Nordic Light on the Darknet: Forensic Investigations on the Tor Network

Stockholm University

Department of Computer and Systems Sciences

Stockholm University

Jesper Bergman (jesperbe@dsv.su.se)

Leeuvarden, November, 2017

S L I D E S

Twitter: #stenden

Who am I?

- Jesper Bergman (jesperbe@dsv.su.se) `https://www.linkedin.com/in/jesper-bergman-52249378/`
- Website and slides: `https://people.dsv.su.se/~jesperbe/pdtor/jesper2.pdf`
- 2017-: PhD Student (in Digital Forensics) at Stockholm University
- 2014-2017: Teaching and Research Assistant at Stockholm University
- MSc Degree in Computer and Systems Sciences (main track: Security and Forensics)

Why am I here?

PhD Student in a research project:

- PDTOR - Police Detectives on the Tor Network[1]
- NL, NO, UK, SE - The Swedes do the digital forensics part

[1] https://www.nordforsk.org/en/programmes-and-projects/projects/police-detectives-on-the-tor-network-a-study-on-tensions-betwee

Presentation Objectives and Outline

- Informal - "popular 'science'" kind of presentation
- Shed light on Scandinavian (criminal) darknet investigations
- Identify and address problems/challenges
- Propose solutions and fend off challenges
- Teach and spread awareness

So what about the title ”Nordic Light”?

Fig. 1 - Auraborealis over Stockholm (Photo: Johan Person)

So what is acutally the Darknet?

So what is actually the Darknet?

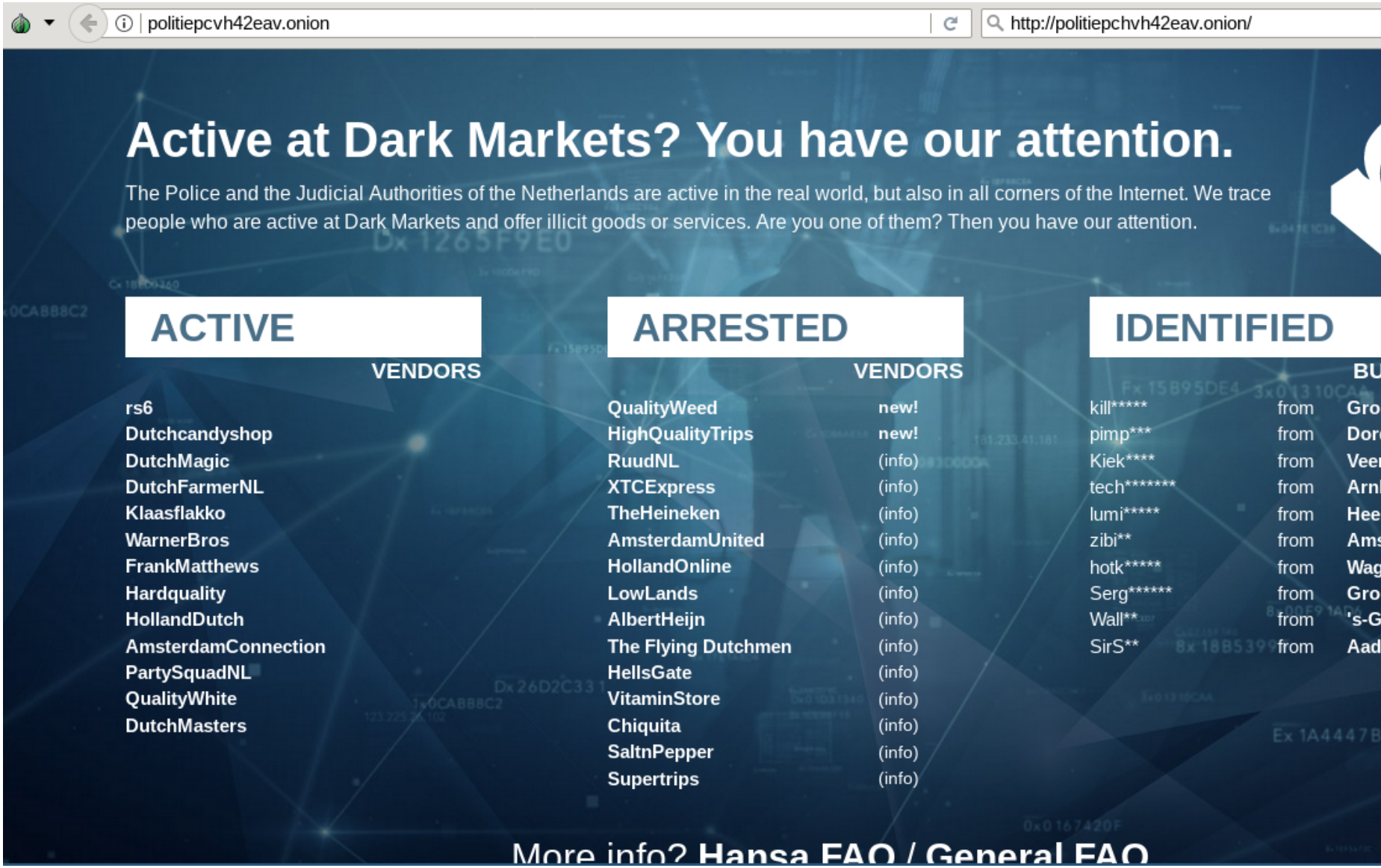
So what is the Darknet?

