Prof. Dr. A. Raab-Düsterhöft, Hochschule Wismar
Bachelor „IT-Forensik“

Modul „Informationsrecherche im Internet“

Alternative Praktikumsaufgabe 29.3.2019

Thema: Auskundschaften von Informationen

Gruppe MUE6

Oliver Dzombic, Tobias Stauder, Florian Weijers

„Ein gut vorbereiteter Hacker verbringt ca. 90 Prozent seines Aufwands mit der Erstellungeines Sicherheitsprofils (Footprinting). Nur ca. 10 Prozent seines Aufwands wendet er fürdie eigentliche Ausführung des Angriffs auf.....Bei der Erstellung eines Sicherheitsprofils helfen die folgenden Werkzeuge:-Per DNS-Report oder whois-Abfrage können die öffentlichen Nameserver im Internetüber die Domänen des Unternehmens befragt werden.-Mit Hilfe eines Web-Crawlers kann die gesamte Web-Site eines Unternehmens gespiegeltwerden. Anschließend wird auf der lokalen Kopie recherchiert (insbesondere inden Kommentaren und Meta-Tags der HTML-Seiten).-Per Google-Hacking: Geschickt formulierte Suchabfragen liefern vielfältige Informationenüber Betriebssysteme, Datenbanken, Web-Server, E-Mail-Adressen und vielem mehr....Hacker suchen via Googlenach-Betriebssystemen, Datenbanken, Web-Server, E-Mail-Adressen-Login-Seiten-Benutzernamen und Passwörtern-Backups und temporären Dateien-Fehlermeldungen von Web-Servern, Datenbanken und Programmiersprachen-nach Konfigurationsdateien-nach Office-Dokumenten (deren Eigenschaften nützliche Informationen wie bspw.interne Accountnamen enthalten können)und vielem mehr. Üblicherweise werden solche Recherchen nicht manuell, sondern mitHilfeautomatisierter Tools durchgeführt.“

Aus: Manu Carus„Ethical Hacking–Strategien für Ihre Sicherheit“, Software & Support Verlag GmbHentwickler.press, 2008, S.78 ff.Das Buch wird u.a. im Studiengang „IT-Forensik“im Modul „Ethical Hacking“genutzt.

Aufgabenstellung:

1. Wählen Sie eine Institution, ein Unternehmen, ein Verein, ein Shop oder ähnliches!

2. Recherchieren Sie im Internet nach aktuellen Werkzeugen, mit denen man Footprinting-Recherchen durchführen kann! Dokumentieren Sie die gefundenen Tools und nutzen Sie diese anhand einer Beispiel-Domain.Listen Sie alle Informationen auf, die Sie über das Unternehmen, die Institution, etc. gefunden haben.

3. Formulieren Sie Google-Abfragen, die oben genannte Informationen bzgl. des Unternehmens, der Institution, etc. (versuchen zu) liefern! Dokumentieren Sie diese!

4. Recherchieren Sie im Dark web, welche Informationen Sie zu dem Unternehmen, der Institution, etc. gefunden haben. Installieren Sie einen TOR-Browser, um eine Dark Web-Suche durchzuführen.

5. Dokumentieren Sie Ihr Vorgehen im Dark Web und die gefundenen Informationen!

zu 1. Auswahl des Zieles der Recherche.

Nach Überlegungen und Recherchen im Internet nach relevanten Seiten wurde eine zufällige Seite mit nicht besonderem öffentlichen Interesse gewählt.
Ziel der Recherche war die allgemeine Analyse der Seite als Institution im Internet.
Der Name “Sauf.ca” begründet sich aus dem französischen und bedeutet etwa “ausser, dass” oder “ausserdem”. Die Seite wird augenscheinlich von jungem Publikum besucht, um dort gespeicherte Videos o.ä. anzusehen. Im überschlagenen Sinne handelt es sich um eine Art kleineres Youtube.
Bei den Videos handelt es sich teilweise um Spaßvideos, Gewaltvideos und Pornografie.

2. Footprinting-Recherche

A)

Wir prüfen zunächst die Ergebnisse, welche die DNS Server zum Untersuchsziel liefern und benutzen hierbei das Standardprogramm dig:

dig +nocmd sauf.ca any +multiline +answer

```
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60830
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;sauf.ca.            IN ANY

;; ANSWER SECTION:
sauf.ca.            4445 IN     A 176.9.123.245

;; Query time: 15 msec
;; SERVER: 192.168.178.1#53(192.168.178.1)
;; WHEN: Thu Jun 20 12:14:47 CEST 2019
;; MSG SIZE  rcvd: 52
```

Wie wir sehen, ist die DNS Zone nicht sehr spektakulär. Es sind lediglich zwei Einträge vorhanden.

Sauf.ca IN ANY bedeutet, dass ein sog. Wildcard für sauf.ca gesetzt wurde. Das bedeutet, dass man eine beliebige subdomain beliebiger Dimension (also auch ein sub3.sub2.sub1.sauf.ca) ansprechen kann und man immer bei der für sauf.ca eingetragenen IP Adresse landet.

Und diese ist durch einen A Record auf 176.9.123.245 gesetzt worden:

sauf.ca IN A 176.9.123.245

Die Zahl 4445 gibt die TTL (Time To Live) des Records an. Also wie lange dieser gültig ist.

B)

Wir prüfen über eine schnelle Traceroute welcher Provider das Untersuchungsziel hostet:

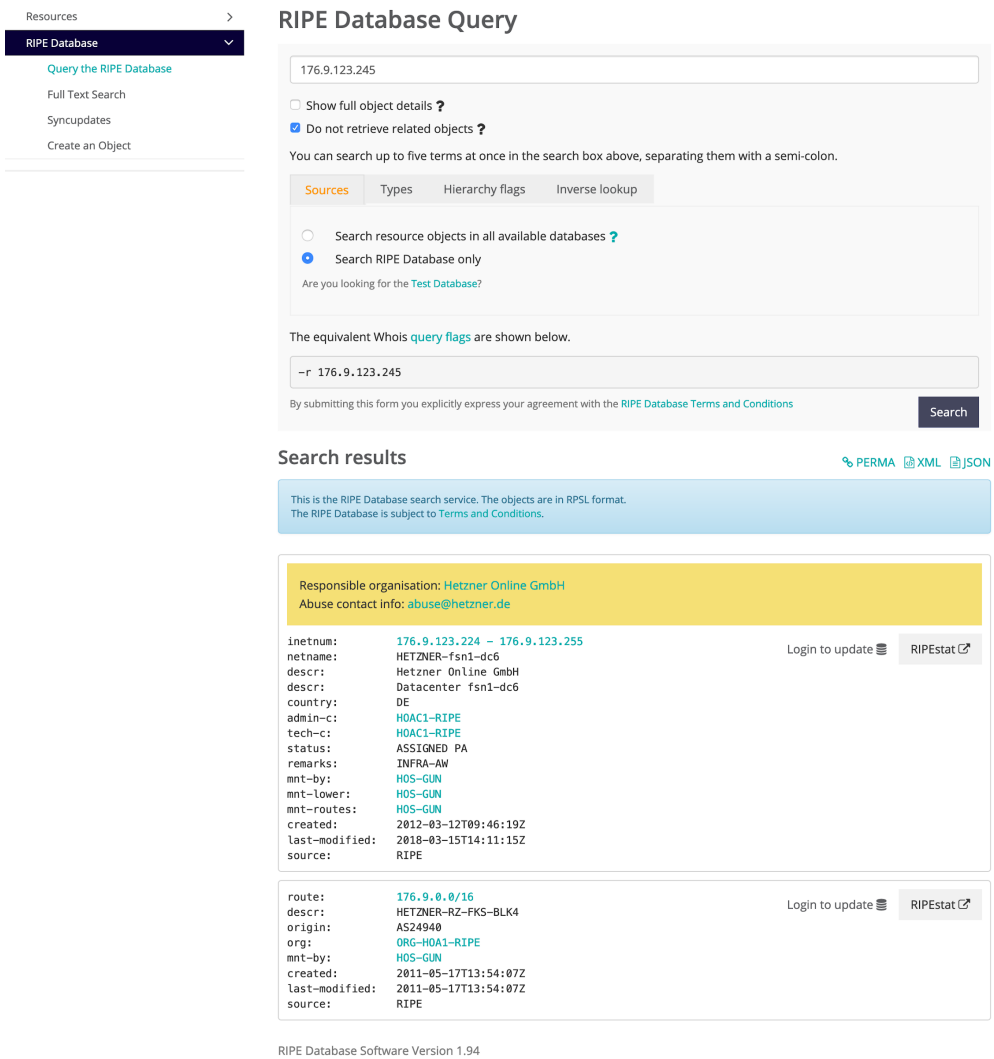
```
traceroute to sauf.ca (176.9.123.245), 64 hops max, 52 byte packets
 1  fritz.box (192.168.178.1)  3.924 ms  3.531 ms  3.712 ms
 2  host-62-245-142-149.customer.m-online.net (62.245.142.149)  12.467 ms  12.501 ms  12.809
ms
```

3 host-62-245-142-148.customer.m-online.net (62.245.142.148) 12.878 ms 79.832 ms 63.696 ms
4 xe-2-0-0.r5.nue1.m-online.net (212.18.6.77) 12.639 ms
xe-2-0-1.r5.nue1.m-online.net (212.18.6.79) 19.692 ms 14.034 ms
5 nix-gw.hetzner.de (195.85.217.16) 14.318 ms 12.614 ms 14.708 ms
6 core22.fsn1.hetzner.com (213.239.252.242) 15.477 ms
core21.fsn1.hetzner.com (213.239.252.238) 15.417 ms
core22.fsn1.hetzner.com (213.239.252.242) 16.793 ms
7 ex9k2.dc6.fsn1.hetzner.com (213.239.229.82) 15.225 ms 17.943 ms
ex9k2.dc6.fsn1.hetzner.com (213.239.229.86) 16.029 ms
8 triphasia.seos.fr (176.9.123.245) 17.258 ms 17.213 ms 17.024 ms

Recht unspektakulär kommen wir bei Hetzner, einem deutschen Massenhoster heraus.

