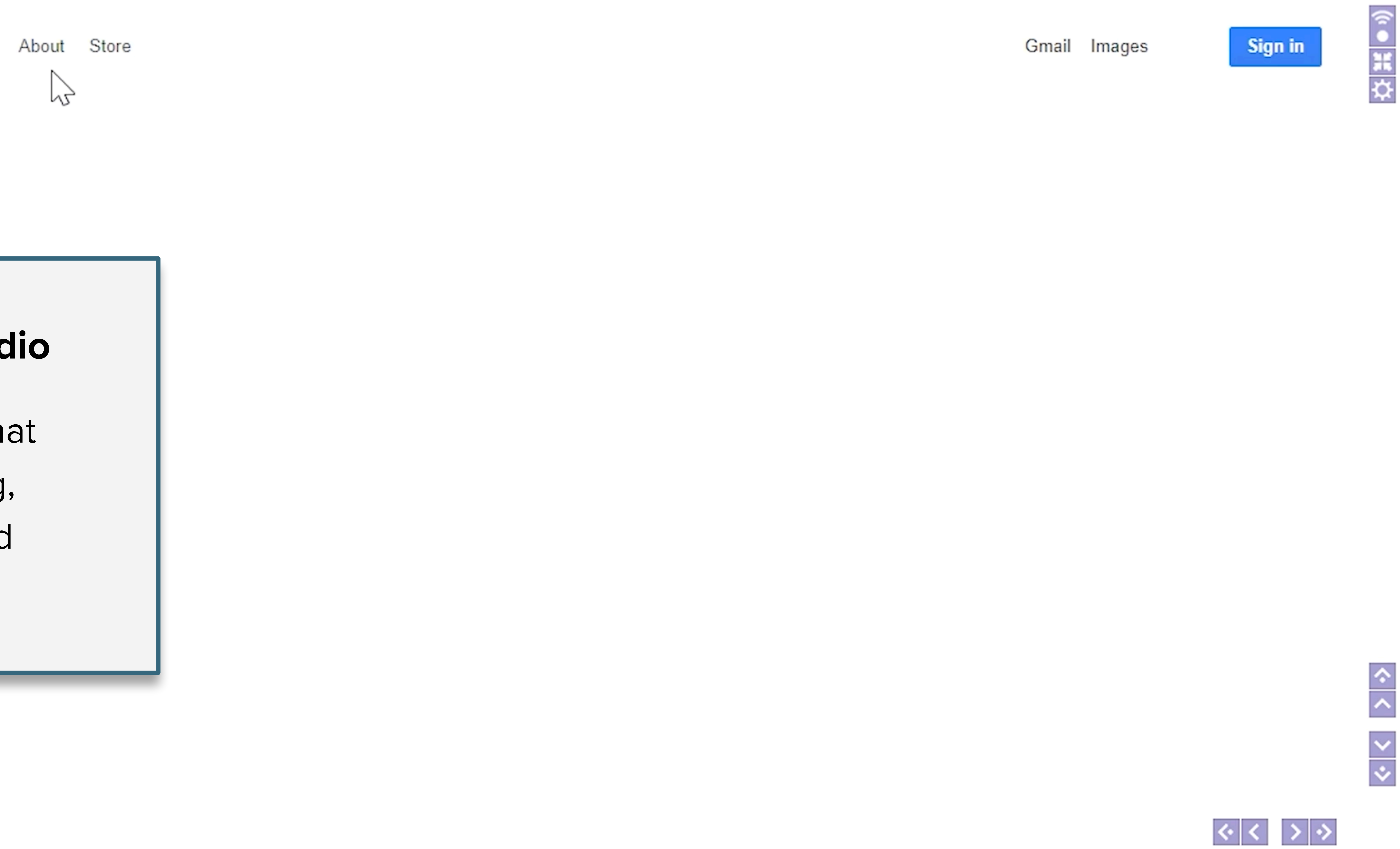
Behavior Analysis

Bots always click in the same spot, humans don't.

