Системы распределения трафика

и новые аспекты в нахождении вредоносного кода

Максим Гончаров

TREND MICRO™ Securing Your Journey to the Cloud

конференция РусКрипто'2011

TDS -> Traffic Direction System

Система распределения трафика

Мотивация

Volume makes money

TDS makes volume

Мотивация

Обьем приносит деньги

TDS приносит объем

Редирект

mod_rewrite

Javascript

Flash

HTTP Header

Click

META

IFrame

HTTP Header

заголовки HTTP

referer

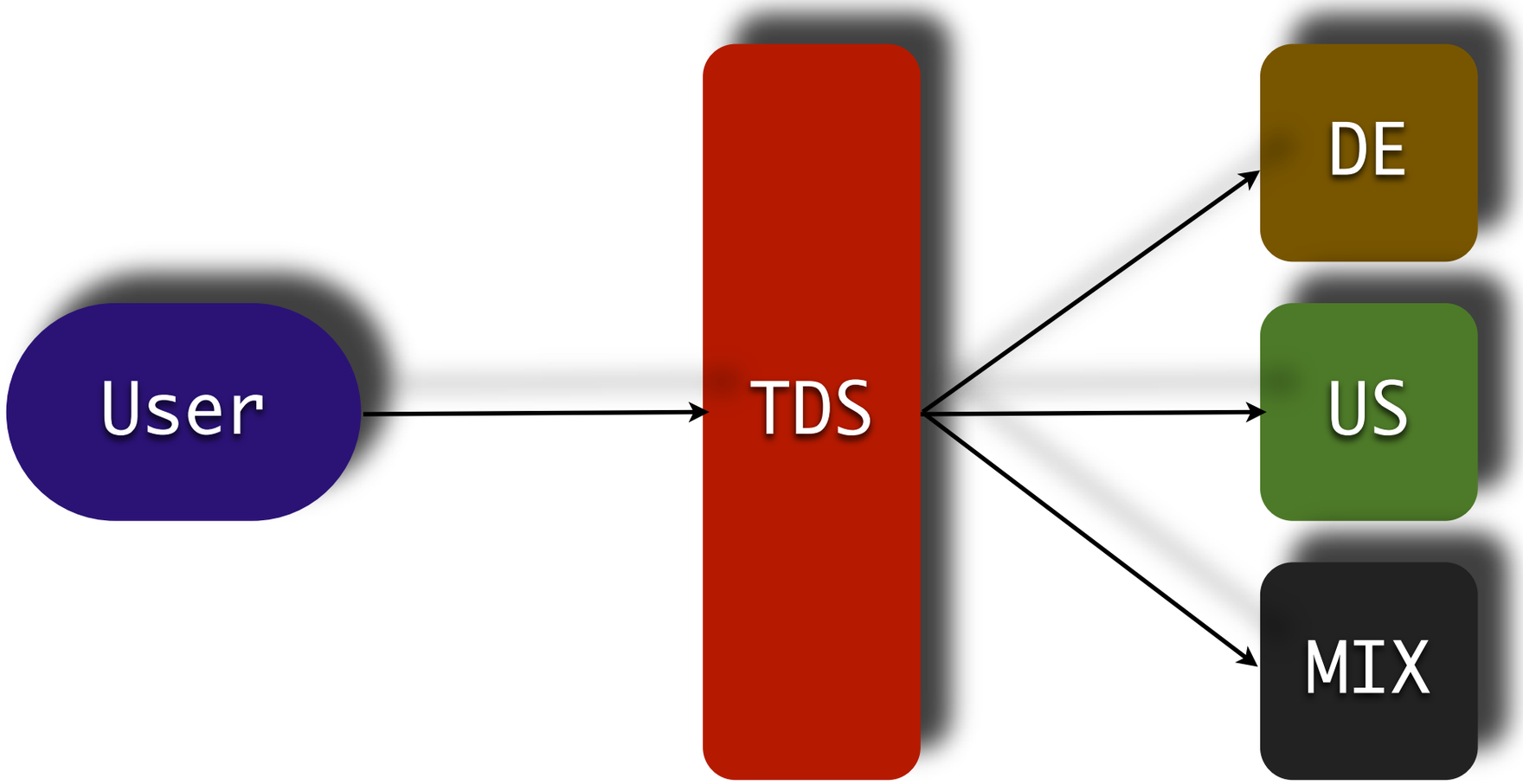
GET /1/1/typical.php HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, application/x-shockwave-flash, */*
Referer: http://www.trendmicro.com/news
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 2.0.50727)
Host: www.just-a-stie.com
Connection: Keep-Alive

