# TTM4175 Introduction to Communication Technology and data security

## Introduction to Ethical Hacking

NTNU

Norwegian University of Science and Technology

Laszlo Erdödi

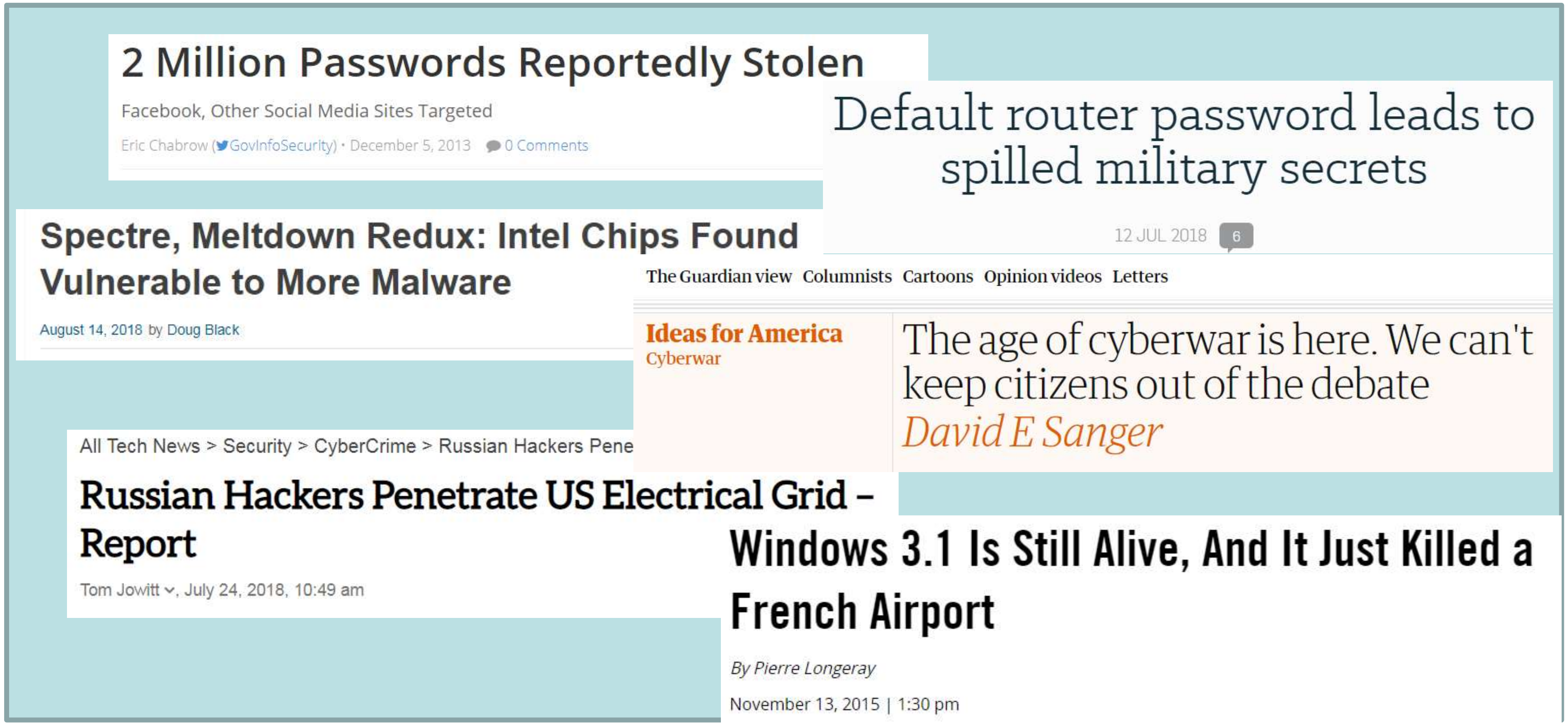
laszlo.erdodi@ntnu.no

# 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



2 Million Passwords Reportedly Stolen

Facebook, Other Social Media Sites Targeted

Eric Chabrow (GovInfoSecurity) • December 5, 2013 0 Comments

Default router password leads to spilled military secrets

12 JUL 2018 6

Spectre, Meltdown Redux: Intel Chips Found Vulnerable to More Malware

August 14, 2018 by Doug Black

The Guardian view Columnists Cartoons Opinion videos Letters

Ideas for America
Cyberwar

The age of cyberwar is here. We can't keep citizens out of the debate
*David E Sanger*

All Tech News > Security > CyberCrime > Russian Hackers Pene

Russian Hackers Penetrate US Electrical Grid – Report

Tom Jowitt, July 24, 2018, 10:49 am

Windows 3.1 Is Still Alive, And It Just Killed a French Airport

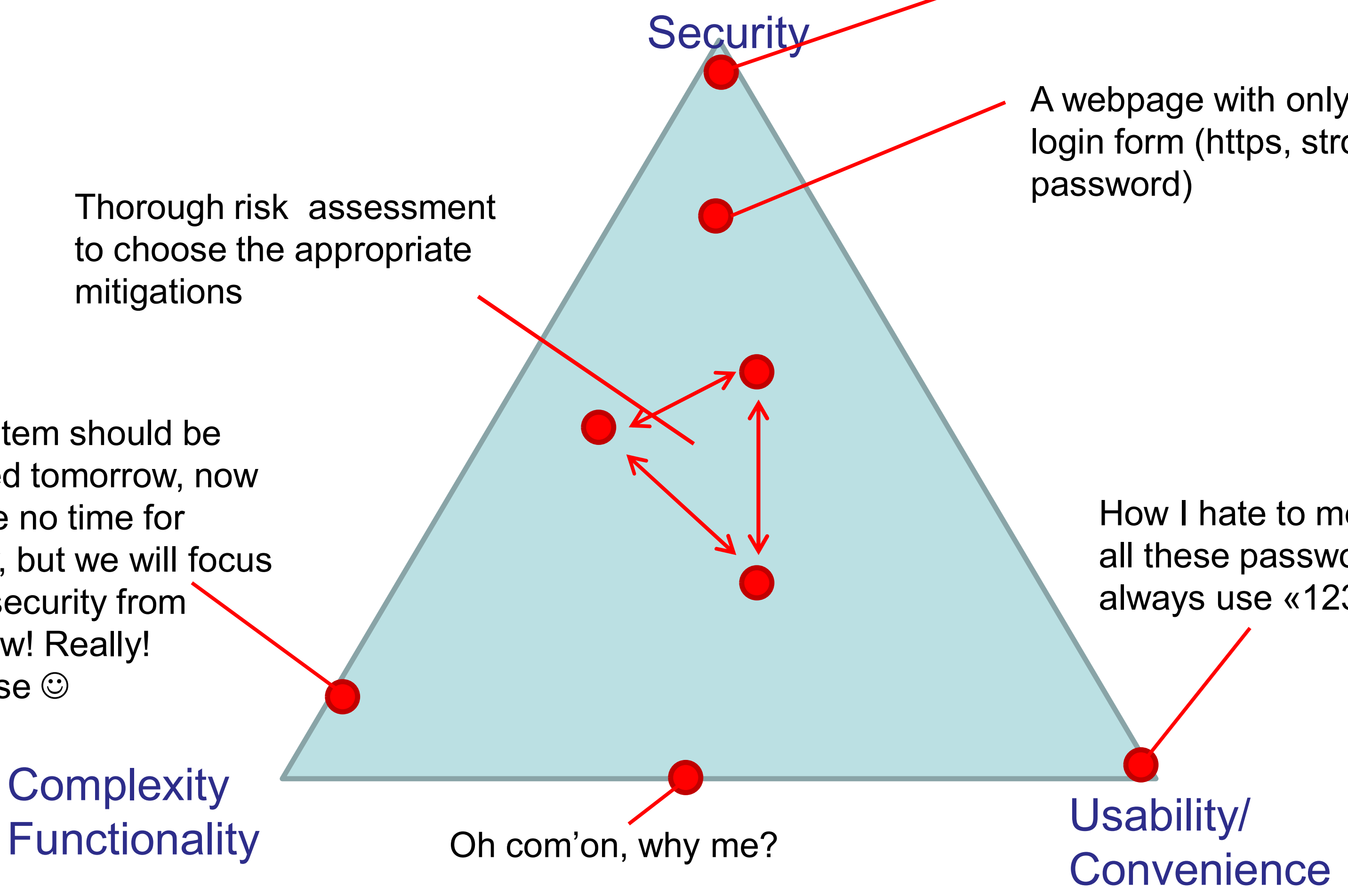
*By Pierre Longeray*

November 13, 2015 | 1:30 pm

# 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 not plug the cable out? ☺

A webpage with only one login form (https, strong password)

Thorough risk  assessment to choose the appropriate mitigations

The system should be launched tomorrow, now we have no time for security, but we will focus on the security from tomorrow! Really!
Of course ☺

How I hate to memorize all these passwords, I always use «123456»

Oh com’on, why me?