Bots type with lightning speed, humans don't.

Basic behavior analysis catches all simple bots.

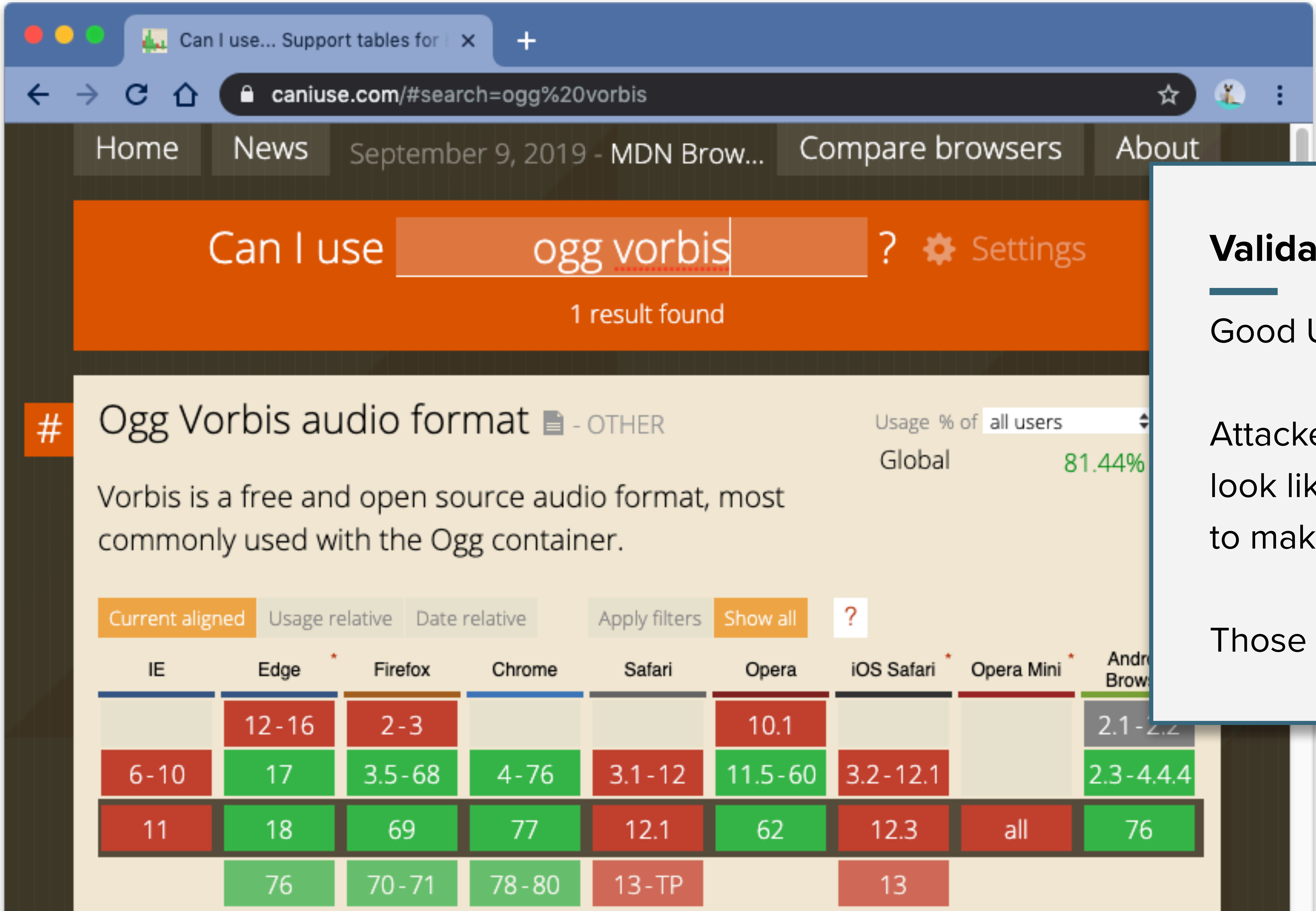
Iteration 6: Human Behavior Emulation



Browser Automation Studio

BAS is an automation tool that combines CAPTCHA solving, proxy rotation, and emulated human behavior.

