UNIVERSITY OF LIVERPOOL

CYBER SECURITY SOCIETY

Welcome Session: OSINT + Crypto

Meet the Committee

President	Tom
Vice-President	Matt
Secretary	Harlan
Events & Sponsorship	Meg
Treasurer	Elliott

What is OSINT?

OSINT (Open-Source Intelligence) is a term used to refer to gathering and analysing information from publicly available sources.

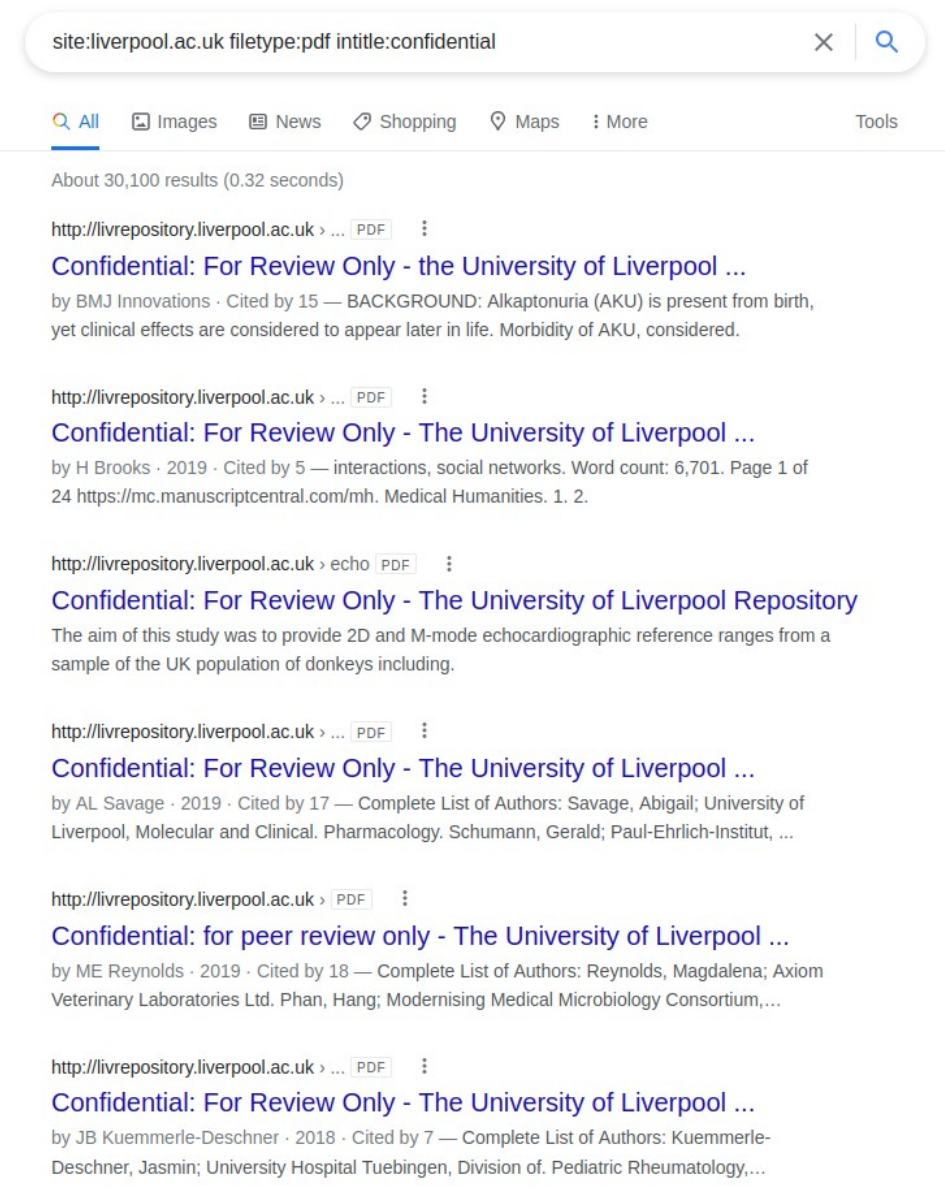
Steps

1. Collect information
2. Extract information
3. Analyse information
4. Type gg wp In chat

Technique: Google dork

Google dorking is when you use advanced search filters on a search engine (doesn’t have to be google)

site: inurl: filetype: intext: allintext: intitle:



site:liverpool.ac.uk filetype:pdf intitle:confidential

About 30,100 results (0.32 seconds)

http://livrepository.liverpool.ac.uk › ... PDF

Confidential: For Review Only - the University of Liverpool ...

