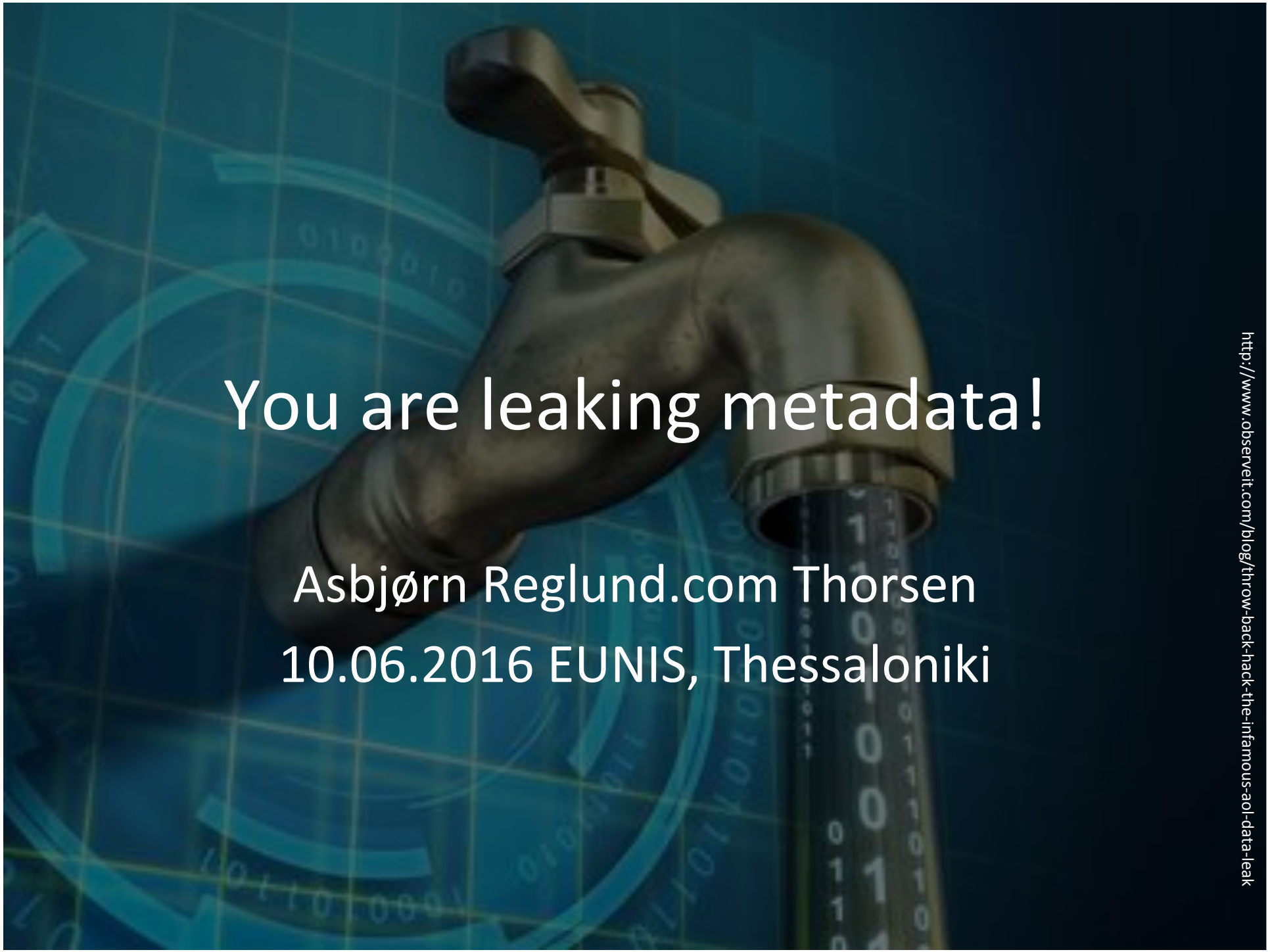


You are leaking metadata!

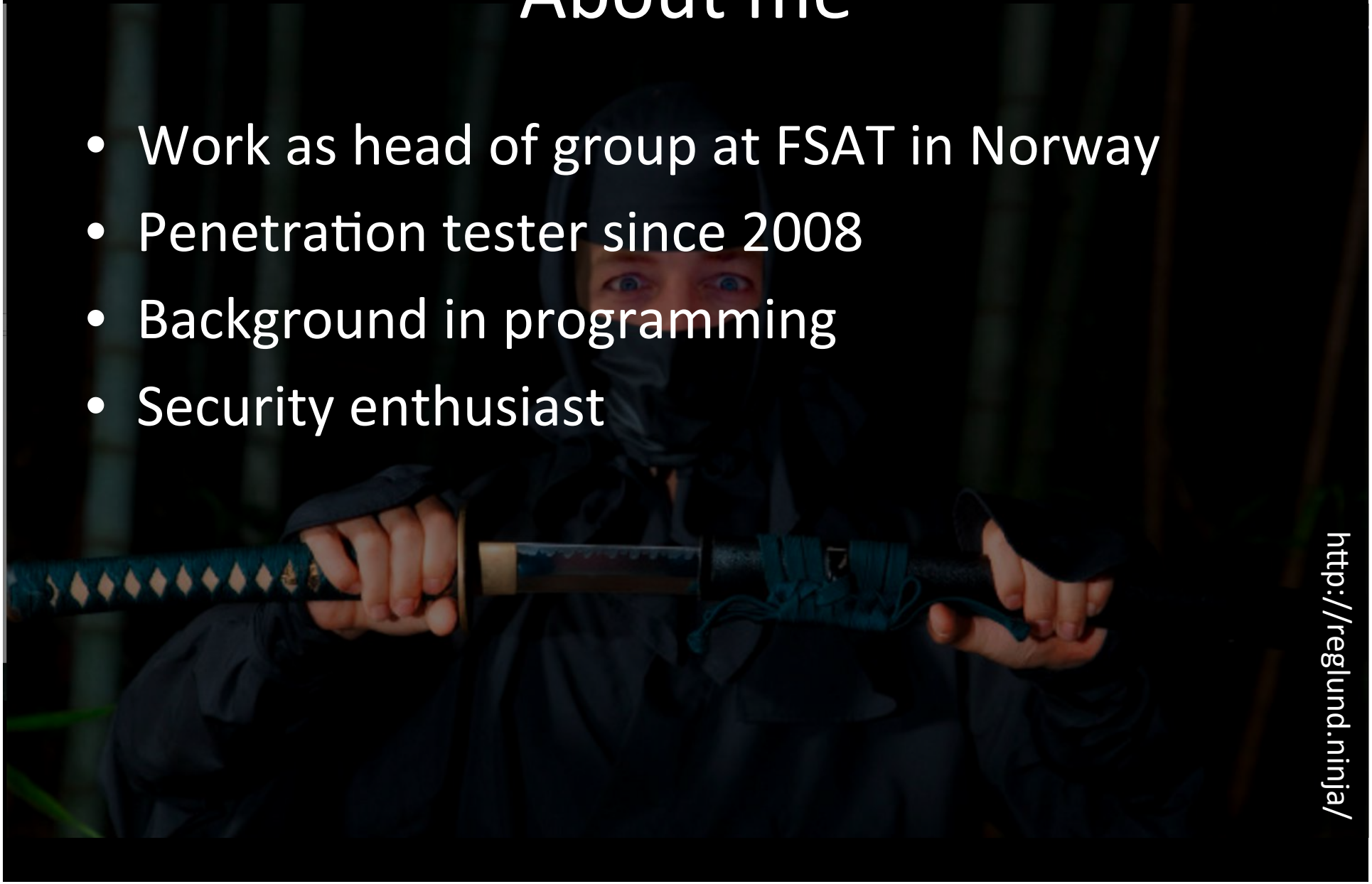
Asbjørn Reglund.com Thorsen

10.06.2016 EUNIS, Thessaloniki

http://www.observeit.com/blog/throw-back-hack-the-infamous-aol-data-leak

About me

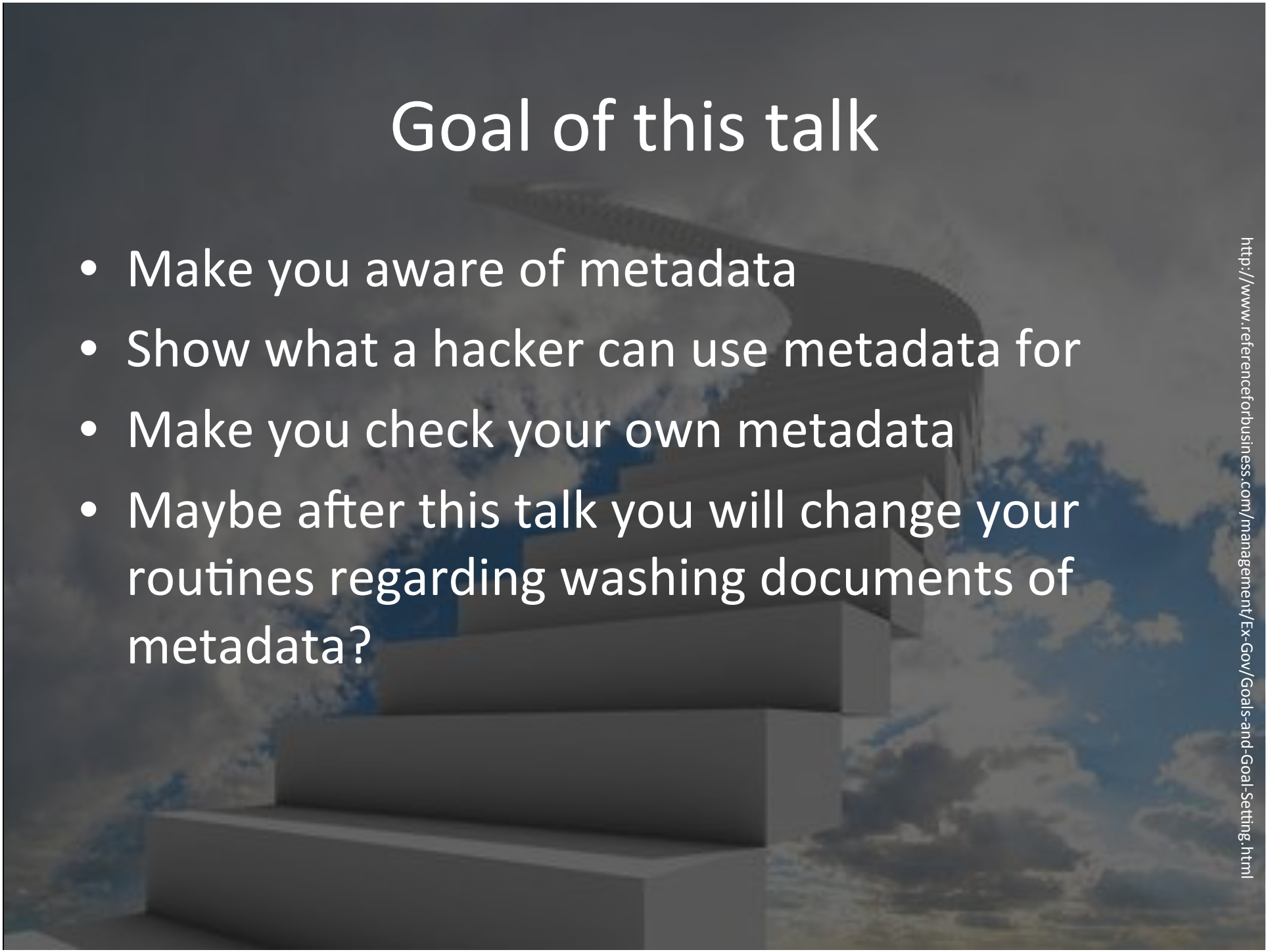
- Work as head of group at FSAT in Norway
- Penetration tester since 2008
- Background in programming
- Security enthusiast



