Exploring the DarkWeb: Fighting Cybercrime with SENSEI and CRATOR

Dr. Giuseppe Cascavilla

JADS Jheronimus Academy of Data Science

Outline

- Introduction to the WWW
- Surface, Deep and Dark Web
- How deep is the Dark Web
- The Dark Economy
- What's in there
- CRATOR and SENSEI
- State of the Art of Cybercrime fighting

The World Wide Web

What is the WWW?

It is all the Web pages, pictures, videos and other online content that can be accessed via a Web browser. The World Wide Web (WWW) is a network of online content that is formatted in HTML and accessed via HTTP. The term refers to all the interlinked HTML pages that can be accessed over the Internet.

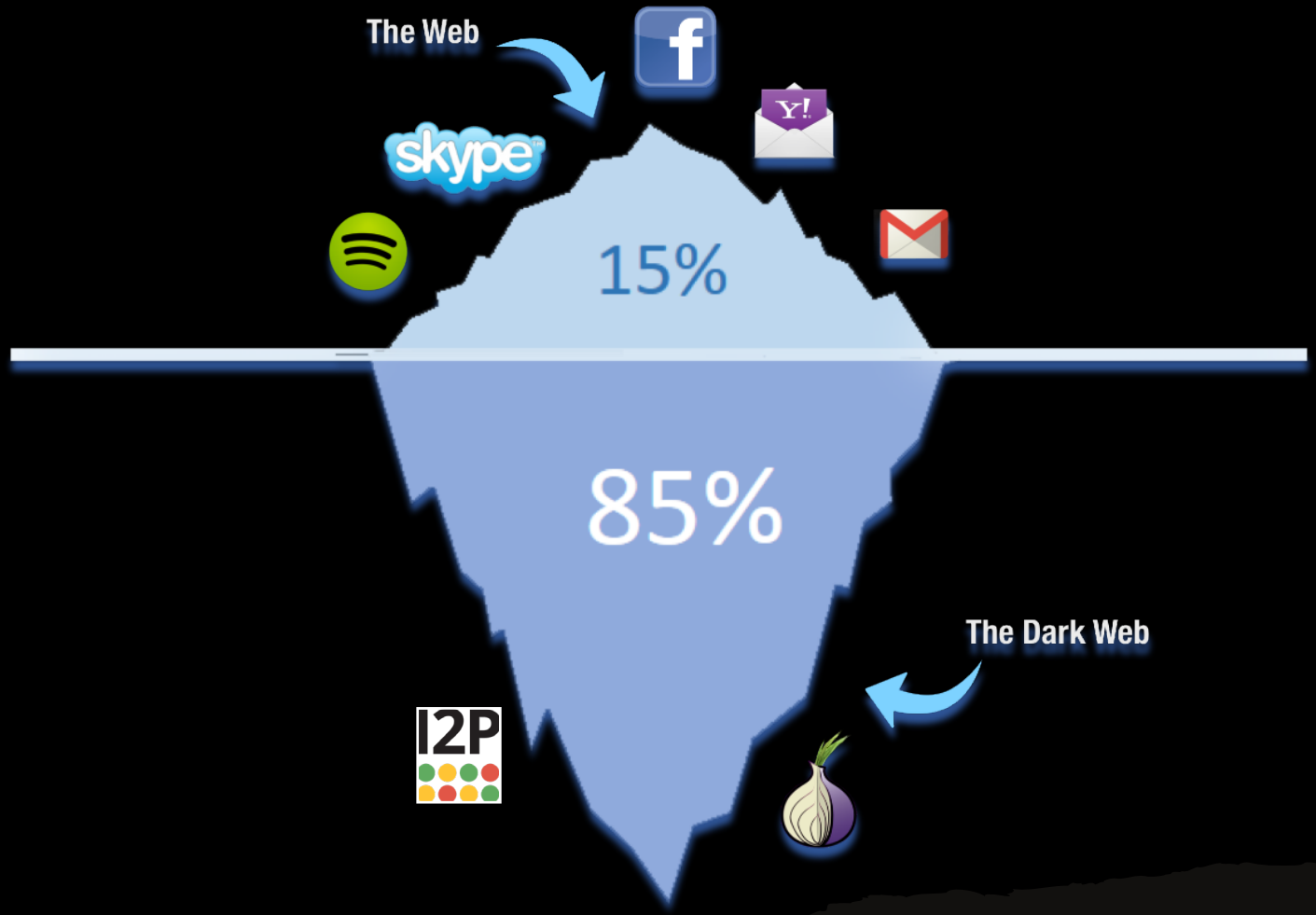
What is Internet?

The Internet is the actual network of networks where all the information resides. Things like Telnet, FTP, Internet gaming, Internet Relay Chat (IRC), and e-mail are all part of the Internet, but are not part of the World Wide Web.

