BTSF

Advance internet tools – Pat BEARDMORE

Contract number 2017 96 05 – New Food Investigation Techniques – Phase II - *Course 2b: E-Commerce of food advanced*

European Commission

BTSF Hello – again ☺

- Hands up who I met at the previous course?
- A quick word about my style of presenting
- Don’t just sit there ☺
- Win a mug!!
- We can also chat over lunch and coffee.

BTSF What is advanced?

- Not too advanced
- Still relatively basic
- Takes years to be an expert
- This course is just a taster
- Take from it what you want

BTSF Let’s look at VPNs

- So, what do we remember about our old friend, the IP address?
- How do they help us?
- How do they pose a risk to investigators?

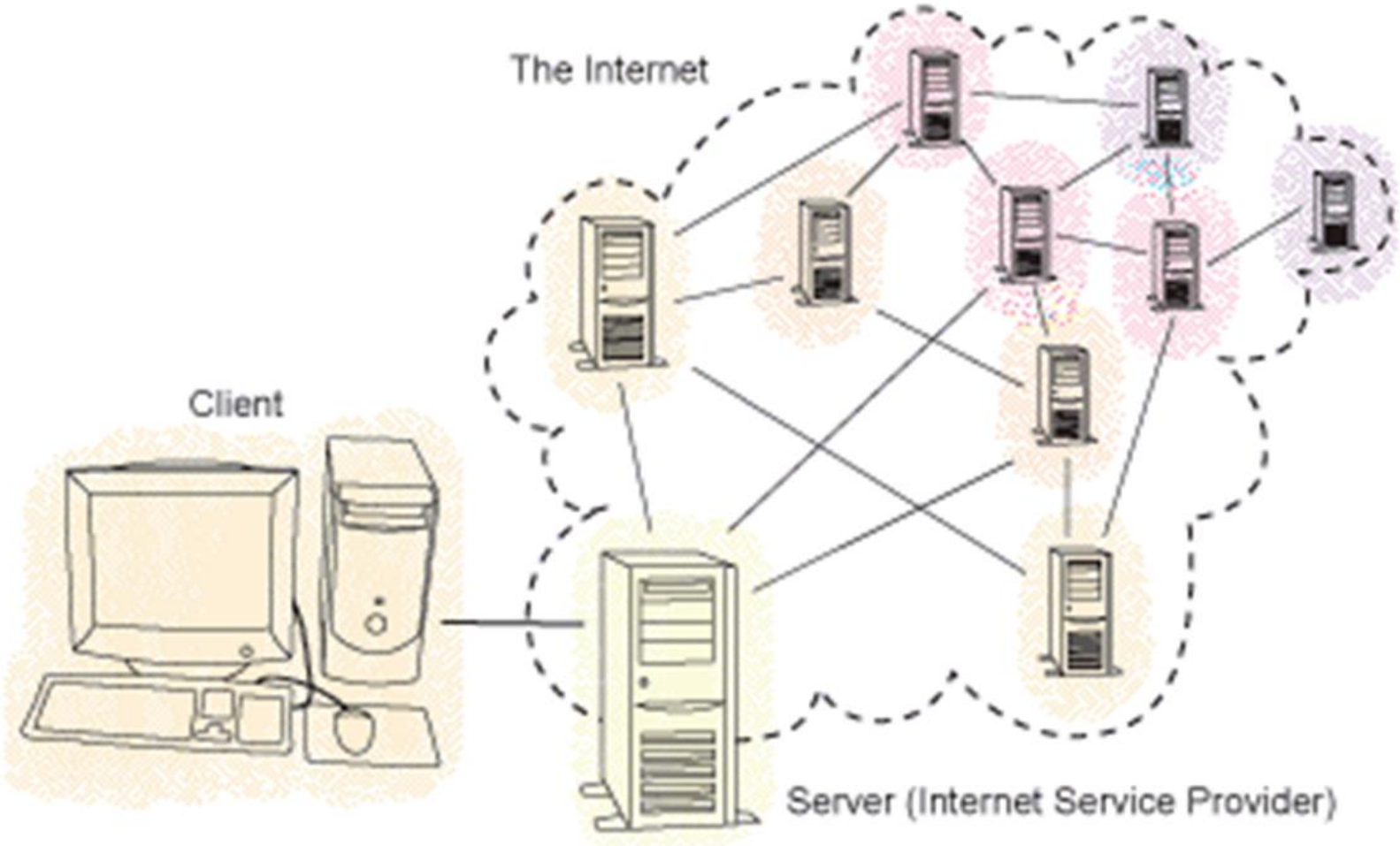
BTSF Let’s look at VPNs

- Virtual Private Network
- A private network over a public network?
- How private? – by using encryption

BTSF Let’s look at VPNs - privacy

European Commission

BTSF



BTSF Advantages of VPNs

- Security
- Login flexibility re geography
- Hides your IP address
- Hides your location
- Appear to be from another country

BTSF Advantages to investigations

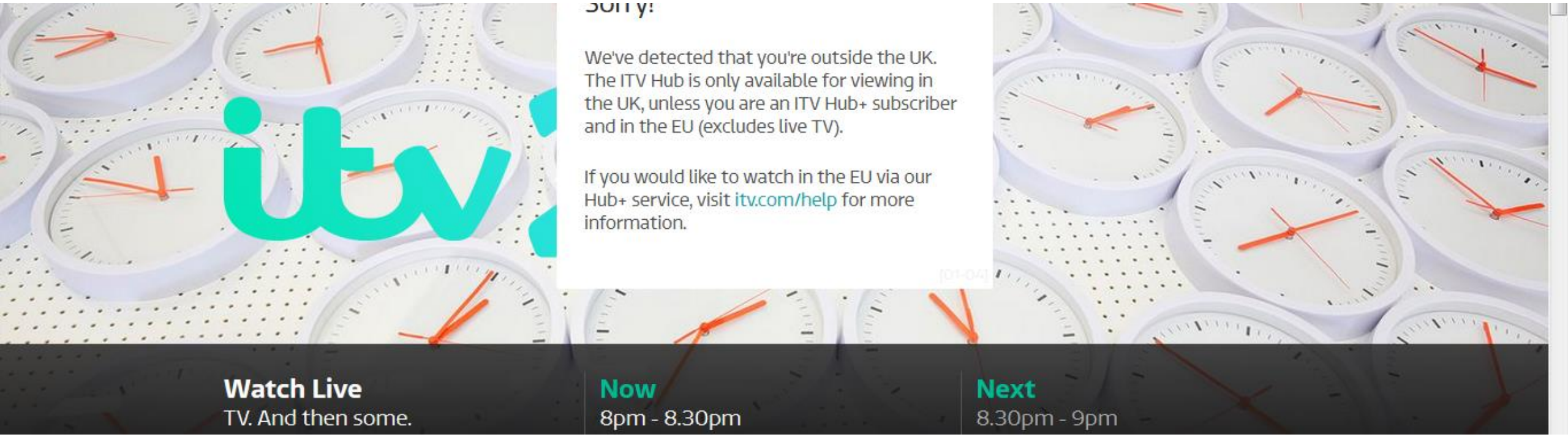
- Do you need a standalone PC?
- Do you need a standalone ISP account?
- It’s a point for discussion
- No right/wrong answer

