



An introduction to Open Source Intelligence

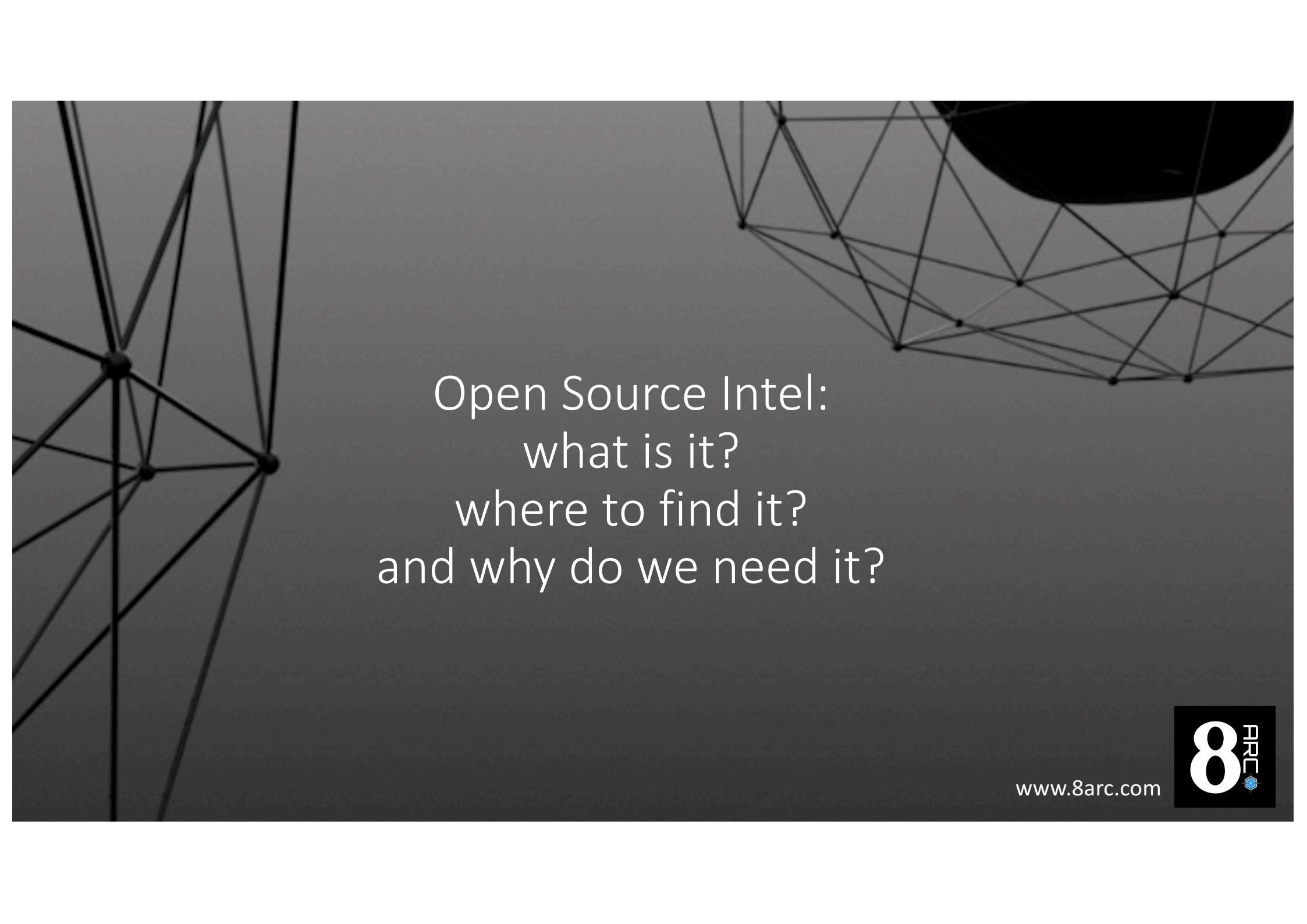
www.8arc.com



Introduction

www.8arc.com





Open Source Intel:
what is it?
where to find it?
and why do we need it?