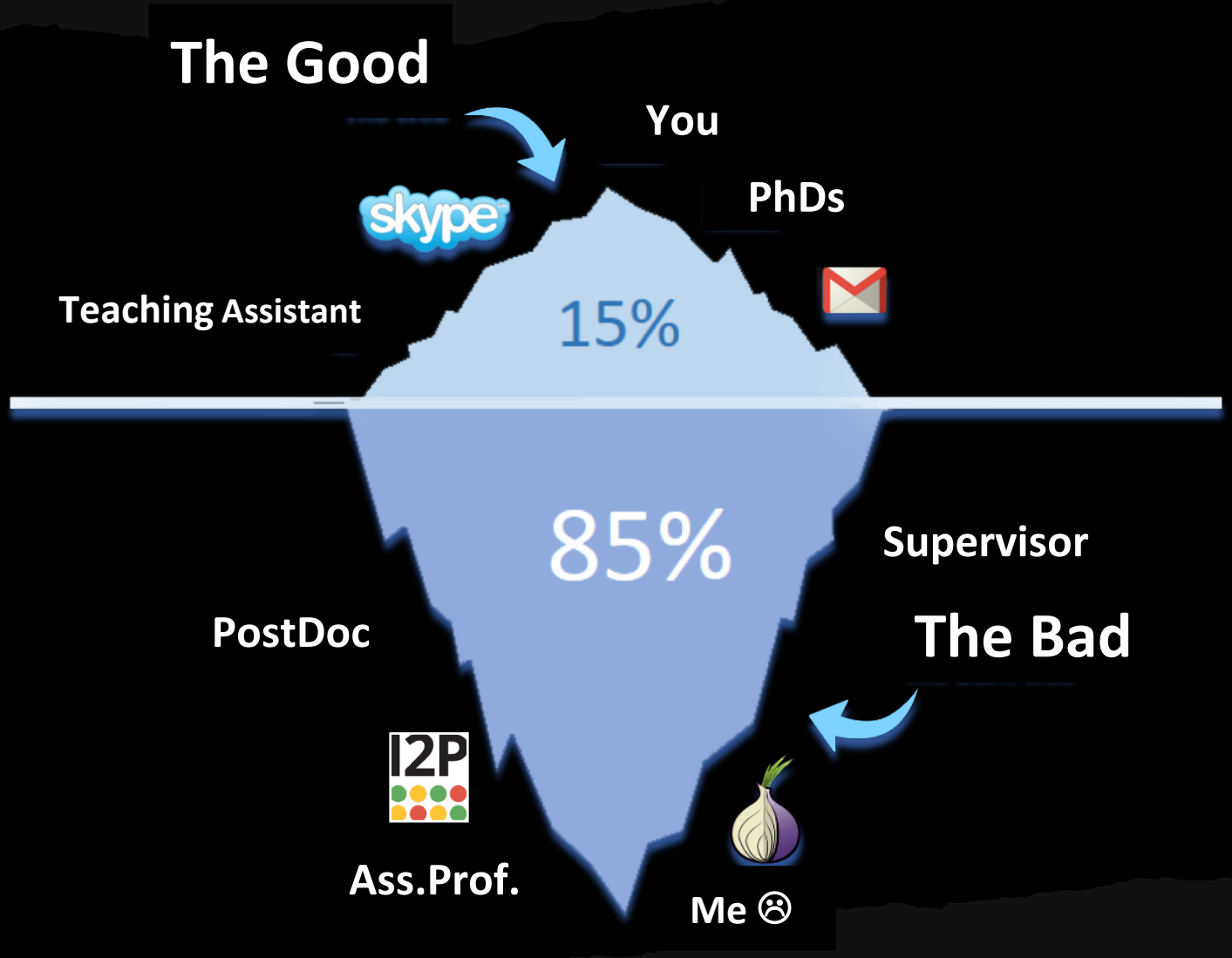
The Internet Map

Source: http://internet-map.net/#12-119.35335706687904-106.93210525876998

Internet Division



Office Division



The Good, the Bad, and the Ugly

GOOD - The **Surface Web** is what users access in their regular day-to-day activity.

The Good, the Bad, and the Ugly

GOOD - The **Surface Web** is what users access in their regular day-to-day activity.

BAD - The **Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Some pages are part of the Deep Web because they do not use common top-level domains. The majority of the 'Deep Web' is made up of databases, data that do not have to be indexed, news and newspaper reporting information censored in countries where the freedom is mined.

The Good, the Bad, and the Ugly

GOOD - The **Surface Web** is what users access in their regular day-to-day activity.

BAD - The **Deep Web** is the portion of the web that is not indexed or searchable by ordinary search engines. Some pages are part of the Deep Web because they do not use common top-level domains. The majority of the 'Deep Web' is made up of databases, data that do not have to be indexed, news and newspaper reporting information censored in countries where the freedom is mined.

UGLY - The **Dark Web** is a less accessible subset of the Deep Web that relies on connections made between trusted peers and requires specialized software, tools, or equipment to access. Two popular tools are used to access this portion of internet: Tor and I2P. Malicious actors use the Dark Web to communicate about, sell, and/or distribute illegal content or items such as drugs, illegal weapons, malware, and stolen data.

How big it is the Dark web?

TECH

The ‘deep web’ may be 500 times bigger than the normal web. Its use go well beyond buying drugs

PUBLISHED THU, SEP 6 2018•1:53 AM EDT | UPDATED THU, SEP 6 2018•8:38 PM EDT

How big is the Dark web?

The count of **live reachable .onion** domains comes to less than **0.006%** of the number of clear web site domains.

Though the Dark web is often portrayed as a cast and mysterious part of internet, it is **actually TINY** compared to the “clear web”.

Recorded Future spidered about 260.000 onion pages to approximate the full reachable Tor Network from a starting set of .onion sites that have been pulled from a public list.

Only around 8.416 .onion domains had a live site out of about 55.828 .onion domains found (15%).

Uptime even on popular dark web sites is well below the 99.999% “five nines” availability.

https://go.recordedfuture.com/hubfs/reports/cta-2019-0507.pdf
https://www.spiceworks.com/it-security/security-general/articles/dark-web-vs-deep-web/

… and the Deep web?

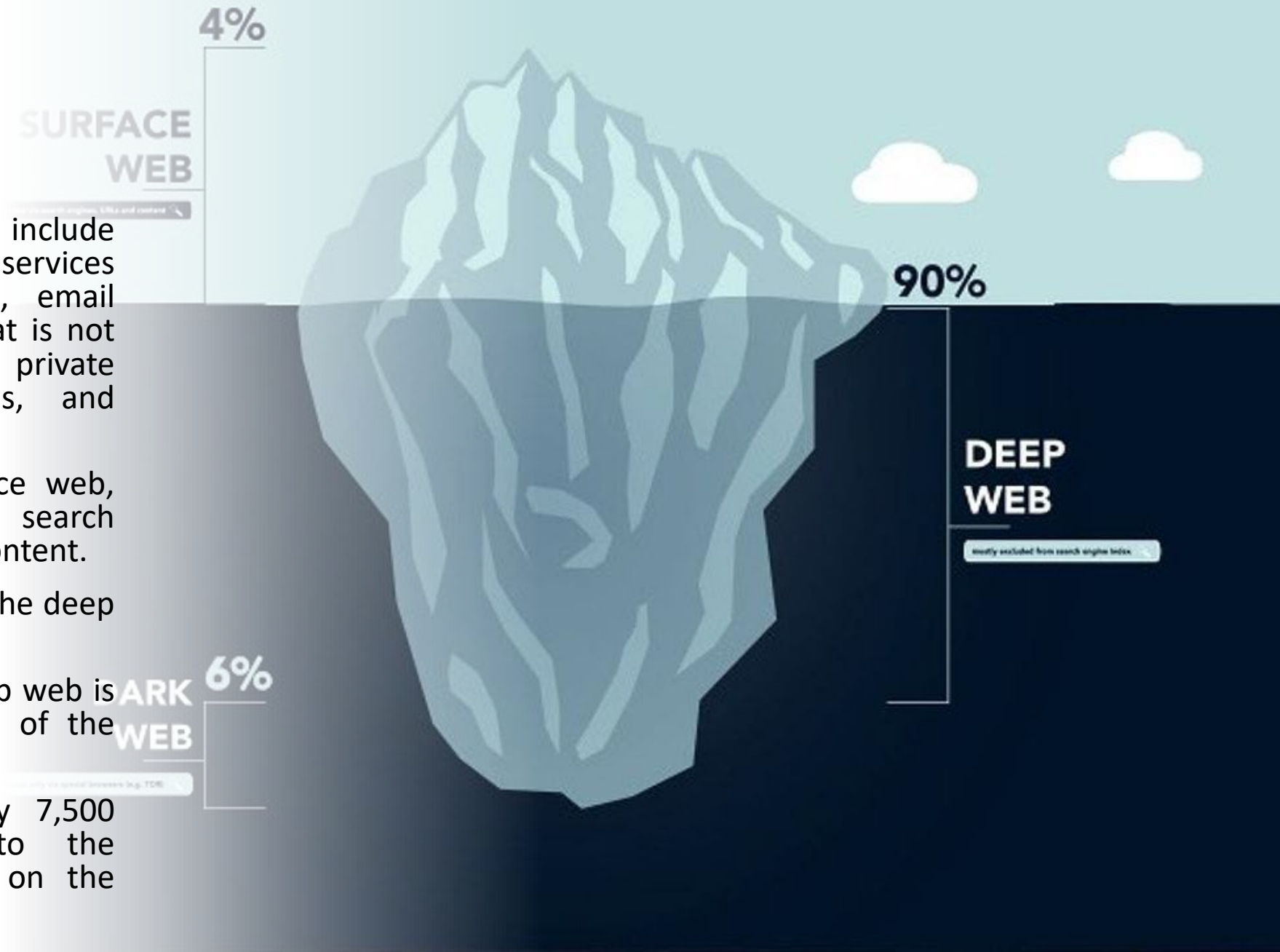
The Deep web hosts pages that include paywalled websites, pay-to-access services such as Netflix, private databases, email mailboxes, and any other content that is not indexed by web search engines, like private posts on social media platforms, and electronic health records.