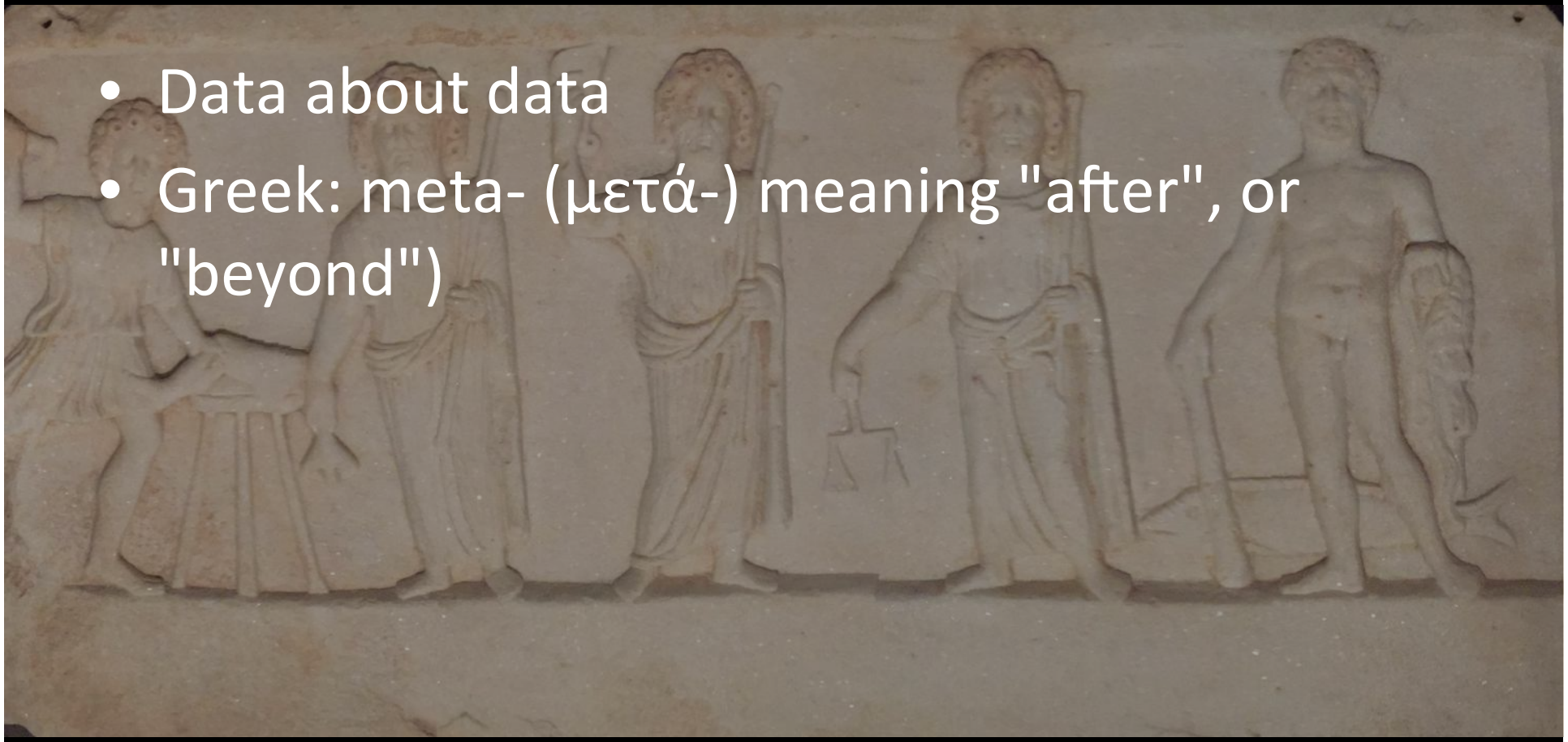
http://reglund.ninja/

Goal of this talk

- Make you aware of metadata
- Show what a hacker can use metadata for
- Make you check your own metadata
- Maybe after this talk you will change your routines regarding washing documents of metadata?



What is metadata?



- Data about data
- Greek: meta- (μετά-) meaning "after", or "beyond")


THEY'RE ONLY COLLECTING
"METADATA"
memegenerator.net

Why metadata matters

- They know you rang a phone sex service at 2:24 am and spoke for 18 minutes. But they don't know what you talked about
- They know you called the suicide prevention hotline from Golden Gate Bridge. But the topic of the call remains a secret.
- They know you spoke with an HIV testing service, then your doctor, then your health insurance company in the same hour. But they don't know what was discussed.

Source: 30C3 Electronic Frontier Foundation

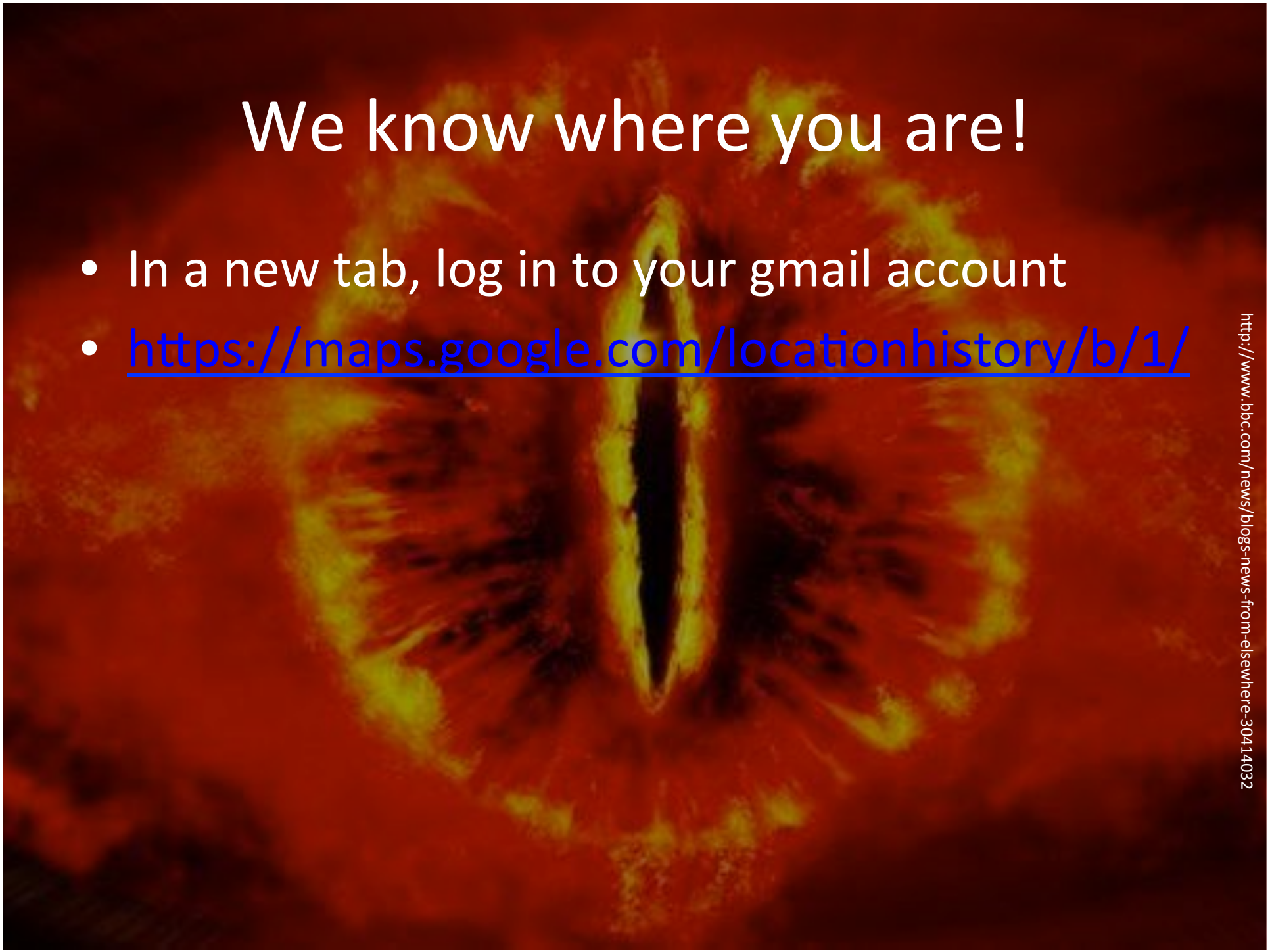
Metadata findings

- Usernames
- Mail addresses
- Passwords
- Printers
- Software versions
- GPS coordinates
- Dates
- Author
- Camera type
- Rotation
- Computer names
- And much more..