language

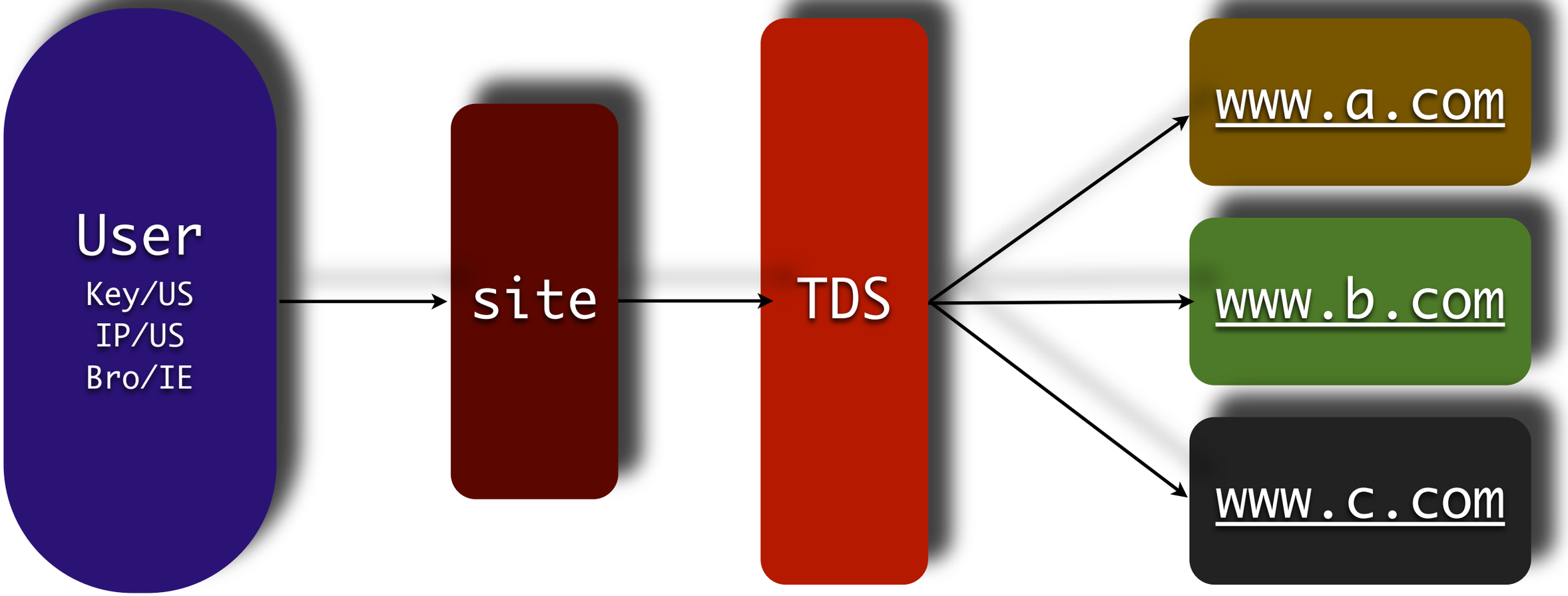
browser

OS

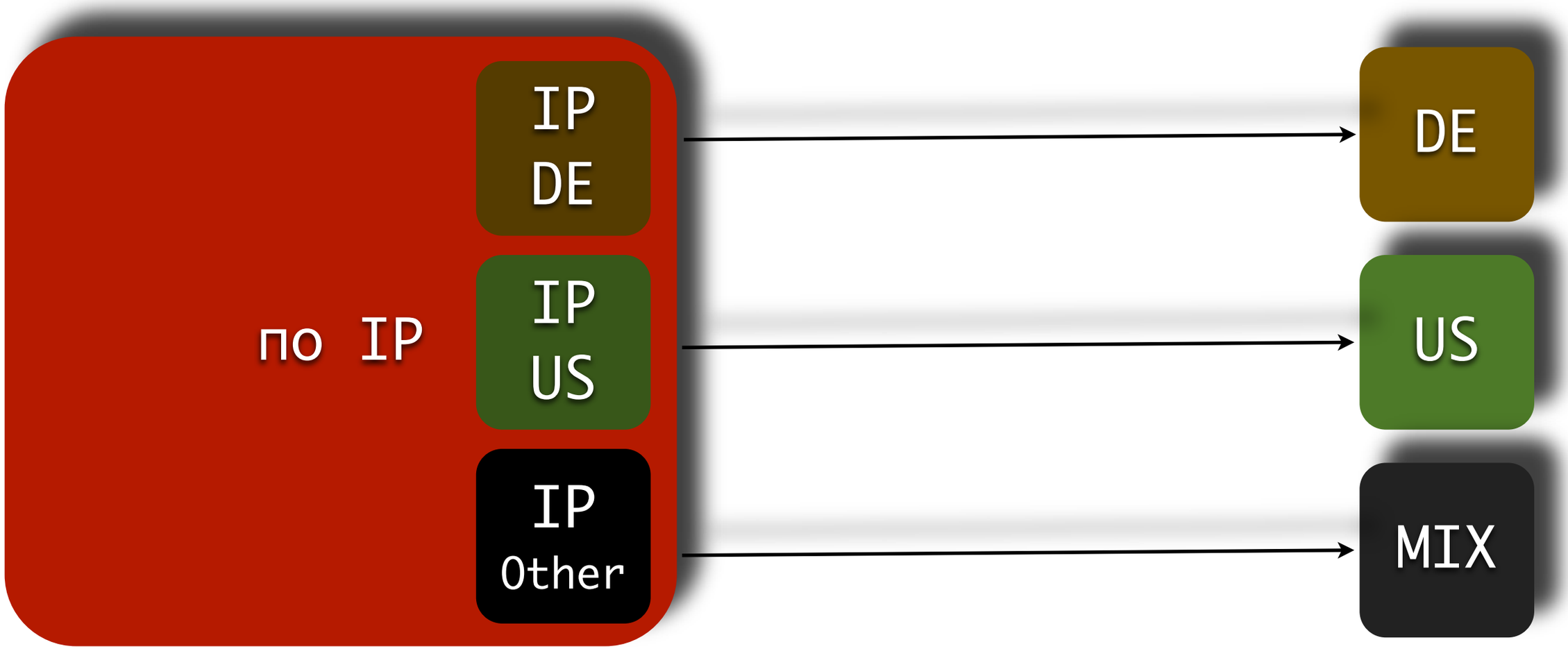
Теория и практика



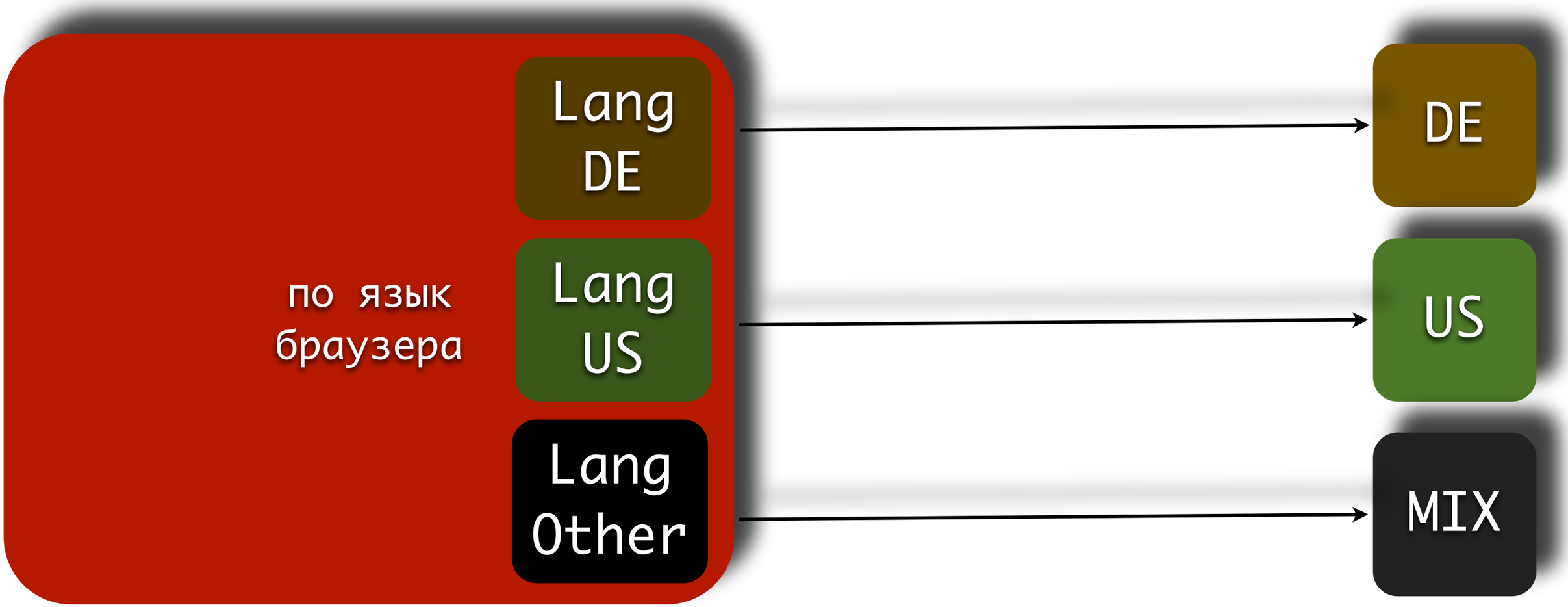
Теория и практика



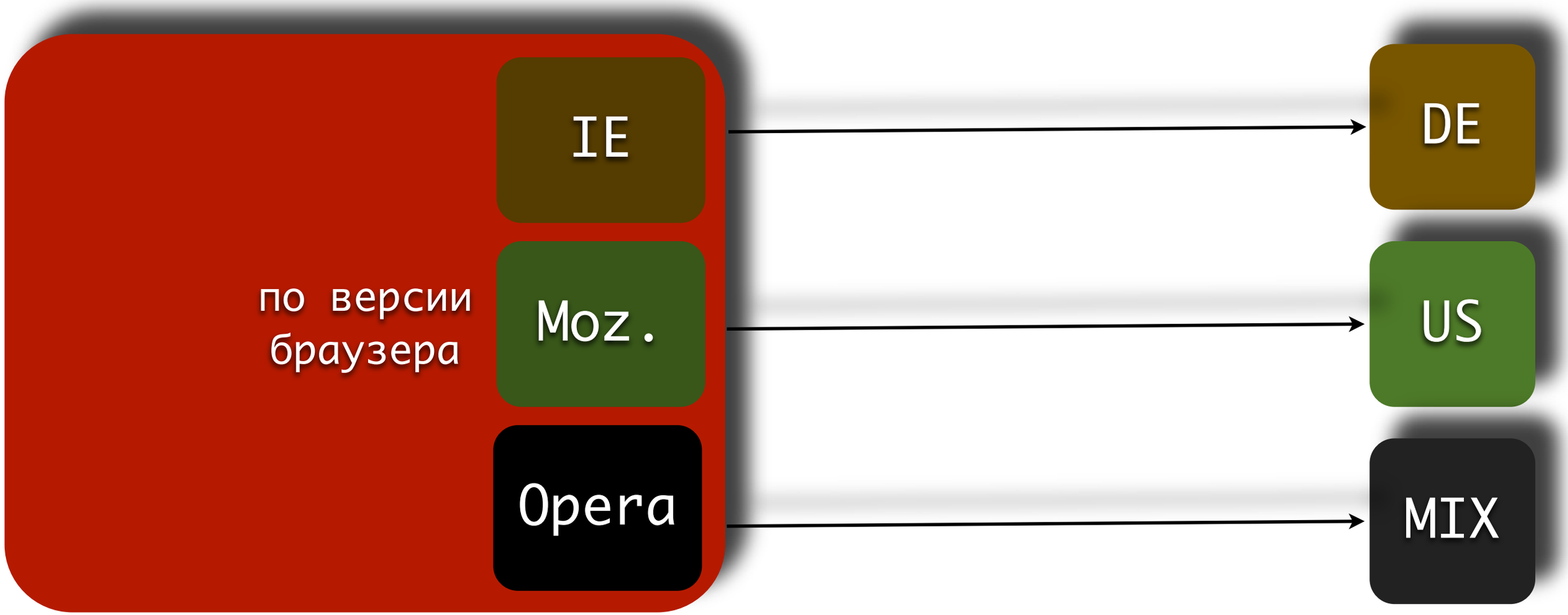
Теория и практика



Теория и практика



Теория и практика



HTTP Статус Код

- 300 multiple choices [Множество выборов]
- 301 moved permanently [Перемещено окончательно]
- 302 found [Найдено]
- 303 see other [Смотреть другое]
- 304 not modified [Не изменялось]
- 305 use proxy [Использовать прокси]
- 306 switch Proxy [*зарезервировано*]
- 307 temporary redirect [Временное перенаправление]

301 moved permanently

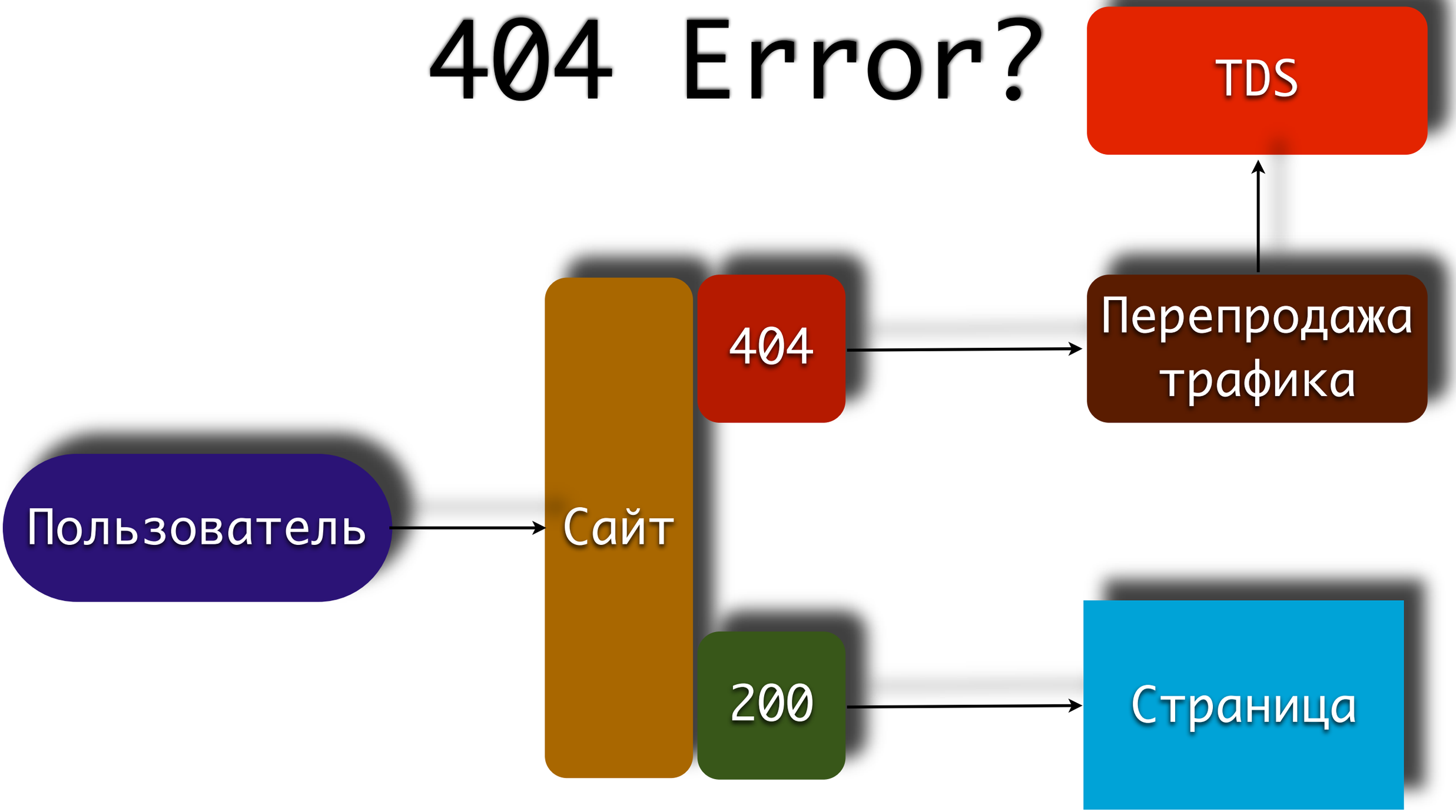
[Перемещено окончательно]

302 found/moved

[Найдено / Перемещено]


SOUTH
INTERSTATE
CALIFORNIA
404
ERROR

404 Error?


TDS
404
Перепродажа трафика
Пользователь
Сайт
200
Страница

Траффик

- Отбор по региону (GeoIP)
- Отбор по уникальному IP
- Отбор по HTTP_REFERER
- Отбор по временным рамкам
- Отбор по разновидности браузера
- Отбор по типу операционной системы
- Определение сборщика (crawler detect)
- Отсев по известным IP адресам

Отбор по региону

TDS

Result

Отбор по региону

MaxMind®

GeoLocalSEO
Go Local on the World Wide Web

IP2LOCATION™

hostip.info
My IP Address Lookup and GeoTargeting Community Geotarget IP Project – what country, city IP addresses map to

Временные рамки

TDS

Result

Тип браузера

TDS

Result

Наблюдения и факты

- Adult или Non adult трафик
- Распространение вредоносного кода
- Оптимизация поисковых запросов
- Залоговый трафик
- Украденые клики
- Модель заработка
- Пример владельца TDS

Adult или Non adult.

Traffic + Power.us

BuyAdultTraffic.Us

Welcome to Tp BuyAdultTraffic.Us! v1.10. As leaders in Adult Traffic Promotion we are capable of maximizing your ROI at the lowest prices on the internet.

