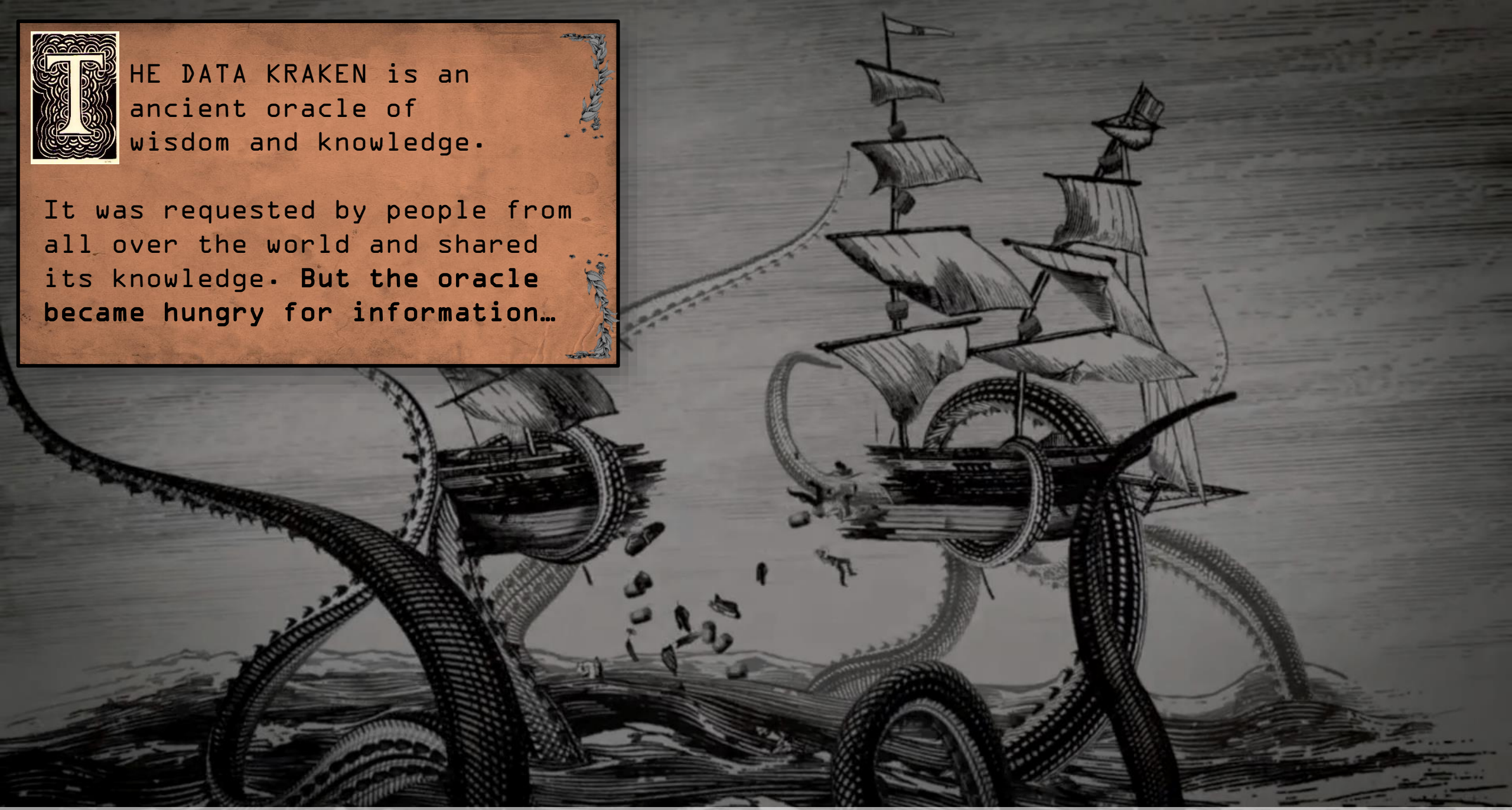
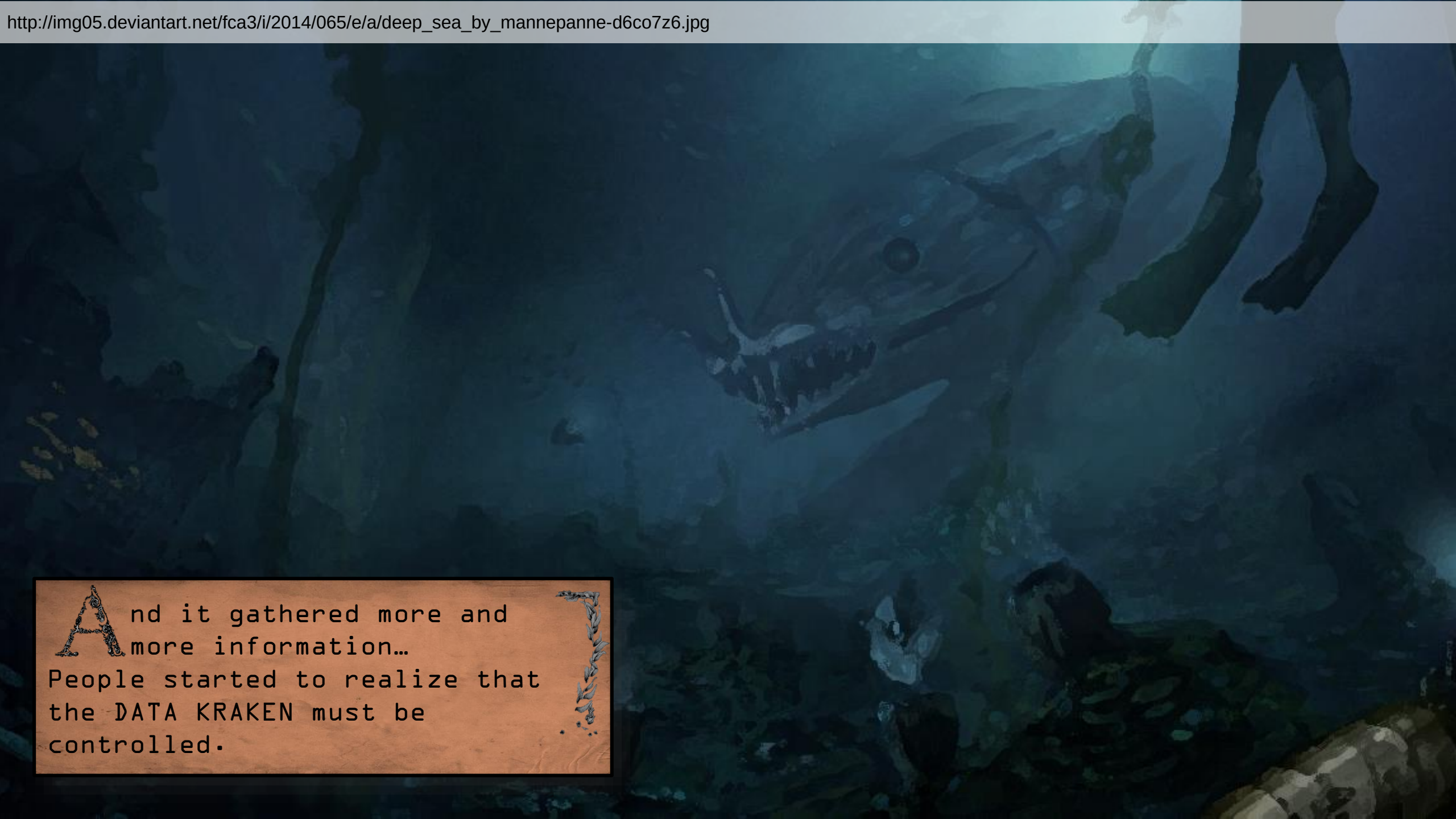


http://www.fubiz.net/wp-content/uploads/2012/03/the-kraken-existence2.jpg

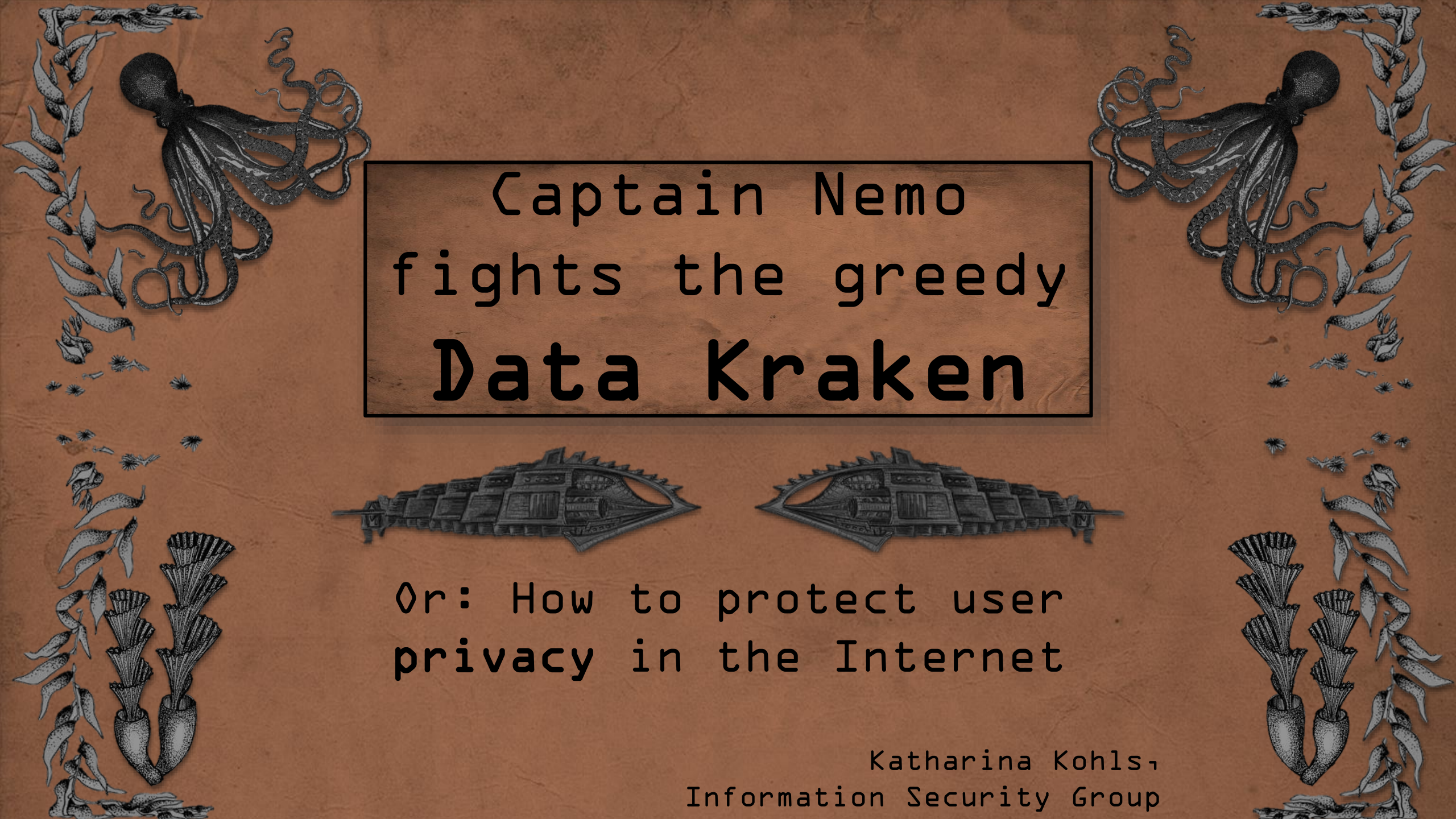
http://www.pxleyes.com/blog/wp-content/uploads/showcases/underwater-digital-paintings/14.jpg

http://www.desktopimages.org/pictures/2015/0727/1/kraken-pics-330784.jpg

http://img05.deviantart.net/fca3/i/2014/065/e/a/deep_sea_by_mannepanne-d6co7z6.jpg



http://geektyrant.com/news/the-wolverine-director-james-mangold-will-helm-captain-nemo-for-disney



Captain Nemo fights the greedy Data Kraken

Or: How to protect user **privacy** in the Internet

Katharina Kohls,
Information Security Group

Privacy Research @ InfSec

Private and anonymous communication, digital forgetting


Anonymous communication
Private communication
Digital forgetting
Nemo Crew
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
50 0 50 100 150
IRELAND
ENGLAND
HOLLAND
Dublin
Waterford
Wexford
Kinsale
Hull
Yarmouth
Southwold Bay
Harwich
Landguard Fort
Gabbard Shoal
Galloper Sand
Kentish Knock
London
Thames
Tilbury
Sheerness
Chatham
North Foreland
Goodwin Sands
Deal
Dover
Dunkirk
Calais
Mardyk
Portsmouth
Plymouth
Portland
Lands End
Falmouth
Scilly Is.
Dartmouth
Cape de la Hogue
Dieppe
Havre
Channel Is.
Bristol
Belle Isle
Schelling
Brandaris
Vlie
Texel
Kykduin
Amsterdam
Katwijk
Scheveningen
Hague
Rotterdam
Bergen-op-Zoom
R. Meuse
R. Rhine
R. Ems
52°
48°
8°
4°
0°
Cambridge University Press.
Stanford's Geog! Estabt, London

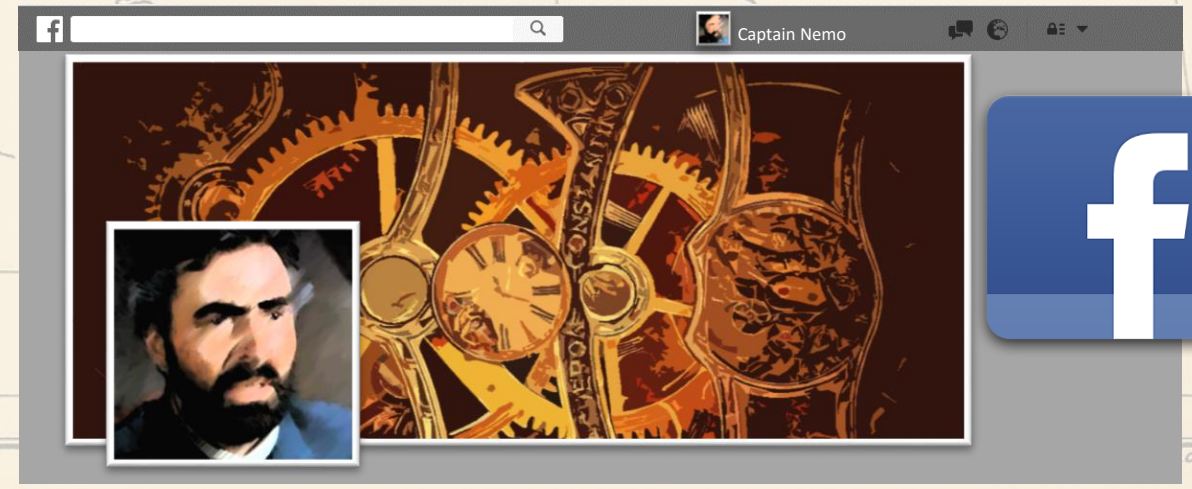

Anonymous communication
Private communication
Nemo Crew
Digital forgetting
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
50 0 50 100 150
IRELAND
ENGLAND
HOLLAND
Dublin
Waterford
Wexford
Kinsale
Hull
Yarmouth
Southwold Bay
Harwich
Landguard Fort
Gabbard Shoal
Galloper Sand
Kentish Knock
London
Thames
Tilbury
Sheerness
Chatham
North Foreland
Goodwin Sands
Deal
Dover
Dunkirk
Calais
Gravelines
Mardyk
Beachy Head
Portsmouth
Isle of Wight
St Helens
Portland
Plymouth
Tor Bay
Dartmouth
Falmouth
Lands End
Scilly Is.
Cape de la Hogue
Channel Is.
Dieppe
Havre
Bristol
R. Blavet
Belle Isle
Schelling
Brandaris
Vlie
Texel
Kykduin
Amsterdam
Katwijk
Scheveningen
Hague
Rotterdam
Helvoetsluis
Bergen-op-Zoom
R. Meuse
R. Rems
52°
48°
8°
4°
0°
Cambridge University Press.
Stanford's Geog! Estabt, London