C)

Wir machen einen schnellen Gegencheck auf die IP des Untersuchungsziels (176.9.123.245) über die RIPE Datenbank, welche in Europa und dem mittleren Osten für die Vergabe der Internet Adressen offiziell zuständig ist:



Das Suchergebnis wird also auch von der RIPE Datenbank gestützt und wir können nunmehr davon ausgehen, dass der Server von Hetzner gehostet wird.

Darüber hinaus können wir davon ausgehen, dass der Server in Deutschland gehostet wird. Dies können wir mit sehr hoher Sicherheit auf Basis der gemessenen Latenzen der Hops in der Traceroute bestimmen.

So starten wir im 1. Hop (fritz.box) in unserem eigenen Netz und gehen im 2. Hop (host-62-245-142-149.customer.m-online.net) auf unseren eigenen Internetprovider.

Wie wir sehen springt die Latenz, die die IP Pakete haben von etwa 3.5ms auf 12.5ms beim Sprung von unserem LAN in das WAN (dem Internet in dem Fall).

Die Latenzen werden bis zum Endziel (unserem Untersuchungsziel) nur um 5ms größer. Damit muss sich das Ziel, falls nicht besondere Proxy/Puffermethoden angewandt werden, in Deutschland befinden. Andernfalls wären die Latenzen deutlich höher.

Exemplarisch bei einer Traceroute auf wien.at ist zu sehen, dass die Latenzen klar den Übergang von Deutschland nach Österreich zeigen:

```
 4  et-5-0-0.rt-decix-2.m-online.net (82.135.16.137)  15.448 ms  16.727 ms  15.988 ms
 5  decix-aon.highway.telekom.at (80.81.192.69)  20.566 ms  16.425 ms  18.076 ms
 6  lg1-9073.as8447.a1.net (195.3.64.1)  26.602 ms  27.400 ms  31.282 ms
```

Die Latenzen springen auf rund das Doppelte.

D)

Zum Schluss werfen wir noch einen kurzen Blick auf den Server des Untersuchungsziels selbst. Hierbei können wir ggf. herausfinden, welche Ports geöffnet sind und erhalten ggf. sogar Versionsnummern sowie die für den jeweiligen Dienst eingesetzte Softwarepakete.

Wir benutzen hierbei das Standardprogramm nmap:

```
# nmap -sV -v -sS -p1-65535 sauf.ca

Starting Nmap 6.40 ( http://nmap.org ) at 2019-06-20 11:44 CEST
NSE: Loaded 23 scripts for scanning.
Initiating Ping Scan at 11:44
Scanning sauf.ca (176.9.123.245) [4 ports]
Completed Ping Scan at 11:44, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:44
Completed Parallel DNS resolution of 1 host. at 11:44, 0.03s elapsed
Initiating SYN Stealth Scan at 11:44
Scanning sauf.ca (176.9.123.245) [65535 ports]
Discovered open port 443/tcp on 176.9.123.245
Discovered open port 80/tcp on 176.9.123.245
Discovered open port 22/tcp on 176.9.123.245
Completed SYN Stealth Scan at 11:44, 4.84s elapsed (65535 total ports)
```

```
Initiating Service scan at 11:44
Scanning 3 services on sauf.ca (176.9.123.245)
Completed Service scan at 11:44, 12.10s elapsed (3 services on 1 host)
NSE: Script scanning 176.9.123.245.
Nmap scan report for sauf.ca (176.9.123.245)
Host is up (0.0056s latency).
rDNS record for 176.9.123.245: triphasia.seos.fr
Not shown: 65532 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 7.9 (protocol 2.0)
80/tcp  open  http     Apache httpd 2.4.38 ((Unix) OpenSSL/1.1.1b)
443/tcp open  ssl/http Apache httpd 2.4.38 ((Unix) OpenSSL/1.1.1b)
```

Wir können nun erkennen, dass die Ports 22 (ssh), 80 (http) und 443 (https) geöffnet ist. Außerdem erhalten wir die jeweiligen Softwarepakete und Versionsnummern.

In diesem Fall kommt ein Apache Webserver in der Version 2.4.38 als Linux/Unix Version mit einkompiliertem OpenSSL Version 1.1.1b für die Ports 80 und 443 zum Einsatz.

Des weiteren kommt ein OpenSSH 7.9 Server in der Version 7.9 zum Einsatz, welcher die Protokollnummer 2.0 als Verbindung anbietet.

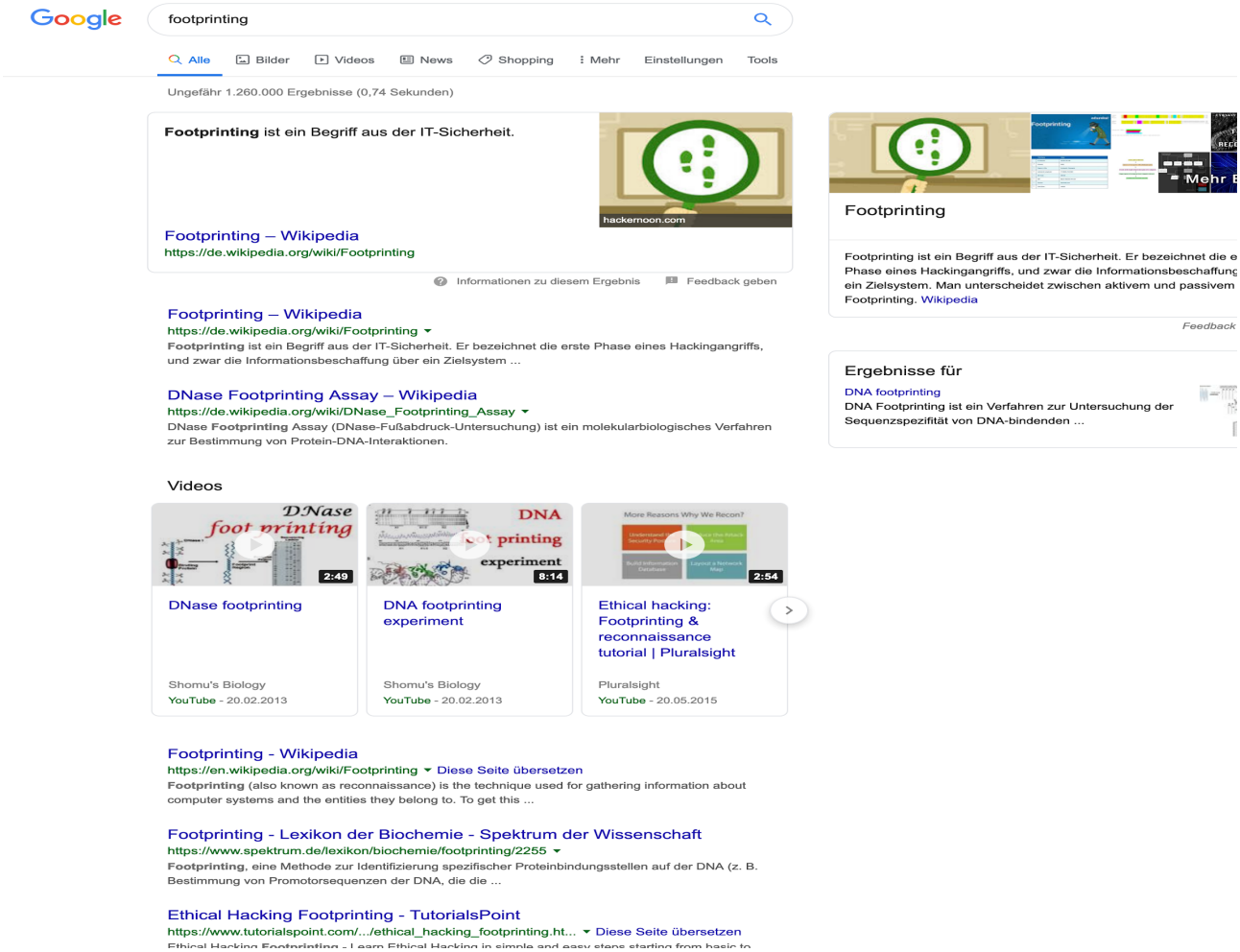
Im nächsten Schritt würde man nun in die öffentlich zugänglichen Bugreports reinschauen um zu prüfen ob die ein oder andere eingesetzte Version ggf. einen Bug hat, welcher ausgenutzt werden könnte um eigenen Code auf dem fremden System von außen zur Ausführung zu bringen (Hacking).