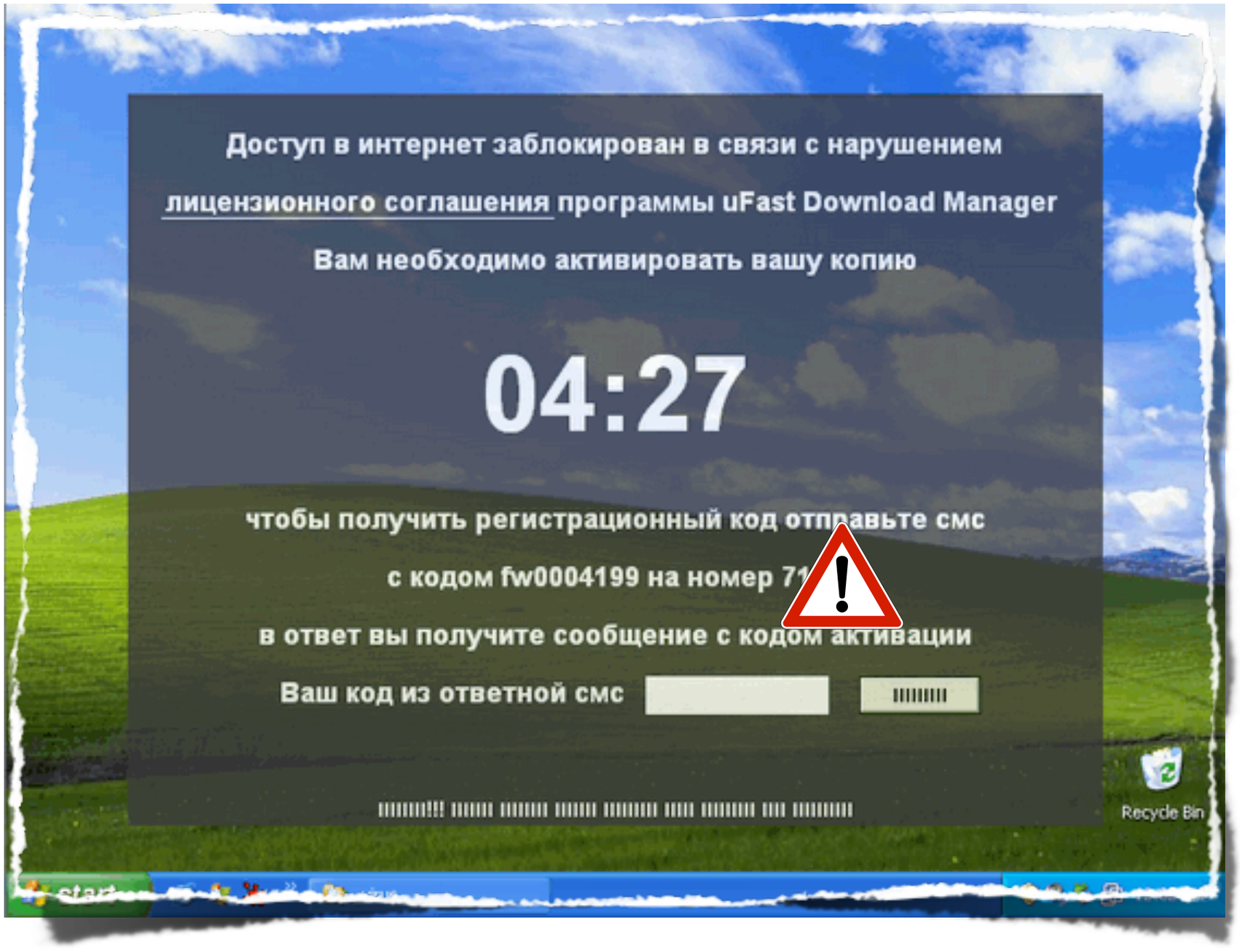
Login Signup FAQs Contact Money Links

Amount	Tarjet 1	Tarjet 2	Price $	Price €	
5,000	Mainstream	Adult	$22.00	€15.40	Buy Now
10,000	Mainstream	Adult	$39.00	€27.30	Buy Now
20,000	Mainstream	Adult	$72.00	€50.39	Buy Now
25,000	Mainstream	Adult	$85.00	€59.49	Buy Now
50,000	Mainstream	Adult	$147.00	€102.86	Buy Now
100,000	Mainstream	Adult	$278.00	€194.52	Buy Now
200,000	Mainstream	Adult	$486.00	€340.03	Buy Now
250,000	Mainstream	Adult	$552.00	€386.21	Buy Now
500,000	Mainstream	Adult	$987.00	€690.56	Buy Now
1,000,000	Mainstream	Adult	$1675.00	€1172.24	Buy Now

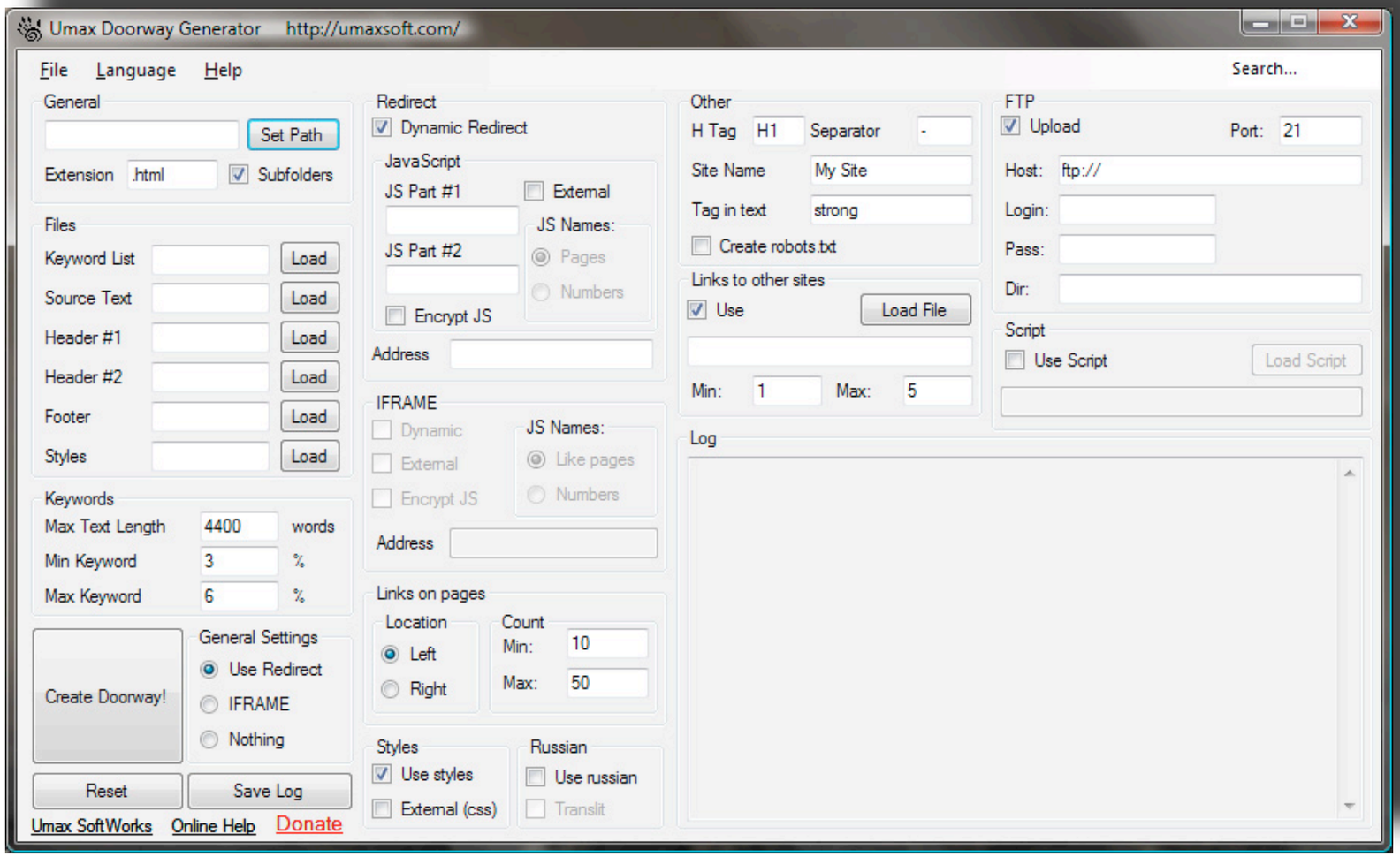
Amount	Tarjet 1	Tarjet 2	Price $	Price €	
10,000	Mainstream	Adult Gay	$49.00	€34.29	Buy Now
50,000	Mainstream	Adult Gay	$197.00	€137.87	Buy Now
250,000	Mainstream	Adult Gay	$786.00	€550.20	Buy Now
500,000	Mainstream	Adult Gay	$1221.00	€854.70	Buy Now

After your payment, will be sent to our panel of account creation.