by BMJ Innovations · Cited by 15 — BACKGROUND: Alkaptonuria (AKU) is present from birth, yet clinical effects are considered to appear later in life. Morbidity of AKU, considered.

http://livrepository.liverpool.ac.uk › ... PDF

Confidential: For Review Only - The University of Liverpool ...

by H Brooks · 2019 · Cited by 5 — interactions, social networks. Word count: 6,701. Page 1 of 24 https://mc.manuscriptcentral.com/mh. Medical Humanities. 1. 2.

http://livrepository.liverpool.ac.uk › echo PDF

Confidential: For Review Only - The University of Liverpool Repository

The aim of this study was to provide 2D and M-mode echocardiographic reference ranges from a sample of the UK population of donkeys including.

http://livrepository.liverpool.ac.uk › ... PDF

Confidential: For Review Only - The University of Liverpool ...

by AL Savage · 2019 · Cited by 17 — Complete List of Authors: Savage, Abigail; University of Liverpool, Molecular and Clinical. Pharmacology. Schumann, Gerald; Paul-Ehrlich-Institut, ...

http://livrepository.liverpool.ac.uk › PDF

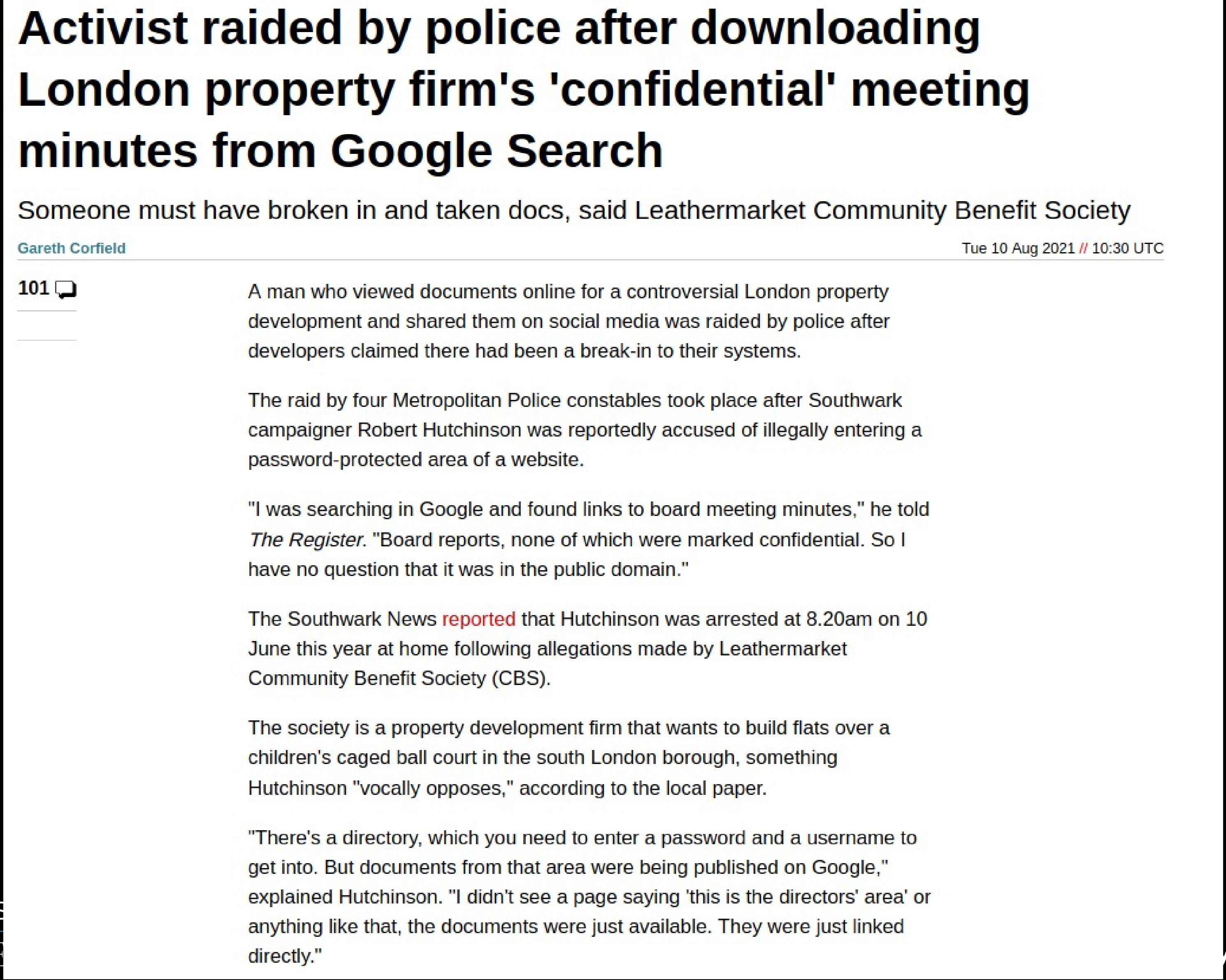
Confidential: for peer review only - The University of Liverpool ...