# 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

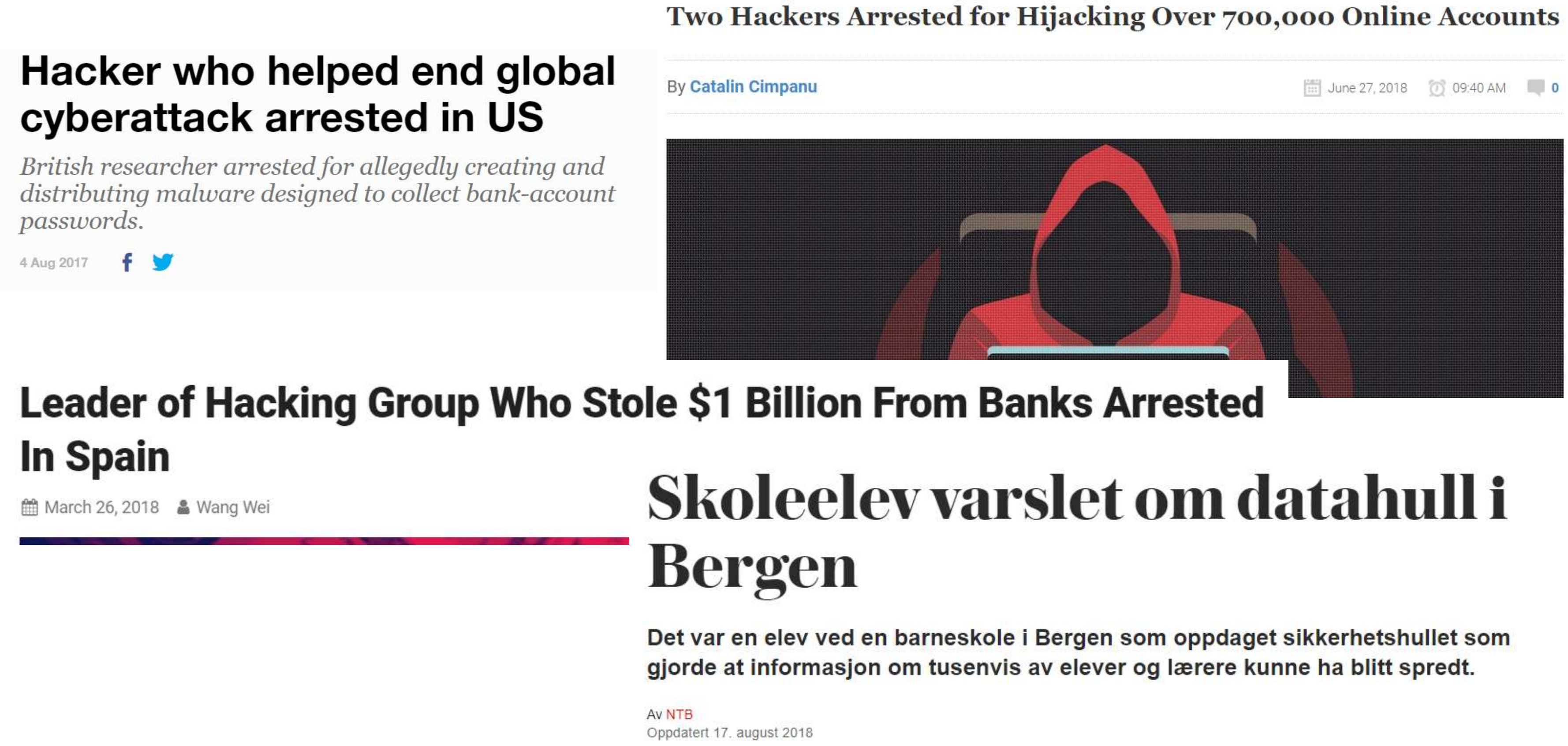
- Break the information security triple (confidentiality, integrity, availability)
  - Steal confidential information
  - Modify data
  - Make services unavailable (Denial Of Service)

- 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?

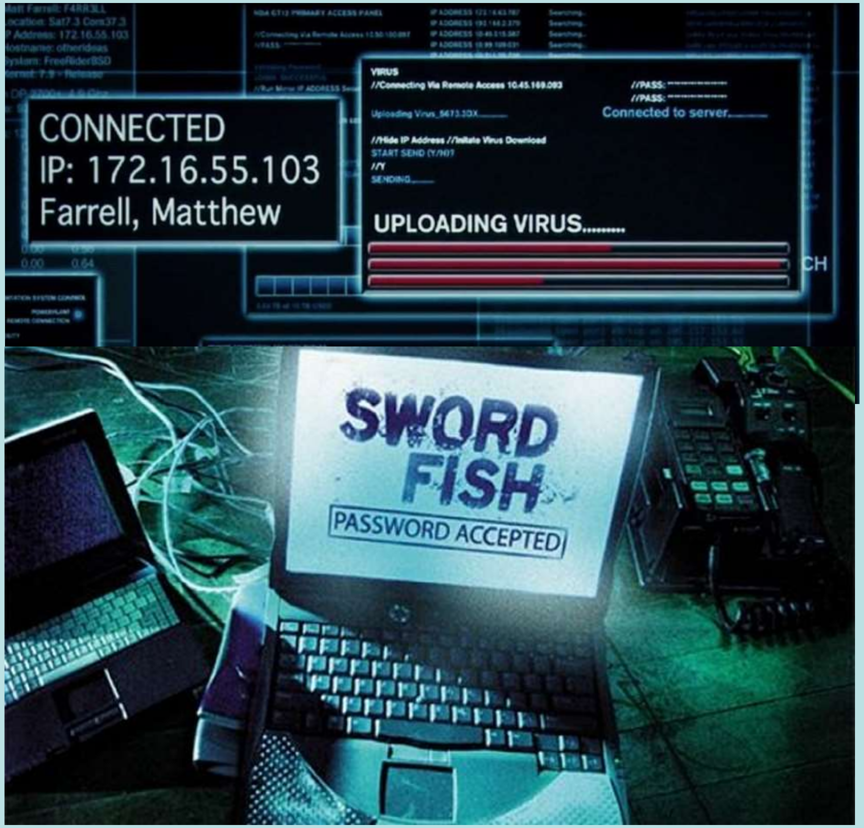
# Differences between ethical and non-ethical hacking

| | |
|---|---|
| • Legal (contract) | • Illegal |
| • Promote the security by showing the vulnerabilities | • Steal information, modify data, make service unavailable for own purpose |
| • Find all vulnerabilities | • Find the easiest way to reach the goal (weakest link) |
| • Without causing harm | • Do not care if the system destroys the system (but not too early) |
| • Document all activities | • Without documentation |
| • Final presentation and report | • Without report, delete all clues |