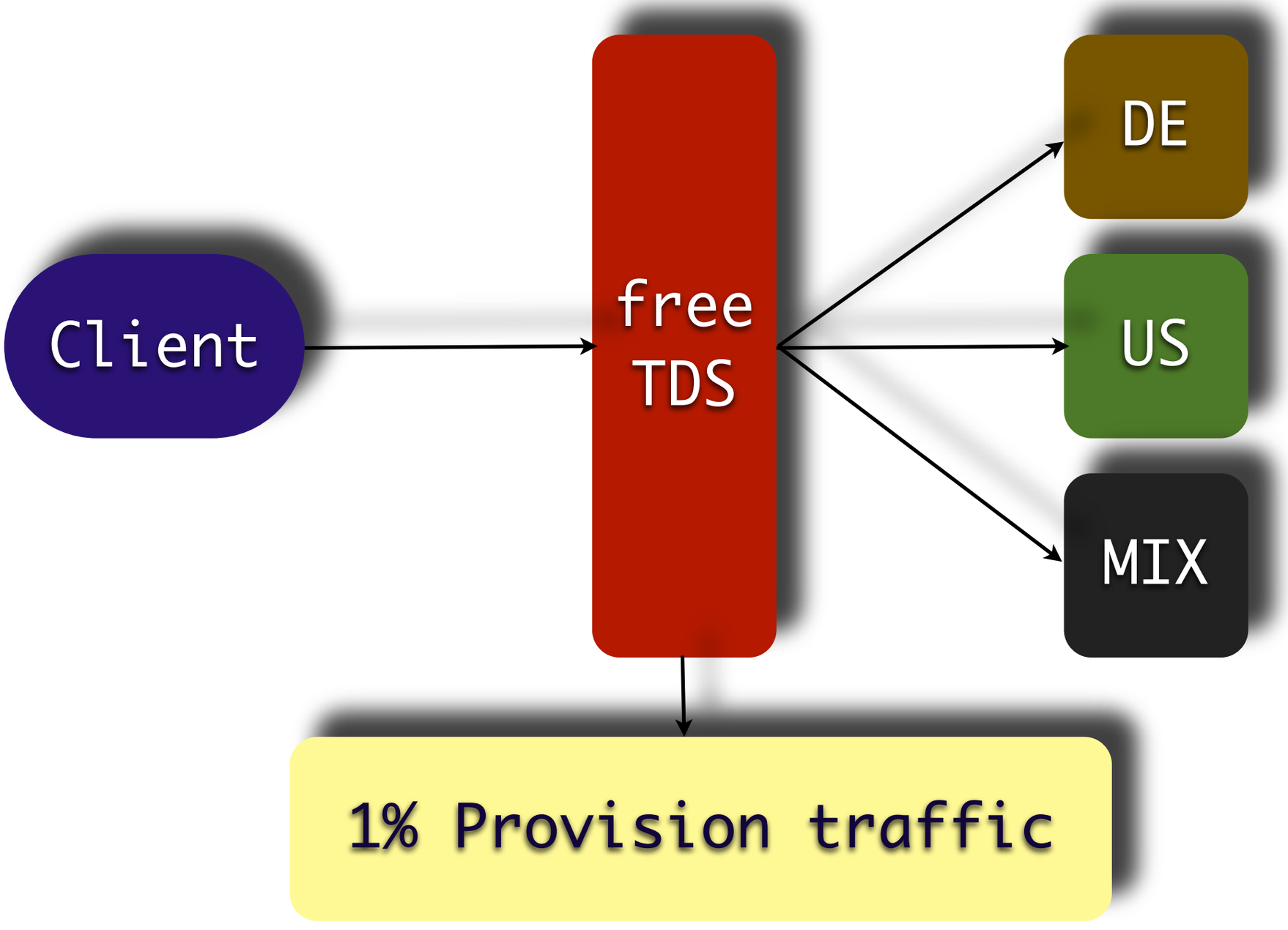
Распространение вредоносного кода



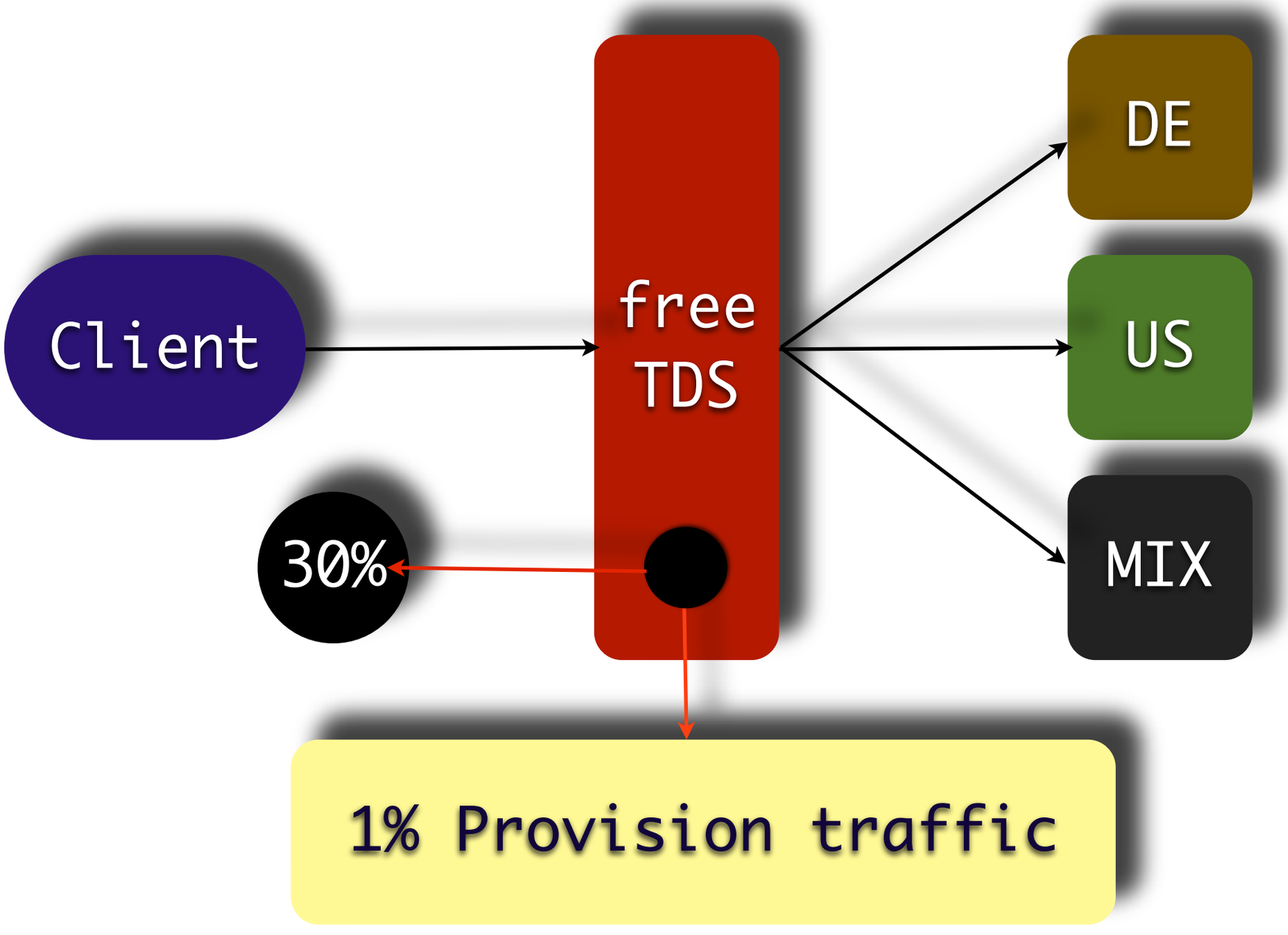
Оптимизация результатов поиска



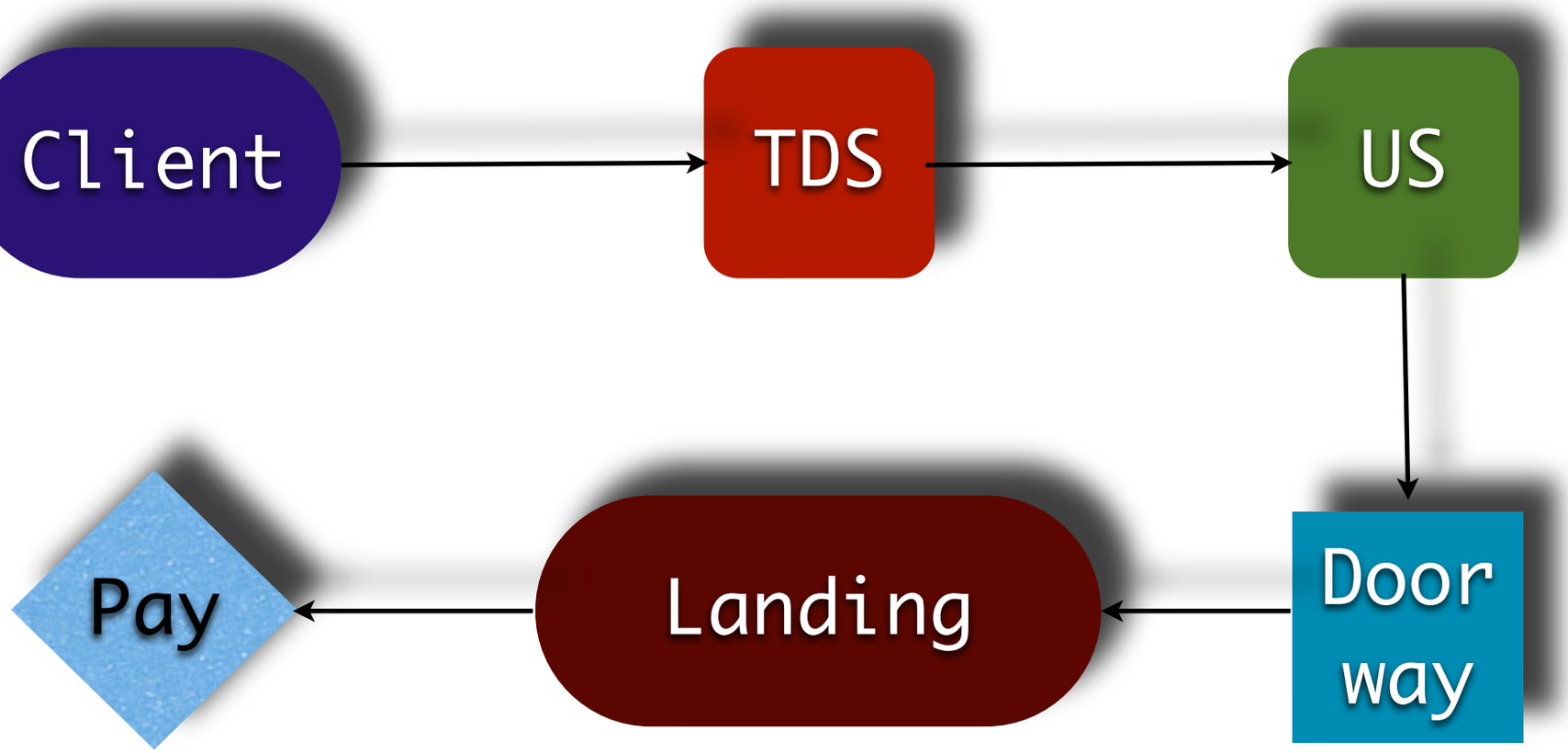
Залоговый трафик



Украденые клики



Модель заработка



Пример владельца TDS

http://open-tds.ru/?id=148968&go=1000000&close=1000000&hash=27a38df0abf6ffbc6c53cf2c21eaa8d6&Usys=x1809C

urce	Date	Information
ow	August 29, 2010 16:41	This information page's creation date
ols	August 29, 2010 16:41	Blacklistings

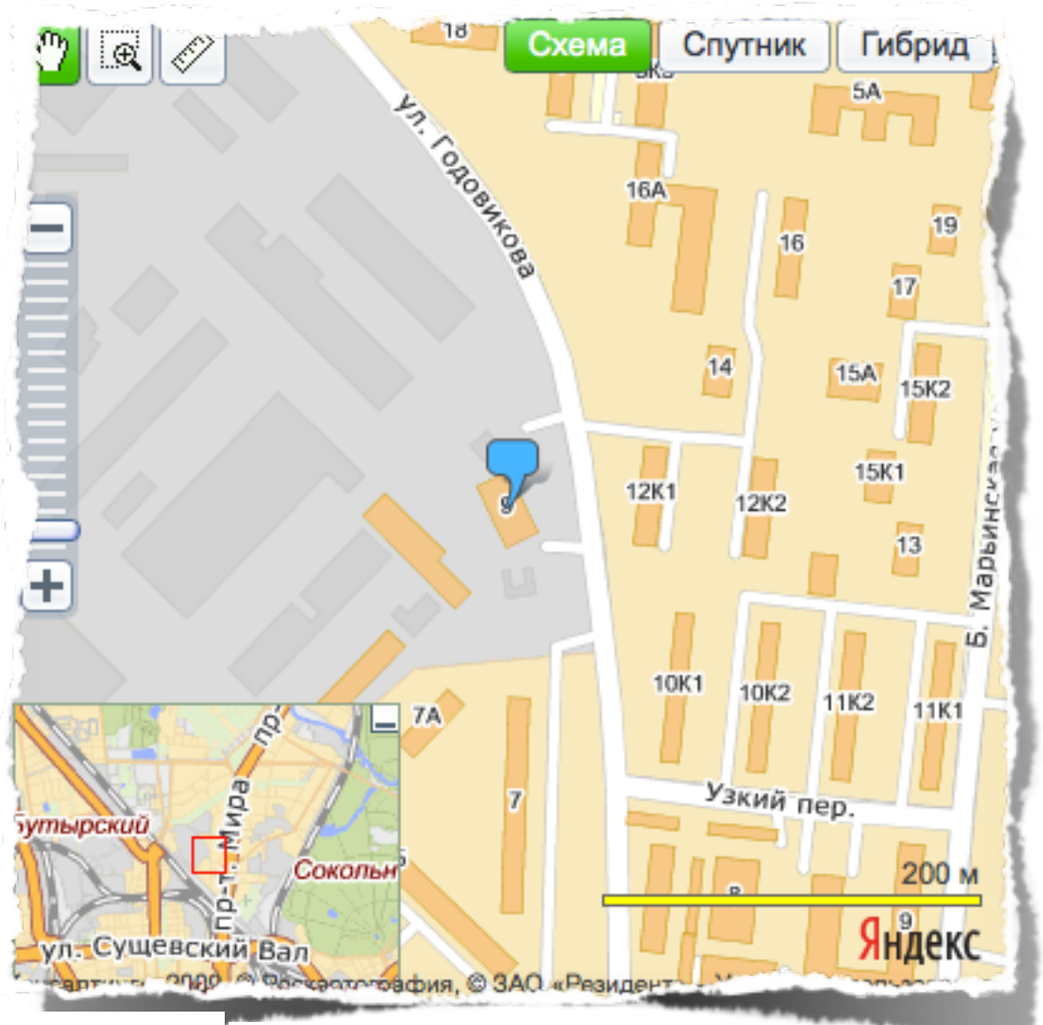
NET 188.64.170
188.64.168.0/21 H1 Network AS6870

Base	Record	Name	IP	Reverse	Route	AS
*.open-tds.ru	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru	188.64.168.0/21 H1 Network	AS6870 H1ASN H1 LL(
h1net188-64-170-7.h1host.ru	a		188.64.170.7 Russian Federation			
ndexite.ru	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
pen-tds.ru	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
redirecturl.ru	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
www.open-tds.ru	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
yahhoou.com	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
yundex.me	a		188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		
www.check-url.com	cname	check-url.com	188.64.170.7 Russian Federation	h1net188-64-170-7.h1host.ru		

Пример владельца TDS

SoftTrade Lab

⚠vich⚠v Max aka MaxTrade.