by ME Reynolds · 2019 · Cited by 18 — Complete List of Authors: Reynolds, Magdalena; Axiom Veterinary Laboratories Ltd. Phan, Hang; Modernising Medical Microbiology Consortium,...

http://livrepository.liverpool.ac.uk › ... PDF

Confidential: For Review Only - The University of Liverpool ...

by JB Kuemmerle-Deschner · 2018 · Cited by 7 — Complete List of Authors: Kuemmerle-Deschner, Jasmin; University Hospital Tuebingen, Division of. Pediatric Rheumatology,...



Activist raided by police after downloading London property firm's 'confidential' meeting minutes from Google Search

Someone must have broken in and taken docs, said Leathermarket Community Benefit Society

Gareth Corfield

Tue 10 Aug 2021 // 10:30 UTC

101

A man who viewed documents online for a controversial London property development and shared them on social media was raided by police after developers claimed there had been a break-in to their systems.

The raid by four Metropolitan Police constables took place after Southwark campaigner Robert Hutchinson was reportedly accused of illegally entering a password-protected area of a website.

"I was searching in Google and found links to board meeting minutes," he told *The Register*. "Board reports, none of which were marked confidential. So I have no question that it was in the public domain."

The Southwark News reported that Hutchinson was arrested at 8.20am on 10 June this year at home following allegations made by Leathermarket Community Benefit Society (CBS).

The society is a property development firm that wants to build flats over a children's caged ball court in the south London borough, something Hutchinson "vocally opposes," according to the local paper.

"There's a directory, which you need to enter a password and a username to get into. But documents from that area were being published on Google," explained Hutchinson. "I didn't see a page saying 'this is the directors' area' or anything like that, the documents were just available. They were just linked directly."

Technique: Wayback machine

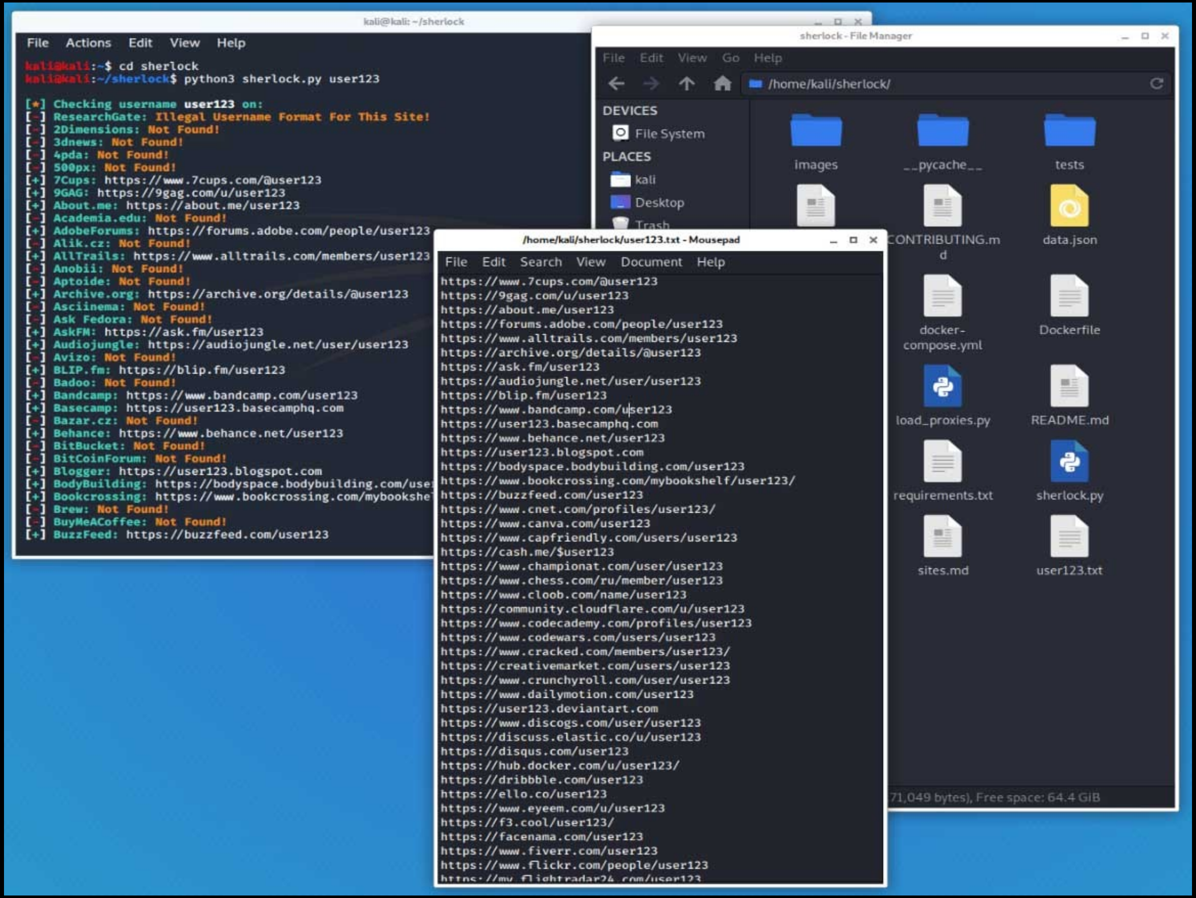
- Using the wayback machine (archive.org/web) you can view snapshots of a website.
- The main use for this is viewing deleted content
- Other ways of doing this are archiving the page yourself or using google’s cached page feature