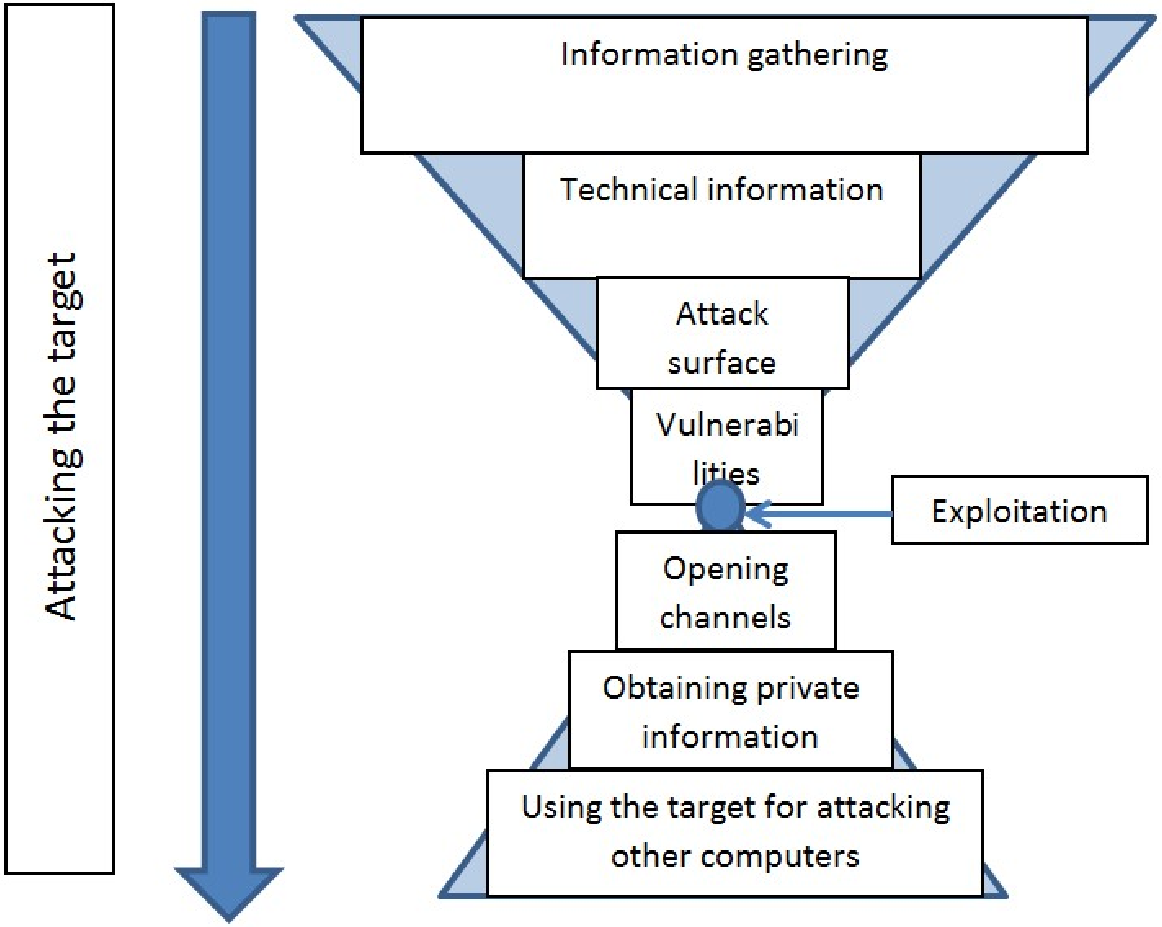
# Main steps of hacking

- 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

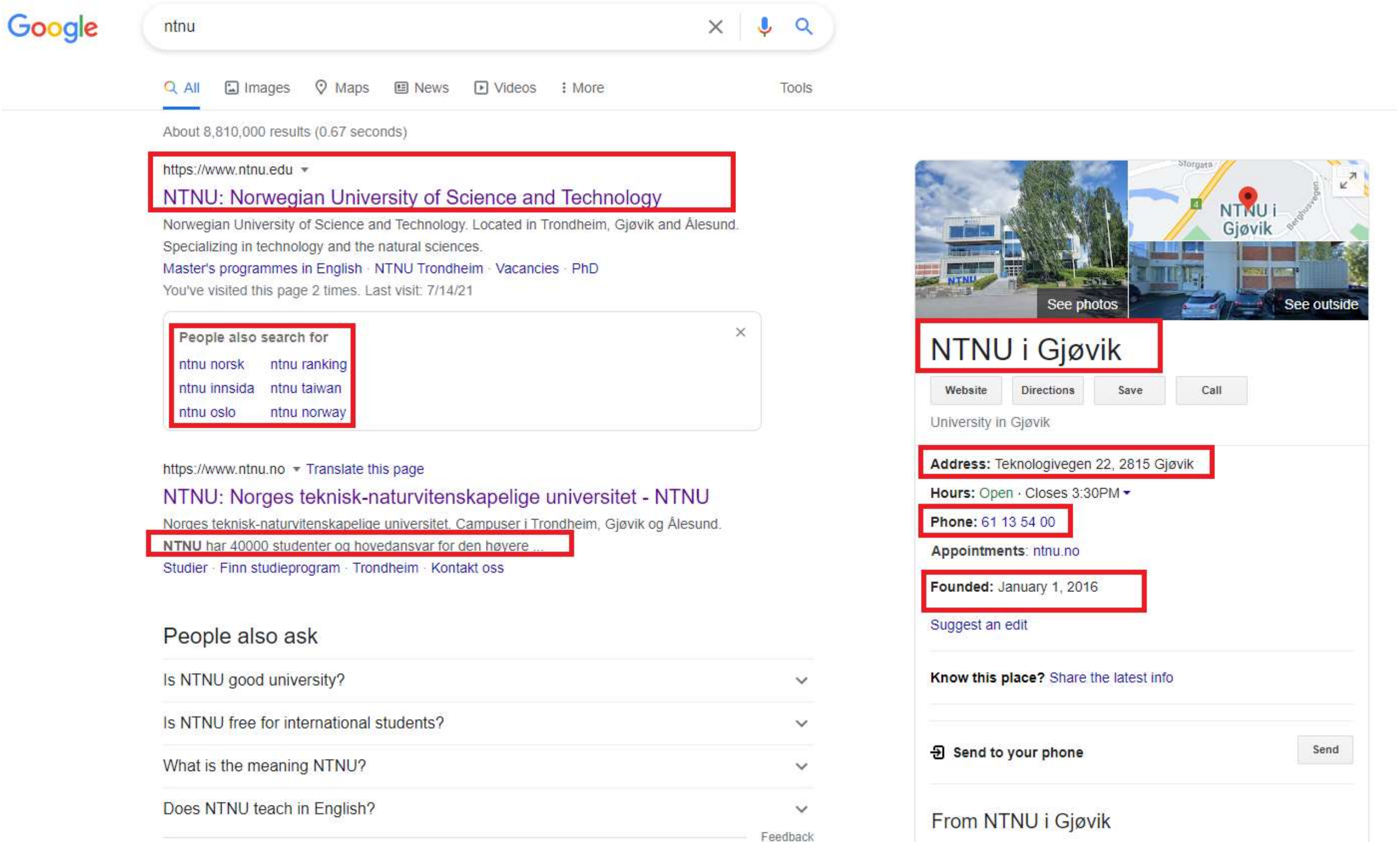
# General information gathering

- 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



About 8,810,000 results (0.67 seconds)

https://www.ntnu.edu

NTNU: Norwegian University of Science and Technology

Norwegian University of Science and Technology. Located in Trondheim, Gjøvik and Ålesund. Specializing in technology and the natural sciences.

Master's programmes in English · NTNU Trondheim · Vacancies · PhD

You've visited this page 2 times. Last visit: 7/14/21

People also search for

| | |
|---|---|
| ntnu norsk | ntnu ranking |
| ntnu innsida | ntnu taiwan |
| ntnu oslo | ntnu norway |

https://www.ntnu.no · Translate this page

NTNU: Norges teknisk-naturvitenskapelige universitet - NTNU

Norges teknisk-naturvitenskapelige universitet. Campuser i Trondheim, Gjøvik og Ålesund. NTNU har 40000 studenter og hovedansvar for den høyere ...

Studier · Finn studieprogram · Trondheim · Kontakt oss

People also ask

Is NTNU good university?

Is NTNU free for international students?

What is the meaning NTNU?

Does NTNU teach in English?

NTNU i Gjøvik

University in Gjøvik

**Address:** Teknologivegen 22, 2815 Gjøvik

**Hours:** Open · Closes 3:30PM

**Phone:** 61 13 54 00

**Appointments:** ntnu.no

**Founded:** January 1, 2016

Suggest an edit

**Know this place?** Share the latest info

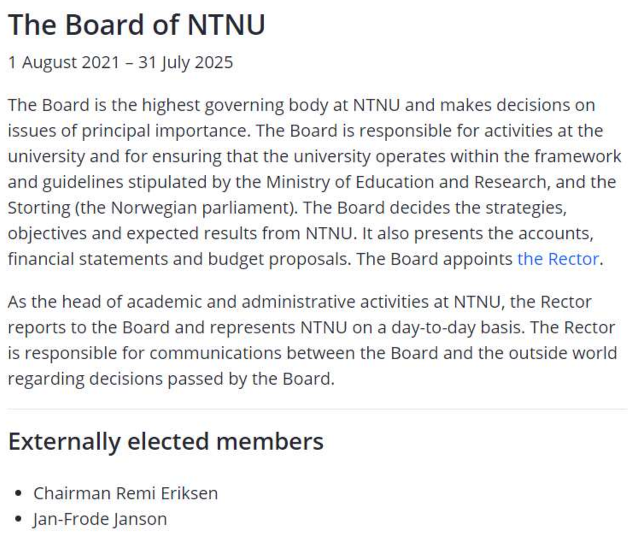
Send to your phone

From NTNU i Gjøvik

- 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



### The Board of NTNU

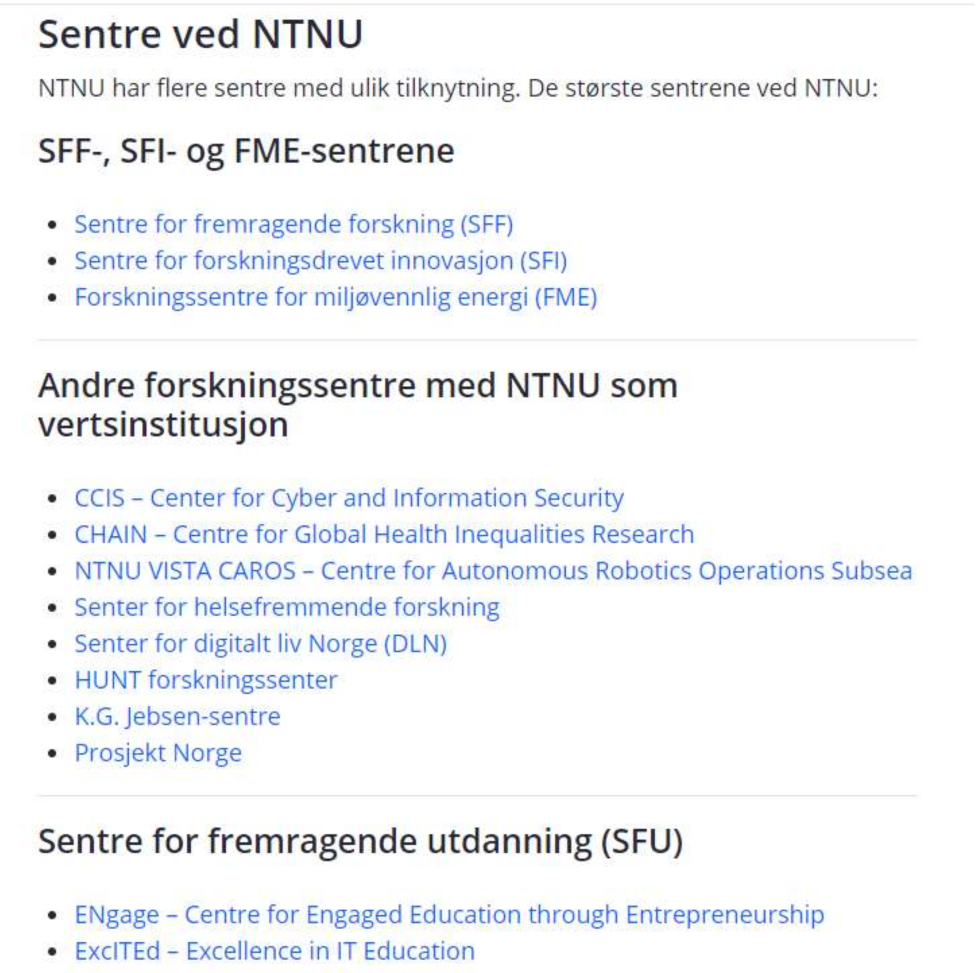
1 August 2021 – 31 July 2025

The Board is the highest governing body at NTNU and makes decisions on issues of principal importance. The Board is responsible for activities at the university and for ensuring that the university operates within the framework and guidelines stipulated by the Ministry of Education and Research, and the Storting (the Norwegian parliament). The Board decides the strategies, objectives and expected results from NTNU. It also presents the accounts, financial statements and budget proposals. The Board appoints the Rector.

As the head of academic and administrative activities at NTNU, the Rector reports to the Board and represents NTNU on a day-to-day basis. The Rector is responsible for communications between the Board and the outside world regarding decisions passed by the Board.

#### Externally elected members

- Chairman Remi Eriksen
- Jan-Frode Janson



### Sentre ved NTNU

NTNU har flere sentre med ulik tilknytning. De største sentrene ved NTNU:

#### SFF-, SFI- og FME-sentrene

- Sentre for fremragende forskning (SFF)
- Sentre for forskningsdrevet innovasjon (SFI)
- Forskningssentre for miljøvennlig energi (FME)

#### Andre forskningssentre med NTNU som vertsinstitusjon

- CCIS – Center for Cyber and Information Security
- CHAIN – Centre for Global Health Inequalities Research
- NTNU VISTA CAROS – Centre for Autonomous Robotics Operations Subsea
- Senter for helsefremmende forskning
- Senter for digitalt liv Norge (DLN)
- HUNT forskningssenter
- K.G. Jebsen-sentre
- Prosjekt Norge