Defense: Browser Consistency Checks



Can I use... Support tables for

caniuse.com/#search=ogg%20vorbis

Home | News | September 9, 2019 - MDN Brow... | Compare browsers | About

Can I use ogg vorbis ? Settings

1 result found

Ogg Vorbis audio format - OTHER

Usage % of all users

Global 81.44%

Vorbis is a free and open source audio format, most commonly used with the Ogg container.

Current aligned | Usage relative | Date relative | Apply filters | Show all | ?

IE	Edge *	Firefox	Chrome	Safari	Opera	iOS Safari *	Opera Mini *	Andr Brows
	12-16	2-3			10.1			2.1-2.2
6-10	17	3.5-68	4-76	3.1-12	11.5-60	3.2-12.1		2.3-4.4.4
11	18	69	77	12.1	62	12.3	all	76
	76	70-71	78-80	13-TP		13		

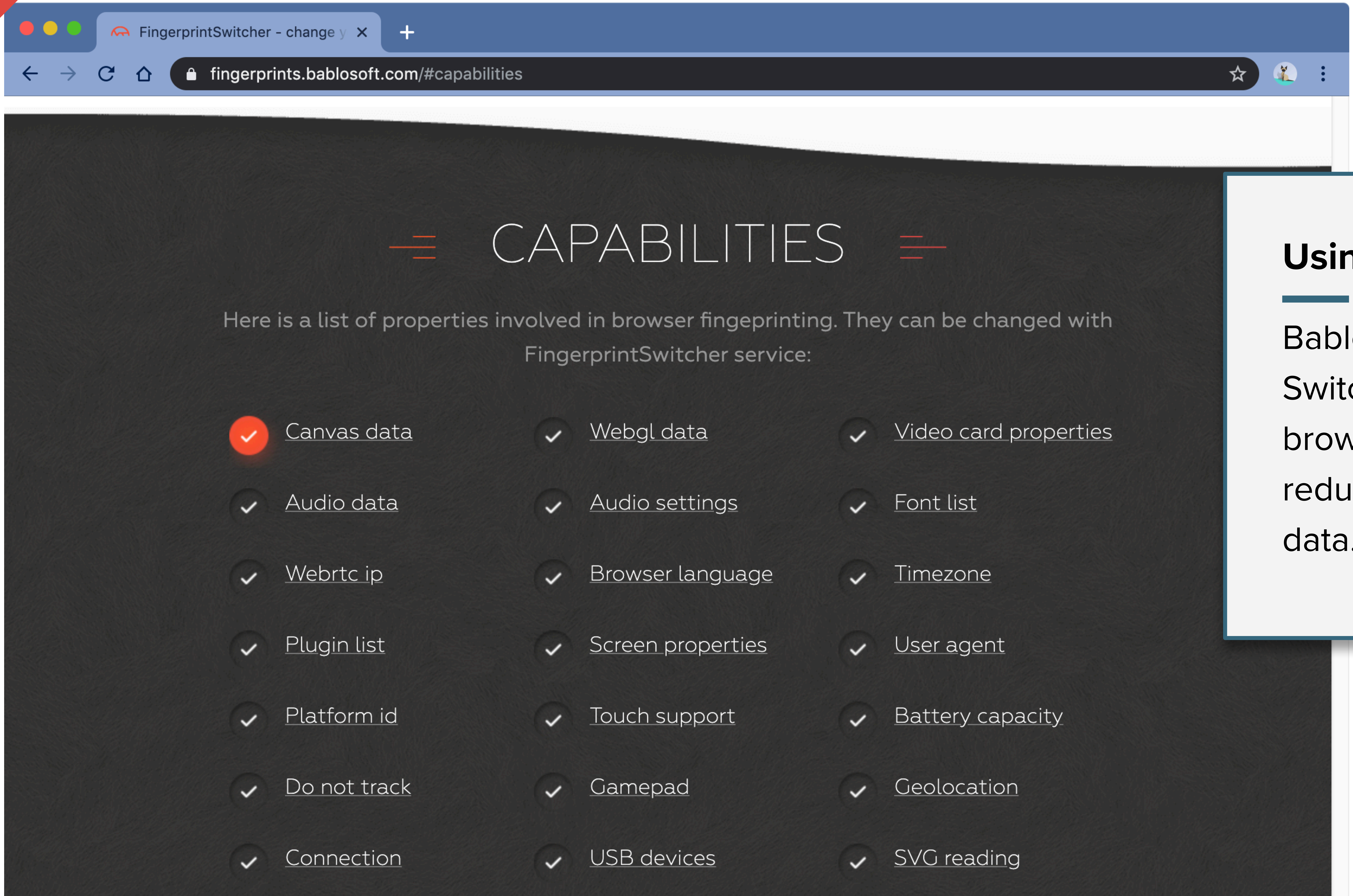
Validating Fingerprints

Good Users don't lie much.

Attackers need a few clients to look like thousands and have to lie to make it convincing.

Those lies add up.

Iteration 7: Use real device data


FingerprintSwitcher - change y
fingerprints.bablosoft.com/#capabilities

CAPABILITIES