Technique: Web enumeration

- /robots.txt : Document telling bots which pages they can and can’t access; often used by annoying ctf makers to hide hints
- /sitemap.xml : An XML formatted list of every page on the website and when they were updated

Technique: Social media

- Quite often you can find more information on people through their social media, normally they use the same handle and/or name on multiple platforms.
- Good places to look: linkedin, twitter, facebook, instagram

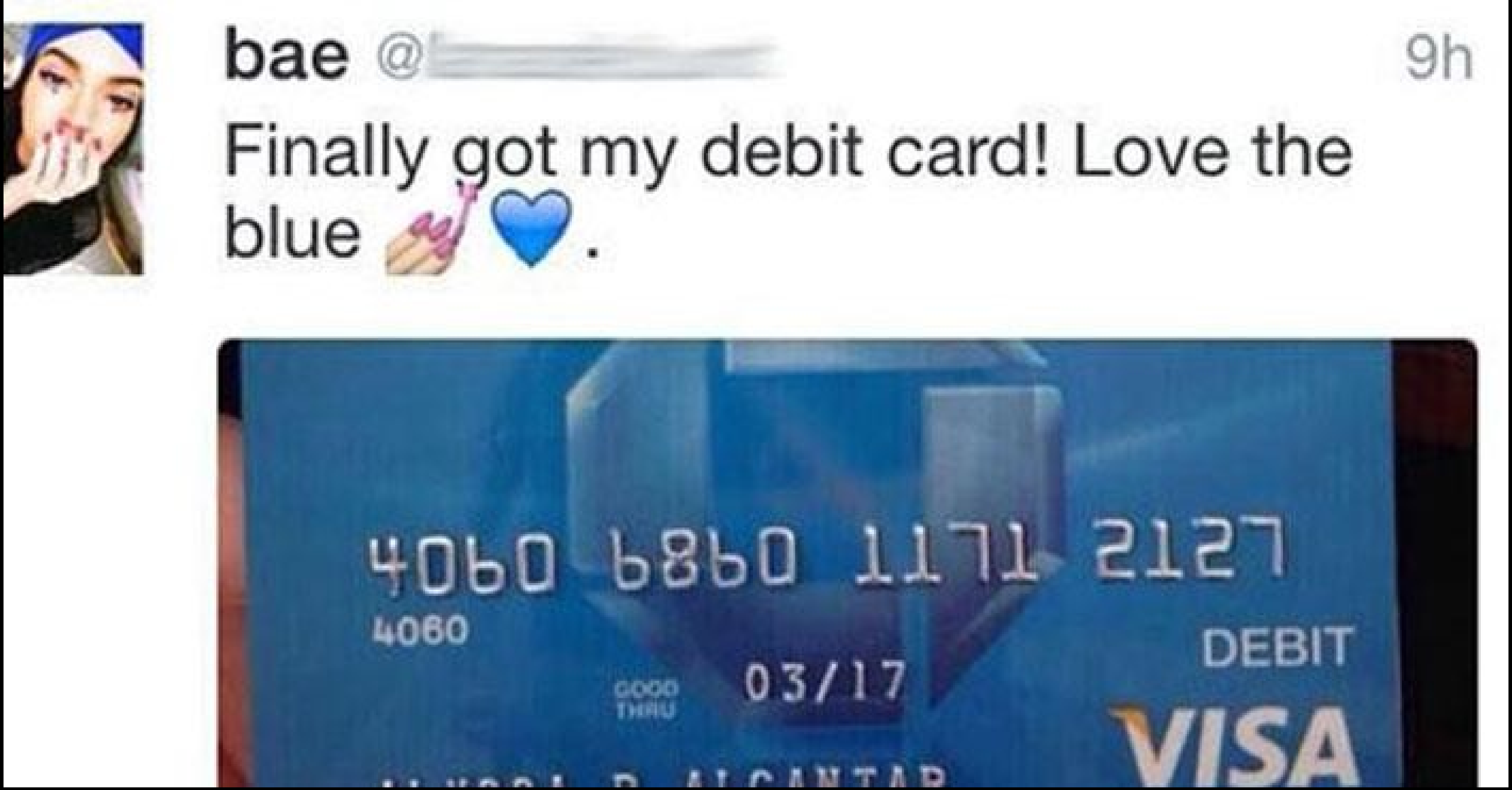


```
kali@kali:~$ cd sherlock
kali@kali:~/sherlock$ python3 sherlock.py user123

[*] Checking username user123 on:
[-] ResearchGate: Illegal Username Format For This Site!
[-] 2Dimensions: Not Found!
[-] 3dnews: Not Found!
[-] 4pda: Not Found!
[-] 500px: Not Found!
[+] 7Cups: https://www.7cups.com/@user123
[+] 9GAG: https://9gag.com/u/user123
[+] About.me: https://about.me/user123
[-] Academia.edu: Not Found!
[+] AdobeForums: https://forums.adobe.com/people/user123
[-] Alik.cz: Not Found!
[+] AllTrails: https://www.alltrails.com/members/user123
[-] Anobii: Not Found!
[-] Aptoide: Not Found!
[+] Archive.org: https://archive.org/details/@user123
[-] Asciinema: Not Found!
[-] Ask Fedora: Not Found!
[+] AskFM: https://ask.fm/user123
[+] Audiojungle: https://audiojungle.net/user/user123
[-] Avizo: Not Found!
[+] BLIP.fm: https://blip.fm/user123
[-] Badoo: Not Found!
[+] Bandcamp: https://www.bandcamp.com/user123
[+] Basecamp: https://user123.basecamphq.com
[-] Bazar.cz: Not Found!
[+] Behance: https://www.behance.net/user123
[-] BitBucket: Not Found!
[-] BitCoinForum: Not Found!
[+] Blogger: https://user123.blogspot.com