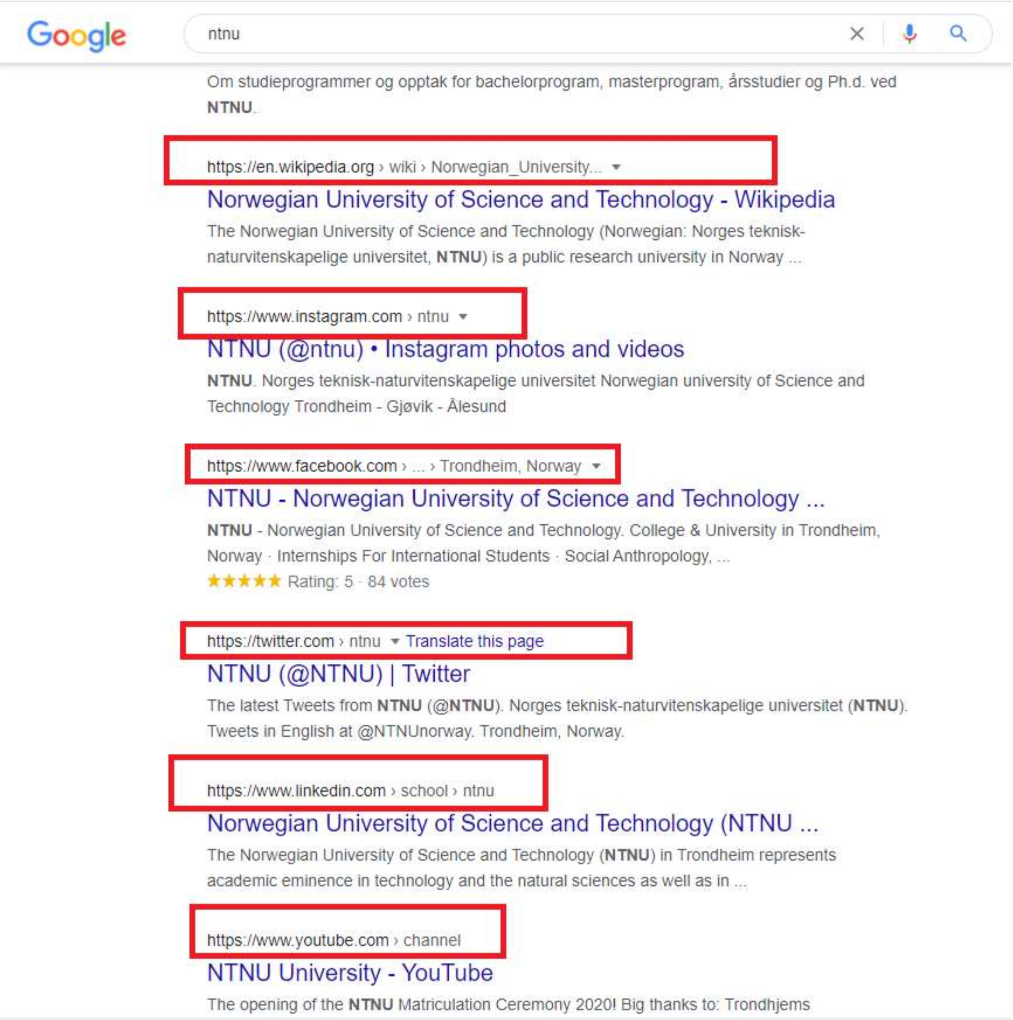
#### Sentre for fremragende utdanning (SFU)

- ENgage – Centre for Engaged Education through Entrepreneurship
- ExcITEd – Excellence in IT Education

# Collecting actual target related information

- Reading the news

- Social media info



ntnu

Om studieprogrammer og opptak for bachelorprogram, masterprogram, årsstudier og Ph.d. ved **NTNU**.

https://en.wikipedia.org › wiki › Norwegian_University... ▾

Norwegian University of Science and Technology - Wikipedia

The Norwegian University of Science and Technology (Norwegian: Norges teknisk-naturvitenskapelige universitet, **NTNU**) is a public research university in Norway ...

https://www.instagram.com › ntnu ▾

NTNU (@ntnu) • Instagram photos and videos

**NTNU**. Norges teknisk-naturvitenskapelige universitet Norwegian university of Science and Technology Trondheim - Gjøvik - Ålesund

https://www.facebook.com › ... › Trondheim, Norway ▾

NTNU - Norwegian University of Science and Technology ...

**NTNU** - Norwegian University of Science and Technology. College & University in Trondheim, Norway · Internships For International Students · Social Anthropology, ...

★★★★★ Rating: 5 · 84 votes

https://twitter.com › ntnu ▾ Translate this page

NTNU (@NTNU) | Twitter

The latest Tweets from **NTNU** (@**NTNU**). Norges teknisk-naturvitenskapelige universitet (**NTNU**). Tweets in English at @NTNUnorway. Trondheim, Norway.

https://www.linkedin.com › school › ntnu

Norwegian University of Science and Technology (NTNU ...

The Norwegian University of Science and Technology (**NTNU**) in Trondheim represents academic eminence in technology and the natural sciences as well as in ...

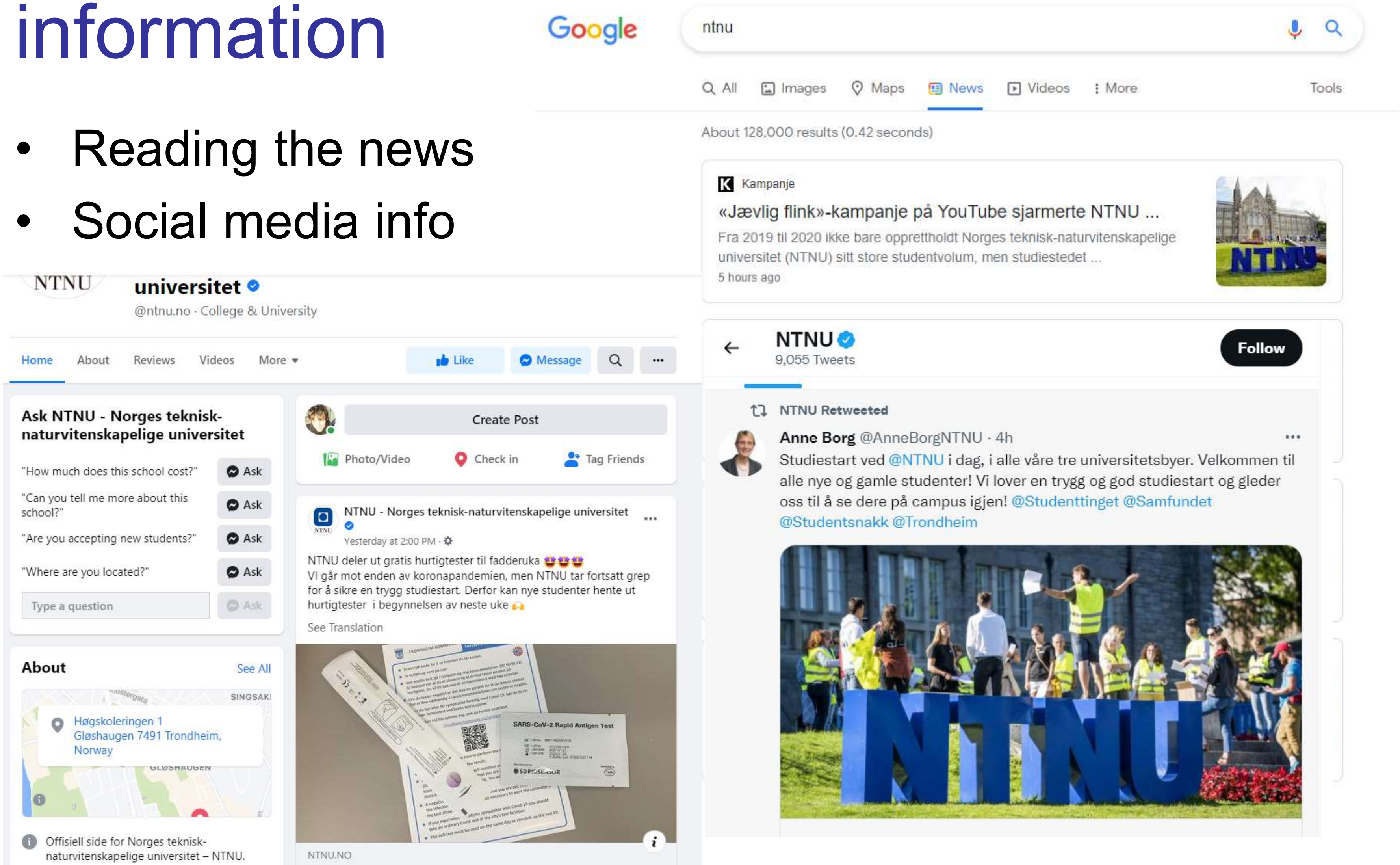
https://www.youtube.com › channel

NTNU University - YouTube

The opening of the **NTNU** Matriculation Ceremony 2020! Big thanks to: Trondhjems

# Collecting actual target related information

- Reading the news
- Social media info



ntnu

All · Images · Maps · News · Videos · More · Tools

About 128,000 results (0.42 seconds)

Kampanje

«Jævlig flink»-kampanje på YouTube sjarmerte NTNU ...

Fra 2019 til 2020 ikke bare opprettholdt Norges teknisk-naturvitenskapelige universitet (NTNU) sitt store studentvolum, men studiestedet ...

5 hours ago

NTNU universitet

@ntnu.no · College & University

Home · About · Reviews · Videos · More · Like · Message

Ask NTNU - Norges teknisk-naturvitenskapelige universitet

"How much does this school cost?" Ask

"Can you tell me more about this school?" Ask

"Are you accepting new students?" Ask

"Where are you located?" Ask

Type a question · Ask

About · See All

Høgskoleringen 1
Gløshaugen 7491 Trondheim, Norway

Offisiell side for Norges teknisk-naturvitenskapelige universitet – NTNU.

Create Post

Photo/Video · Check in · Tag Friends

NTNU - Norges teknisk-naturvitenskapelige universitet

Yesterday at 2:00 PM

NTNU deler ut gratis hurtigtester til fadderuka 🤩🤩🤩
Vi går mot enden av koronapandemien, men NTNU tar fortsatt grep for å sikre en trygg studiestart. Derfor kan nye studenter hente ut hurtigtester i begynnelsen av neste uke 🙌

See Translation

NTNU.NO

NTNU
9,055 Tweets

Follow

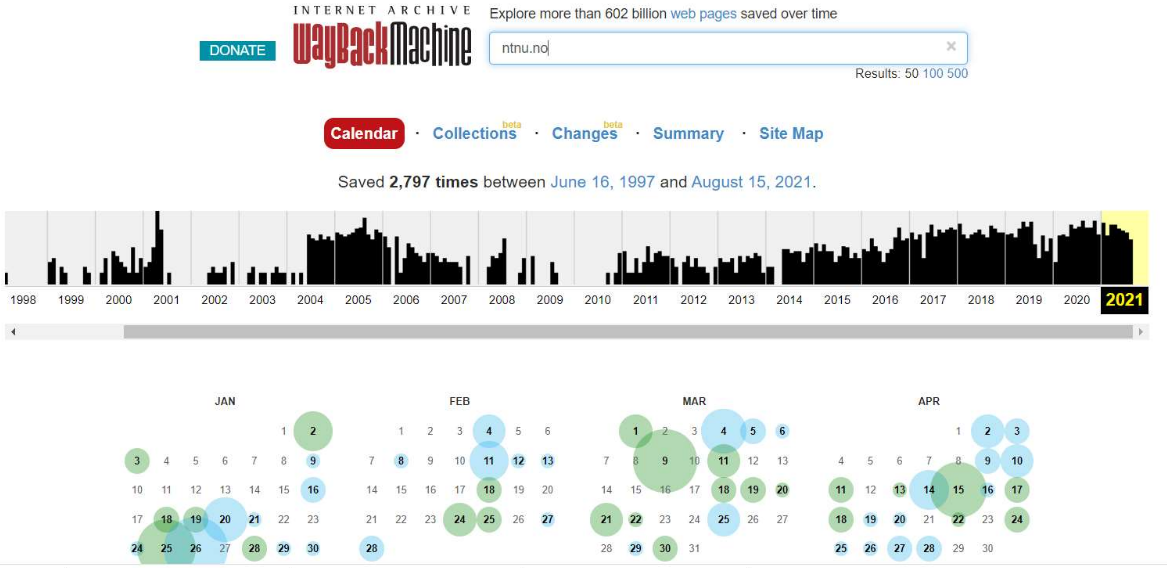
NTNU Retweeted

Anne Borg @AnneBorgNTNU · 4h

Studiestart ved @NTNU i dag, i alle våre tre universitetsbyer. Velkommen til alle nye og gamle studenter! Vi lover en trygg og god studiestart og gleder oss til å se dere på campus igjen! @Studenttinget @Samfundet @Studentsnakk @Trondheim