- Commonly: A censorship-free anonymity network that is not accessible using your regular web browser

Examples:

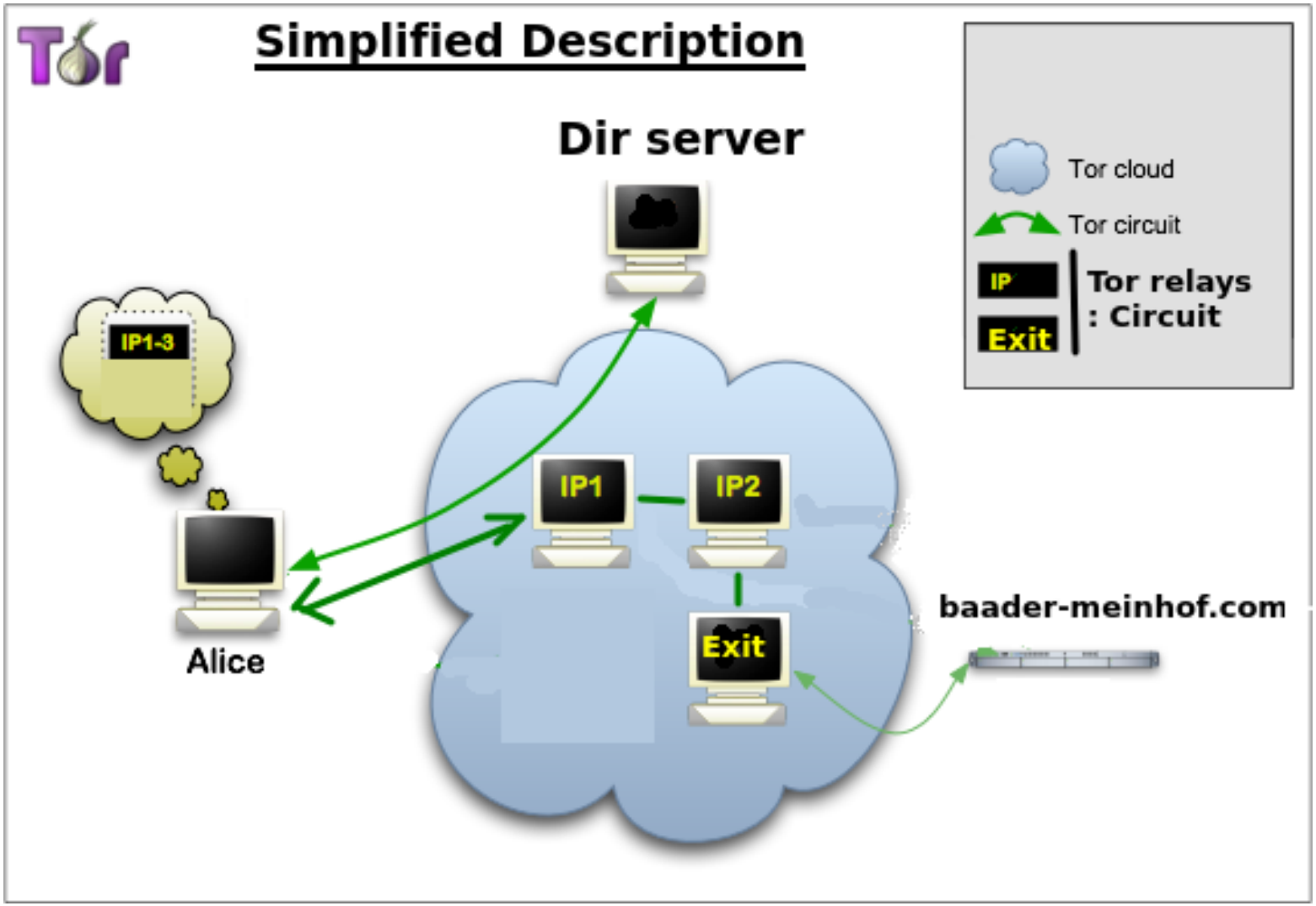
- King James Bible in North Korean: `http://sonofgod5u4eafyv.onion/`
- Facebook: `http://facebookcorewwwi.onion`
- Dutch Police: `http://politiepcvh42eav.onion`
- Dark Markets: drugs/weapons/child abuse material/counterfeit whatever