Anonymous communication

Private communication

Nemo Crew

Digital forgetting

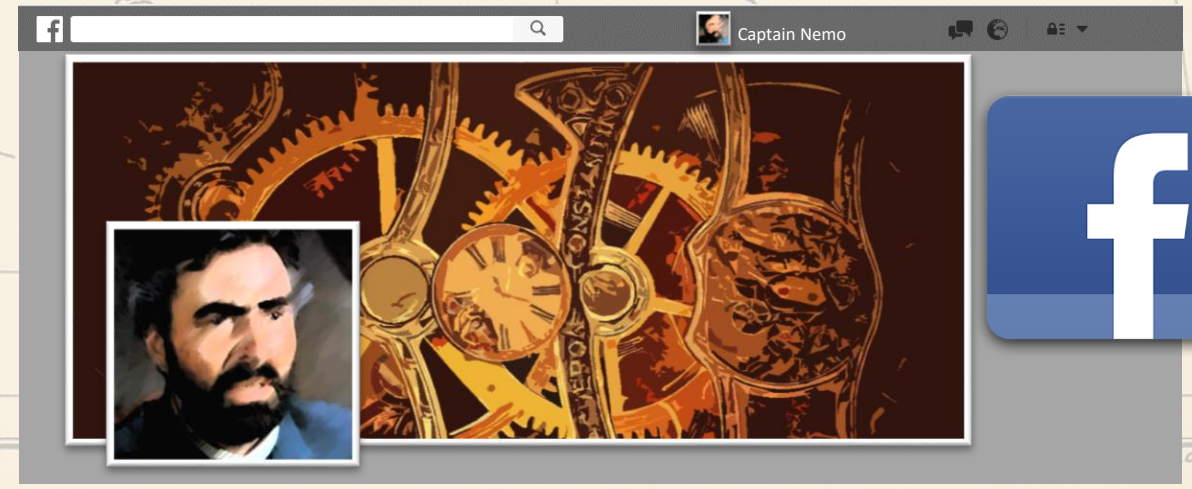


Anonymous communication

Private communication

Nemo Crew

Digital forgetting



Anonymous communication

Private communication

Digital forgetting

Nemo Crew

NORTH SEA AND ENGLISH CHANNEL

THE ANGLO-DUTCH WARS OF THE 17TH CENTURY

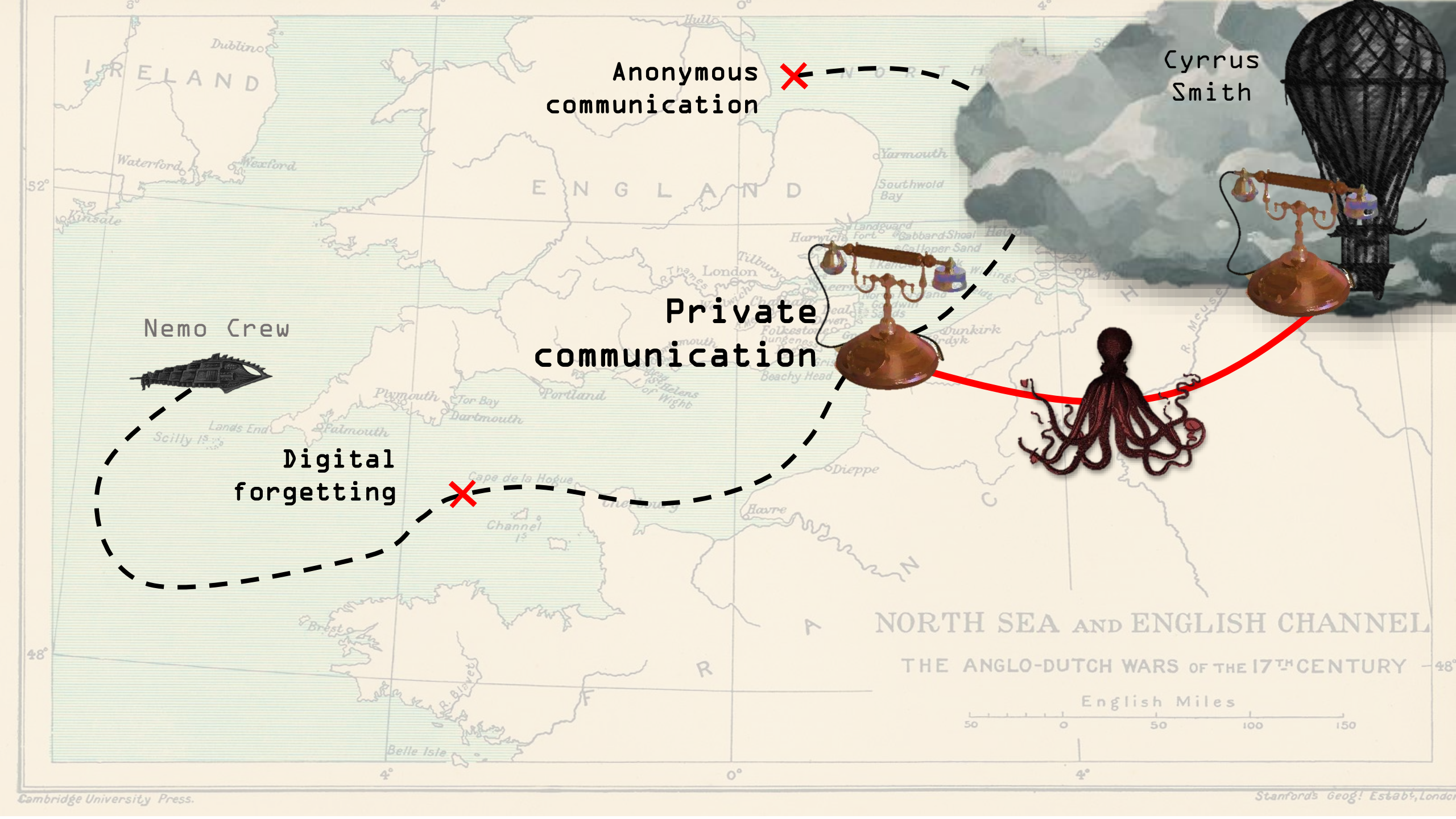
English Miles

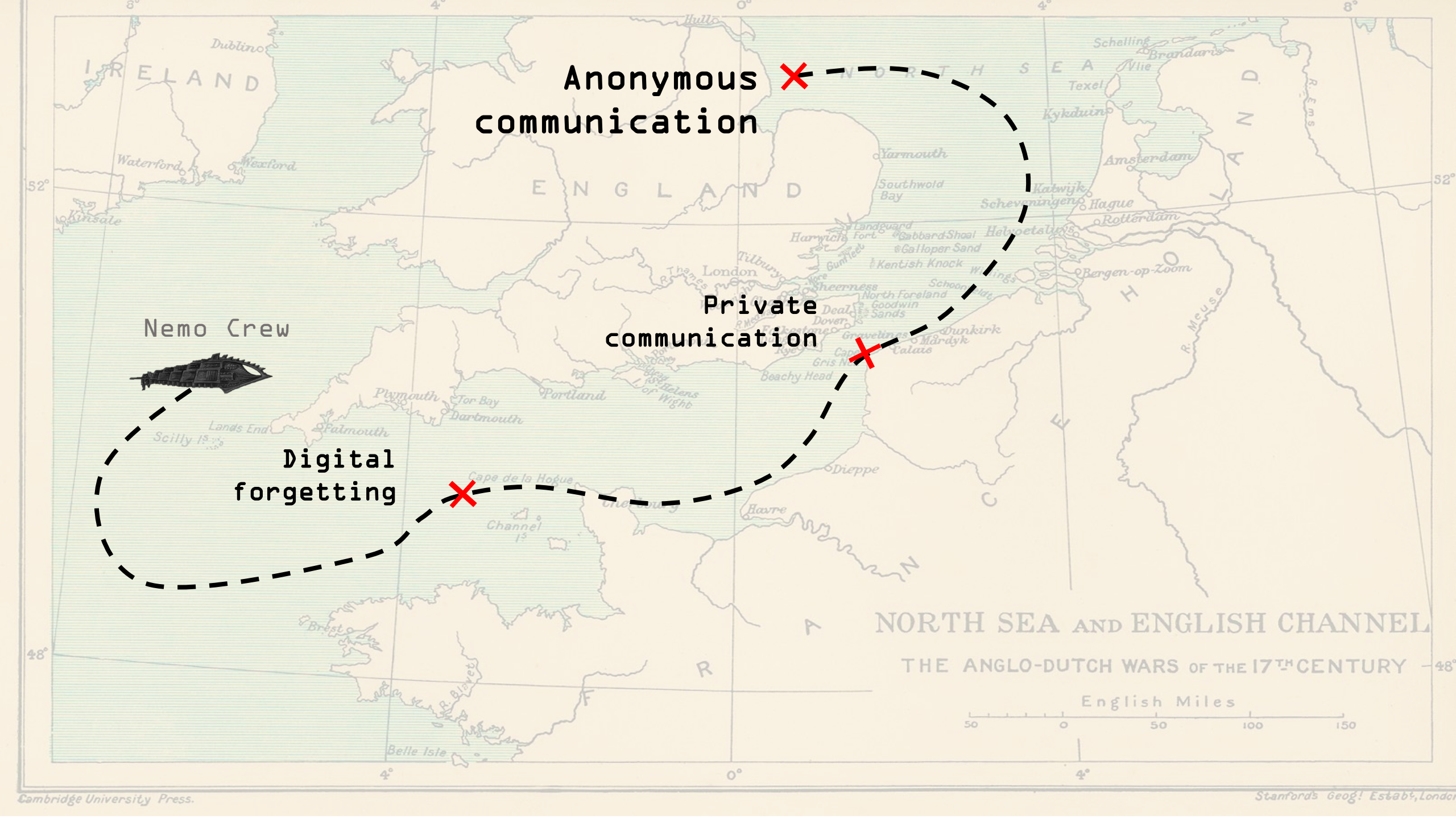
50 0 50 100 150

Cambridge University Press.

Stanford's Geog! Estabt, London


Anonymous
communication
Cyrrus
Smith
Private
communication
Nemo Crew
Digital
forgetting
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
IRELAND
ENGLAND
Cambridge University Press.
Stanford's Geog! Estabt, London


Anonymous
communication
Cyrrus
Smith
Private
communication
Nemo Crew
Digital
forgetting
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
IRELAND
ENGLAND
Cambridge University Press.


Anonymous communication
Private communication
Digital forgetting
Nemo Crew
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
50 0 50 100 150
IRELAND
ENGLAND
HOLLAND
Dublin
Waterford
Wexford
Kinsale
Hull
Yarmouth
Southwold Bay
Harwich
Landguard Fort
Gabbard Shoal
Galloper Sand
Kentish Knock
London
Tilbury
Sheerness
North Foreland
Goodwin Sands
Deal
Dover
Dunkirk
Calais
Gravelines
Mardyk
Beachy Head
Rye
Portland
Plymouth
Tor Bay
Dartmouth
Falmouth
Lands End
Scilly Is.
St Helens
I. of Wight
Cape de la Hogue
Cherbourg
Dieppe
Havre
Channel Is.
Bristol
R. Blavet
Belle Isle
Schelling
Brandaris
Vlie
Texel
Kykduin
Amsterdam
Katwijk
Scheveningen
Hague
Rotterdam
Helvoetsluis
Bergen-op-Zoom
R. Meuse
R. Rhine
R. Thames
52°
48°
8°
4°
0°
Cambridge University Press.
Stanford's Geog! Estabt, London

Anonymous communication

Private communication

Digital forgetting

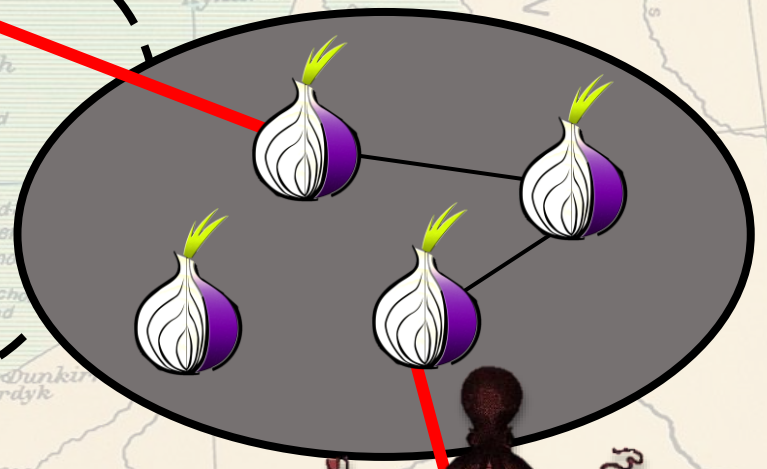
Nemo Crew

Anonymous communication

Private communication

Nemo Crew

Digital forgetting



Anonymous communication

Nemo Crew

Private communication

Digital forgetting

NORTH SEA AND ENGLISH CHANNEL

THE ANGLO-DUTCH WARS OF THE 17TH CENTURY

English Miles

50 0 50 100 150

Cambridge University Press.