[+] BodyBuilding: https://bodyspace.bodybuilding.com/use
[+] Bookcrossing: https://www.bookcrossing.com/mybookshe
[-] Brew: Not Found!
[-] BuyMeACoffee: Not Found!
[+] BuzzFeed: https://buzzfeed.com/user123
```

```
https://www.7cups.com/@user123
https://9gag.com/u/user123
https://about.me/user123
https://forums.adobe.com/people/user123
https://www.alltrails.com/members/user123
https://archive.org/details/@user123
https://ask.fm/user123
https://audiojungle.net/user/user123
https://blip.fm/user123
https://www.bandcamp.com/user123
https://user123.basecamphq.com
https://www.behance.net/user123
https://user123.blogspot.com
https://bodyspace.bodybuilding.com/user123
https://www.bookcrossing.com/mybookshelf/user123/
https://buzzfeed.com/user123
https://www.cnet.com/profiles/user123/
https://www.canva.com/user123
https://www.capfriendly.com/users/user123
https://cash.me/$user123
https://www.championat.com/user/user123
https://www.chess.com/ru/member/user123
https://www.cloob.com/name/user123
https://community.cloudflare.com/u/user123
https://www.codecademy.com/profiles/user123
https://www.codewars.com/users/user123
https://www.cracked.com/members/user123/
https://creativemarket.com/users/user123
https://www.crunchyroll.com/user/user123
https://www.dailymotion.com/user123
https://user123.deviantart.com
https://www.discogs.com/user/user123
https://discuss.elastic.co/u/user123
https://disqus.com/user123
https://hub.docker.com/u/user123/
https://dribbble.com/user123
https://ello.co/user123
https://www.eyeem.com/u/user123
https://f3.cool/user123/
https://facenama.com/user123
https://www.fiverr.com/user123
https://www.flickr.com/people/user123
https://my.flightradar24.com/user123
```

