IN5290 Ethical Hacking

Lecture 1: Introduction to Ethical Hacking, Information Gathering

Universitetet i Oslo

Laszlo Erdödi

Lecture Overview

- What is ethical hacking?
- Steps of penetration testing
- Information gathering techniques

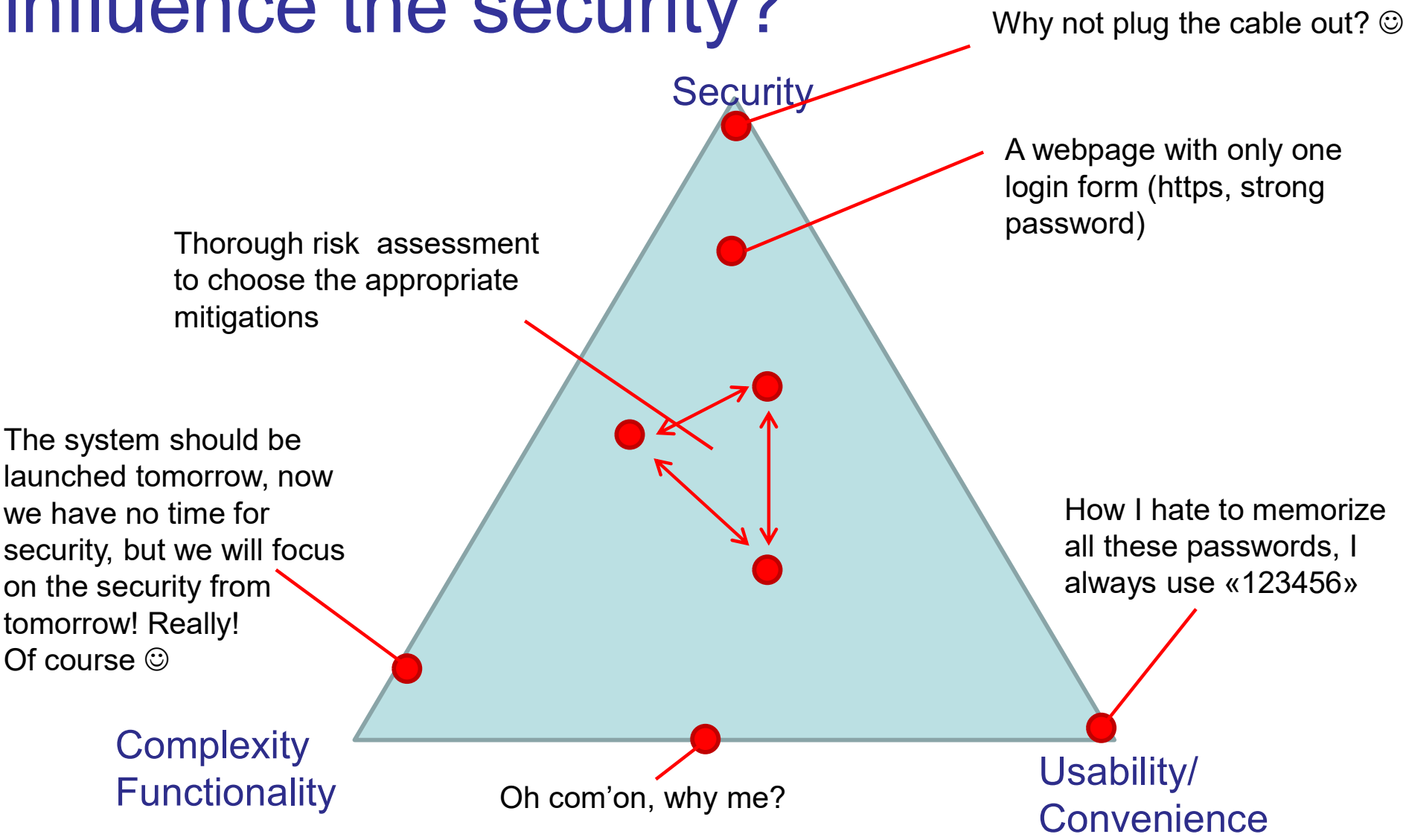
Why ethical hacking is necessary at all?

- Computer systems have several security problems

What is the reason for having so many security issues?

- Lack of money
- Lack of time
- Lack of expertise
- Negligence
- Convenience
- Old systems
- Too complex systems
- 3rd party components
- And many others…

How does the usability and functionality influence the security?



Why ethical hacking is necessary at all?

- Checking the system from the attacker's perspective can reveal serious security deficiencies
- The «attacker» thinks like a real hacker (but not totally)
  - Do we use the same methodology as the real hackers?
  - Do we have the same goals?
  - Do we have to hide ourselves when ethically hacking?
  - What makes hacking ethical?
  - What is allowed and what is not?
- The system security cannot be guaranteed without deep and regular penetration testing
  - Can it be guaranteed with penetration testing? Unfortunately not always perfectly, the keyword is the appropriate mitigation

The motivation behind hacking – Why?

To understand the real hackers, first we have to understand the motivations:

- What a cool thing to be a hacker
- Because I can
- Money
- Revenge
- Annoyance
- Protesting against something
- Organized and well-paid professional groups (mafia and state sponsored groups)

The goal of hacking

- Break the information security triple (confidentiality, integrity, availability)
  - Steal confidential information
  - Modify data
  - Make services unavailable (Denial Of Service)

- To promote security? YES!

Type of hackers

- Black hat hackers: Hacking with malicious intent
- White hat hackers: Perform penetration testing to promote the security
- Script kiddies: amateurs (Usually young kids) using publicly available software tools to attack
- Protest hackers (Protest against something e.g. anonymous)
- Grey hat hackers: Usually white hat, but can be black hat
- Red hat hackers: Stopping black hat hackers by attacking them
- Blue hat hackers: Hacking in order to take revenge
- Green hat hackers: Beginners to hacking

Be ethical and legal, it's never worth doing anything against the law!!!

Hacker who helped end global cyberattack arrested in US

British researcher arrested for allegedly creating and distributing malware designed to collect bank-account passwords.

4 Aug 2017

Two Hackers Arrested for Hijacking Over 700,000 Online Accounts

By Catalin Cimpanu June 27, 2018 09:40 AM 0

Leader of Hacking Group Who Stole $1 Billion From Banks Arrested In Spain

March 26, 2018 Wang Wei

Skoleelev varslet om datahull i Bergen

Det var en elev ved en barneskole i Bergen som oppdaget sikkerhetshullet som gjorde at informasjon om tusenvis av elever og lærere kunne ha blitt spredt.

Av NTB
Oppdatert 17. august 2018

Differences between ethical and non-ethical hacking

- Task: Find the admin password of «*NonExistingBank*»
- How do I start? Which one of these will be used by the black hat and the white hat hackers?
  - Try with the websites, maybe there's a server side scripting flow?
  - Try to apply for an account to have access to password protected sites?
  - Try with low level exploitation against the server?
  - Try to access the DMZ through a less controlled service?
  - Try to sneak inside the building to have access to the internal network?
  - Try social engineering emails against the employees?
  - Try to make friendship with the system admin?