www.8arc.com





Data

Information

Intelligence

www.8arc.com



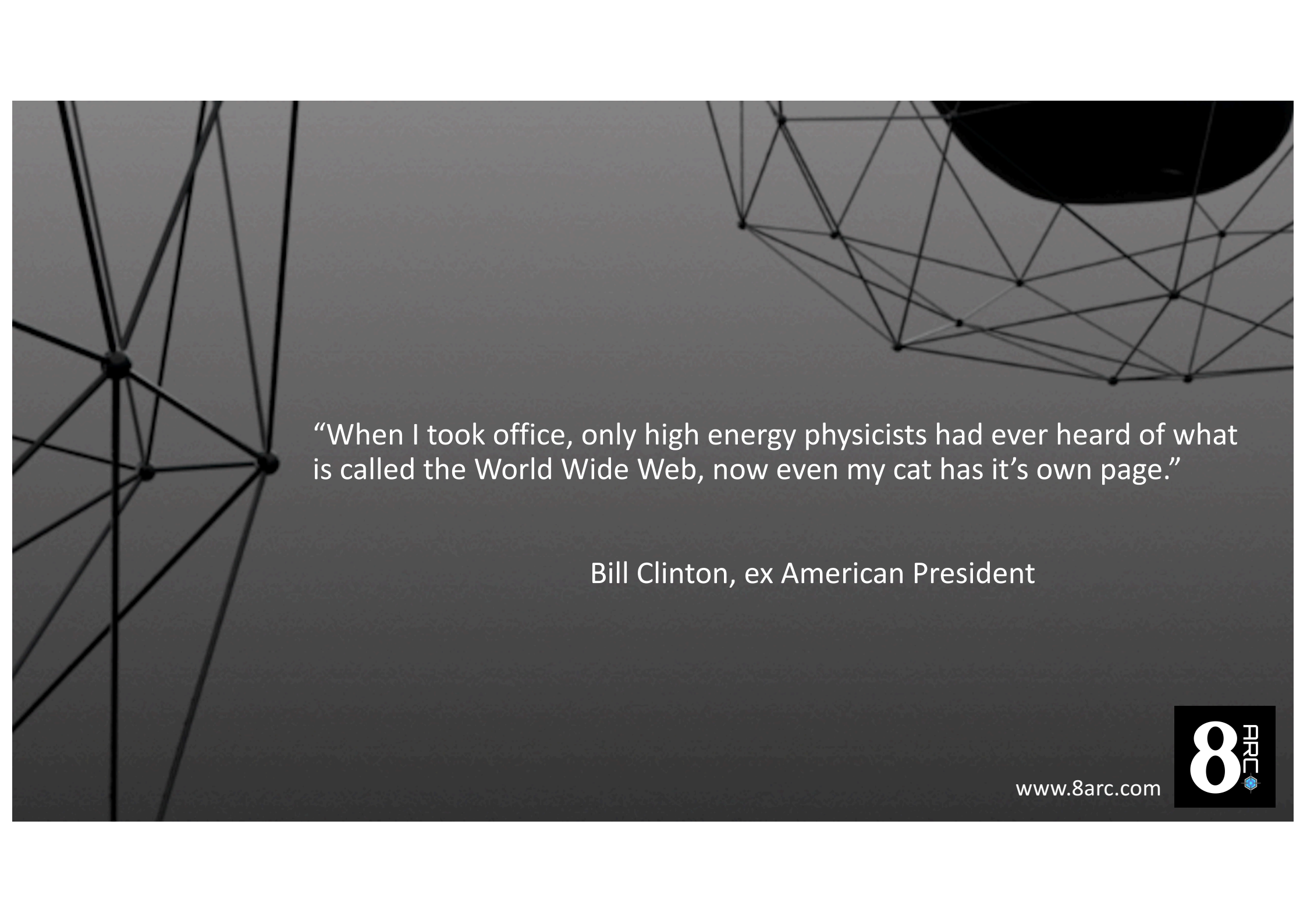
Closed vs Open Source

Closed

- Internal Corporate Information
- Intelligence Database
- Risk Management Documents
- Partner (Agency) Data
- Profiles: current + previous
- Website Analytics (Internal)
- BI Data
- Financial Data
- Intellectual Property
- CRMs
- **HR records**