Разновидности TDS

- Сервис - все готово.
- ПО - все нужно делать самому

TDS как сервис

MegaTDS.ru

Open-TDS.ru

Absolut-tds.ru

TDS как приложение

- Simple TDS
- Sutra TDS (100USD)
- Crazy TDS
- Kalisto TDS
- ILTDS
- Advanced TDS
- Keitaro TDS

Simple TDS

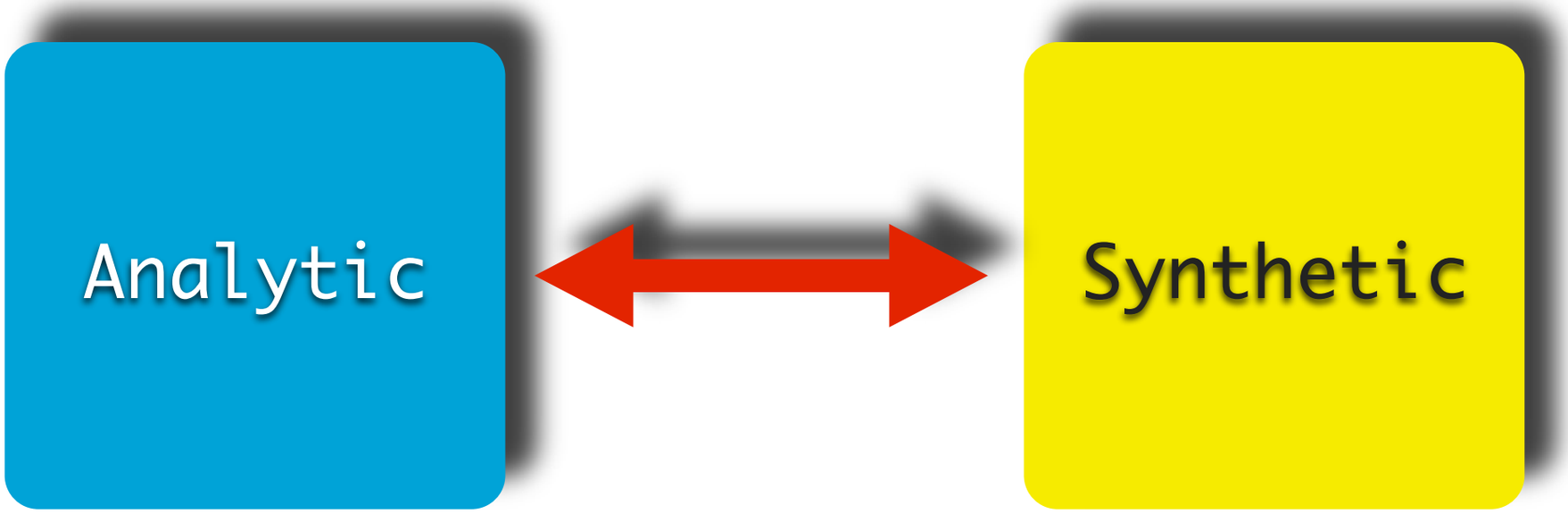
http://www.simpletds.com/

- Пошаговая установка
- Размещение
- Поддержка

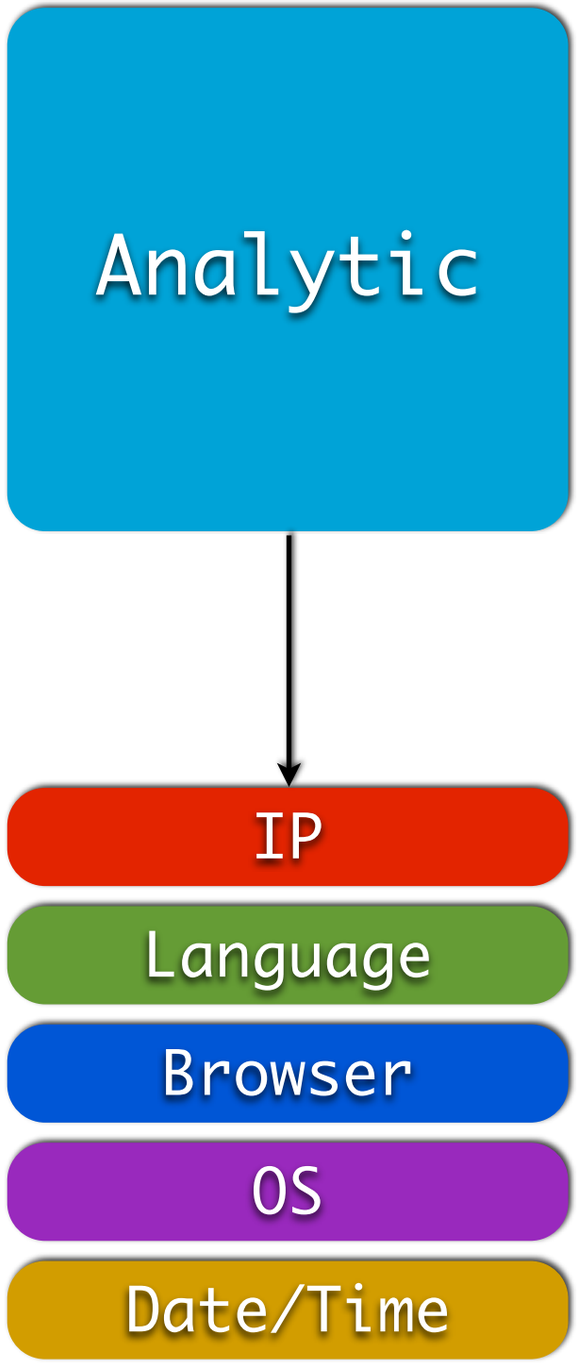
Simple TDS
fingerprint

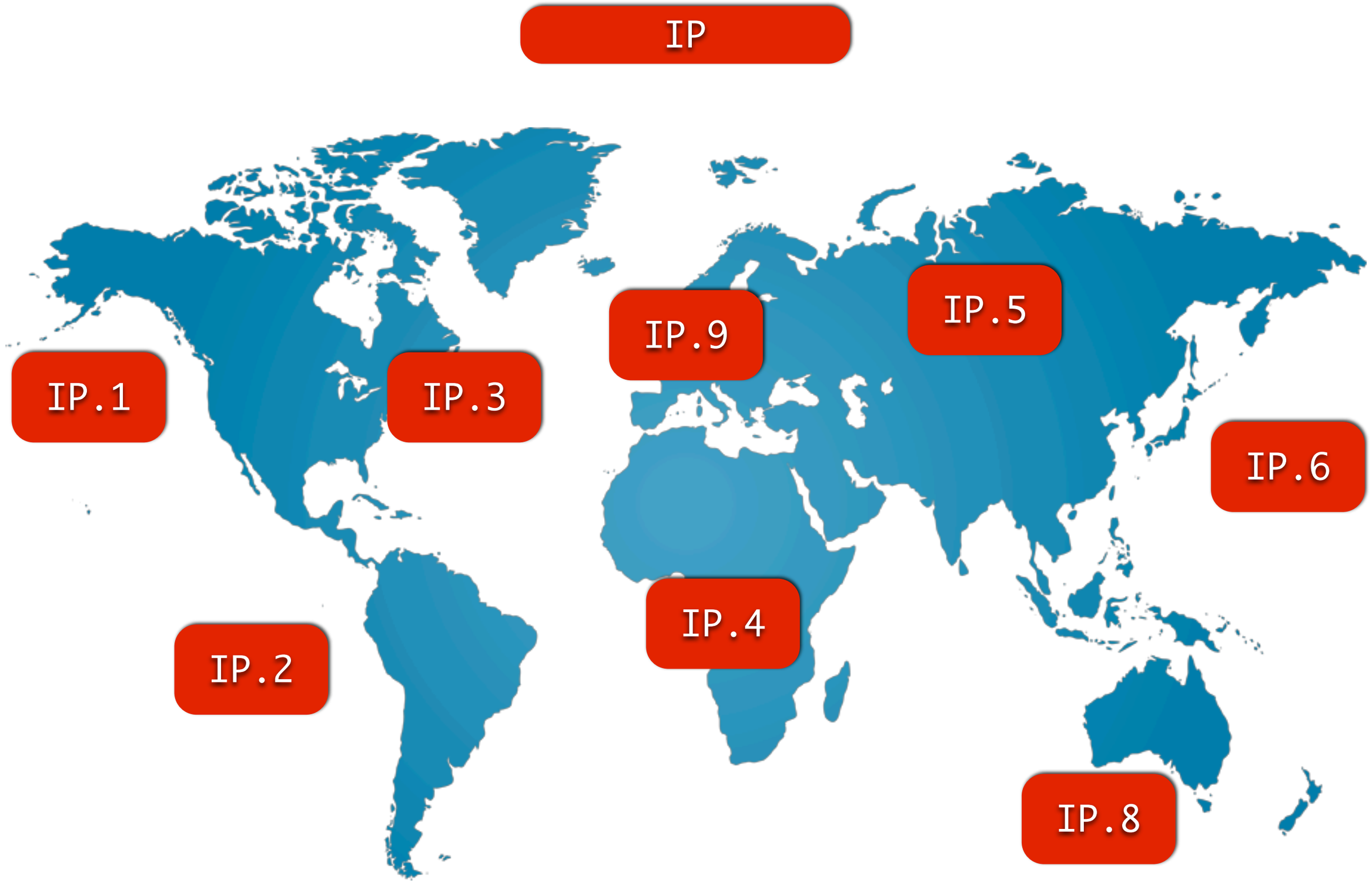
- почти всегда используется go.php для перенаправления трафика
- запрос всегда использует ‘id’, ‘schema’
- существует config.php, login.php
- существует version.php показывает версию