Tremendously vaster than the surface web, with some experts estimating that search engines index less than 1% of online content.

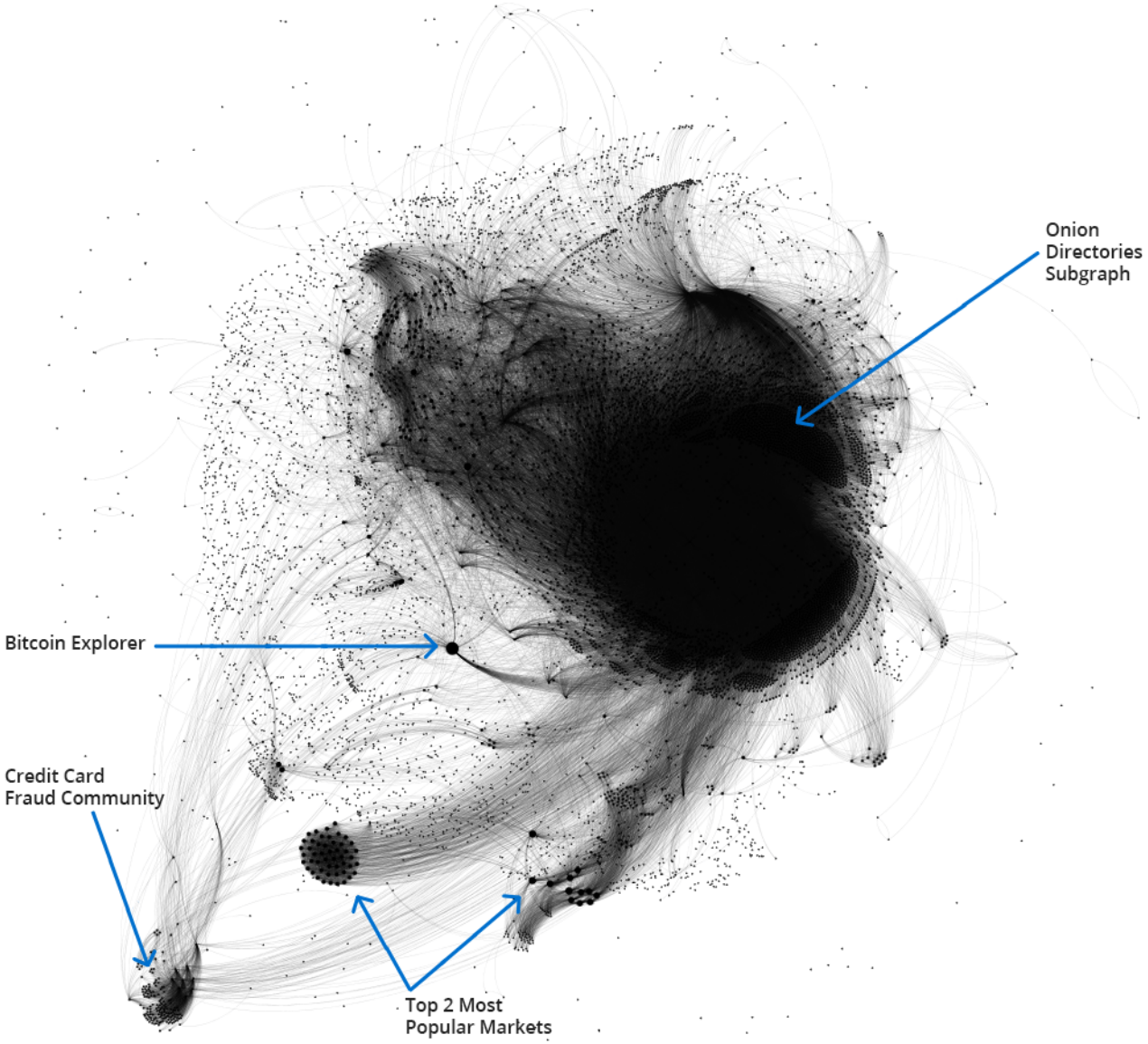
More than 200,000 websites exist on the deep web.

The volume of public data on the deep web is 400 to 500 times greater than that of the surface web.

The deep web hosts approximately 7,500 terabytes of data, compared to the approximately 19 terabytes hosted on the surface web.



What the Dark web looks like?