BTSF It works the other way

- “Bad guys” can use VPNs
- It can hide their IP address
- No longer a “geek” thing
- Becoming much more popular with consumers

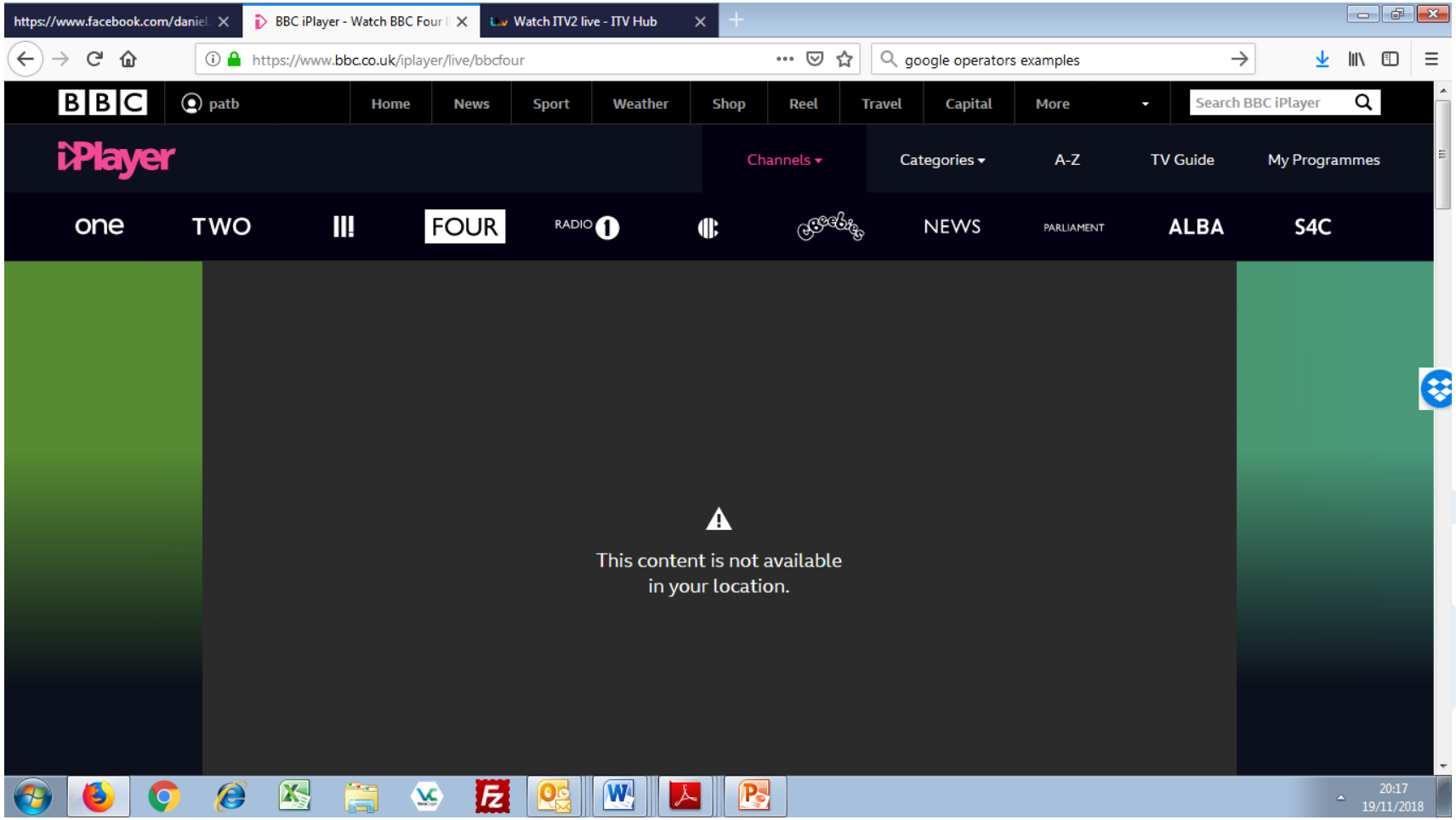
BTSF

Hotel room last night – perfect example



European Commission

BTSF



European Commission

BTSF

Crank up your laptops.
Go to:

www.whatismyipaddress.com

(some websites update their content based on the location of the IP address)