Open

- Accounts
- Whois
- Google (search engines)
- Public facing documents
- News Channels
- **Peer to Peer Forum**
- Website Analytics (External)
- Social Media
- Company Information
- Personnel details

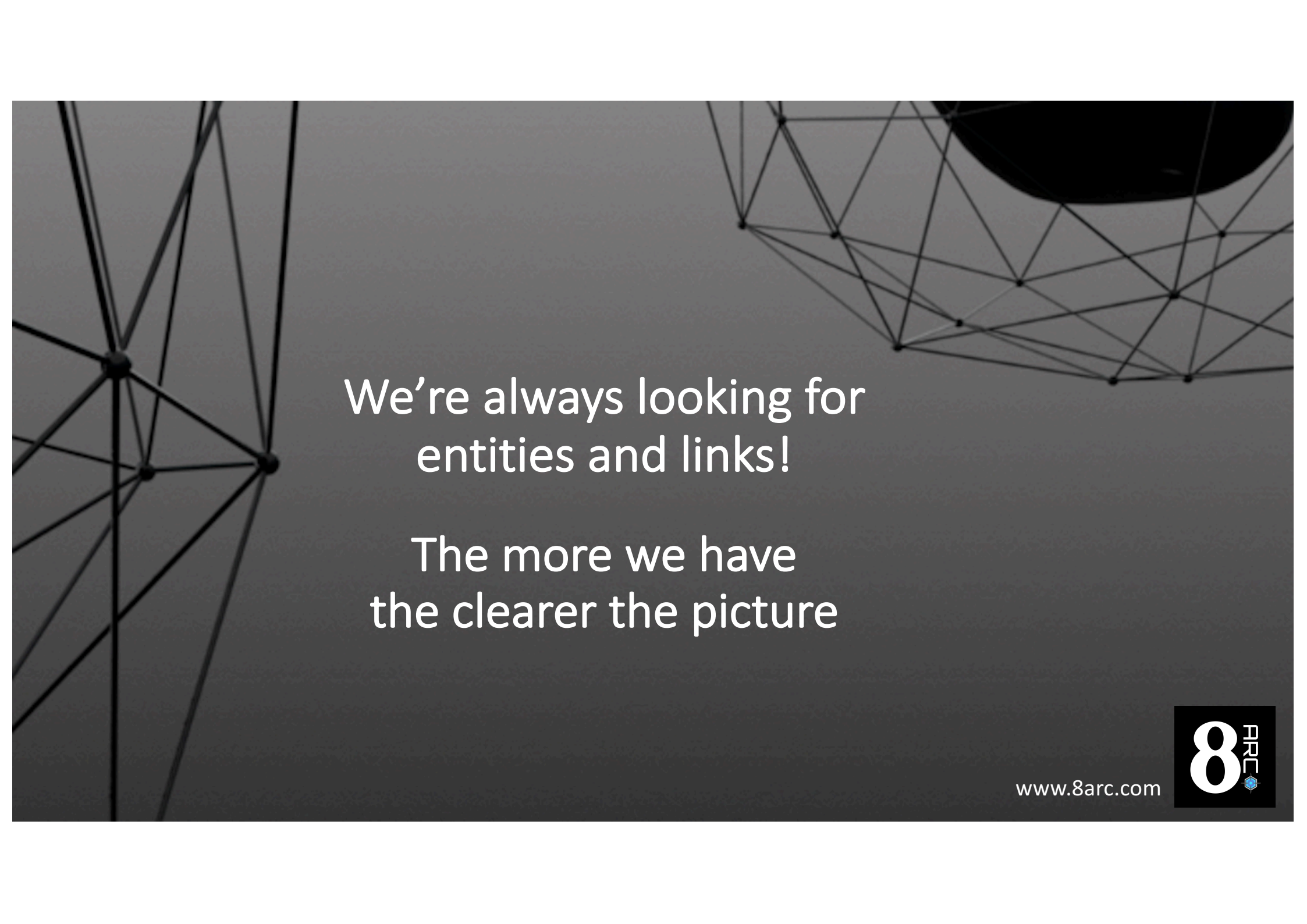


“When I took office, only high energy physicists had ever heard of what is called the World Wide Web, now even my cat has it’s own page.”