Here is a list of properties involved in browser fingerprinting. They can be changed with FingerprintSwitcher service:

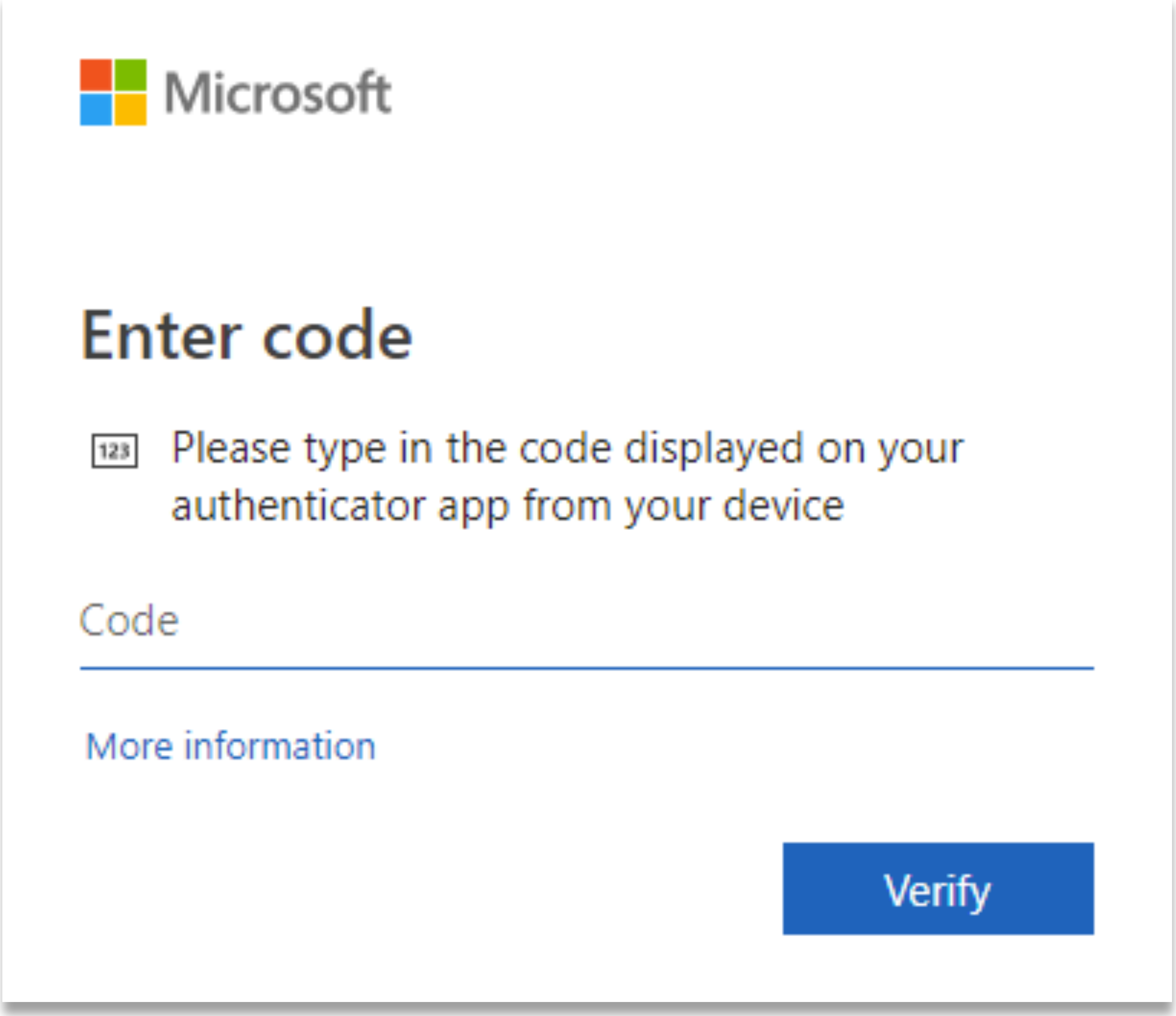
- ✓ Canvas data
- ✓ Audio data
- ✓ Webrtc ip
- ✓ Plugin list
- ✓ Platform id
- ✓ Do not track
- ✓ Connection
- ✓ Webgl data
- ✓ Audio settings
- ✓ Browser language
- ✓ Screen properties
- ✓ Touch support
- ✓ Gamepad
- ✓ USB devices
- ✓ Video card properties
- ✓ Font list
- ✓ Timezone
- ✓ User agent
- ✓ Battery capacity
- ✓ Geolocation
- ✓ SVG reading