Детектирование TDS

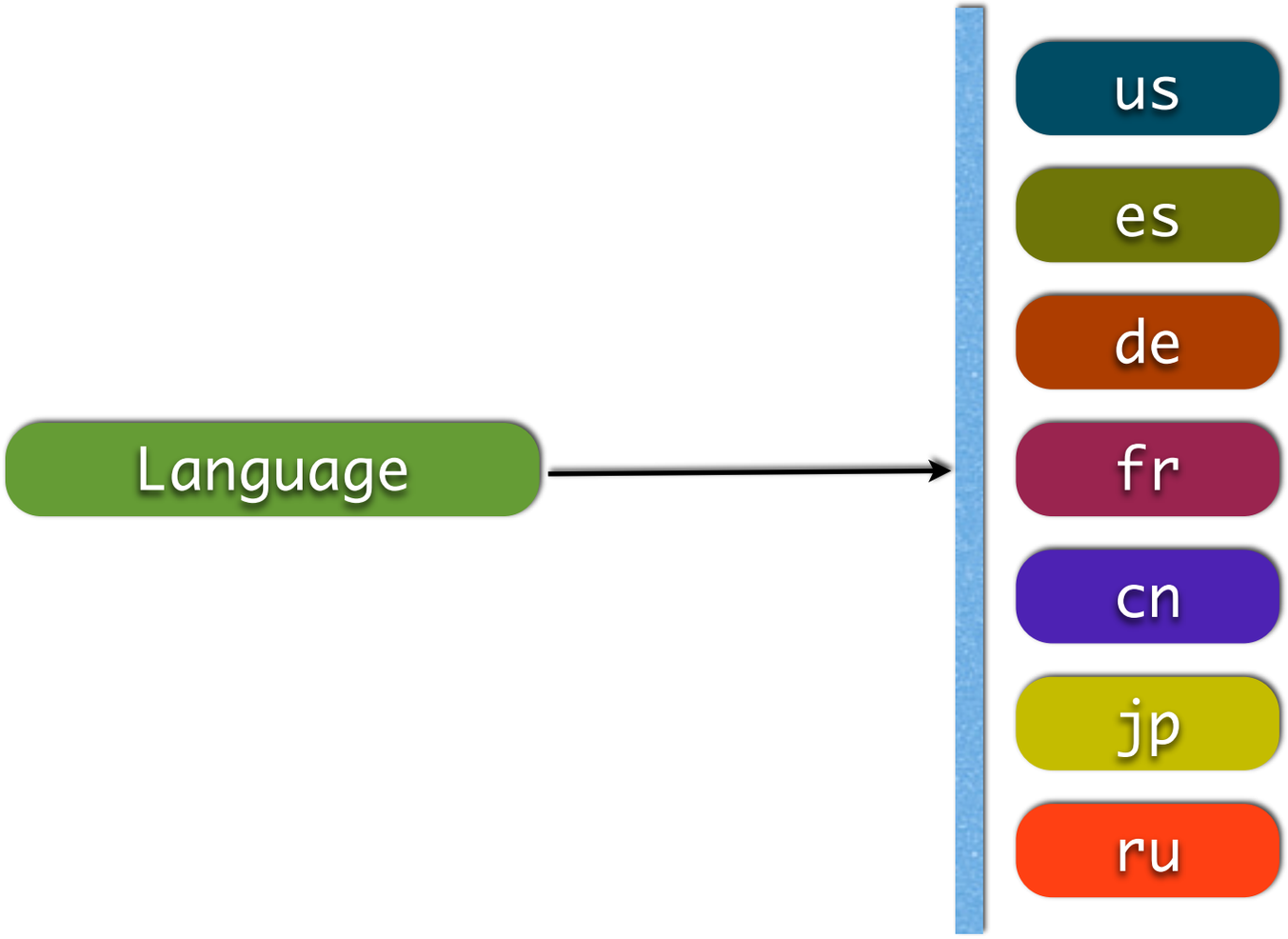


Детектирование TDS

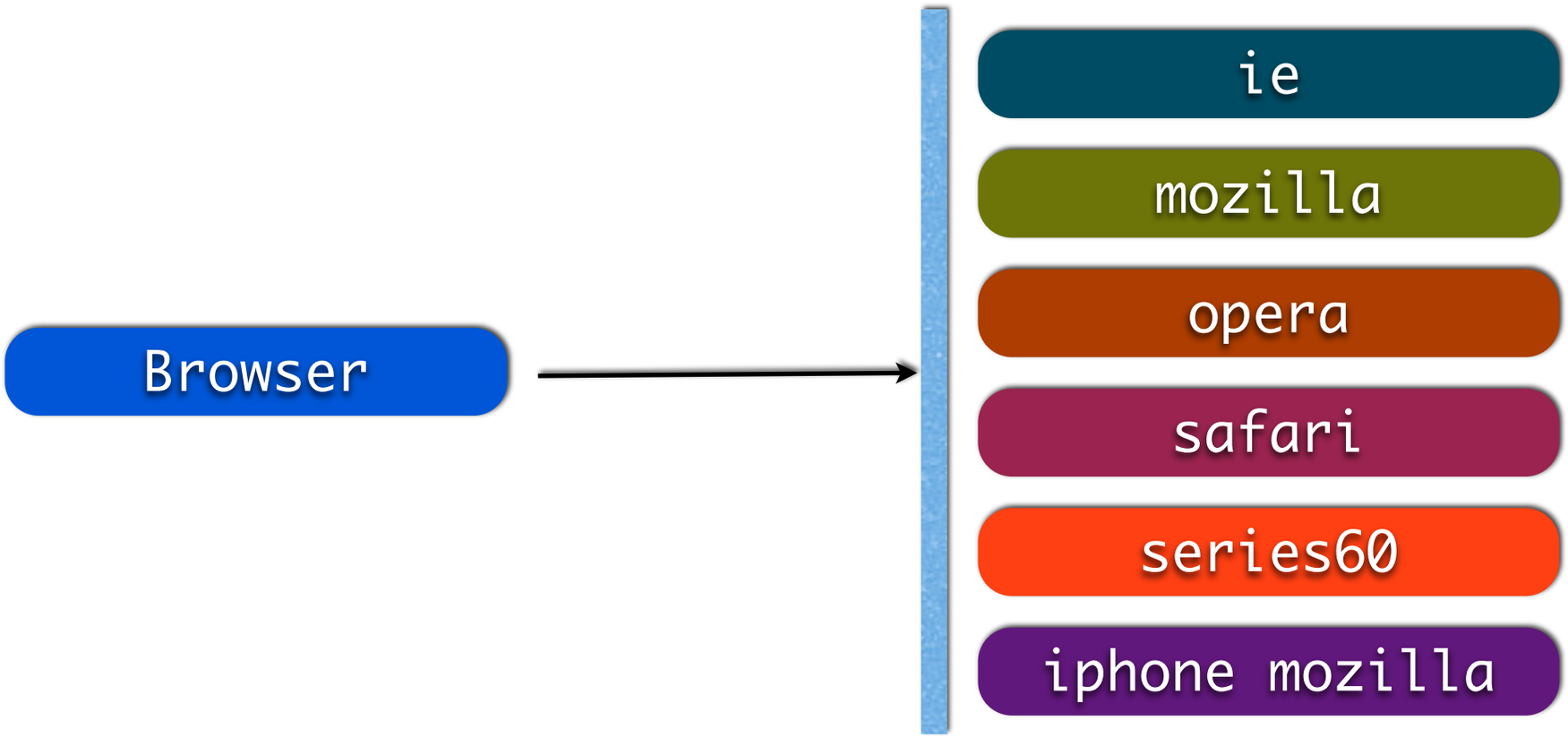



IP
IP.1
IP.2
IP.3
IP.4
IP.5
IP.6
IP.8
IP.9

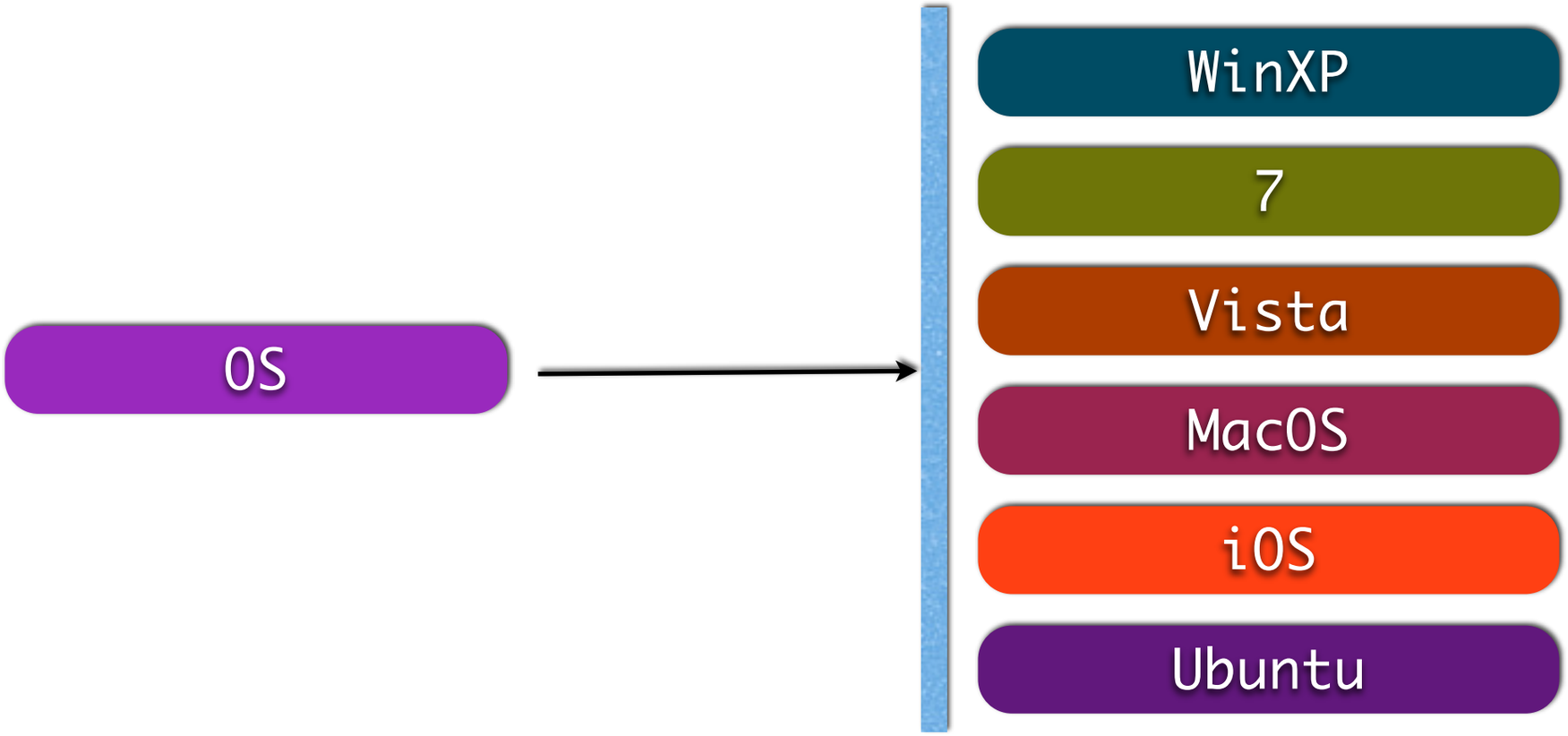
Детектирование TDS



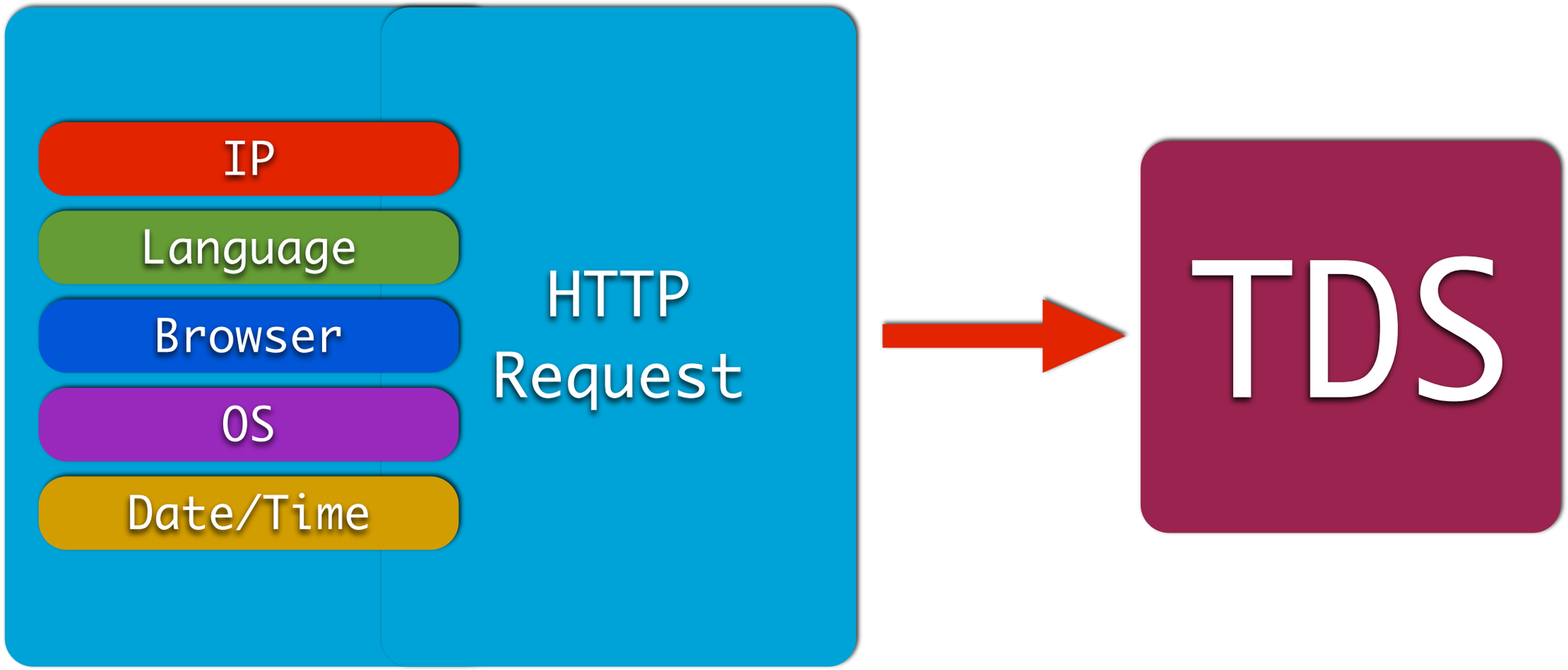
Детектирование TDS



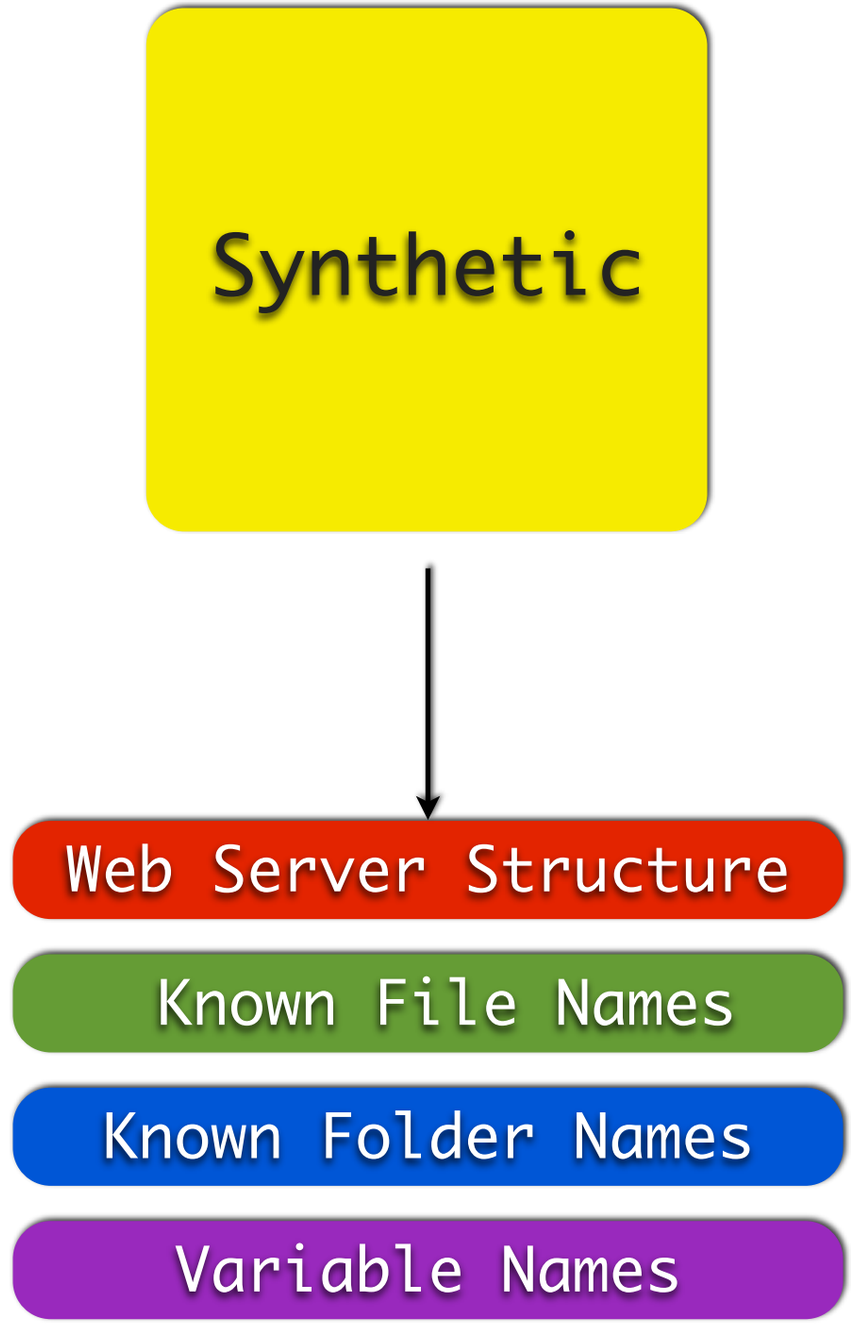
Детектирование TDS