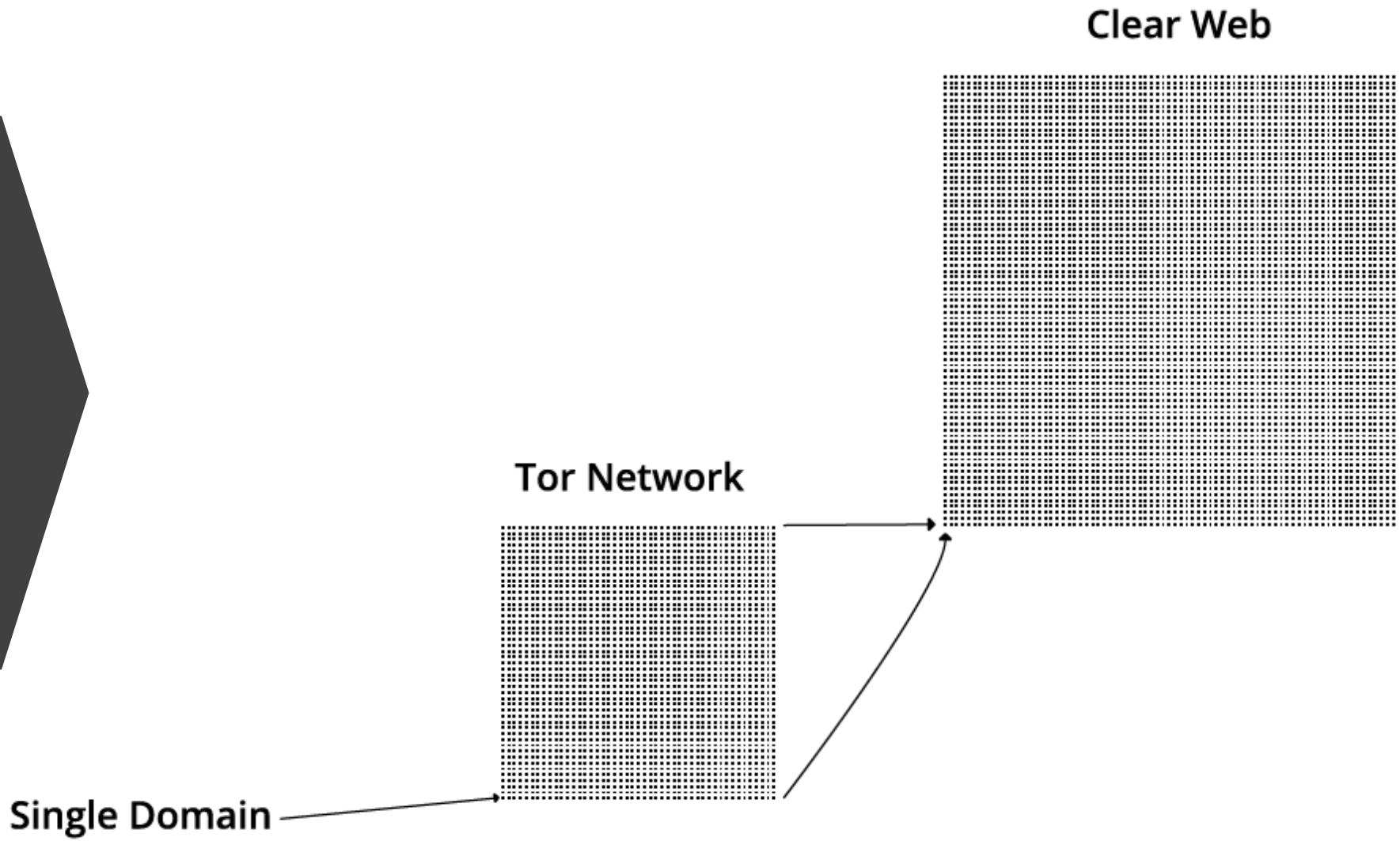
Graphical representation of 8,416 onion domains.

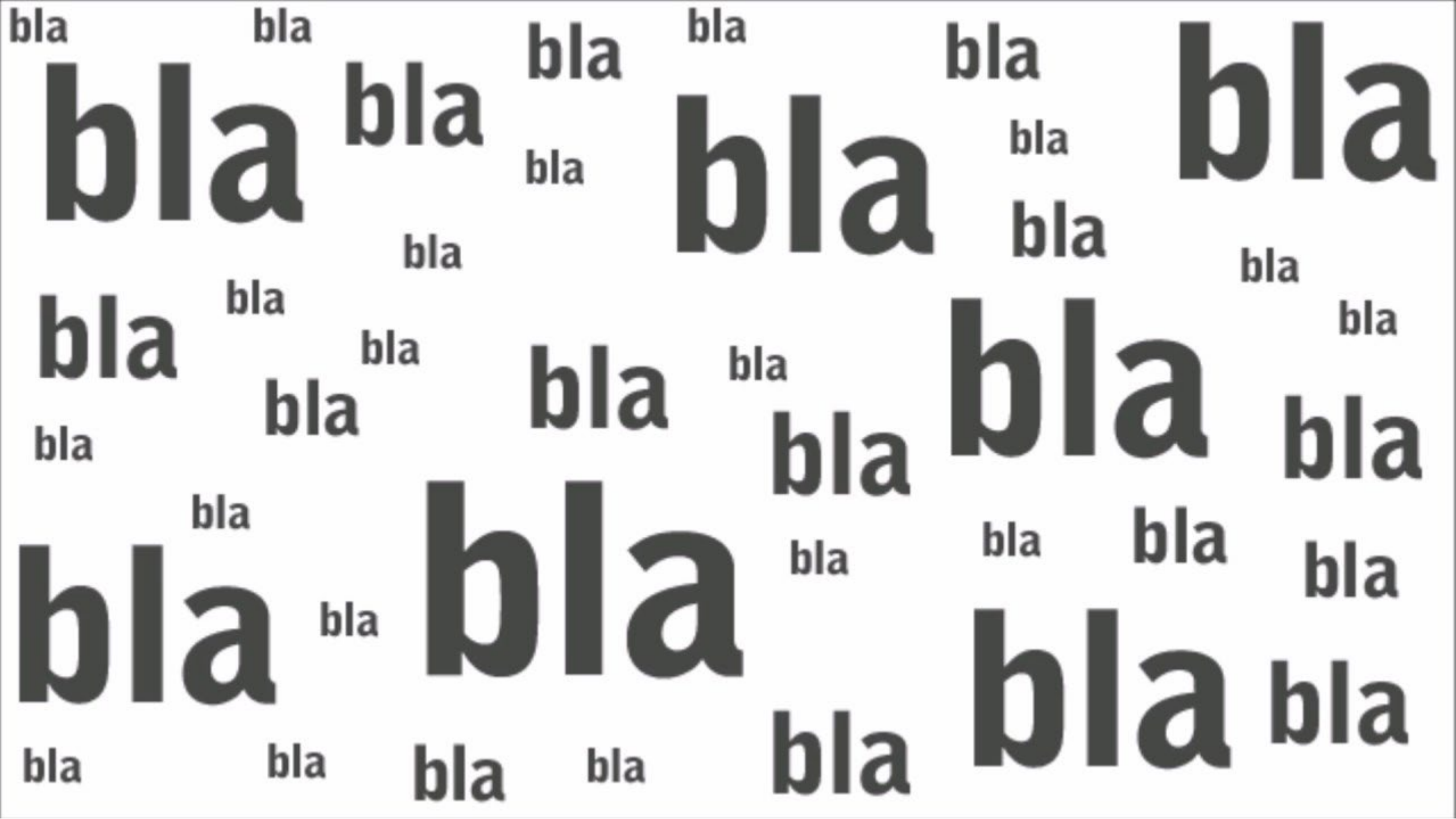
Each point is a site.