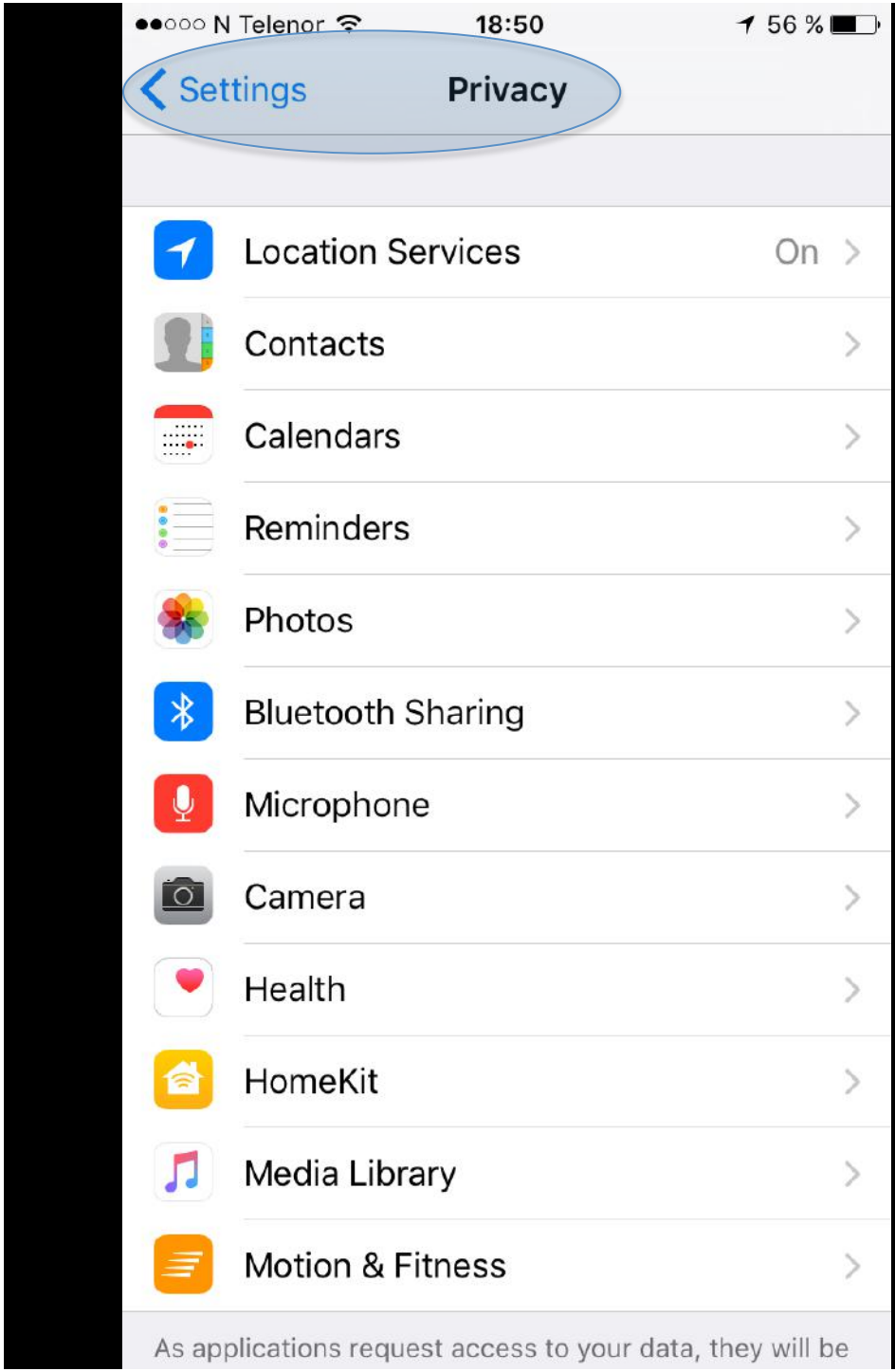
https://hubslide.com/chema-alonso/defcon-21-fear-the-evil-foca-mitm-attacks-using-ipv6-s56d4bd2f8d070ead0e63bd79.html

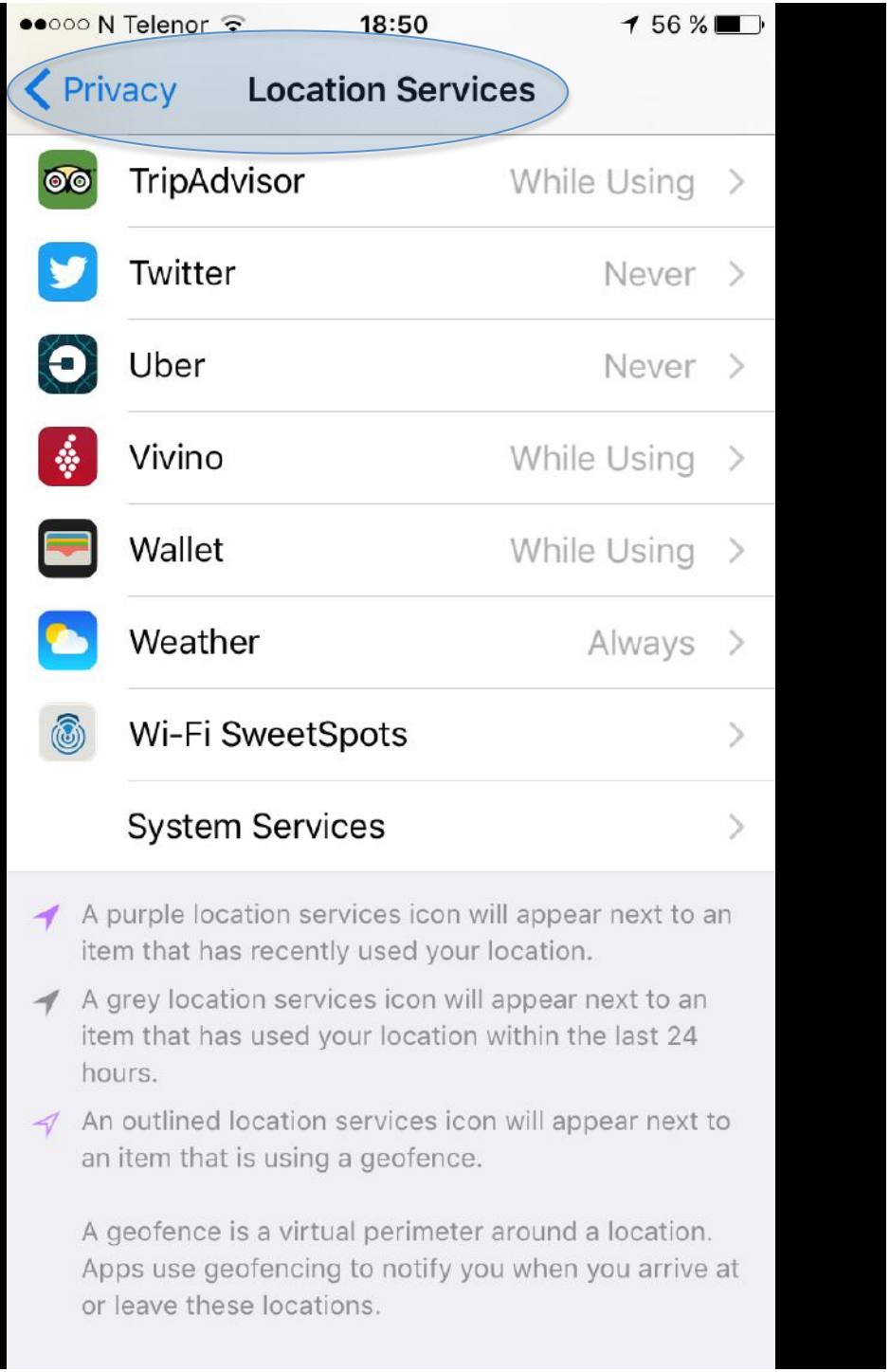
We know where you are!

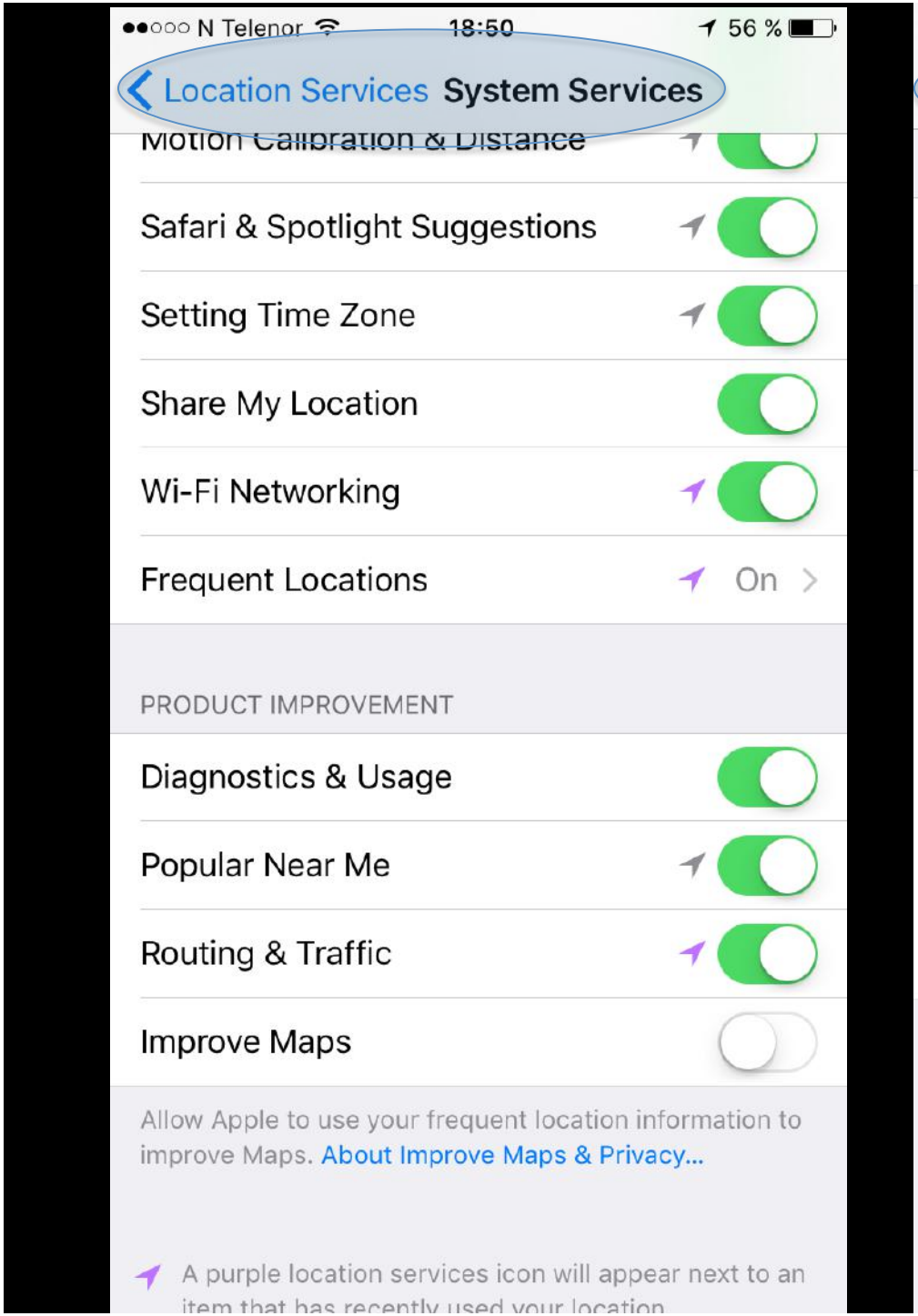
- In a new tab, log in to your gmail account
- https://maps.google.com/locationhistory/b/1/