Детектирование TDS



Детектирование TDS



Детектирование TDS

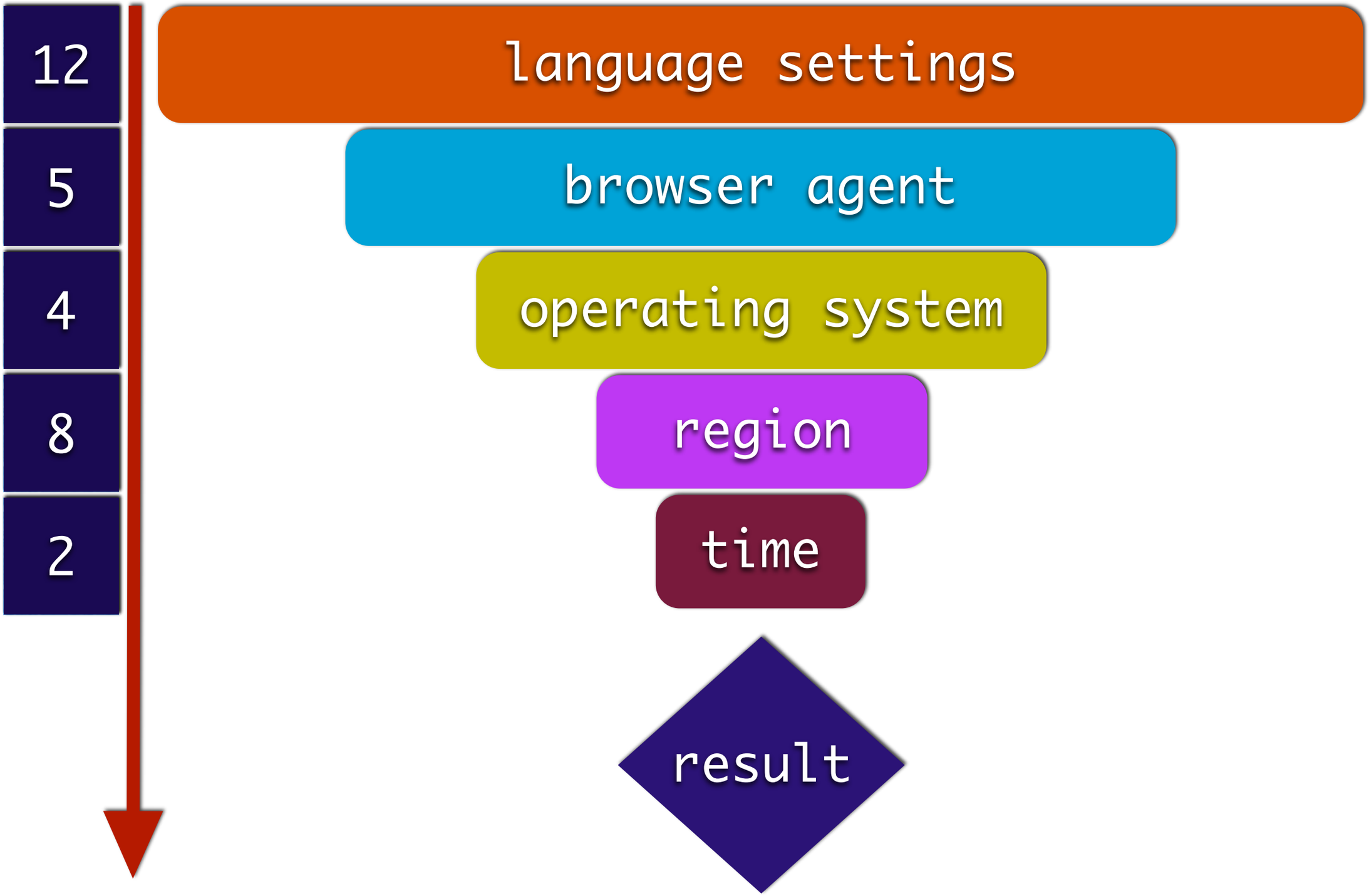
request

Analytic

Synthetic

result

Логика опроса TDS

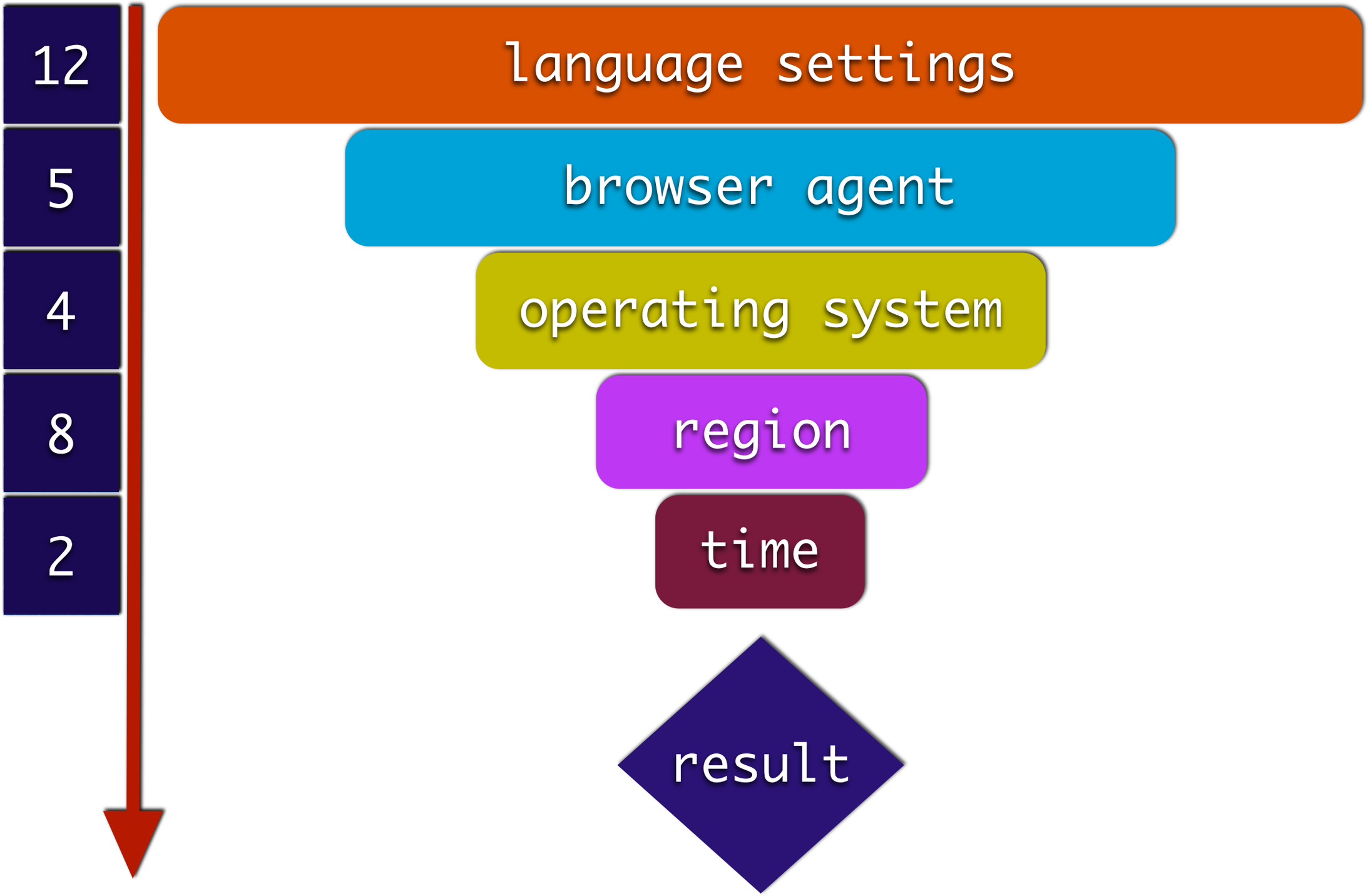


Логика опроса TDS

language settings

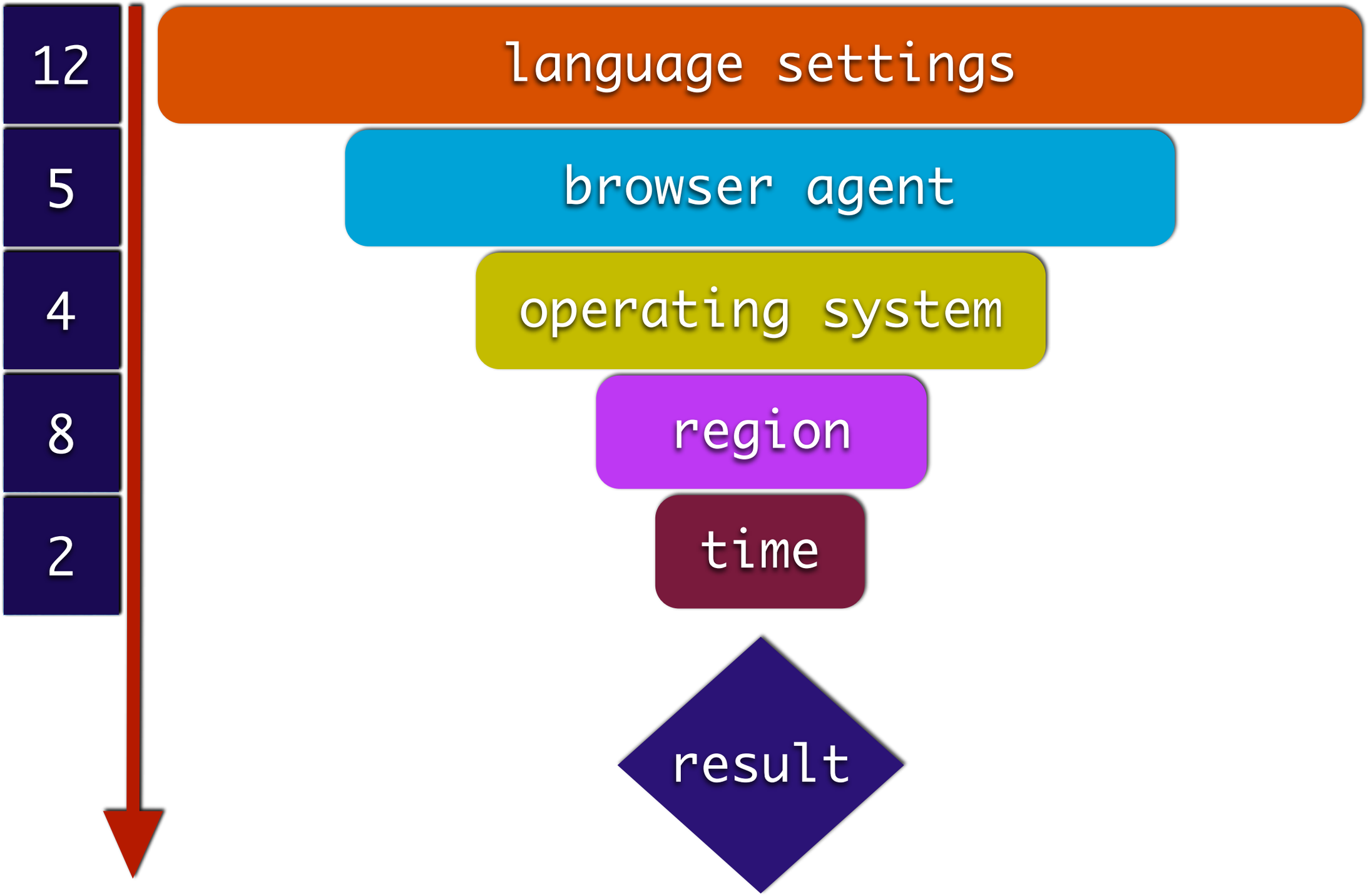
- en-us
- es
- fr
- de
- ru
- pl
- jp
- cn
- pt
- it
- ro
- bg