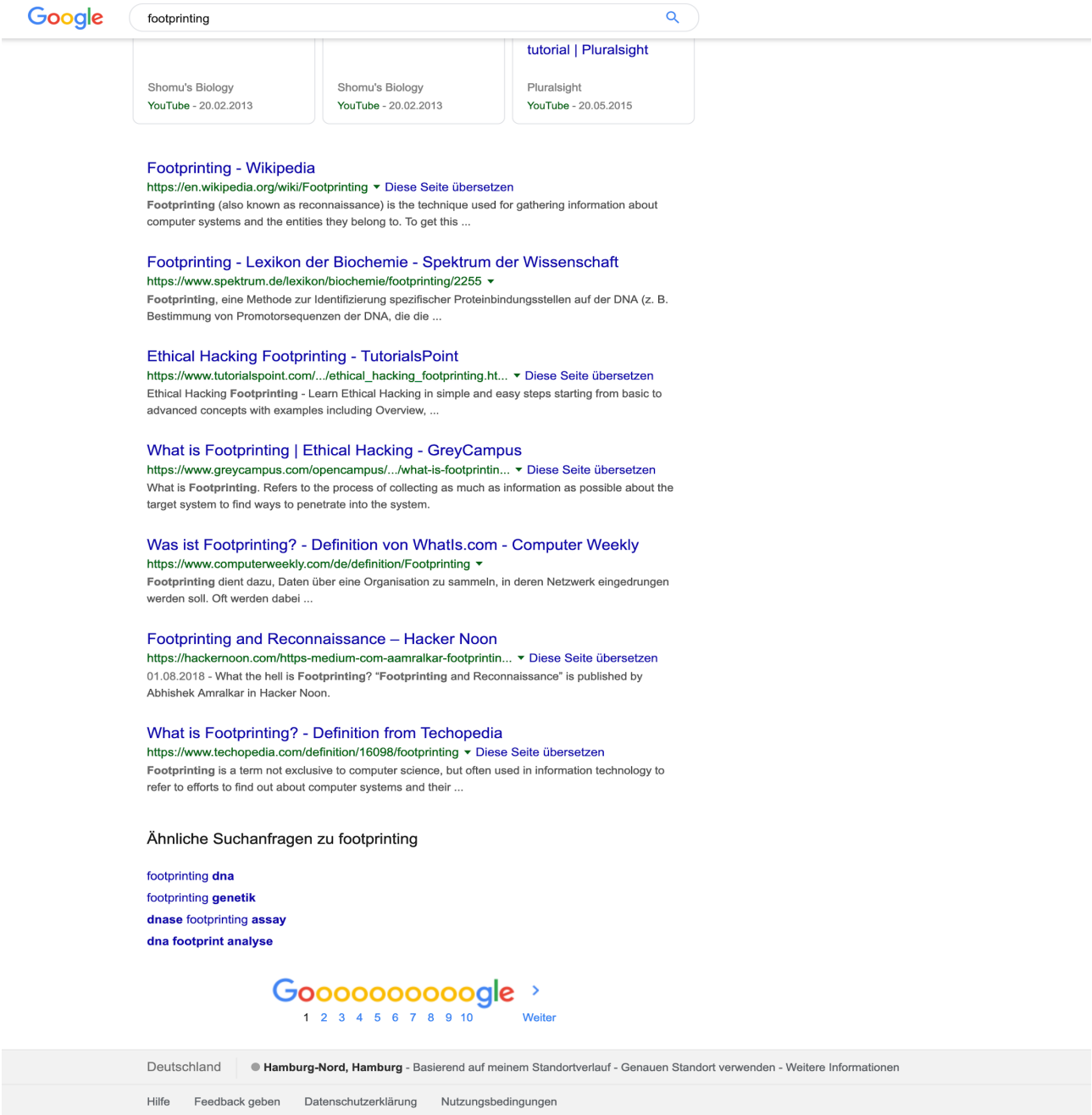
Hierbei darf man aber nicht vergessen, dass die gezeigten Informationen nicht zwangsläufig korrekt sein müssen.
Entsprechendes Knowhow und/oder kriminelle Energie vorausgesetzt, könnte man die jeweiligen Serverdienste auch selbst kompilieren und dabei falsche Informationen eintragen mit welchen sich der jeweilige Dienst dann nach außen identifiziert.

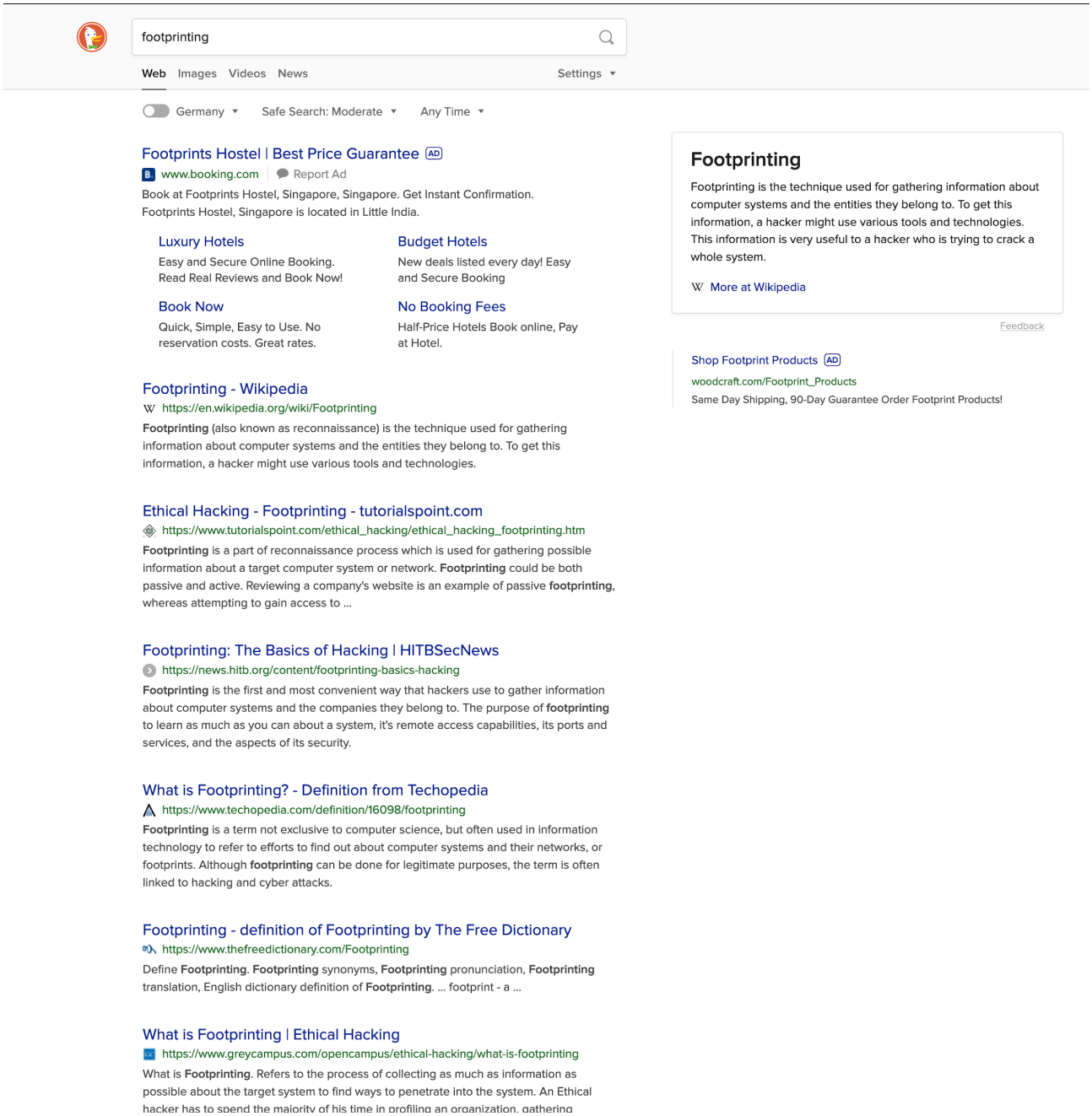
E)