https://sherlock-project.github.io/

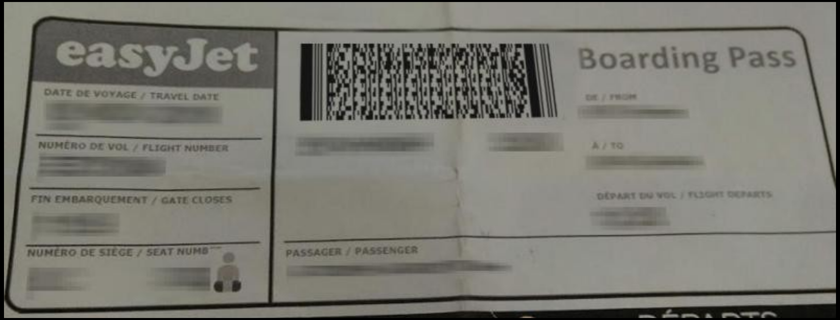


bae @[redacted] 9h

Finally got my debit card! Love the blue 💅💙.

Technique: QR/Barcodes

QR codes and Barcodes are just ways of storing information: often by scanning them you can read sensitive information



easyJet

Boarding Pass

DATE DE VOYAGE / TRAVEL DATE
[redacted]

NUMÉRO DE VOL / FLIGHT NUMBER
[redacted]

FIN EMBARQUEMENT / GATE CLOSES
[redacted]

NUMÉRO DE SIÈGE / SEAT NUMB
[redacted]

PASSAGER / PASSENGER
[redacted]

DE / FROM
[redacted]

A / TO
[redacted]

DÉPART DU VOL / FLIGHT DEPARTS
[redacted]