European Commission

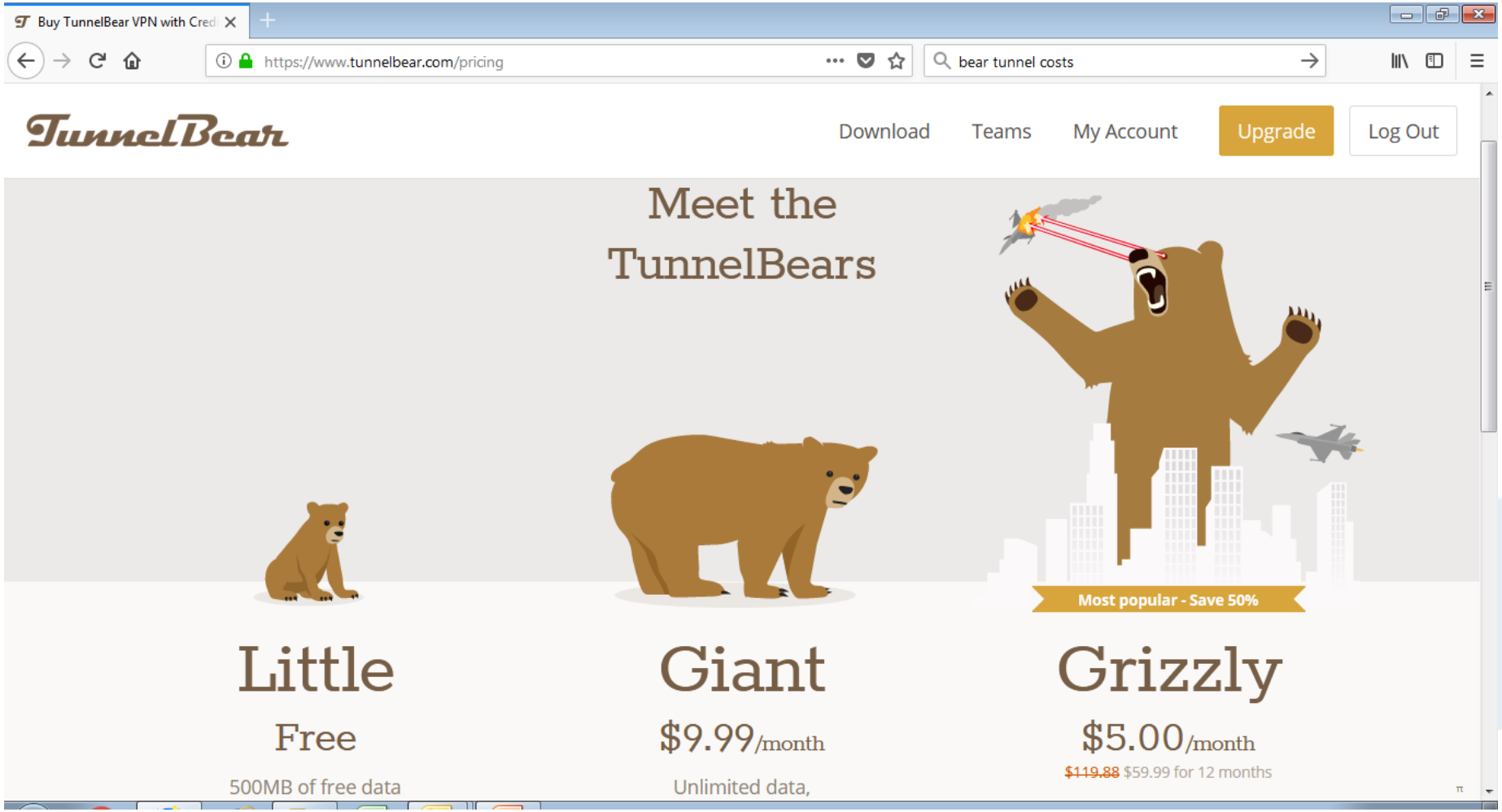
BTSF

- **“In five years, everyone will have a VPN.**

- **VPN awareness will continue to expand as consumers begin to comprehend the degree to which their ISPs and other tech entities regularly infringe on their privacy.”**

Tech Radar Aug 2018

BTSF Costs



European Commission

BTSF You don’t have to use VPN

- Know that it’s an option
- Know the “pros and cons”
- There’s no rush

BTSF

Facebook

European Commission

BTSF Facebook - quick quiz

- ✓Who created Facebook?
- ✓How many users, as of second quarter, 2018?
- ✓How long does the average US member spend on Facebook?
- ✓Name the Hollywood movie based on the creation of Facebook?

BTSF Facebook = OSINT

- ✓Open Source Intelligence
- ✓Intel rather than evidence
- ✓Always remember the difference
- ✓Rules of evidence/rules of “unused material”

BTSF Facebook - possible uses

- Direct sales
- Consumer feedback
- Intel on individuals (location, finance, background)
- Connections, conspiracy

BTSF Facebook - setting up new account

- ✓Don’t use personal accounts
- ✓Set up a dummy account
- ✓Minimal content if just to get into Facebook
- ✓A fake account is much trickier – let’s discuss

BTSF Facebook - finding individuals

- Name - “people named John Smith”
- Employment “people who work at Microsoft”
- Location

https://www.facebook.com/search/str/denver/pages-named/residents/present

BTSF Facebook - finding individuals

- You can combine two search criteria:

- https://www.facebook.com/search/str/denver/pages-named/residents/present/str/chef/pages-named/employees/present/intersect