Differences between ethical and non-ethical hacking

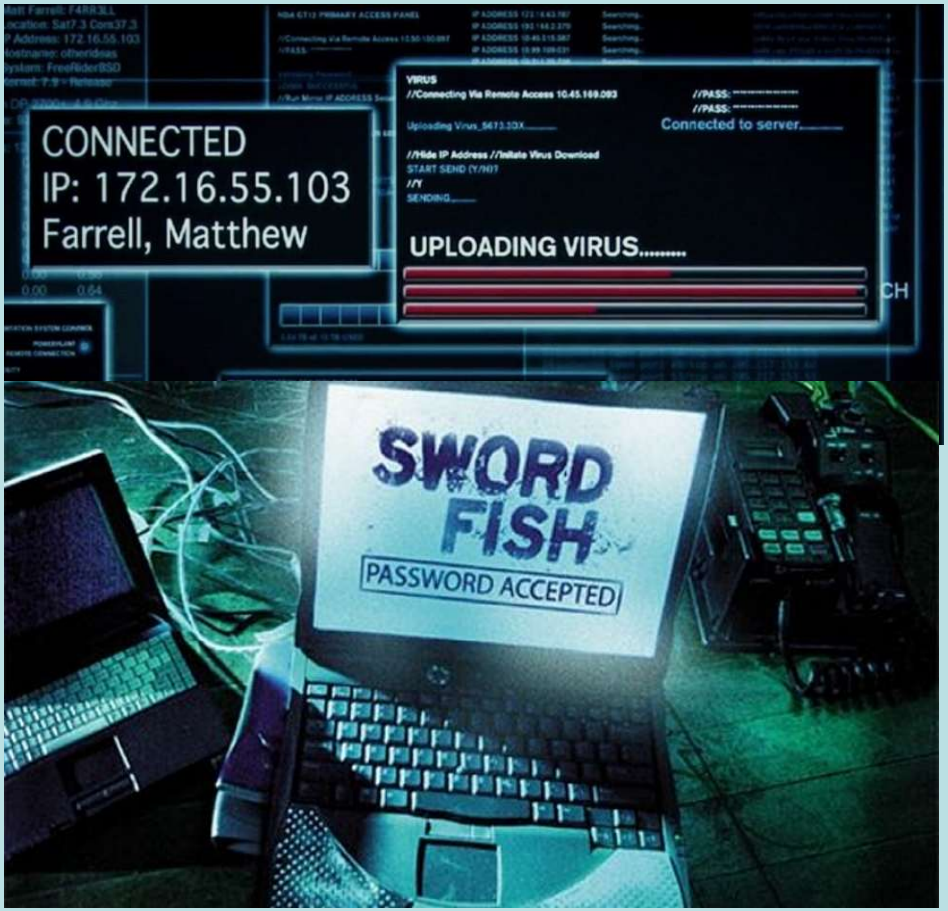
- Legal (contract)
- Promote the security by showing the vulnerabilities
- Find all vulnerabilities
- Without causing harm
- Document all activities
- Final presentation and report

- Illegal
- Steal information, modify data, make service unavailable for own purpose
- Find the easiest way to reach the goal (weakest link)
- Do not care if the system destroys the system (but not too early)
- Without documentation
- Without report, delete all clues

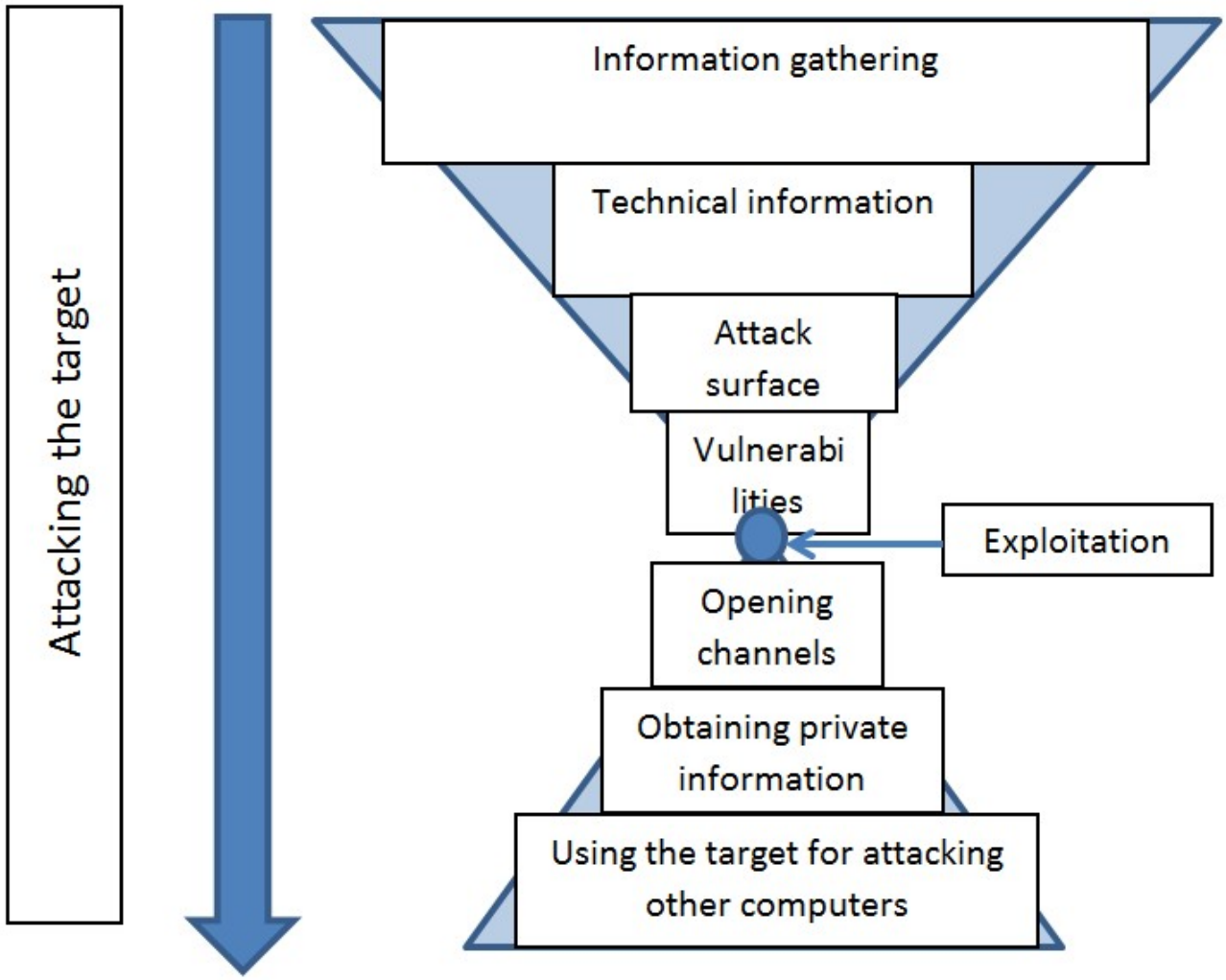
Main steps of hacking

- Information gathering
- Identifying the target domain
- Finding vulnerabilities
- Exploiting the vulnerabilities
- Lateral movements
- Carry out the goal

Spectacular, but not real! ☺



Steps of an attack with available info as the hacking process proceeds



Detailed steps of hacking

1. General information gathering: collecting all available information from the target and systemize the information
2. Technical information gathering: collecting network and system specific information like target ip ranges
3. Identifying available hosts in the target network (which computer can be attacked)
4. Identifying available services in the target network (which service can be attacked)
5. Manual mapping of the services (to check how it looks like, the impressions, system reactions, mitigations, etc.)