Логика опроса TDS



Логика опроса TDS

Логика опроса TDS

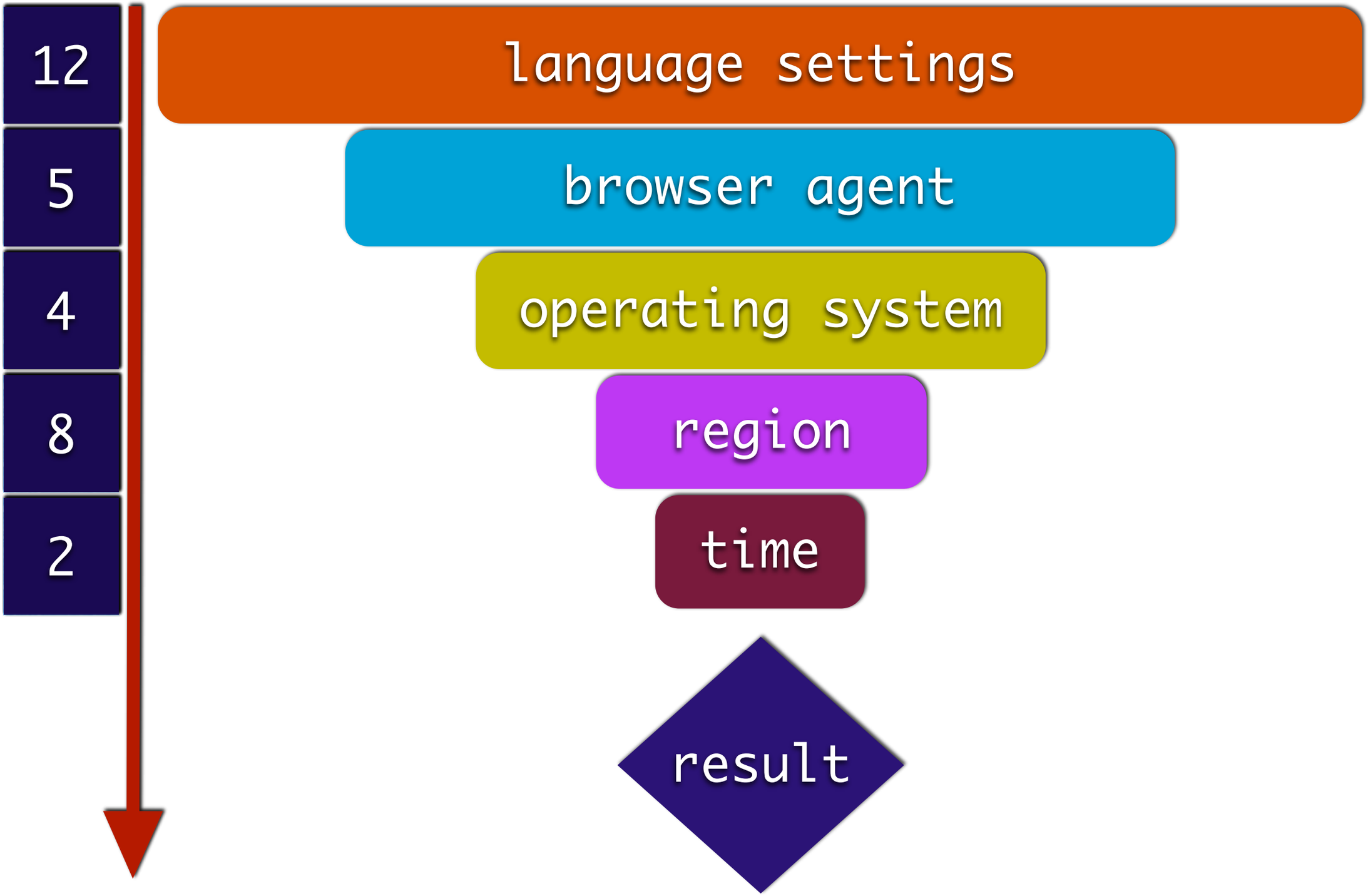


Логика опроса TDS

operating system

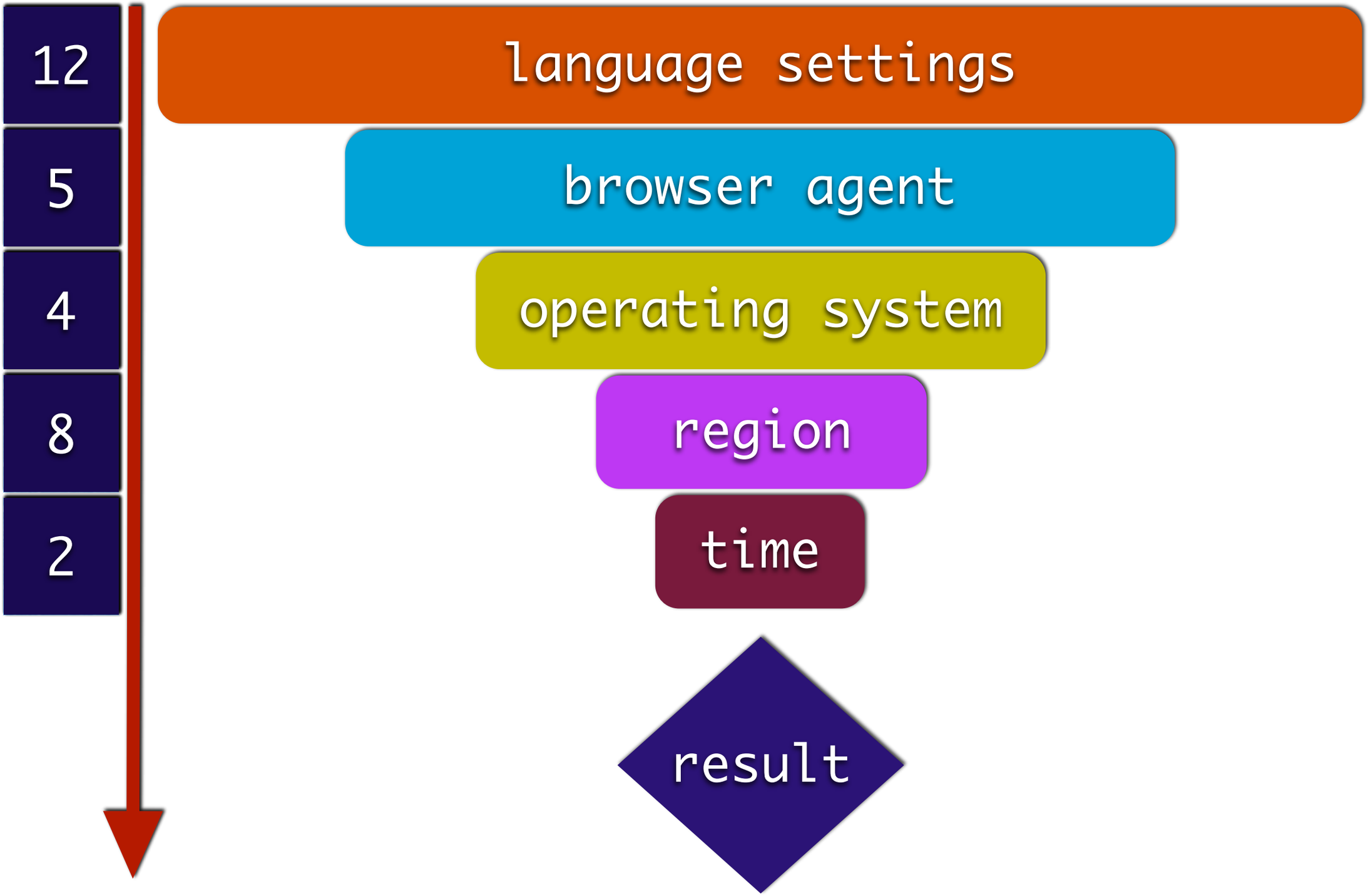
- windows OS
- MacOS
- Linux Generic
- iOS

Логика опроса TDS

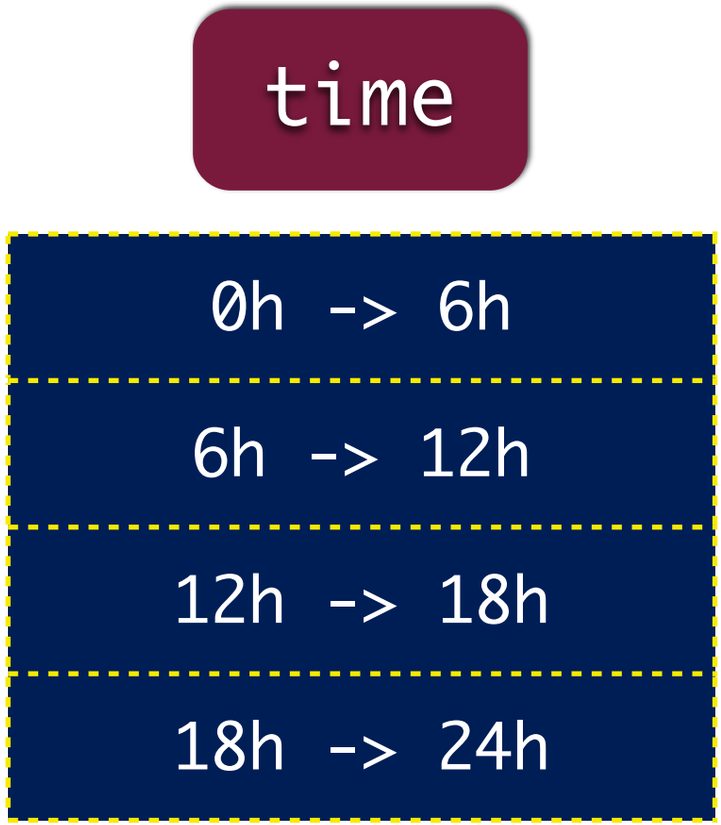


Логика опроса TDS

Логика опроса TDS



Логика опроса TDS



опрос по L10n

attempt	region	language	os	agent
1	us west	en	windows	ie
2	russia	ru	windows	ie
3	japan	jp	windows	ie
4	germany	de	windows	ie
5	us east	en	windows	ie
6	russia	ru	windows	ie
7	france	fr	windows	ie

Опрос по браузеру

attempt	region	language	os	agent
1	us west	en	windows	ie
2	us west	en	windows	opera
3	us west	en	windows	mozilla
4	us west	en	windows	s60
5	us west	en	windows	safari
6	us west	en	MacOS	mozilla
7	us west	en	windows	safari

Вопросы?

max_goncharov@trendmicro.com

Спасибо!

max_goncharov@trendmicro.com