Stanford's Geog! Estabt, London

Anonymous
communication
Tor anti traffic
analysis

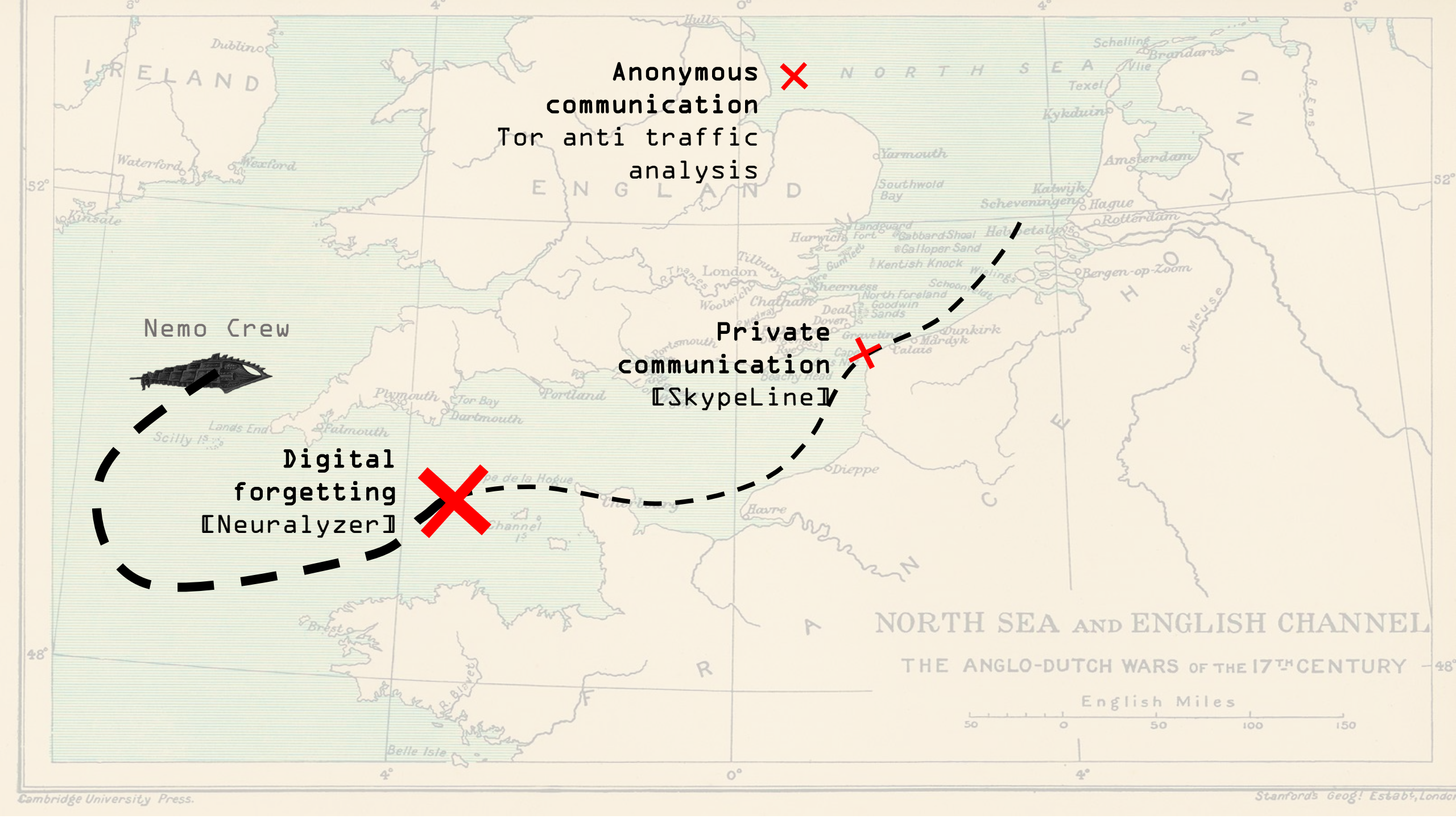
Nemo Crew

Private
communication
[SkypeLine]

Digital
forgetting
[Neuralyzer]

NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
50 0 50 100 150

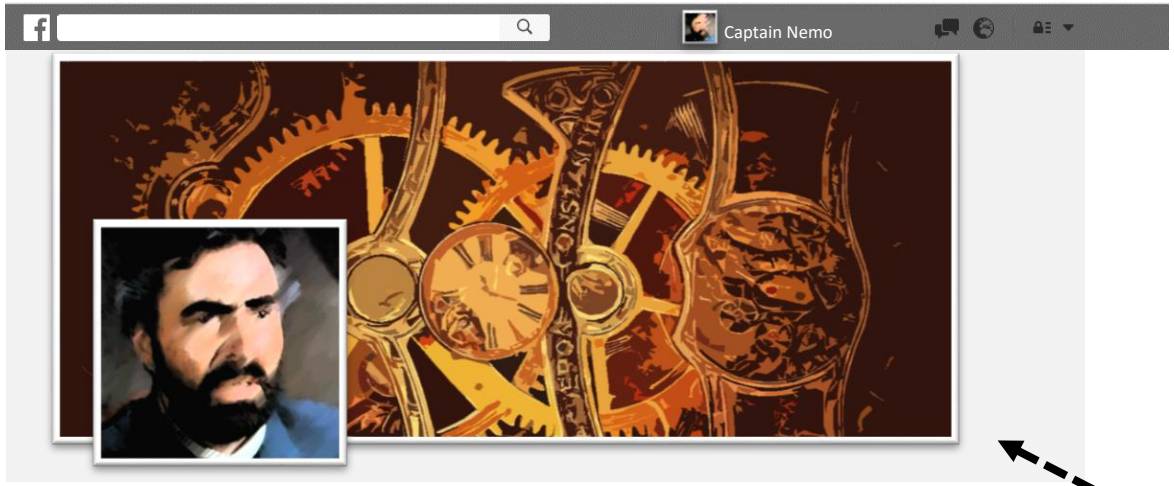
Cambridge University Press.
Stanford's Geog! Estabt, Londo


Anonymous
communication
Tor anti traffic
analysis
Nemo Crew
Private
communication
[SkypeLine]
Digital
forgetting
[Neuralyzer]
NORTH SEA AND ENGLISH CHANNEL
THE ANGLO-DUTCH WARS OF THE 17TH CENTURY
English Miles
Cambridge University Press.

Neuralyzer

Flexible expiration times for the revocation of online data

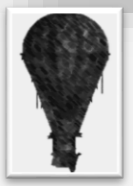
(CODASPY ‘16)


Captain Nemo

Captain Nemo

Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm

Nautilus II – beauty isn't she? 😍😍

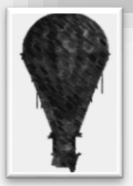


Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm

Captain Nemo

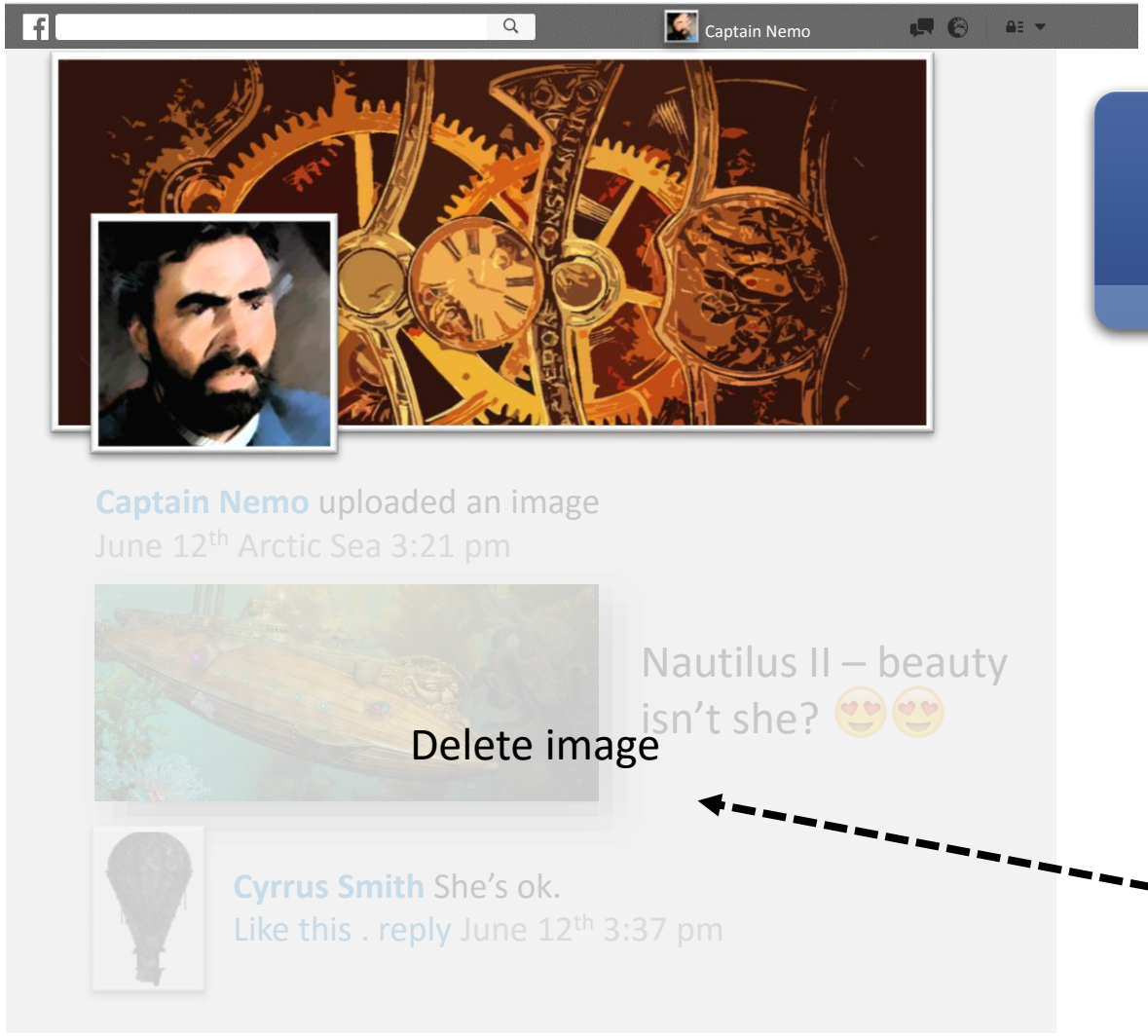
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm

Nautilus II – beauty isn't she? 😍😍



Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm

Facebook data storage



Facebook data storage

No control over servers:
no ultimate revocation

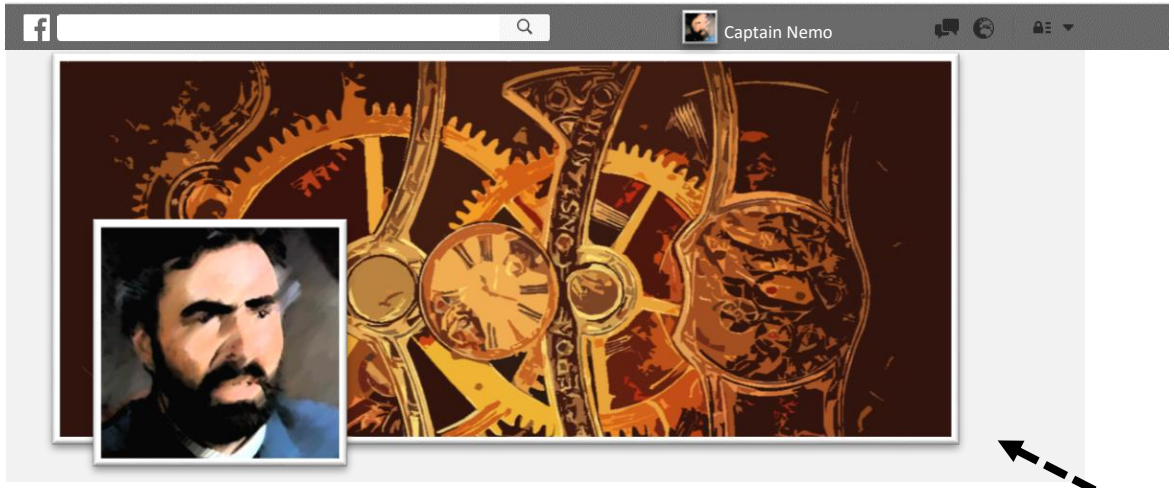
Motivation

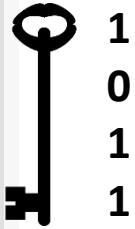
Problem:

Once you upload data to the Internet, you can hardly revoke it later.

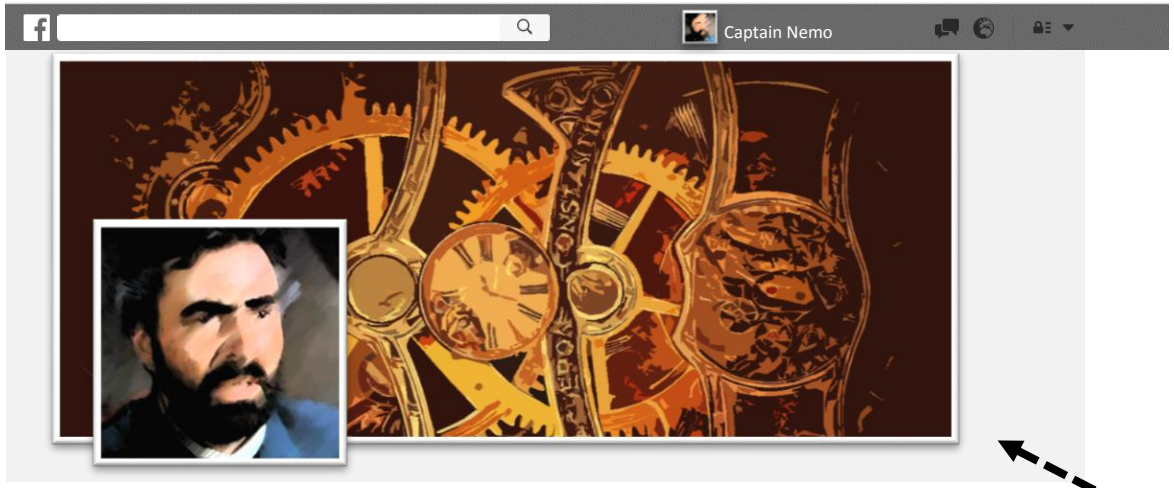
Solution:

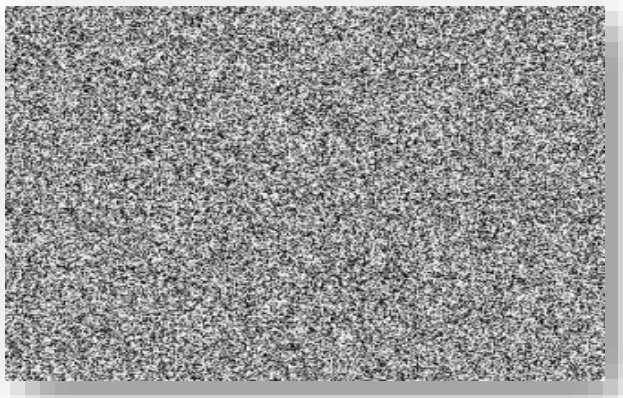
- Encrypt data before upload
- Use distributed infrastructure to share key
- Let key expire to revoke access
- **User requests define lifetime of key**