Detailed steps of hacking

6. Automatic vulnerability scanning (intelligent tools with huge vulnerability database)
7. Manual verification of the findings (to check if the previous findings are real – true positive)
8. Exploitation
9. Lateral movements (to move through the network)
10. Ensure access until the end of the project
11. Collect info – achieve primary and secondary goals
12. Remove clues
13. Reporting and presentation
14. Removing the attacking files!!! (tools, data, script created temporarily during the pentest)

Type of ethical hacking projects

From the attacker's location point of view:

- External penetration testing
- Web hacking
- Internal penetration testing
- Wireless penetration testing
- Social Engineering

From the attacker's access (right) point of view:

- Black box testing
- Grey box testing
- White box testing

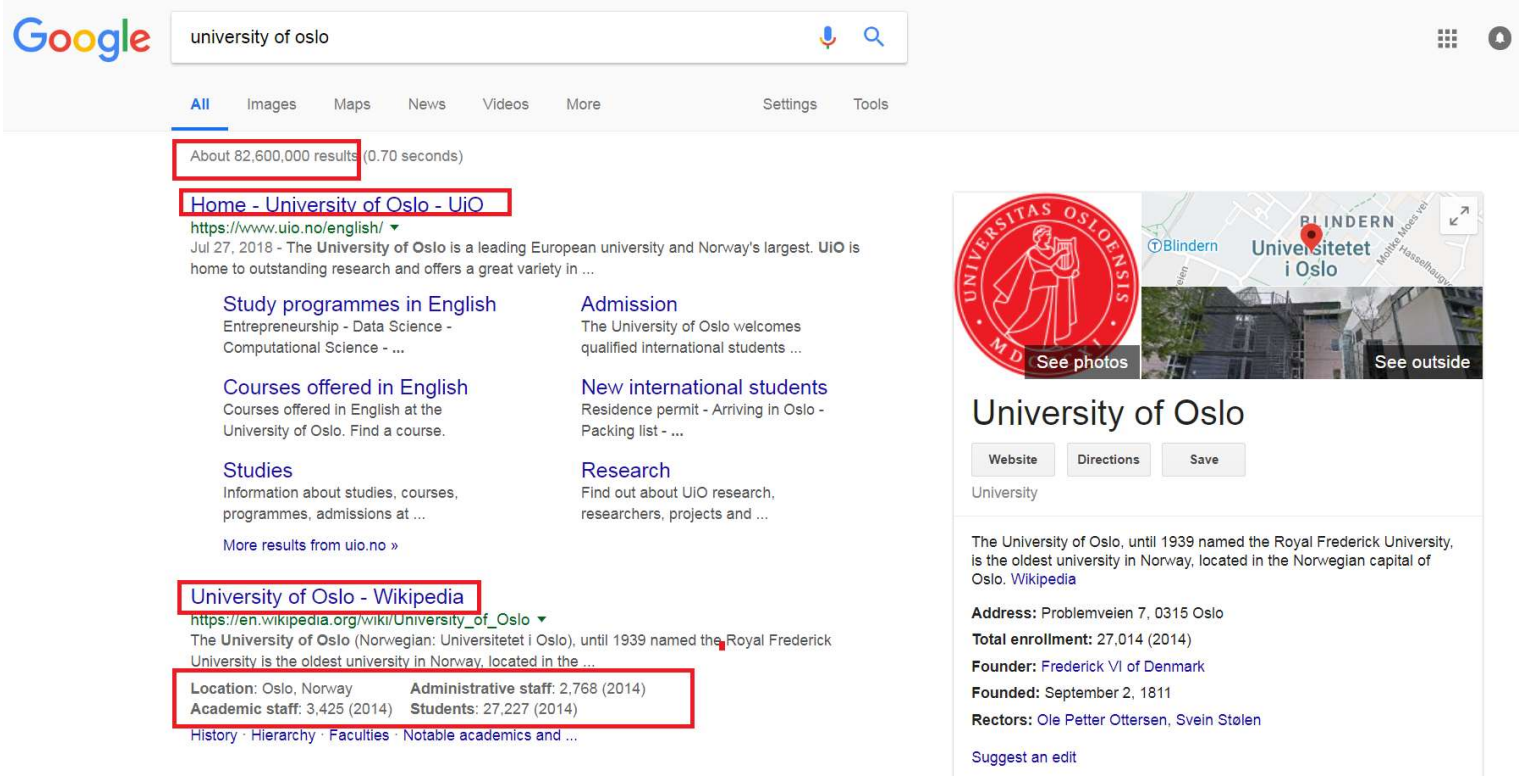
General information gathering

- Usually the first step of every attack
- Before getting contact with the target we need to prepare for the attack
- General information gathering covers all the efforts that is done for collecting all the information from the target
- The collected information should be analyzed as well in order to filter the important information
- Sometimes it is not obvious which information will be useful later, all information should be systemized
- The result of the information gathering is a huge dataset with dedicated information (e.g. user lists, etc.)

Methods to do information gathering

- Google and all search engines are best friends ☺
  - Simple search engine queries
  - Specific search engine queries (google hacking, see later)
  - Cached data (data that are not online right now, but can be restored)
- The social media is another best friend ☺
- Companies and persons spread lots of information from themselves
- We can create personal and company profiles
- We can identify key persons and other key information

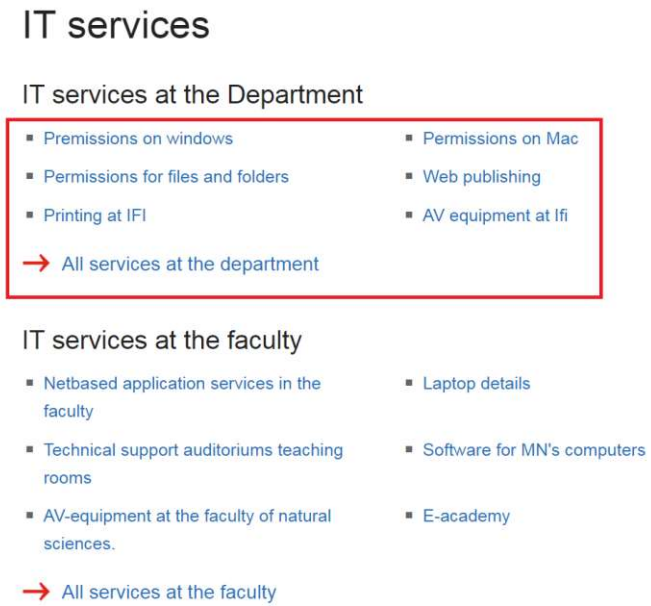
Simple information gathering using Google

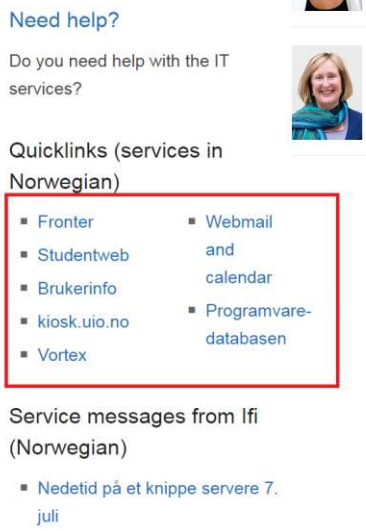


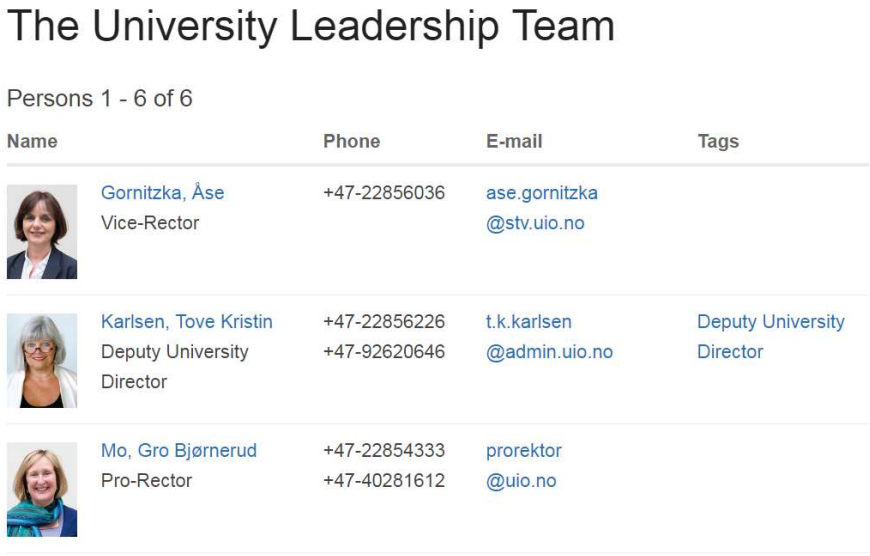
- Default website (domain name), other sites
- History, several public data (faculties, number of staff members)