- This will list all chefs in Denver

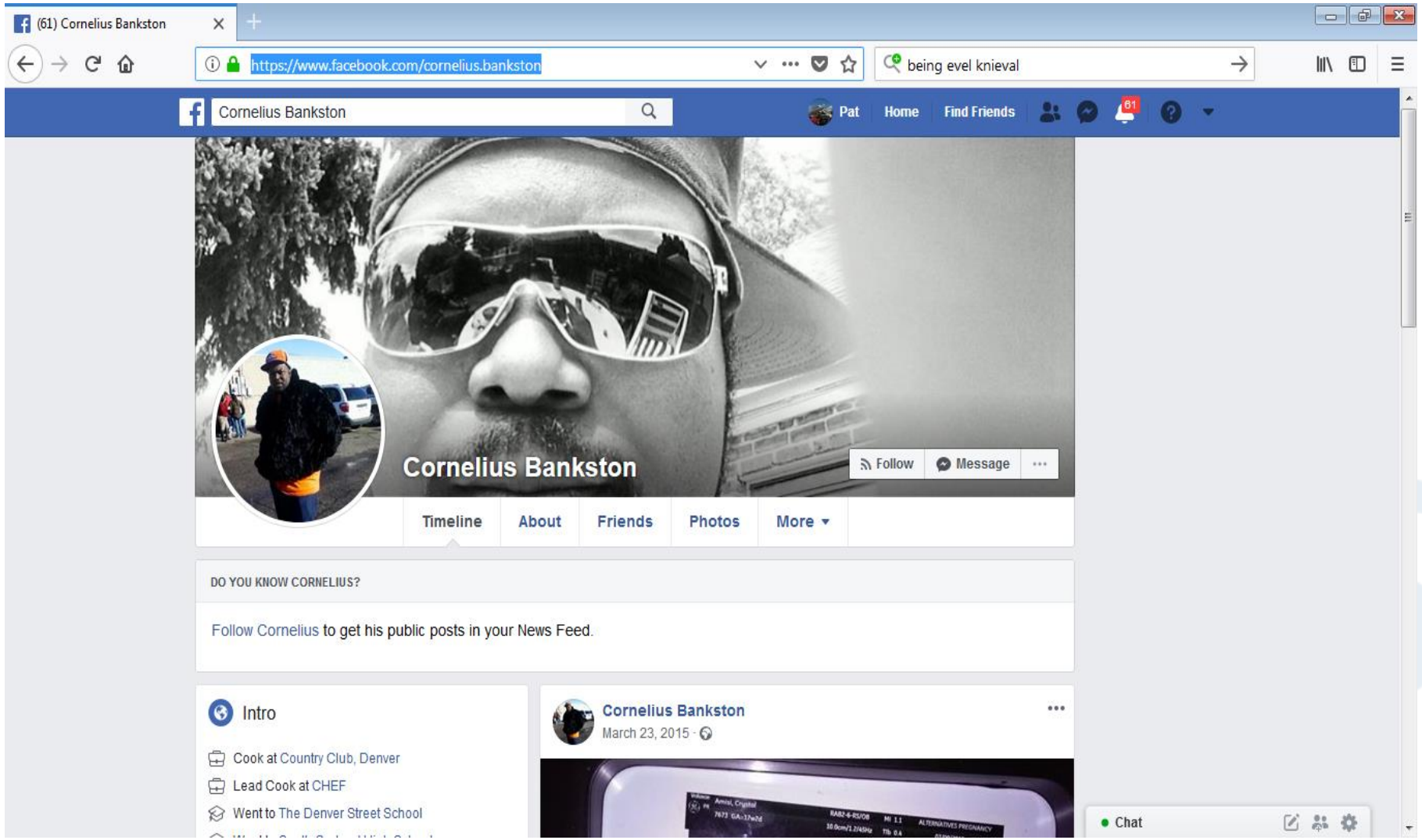
BTSF Facebook - user numbers

- Every individual Facebook user has a unique number. This can be useful
- We can find it within the HTML source code
- Remember that? Do we need two mins revision?

BTSF Facebook - user numbers

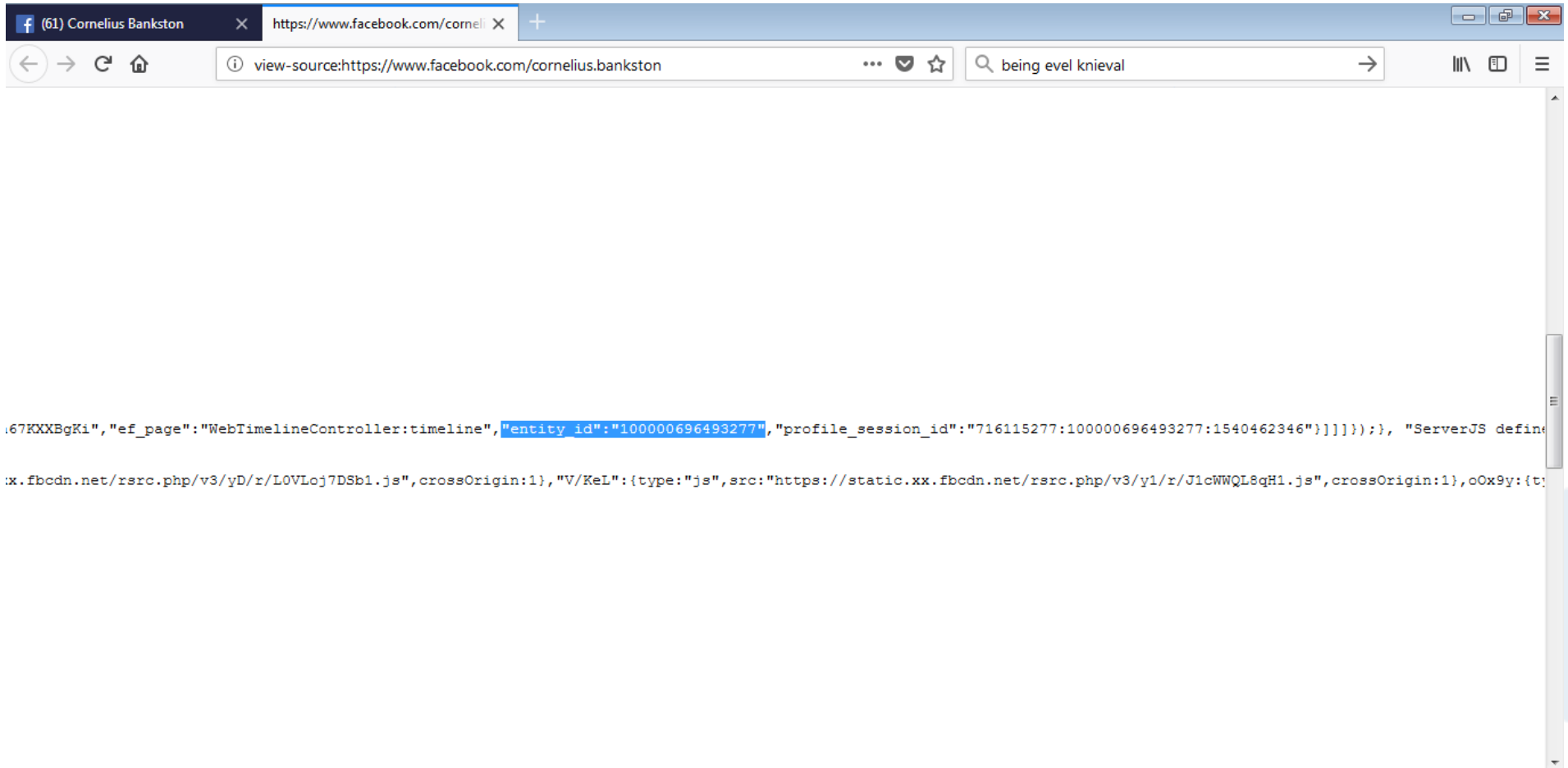
- Go to the user Facebook profile
- View the source code of that page
- Search for “entity_id”
- The number next to this is the unique user number
- Here’s an example