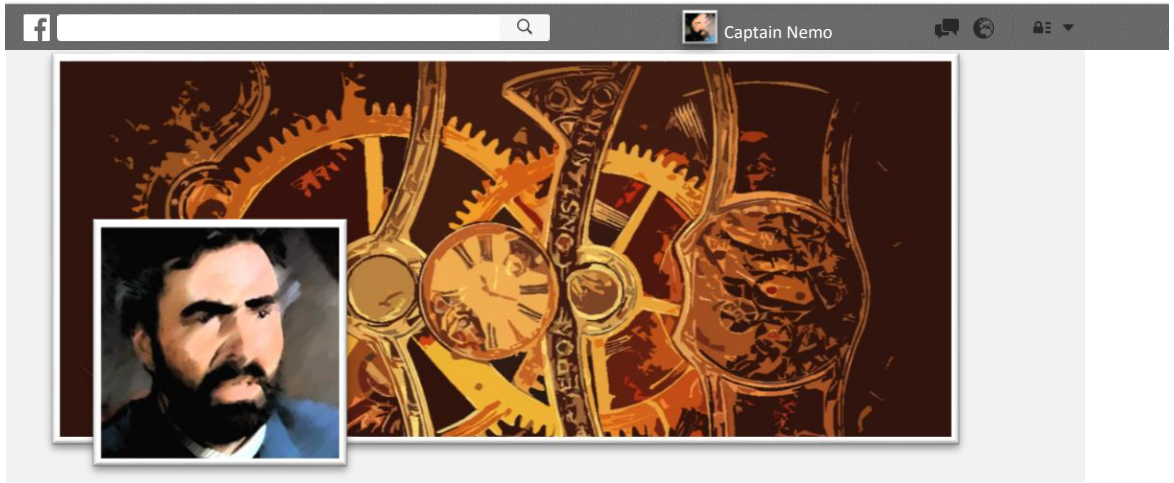


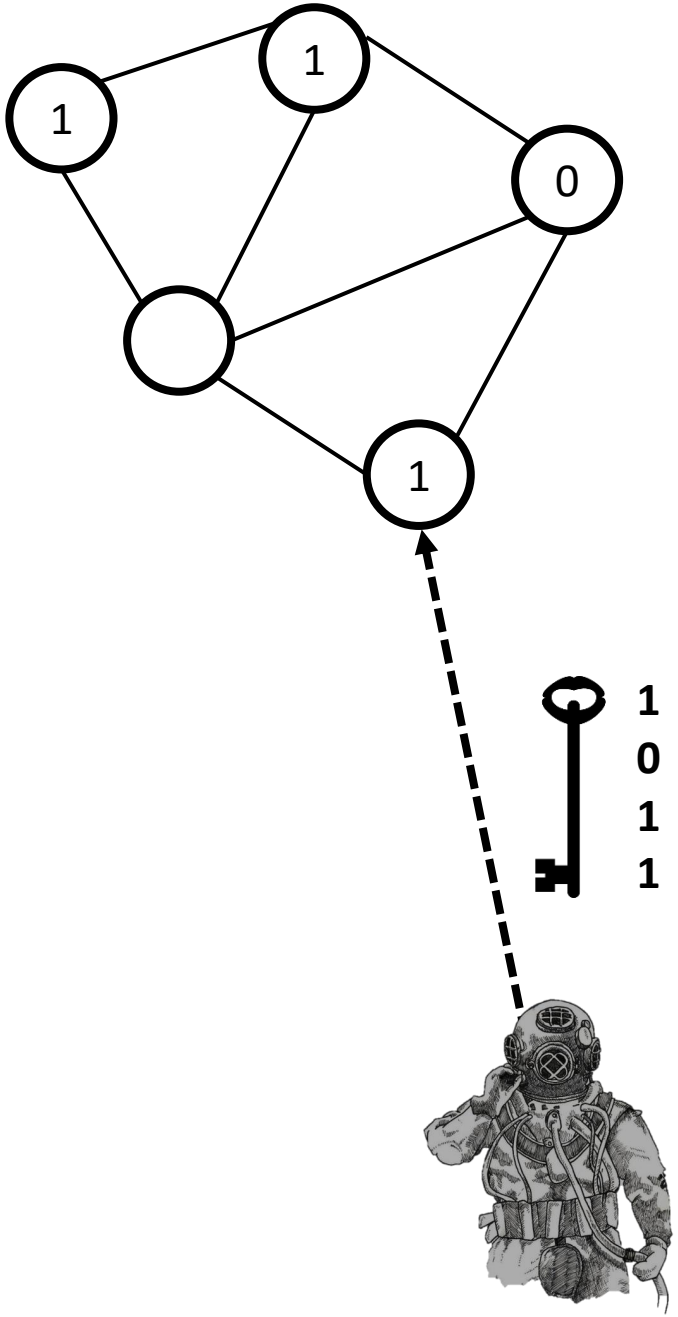
1
0
1
1

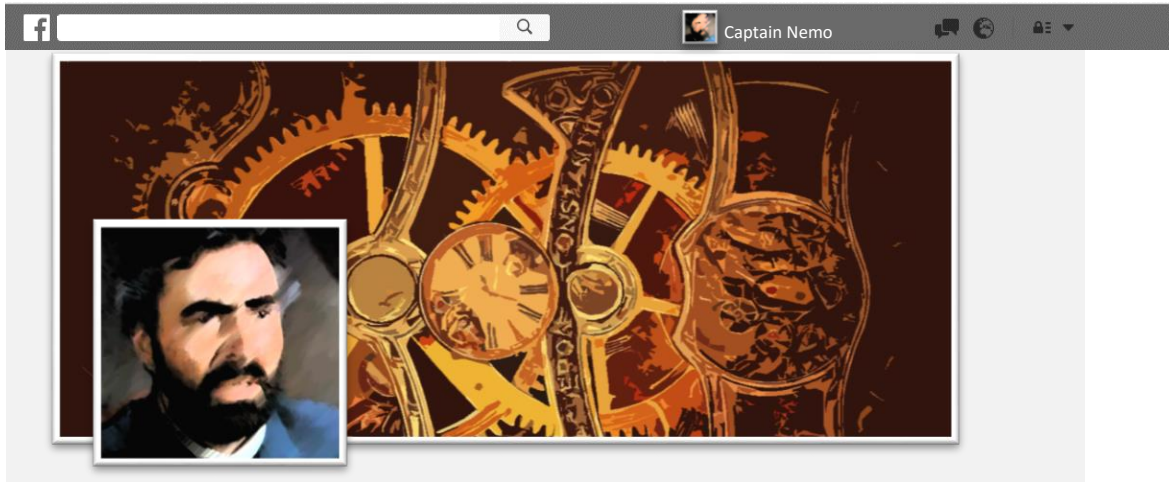


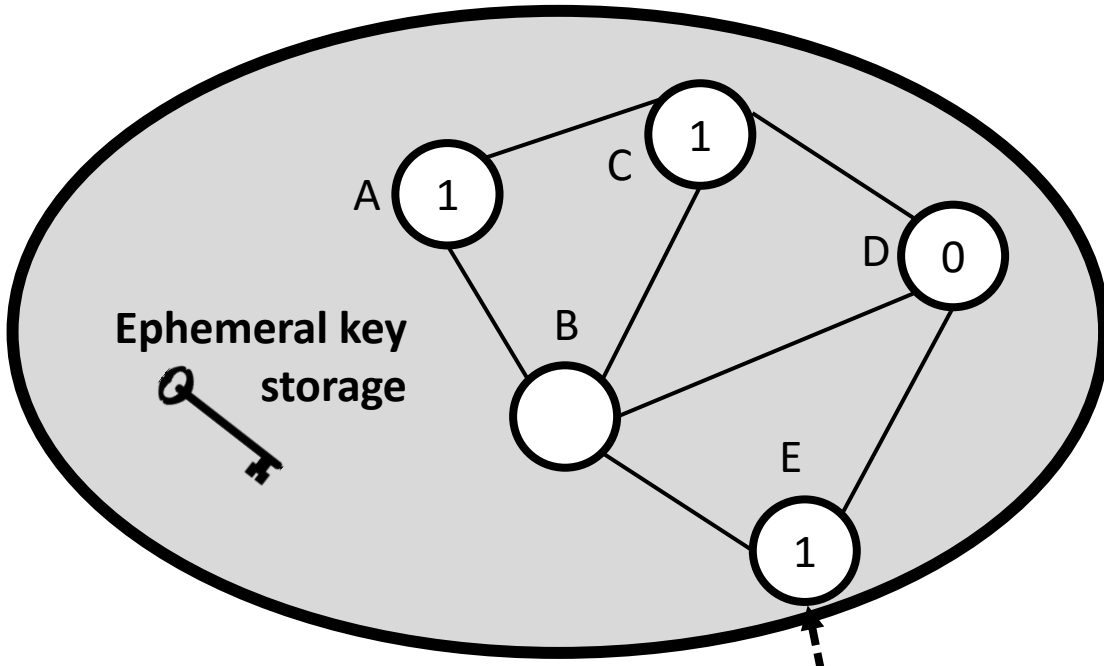


1
0
1
1


Captain Nemo


1
1
0
1
1
0
1
1



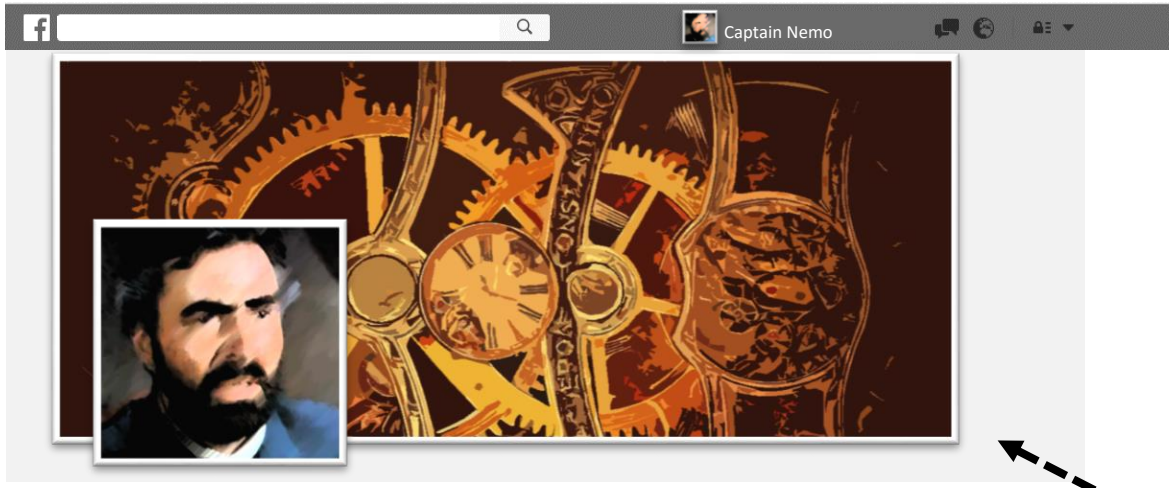


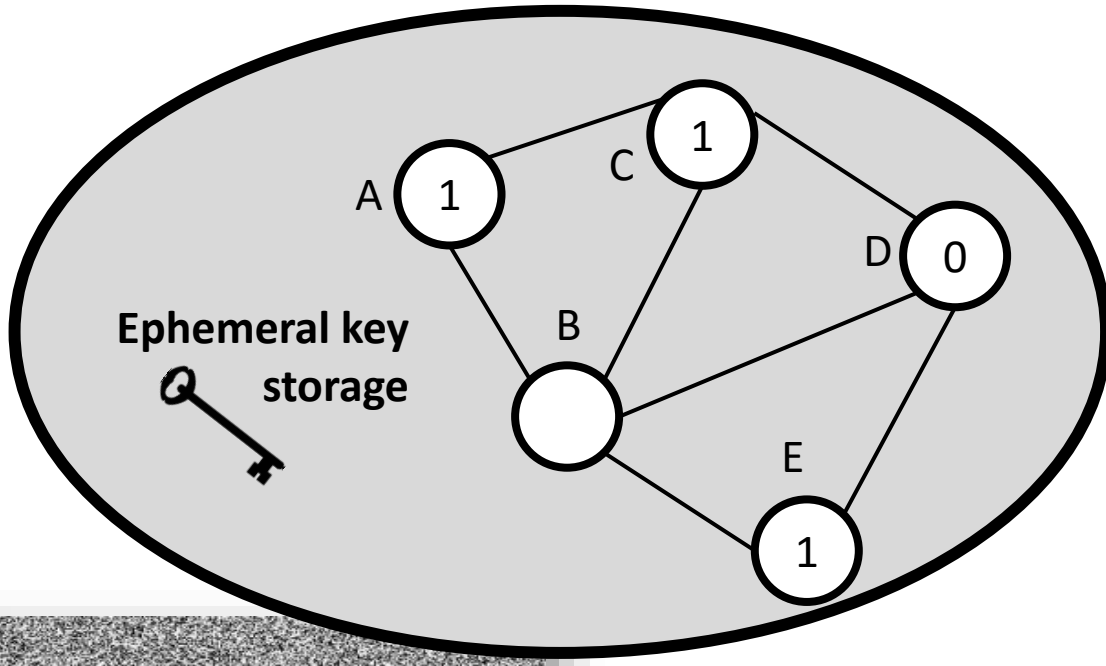
DNS infrastructure

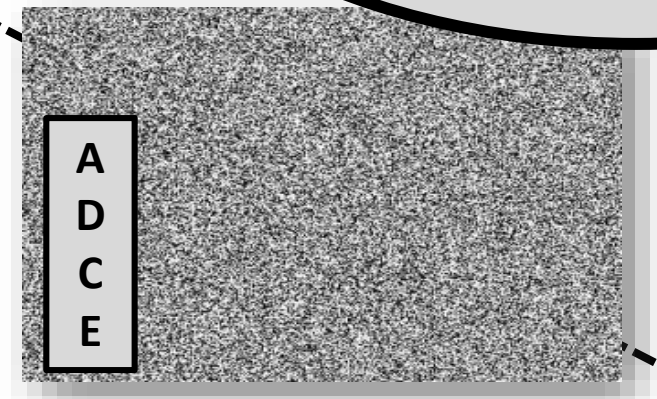
- 1-bits are *cached* entries in resolvers
- 0-bits are *uncached* entries

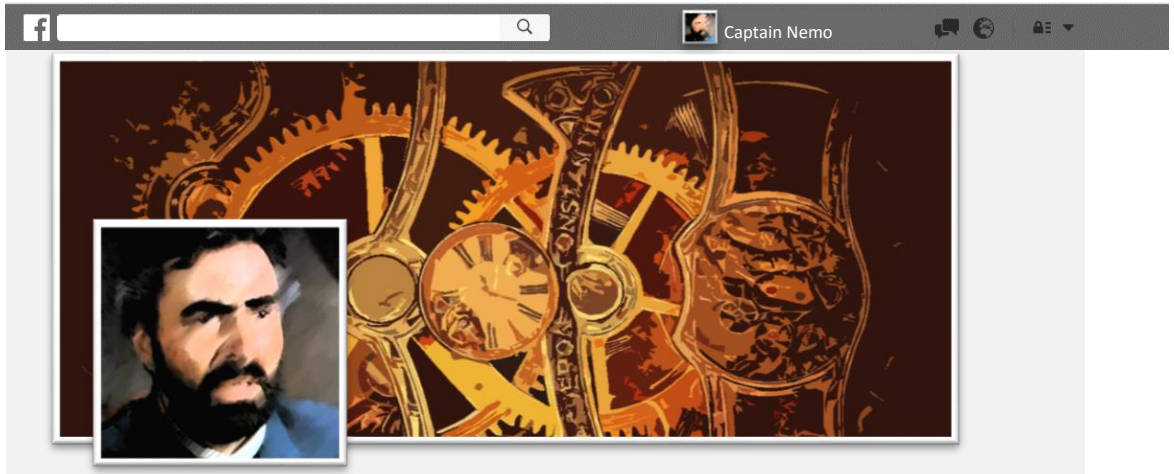
→Perform recursive DNS requests to cache domains

