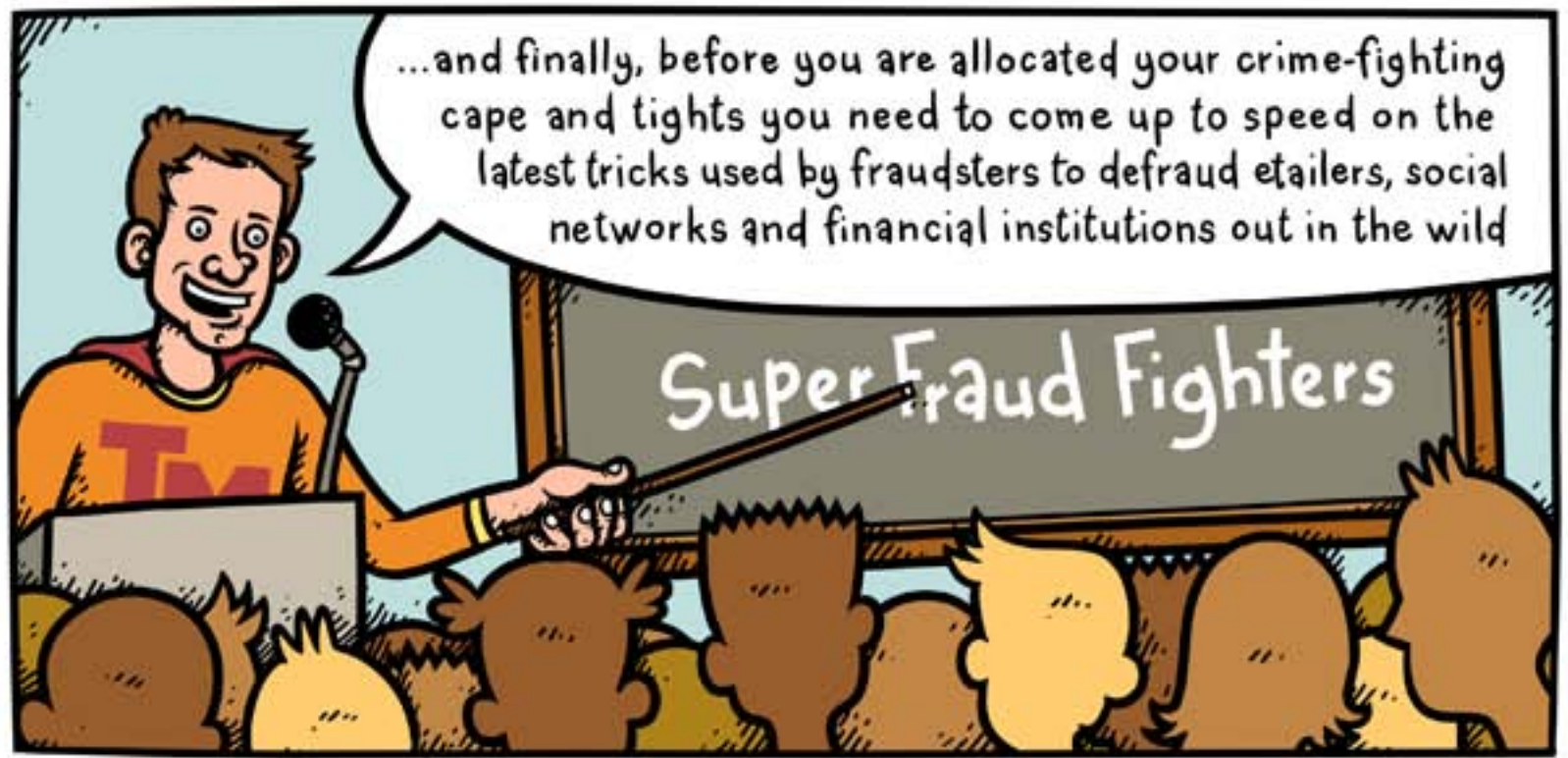


Alisdair of ThreatMetrix Presents
**WEBFRAUD 101:
BOTNETS
and
PROXIES**



The use of proxies used to be reserved for smart guys, but now even dummies can do it at the click of a button at any one of a thousand free websites



Now, not all proxy servers are made equal, so you need to have technology that can accurately tell the difference

1. Corporate Proxies: legitimate companies use special proxies to improve security and performance



2. Anonymizing Proxies: used by fraudsters and the privacy conscious to spoof their IP Address

3. Hidden Proxies: Harder to detect proxies that are used to hide the true IP Geolocation of a fraudster

4. Botnet Proxies: When an unsuspecting user's PC is used by fraudster to originate from a innocent looking IP Address



My IT team says that they already detect proxy IP Addresses, does that mean I'm protected?