BTSF



European Commission

BTSF



European Commission

BTSF Facebook - user numbers

- If you copy the number into the profile instead of the name, you can confirm the number is correct
- This number can be inserted into specific search terms for better search results
- https://www.facebook.com/search/100000696493277/photos-liked
- This includes photos from other people's pages

BTSF Facebook - search options

- ✓/places visited
- ✓/photos-liked
- ✓/pages-liked
- ✓/groups
- ✓/employers
- ✓/photos of (tagged)

- ✓Just a selection

BTSF Facebook - search options - friends

- https://www.facebook.com/search/100000696493277/friends/photos-liked

- This can be useful if there is little info on the target's own page

- It gives some kind of background or context

BTSF Facebook - small exercise

Remember who established Facebook?

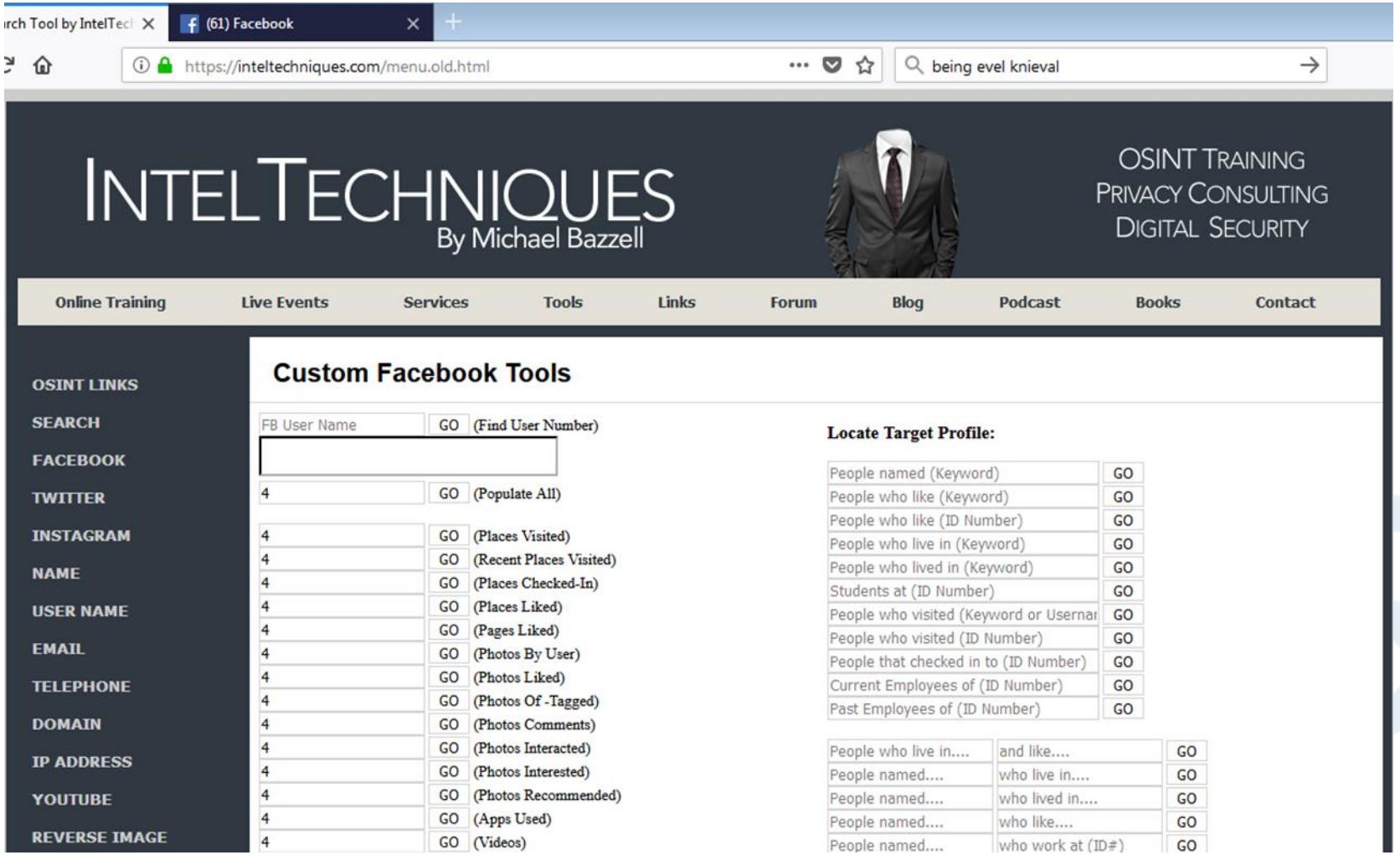
BTSF Facebook - common results

- Sometimes, proving a connection can be useful
- https://www.facebook.com/search/4/photos-liked/5/photos-liked/intersect
- “intersect” means only list results that apply to both users
- Who is number 5?