So what is the Darknet? cont'd



So what is the Darknet? cont'd

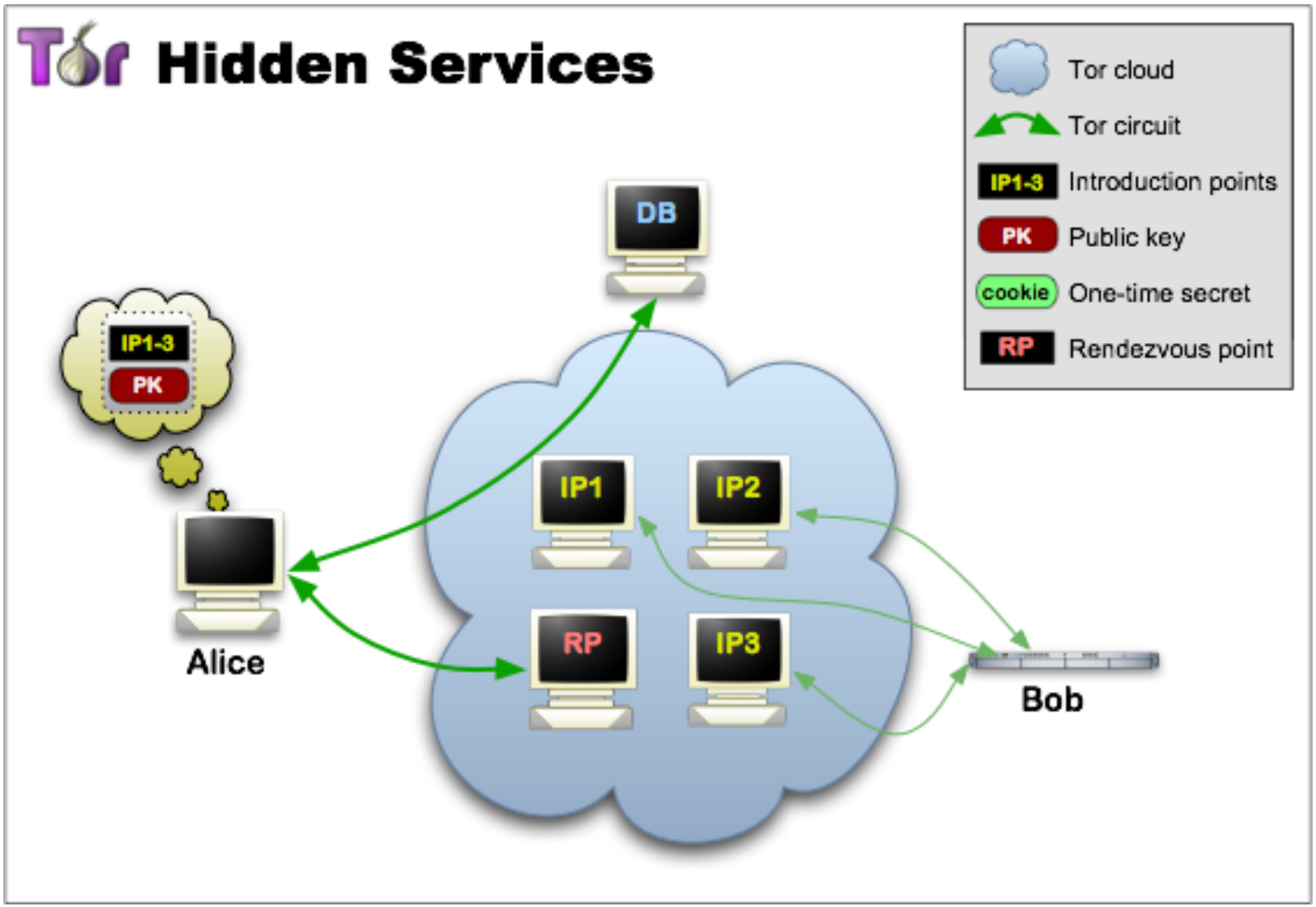
Firstly: What is the Tor network?