Simple information gathering using Google

- Keypersons with contact details
- Important pages
- Services

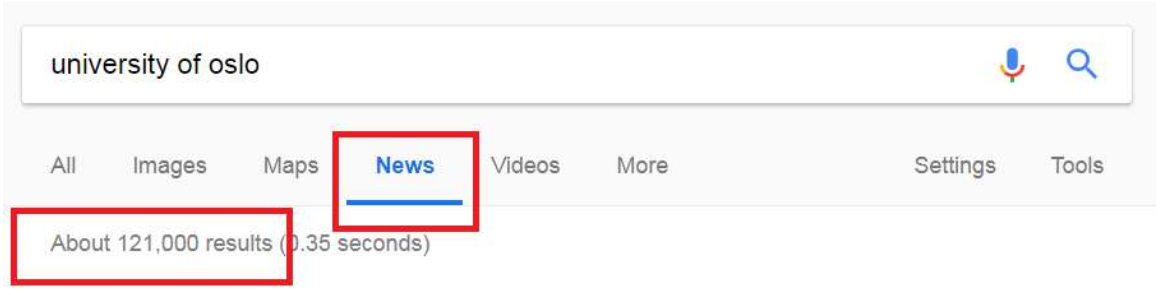






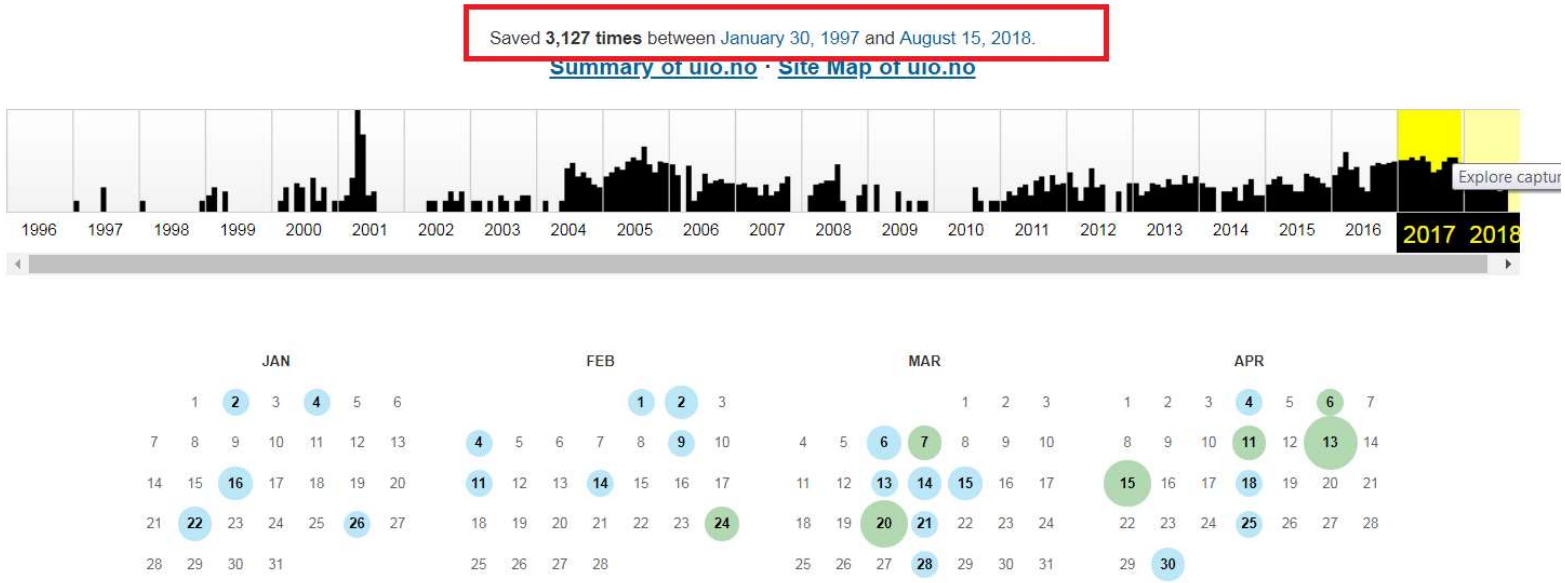
Collecting actual target related information