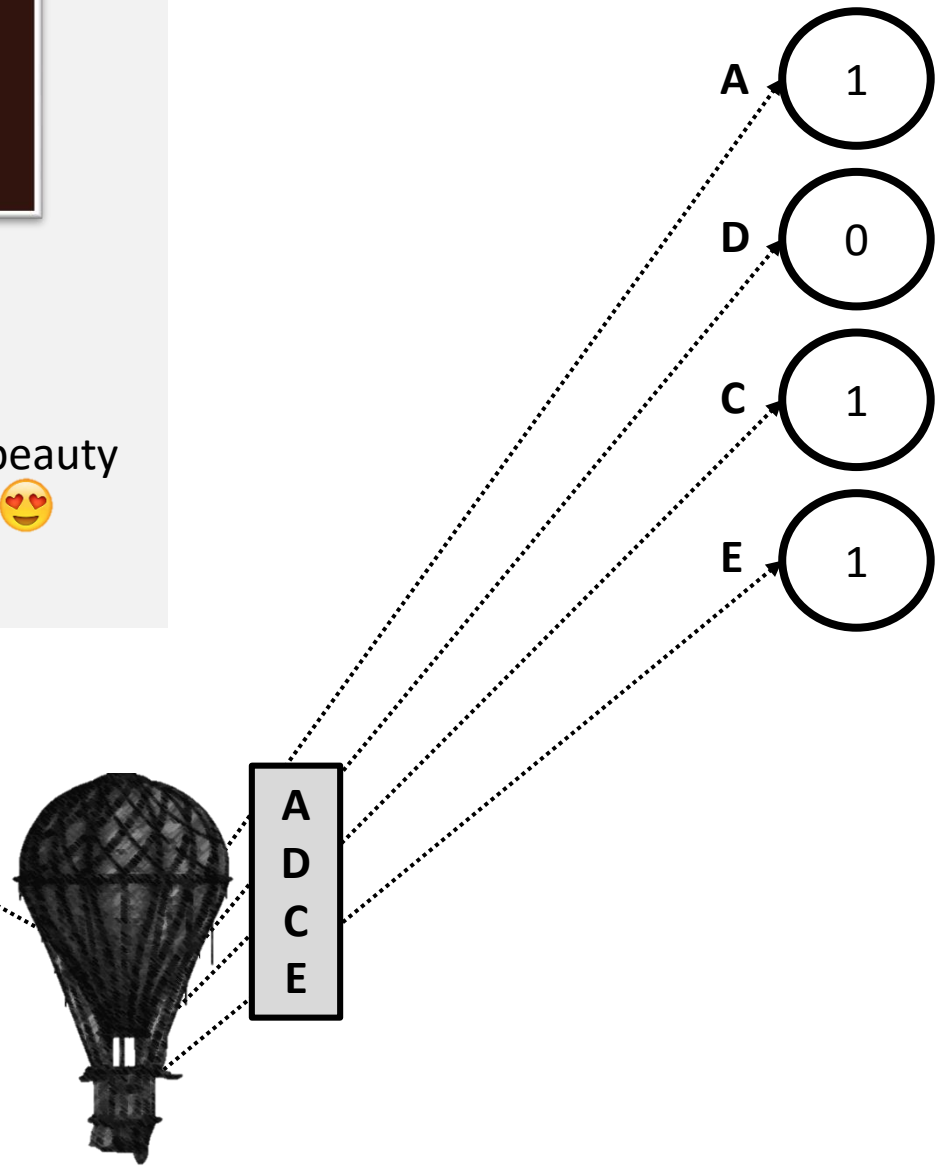
→Domains and resolvers represent key bits


Captain Nemo


A
1
C
1
D
0
B
E
1
Ephemeral key
storage

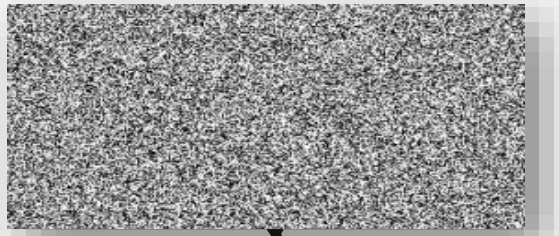

A
D
C
E


Captain Nemo
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm
Nautilus II – beauty isn't she? 😍😍

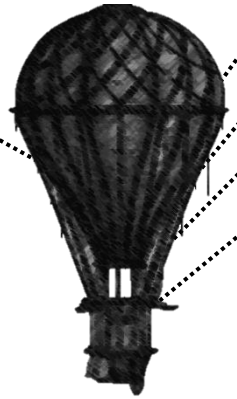

A
1
D
0
C
1
E
1
A
D
C
E

Captain Nemo

Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm



Nautilus II – beauty isn't she? 😍😍

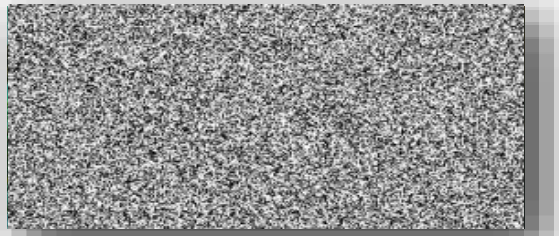


A D C E

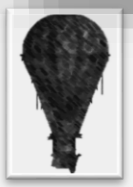
A 1
D 0
C 1
E 1

Captain Nemo

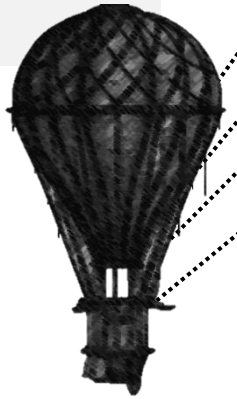
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm



Nautilus II – beauty isn't she? 😍😍

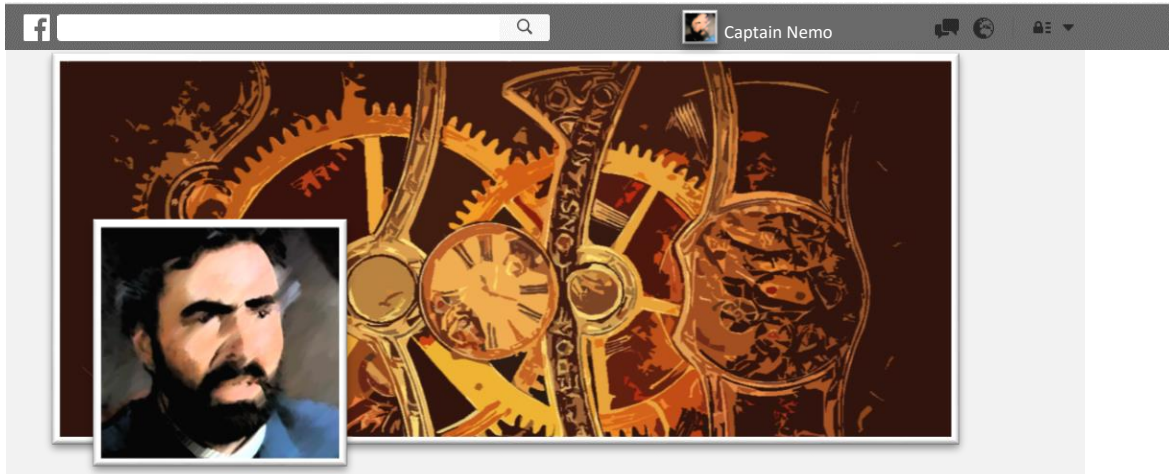


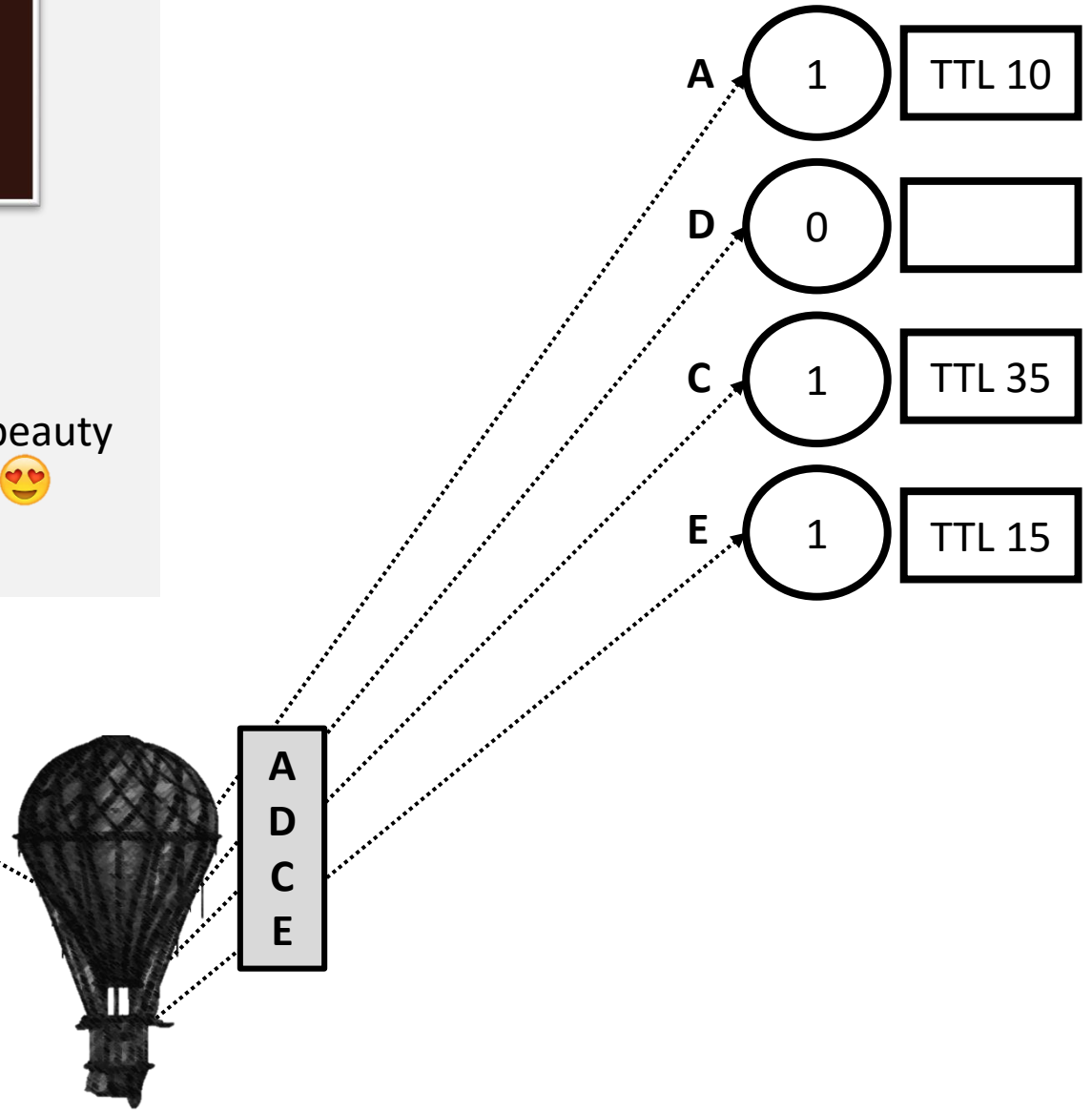
Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm

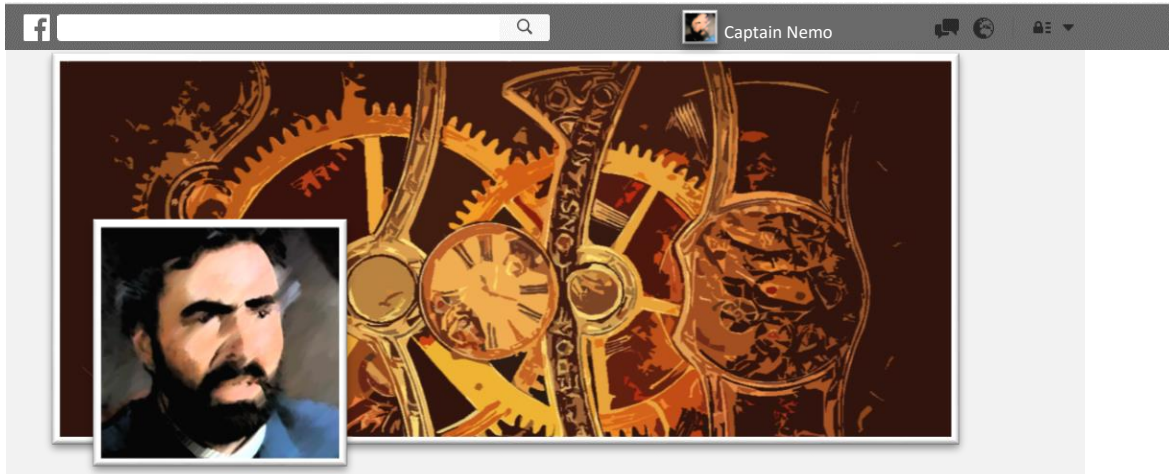


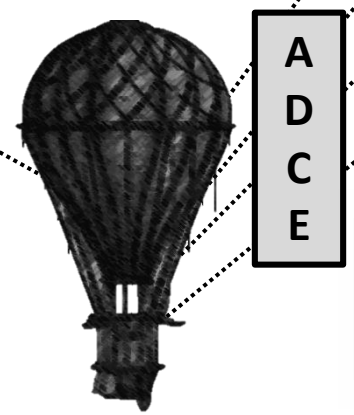
A D C E

A 1
D 0
C 1
E 1


Captain Nemo
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm
Nautilus II – beauty isn't she? 😍😍