Using Real Values

Bablosoft's Fingerprint Switcher gives you real browser fingerprints, reducing the lies in your data.

Jarrod Overson - @jsoverson

Defense: MFA and risk scoring

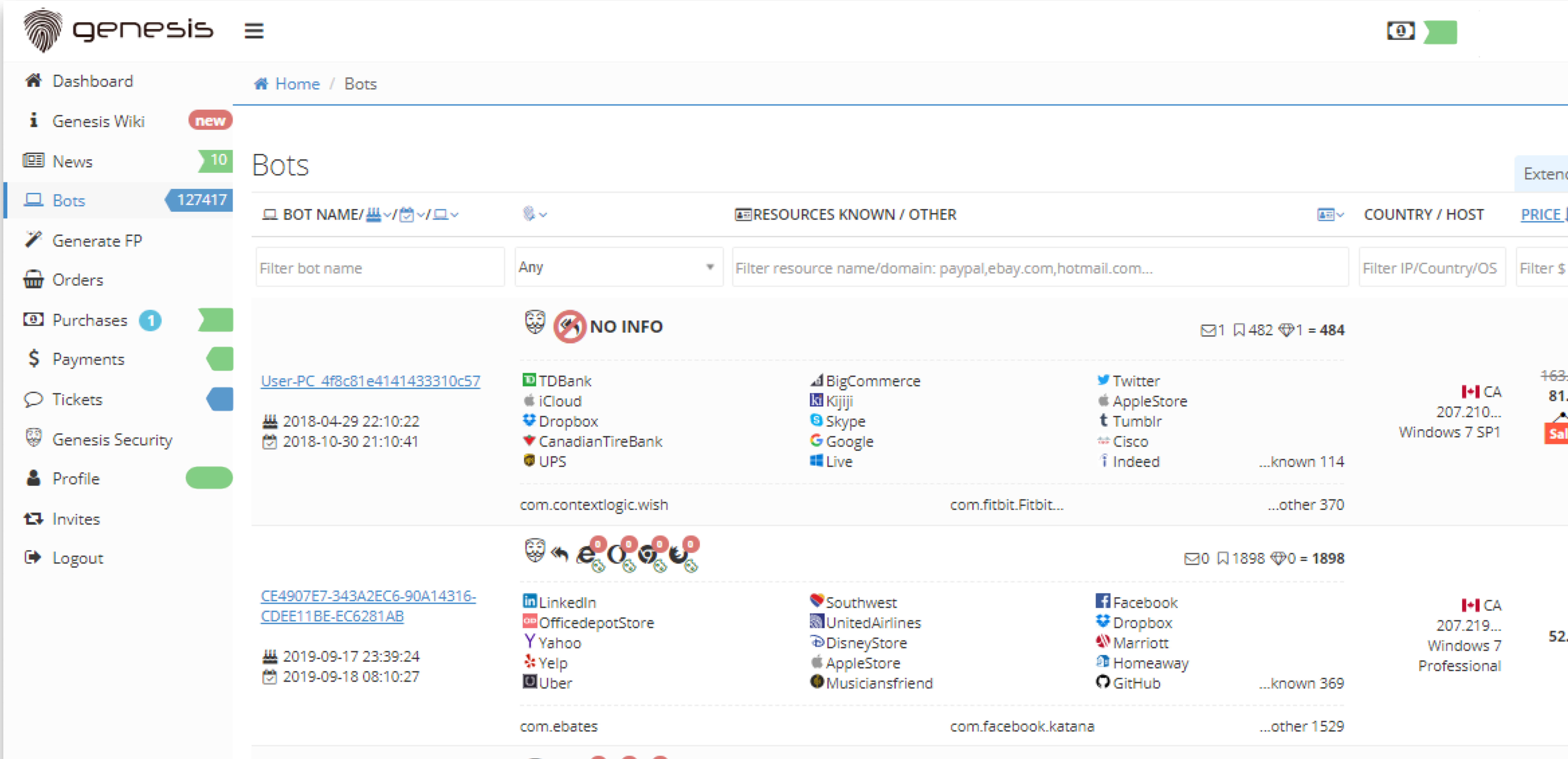


Microsoft

Enter code

Please type in the code displayed on your authenticator app from your device

Iteration 8: Hijack sessions and user computers.



Bots

BOT NAME/ / /		RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...	Filter IP/Country/OS	Filter $
User-PC_4f8c81e4141433310c57 2018-04-29 22:10:22 2018-10-30 21:10:41	NO INFO	1 482 1 = 484 TDBank, iCloud, Dropbox, CanadianTireBank, UPS, BigCommerce, Kijiji, Skype, Google, Live, Twitter, AppleStore, Tumblr, Cisco, Indeed ...known 114 com.contextlogic.wish com.fitbit.Fitbit... ...other 370	CA 207.210... Windows 7 SP1	~~163.~~ 81. Sal
CE4907E7-343A2EC6-90A14316-CDEE11BE-EC6281AB 2019-09-17 23:39:24 2019-09-18 08:10:27	0 0 0 0	0 1898 0 = 1898 LinkedIn, OfficedepotStore, Yahoo, Yelp, Uber, Southwest, UnitedAirlines, DisneyStore, AppleStore, Musiciansfriend, Facebook, Dropbox, Marriott, Homeaway, GitHub ...known 369 com.ebates com.facebook.katana ...other 1529	CA 207.219... Windows 7 Professional	52.

What's driving evolution?

How has automation evolved?

Where do we go from here?

As a company: bring security & fraud into UX decisions

The best defenses are internal.

Limit, delay, and vary feedback in the UX.

Advanced adversaries are developers. Don't aid them with helpful messages.