BTSF Facebook - time saver

- ✓ There are many online tools to assist with Facebook investigations
- ✓ One example:
- ✓ https://inteltechniques.com/menu.old.html

BTSF



European Commission

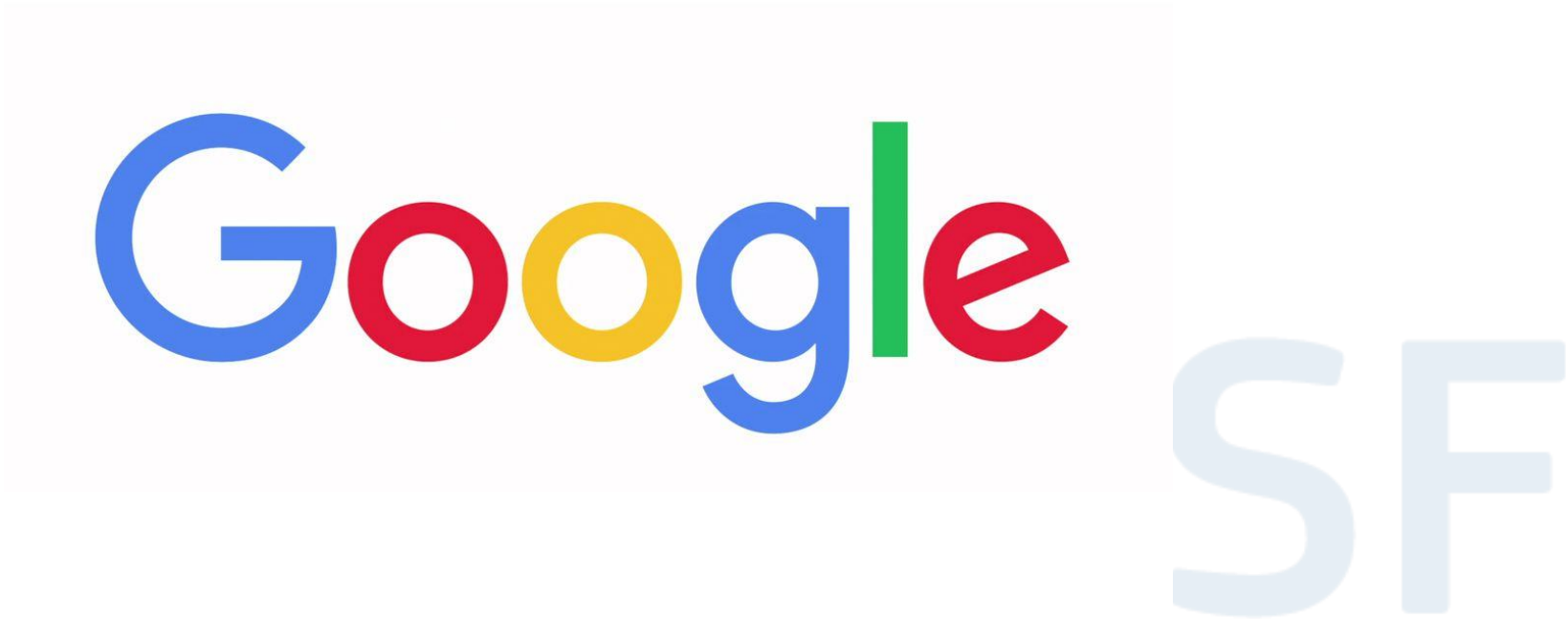
BTSF Facebook - time saver - remember

- This is intel only at this time
- Facebook change what can and can’t be done (without telling us)
- Online tools are updated. Do they work?

BTSF Facebook - remember

- We have only scratched the surface
- This is just a taster
- Some people just do this for a living! Full time OSINT investigators.
- If you have a very big case, consider getting help. (colleagues or contractors)
- There are books out there, inches thick!!

BTSF



European Commission

BTSF Google searching

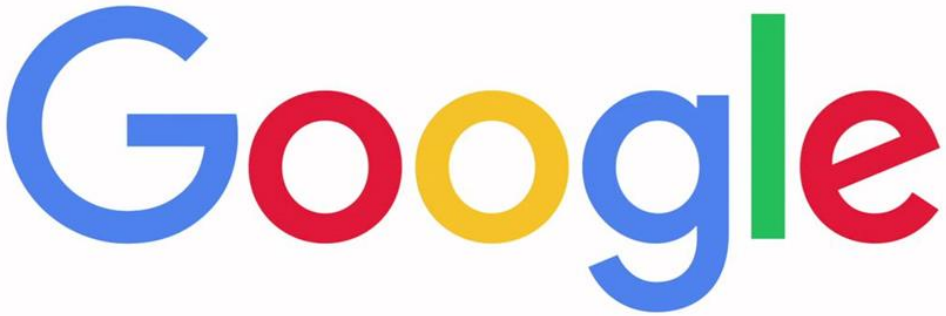
- Accurate/targeted google searching can save time and give better results
- Are we all happy with how Google works? (5 min revision?)
- Most people just type a word in

BTSF Google searching

- Don’t forget “quotation marks”
- Useful when searching e-mail addresses
- Quick and easy tool

BTSF Google operators

- **Operators**: additional words added to searches to make them more targeted
- **Example**: site operator
- **Site**: microsoft.com "bill gates"
- Only searches for the words within the domain (remember what a domain is?)



BTSF Google operators

- File type operator
- “microsoft” filetype: **xls**
- Revise file extensions for this tool
- “cv” “target name” filetype: **pdf**
- Useful to see if a suspect has ever posted a CV?

BTSF Google operators

- Excluding words – the hyphen
- Very useful, can be used in multiples
- You can keep adding them if results are too high
- Microsoft – software - usa

BTSF Google operators

- Search the URL only
- Could be useful for specific product or ingredient
- inurl: cornflour