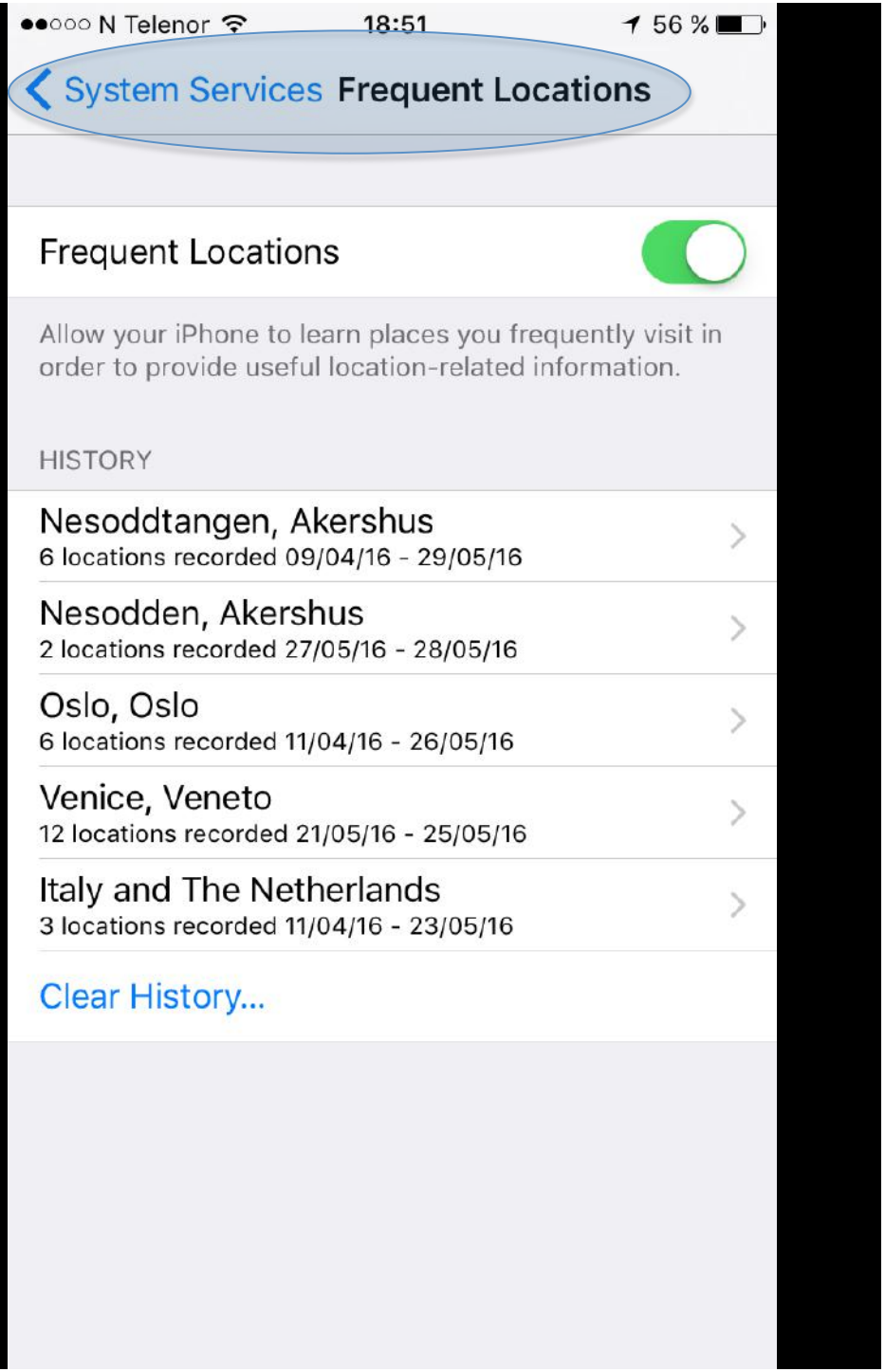


http://www.bbc.com/news/blogs-news-from-elsewhere-30414032


●●○○○ N Telenor
18:50
56 %
Settings
Privacy
Location Services
On
Contacts
Calendars
Reminders
Photos
Bluetooth Sharing
Microphone
Camera
Health
HomeKit
Media Library
Motion & Fitness
As applications request access to your data, they will be

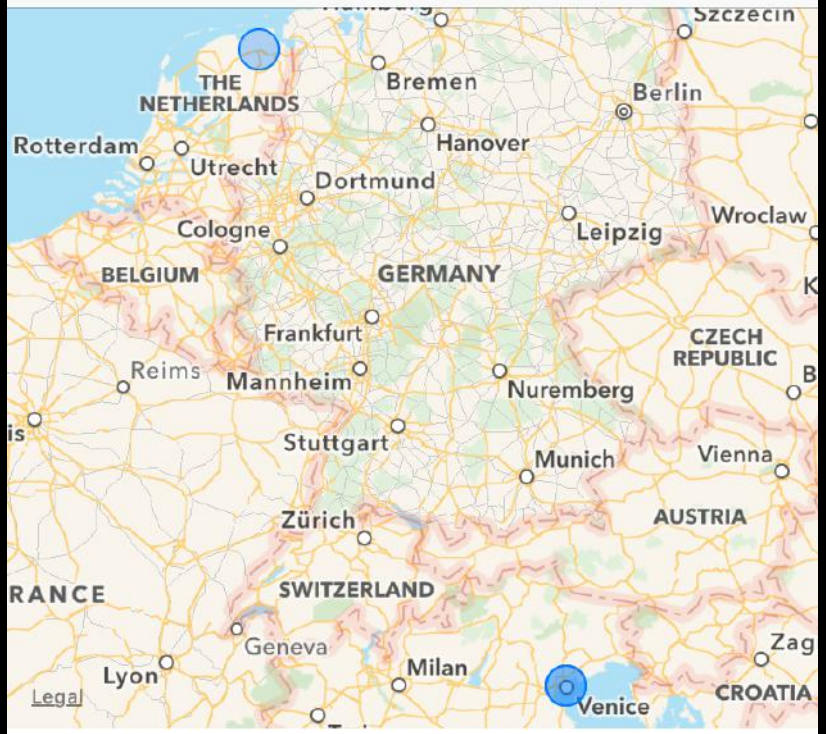

●●○○○ N Telenor
18:50
56 %
Privacy
Location Services
TripAdvisor
While Using
Twitter
Never
Uber
Never
Vivino
While Using
Wallet
While Using
Weather
Always
Wi-Fi SweetSpots
System Services
A purple location services icon will appear next to an item that has recently used your location.
A grey location services icon will appear next to an item that has used your location within the last 24 hours.
An outlined location services icon will appear next to an item that is using a geofence.
A geofence is a virtual perimeter around a location. Apps use geofencing to notify you when you arrive at or leave these locations.


●●○○○ N Telenor
18:50
56 %
Location Services
System Services
Motion Calibration & Distance
Safari & Spotlight Suggestions
Setting Time Zone
Share My Location
Wi-Fi Networking
Frequent Locations
On
PRODUCT IMPROVEMENT
Diagnostics & Usage
Popular Near Me
Routing & Traffic
Improve Maps
Allow Apple to use your frequent location information to improve Maps. About Improve Maps & Privacy...
A purple location services icon will appear next to an item that has recently used your location


●●○○○ N Telenor
18:51
56 %
System Services
Frequent Locations
Frequent Locations
Allow your iPhone to learn places you frequently visit in order to provide useful location-related information.
HISTORY
Nesoddtangen, Akershus
6 locations recorded 09/04/16 - 29/05/16
Nesodden, Akershus
2 locations recorded 27/05/16 - 28/05/16
Oslo, Oslo
6 locations recorded 11/04/16 - 26/05/16
Venice, Veneto
12 locations recorded 21/05/16 - 25/05/16
Italy and The Netherlands
3 locations recorded 11/04/16 - 23/05/16
Clear History...

●●○○○ N Telenor 18:52 55 %

Back **Italy and The Netherlands**



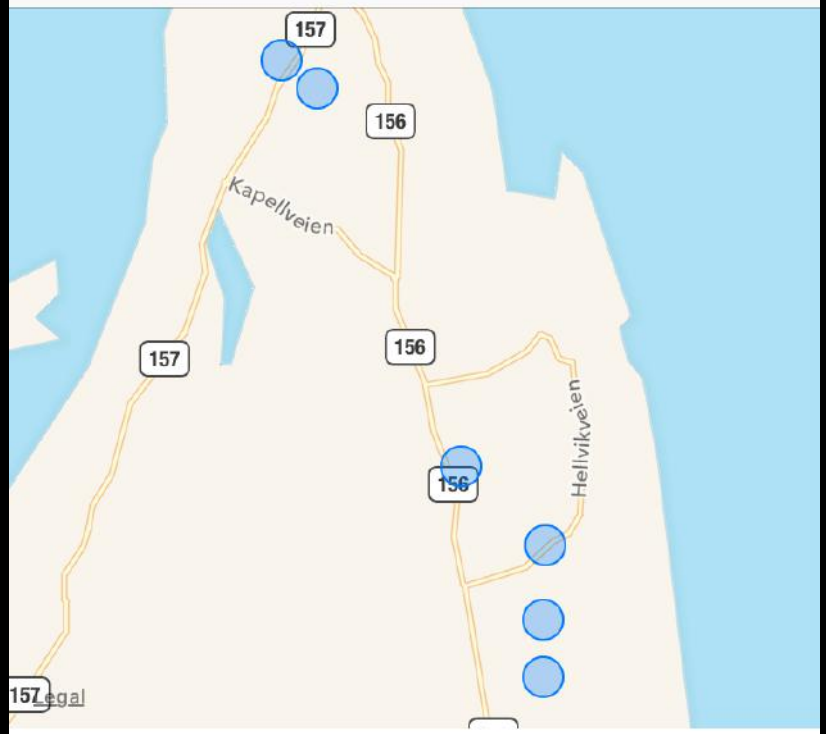
Gedempte Zuiderdiep
5 visits recorded since 11 April 2016