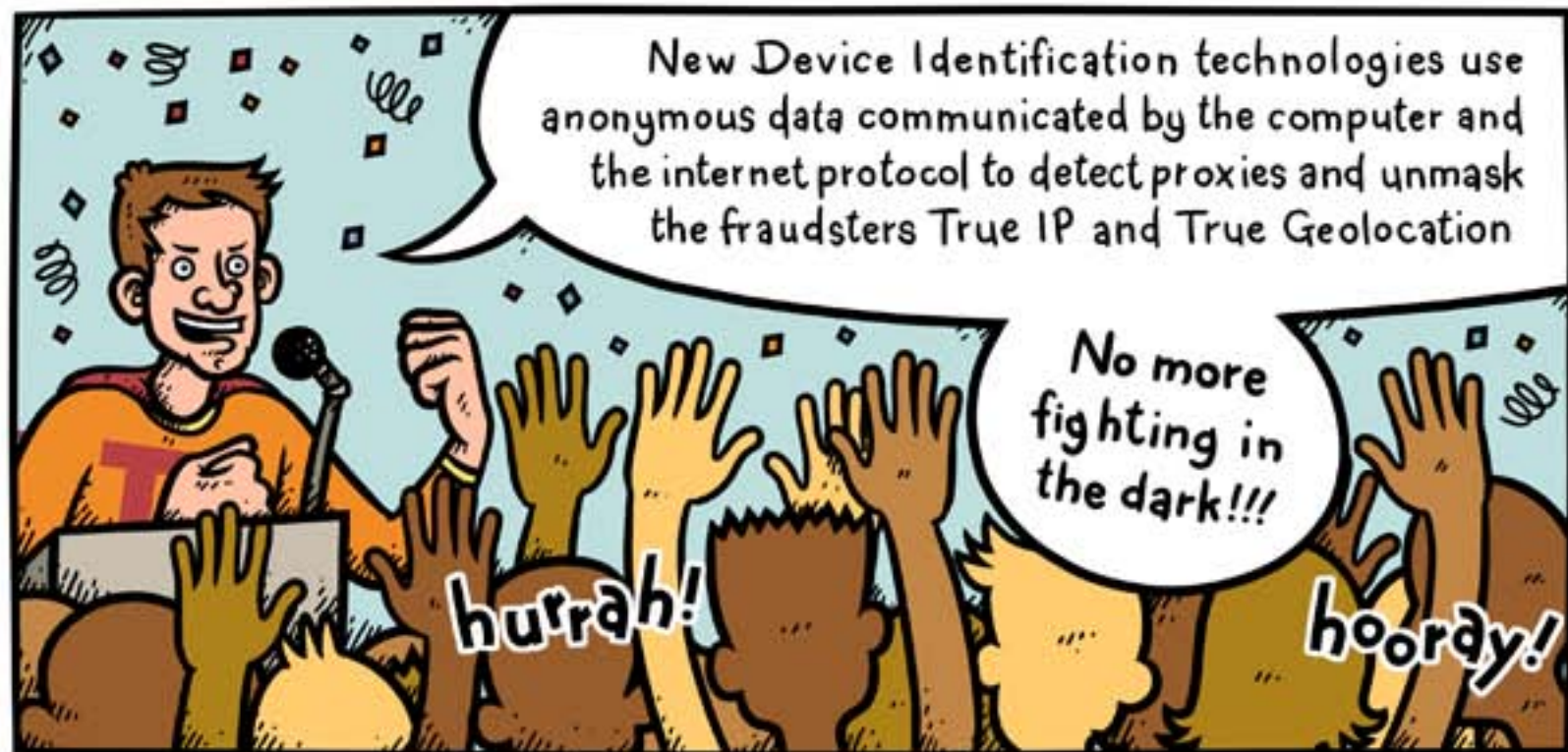


No. Proxy IP Address lists need to be continually updated when new ones are found, and fraudsters are always one step ahead!



IP Addresses are also highly disposable, and the newer hidden proxies and botnet proxies are built to evade scanning....





True IP Detection: detecting differences between the proxy IP Address and the fraudster's real IP Address leaked by the browser



True Location: detecting the fraudsters real location based on device intelligence e.g fonts, browser language and timezone



Packet Signature: automatically detect a proxy based on differences in the browser and packet signature