From the image you can notice some major site.

JADS Jheronimus Academy of Data Science

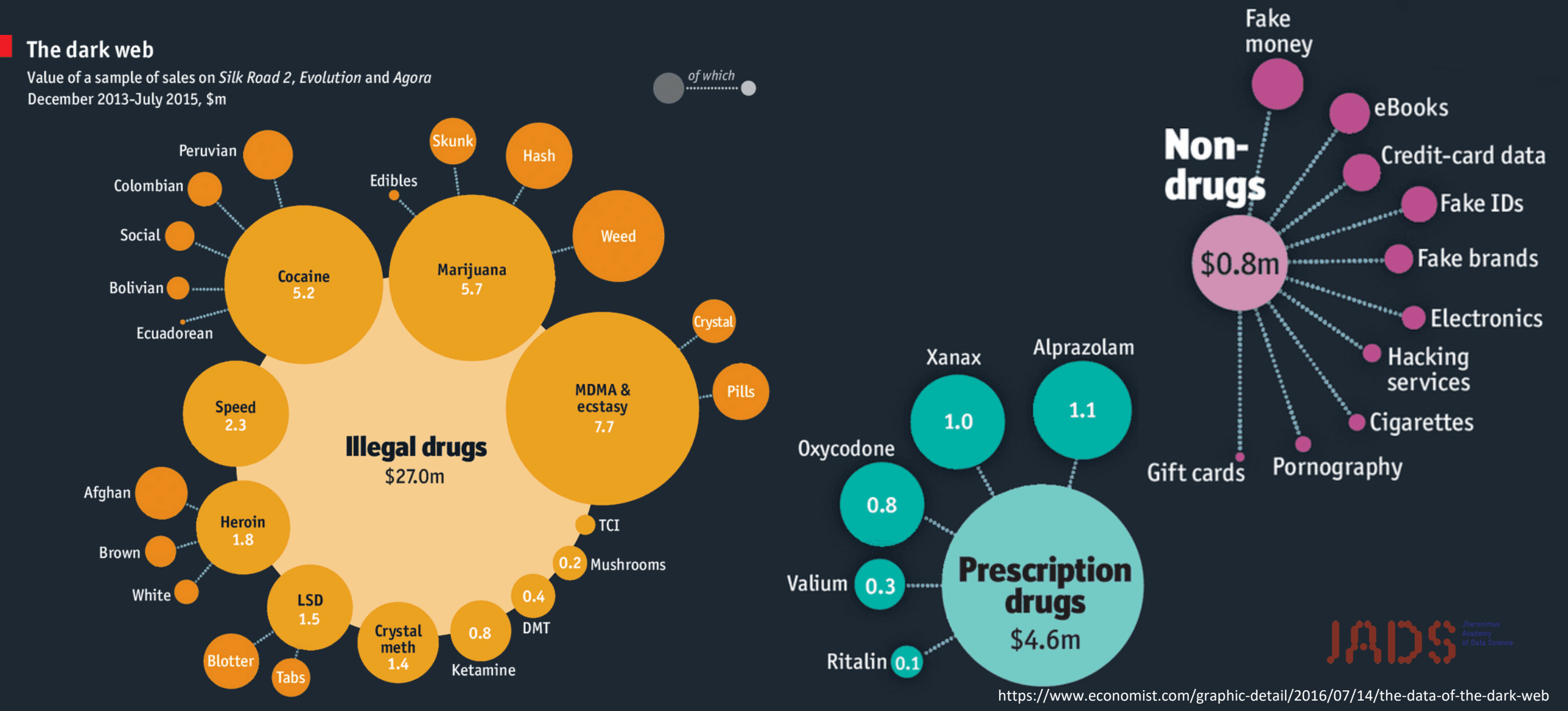
Dark Web Vs. Clear Web




bla

EVERYBODY
38
CALM DOWN

The Economist: Dark economy $$



https://www.economist.com/graphic-detail/2016/07/14/the-data-of-the-dark-web

Dark economy $$

In 2021, Darknet markets made $2.1 billion in cryptocurrency.
Over $1.8 billion of this revenue was generated from drug sales, while the remaining $300 million came from fraud shops. In comparison, Darknet market revenue in 2020 was around $1.8 billion, and approximately $1.4 billion in 2019.

JADS Jheronimus Academy of Data Science

https://vpnalert.com/resources/darknet-statistics/

Dark economy $$

In 2021, Darknet markets made $2.1 billion in cryptocurrency.
Over $1.8 billion of this revenue was generated from drug sales, while the remaining $300 million came from fraud shops. In comparison, Darknet market revenue in 2020 was around $1.8 billion, and approximately $1.4 billion in 2019.

Hydra was the largest Darknet marketplace by revenue in 2021.
Hydra, the Darknet market exclusively tailored for Russian-speaking users, generated over 80% of the total Darknet revenue in 2021.

JADS Jheronimus Academy of Data Science

https://vpnalert.com/resources/darknet-statistics/

Dark economy $$

In 2021, Darknet markets made $2.1 billion in cryptocurrency.
Over $1.8 billion of this revenue was generated from drug sales, while the remaining $300 million came from fraud shops. In comparison, Darknet market revenue in 2020 was around $1.8 billion, and approximately $1.4 billion in 2019.

Hydra was the largest Darknet marketplace by revenue in 2021.
Hydra, the Darknet market exclusively tailored for Russian-speaking users, generated over 80% of the total Darknet revenue in 2021.

The average value of a Darknet drug transaction increased in 2021.
In 2016, the average drug transaction on Darknet drug sites was $160, rising to over $490 worth of cryptocurrency in 2021.

JADS Jheronimus Academy of Data Science

https://vpnalert.com/resources/darknet-statistics/

Dark economy $$

In 2021, Darknet markets made $2.1 billion in cryptocurrency.
Over $1.8 billion of this revenue was generated from drug sales, while the remaining $300 million came from fraud shops. In comparison, Darknet market revenue in 2020 was around $1.8 billion, and approximately $1.4 billion in 2019.

Hydra was the largest Darknet marketplace by revenue in 2021.
Hydra, the Darknet market exclusively tailored for Russian-speaking users, generated over 80% of the total Darknet revenue in 2021.

The average value of a Darknet drug transaction increased in 2021.
In 2016, the average drug transaction on Darknet drug sites was $160, rising to over $490 worth of cryptocurrency in 2021.

Direct buyer-seller drug transactions on the Darknet increased in 2021.
More buyers were doing business with sellers directly and bypassing Darknet markets in 2021. Direct buyer-vendor transactions amounted to less than $25 million in 2016, rapidly growing to over $100 million in 2021.