Fondamenta Daniele Manin
2 visits recorded since 23 May 2016

Piazzale de la Colonna
1 visit recorded since 23 May 2016

●●○○○ N Telenor 18:52 55 %

Frequent Locations **Nesoddtangen**



Home
60 visits recorded since 9 April 2016

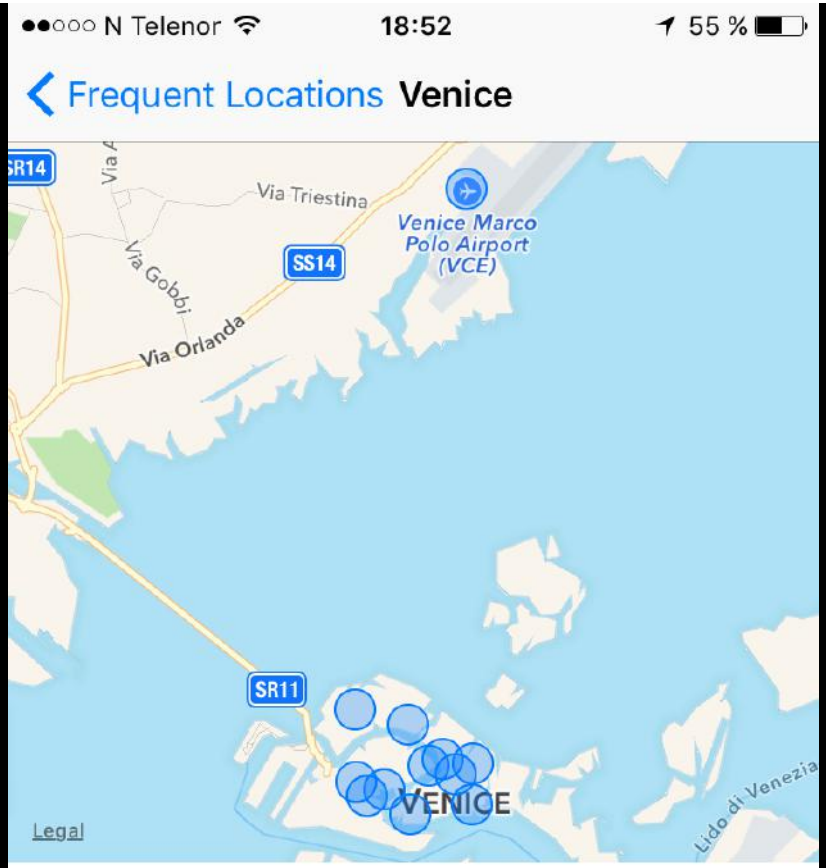
Fjordvangveien
8 visits recorded since 15 April 2016

Bergtunveien
7 visits recorded since 19 April 2016

Vestveien
5 visits recorded since 15 April 2016

Sjølies vei
4 visits recorded since 22 April 2016

Kongleveien
3 visits recorded since 16 April 2016



Calle del Campanel detta Civran o Grimani
12 visits recorded since 21 May 2016

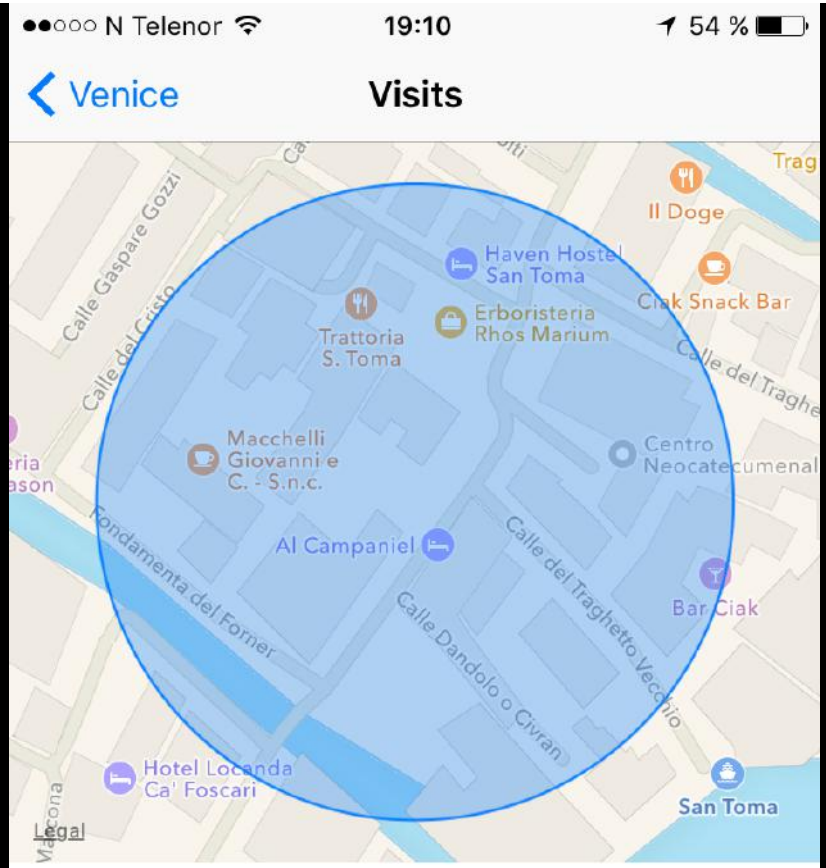
Campo Rialto Novo
8 visits recorded since 21 May 2016

