



A Guide To FaudFox And Anti-Fingerprinting

Introduction

Lets start from browser fingerprint which is exactly how you get declines! so what is browser finger print ? anything from browser can help store / shop / payment processor to detect you are same person who tried to card them.

for understanding what they exactly can use against you simply head to [Here](#)

you will see different fields here .

User-agent :

which will exactly tell them your browser / OS / and exact version of them

HTTP_ACCEPT Headers :

the headers your browser accept just read HTTP RFC to understand more

Browser Plugin Details :

plugins loaded on your browser which can be your player / reader / anything can be loaded inside browser

Time Zone :

your current system time zone

Screen Size and Color Depth :

very interesting one will detect your screen size from size of your browser and that's why you should never change your tor window size

System Fonts :

fonts you've installed they detect it by flash plugin

Are Cookies Enabled :

does your browser accept cookie ? cookies can be very unique identification and you could've detected with this very easy

Limited Supercookie Test :

far more than cookies DOM and local storage in simple word more permanent cookies

Now head to whoer.net and click on extended version , again you will see same things with some more fields like DNS, ip range , JAVA, JavaScript, WebRTC, Flash, ActiveX and again screen , language and time zone.

As you may don't know all of these can be used as an anti-fraud measurement but how ? every single plugin like flash and java / java-script will lead more programmatically control against clients it means stores can use these tools to detect your real location/IP/DNS which can easily detect you as a carder and decline the order . So can we disable these plugins and we are done ?

NO !

If you disable anything its again very suspicion because you don't like normal customer.

So what is the solution ? the solution is properly spoof your identification to look like real card owner. we always hear stupid and funny things like card-able store not card-able store . there is no such a thing exist we surprised how many people here without any knowledge spread wrong information ! if the website is a online store which accept credit cards it means it can be carded as well if you can't which only means you didn't spoof anything correctly even one mistake in all of anti-fraud measurement can lead to order decline and finally what people call it card-able site is just a site with poor or without anti-fraud system that's all!

next funny thing we hear is changing your hard drive , mac address and hardware related stuff . this is ridiculous as long as you don't install anything which means you only use a browser for communicating with a website there is no way for them to access to such info if they can access to these info everybody else can so you have to put your browsers in trash and millions of dollar spent on browser secure means nothing! so spoofing is important but changing your mac address (while browsing) is meaningless .

Anti-Detect and FraudFox

Anti-Detect and **FraudFox** are both tools for beating browser finger prints

Antidetec current version is 6.3 you can look at their site [Here](http://antidetec.net/)
<http://antidetec.net/>

The latest 6.3 version with many bugfixes, user asked features added. Browser generation extended functions: you can make your FF looks like: ff, chrome, ie, opera, android or macintosh. You can change useragent, OS, language, browser version, platform, flash (version, language, os, fonts, resolution), screen resolution, appname, codename, vendor, product and many other things, you can make thousands of unique browser fingerprints.



One button generator? We have it! After you choose preferred options (random mode also available) you can click only one generate button and software will always generate an unique fingerprint for you.

One button system cleaner? No problem ;) If you dont like to click and click and click ccleaner checkboxes.. well.. we give you lesson how to clean you virtual machine with one button click always.

You can use this software for anonymous registering anywhere and anytime with Firefox. The price of this tool vary between \$500 to \$1200

Fraud Fox current version is 1.5 their legit website here
<http://palantirbhqyufyu.onion>

FFox is the all-in-one tool for user-agent and device spoofing and perhaps the most advanced and fully detailed virtual machine on its class ever created. Never has there been any like it!

Anti-canvassing Options Included

FFox offers customization options on the HTML 5 canvas element so that you have complete control over it.

Prevents IP and DNS leakage

WebRTC and DNS requests are forced to follow VPN or SOCKS protocol. Unencrypted data leakage is well managed.

Truly Anonymous Browsing

More than simple user-agent editing, FFox offers a lot more features such as device details manipulation via the VM console, changing the network footprint via obfuscate button, and a lot more. It is also open to further software installations such as a VPN client within the VM to be able to boost up your anonymous browsing. The price of this software is \$100 per month

So if you read to know you should understand what they are doing they just try to spoof your fingerprint to be same as card holder which one is better ? they are doing the same job bot their license model and some of their features are different you can read their features in their websites and determine which one you prefer.

Do you need these software ? For automating the spoofing process and categorizing your job yes for successful carding NO ! As we already explained if you know how you will get detected you can just find a workaround for it .

Here is the guide for "Stop Firefox leaking data about you" you can read and just do it step by step from [Here](#)

For example you can simply disable WebRTC leak using about:config in Firefox as easy as one click

Conclusion

this was a short introduction about browser fingerprinting and workaround for it. so in conclusion tools like FF and AD are very handy but not required you have to understand how particular targeted store will detect you as carder and find a workaround.