- Reading the news
- Social media info



Collecting cached information

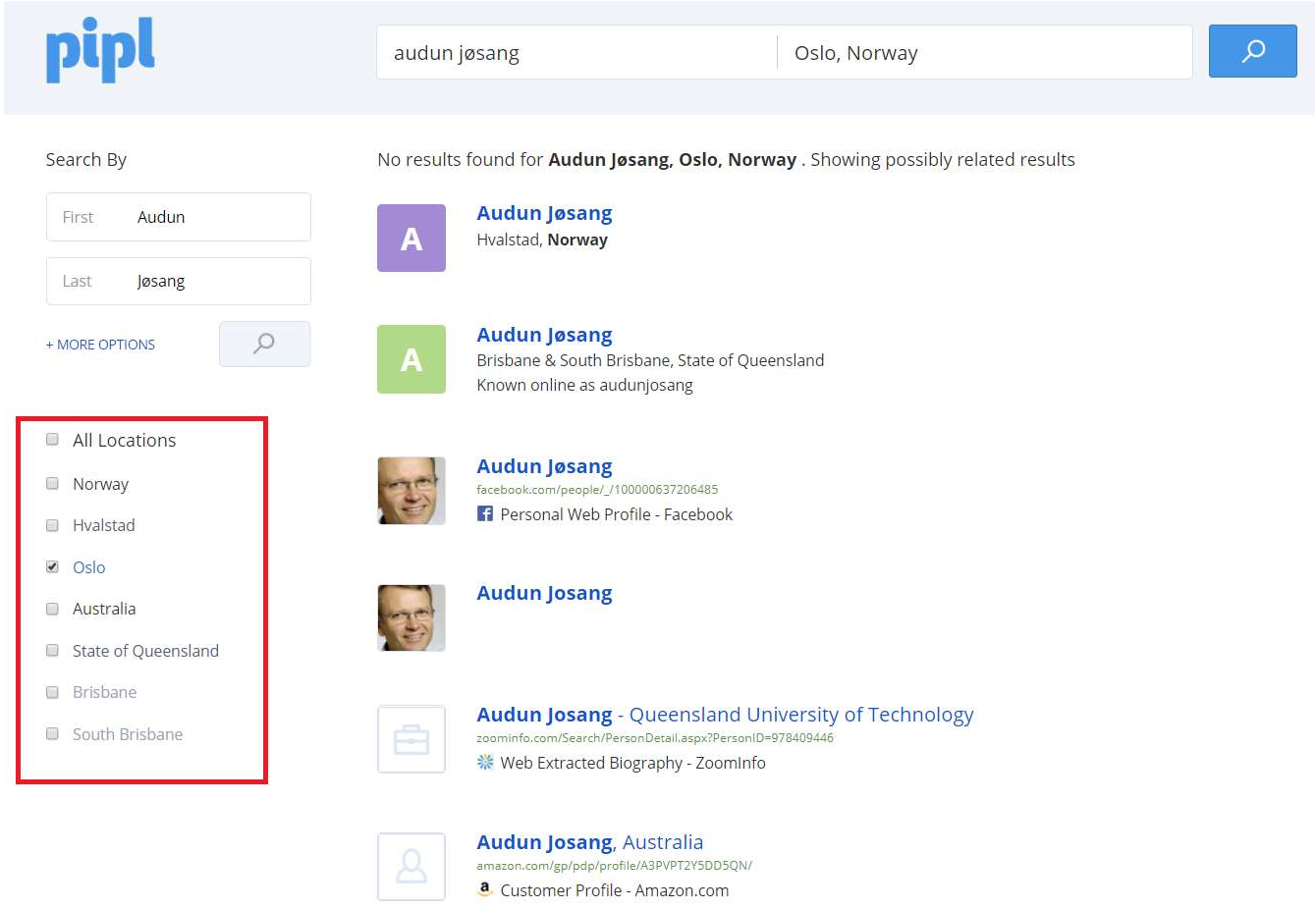
- Archive.org wayback machine



- Google cached results

Pipl.com – Finding accounts

- Personal information
- Net catalogues
- Academic records
- Social accounts



Using social media to build personal profile

- Work and education
- Places of living
- Contact info
- Family relationships
- Details
- Life events
- Photos
- Favorites (music, sports, films, etc..)
- Friends
- Timeline data

Using social media to carry out social engineering attacks - examples

Social Engineering using private information:

Isak spent 5 days at the Scandic Hotel Kristiansand. He posted on Facebook (Checked in Scandic Kristiansand). 5 days later Isak receives an email from the ‘’Hotel’’ (attacker). Dear guests! Our hotel would like to surprise all our guests between the age of 14 and 24 who visited us during the last month with a SuperMario Cart game as a summer holiday surprise. Please fill in the following form and provide your address: **link** We hope you enjoyed your stay at our hotel, etc..

Building personal profile using social media

Stine has a Facebook account where she listed all her favorites. One of her favorite singer is Rihanna. The attacker brute-forces Stina’s password and finds out that one of her passwords is Diamonds2012. The attacker logs in to Stine’s Facebook account and steals private photos, writes weird messages to her friends, etc.

Everyone can be misled, it’s just a question of timing and story!

Every information can be important, hackers collect all available information and systemize them before planning the attack!

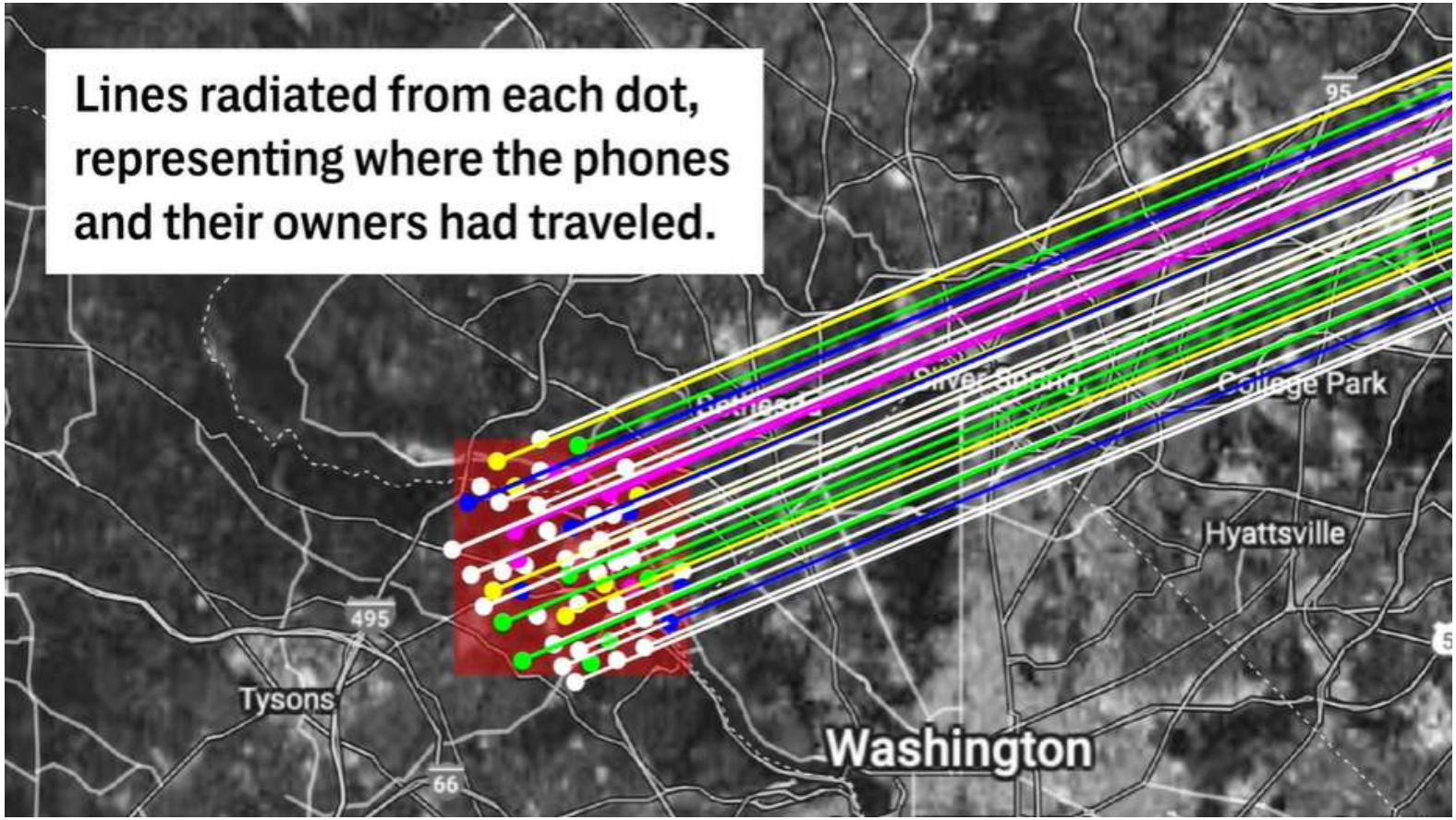
OSINT tools

- Maltego (collecting information using various sources)
- Shodan (Finding IoTs, vulnerabilities in IoTs)
- Google dorks (special search engine expressions)
- Metagoofil (collecting metadata)
- Recon-ng (Modular information gathering tool)
- Checkusernames.com (search for users on social media)
- TinEye (reverse image search)
- Knowem.com (social media profiles)
- Darksearch.io
- Many others…

Twitter search ☺

Elon: Can you take this down? It is a security risk.
Sweeney: Yes I can but it'll cost you a Model 3 only joking unless?
Elon: How about $5k for this account and generally helping make it harder for crazy people to track me?
Sweeney: Sounds doable, account and all my help. Any chance to up that to $50K?