Calle de la Madona
7 visits recorded since 22 May 2016

Corte del Fontego
7 visits recorded since 21 May 2016

Sotoportego del Stramazzer o Sernagiotto
3 visits recorded since 23 May 2016

Fondamenta Minotto
2 visits recorded since 24 May 2016



09:45 - 10:00
25/05/16

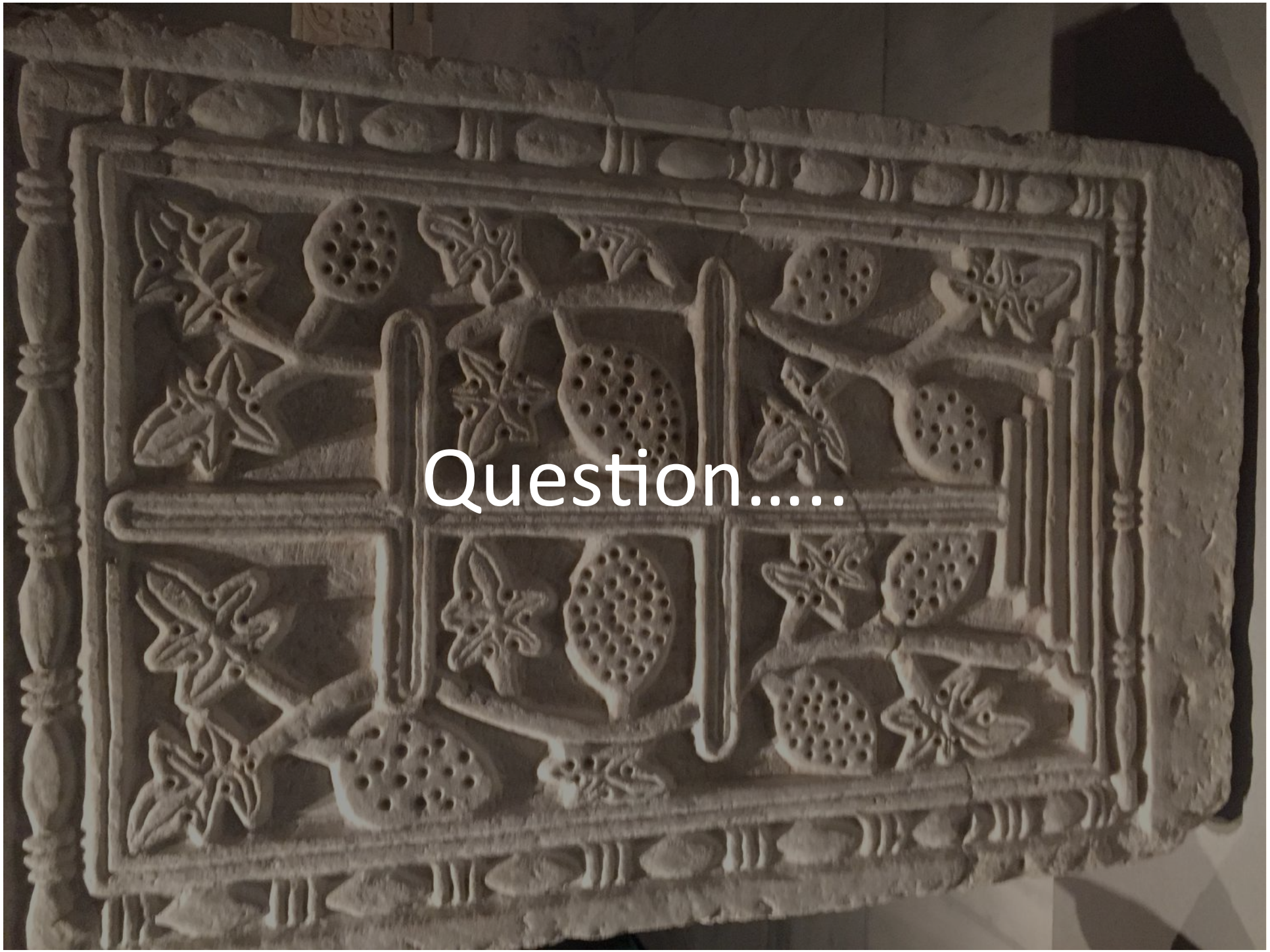
22:15 - 09:15
24/05/16 - 25/05/16

15:30 - 17:45
24/05/16

22:45 - 09:30
23/05/16 - 24/05/16

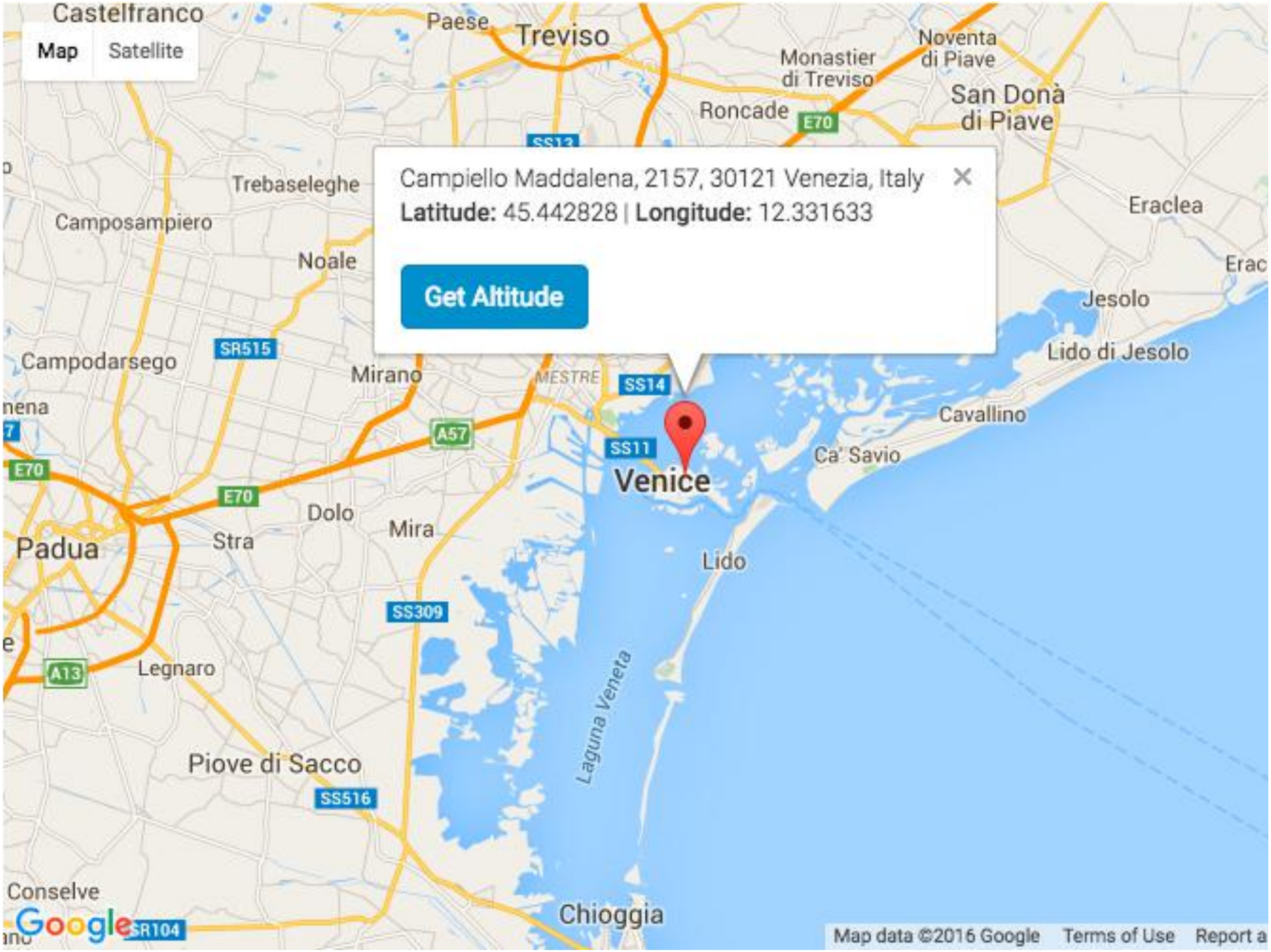
18:30 - 20:00
23/05/16

09:45 - 10:15
23/05/16

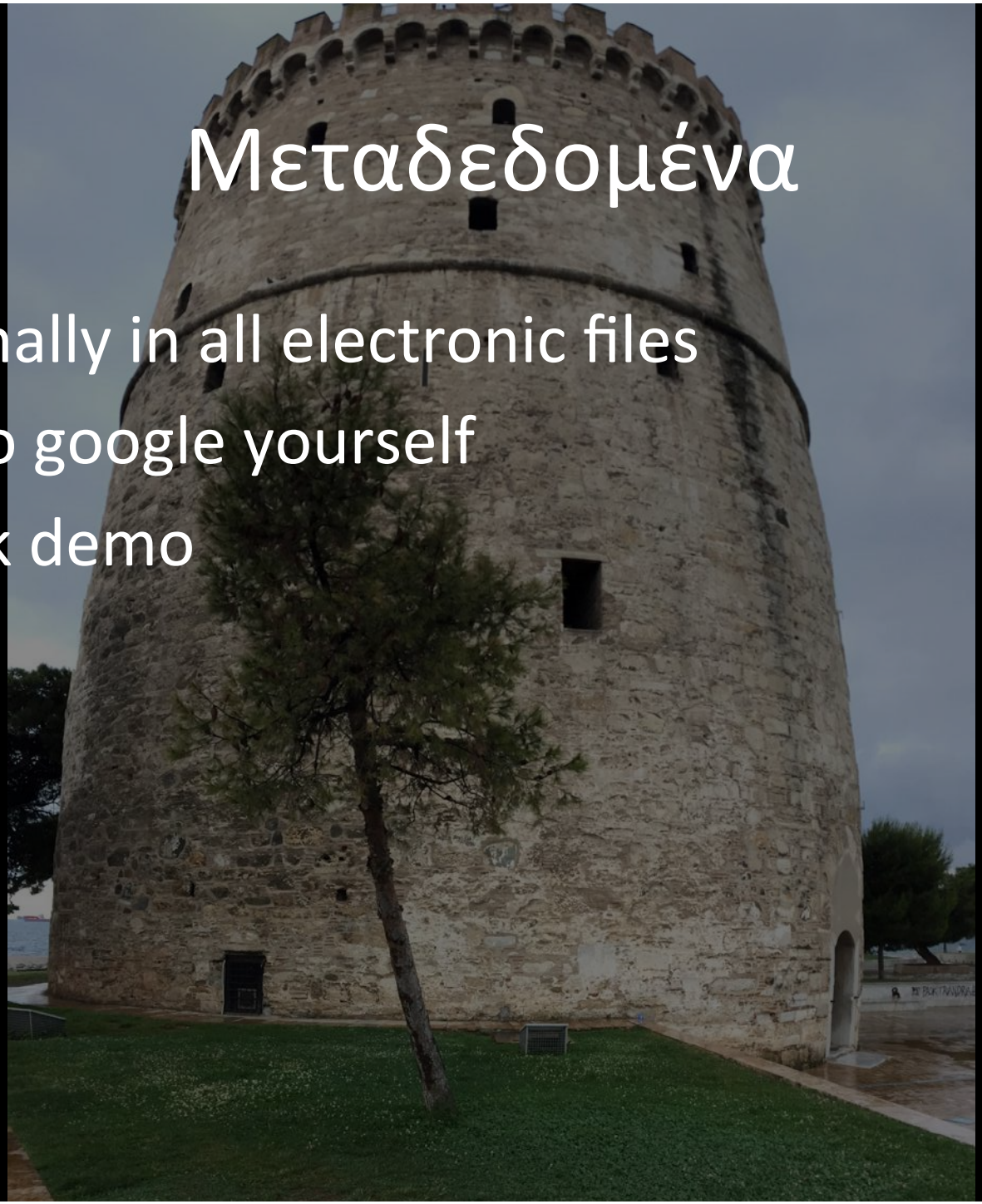

Question……


Where is this picture taken?

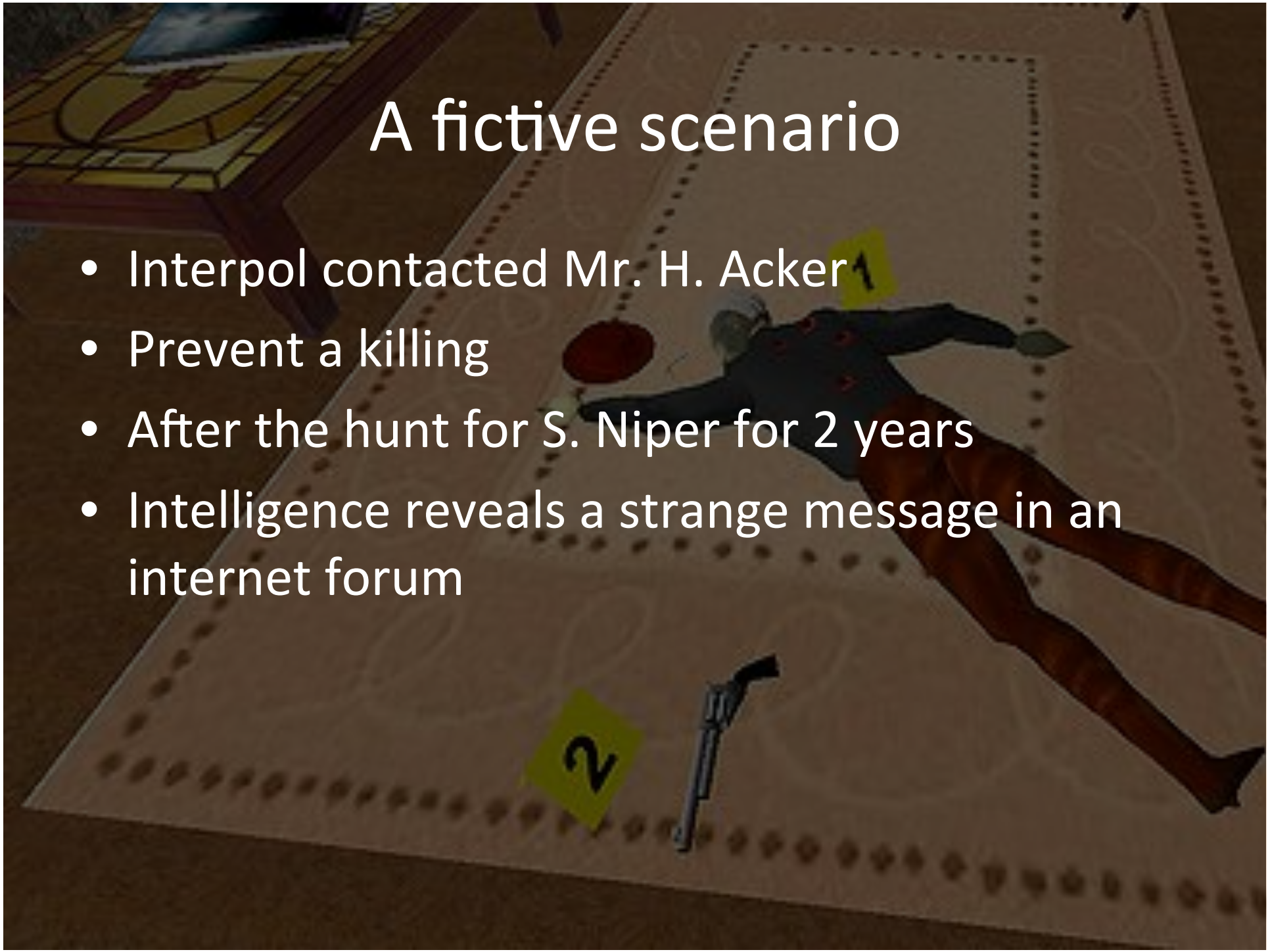

exiftool -gpsposition where_is_this.jpg


Map
Satellite
Campiello Maddalena, 2157, 30121 Venezia, Italy
Latitude: 45.442828 | Longitude: 12.331633
Get Altitude
Castelfranco
Paese
Treviso
Monastier di Treviso
Noventa di Piave
San Donà di Piave
Roncade
E70
Trebaseleghe
Camposampiero
Noale
Eraclea
Jesolo
Lido di Jesolo
Campodarsego
SR515
Mirano
MESTRE
SS14
Cavallino
A57
SS11
Ca' Savio
Venice
E70
Dolo
Mira
Padua
Stra
Lido
SS309
A13
Legnaro
Laguna Veneta
Piove di Sacco
SS516
Conselve
Chioggia
SR104
Google
Map data ©2016 Google
Terms of Use
Report a