A
1
TTL 10
D
0
C
1
TTL 35
E
1
TTL 15
A
D
C
E





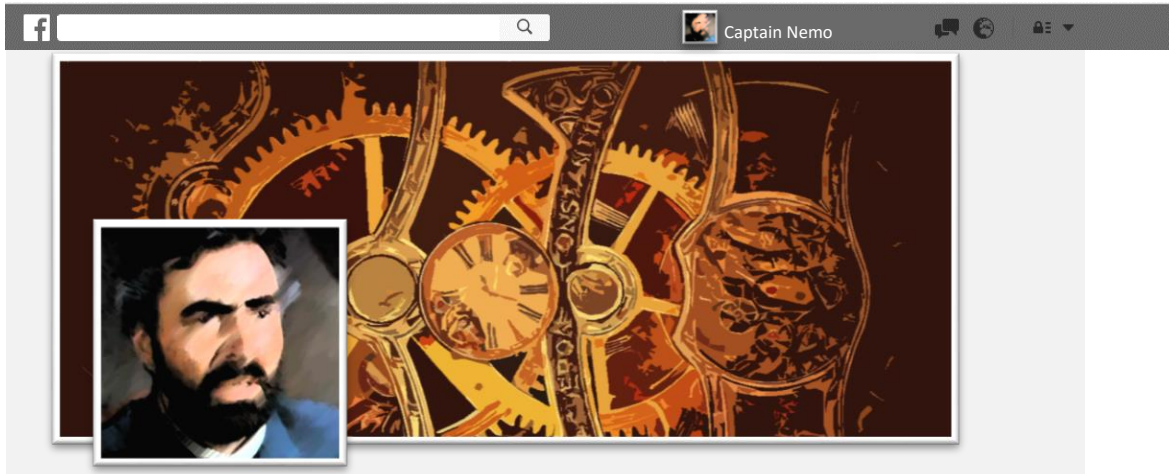
A D C E

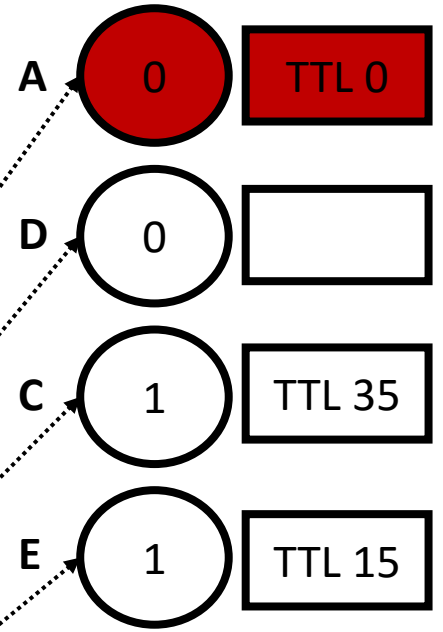
A 1 TTL 10

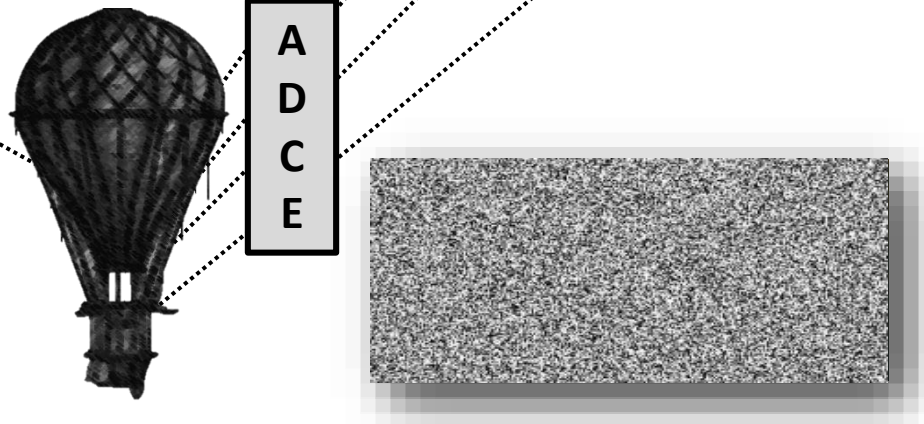
D 0

C 1 TTL 35

E 1 TTL 15

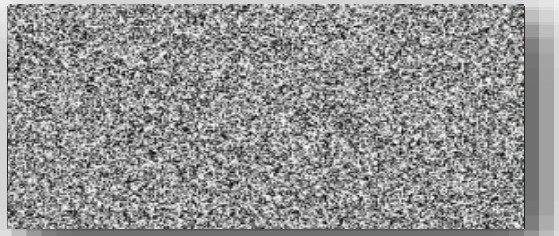

Captain Nemo
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm
Nautilus II – beauty isn't she? 😍😍


A
0
TTL 0
D
0
C
1
TTL 35
E
1
TTL 15

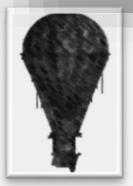

A
D
C
E

Captain Nemo

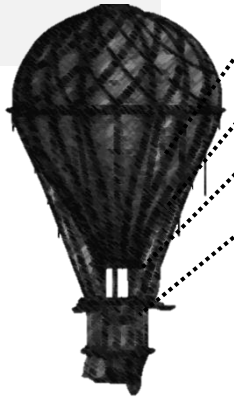
Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm



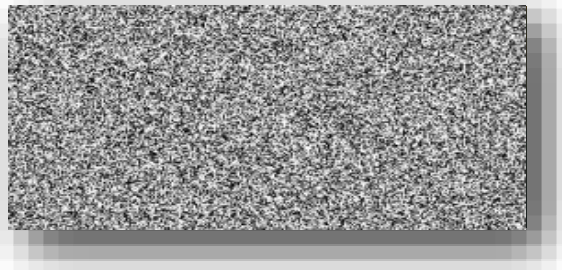
Nautilus II – beauty isn't she? 😍😍



Cyrrus Smith Your camera is not that good…
Like this . reply June 12th 3:37 pm



A D C E

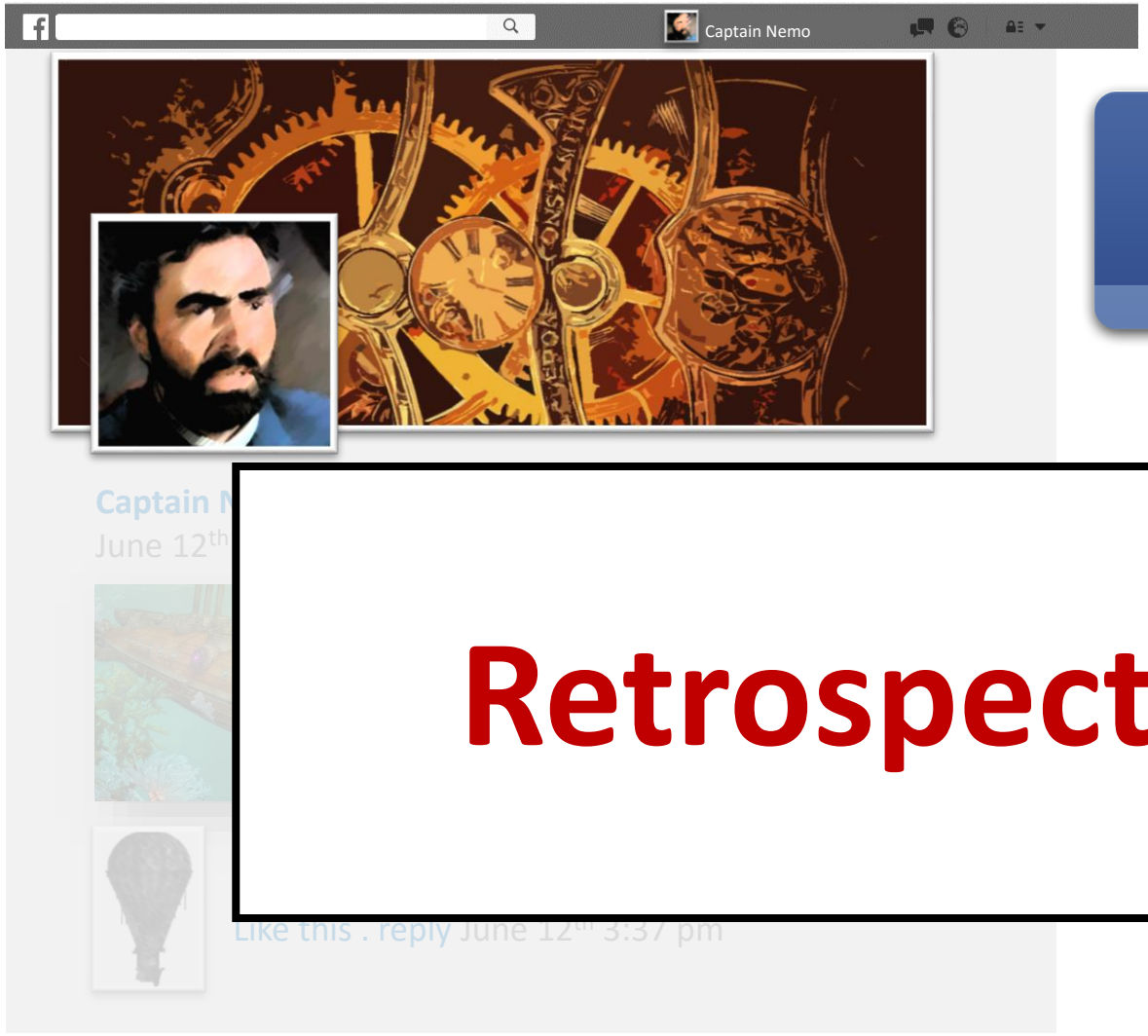


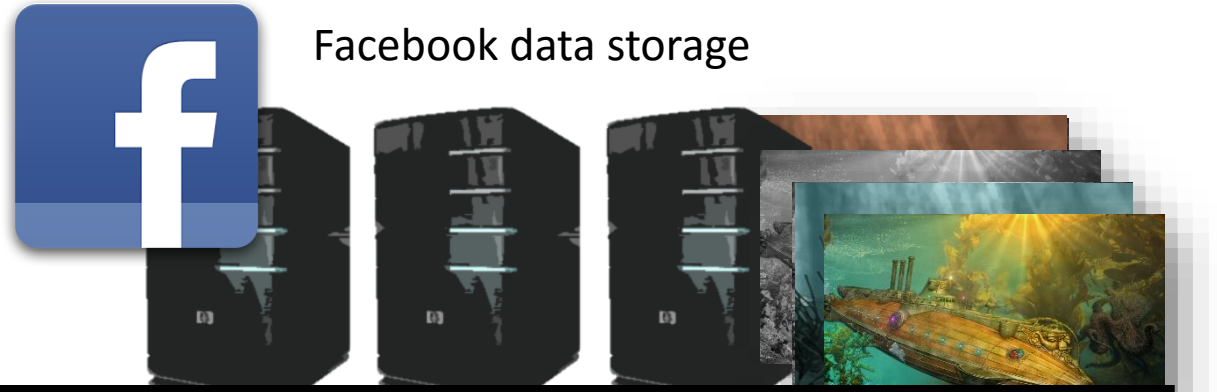
A 0 TTL 0

D 0

C 1 TTL 35

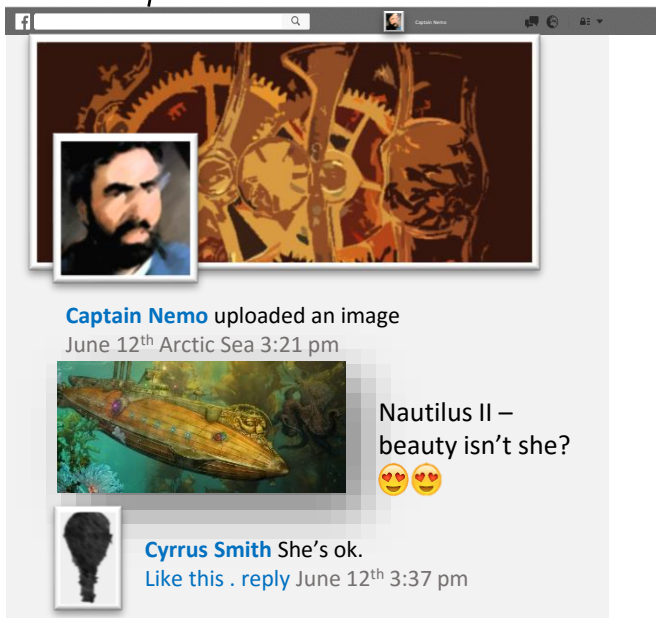
E 1 TTL 15





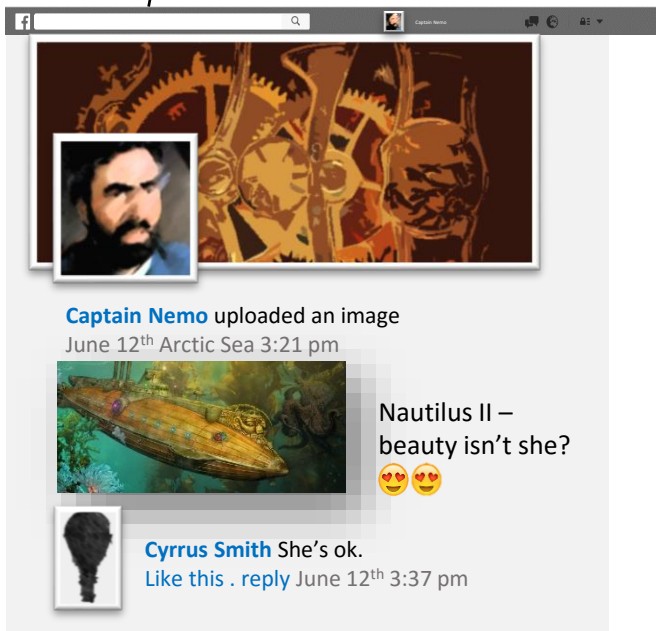
Retrospective adversary

Upload


Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm
Nautilus II – beauty isn't she?
😍😍
Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm

Upload

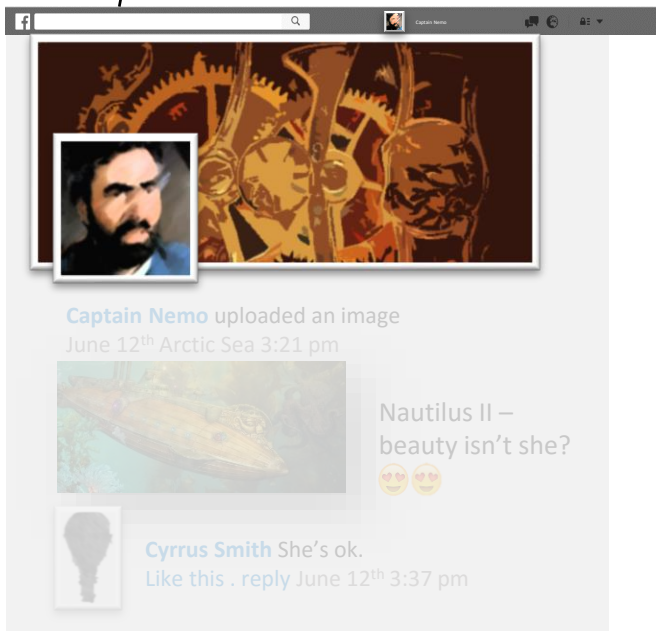
Revocation



Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm

Nautilus II –
beauty isn't she?
😍😍

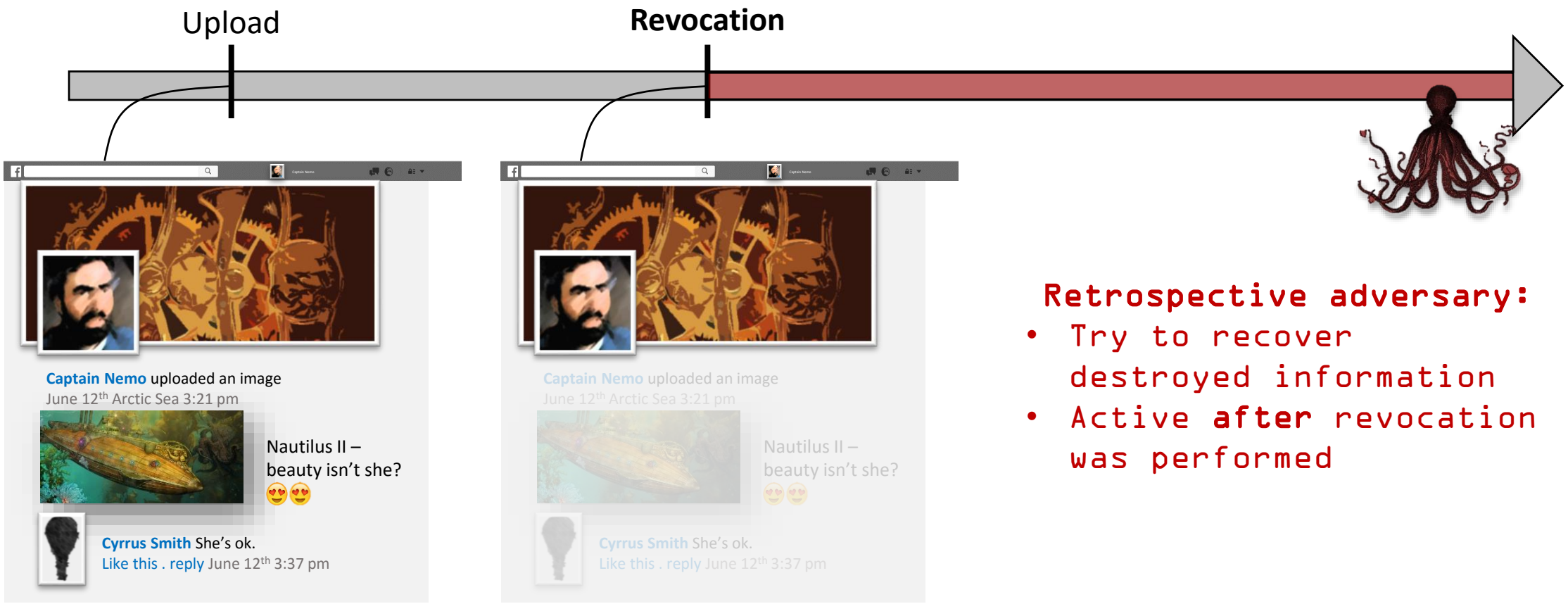
Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm



Captain Nemo uploaded an image
June 12th Arctic Sea 3:21 pm

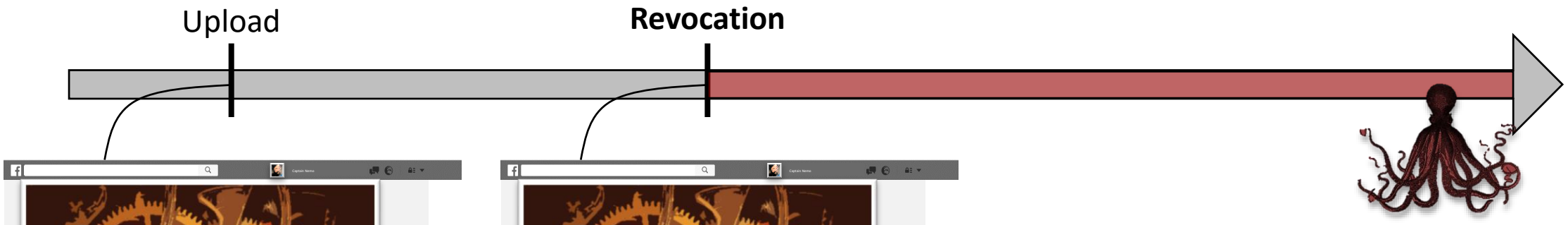
Nautilus II –
beauty isn't she?
😍😍

Cyrrus Smith She's ok.
Like this . reply June 12th 3:37 pm



Retrospective adversary:

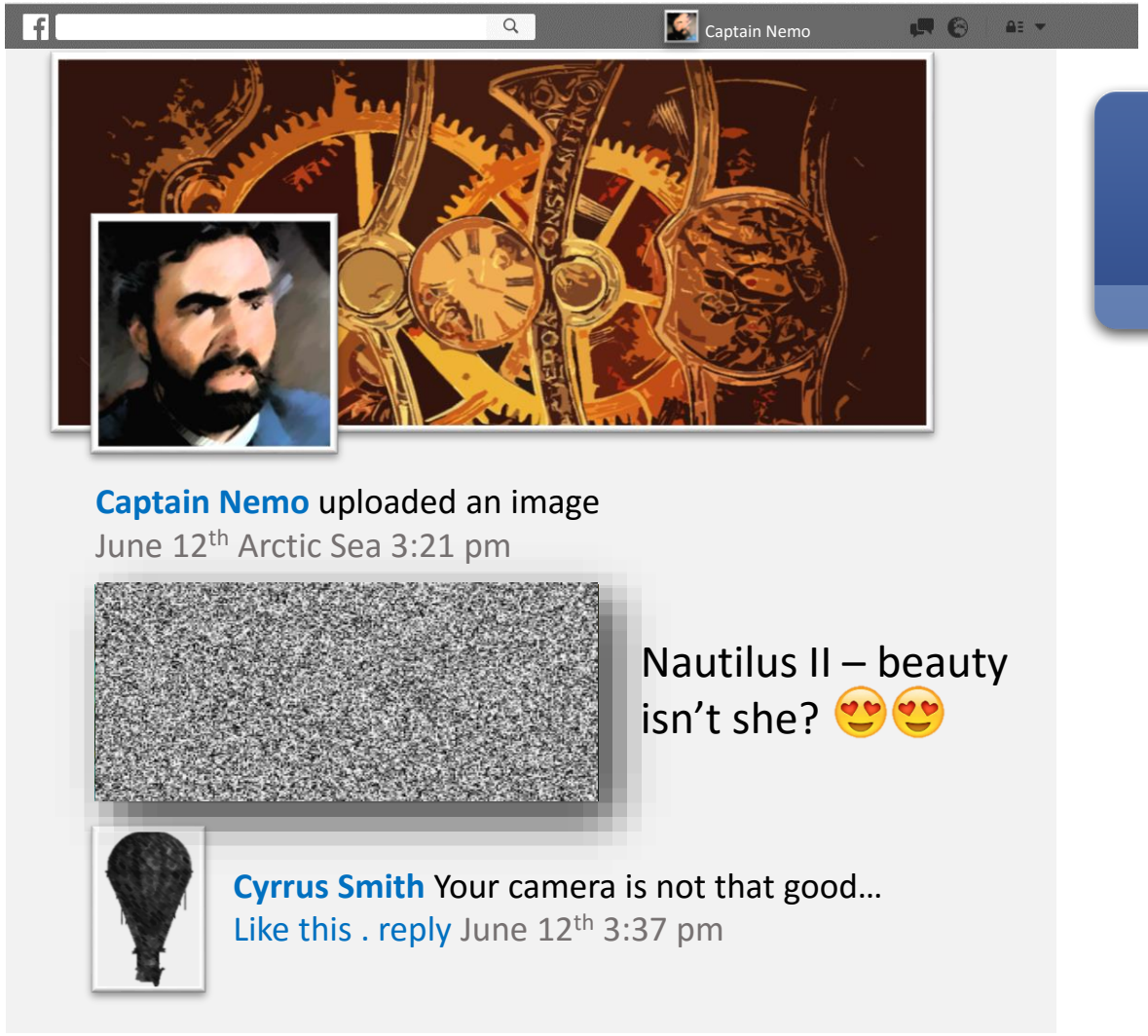
- Try to recover destroyed information
- Active **after** revocation was performed



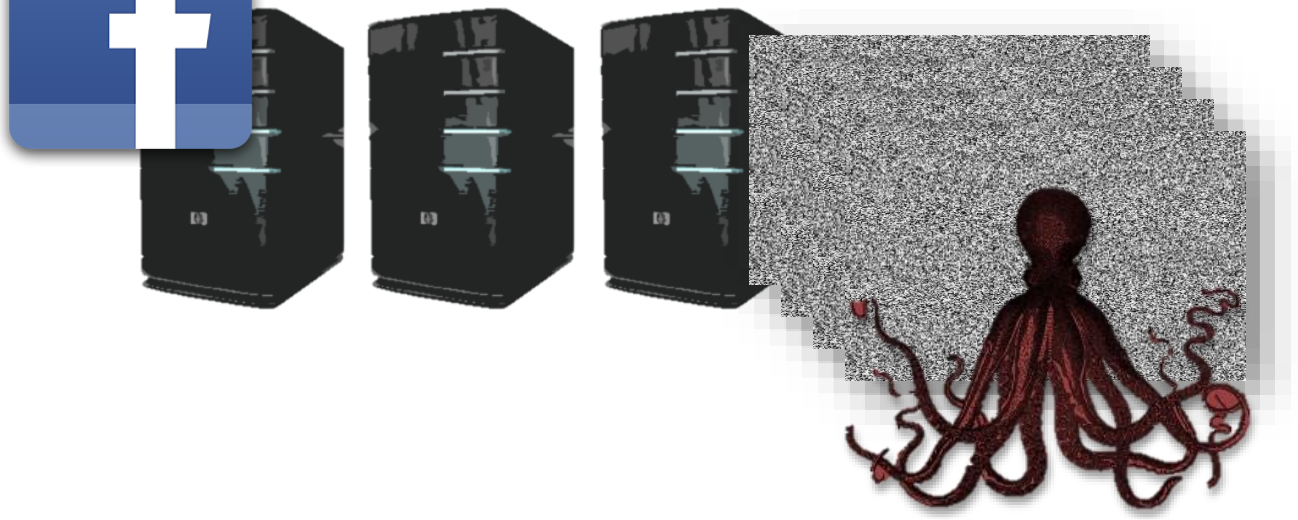
Retrospective adversary:

- Try to recover destroyed information
- Active **after** revocation was performed

Yes, images and keys can be copied at any time before. We cannot prevent this (yet).



Facebook data storage



Retrospective adversary
Attack after revocation

Neuralyzer

Flexible expiration times for the revocation of online data

Flexible Expiration Times

Problem:

Predefined and fixed lifetimes require assumptions on what will happen. **[EphPub'11], [Ephemerizer'05], [Vanish'09]**

Solution:

- **User behavior defines lifetime of key**
- Access behavior as revocation metric
- Requests refresh key lifetime
- Interest triggers revocation

Flexible Expiration Times

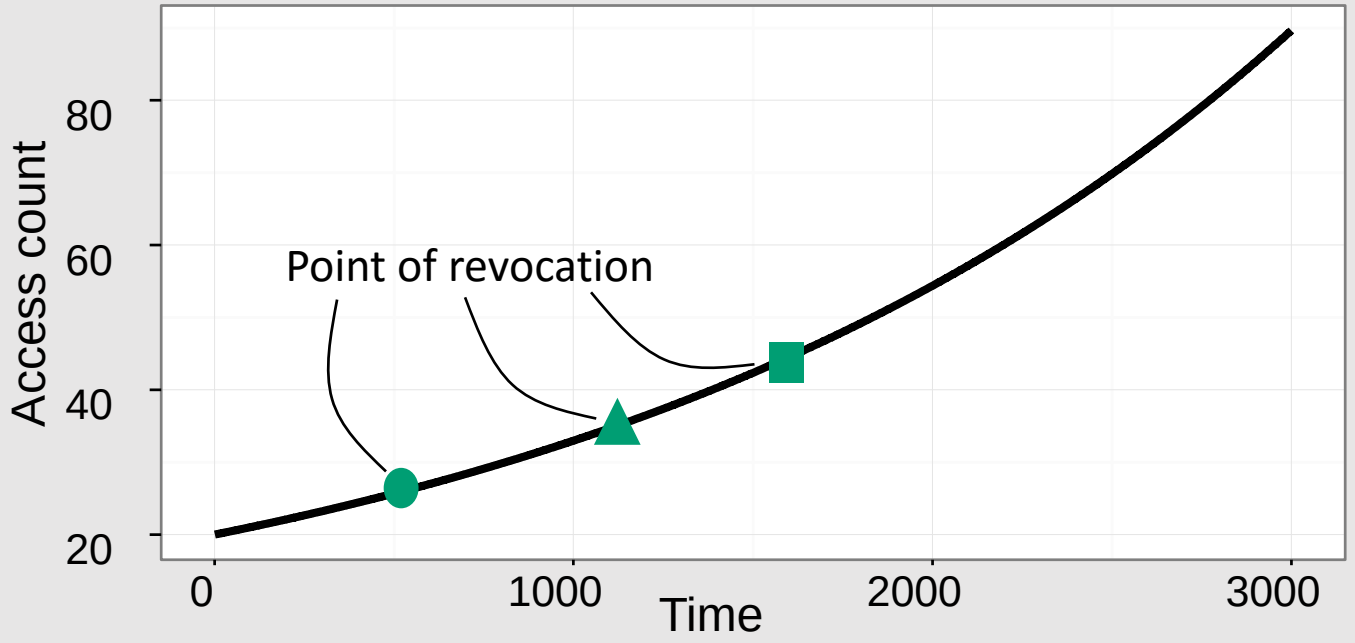
Problem:

Pr
ha

So

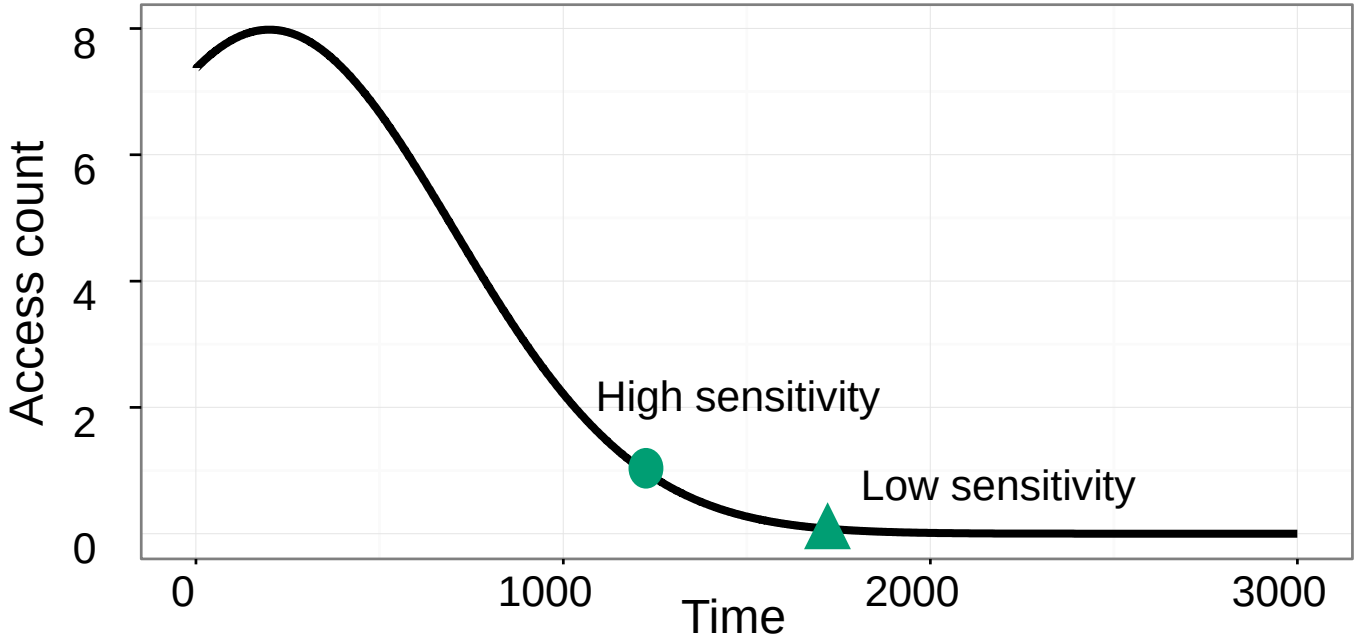
- **U**
- Access behavior as revocation metric
- Requests refresh key lifetime
- Interest triggers revocation