# Collecting cached information

- Archive.org wayback machine

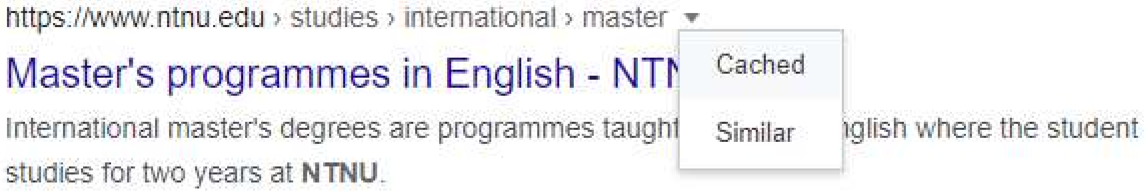


Explore more than 602 billion web pages saved over time

ntnu.no

Saved **2,797 times** between June 16, 1997 and August 15, 2021.

- Google cached results



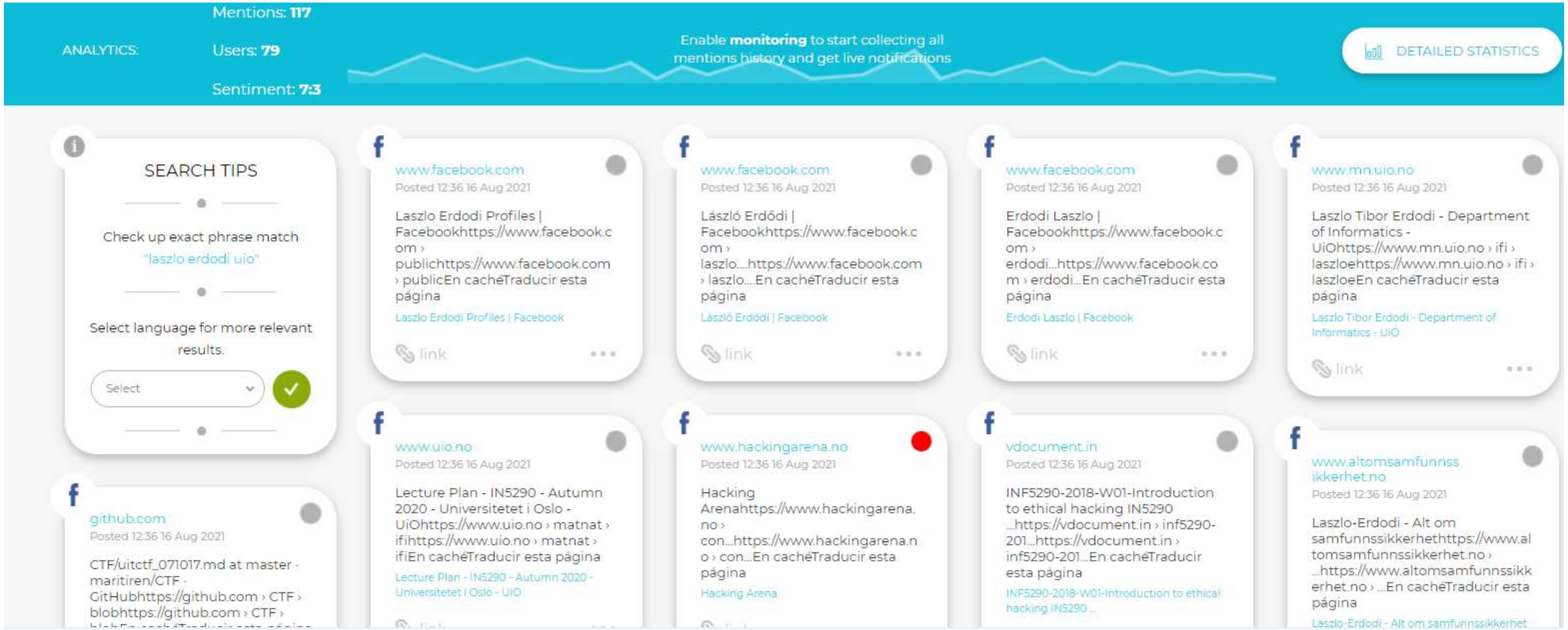
https://www.ntnu.edu › studies › international › master

Master's programmes in English - NTN

International master's degrees are programmes taught ...nglish where the student studies for two years at **NTNU**.

# Searching on Social Media

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



ANALYTICS: Mentions: **117** Users: **79** Sentiment: **7:3**

Enable **monitoring** to start collecting all mentions history and get live notifications

SEARCH TIPS

Check up exact phrase match "laszlo erdodi uio"

Select language for more relevant results.

github.com
Posted 12:36 16 Aug 2021

CTF/uitctf_071017.md at master - maritiren/CTF - GitHubhttps://github.com › CTF › blobhttps://github.com › CTF ›

www.facebook.com
Posted 12:36 16 Aug 2021

Laszlo Erdodi Profiles | Facebookhttps://www.facebook.com › publichttps://www.facebook.com › publicEn cachéTraducir esta página

Laszlo Erdodi Profiles | Facebook

www.uio.no
Posted 12:36 16 Aug 2021

Lecture Plan - IN5290 - Autumn 2020 - Universitetet i Oslo - UiOhttps://www.uio.no › matnat › ifihttps://www.uio.no › matnat › ifiEn cachéTraducir esta página

Lecture Plan - IN5290 - Autumn 2020 - Universitetet i Oslo - UiO

www.facebook.com
Posted 12:36 16 Aug 2021

László Erdődi | Facebookhttps://www.facebook.com › laszlo....https://www.facebook.com › laszlo....En cachéTraducir esta página

László Erdődi | Facebook

www.hackingarena.no
Posted 12:36 16 Aug 2021

Hacking Arenahttps://www.hackingarena.no › con...https://www.hackingarena.no › con...En cachéTraducir esta página

Hacking Arena

www.facebook.com
Posted 12:36 16 Aug 2021

Erdodi Laszlo | Facebookhttps://www.facebook.com › erdodi...https://www.facebook.com › erdodi...En cachéTraducir esta página

Erdodi Laszlo | Facebook

vdocument.in
Posted 12:36 16 Aug 2021

INF5290-2018-W01-Introduction to ethical hacking IN5290 ...https://vdocument.in › inf5290-201...https://vdocument.in › inf5290-201...En cachéTraducir esta página

INF5290-2018-W01-Introduction to ethical hacking IN5290 ...

www.mn.uio.no
Posted 12:36 16 Aug 2021

Laszlo Tibor Erdodi - Department of Informatics - UiOhttps://www.mn.uio.no › ifi › laszloehttps://www.mn.uio.no › ifi › laszloeEn cachéTraducir esta página

Laszlo Tibor Erdodi - Department of Informatics - UiO

www.altomsamfunnssikkerhet.no
Posted 12:36 16 Aug 2021

Laszlo-Erdodi - Alt om samfunnssikkerhethttps://www.altomsamfunnssikkerhet.no › ...https://www.altomsamfunnssikkerhet.no › ...En cachéTraducir esta página

Laszlo-Erdodi - Alt om samfunnssikkerhet

# 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.

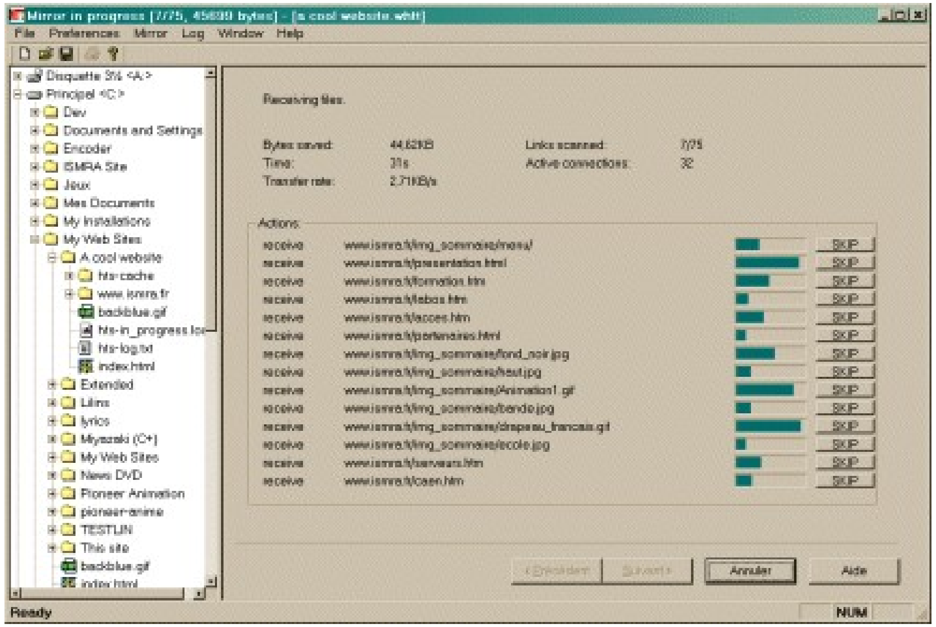
**Everyone can be misled, it's just a question of timing and story!**

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

# Collecting information from webpages

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

**Httrack demo …**



Receiving files.