Μεταδεδομένα

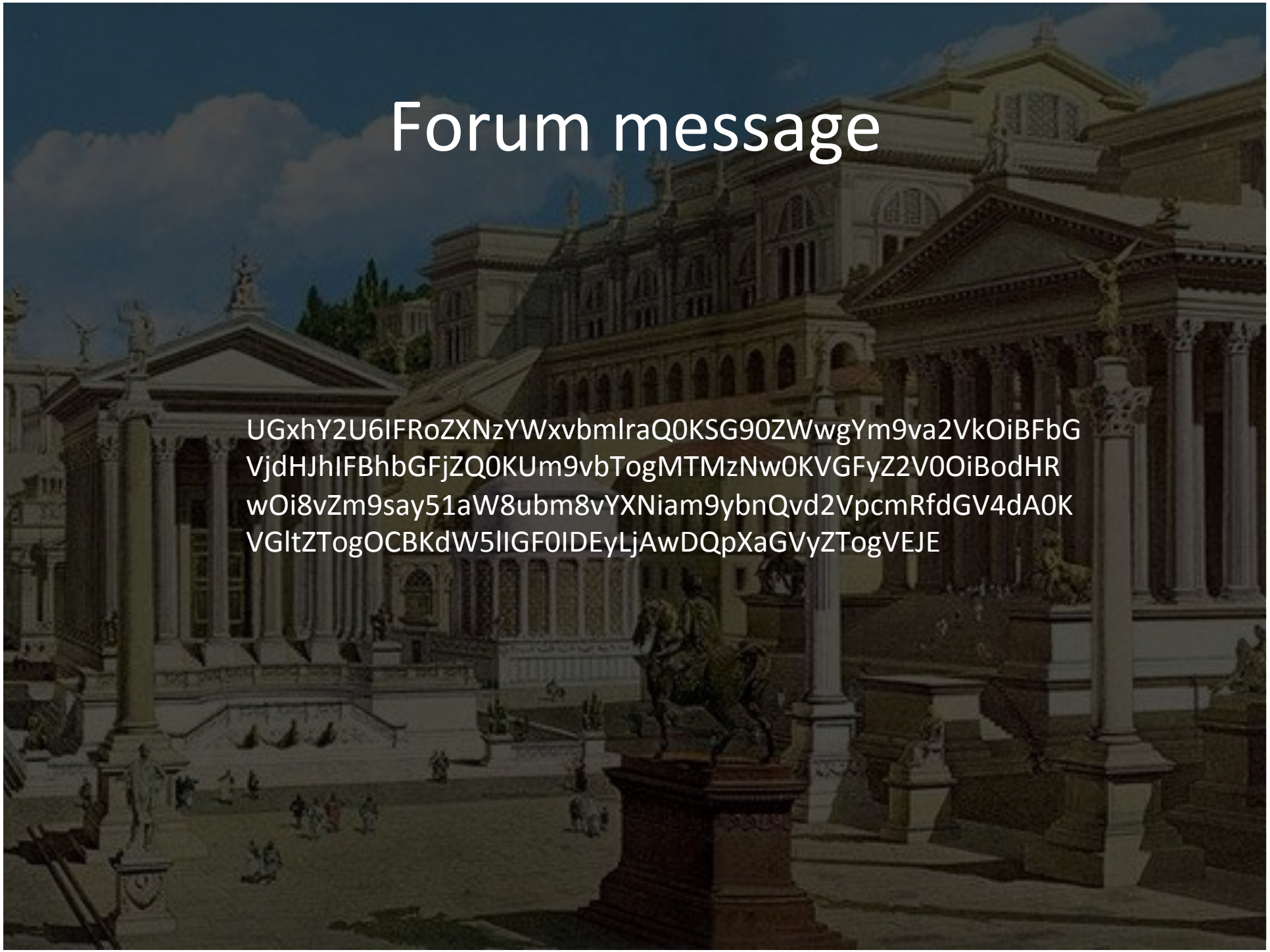


- Normally in all electronic files
- Try to google yourself
- Quick demo



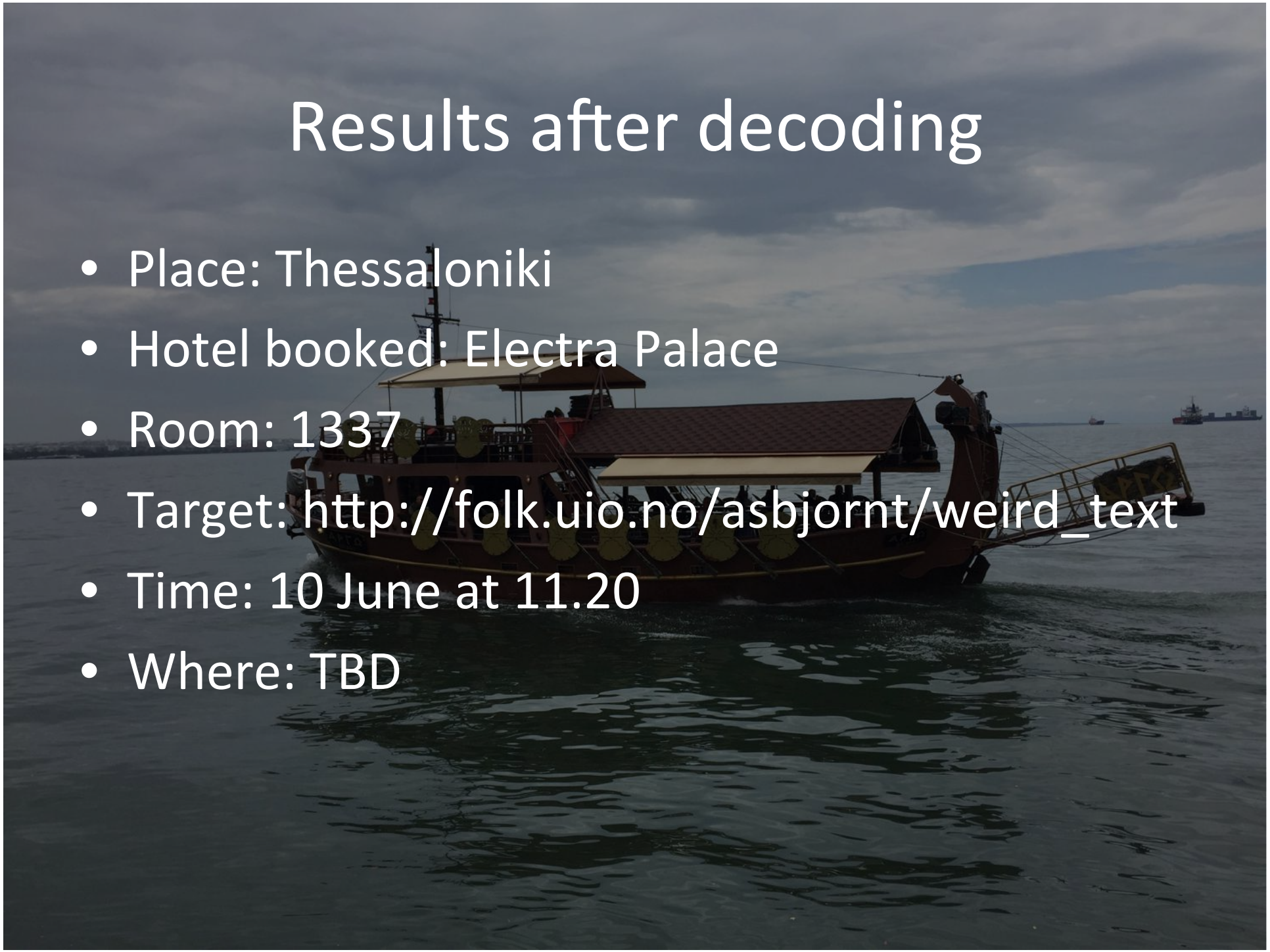
A fictive scenario

- Interpol contacted Mr. H. Acker
- Prevent a killing
- After the hunt for S. Niper for 2 years
- Intelligence reveals a strange message in an internet forum



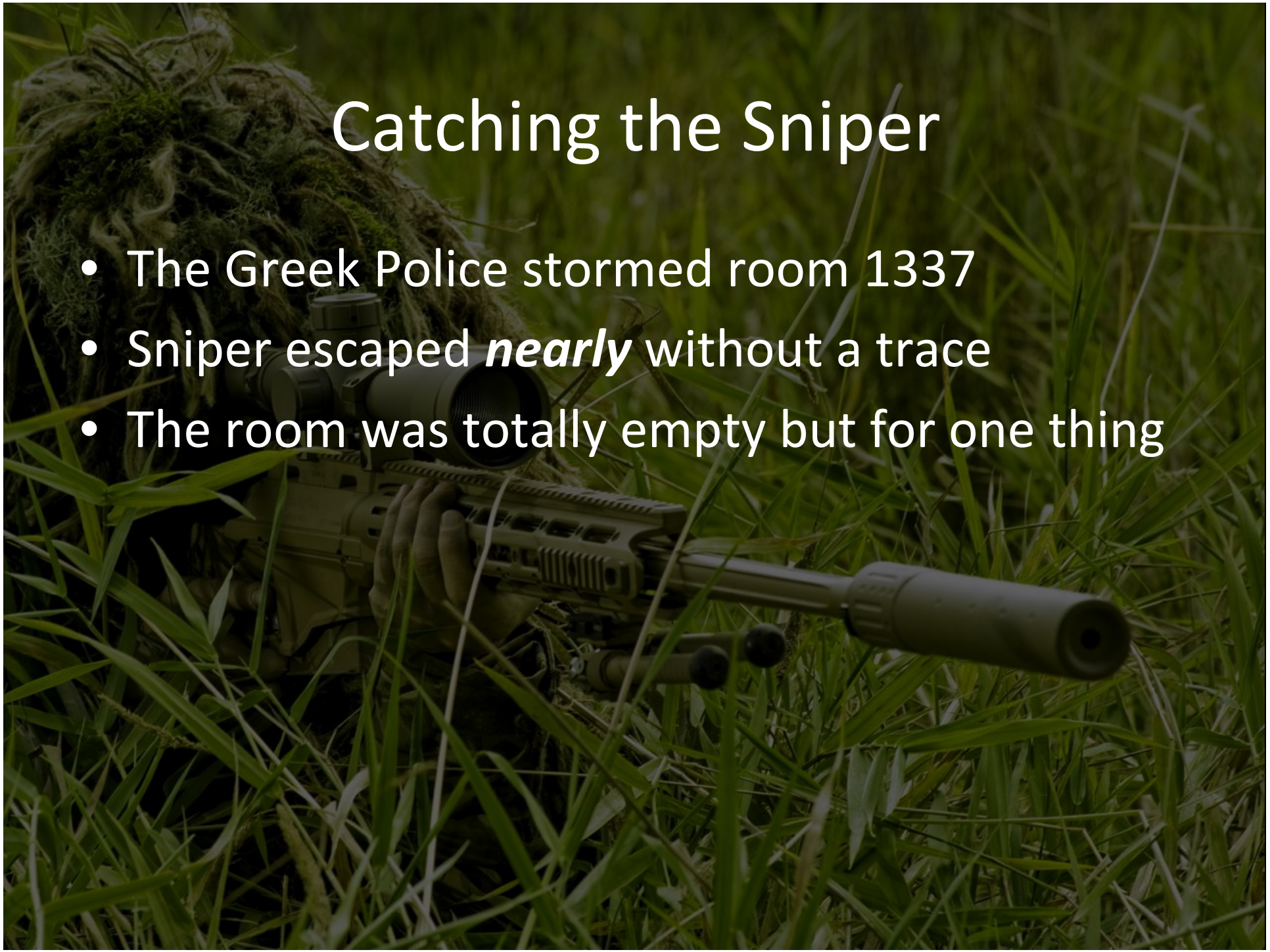
Forum message

UGxhY2U6IFRoZXNzYWxvbmlraQ0KSG90ZWwgYm9va2VkOiBFbG
VjdHJhIFBhbGFjZQ0KUm9vbTogMTMzNw0KVGFyZ2V0OiBodHR
wOi8vZm9say51aW8ubm8vYXNiam9ybnQvd2VpcmRfdGV4dA0K
VGltZTogOCBKdW5lIGF0IDEyLjAwDQpXaGVyZTogVEJE