Reduce your surface area

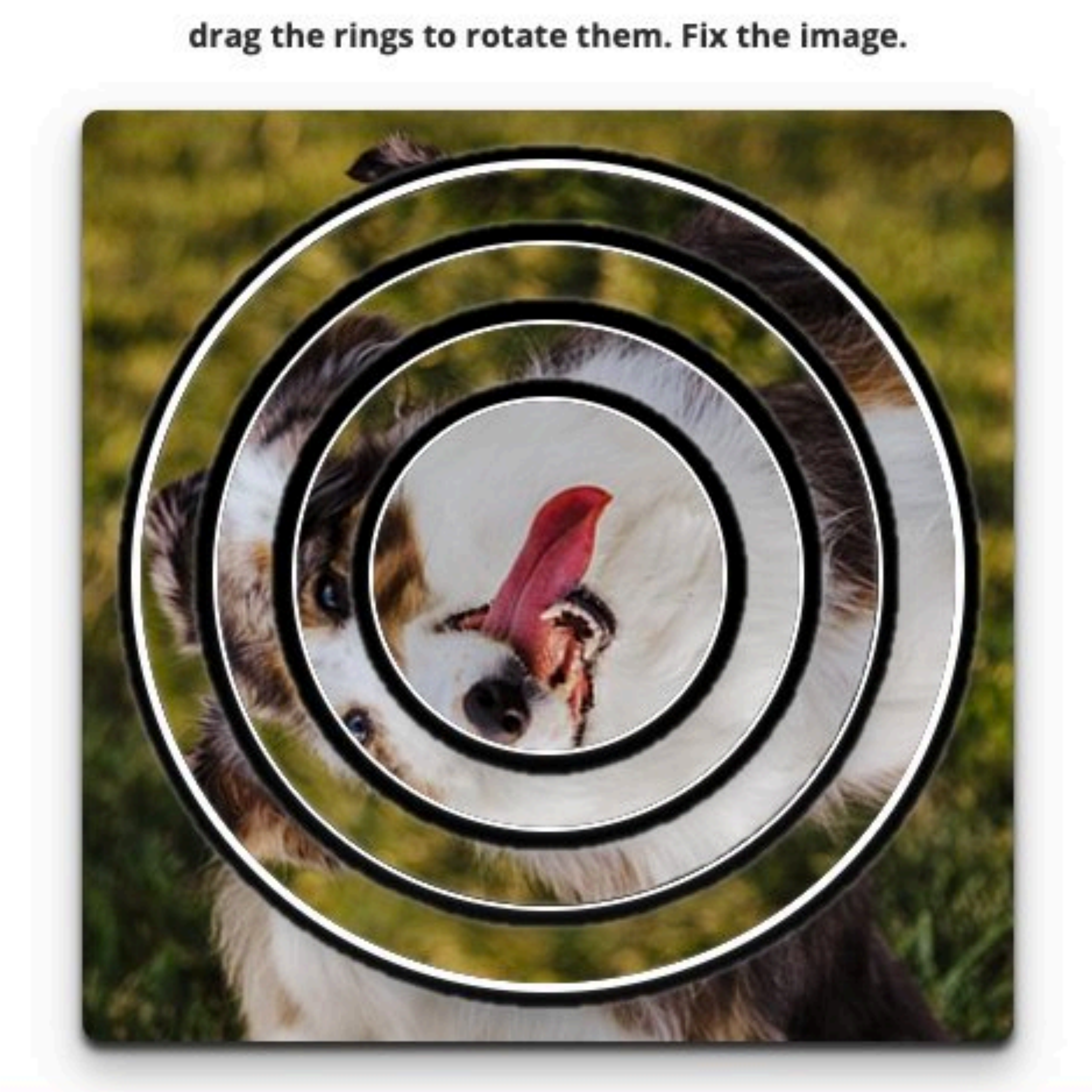
Funnel risk into bottlenecks to simplify modeling and response.