Bill Clinton, ex American President

www.8arc.com





We're always looking for
entities and links!

The more we have
the clearer the picture

www.8arc.com



Investigation Environment

www.8arc.com



Things to consider?

- **Stand alone network/machine**
- Dedicated broadband – dynamic IP address (mobile broadband)
- Back up broadband & network/machine
- Standard software – anti virus, firewall, IDS / IPS / Operating System, browser etc.
- Specialist software – OSINT / intelligence / evidential software & capture tools
- **Online legends**
- Visualisation Tools
- Build a jumpkit

Also consider...

- **Define a set file structure**
- Set a file naming convention
- Keep an investigation log / workbook
- **Investigation Plan**
- Risk assessment
- VPNs & Proxies (AWS)
- Set your standpoint on anonymity

Anonymity

www.8arc.com



Anonymity & Digital Footprints

- Digital footprints are the trail left by interactions with digital environments
- These interactions are used to profile you
- To footprint or not to footprint?

Operating Systems Pros & Cons

- Linux
- Windows
- Mac OS
- Chrome
- IOS
- Android
- (Virtual Machines)

Browsers, Dev Options, Add-ons

www.8arc.com



Browsers



Lynx Text Browser

Lynx Information

Lynx

Lynx is a text browser for the World Wide Web. Lynx 2.8.3 runs on Un*x, VMS, Windows 95/98/NT but not 3.1 or 3.11, on DOS (386 or higher) and OS/2 EMX. The current developmental version is also available for testing. Ports to Mac are in beta test.

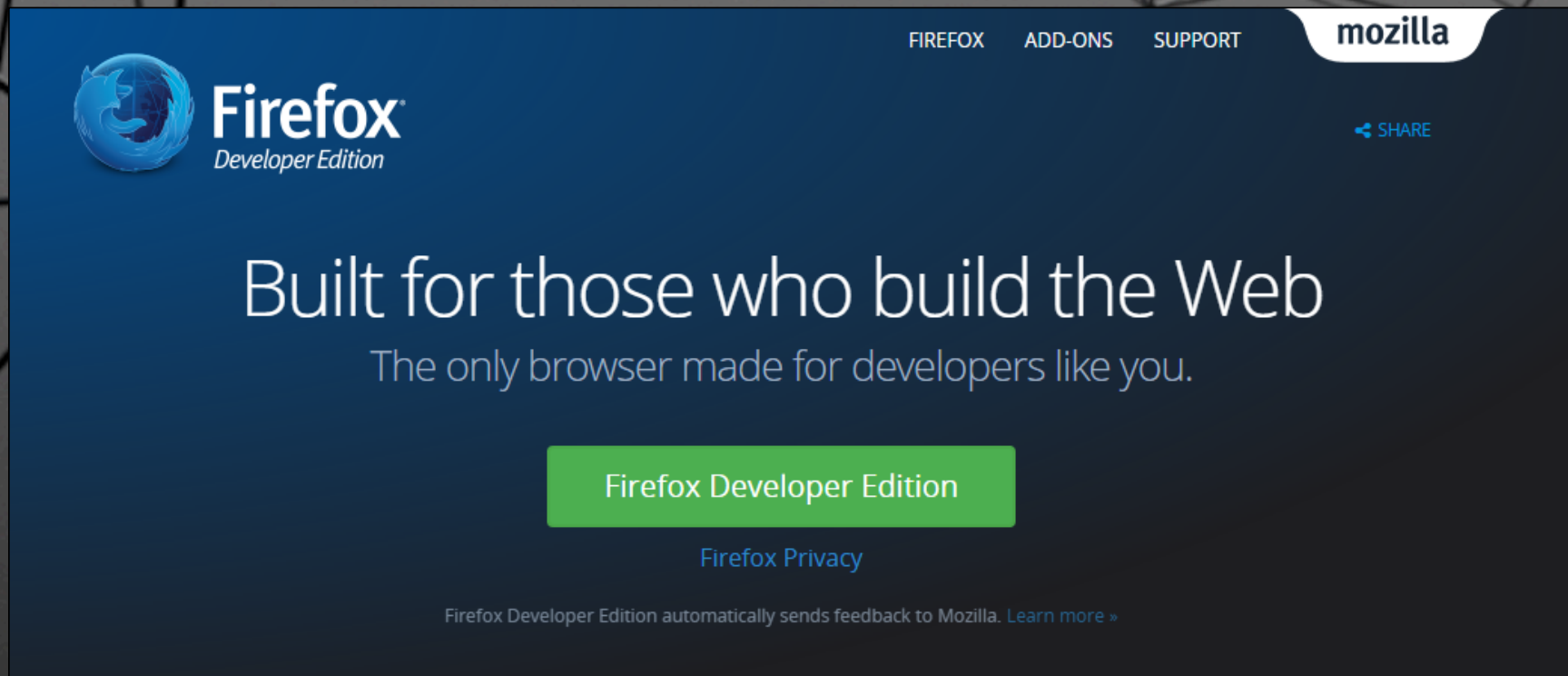
- * Many user questions are answered in the online help provided with Lynx. Press the '?' key to find this help.
- * If you are encountering difficulty with Lynx you may write to lynx-dev@sig.net. Be as detailed as you can about the URL where you were on the Web when you had trouble, what you did, what Lynx version you have (try '=' key), and what OS you have. If you are using an older version, you may well need to upgrade.