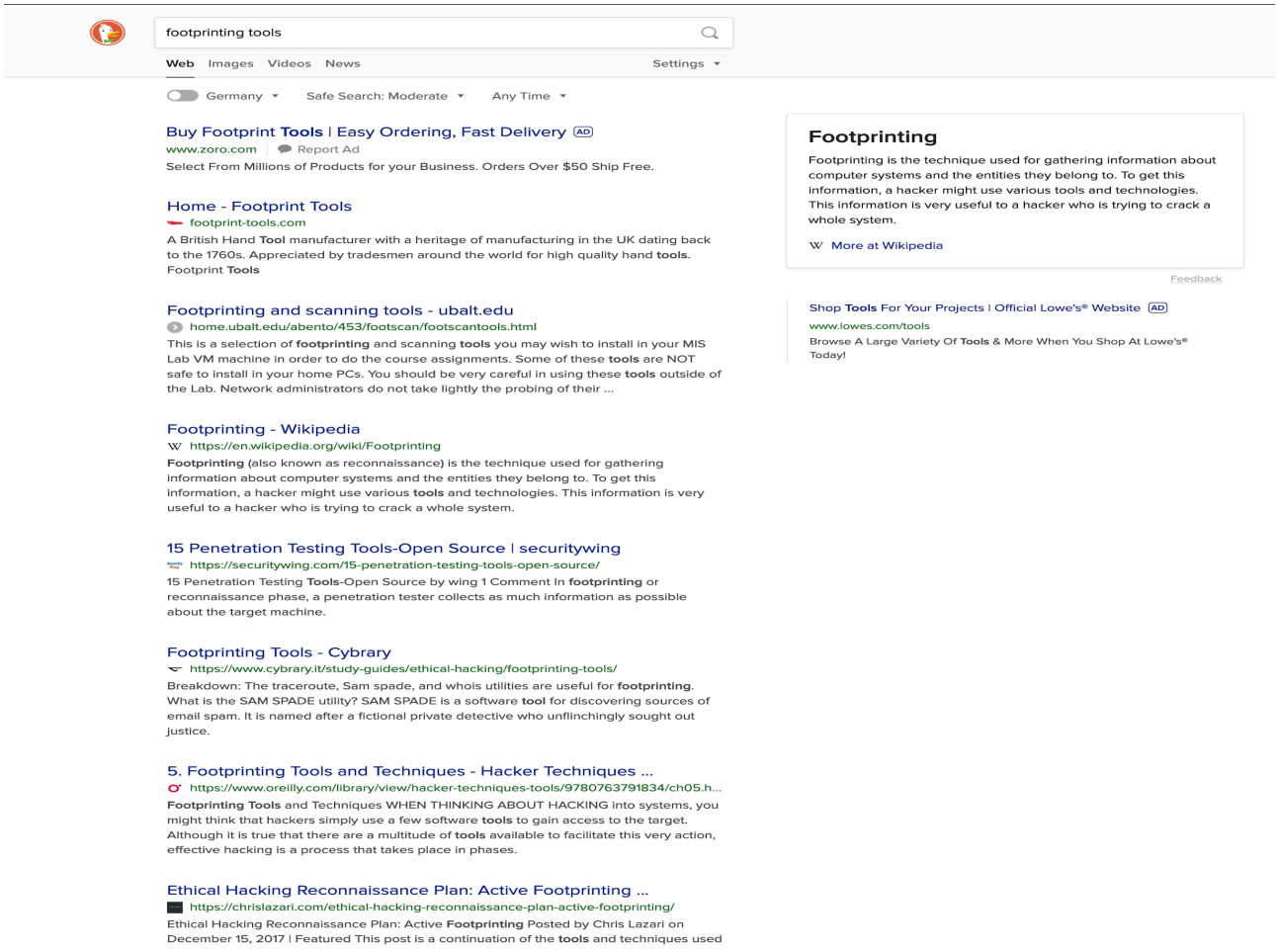
Nun widmen wir uns dem Thema Footprinting und befragen die Suchmaschinen zu diesem Thema.
Hierbei sollte man neben den (sehr offensiven) kommerziellen Suchmaschinen wie Google, Yahoo und Bing immer auch nicht kommerzielle Suchmaschinen befragen.
Aus den Erfahrungen des Autors heraus manipulieren die kommerziellen Suchmaschinen das Suchergebnis in vielen Fällen in eine von der jeweiligen Suchmaschine gewollten Richtung. Dies kann dann auch durchaus über das normale Maß der Fluktuation der Suchmaschinenergebnisse durch unterschiedliche Algorithmen hinausgehen.

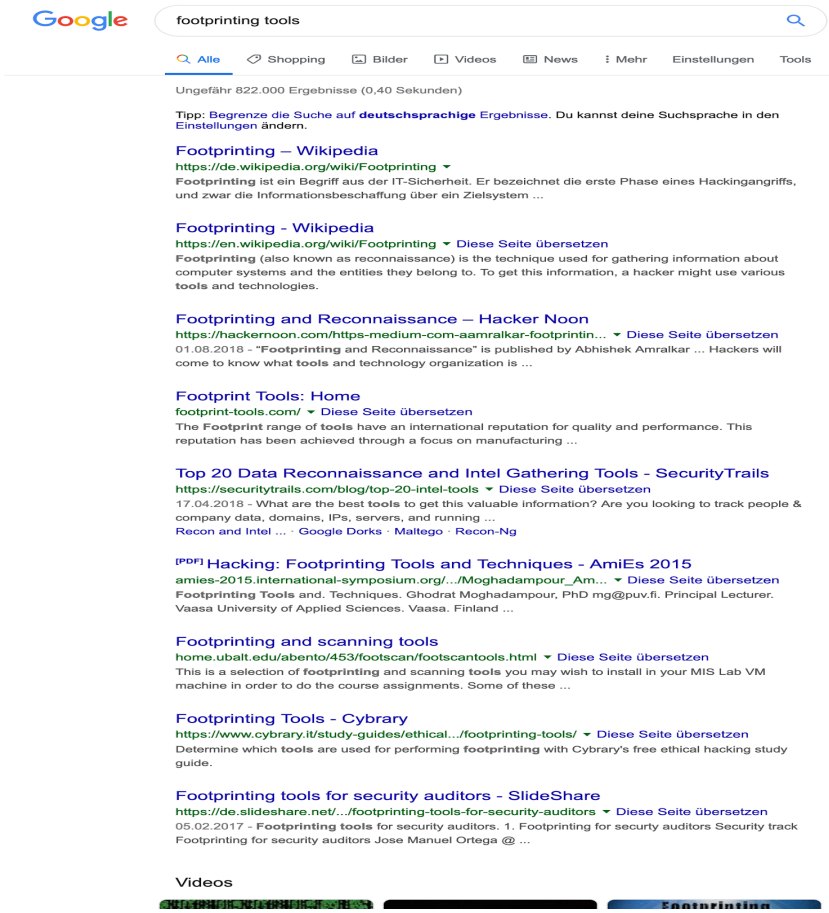
Exemplarisch soll hier der Vergleich zwischen Google und DuckDuckGo, bei unterschiedlichen Suchworten skizziert werden:




Google
footprinting
tutorial | Pluralsight
Shomu's Biology
YouTube - 20.02.2013
Shomu's Biology
YouTube - 20.02.2013
Pluralsight
YouTube - 20.05.2015
Footprinting - Wikipedia
https://en.wikipedia.org/wiki/Footprinting Diese Seite übersetzen
Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this ...
Footprinting - Lexikon der Biochemie - Spektrum der Wissenschaft
https://www.spektrum.de/lexikon/biochemie/footprinting/2255
Footprinting, eine Methode zur Identifizierung spezifischer Proteinbindungsstellen auf der DNA (z. B. Bestimmung von Promotorsequenzen der DNA, die die ...
Ethical Hacking Footprinting - TutorialsPoint
https://www.tutorialspoint.com/.../ethical_hacking_footprinting.ht... Diese Seite übersetzen
Ethical Hacking Footprinting - Learn Ethical Hacking in simple and easy steps starting from basic to advanced concepts with examples including Overview, ...
What is Footprinting | Ethical Hacking - GreyCampus
https://www.greycampus.com/opencampus/.../what-is-footprintin... Diese Seite übersetzen
What is Footprinting. Refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system.
Was ist Footprinting? - Definition von WhatIs.com - Computer Weekly
https://www.computerweekly.com/de/definition/Footprinting
Footprinting dient dazu, Daten über eine Organisation zu sammeln, in deren Netzwerk eingedrungen werden soll. Oft werden dabei ...
Footprinting and Reconnaissance – Hacker Noon
https://hackernoon.com/https-medium-com-aamralkar-footprintin... Diese Seite übersetzen
01.08.2018 - What the hell is Footprinting? “Footprinting and Reconnaissance” is published by Abhishek Amralkar in Hacker Noon.
What is Footprinting? - Definition from Techopedia
https://www.techopedia.com/definition/16098/footprinting Diese Seite übersetzen
Footprinting is a term not exclusive to computer science, but often used in information technology to refer to efforts to find out about computer systems and their ...
Ähnliche Suchanfragen zu footprinting
footprinting dna
footprinting genetik
dnase footprinting assay
dna footprint analyse
Goooooooooogle
1 2 3 4 5 6 7 8 9 10 Weiter
Deutschland Hamburg-Nord, Hamburg - Basierend auf meinem Standortverlauf - Genauen Standort verwenden - Weitere Informationen
Hilfe Feedback geben Datenschutzerklärung Nutzungsbedingungen


footprinting
Web Images Videos News Settings
Germany Safe Search: Moderate Any Time
Footprints Hostel | Best Price Guarantee AD
www.booking.com Report Ad
Book at Footprints Hostel, Singapore, Singapore. Get Instant Confirmation. Footprints Hostel, Singapore is located in Little India.
Luxury Hotels
Easy and Secure Online Booking. Read Real Reviews and Book Now!
Budget Hotels
New deals listed every day! Easy and Secure Booking
Book Now
Quick, Simple, Easy to Use. No reservation costs. Great rates.
No Booking Fees
Half-Price Hotels Book online, Pay at Hotel.
Footprinting - Wikipedia
https://en.wikipedia.org/wiki/Footprinting
Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies.
Ethical Hacking - Footprinting - tutorialspoint.com
https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_footprinting.htm
Footprinting is a part of reconnaissance process which is used for gathering possible information about a target computer system or network. Footprinting could be both passive and active. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to ...
Footprinting: The Basics of Hacking | HITBSecNews
https://news.hitb.org/content/footprinting-basics-hacking
Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of footprinting to learn as much as you can about a system, it's remote access capabilities, its ports and services, and the aspects of its security.
What is Footprinting? - Definition from Techopedia
https://www.techopedia.com/definition/16098/footprinting
Footprinting is a term not exclusive to computer science, but often used in information technology to refer to efforts to find out about computer systems and their networks, or footprints. Although footprinting can be done for legitimate purposes, the term is often linked to hacking and cyber attacks.
Footprinting - definition of Footprinting by The Free Dictionary
https://www.thefreedictionary.com/Footprinting
Define Footprinting. Footprinting synonyms, Footprinting pronunciation, Footprinting translation, English dictionary definition of Footprinting. ... footprint - a ...
What is Footprinting | Ethical Hacking
https://www.greycampus.com/opencampus/ethical-hacking/what-is-footprinting
What is Footprinting. Refers to the process of collecting as much as information as possible about the target system to find ways to penetrate into the system. An Ethical hacker has to spend the majority of his time in profiling an organization, gathering
Footprinting
Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.
More at Wikipedia
Feedback
Shop Footprint Products AD
woodcraft.com/Footprint_Products
Same Day Shipping, 90-Day Guarantee Order Footprint Products!