Build a system of dials and levers

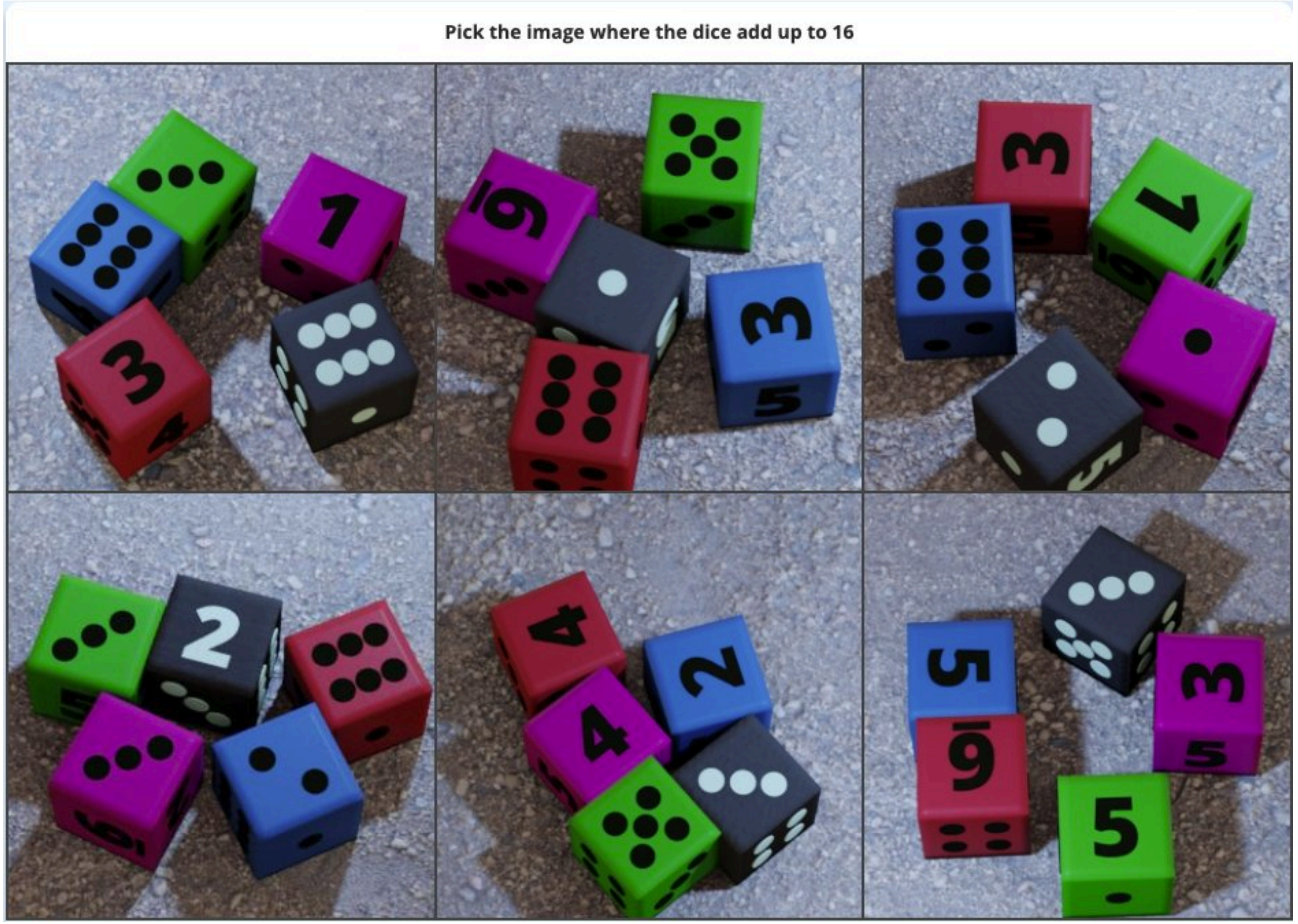
Adversaries iterate quickly and defenses need to change rapidly. Build for speed.

Stop using CAPTCHAs

They are trivially bypassed and are more frustrating to users than adversaries.



drag the rings to rotate them. Fix the image.



Pick the image where the dice add up to 16

Thank you!

@jsoverson on twitter, medium

Visit vino.dev to learn about what I'm up to next.