JADS Jheronimus Academy of Data Science

https://vpnalert.com/resources/darknet-statistics/

Dark economy $$

In 2021, Darknet markets made $2.1 billion in cryptocurrency.
Over $1.8 billion of this revenue was generated from drug sales, while the remaining $300 million came from fraud shops. In comparison, Darknet market revenue in 2020 was around $1.8 billion, and approximately $1.4 billion in 2019.

Hydra was the largest Darknet marketplace by revenue in 2021.
Hydra, the Darknet market exclusively tailored for Russian-speaking users, generated over 80% of the total Darknet revenue in 2021.

The average value of a Darknet drug transaction increased in 2021.
In 2016, the average drug transaction on Darknet drug sites was $160, rising to over $490 worth of cryptocurrency in 2021.

Direct buyer-seller drug transactions on the Darknet increased in 2021.
More buyers were doing business with sellers directly and bypassing Darknet markets in 2021. Direct buyer-vendor transactions amounted to less than $25 million in 2016, rapidly growing to over $100 million in 2021.

The Darknet drug market was worth over $27 million in 2022.
Over 60% of the Darknet markets deal exclusively with drugs. Popular drugs in these Darknet marketplaces include MDMA, Ecstasy, marijuana, cocaine, heroin, crystal meth, Xanax, oxycodone, valium, Ritalin, and alprazolam.

JADS Jheronimus Academy of Data Science

https://vpnalert.com/resources/darknet-statistics/

Price List

Social Media Account

Hacked Gmail Account $60
Instagram followers x1000 $2

Forged Documents

Maltese Passport $4000
French Passport $3000
Fake US green card $450

Credit Card

Credit card details, account balance up to $5K. $110
UK hacked credit card with CCV $20.
Cloned Mastercard with PIN $20

Malware

Premium-quality, per 1000 installs $4500.
Android OS per 1000 installs $600. Medium quality, 70% success rate $75

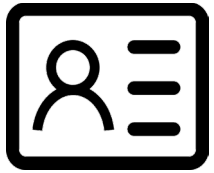
https://www.privacyaffairs.com/dark-web-price-index-2023/

Money, data, and violence

Silk Road made $213 million trade before going down in dust: The name ‘Silk Road’ crops in almost every discussion related to darknet marketplaces. It is one of the first forums to bring together a large number of buyers and sellers of illegal items together on the Dark Web.

The Dark Web made FBI the second-largest owner of Bitcoins: As the authorities cracked down the operations of Silk Road, the subsequently confiscated a lot of bitcoins from various accounts of Ulbricht. They got 144,000 bitcoins from Ulbricht’s rented servers in Iceland.

FBI has still done nothing of these bitcoins, and their current aggregate value is around $1.2 billion. It will be interesting to know how FBI plans to deal with all those digital assets.



Information from 620 million accounts was available for sale on the dark web: We often come across the news of hackers getting into website servers and stealing away account information of millions of users. If you ever wondered, what would one do with these millions of accounts, then selling them is one of the answers.

A report showed that account information stolen from 16 websites, making up for 620 million user accounts, was on sale on the darknet. Not all the compromised websites knew that their servers were breached.

Allegedly, there are **hitmen for hire** on the dark web: There are websites on the dark web that claim to do all kinds of dirty jobs for customers, including taking lives.

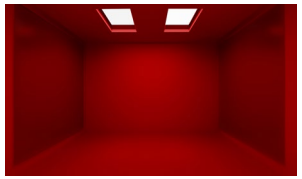
However, all of them turn out to be a scam to rob people of their bitcoins. Once the user transfers the digital currency to the site’s wallet, there are no killings but just some false promises.

JADS Jheronimus Academy of Data Science

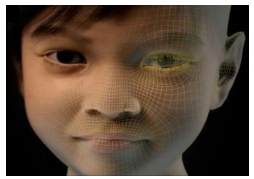
Money, data, and violence

Darknet is a human trafficking marketplace: It's an issue not discussed very often, but that should not undermine its importance. Of all the things that are bought and sold on the dark web, human trafficking is its ugliest form. It is a huge marketplace, and people of all age and sex are a victim of this.

Dark web offers the layer of anonymity to such traffickers, making it easier for them to stay away from the reach of law.



People pay to live stream violence on the dark web: Adding to the list of disturbing things on the dark web, you might be surprised to know of the possibility of the existence of red rooms on darknet. Red rooms are supposedly meant to live stream pornography, usually involving child.



terre des hommes
stops child exploitation

A child pornography website with about 90,000 users got busted: Authorities across the globe have found it difficult to put an end on the regulation of child pornographic content on the internet. Darknet turns out to be a huge roadblock in the endeavor. *The authorities behind the bust reported that the forum had almost 90,000 users from across the globe.*

Terrorist organizations use the dark web to recruit more terrorists: Terrorist groups are getting increasingly active on dark web to stay away from the reach of authorities. It is a difficult task first to find the darknet website operated by such groups, then to find out who is behind the website and identify those are actively participating on the website.

JADS Jheronimus Academy of Data Science

Enter
DARKNET
PgUp
PgDn
End

CRATOR

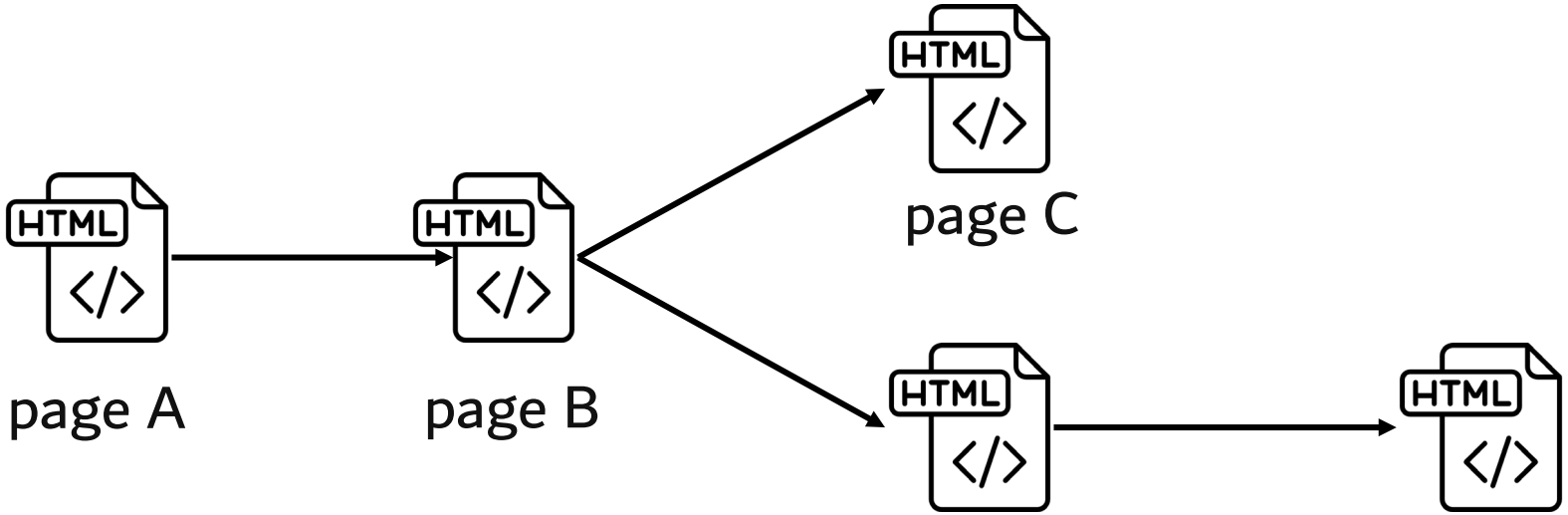
What's a crawler?