So what is the Darknet? cont'd

Secondly: What is the Darknet?

- Hidden Services - Only accessible from the Tor network (e.g. Tor browser)



When Anyone can host Anything Anonymously

https://www.deepdotweb.com/2017/11/18/netherlands-police-bust-darknet-trafficking-group/

So what about the "Nordic Light" mentioned?

- Interviewing Swedish police officers and investigators
- Analysing court documents and forensic reports

Nordic Light over the Darknet

Notable cases:

- 2015-2016: Biggest darknet dealers convicted and 3000 possibly Swedish buyers identified in an international cooperation[2]
- 2016: Big case, big darknet dealer sentenced to six years in prison[3]

[2] `https://polisen.se/Arkiv/Nyhetsarkiv/Gemensam/Tusentals-kopare-av-droger-pa-natet-identifierade/`

[3] The Court of Appeal for Western Sweden in Gothenburg, verdict ID: B3847-16

Case Study - The 42 year old

- 42 year old man from western Sweden
- Caught by Swedish Customs
- 2014-2016: Selling on Agora, Nucleus, Evolution and more

Case Study - The 42 year old cont'd

Preparat	Antal för-säljningar	Summa (tabletter)	USD	SEK
Ksalol/Xanor Alprazolam 1 mg	257	7 540	14160,08	119 440,27
Bensedin, diazepam 10 mg	235	12 075	16228,65	136 888,66
Iktorivil Roche2 Klonazepam 2 mg	181	6 330	8472,37	71 464,44
"Snabba" kapslar	61	550	3171,17	26 748,82
Tesla Orange 200-250 mg	28	465	6077,58	51 264,39
Green WhatsApp 180 mg	1	10	71,37	602,01
Zolpidem 10 mg	2	100	166,90	1 407,80
100 Ksalol 200 st Ikto spec Boo	1	300	354,65	2 991,47
SUMMA		**27 370**	**48 702,77**	**41 0807,86**

Fig. 2 - Table of illicit goods sold by the 35 year old on Nucleaus dark market during 2015

Case Study - The 42 year old cont'd

What about his operational security (op-sec)?

- Dark markets available (only) on the Tor network
- Encryption techniques (GPG)
- @countermail.com/hushmail.com address
- Bitcoin for anonymous payments
- iPhone 5

Case Study - The 42 year old cont'd

What about his operational security (op-sec)?

- Unencrypted Samsung Galaxy S6 (pictures, email conversations etc.)
- Unencrypted external hard drive (screenshots, documents, pictures etc.)
- Unencrypted passwords stored on unencrypted Windows computer
- @gmail.com address

Case Study - The 42 year old cont'd

Humorous points:

- Alias: "erkran" - "Er Kran" - You Supplier (Swedish slang)
- gafpvd@gmail.com - (Previously used abbreviation for "Do Anything For Money")

Case Study - The 42 year old cont'd

GAFP-01

GAFP-02

GAFP-03

GAFP-04

Challenges of Darknet Forensic Investigations

- Encryption
- High level of anonymity in darknets
- Limited traces of Tor activity in computers and smartphones
- Limited knowledge and competence among investigators and examiners

Summary of the Nordic-Euorpean Light over the Darknet

- Collaboration: police, customs, tax agencies, post offices etc.
- Targeted monitoring of dark markets
- Digital forensic methods for these cases
- Sharing of knowledge
- Educate the police officers, investigators, prosecutors, lawyers, soliciters etc.

Dankjewel.

jesperbe@dsv.su.se

Twitter:@jesperatsu