Phone tracking allows to identify CIA and NSA workers? (Anomaly Six)

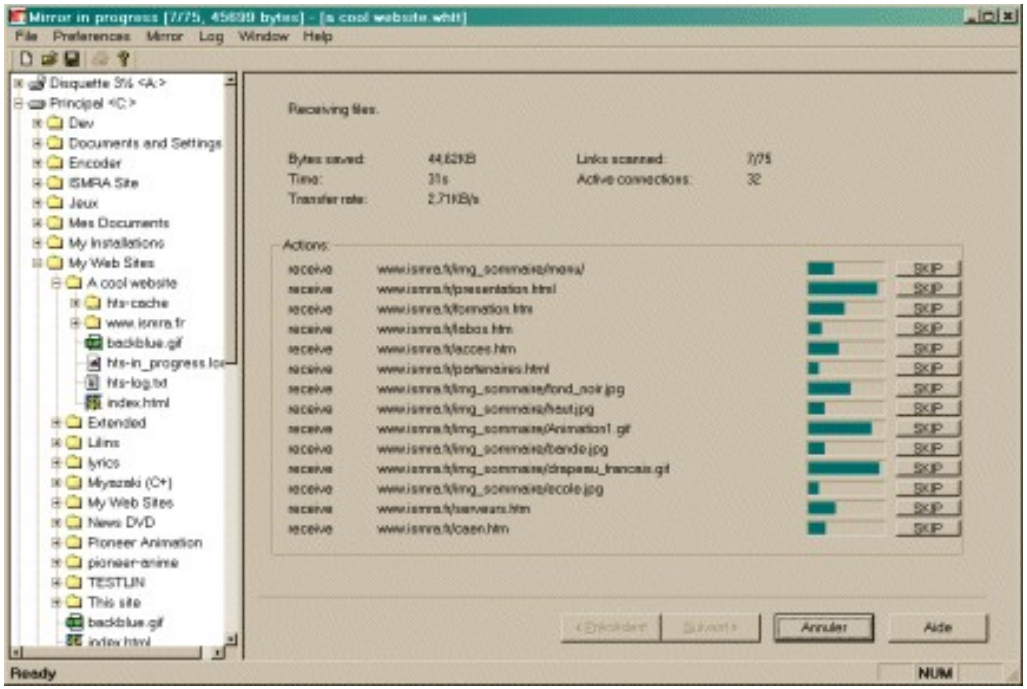


https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-zignal-surveillance-cia-nsa/

Collecting information from webpages

- All static information can be downloaded at once (noisy, but useful)
- Several tools exist like *wget* or *Httrack*

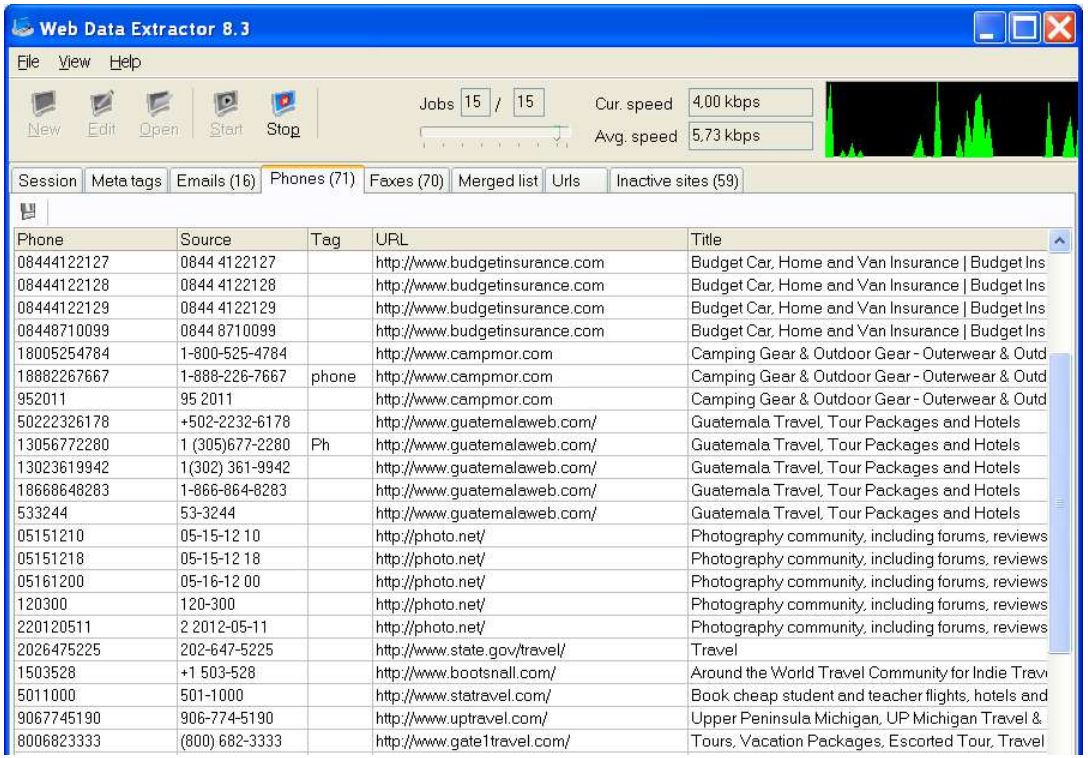
Httrack demo …



Specific information search

- We can look for specific info such as email addresses, phone numbers, meta data, etc.