"Web Crawler is an Internet bot that systematically browses the World Wide Web and that is typically operated by search engines for the purpose of Web indexing (web spidering)."

Crawler Strategies

The web can be viewed as an extensive directed graph, with **pages** as **nodes** and **hyperlinks** as the **edges** connecting these pages.

Need to navigate the graph to download and extract all the possible pages.

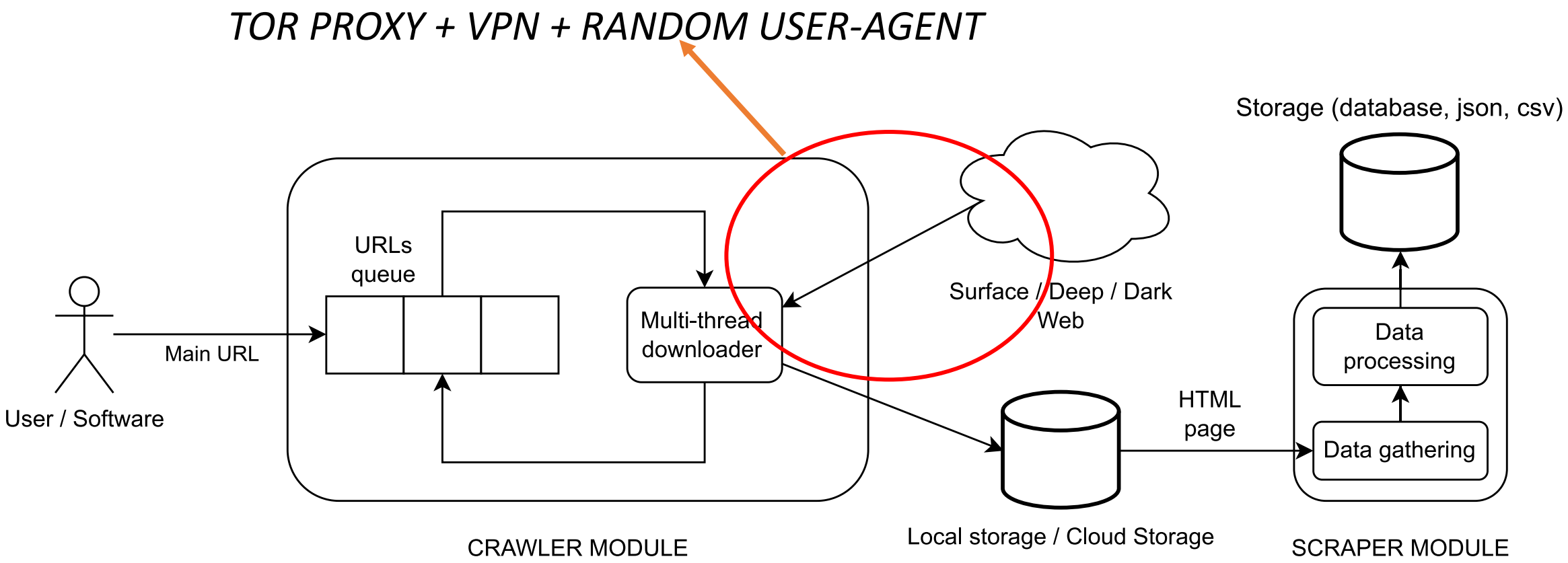


JADS Jheronimus Academy of Data Science

Crawling the Dark Web - Challanges

- Send requests under Tor in a Python script.
- Avoid making excessive requests
- Handle captchas and other security checks