footprinting tools
Web Images Videos News Settings
Germany Safe Search: Moderate Any Time
Buy Footprint Tools | Easy Ordering, Fast Delivery AD
www.zoro.com Report Ad
Select From Millions of Products for your Business. Orders Over $50 Ship Free.
Home - Footprint Tools
footprint-tools.com
A British Hand Tool manufacturer with a heritage of manufacturing in the UK dating back to the 1760s. Appreciated by tradesmen around the world for high quality hand tools. Footprint Tools
Footprinting and scanning tools - ubalt.edu
home.ubalt.edu/abento/453/footscan/footscantools.html
This is a selection of footprinting and scanning tools you may wish to install in your MIS Lab VM machine in order to do the course assignments. Some of these tools are NOT safe to install in your home PCs. You should be very careful in using these tools outside of the Lab. Network administrators do not take lightly the probing of their ...
Footprinting - Wikipedia
https://en.wikipedia.org/wiki/Footprinting
Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.
15 Penetration Testing Tools-Open Source | securitywing
https://securitywing.com/15-penetration-testing-tools-open-source/
15 Penetration Testing Tools-Open Source by wing 1 Comment In footprinting or reconnaissance phase, a penetration tester collects as much information as possible about the target machine.
Footprinting Tools - Cybrary
https://www.cybrary.it/study-guides/ethical-hacking/footprinting-tools/
Breakdown: The traceroute, Sam spade, and whois utilities are useful for footprinting. What is the SAM SPADE utility? SAM SPADE is a software tool for discovering sources of email spam. It is named after a fictional private detective who unflinchingly sought out justice.
5. Footprinting Tools and Techniques - Hacker Techniques ...
https://www.oreilly.com/library/view/hacker-techniques-tools/9780763791834/ch05.h...
Footprinting Tools and Techniques WHEN THINKING ABOUT HACKING into systems, you might think that hackers simply use a few software tools to gain access to the target. Although it is true that there are a multitude of tools available to facilitate this very action, effective hacking is a process that takes place in phases.
Ethical Hacking Reconnaissance Plan: Active Footprinting ...
https://chrislazari.com/ethical-hacking-reconnaissance-plan-active-footprinting/
Ethical Hacking Reconnaissance Plan: Active Footprinting Posted by Chris Lazari on December 15, 2017 | Featured This post is a continuation of the tools and techniques used
Footprinting
Footprinting is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various tools and technologies. This information is very useful to a hacker who is trying to crack a whole system.
More at Wikipedia
Feedback
Shop Tools For Your Projects | Official Lowe's® Website AD
www.lowes.com/tools
Browse A Large Variety Of Tools & More When You Shop At Lowe's® Today!



Google

footprinting tools

Alle Shopping Bilder Videos News Mehr Einstellungen Tools

Ungefähr 822.000 Ergebnisse (0,40 Sekunden)

Tipp: Begrenze die Suche auf **deutschsprachige** Ergebnisse. Du kannst deine Suchsprache in den Einstellungen ändern.

Footprinting – Wikipedia
https://de.wikipedia.org/wiki/Footprinting
Footprinting ist ein Begriff aus der IT-Sicherheit. Er bezeichnet die erste Phase eines Hackingangriffs, und zwar die Informationsbeschaffung über ein Zielsystem ...

Footprinting - Wikipedia
https://en.wikipedia.org/wiki/Footprinting Diese Seite übersetzen
Footprinting (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a hacker might use various **tools** and technologies.

Footprinting and Reconnaissance – Hacker Noon
https://hackernoon.com/https-medium-com-aamralkar-footprintin... Diese Seite übersetzen
01.08.2018 - “**Footprinting** and Reconnaissance” is published by Abhishek Amralkar ... Hackers will come to know what **tools** and technology organization is ...

Footprint Tools: Home
footprint-tools.com/ Diese Seite übersetzen
The **Footprint** range of **tools** have an international reputation for quality and performance. This reputation has been achieved through a focus on manufacturing ...

Top 20 Data Reconnaissance and Intel Gathering Tools - SecurityTrails
https://securitytrails.com/blog/top-20-intel-tools Diese Seite übersetzen
17.04.2018 - What are the best **tools** to get this valuable information? Are you looking to track people & company data, domains, IPs, servers, and running ...
Recon and Intel ... · Google Dorks · Maltego · Recon-Ng

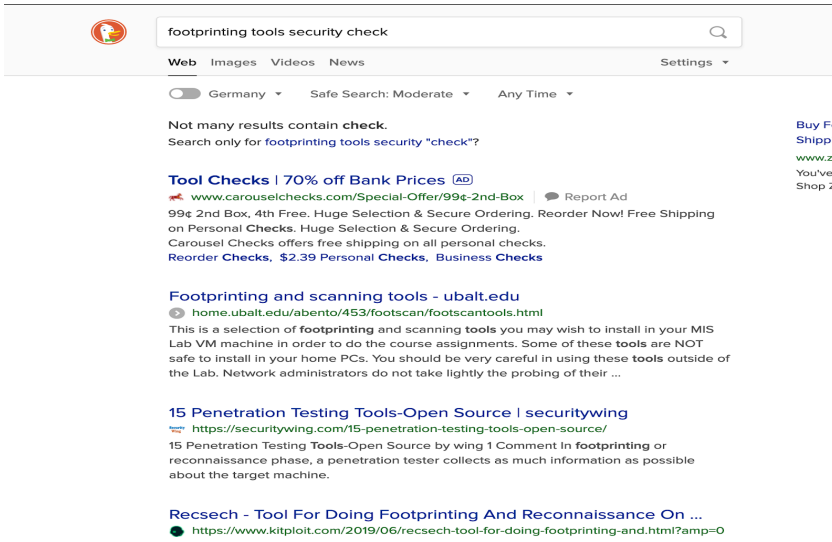
[PDF] Hacking: Footprinting Tools and Techniques - AmiEs 2015
amies-2015.international-symposium.org/.../Moghadampour_Am... Diese Seite übersetzen
Footprinting Tools and. Techniques. Ghodrat Moghadampour, PhD mg@puv.fi. Principal Lecturer. Vaasa University of Applied Sciences. Vaasa. Finland ...

Footprinting and scanning tools
home.ubalt.edu/abento/453/footscan/footscantools.html Diese Seite übersetzen
This is a selection of **footprinting** and scanning **tools** you may wish to install in your MIS Lab VM machine in order to do the course assignments. Some of these ...

Footprinting Tools - Cybrary
https://www.cybrary.it/study-guides/ethical.../footprinting-tools/ Diese Seite übersetzen
Determine which **tools** are used for performing **footprinting** with Cybrary's free ethical hacking study guide.

Footprinting tools for security auditors - SlideShare
https://de.slideshare.net/.../footprinting-tools-for-security-auditors Diese Seite übersetzen
05.02.2017 - **Footprinting tools** for security auditors. 1. Footprinting for securty auditors Security track Footprinting for security auditors Jose Manuel Ortega @ ...

Videos



footprinting tools security check

Web Images Videos News Settings

Germany Safe Search: Moderate Any Time

Not many results contain **check**.
Search only for footprinting tools security “check”?

Tool Checks | 70% off Bank Prices AD
www.carouselchecks.com/Special-Offer/99¢-2nd-Box Report Ad
99¢ 2nd Box, 4th Free. Huge Selection & Secure Ordering. Reorder Now! Free Shipping on Personal **Checks**. Huge Selection & Secure Ordering.
Carousel Checks offers free shipping on all personal checks.
Reorder **Checks**, $2.39 Personal **Checks**, Business **Checks**

Footprinting and scanning tools - ubalt.edu
home.ubalt.edu/abento/453/footscan/footscantools.html
This is a selection of **footprinting** and scanning **tools** you may wish to install in your MIS Lab VM machine in order to do the course assignments. Some of these **tools** are NOT safe to install in your home PCs. You should be very careful in using these **tools** outside of the Lab. Network administrators do not take lightly the probing of their ...

15 Penetration Testing Tools-Open Source | securitywing
https://securitywing.com/15-penetration-testing-tools-open-source/
15 Penetration Testing **Tools**-Open Source by wing 1 Comment In **footprinting** or reconnaissance phase, a penetration tester collects as much information as possible about the target machine.

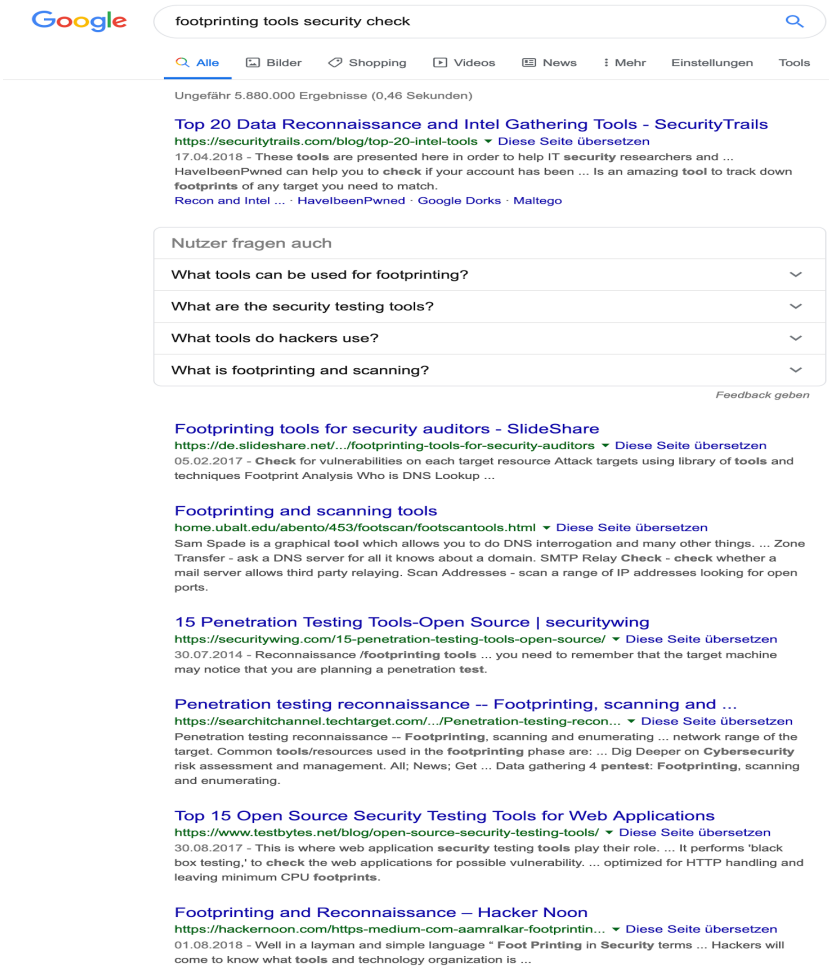
Recsech - Tool For Doing Footprinting And Reconnaissance On ...
https://www.kitploit.com/2019/06/recsech-tool-for-doing-footprinting-and.html?amp=0
Recsech is a **tool** for doing **Footprinting** and Reconnaissance on the target web. Recsech collects information such as DNS Information, Sub Domains, HoneySpot Detected, Subdomain takeovers, Reconnaissance On Github and much more you can see in Features in **tools** .