Bytes saved: 44,62KB  Links scanned: 7/75
Time: 31s  Active connections: 32
Transfer rate: 2,71KB/s

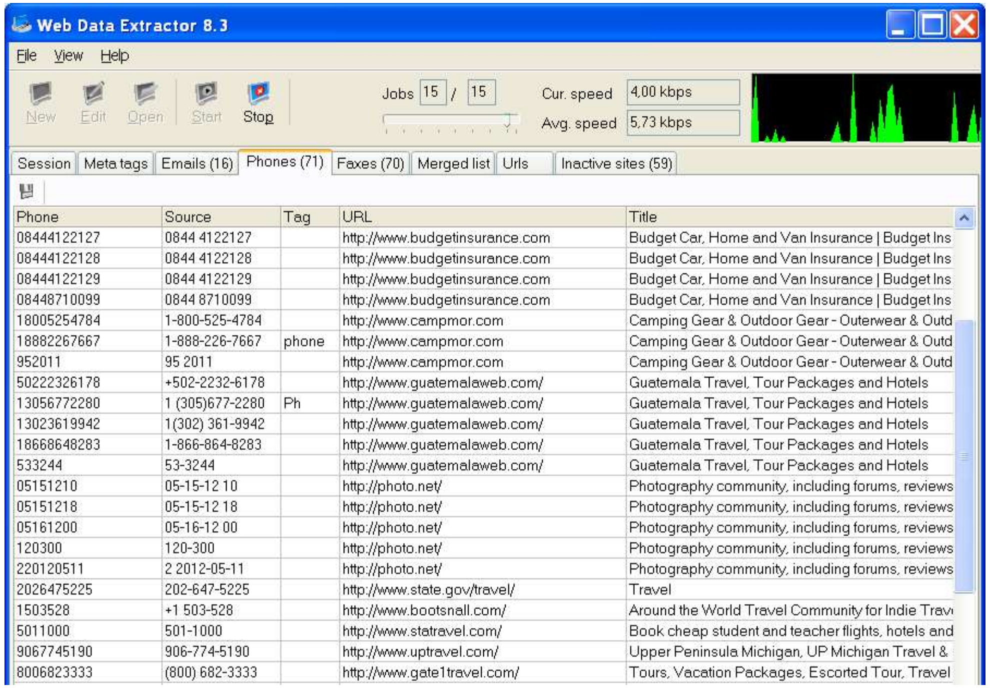
Actions:

```
receive   www.ismra.fr/img_sommaire/menu/                    SKIP
receive   www.ismra.fr/presentation.html                     SKIP
receive   www.ismra.fr/formation.htm                         SKIP
receive   www.ismra.fr/labos.htm                             SKIP
receive   www.ismra.fr/acces.htm                             SKIP
receive   www.ismra.fr/partenaires.html                      SKIP
receive   www.ismra.fr/img_sommaire/fond_noir.jpg            SKIP
receive   www.ismra.fr/img_sommaire/haut.jpg                 SKIP
receive   www.ismra.fr/img_sommaire/Animation1.gif           SKIP
receive   www.ismra.fr/img_sommaire/bando.jpg                SKIP
receive   www.ismra.fr/img_sommaire/drapeau_francais.gif     SKIP
receive   www.ismra.fr/img_sommaire/ecole.jpg                SKIP
receive   www.ismra.fr/serveurs.htm                          SKIP
receive   www.ismra.fr/caen.htm                              SKIP
```

# Specific information search

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

**Web Data Extractor demo …**



Jobs 15 / 15

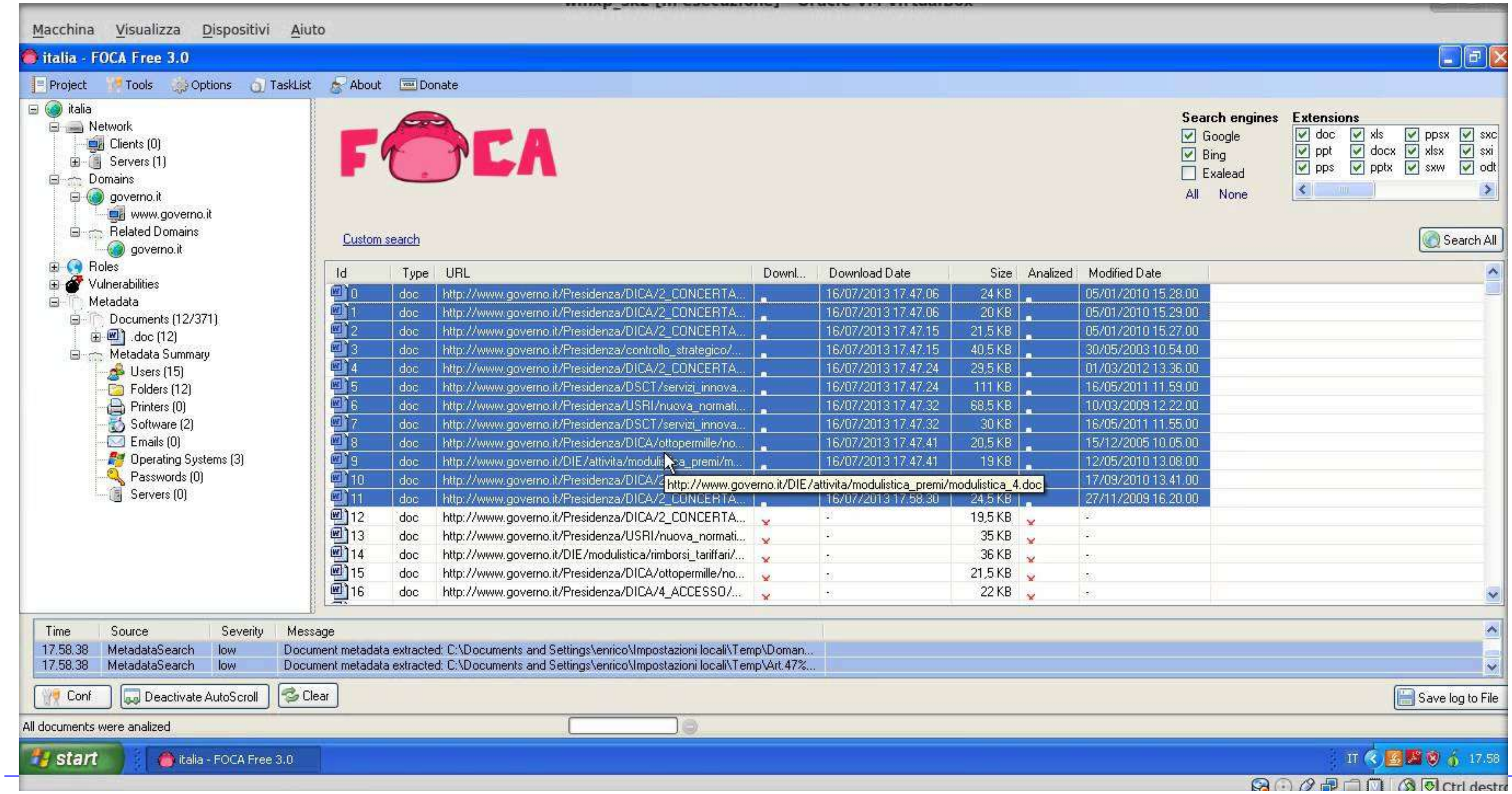
Cur. speed 4,00 kbps

Avg. speed 5,73 kbps

| 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



Search engines
☑ Google
☑ Bing
□ Exalead
All None

Extensions
☑ doc ☑ xls ☑ ppsx ☑ sxc
☑ ppt ☑ docx ☑ xlsx ☑ sxi
☑ pps ☑ pptx ☑ sxw ☑ odt

| Id | Type | URL | Downl... | Download Date | Size | Analized | Modified Date |
|---|---|---|---|---|---|---|---|
| 0 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | | 16/07/2013 17.47.06 | 24 KB | | 05/01/2010 15.28.00 |
| 1 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | | 16/07/2013 17.47.06 | 20 KB | | 05/01/2010 15.29.00 |
| 2 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | | 16/07/2013 17.47.15 | 21,5 KB | | 05/01/2010 15.27.00 |
| 3 | doc | http://www.governo.it/Presidenza/controllo_strategico/... | | 16/07/2013 17.47.15 | 40,5 KB | | 30/05/2003 10.54.00 |
| 4 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | | 16/07/2013 17.47.24 | 29,5 KB | | 01/03/2012 13.36.00 |
| 5 | doc | http://www.governo.it/Presidenza/DSCT/servizi_innova... | | 16/07/2013 17.47.24 | 111 KB | | 16/05/2011 11.59.00 |
| 6 | doc | http://www.governo.it/Presidenza/USRI/nuova_normati... | | 16/07/2013 17.47.32 | 68,5 KB | | 10/03/2009 12.22.00 |
| 7 | doc | http://www.governo.it/Presidenza/DSCT/servizi_innova... | | 16/07/2013 17.47.32 | 30 KB | | 16/05/2011 11.55.00 |
| 8 | doc | http://www.governo.it/Presidenza/DICA/ottopermille/no... | | 16/07/2013 17.47.41 | 20,5 KB | | 15/12/2005 10.05.00 |
| 9 | doc | http://www.governo.it/DIE/attivita/moduli[illegible]a_premi/m... | | 16/07/2013 17.47.41 | 19 KB | | 12/05/2010 13.08.00 |
| 10 | doc | http://www.governo.it/Presidenza/DICA/2 | | | | | 17/09/2010 13.41.00 |
| 11 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | | 16/07/2013 17.58.30 | 24,5 KB | | 27/11/2009 16.20.00 |
| 12 | doc | http://www.governo.it/Presidenza/DICA/2_CONCERTA... | ✗ | - | 19,5 KB | ✗ | - |
| 13 | doc | http://www.governo.it/Presidenza/USRI/nuova_normati... | ✗ | - | 35 KB | ✗ | - |
| 14 | doc | http://www.governo.it/DIE/modulistica/rimborsi_tariffari/... | ✗ | - | 36 KB | ✗ | - |
| 15 | doc | http://www.governo.it/Presidenza/DICA/ottopermille/no... | ✗ | - | 21,5 KB | ✗ | - |
| 16 | doc | http://www.governo.it/Presidenza/DICA/4_ACCESSO/... | ✗ | - | 22 KB | ✗ | - |