Maintained by lynxdev@browser.org.

Commands: Use arrow keys to move, '?' for help, 'q' to quit, '<' to go back.

Arrow keys: Up and Down to move. Right to follow a link; Left to go back.
H)elp O)ptions P)rint G)o M)ain screen Q)uit /=search [delete]=history list

Browsers Dev Options

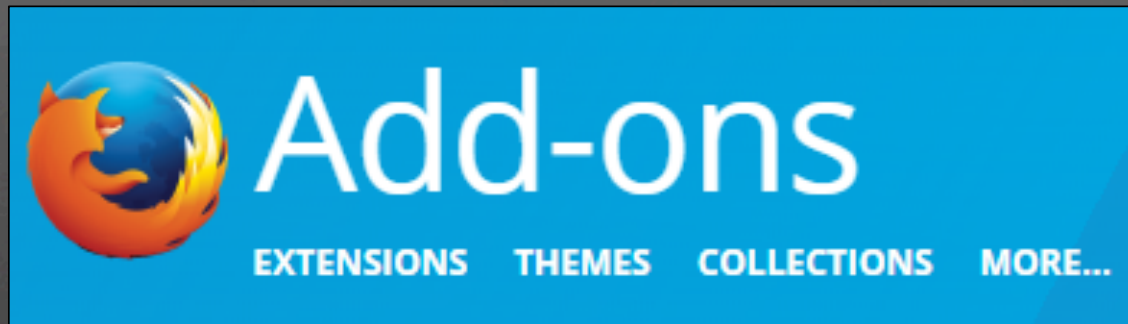


The screenshot shows the Firefox Developer Edition website. At the top right, there are navigation links for 'FIREFOX', 'ADD-ONS', and 'SUPPORT', followed by the 'mozilla' logo. On the left, the Firefox logo is accompanied by the text 'Firefox Developer Edition'. A 'SHARE' button is visible on the right. The main heading reads 'Built for those who build the Web' with the subtext 'The only browser made for developers like you.' Below this is a prominent green button labeled 'Firefox Developer Edition' and a link for 'Firefox Privacy'. At the bottom, a small note states 'Firefox Developer Edition automatically sends feedback to Mozilla. Learn more »'.