Tripwire Analysis: detecting when web content has been changed or stripped out

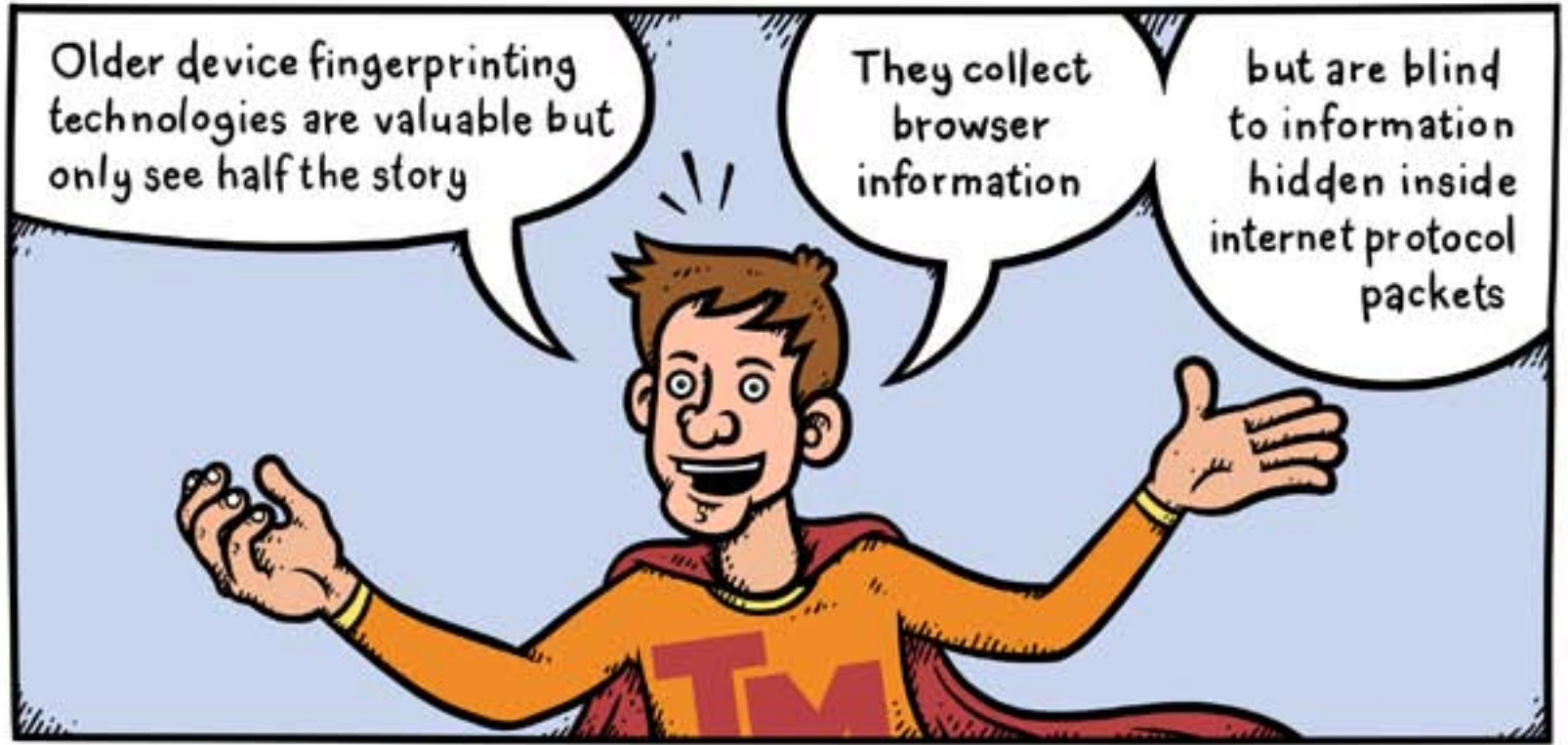
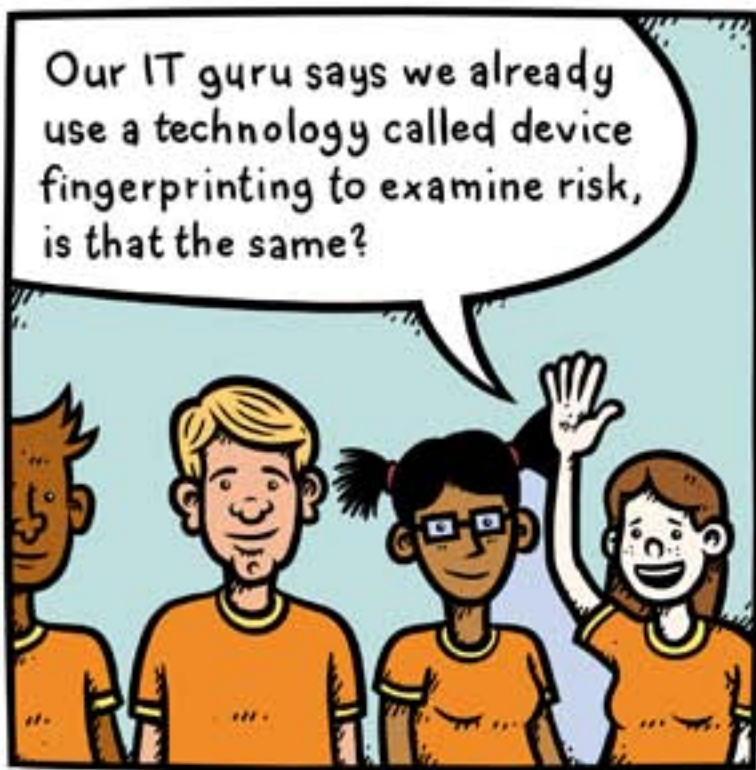
Web Protocol Signature: analyzing web protocol headers (HTTP Protocol) to detect and classify a proxy

Device History: tracing use of multiple IP Addresses and IP Geolocations by the same device over time



HTTP





You think you're seeing the customer's computer but your site could actually be talking to a proxy



What's worse is that proxies can change and manipulate the information communicated by the browser on the fly to hide their tracks



Operating system

Connection Speed

Proxy Type

Device Type

SERVER