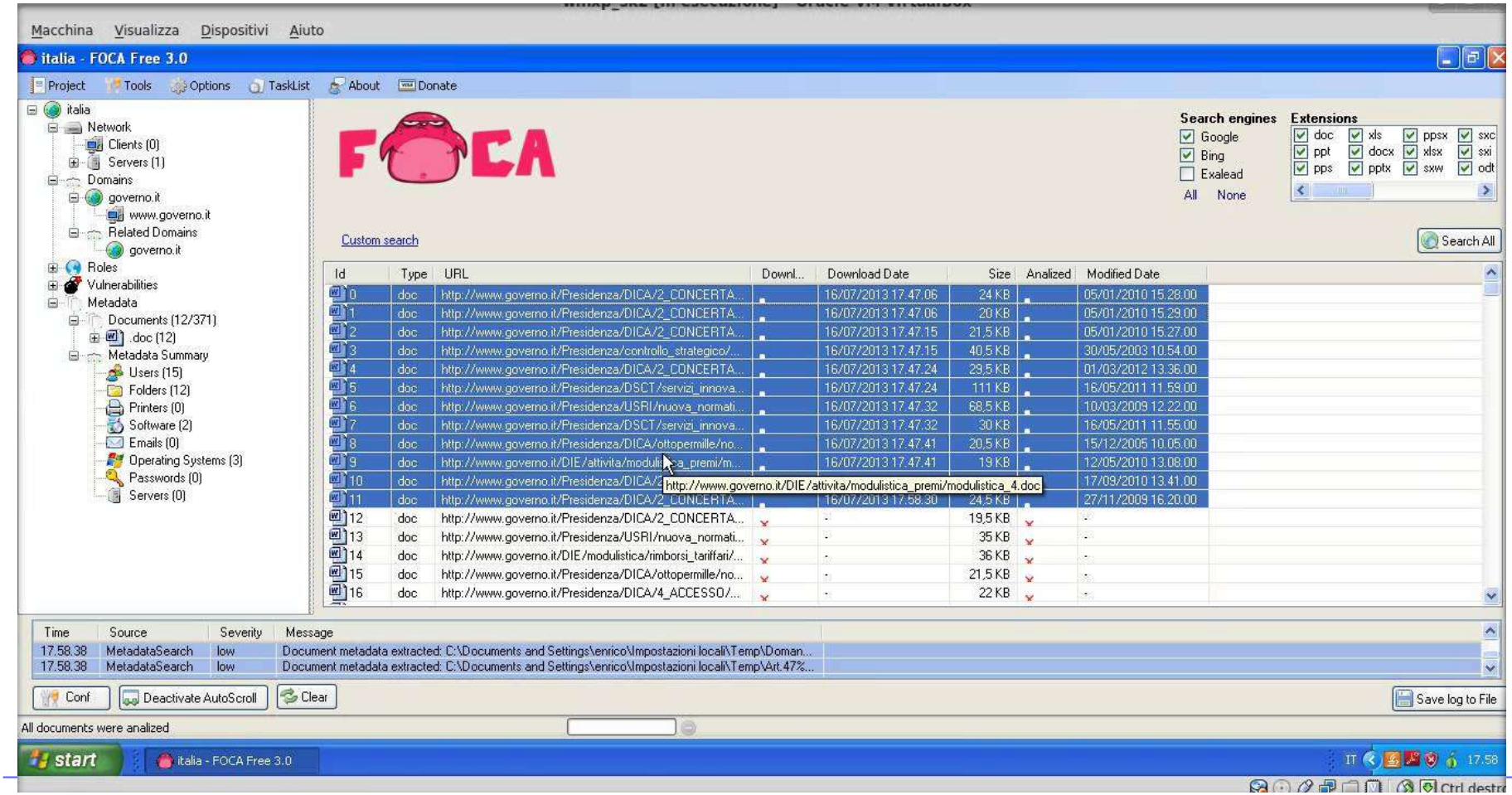
Web Data Extractor demo …



Phone	Source	Tag	URL	Title
08444122127	0844 4122127		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance | Budget Ins
08444122128	0844 4122128		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance | Budget Ins
08444122129	0844 4122129		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance | Budget Ins
08448710099	0844 8710099		http://www.budgetinsurance.com	Budget Car, Home and Van Insurance | Budget Ins
18005254784	1-800-525-4784		http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
18882267667	1-888-226-7667	phone	http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
952011	95 2011		http://www.campmor.com	Camping Gear & Outdoor Gear - Outerwear & Outd
50222326178	+502-2232-6178		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
13056772280	1 (305)677-2280	Ph	http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
13023619942	1(302) 361-9942		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
18668648283	1-866-864-8283		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
533244	53-3244		http://www.guatemalaweb.com/	Guatemala Travel, Tour Packages and Hotels
05151210	05-15-12 10		http://photo.net/	Photography community, including forums, reviews
05151218	05-15-12 18		http://photo.net/	Photography community, including forums, reviews
05161200	05-16-12 00		http://photo.net/	Photography community, including forums, reviews
120300	120-300		http://photo.net/	Photography community, including forums, reviews
220120511	2 2012-05-11		http://photo.net/	Photography community, including forums, reviews
2026475225	202-647-5225		http://www.state.gov/travel/	Travel
1503528	+1 503-528		http://www.bootsnall.com/	Around the World Travel Community for Indie Trav
5011000	501-1000		http://www.statravel.com/	Book cheap student and teacher flights, hotels and
9067745190	906-774-5190		http://www.uptravel.com/	Upper Peninsula Michigan, UP Michigan Travel &
8006823333	(800) 682-3333		http://www.gate1travel.com/	Tours, Vacation Packages, Escorted Tour, Travel

Specific information search

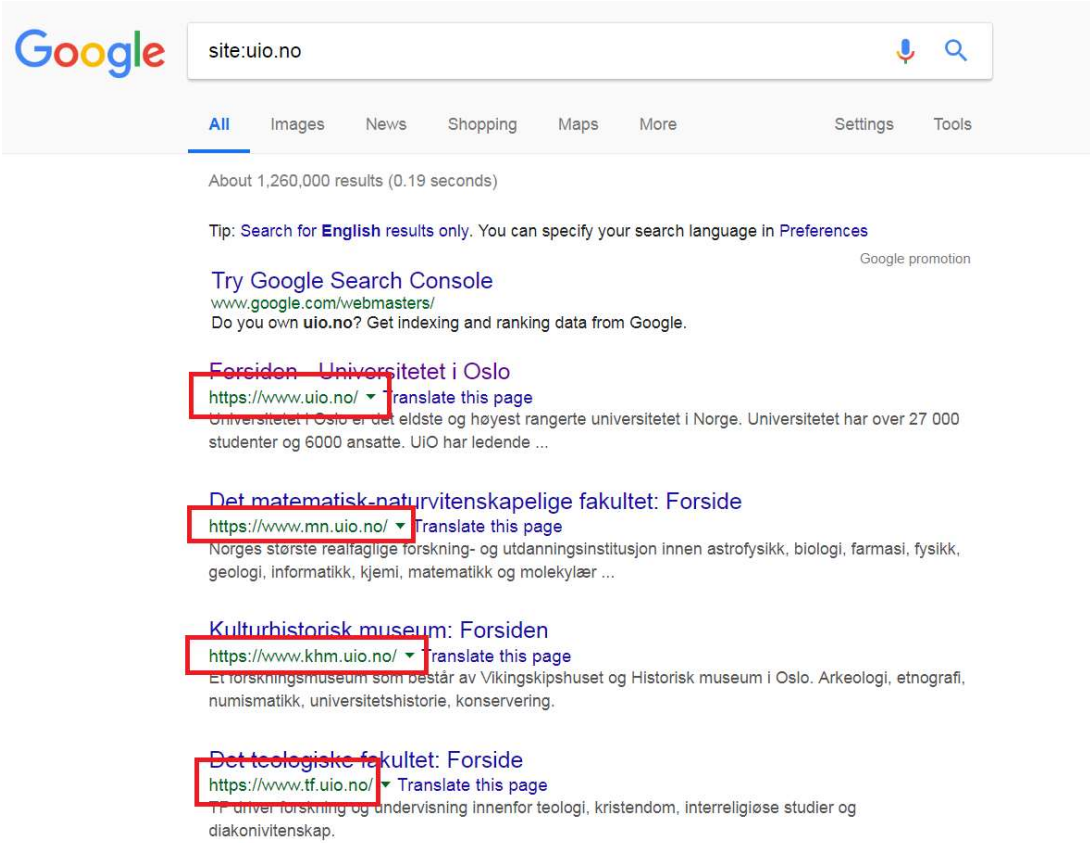
- *Foca* is able to find documents by extensions
- It also shows several technical information



Information gathering with Google hacking

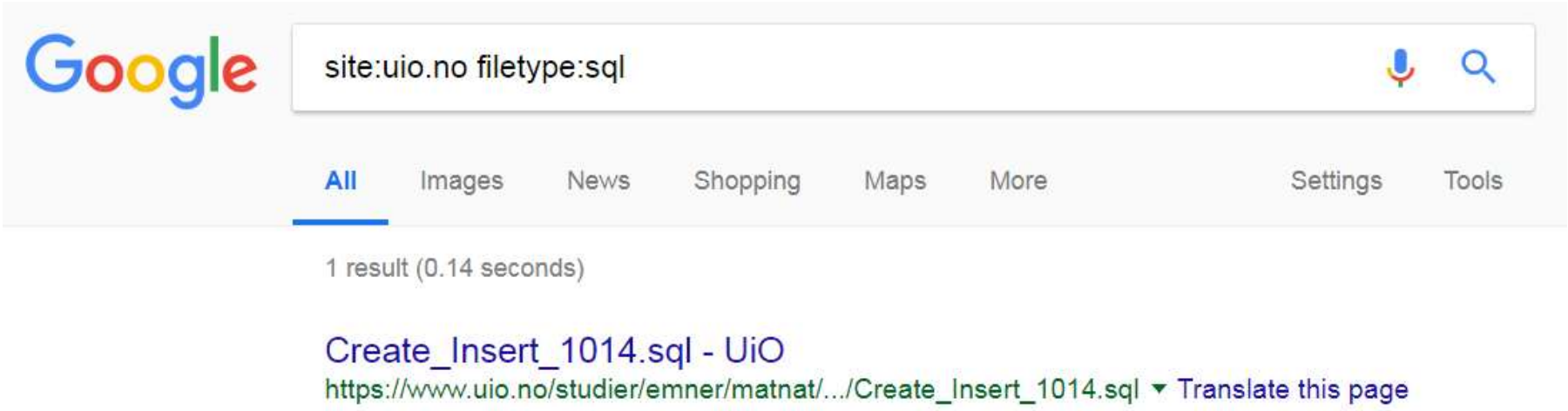
- Using specific Google queries we can use smart filtering or get «hidden» data
- Filter to domain: use the site keyword
- Negative filtering is also possible:

  site:uio.no -www



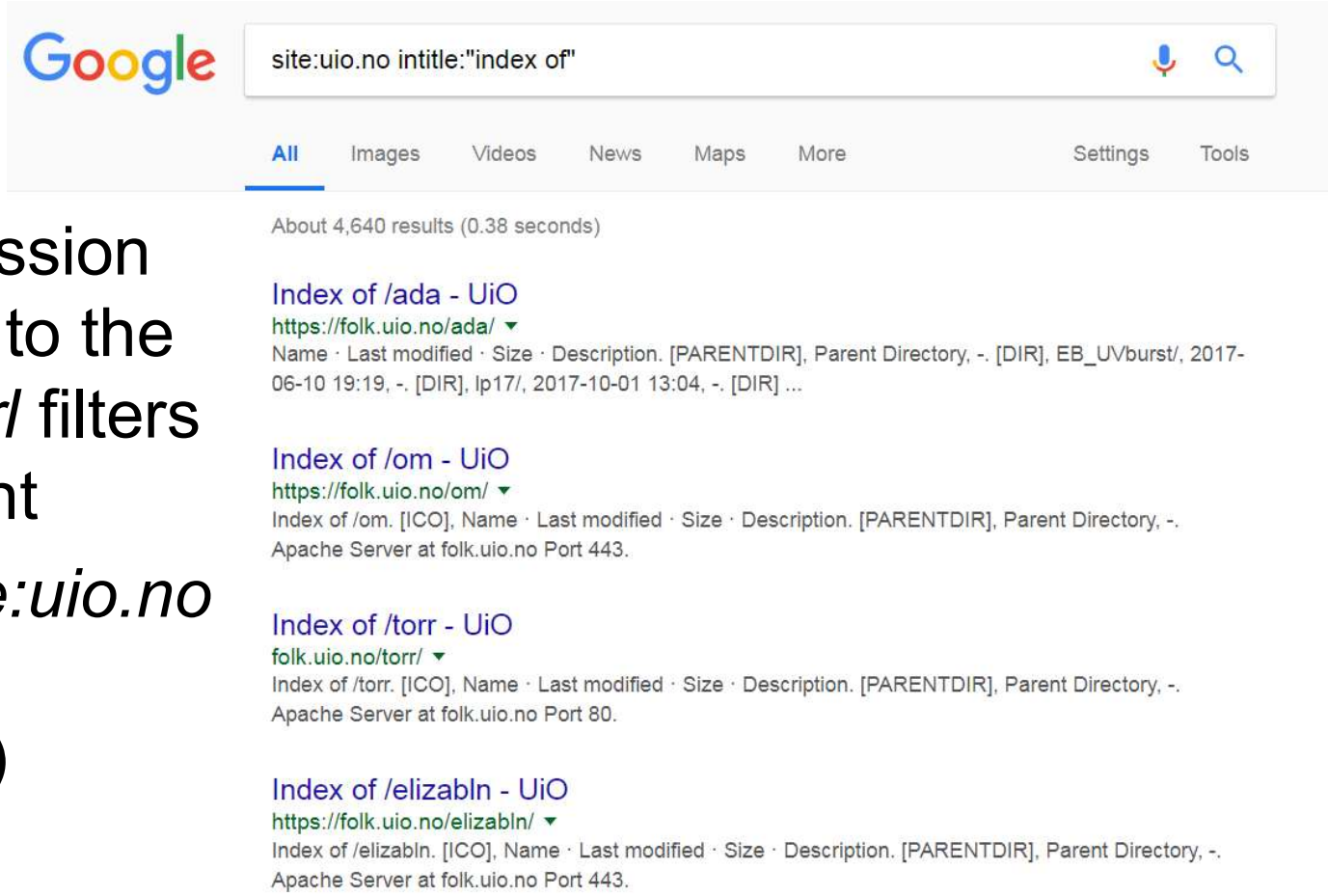
Information gathering with Google hacking

- Filter to file type with extension: use the type keyword
- Interesting file extensions: doc, xls, txt, conf, inc, sql, …
- Expressions can be combined



Information gathering with Google hacking

- The *intitle* expression filters according to the site title, the *inurl* filters for the url content
- Try this one: *site:uio.no intitle:"index of"* (directory listing)



Information gathering with Google hacking

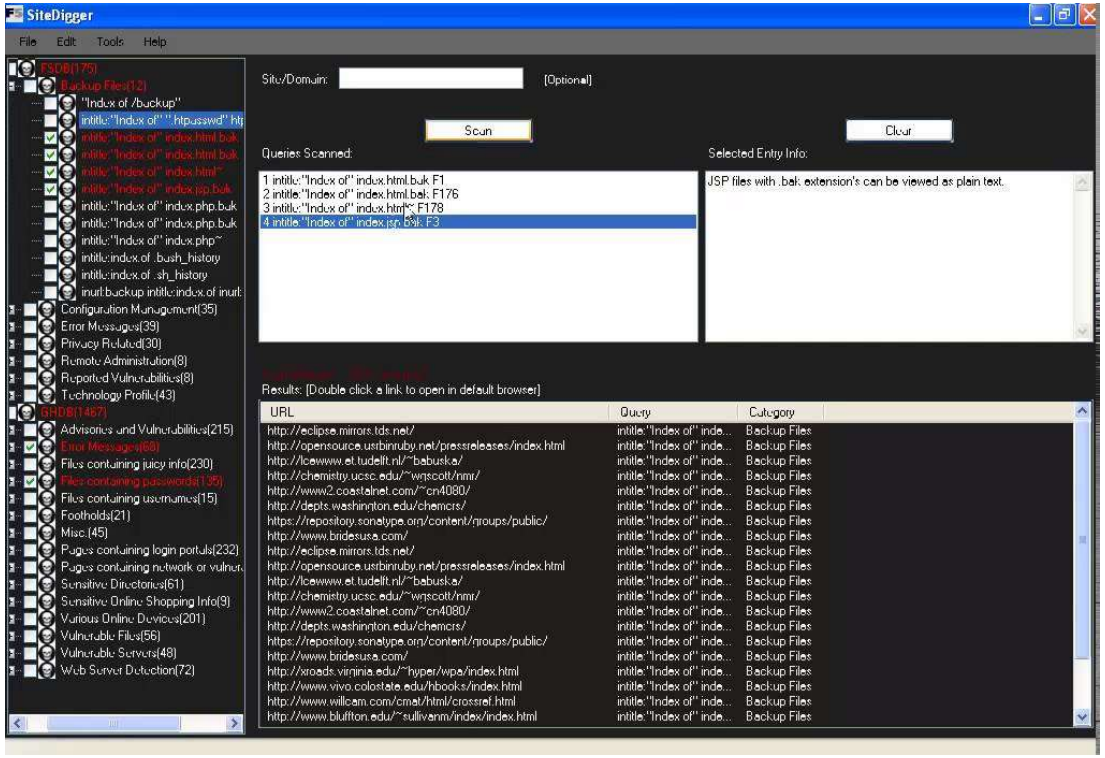
There is a database (google hack database – ghdb) that contains up-to-date google hack expressions (check the exploit-db website)

Tools supporting automatic Google hacking

SiteDigger (by FoundStone) is an old tool that carries out google hacking using its own database

Wikto is also capable using Google API key (1000 requests/day)

SiteDigger demo …



What is needed for the lectures and workshops throughout the semester?

Kali Linux (http://kali.org)

- Debian based Linux distribution with hundreds of preinstalled hacking tools
- Easy to use, tools are classified according to the hacking tasks and steps (info gathering, forensics, vulnerability assessment, etc.)
- Easy to install (ready and up-up-to-date Vmware and Virtualbox images)

End of lecture