www.8arc.com



Browser Add-Ons



www.8arc.com




Demo - Lightbeam

about site info filters credits

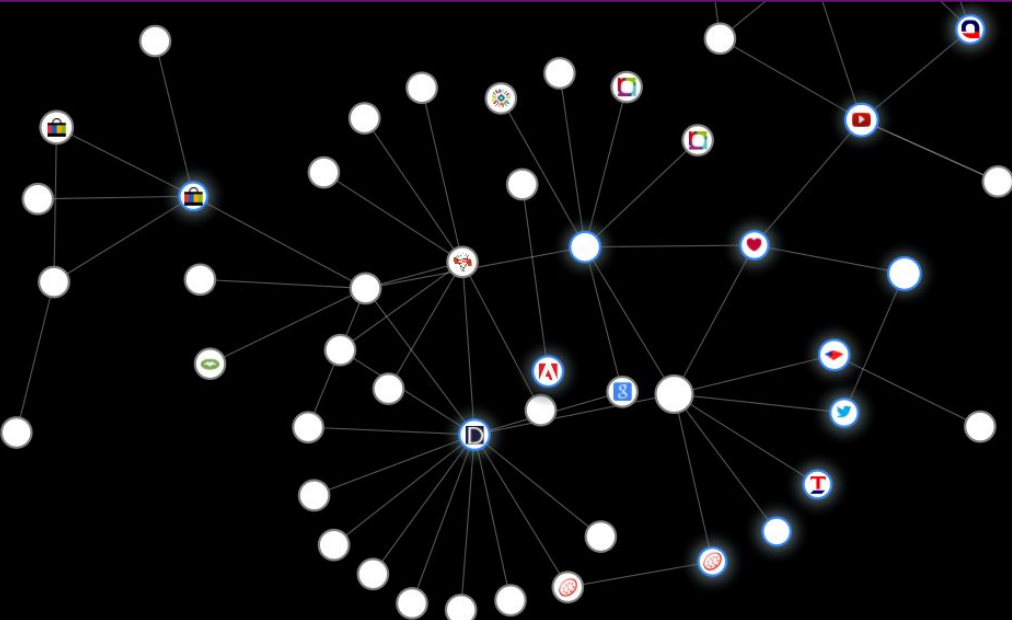
- Reset
- Export
- Zoom In
- Zoom Out
- Hide Panel

Mouse over any circle to see how that site uses third-party cookies.

 Mediamath

The site mathtag.com is potentially aware of your visits to the following websites.

- visualdna.com
- debenhams.com



Add-ons – a few more

- Exif Viewer – (Alan Raskin)
- FireShot
- Unshorten.it!
- User Agent Overrider
- Live http headers
- Cookies Manager+

If you don't like something,
Change it!

Windows + R %APPDATA%

then Mozilla – Firefox - Profiles

Select the right profile

Select Extensions

Add-Ons will be in an xpi file

Extract as you would a zip file

www.8arc.com



Capture Tools

www.8arc.com



Snagit / Camtasia

 TechSmith®

www.8arc.com



FireShot



www.8arc.com



Httrack



www.8arc.com



Search Engines

- Google
- Bing
- Yahoo
- Duckduckgo
- Dogpile
- Httrack?

A dark gray background featuring a wireframe sphere structure composed of black lines and dots, resembling a geodesic dome or a network diagram. The sphere is partially visible, with the top right portion cut off by the edge of the image.

Google Hacking

www.8arc.com



Google Hacking

- **Cache:**

- Intitle:

- Allintitle:

- Inurl:

- Allinurl:

- Filetype: (or ext:)

- Allintext:

- Site:

- Link:

- Inanchor:

- Daterange:

- Numrange:

- View-source

Google Hacking

- **Cache:**

- **'&strip=1'** used with the **'cache:'** operator

- String search by use of speech marks ""

- Logical (Boolean) Operators:

- 'AND' '+'

- 'NOT' '-'

- 'OR' '|'



Other Google areas of interest:

- News
- Finance
- Groups
- **Images**
- Blogs
- Scholar

www.8arc.com



Google Hacking

Demonstration

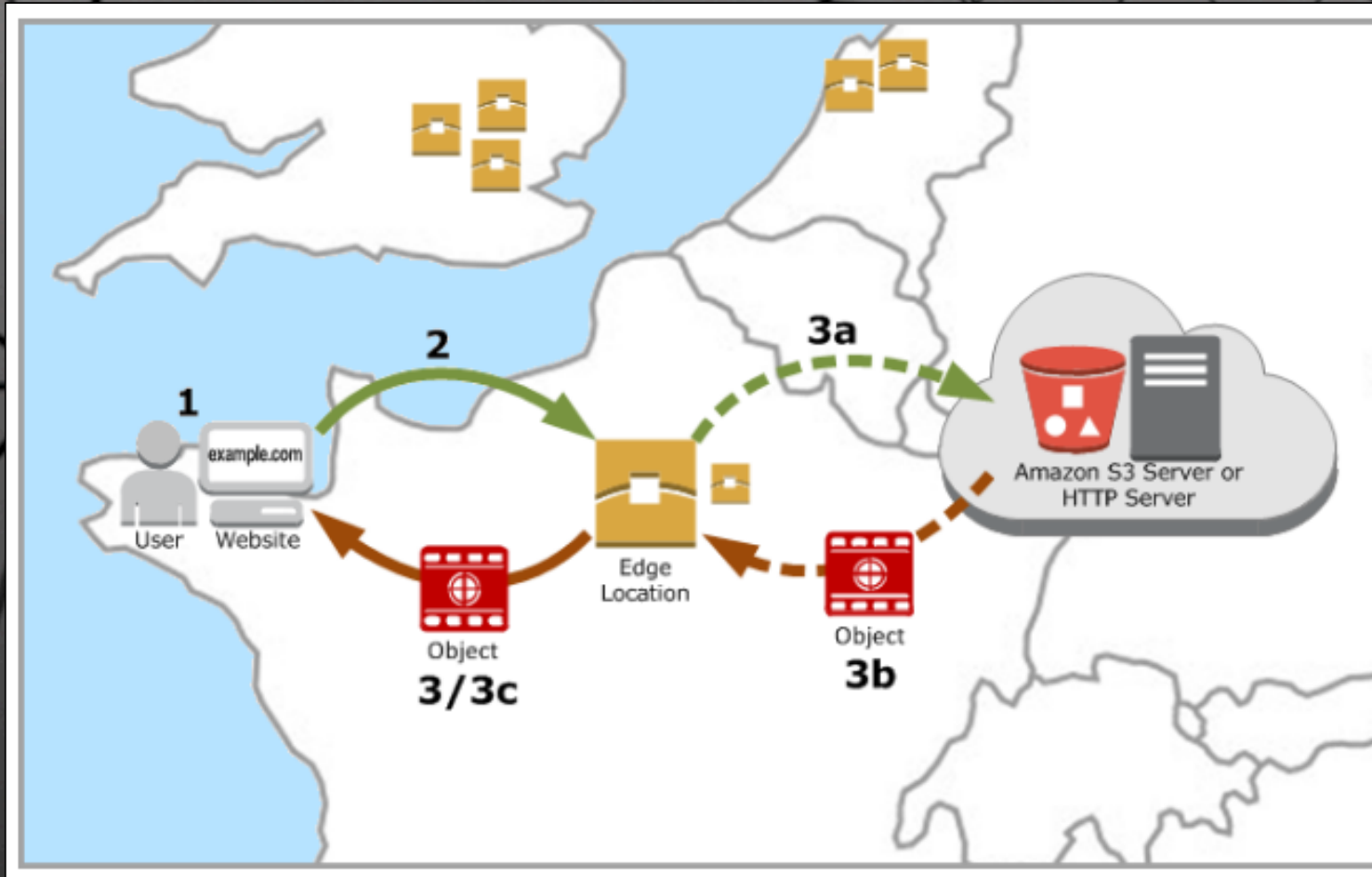
www.8arc.com



Content Delivery Networks

- A system of distributed servers that accelerates delivery of websites, APIs, video content or other web assets.