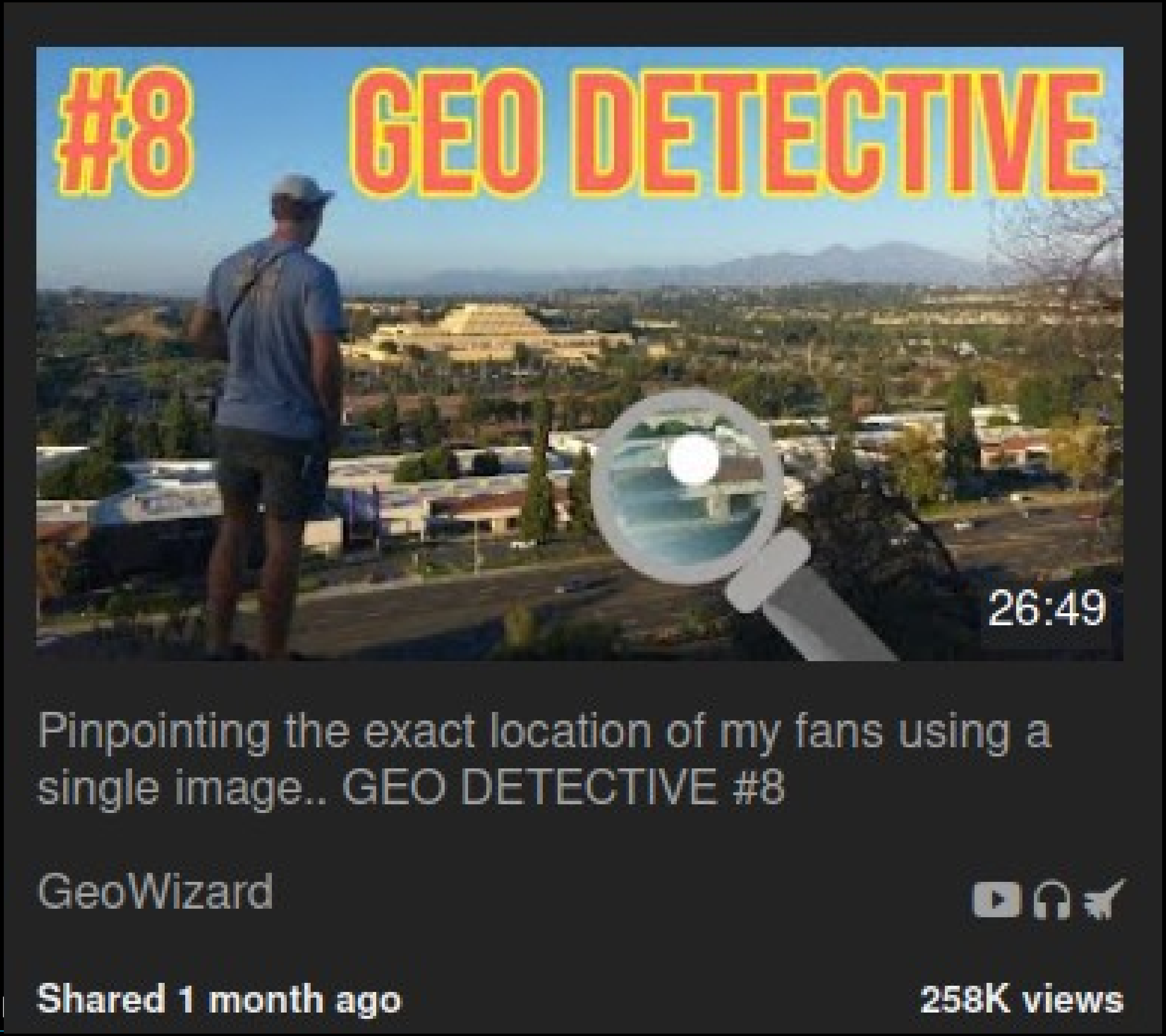
DÉPARTS

Embedded text: M1LEETHACKER/CLIVE EA12BC3 FNJLHREZY42069265 42A 123 1621232 08 2A18
Containing: Lastname/Firstname BookingNo Destination FlightNo Seat

`online-barcode-reader.inliteresearch.com`

Technique: EXIF data

- Extra data contained within image files, can include:
  - Time/date taken
  - Camera make/model
  - Username of account that took photo
  - GPS location where the image was taken
  - + much more
- An easy way to view online: exifdata.com