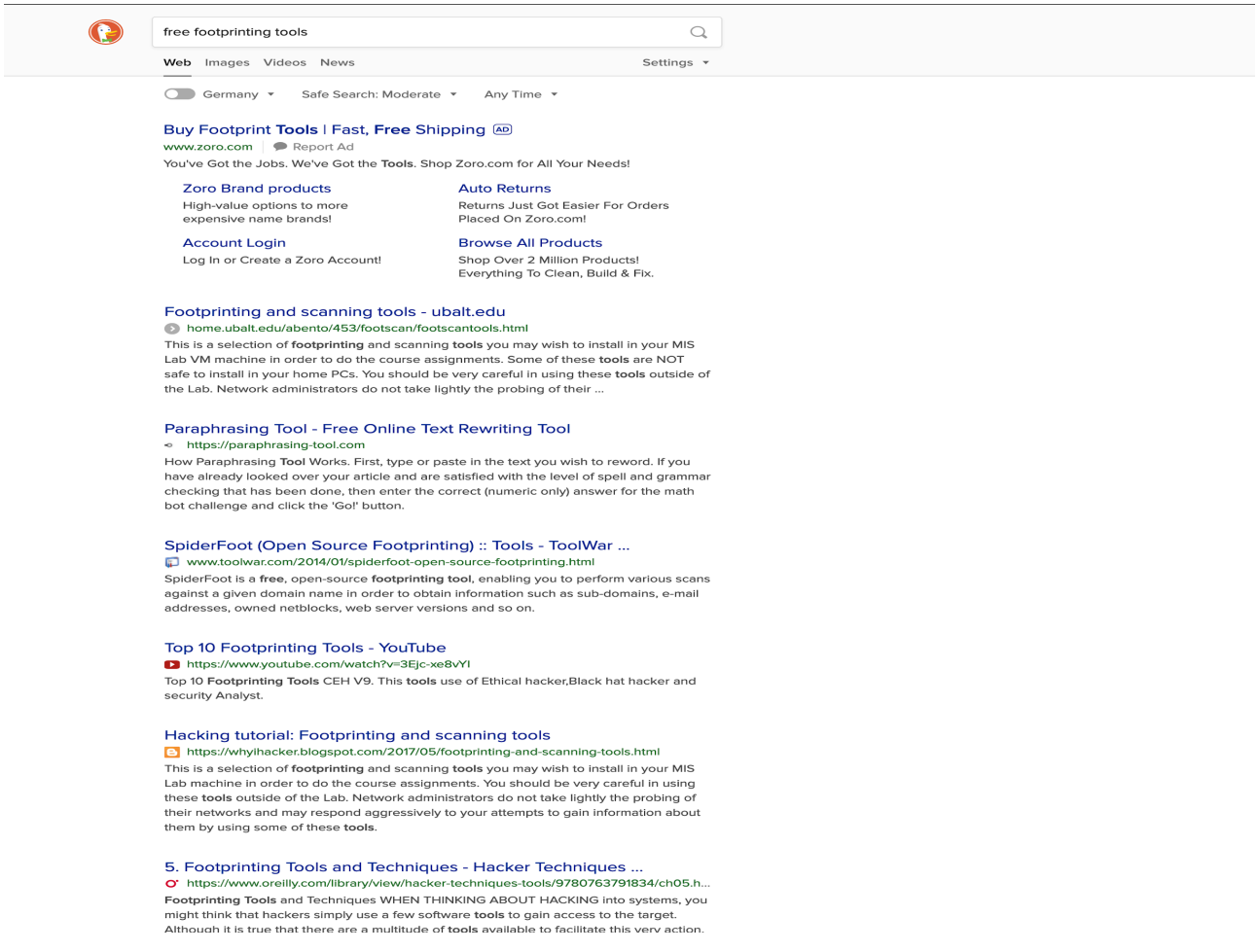
Footprinting: The Basics of Hacking | HITBSecNews
https://news.hitb.org/content/footprinting-basics-hacking
Footprinting is the first and most convenient way that hackers use to gather information about computer systems and the companies they belong to. The purpose of **footprinting** to learn as much as you can about a system, it's remote access capabilities, its ports and services, and the aspects of its **security**.

Footprinting Tools - Cybrary
https://www.cybrary.it/study-guides/ethical-hacking/footprinting-tools/
The **tool** itself can request a DNS server to send back details about a domain, scan IP addresses for open ports, find the route of a packet transmitting between a machine and a remote system, and guess the origin of emails from their headers.

Ethical Hacking Tools - resources.infosecinstitute.com
https://resources.infosecinstitute.com/category/certifications-training/ceh/ethical-hac...
Nmap (Network Mapper) is used to Scan Ports and Map Networks and its very well-known free open source hacker's **tool**. Namp is used by many **security** professionals around the world for network inventory, **check** for open ports, manage service upgrade schedules, and monitor host or service uptime

Buy Footprint **Tools** | Fast, Free Shipping AD
www.zoro.com
You've Got the Jobs. We've Got the **Tools**. Shop Zoro.com for All Your Needs!


Google
footprinting tools security check
Alle
Bilder
Shopping
Videos
News
Mehr
Einstellungen
Tools
Ungefähr 5.880.000 Ergebnisse (0,46 Sekunden)
Top 20 Data Reconnaissance and Intel Gathering Tools - SecurityTrails
https://securitytrails.com/blog/top-20-intel-tools Diese Seite übersetzen
17.04.2018 - These tools are presented here in order to help IT security researchers and ... HavelbeenPwned can help you to check if your account has been ... Is an amazing tool to track down footprints of any target you need to match.
Recon and Intel ... · HavelbeenPwned · Google Dorks · Maltego
Nutzer fragen auch
What tools can be used for footprinting?
What are the security testing tools?
What tools do hackers use?
What is footprinting and scanning?
Feedback geben
Footprinting tools for security auditors - SlideShare
https://de.slideshare.net/.../footprinting-tools-for-security-auditors Diese Seite übersetzen
05.02.2017 - Check for vulnerabilities on each target resource Attack targets using library of tools and techniques Footprint Analysis Who is DNS Lookup ...
Footprinting and scanning tools
home.ubalt.edu/abento/453/footscan/footscantools.html Diese Seite übersetzen
Sam Spade is a graphical tool which allows you to do DNS interrogation and many other things. ... Zone Transfer - ask a DNS server for all it knows about a domain. SMTP Relay Check - check whether a mail server allows third party relaying. Scan Addresses - scan a range of IP addresses looking for open ports.
15 Penetration Testing Tools-Open Source | securitywing
https://securitywing.com/15-penetration-testing-tools-open-source/ Diese Seite übersetzen
30.07.2014 - Reconnaissance /footprinting tools ... you need to remember that the target machine may notice that you are planning a penetration test.
Penetration testing reconnaissance -- Footprinting, scanning and ...
https://searchitchannel.techtarget.com/.../Penetration-testing-recon... Diese Seite übersetzen
Penetration testing reconnaissance -- Footprinting, scanning and enumerating ... network range of the target. Common tools/resources used in the footprinting phase are: ... Dig Deeper on Cybersecurity risk assessment and management. All; News; Get ... Data gathering 4 pentest: Footprinting, scanning and enumerating.
Top 15 Open Source Security Testing Tools for Web Applications
https://www.testbytes.net/blog/open-source-security-testing-tools/ Diese Seite übersetzen
30.08.2017 - This is where web application security testing tools play their role. ... It performs 'black box testing,' to check the web applications for possible vulnerability. ... optimized for HTTP handling and leaving minimum CPU footprints.
Footprinting and Reconnaissance – Hacker Noon
https://hackernoon.com/https-medium-com-aamralkar-footprintin... Diese Seite übersetzen
01.08.2018 - Well in a layman and simple language “ Foot Printing in Security terms ... Hackers will come to know what tools and technology organization is ...



free footprinting tools

Web Images Videos News Settings

Germany Safe Search: Moderate Any Time

Buy Footprint Tools | Fast, Free Shipping AD
www.zoro.com | Report Ad
You've Got the Jobs. We've Got the **Tools**. Shop Zoro.com for All Your Needs!