Example – AWS CloudFront



Building a Jump Kit

www.8arc.com



Robtex



www.8arc.com



Domain Tools



DOMAINTOOLS

www.8arc.com



A few more favs

- Companies House
- Companycheck.co.uk
- Namesense.com
- SameID.net
- Builtwith.com
- Majestic.com (SEO Backlink Checker)

www.8arc.com



PortableApps



PORTABLEAPPS.COM
YOUR DIGITAL LIFE, *ANYWHERE*™

www.8arc.com



Automation & Visualisation

www.8arc.com



Maltego



www.8arc.com





Man & Machine

Machines are good at automation = transforms

Humans are good at pattern recognition = visual graph

www.8arc.com

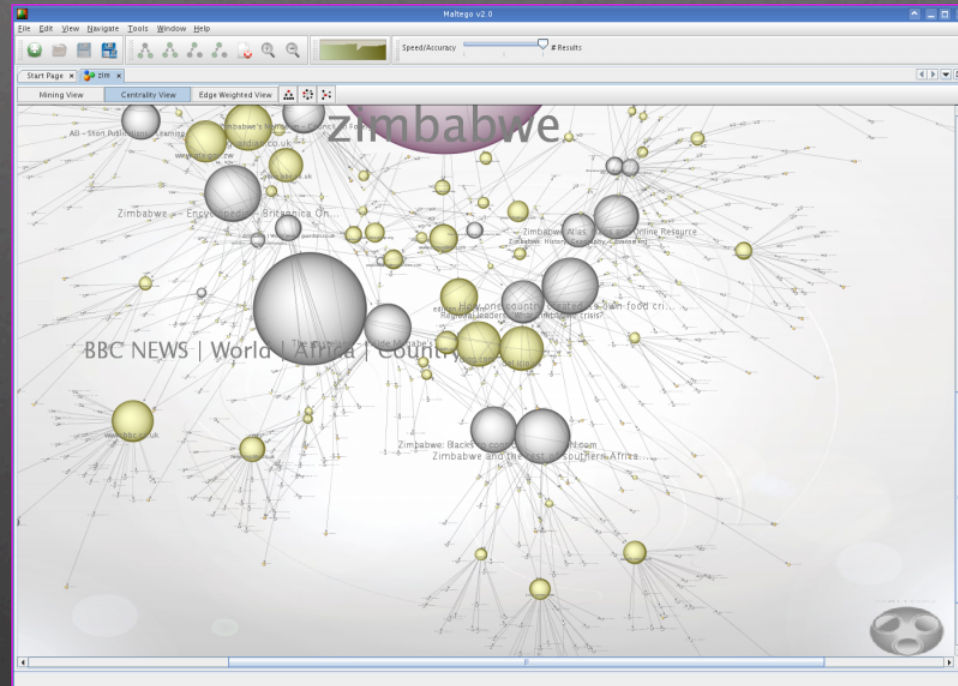


So we have...

Maltego concept:

- Entities: 'things' – information type
 - DNS Name / Person / Phone number / more...
- Transforms: moves one type of thing to another type
 - DNS resolving / Searching / Database access / Deep web

Maltego



Visual Programming



www.8arc.com



Visual Programming via Rapidminer

The screenshot displays the RapidMiner Studio interface. The main workspace shows a process flow with three operators: 'Retrieve Titanic', 'Write Excel', and 'Store'. The 'Store' operator is highlighted with a red border. The left sidebar contains a 'Repository' panel with a list of data sources including 'Titanic (v1)' and 'Titanic Training (v1)', and an 'Operators' panel with a search for 'store' showing various operator categories. The right sidebar shows the 'Parameters' panel for the 'Store' operator and a 'Help' panel with details for the 'Store' operator, including its synopsis: 'This operator stores an IO Object in the data repository.' The bottom status bar indicates 'Activate Wisdom of Crowds' is checked.

Visual Programming



www.8arc.com





connect@8arc.com

Twitter - [@andy8arc](https://twitter.com/andy8arc)

Facebook - [8ARCLTD](https://www.facebook.com/8ARCLTD)

www.8arc.com