http://www.governo.it/DIE/attivita/modulistica_premi/modulistica_4.doc

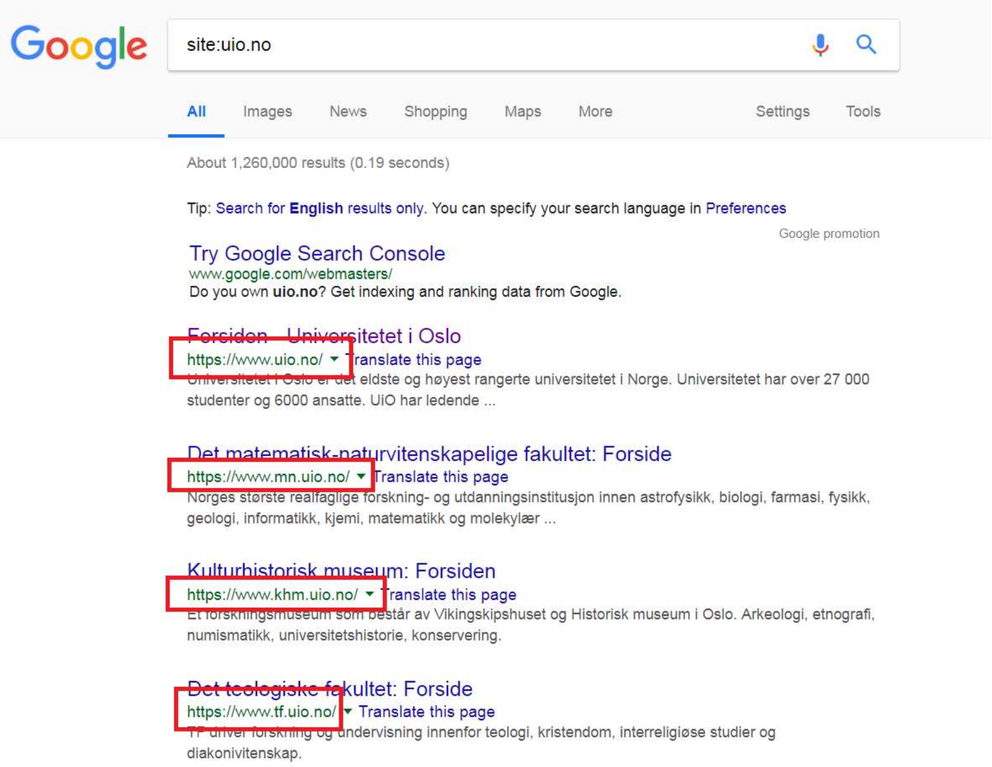
| Time | Source | Severity | Message |
|---|---|---|---|
| 17.58.38 | MetadataSearch | low | Document metadata extracted: C:\Documents and Settings\enrico\Impostazioni locali\Temp\Doman... |
| 17.58.38 | MetadataSearch | low | Document metadata extracted: C:\Documents and Settings\enrico\Impostazioni locali\Temp\Art.47%... |

All documents were analized

# 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*



About 1,260,000 results (0.19 seconds)

Tip: Search for **English** results only. You can specify your search language in Preferences

Google promotion

Try Google Search Console
www.google.com/webmasters/
Do you own **uio.no**? Get indexing and ranking data from Google.

Forsiden - Universitetet i Oslo
https://www.uio.no/ ▾ Translate this page
Universitetet i Oslo er det eldste og høyest rangerte universitetet i Norge. Universitetet har over 27 000 studenter og 6000 ansatte. UiO har ledende ...

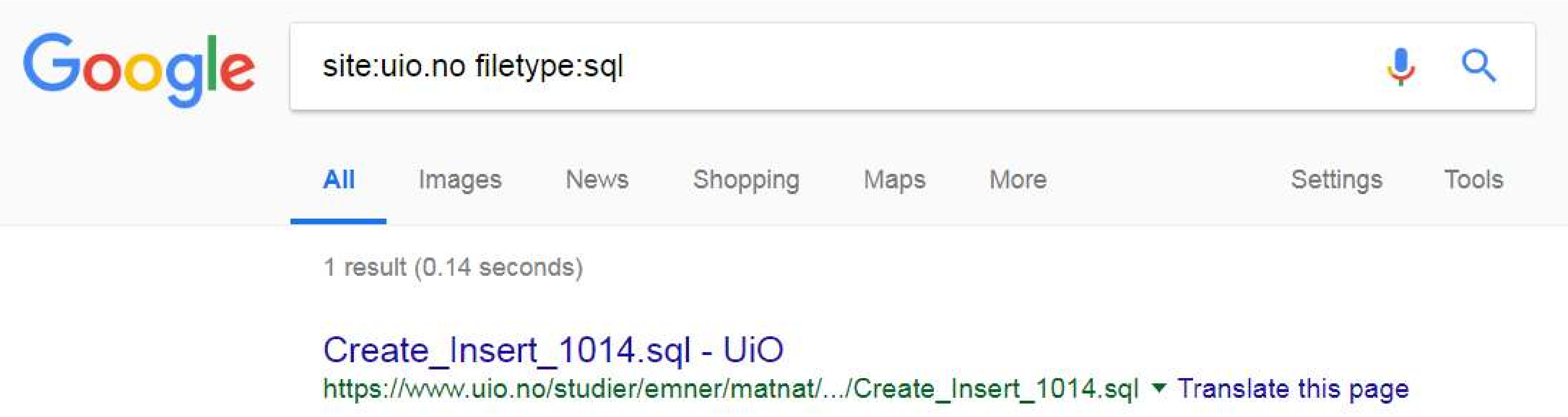
Det matematisk-naturvitenskapelige fakultet: Forside
https://www.mn.uio.no/ ▾ Translate this page
Norges største realfaglige forskning- og utdanningsinstitusjon innen astrofysikk, biologi, farmasi, fysikk, geologi, informatikk, kjemi, matematikk og molekylær ...

Kulturhistorisk museum: Forsiden
https://www.khm.uio.no/ ▾ Translate this page
Et forskningsmuseum som består av Vikingskipshuset og Historisk museum i Oslo. Arkeologi, etnografi, numismatikk, universitetshistorie, konservering.

Det teologiske fakultet: Forside
https://www.tf.uio.no/ ▾ Translate this page
TF driver forskning og undervisning innenfor teologi, kristendom, interreligiøse studier og diakonivitenskap.

# 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

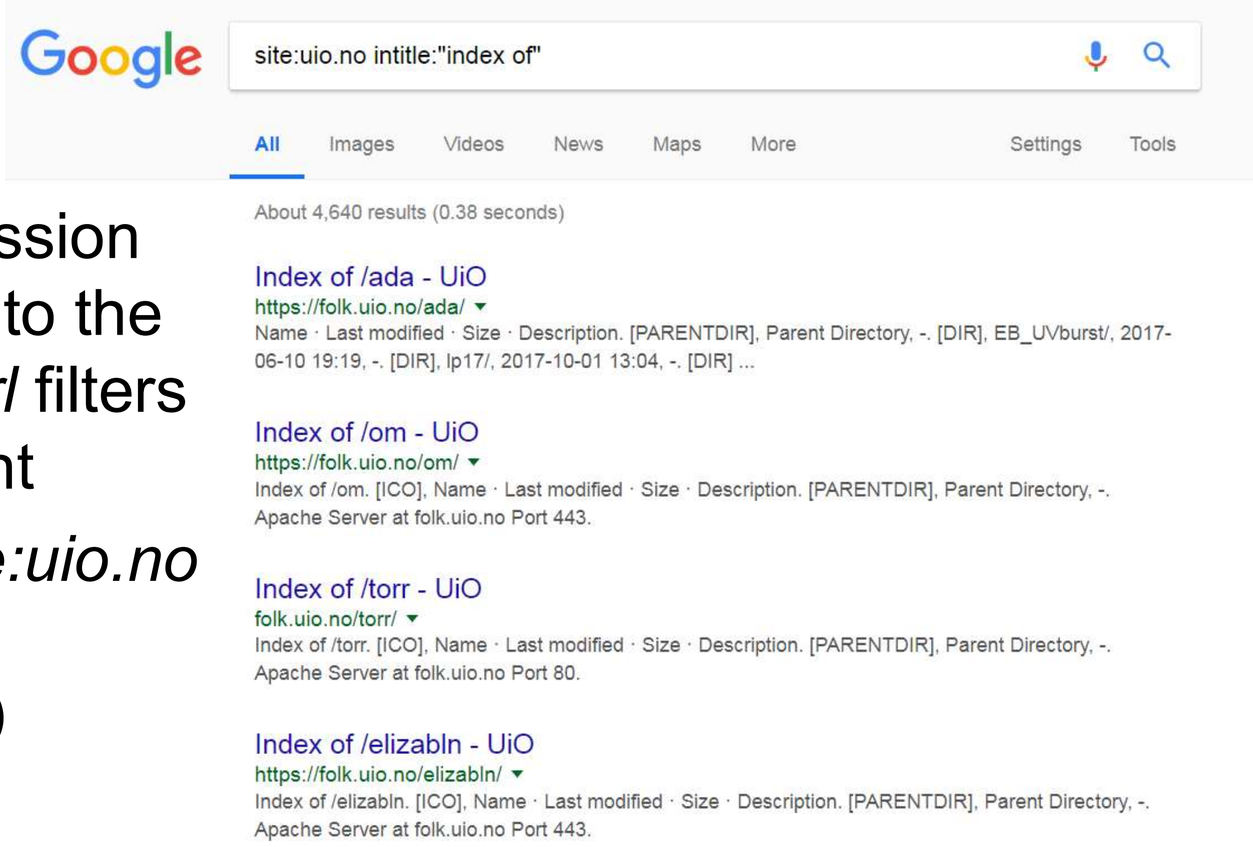


site:uio.no filetype:sql

1 result (0.14 seconds)

Create_Insert_1014.sql - UiO
https://www.uio.no/studier/emner/matnat/.../Create_Insert_1014.sql ▾ Translate this page

# Information gathering with Google hacking



site:uio.no intitle:"index of"

About 4,640 results (0.38 seconds)

Index of /ada - UiO
https://folk.uio.no/ada/
Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [DIR], EB_UVburst/, 2017-06-10 19:19, -. [DIR], lp17/, 2017-10-01 13:04, -. [DIR] ...

Index of /om - UiO
https://folk.uio.no/om/
Index of /om. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 443.