- Zoro Brand products — High-value options to more expensive name brands!
- Auto Returns — Returns Just Got Easier For Orders Placed On Zoro.com!
- Account Login — Log In or Create a Zoro Account!
- Browse All Products — Shop Over 2 Million Products! Everything To Clean, Build & Fix.

Footprinting and scanning tools - ubalt.edu
home.ubalt.edu/abento/453/footscan/footscantools.html
This is a selection of **footprinting** and scanning **tools** you may wish to install in your MIS Lab VM machine in order to do the course assignments. Some of these **tools** are NOT safe to install in your home PCs. You should be very careful in using these **tools** outside of the Lab. Network administrators do not take lightly the probing of their ...

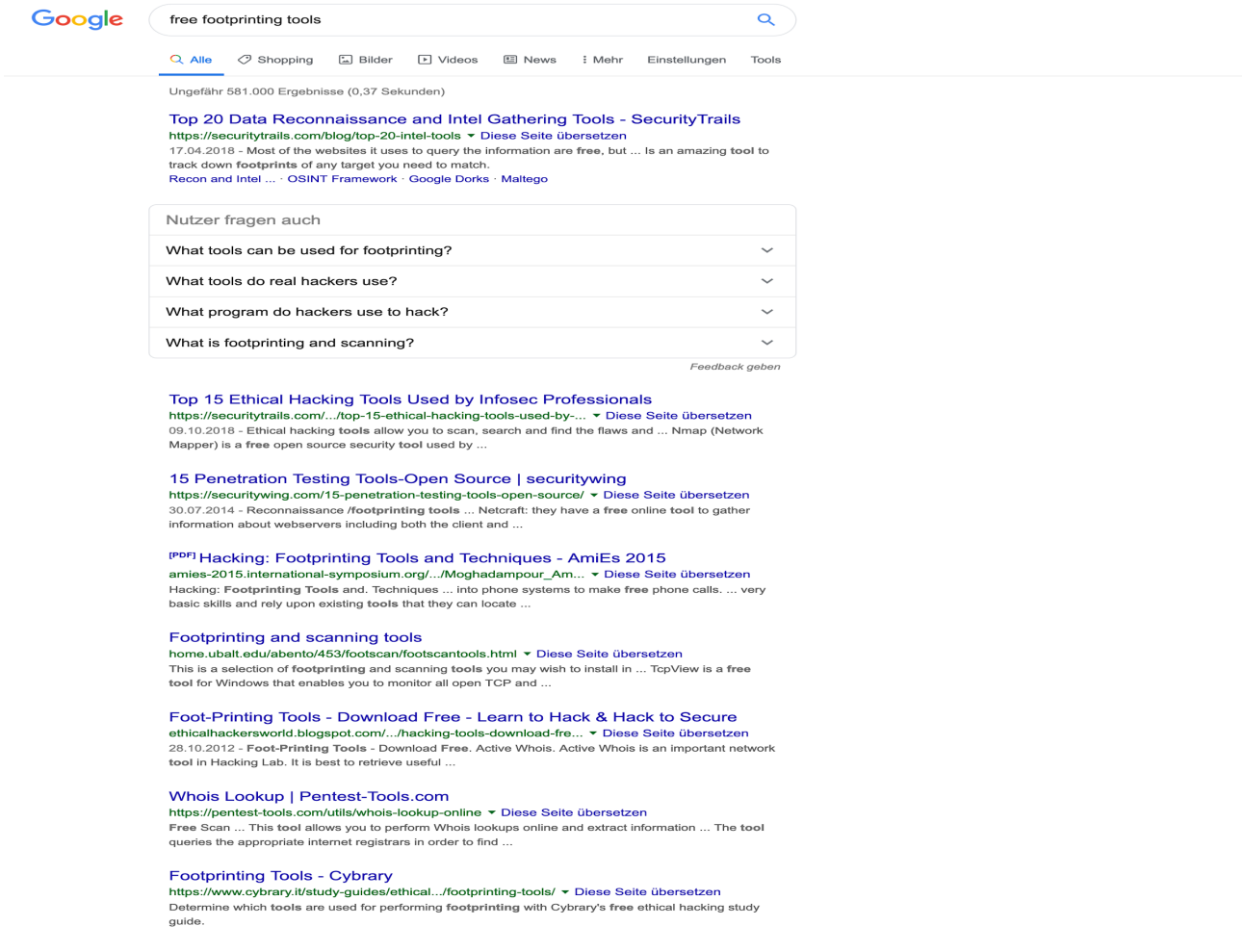
Paraphrasing Tool - Free Online Text Rewriting Tool
https://paraphrasing-tool.com
How Paraphrasing **Tool** Works. First, type or paste in the text you wish to reword. If you have already looked over your article and are satisfied with the level of spell and grammar checking that has been done, then enter the correct (numeric only) answer for the math bot challenge and click the 'Go!' button.

SpiderFoot (Open Source Footprinting) :: Tools - ToolWar ...
www.toolwar.com/2014/01/spiderfoot-open-source-footprinting.html
SpiderFoot is a **free**, open-source **footprinting tool**, enabling you to perform various scans against a given domain name in order to obtain information such as sub-domains, e-mail addresses, owned netblocks, web server versions and so on.

Top 10 Footprinting Tools - YouTube
https://www.youtube.com/watch?v=3Ejc-xe8vYI
Top 10 **Footprinting Tools** CEH V9. This **tools** use of Ethical hacker,Black hat hacker and security Analyst.

Hacking tutorial: Footprinting and scanning tools
https://whyihacker.blogspot.com/2017/05/footprinting-and-scanning-tools.html
This is a selection of **footprinting** and scanning **tools** you may wish to install in your MIS Lab machine in order to do the course assignments. You should be very careful in using these **tools** outside of the Lab. Network administrators do not take lightly the probing of their networks and may respond aggressively to your attempts to gain information about them by using some of these **tools**.

5. Footprinting Tools and Techniques - Hacker Techniques ...
https://www.oreilly.com/library/view/hacker-techniques-tools/9780763791834/ch05.h...
Footprinting Tools and Techniques WHEN THINKING ABOUT HACKING into systems, you might think that hackers simply use a few software **tools** to gain access to the target. Although it is true that there are a multitude of **tools** available to facilitate this very action.



Google free footprinting tools

Alle Shopping Bilder Videos News Mehr Einstellungen Tools

Ungefähr 581.000 Ergebnisse (0,37 Sekunden)

Top 20 Data Reconnaissance and Intel Gathering Tools - SecurityTrails
https://securitytrails.com/blog/top-20-intel-tools Diese Seite übersetzen
17.04.2018 - Most of the websites it uses to query the information are **free**, but ... Is an amazing **tool** to track down **footprints** of any target you need to match.
Recon and Intel ... · OSINT Framework · Google Dorks · Maltego

Nutzer fragen auch
- What tools can be used for footprinting?
- What tools do real hackers use?
- What program do hackers use to hack?
- What is footprinting and scanning?

Feedback geben

Top 15 Ethical Hacking Tools Used by Infosec Professionals
https://securitytrails.com/.../top-15-ethical-hacking-tools-used-by-... Diese Seite übersetzen
09.10.2018 - Ethical hacking **tools** allow you to scan, search and find the flaws and ... Nmap (Network Mapper) is a **free** open source security **tool** used by ...

15 Penetration Testing Tools-Open Source | securitywing
https://securitywing.com/15-penetration-testing-tools-open-source/ Diese Seite übersetzen
30.07.2014 - Reconnaissance /**footprinting tools** ... Netcraft: they have a **free** online **tool** to gather information about webservers including both the client and ...

[PDF] Hacking: Footprinting Tools and Techniques - AmiEs 2015
amies-2015.international-symposium.org/.../Moghadampour_Am... Diese Seite übersetzen
Hacking: **Footprinting Tools** and. Techniques ... into phone systems to make **free** phone calls. ... very basic skills and rely upon existing **tools** that they can locate ...