BTSF Google operators

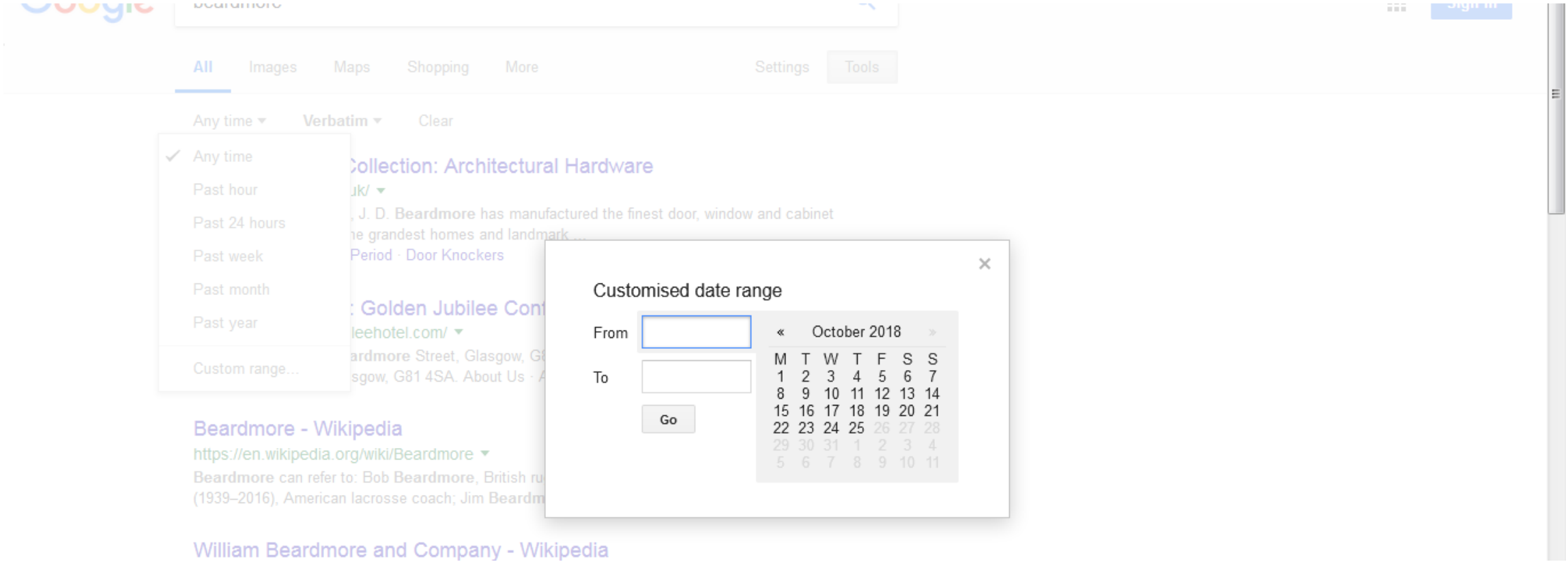
- ✓Unsure on some details?
- ✓Consider the “or” operator
- ✓“pat beardmore” OR “patrick berdmore”
- ✓OR must be upper case (easy to forget)
- ✓Quiz time ☺

BTSF

Google searches and time

- Often, we come to an investigation late
- Media coverage and social media can mask more original data
- We can focus on “time windows”
- Click on the “tools” button

BTSF



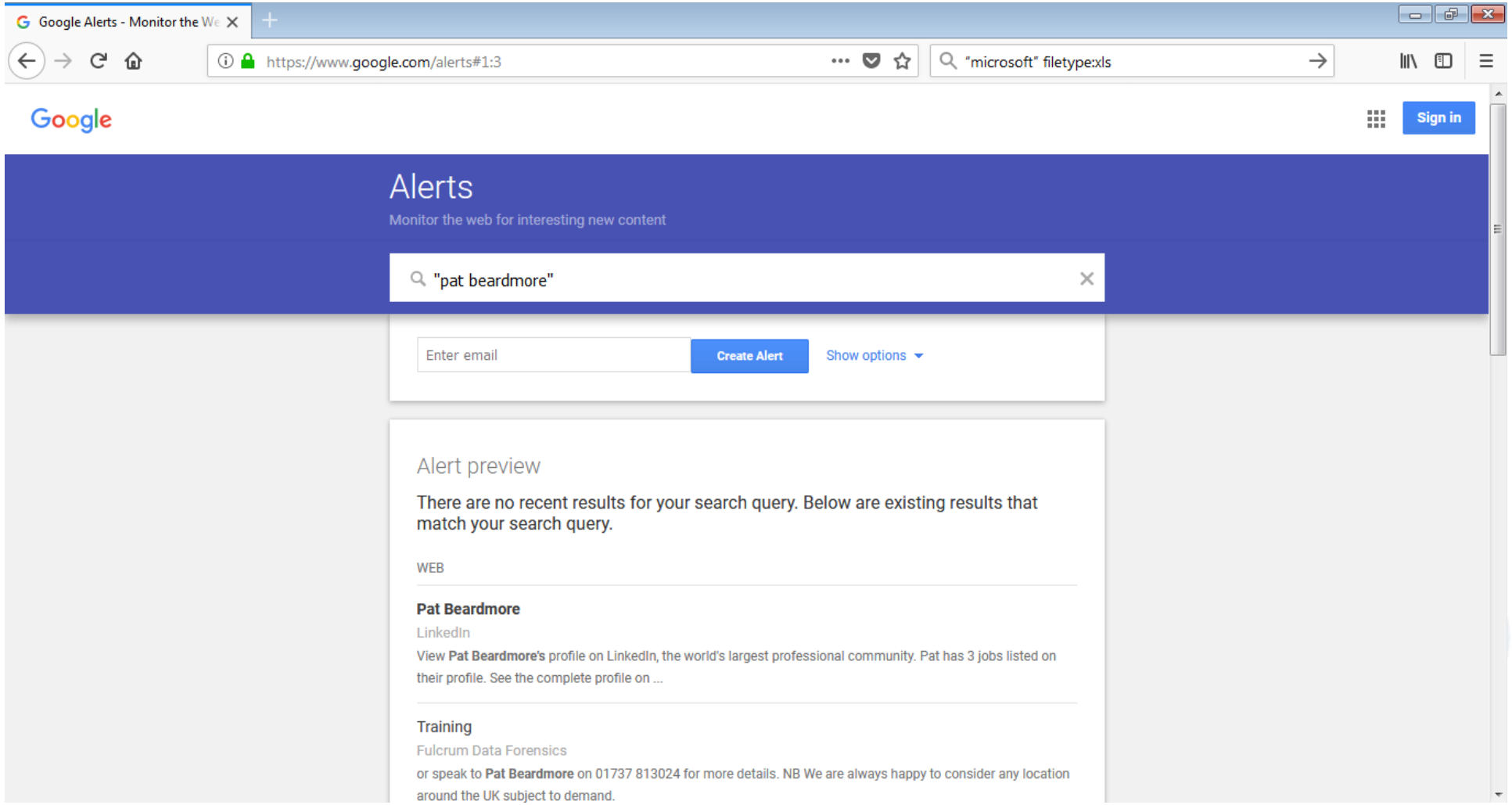
European Commission

BTSF

Google searches and alerts

- ✓Perfect for research projects, media monitoring and market trends
- ✓www.google.com/alerts
- ✓You do need a google account for this
- ✓You receive a daily e-mail with updated alerts

BTSF


Google Alerts - Monitor the We
https://www.google.com/alerts#1:3
"microsoft" filetype:xls
Google
Sign in
Alerts
Monitor the web for interesting new content
"pat beardmore"
Enter email
Create Alert
Show options
Alert preview
There are no recent results for your search query. Below are existing results that match your search query.
WEB
Pat Beardmore
LinkedIn
View Pat Beardmore's profile on LinkedIn, the world's largest professional community. Pat has 3 jobs listed on their profile. See the complete profile on ...
Training
Fulcrum Data Forensics
or speak to Pat Beardmore on 01737 813024 for more details. NB We are always happy to consider any location around the UK subject to demand.