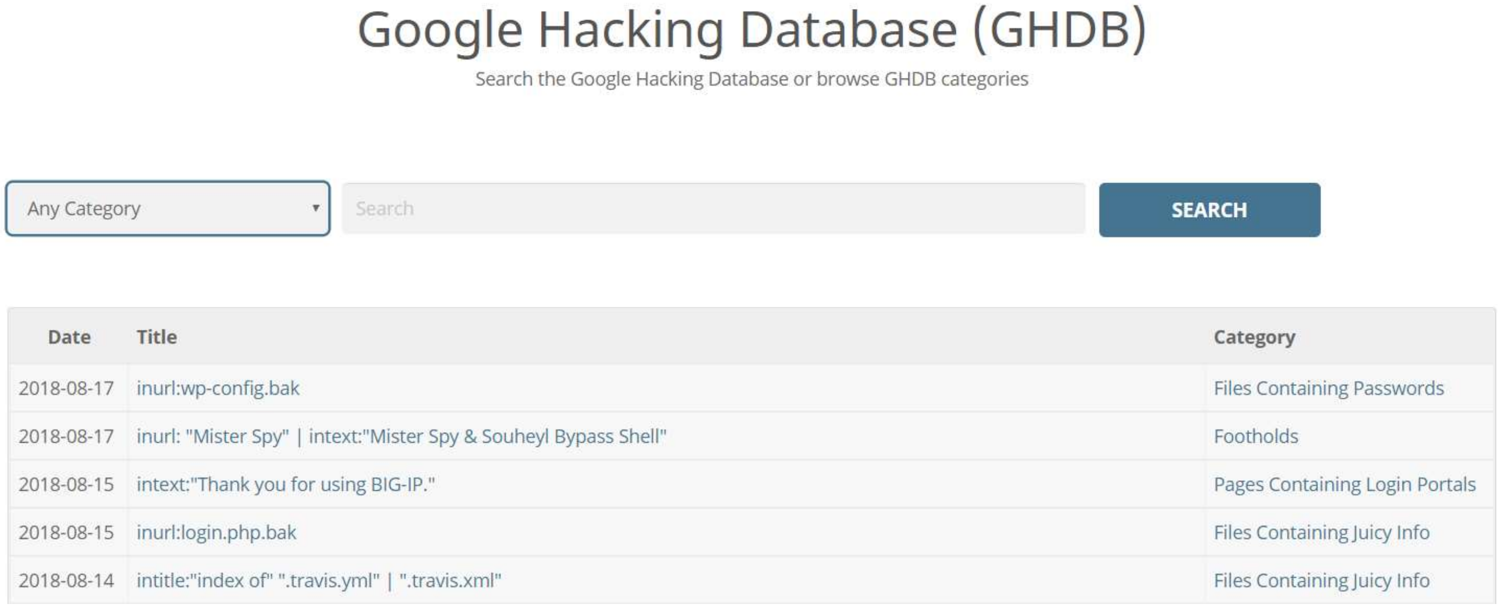
Index of /torr - UiO
folk.uio.no/torr/
Index of /torr. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 80.

Index of /elizabln - UiO
https://folk.uio.no/elizabln/
Index of /elizabln. [ICO], Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. Apache Server at folk.uio.no Port 443.

- 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)



Google Hacking Database (GHDB)

Search the Google Hacking Database or browse GHDB categories

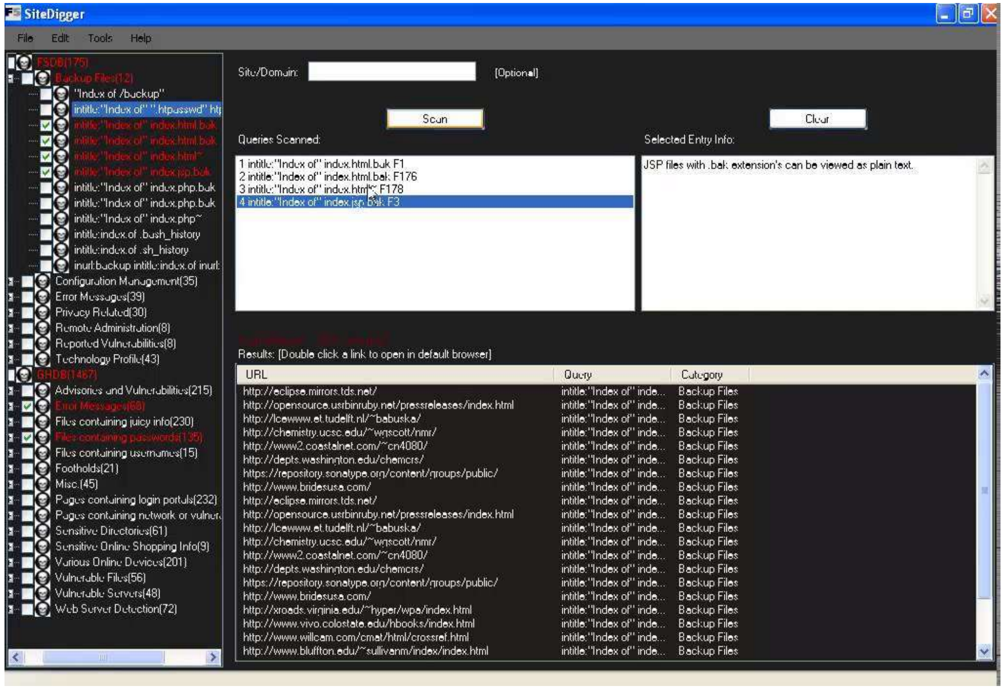
| Date | Title | Category |
|---|---|---|
| 2018-08-17 | inurl:wp-config.bak | Files Containing Passwords |
| 2018-08-17 | inurl: "Mister Spy" \| intext:"Mister Spy & Souheyl Bypass Shell" | Footholds |
| 2018-08-15 | intext:"Thank you for using BIG-IP." | Pages Containing Login Portals |
| 2018-08-15 | inurl:login.php.bak | Files Containing Juicy Info |
| 2018-08-14 | intitle:"index of" ".travis.yml" \| ".travis.xml" | Files Containing Juicy Info |

# 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 …**



- ☐ FSDB(175)
  - ☐ Backup Files(12)
    - ☐ "Index of /backup"
    - ☐ intitle:"Index of" ".htpasswd" htp
    - ☑ intitle:"Index of" index.html.bak
    - ☑ intitle:"Index of" index.html.bak
    - ☑ intitle:"Index of" index.html~
    - ☑ intitle:"Index of" index.jsp.bak
    - ☐ intitle:"Index of" index.php.bak
    - ☐ intitle:"Index of" index.php.bak
    - ☐ intitle:"Index of" index.php~
    - ☐ intitle:index.of .bash_history
    - ☐ intitle:index.of .sh_history
    - ☐ inurl:backup intitle:index.of inurl:
  - ☐ Configuration Management(35)
  - ☐ Error Messages(39)
  - ☐ Privacy Related(30)
  - ☐ Remote Administration(8)
  - ☐ Reported Vulnerabilities(8)
  - ☐ Technology Profile(43)
- ☐ GHDB(1467)
  - ☐ Advisories and Vulnerabilities(215)
  - ☑ Error Messages(68)
  - ☐ Files containing juicy info(230)
  - ☑ Files containing passwords(135)
  - ☐ Files containing usernames(15)
  - ☐ Footholds(21)
  - ☐ Misc.(45)
  - ☐ Pages containing login portals(232)
  - ☐ Pages containing network or vulner
  - ☐ Sensitive Directories(61)
  - ☐ Sensitive Online Shopping Info(9)
  - ☐ Various Online Devices(201)
  - ☐ Vulnerable Files(56)
  - ☐ Vulnerable Servers(48)
  - ☐ Web Server Detection(72)

Site/Domain: [Optional]

Queries Scanned:

```
1 intitle:"Index of" index.html.bak F1
2 intitle:"Index of" index.html.bak F176
3 intitle:"Index of" index.html~ F178
4 intitle:"Index of" index.jsp.bak F3
```

Selected Entry Info:

JSP files with .bak extension's can be viewed as plain text.

Results: [Double click a link to open in default browser]

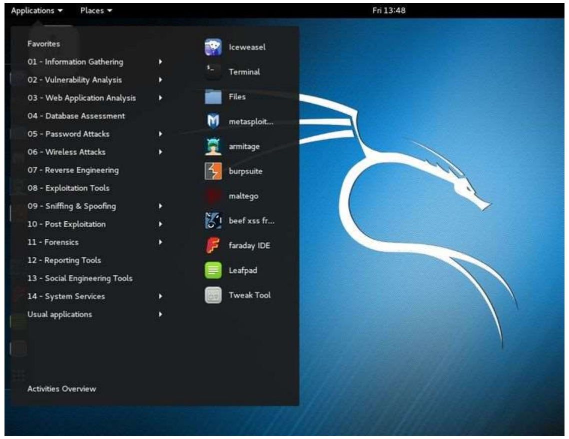
| URL | Query | Category |
|---|---|---|
| http://eclipse.mirrors.tds.net/ | intitle:"Index of" inde... | Backup Files |
| http://opensource.usrbinruby.net/pressreleases/index.html | intitle:"Index of" inde... | Backup Files |
| http://lcewww.et.tudelft.nl/~babuska/ | intitle:"Index of" inde... | Backup Files |
| http://chemistry.ucsc.edu/~wgscott/nmr/ | intitle:"Index of" inde... | Backup Files |
| http://www2.coastalnet.com/~cn4080/ | intitle:"Index of" inde... | Backup Files |
| http://depts.washington.edu/chemcrs/ | intitle:"Index of" inde... | Backup Files |
| https://repository.sonatype.org/content/groups/public/ | intitle:"Index of" inde... | Backup Files |
| http://www.bridesusa.com/ | intitle:"Index of" inde... | Backup Files |
| http://eclipse.mirrors.tds.net/ | intitle:"Index of" inde... | Backup Files |
| http://opensource.usrbinruby.net/pressreleases/index.html | intitle:"Index of" inde... | Backup Files |
| http://lcewww.et.tudelft.nl/~babuska/ | intitle:"Index of" inde... | Backup Files |
| http://chemistry.ucsc.edu/~wgscott/nmr/ | intitle:"Index of" inde... | Backup Files |
| http://www2.coastalnet.com/~cn4080/ | intitle:"Index of" inde... | Backup Files |
| http://depts.washington.edu/chemcrs/ | intitle:"Index of" inde... | Backup Files |
| https://repository.sonatype.org/content/groups/public/ | intitle:"Index of" inde... | Backup Files |
| http://www.bridesusa.com/ | intitle:"Index of" inde... | Backup Files |
| http://xroads.virginia.edu/~hyper/wpa/index.html | intitle:"Index of" inde... | Backup Files |
| http://www.vivo.colostate.edu/hbooks/index.html | intitle:"Index of" inde... | Backup Files |
| http://www.willcam.com/cmat/html/crossref.html | intitle:"Index of" inde... | Backup Files |
| http://www.bluffton.edu/~sullivanm/index/index.html | intitle:"Index of" inde... | Backup Files |

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

**Kali Linux ([http://kali.org](http://kali.org))**

KALI
BY OFFENSIVE SECURITY

- 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