Results after decoding

- Place: Thessaloniki
- Hotel booked: Electra Palace
- Room: 1337
- Target: http://folk.uio.no/asbjornt/weird_text
- Time: 10 June at 11.20
- Where: TBD



Catching the Sniper

- The Greek Police stormed room 1337
- Sniper escaped ***nearly*** without a trace
- The room was totally empty but for one thing

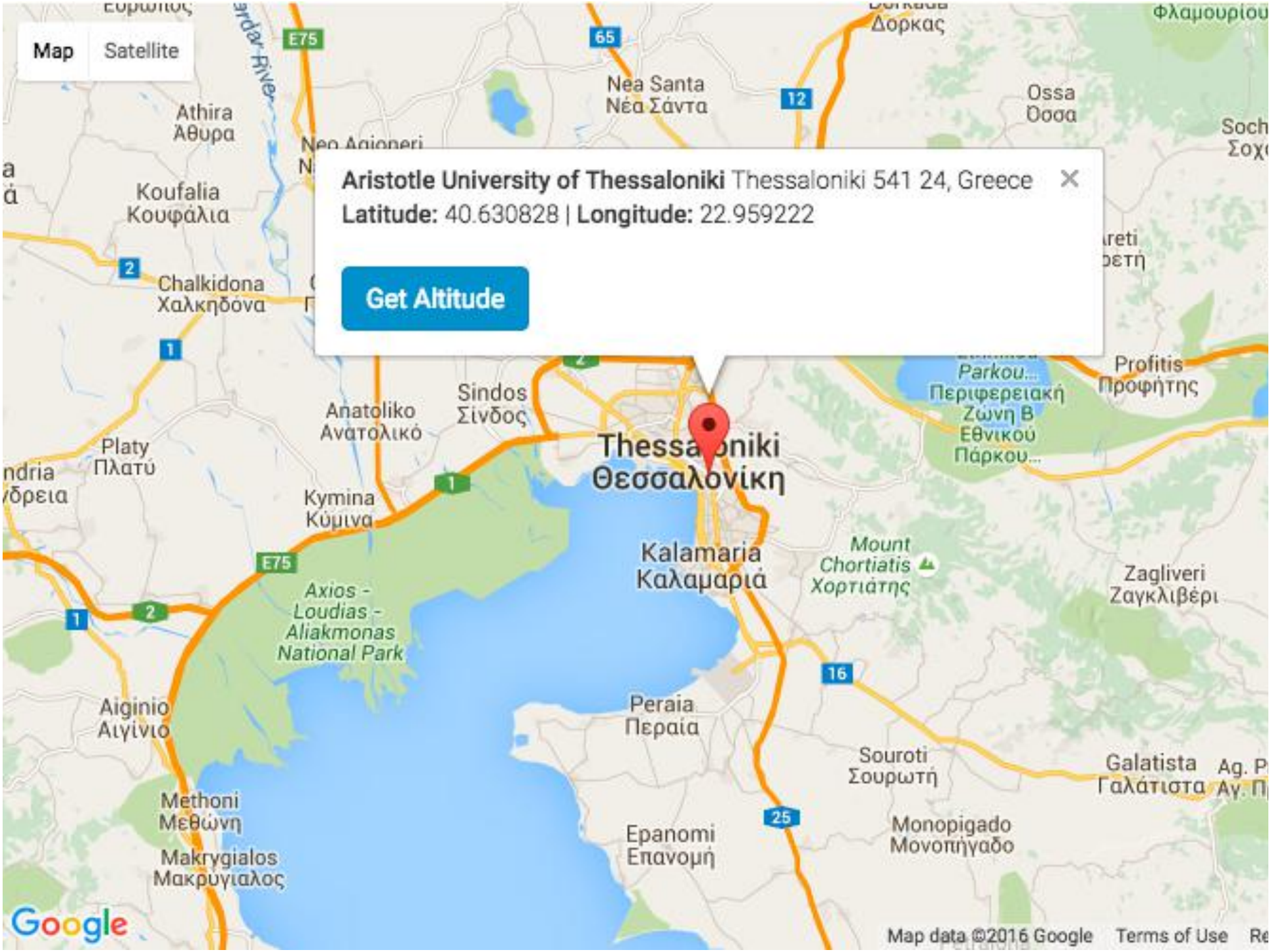

EUNIS
21st CONGRESS
DUNDEE 2015

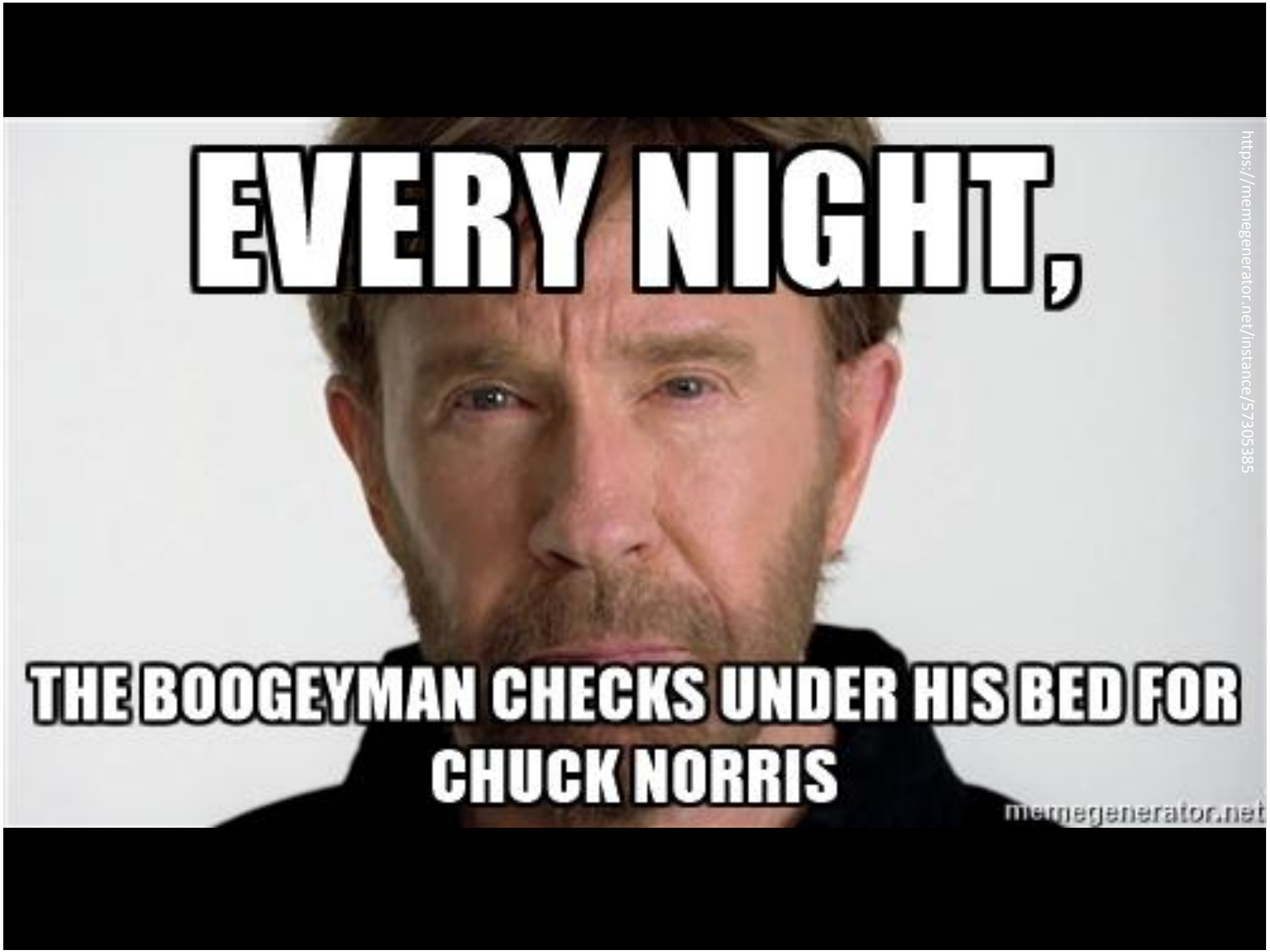
Analyzing the memory stick

- Would you put this usb stick into your laptop?
  - Why?
  - Why not?

Analyzing Data

- Lets look at the files on the memory stick..


Map
Satellite
Aristotle University of Thessaloniki Thessaloniki 541 24, Greece
Latitude: 40.630828 | Longitude: 22.959222
Get Altitude
Athira
Άθυρα
Koufalia
Κουφάλια
Chalkidona
Χαλκηδόνα
Nea Santa
Νέα Σάντα
Ossa
Όσσα
Sindos
Σίνδος
Anatoliko
Ανατολικό
Platy
Πλατύ
Kymina
Κύμινα
Thessaloniki
Θεσσαλονίκη
Kalamaria
Καλαμαριά
Mount
Chortiatis
Χορτιάτης
Zagliveri
Ζαγκλιβέρι
Profitis
Προφήτης
Axios -
Loudias -
Aliakmonas
National Park
Aiginio
Αιγίνιο
Peraia
Περαία
Souroti
Σουρωτή
Galatista
Γαλάτιστα
Methoni
Μεθώνη
Epanomi
Επανομή
Monopigado
Μονοπήγαδο
Makrygialos
Μακρυγιαλος
Google
Map data ©2016 Google
Terms of Use


EVERY NIGHT,
THE BOOGEYMAN CHECKS UNDER HIS BED FOR CHUCK NORRIS
memegenerator.net
https://memegenerator.net/instance/57305385

Interpol: GOT HIM!

Sum up

- Interpol found a strange forum post
- We used some techniques to drill down to the metadata
- S. Niper did not think about the metadata
- We did!
- Google! Bing!

Exiftool
free and relatively simple

- exiftool -all:all => read all the tags.
- exiftool -all:all= => remove all the tags
- Lots of other tools
- Foca (Chema Alonso)
- http://metadatascrubbing.blogspot.gr/

http://www.giantbomb.com/forums/off-topic-31/are-thumbs-ups-lame-434157/

Slides or Hacked

Your choice ;-)

Thank you for your attention!

Contact info

- Mail: asbjornt@fsat.no
- Twitter: @fuzzerman
- Security blog: https://Reglund.com
- Linkedin: https://no.linkedin.com/in/reglund/

Questions?

http://launchany.com/10-questions-your-api-document-must-answer/