BTSF

Web scraping

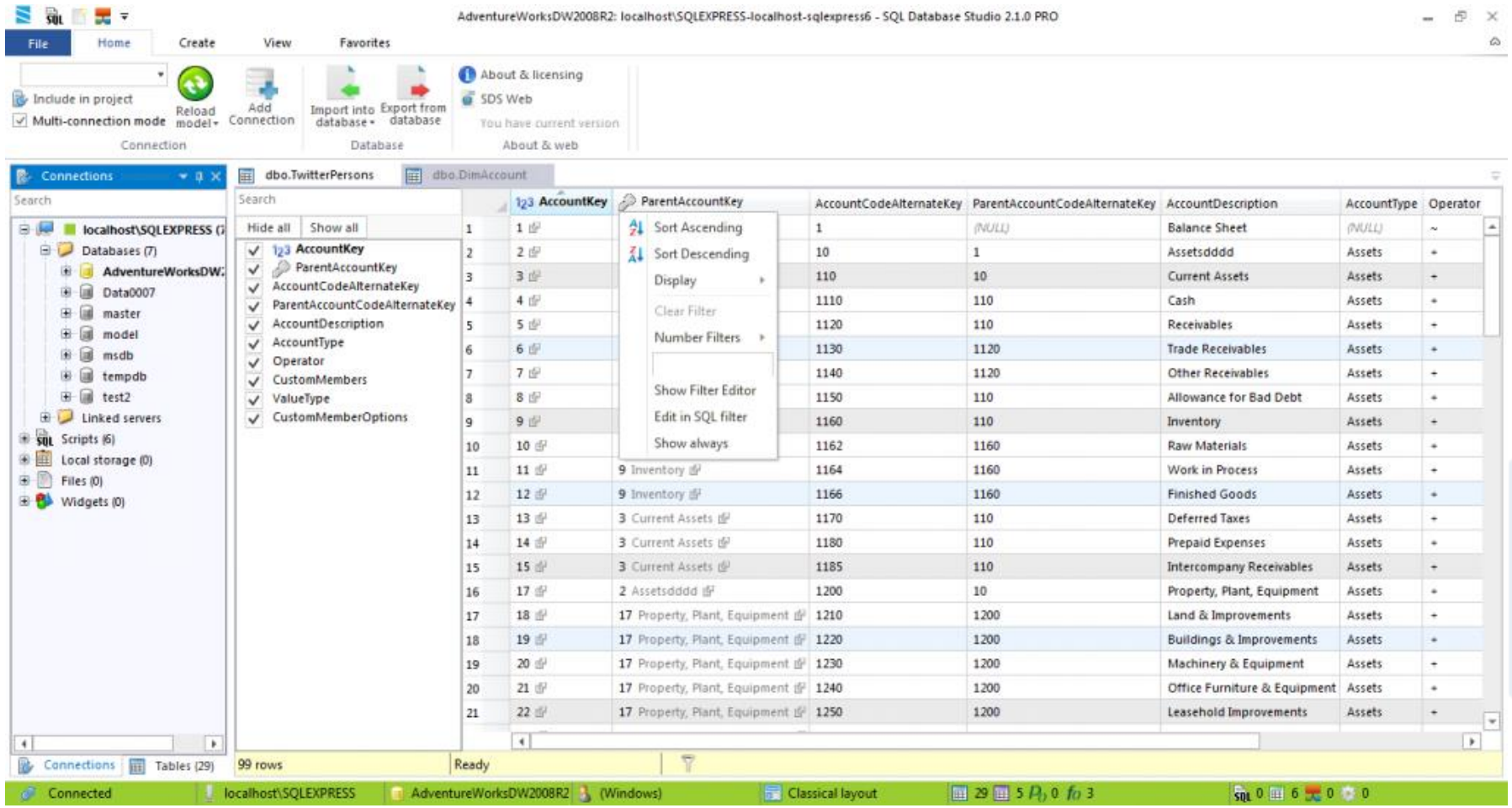
- The extraction of specific data from web sites
- This can be done manually
- Remember the previous course?
- Let’s revisit manual data extraction

BTSF

Web scraping

- Manual extraction can be useful when you are looking for small amounts of specific data within a small data field
- But it’s too slow for wider use
- There are many tools available that automate the process
- Let’s take a look

BTSF SQL Database Example



European Commission

Any questions on anything we have covered?

BTSF

Bonus Session!

Securing evidence via encryption

European Commission

BTSF Encrypting evidence

- Secure
- Prevents leakage
- Locks in continuity
- Fits into a quality procedure

European Commission

BTSF

Encrypting evidence

- ✓“Live encryption”,
- ✓“on-the-fly encryption”,
- ✓“transparent encryption”,
- ✓“real-time encryption”
- ✓All the same thing

BTSF

Encrypting evidence

- Consider using USB flash drives
- cheap
- simple
- reliable
- But still…what's the "golden rule"????

BTSF

Encrypting evidence

- ✓Separate drive for each case
- ✓And each officer?
- ✓Labelled and accounted for
- ✓Manage passwords
- ✓Passphrases are better

BTSF

European Commission

BTSF

Thank you

European Commission
Consumers, Health and Food Executive Agency
DRB A3/042
L-2920 Luxembourg

AENOR INTERNACIONAL
6, Genova street. 28004. Madrid, SPAIN
Tel: +34 91 432 61 25
Mail: 20179605NFIT@aenor.com
www.btsf-aenor.com

European Commission