Example



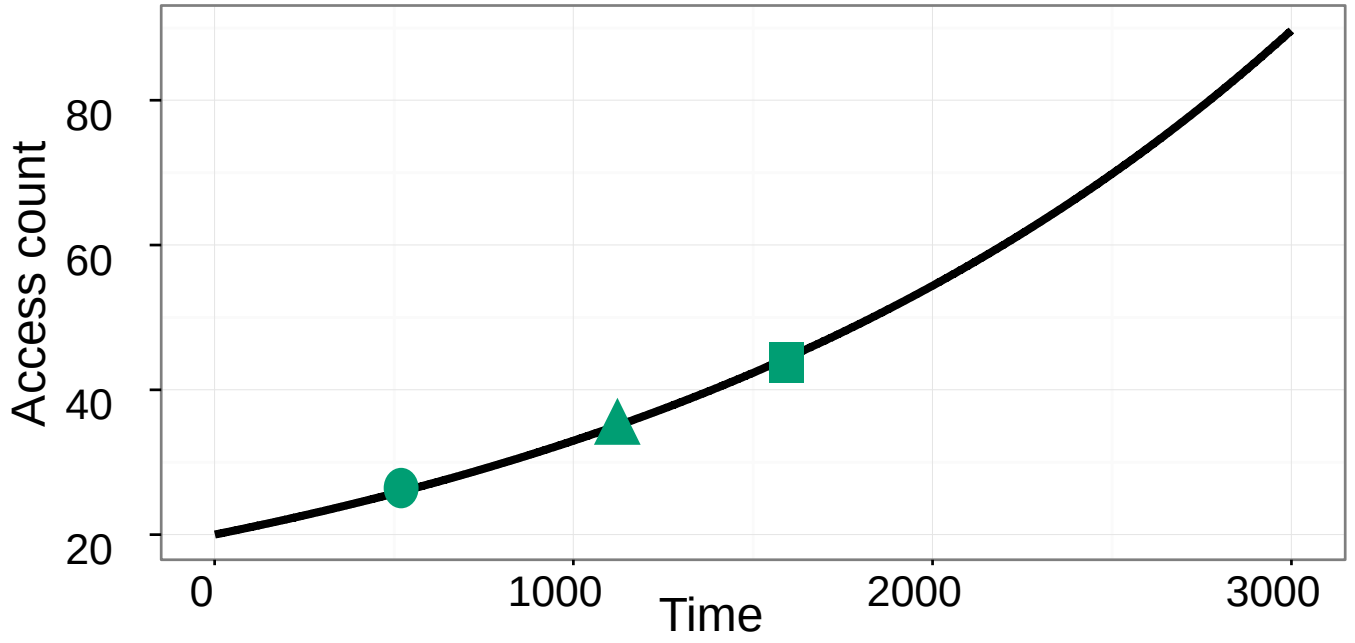
Excessive access

- Probabilistic revocation
- Destroy key with unexpected growth of interest



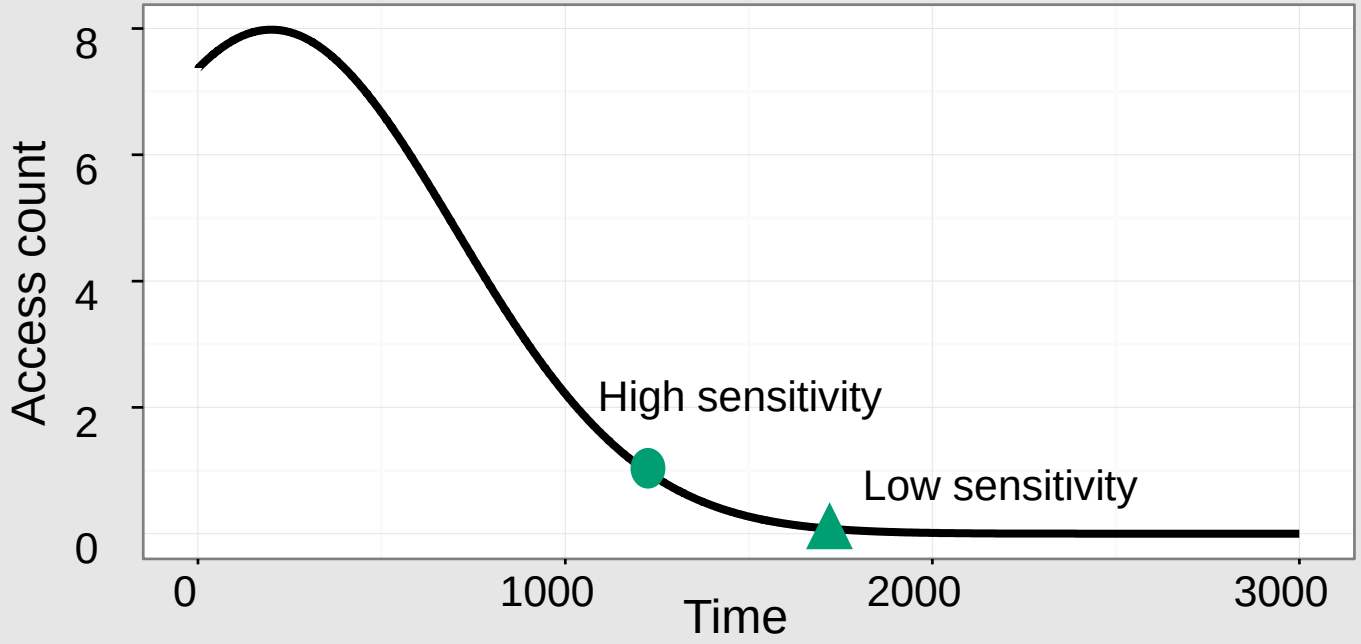
Drop of interest

- Revocation by insufficient number of refreshes
- Sensitivity given by error correction



Excessive access

- Probabilistic revocation
- Destroy key with unexpected growth of interest



Drop of interest

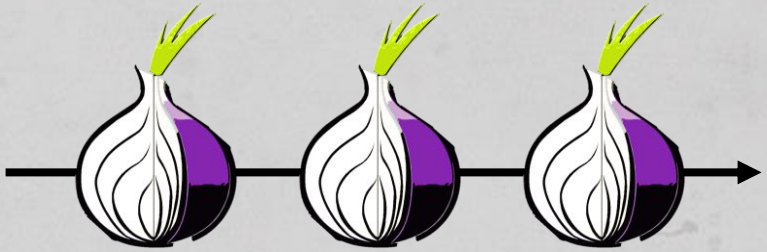
- Revocation by insufficient number of refreshes
- Sensitivity given by error correction

Conclusion

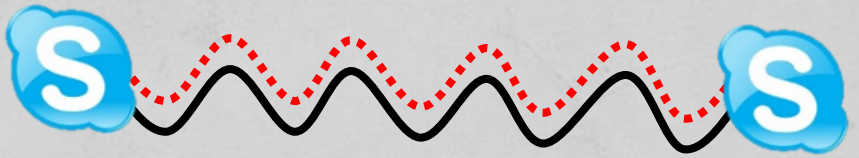
Challenges of privacy research

Challenges of privacy research

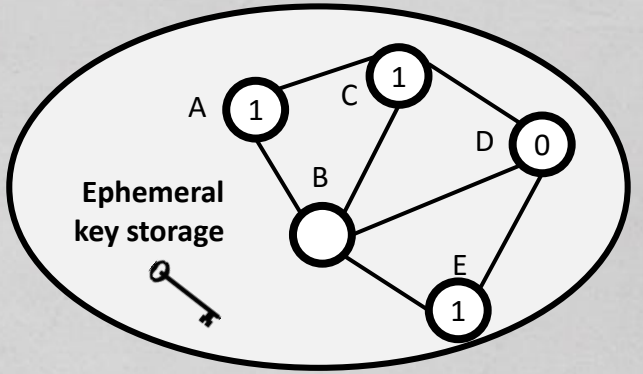
- **Anonymous communication**
  - De-anonymization attacks, e.g., on Tor
  - Blocking and censorship of services



- **Private communication**
  - Blacklisting and blocking of critical content
  - Circumvention by hidden communication, e.g., through Skype



- **Digital forgetting**
  - Example: Neuralyzer project
  - Encryption and revocation of shared key information
  - User-driven revocation heuristics




Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.
Gary Kovacs (Mozilla)

Privacy is not an option, and it shouldn't be the price we accept for just getting on the Internet.

Gary Kovacs (Mozilla)

Thank You! Questions?

[Neuralyzer]: Flexible Expiration Times for the Revocation of Online Data
Apostolis Zarras, Katharina Kohls, Markus Dürmuth, Christina Pöpper
CODASPY '16 ACM Conference on Data and Application Security and Privacy
(Outstanding Paper Award)

[SkypeLine]: Robust Hidden Data Transmission for VoIP
Katharina Kohls, Dorothea Kolossa, Thorsten Holz, Christina Pöpper
ASIACCS ‘16 ACM Symposium on Information, Computer and Communications Security

[Tor Mix or not Tor Mix]
Under Submission @ PETS

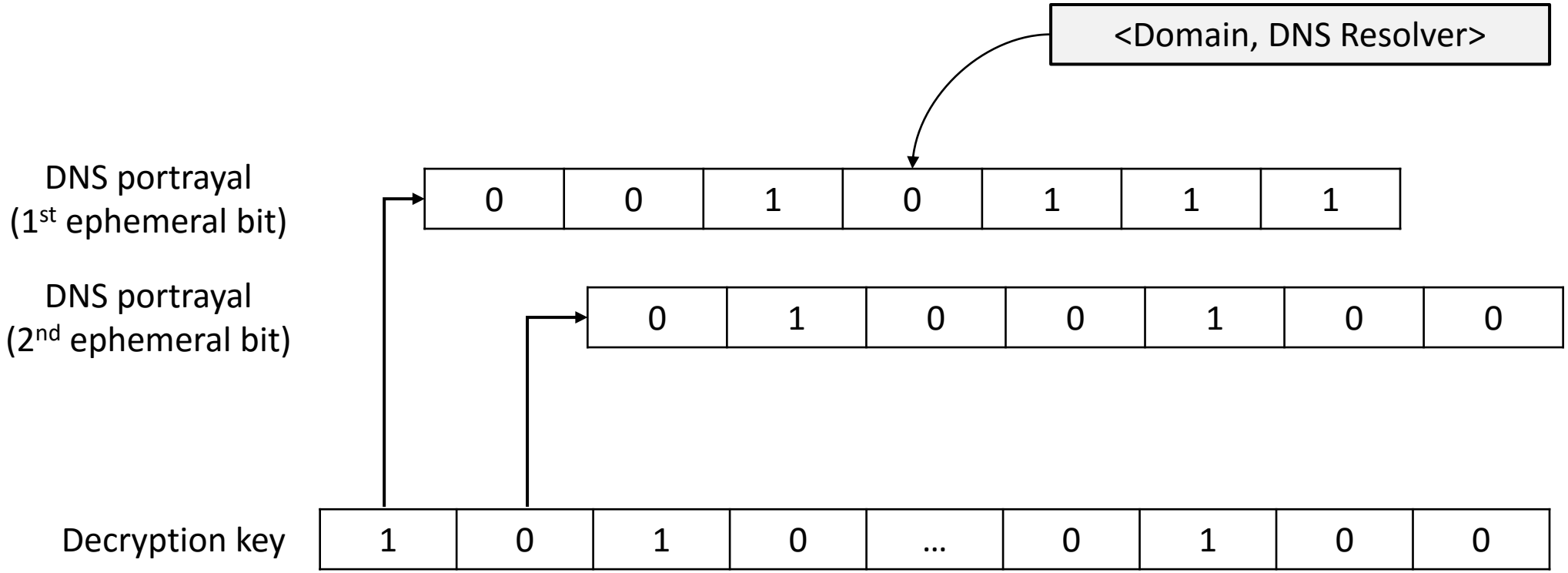
Image sources

1. http://www.fubiz.net/wp-content/uploads/2012/03/the-kraken-existence2.jpg
2. http://www.pxleyes.com/blog/wp-content/uploads/showcases/underwater-digital-paintings/14.jpg
3. http://www.desktopimages.org/pictures/2015/0727/1/kraken-pics-330784.jpg
4. http://img05.deviantart.net/fca3/i/2014/065/e/a/deep_sea_by_mannepanne-d6co7z6.jpg
5. http://geektyrant.com/news/the-wolverine-director-james-mangold-will-helm-captain-nemo-for-disney
6. http://www.disneysub.com/mr/nautilus02.jpg
7. https://encrypted-tbn1.gstatic.com/images?q=tbn:ANd9GcQvMq0mc9PdwJQBKiliKlxo8eYP9ry-mjABCcimpQ_Q2jThgAcK9A
8. https://www.nationstates.net/images/flags/uploads/captain_nemo_of_the_nautilus__65524.jpg
9. http://static1.squarespace.com/static/533b2afce4b058072a85a48e/t/533c8520e4b0a3ebd0e32e0c/1468329676015/?format=1500w
10. http://sf.co.ua/14/03/wallpaper-982053.jpg
11. https://s-media-cache-ak0.pinimg.com/564x/0a/05/72/0a05723576898ff0d3df7cf0b674afa2.jpg
12. https://s-media-cache-ak0.pinimg.com/236x/c8/c3/3f/c8c33f07dccdb34bdd78547ae2826eef.jpg
13. https://cnet1.cbsistatic.com/hub/i/r/2014/03/19/31f386cc-b0b5-11e3-a24e-d4ae52e62bcc/thumbnail/670x503/4caca097625818d24a13dbe9ea4a04f0/Skype-logo.png
14. http://thatstheish.com/wp-content/uploads/2015/05/tor-logo1.jpg
15. http://4.bp.blogspot.com/-EI_hjM7E_0Y/U7GExGRzIPI/AAAAAAAAAgs/2LSzIWg-qQQ/s1600/tentacles_render3.jpg
16. http://eskipaper.com/images/octopus-tentacles-1.jpg
17. https://pixabay.com/static/uploads/photo/2015/05/17/10/51/facebook-770688_960_720.png
18. http://static.independent.co.uk/s3fs-public/thumbnails/image/2015/02/05/10/Heart-eyes-emoji.png

Appendix

Room for all the equations!

DNS portrayal



`recover` and `refresh`

Key recovery

- Recover key bit from portrayal
- Empirical threshold $\mathbf{x}$ for decision

$$\textbf{recover}\begin{cases}\sum_{n=0}^{N-1} c_{i,n} \geq x : 1\\ \sum_{n=0}^{N-1} c_{i,n} < x : 0\end{cases}$$

Key refreshing

- Check remaining TTLs of cached entries
- Cache 0-bits in portrayal

$$\textbf{refresh}\begin{cases}\left(median\left(ttl_{i,n}\right) < t_1\right)\vee\\ \quad\left(\exists n: ttl_{i,n} < t_2\right) : 1\\ \left(median\left(ttl_{i,n}\right) \geq t_1\right)\wedge\\ \quad\left(\exists n: ttl_{i,n} \geq t_2\right) : 0\end{cases}$$