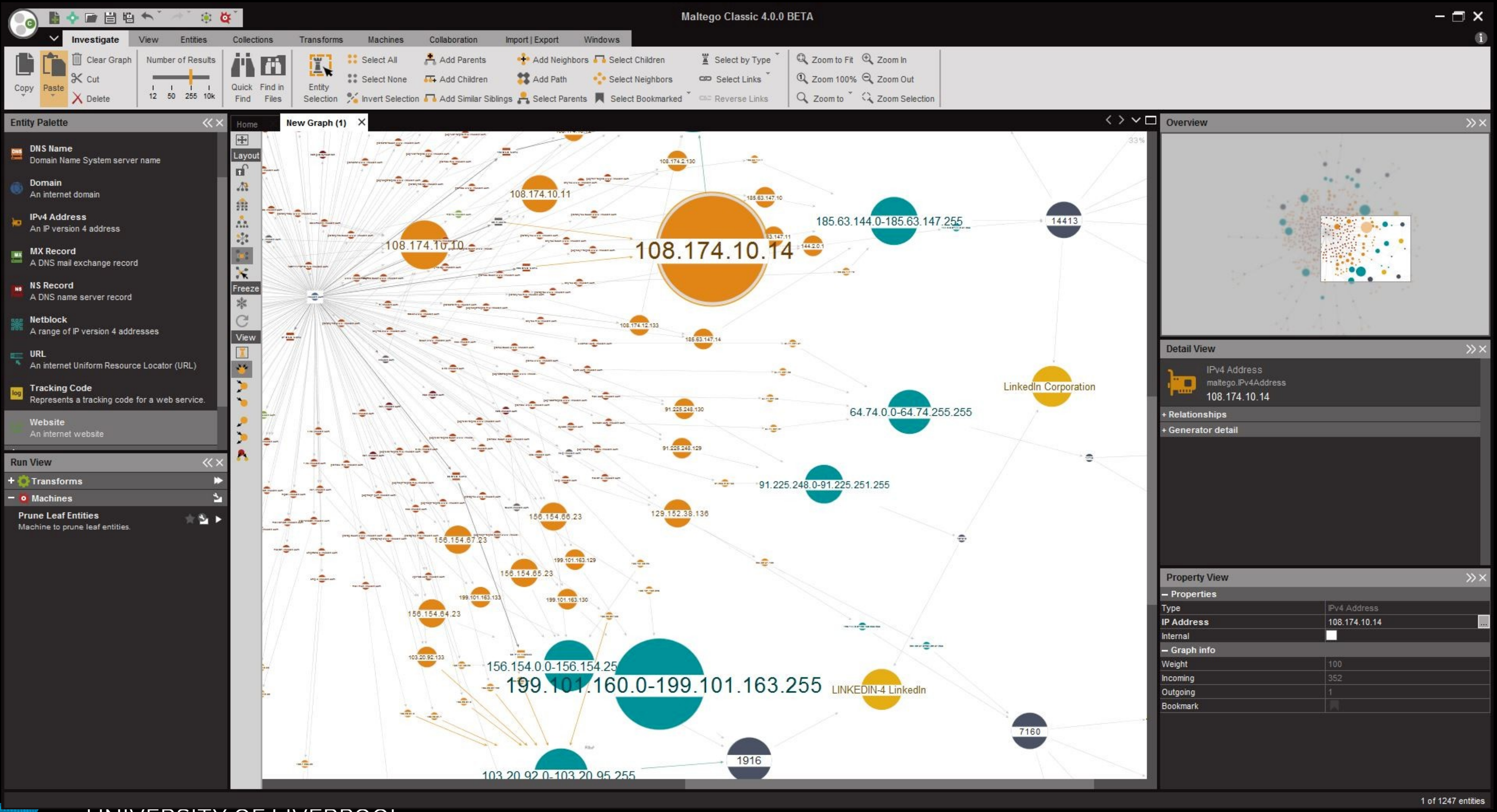


Pinpointing the exact location of my fans using a single image.. GEO DETECTIVE #8

GeoWizard

Shared 1 month ago

258K views



– Properties

Type: IPv4 Address

IP Address: 108.174.10.14

Internal: □

– Graph info

Weight: 100

Incoming: 352

Outgoing: 1

Bookmark:

Simple Crypto and Crypto RE

Why bother?

- Modern cryptography is very good, and often requires some significant mathematics to break
- Pretty much every country has agencies built to mess with your cryptosystems
- Many people don’t bother to encrypt their services
- It’s boring

Why bother?

- Security of components does not imply security of the whole
  - If you know I’m encrypting “yes” or “no” with the world’s best cypher, and you see a two letter encrypted word, you know the message
  - People still write their own massively flawed systems
- Organisations messing with cryptography is why we need more people in cryptography
- Google reckons more than 90% of web traffic is encrypted
- Cryptanalysis is one of the most financially and intellectually rewarding forms of hacking, and has a history that dates back thousands of years

Terminology

- Symbols: whatever you’re working with (letters, bytes, numbers)
- Cypher: something that *reversibly* replaces symbols according to a key
- Hash: something that *irreversibly* replaces symbols
- Encrypt: apply a cypher to something
- Decrypt: undo encryption
- Plaintext: what you’re encrypting
- Cyphertext: what you’re decrypting

Cryptanalysis 101: Patterns

- Encrypted text should look random
- Repeating sequences
- Common behaviour between different keys/ptexts/ctexts
- Structure in output
- Anything that looks weird

Cryptanalysis 102: Oracles

- Something that leaks information to you
- Types
  - Chosen-plaintext
  - Chosen-cyphertext
  - Known-plaintext
  - Padding
  - Many more
- Example: OTP break

Cryptanalysis 103: Black boxes

- Sometimes cryptography is complex, so just ignore it
- Black boxing: ignoring the inner-workings of a system to try to understand its *purpose*
- Differential cryptanalysis
- Sometimes breaking into many smaller black boxes help
- Try spamming inputs like ‘aaaaaaaa’ or ‘abcdefg’ to see how each position/letter is effected by the cypher

Basic crypto RE

- Crypto code is always obscure
- Try to work out the *role* of code, not it’s literal function
- Try running individual bits of code by themselves to see what they do
- Try removing bits of code to see what they contribute
- Try writing equivalent code to see if you can match the output
- TAKE NOTES OF WHAT YOU DISCOVER!!!

Time for you to try

Register an account at ctf.cybersoc.cf

Use your uni email, once you’re signed in find the “Welcome” challenges.