Dark Web crawler architecture

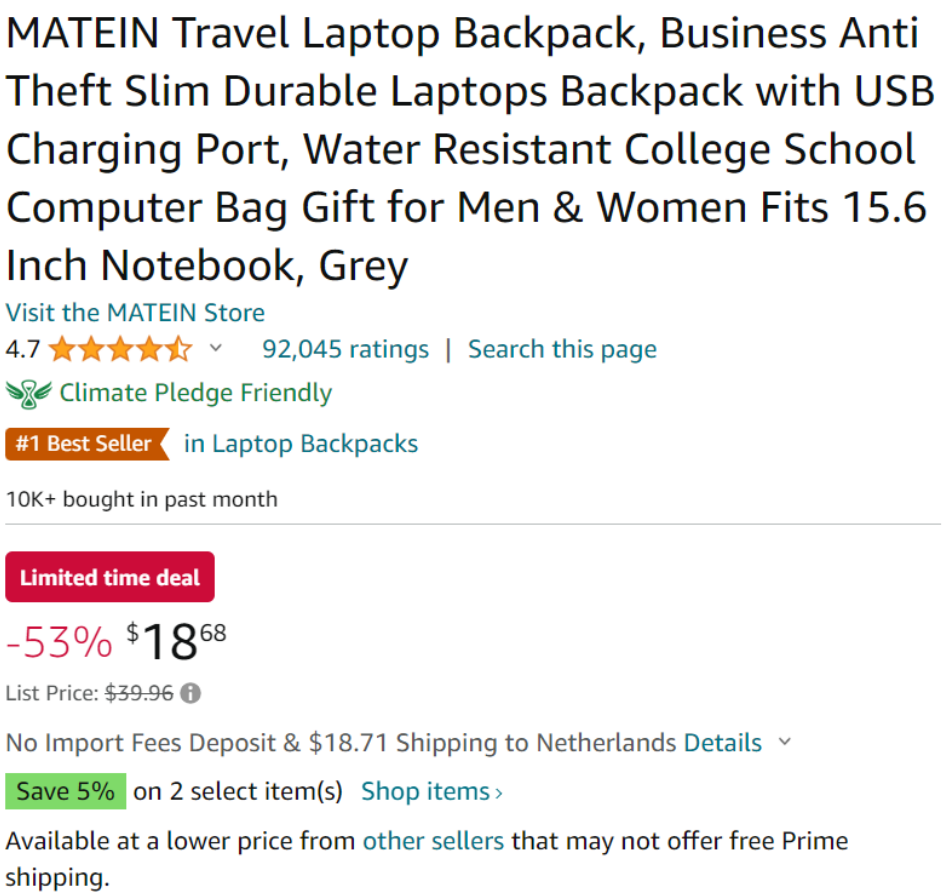


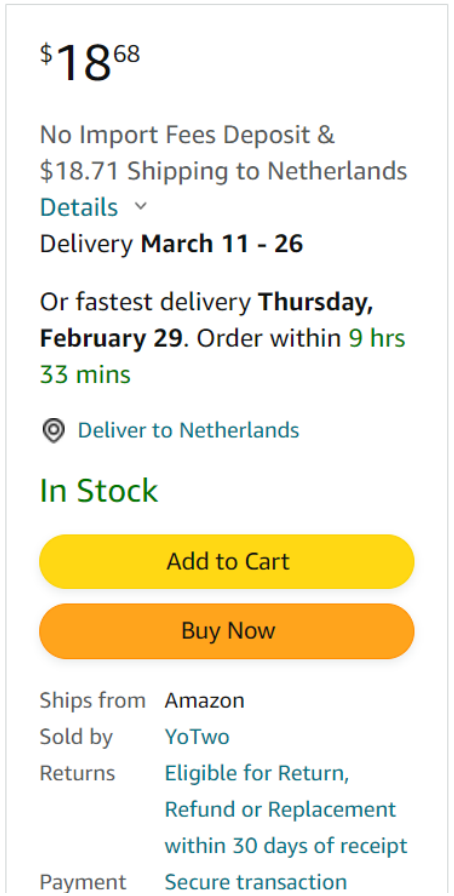
JADS Jheronimus Academy of Data Science

What's a scraper?

"Web scraping is the process of using bots to extract content and data from a website."

Data scraper: example





Title: MATEIN Travel Laptop…

Rating: 4.7

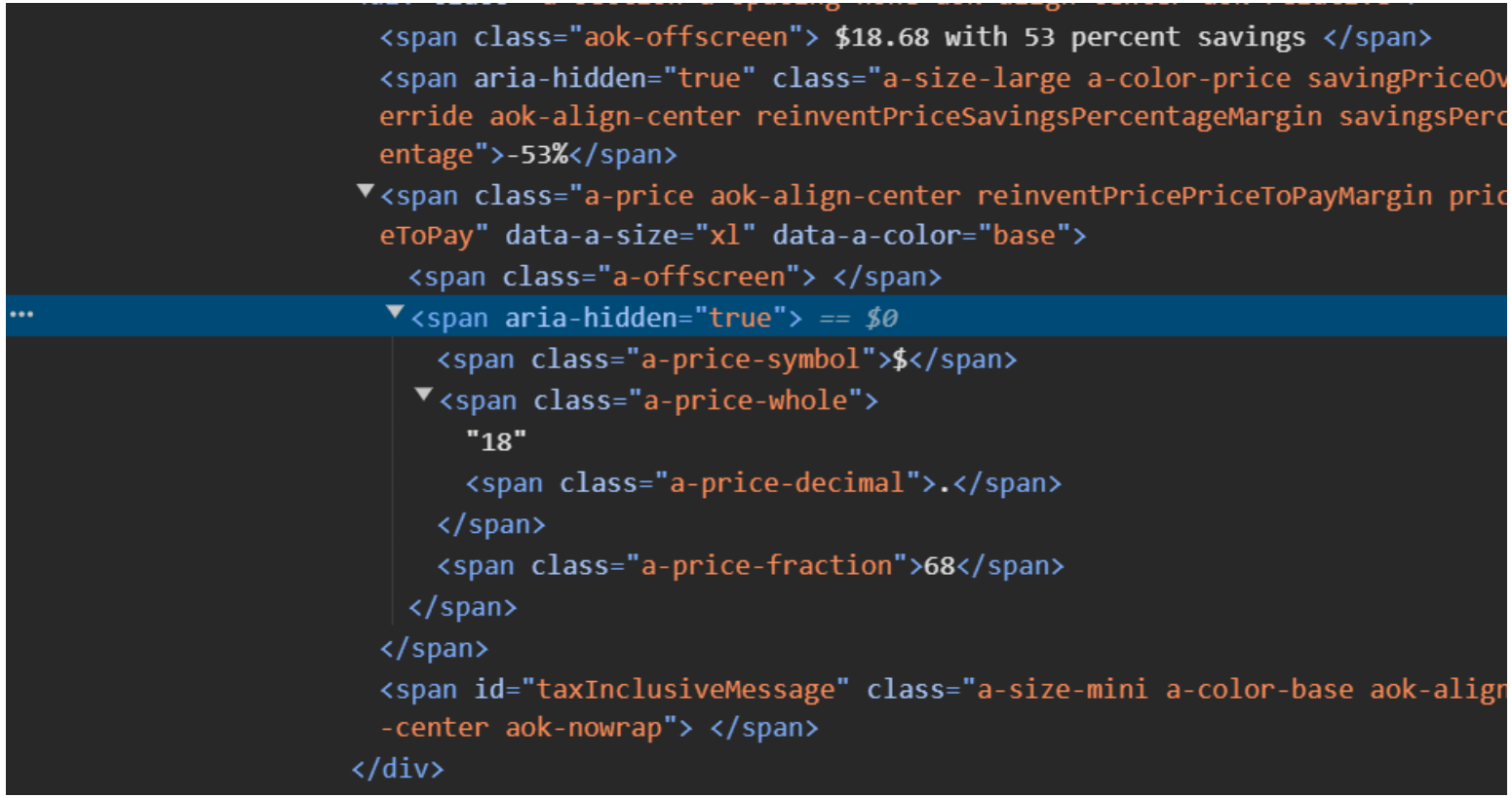
Price: 18.58$

Ships from: Amazon

Ships to: YoTwo

JADS Jheronimus Academy of Data Science

Data scraper: example



Price scraping rule

Tag: span

Class:
a-price aok-align-center reinventPricePriceToPayMarg in priceToPay

JADS Jheronimus Academy of Data Science

CRATOR and SENSEI

Solutions (?)

Terre des hommes

Proteggiamo i bambini insieme

INTERPOL

PROTECT

ANITA

ADVANCED TOOLS FOR FIGHTING ONLINE ILLEGAL TRAFFICKING

MAGNETO

Fighting Against Crime and Terrorism

European Commission

Human Trafficking
EU Projects and Funding (274)

JADS Jheronimus Academy of Data Science

Thank You

Contact

Giuseppe Cascavilla

g.cascavilla@jads.nl