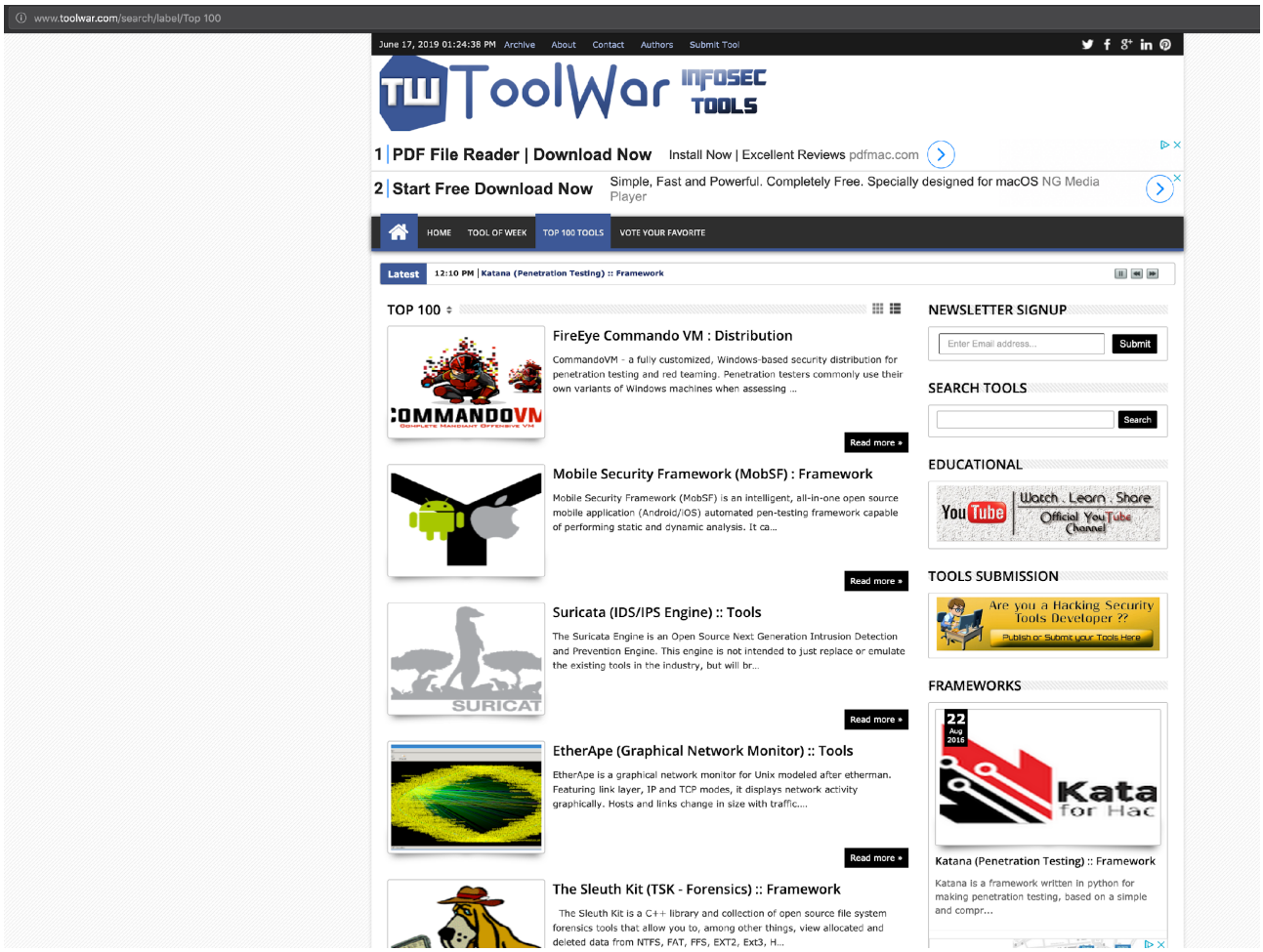
Footprinting and scanning tools
home.ubalt.edu/abento/453/footscan/footscantools.html Diese Seite übersetzen
This is a selection of **footprinting** and scanning **tools** you may wish to install in ... TcpView is a **free tool** for Windows that enables you to monitor all open TCP and ...

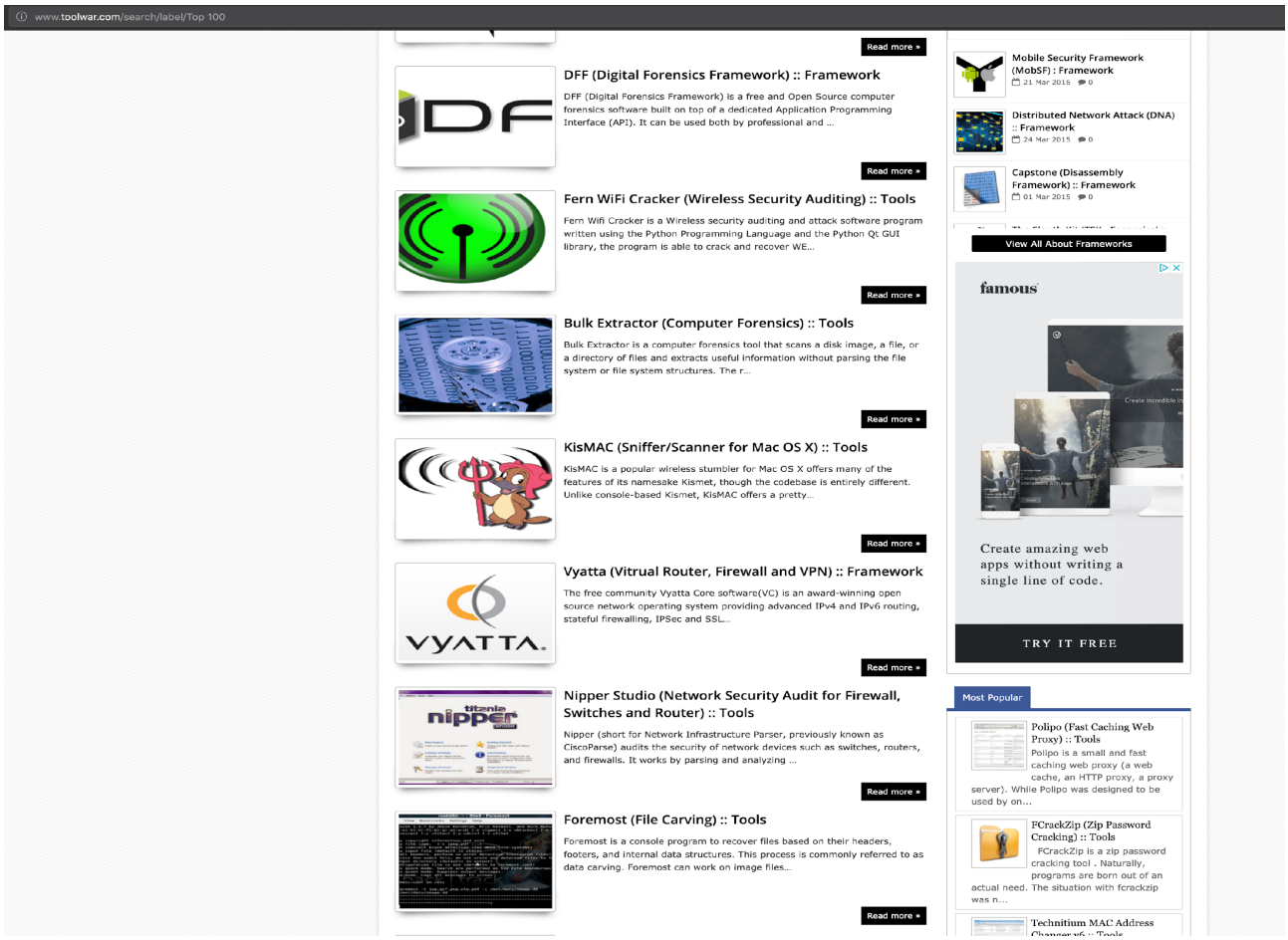
Foot-Printing Tools - Download Free - Learn to Hack & Hack to Secure
ethicalhackersworld.blogspot.com/.../hacking-tools-download-fre... Diese Seite übersetzen
28.10.2012 - **Foot-Printing Tools** - Download **Free**. Active Whois. Active Whois is an important network **tool** in Hacking Lab. It is best to retrieve useful ...

Whois Lookup | Pentest-Tools.com
https://pentest-tools.com/utils/whois-lookup-online Diese Seite übersetzen
Free Scan ... This **tool** allows you to perform Whois lookups online and extract information ... The **tool** queries the appropriate internet registrars in order to find ...

Footprinting Tools - Cybrary
https://www.cybrary.it/study-guides/ethical.../footprinting-tools/ Diese Seite übersetzen
Determine which **tools** are used for performing **footprinting** with Cybrary's **free** ethical hacking study guide.

DuckDuckGo hat dann Listen wie diese gefunden:




www.toolwar.com/search/label/Top 100
Read more »
DFF (Digital Forensics Framework) :: Framework
DFF (Digital Forensics Framework) is a free and Open Source computer forensics software built on top of a dedicated Application Programming Interface (API). It can be used both by professional and ...
Read more »
Fern WiFi Cracker (Wireless Security Auditing) :: Tools
Fern Wifi Cracker is a Wireless security auditing and attack software program written using the Python Programming Language and the Python Qt GUI library, the program is able to crack and recover WE...
Read more »
Bulk Extractor (Computer Forensics) :: Tools
Bulk Extractor is a computer forensics tool that scans a disk image, a file, or a directory of files and extracts useful information without parsing the file system or file system structures. The r...
Read more »
KisMAC (Sniffer/Scanner for Mac OS X) :: Tools
KisMAC is a popular wireless stumbler for Mac OS X offers many of the features of its namesake Kismet, though the codebase is entirely different. Unlike console-based Kismet, KisMAC offers a pretty...
Read more »
Vyatta (Vitrual Router, Firewall and VPN) :: Framework
The free community Vyatta Core software(VC) is an award-winning open source network operating system providing advanced IPv4 and IPv6 routing, stateful firewalling, IPSec and SSL...
Read more »
Nipper Studio (Network Security Audit for Firewall, Switches and Router) :: Tools
Nipper (short for Network Infrastructure Parser, previously known as CiscoParse) audits the security of network devices such as switches, routers, and firewalls. It works by parsing and analyzing ...
Read more »
Foremost (File Carving) :: Tools
Foremost is a console program to recover files based on their headers, footers, and internal data structures. This process is commonly referred to as data carving. Foremost can work on image files...
Read more »
Mobile Security Framework (MobSF) : Framework
21 Mar 2016 0
Distributed Network Attack (DNA) :: Framework
24 Mar 2015 0
Capstone (Disassembly Framework) :: Framework
01 Mar 2015 0
View All About Frameworks
famous
Create amazing web apps without writing a single line of code.
TRY IT FREE
Most Popular
Polipo (Fast Caching Web Proxy) :: Tools
Polipo is a small and fast caching web proxy (a web cache, an HTTP proxy, a proxy server). While Polipo was designed to be used by on...
FCrackZip (Zip Password Cracking) :: Tools
FCrackZip is a zip password cracking tool . Naturally, programs are born out of an actual need. The situation with fcrackzip was n...
Technitium MAC Address

Und Google wie diese:

company data, domains, IPs, servers, and running software?

We have the right answer to those questions. On this post, we will show you the top best Recon and Intel information gathering tools for IT Security Researchers.

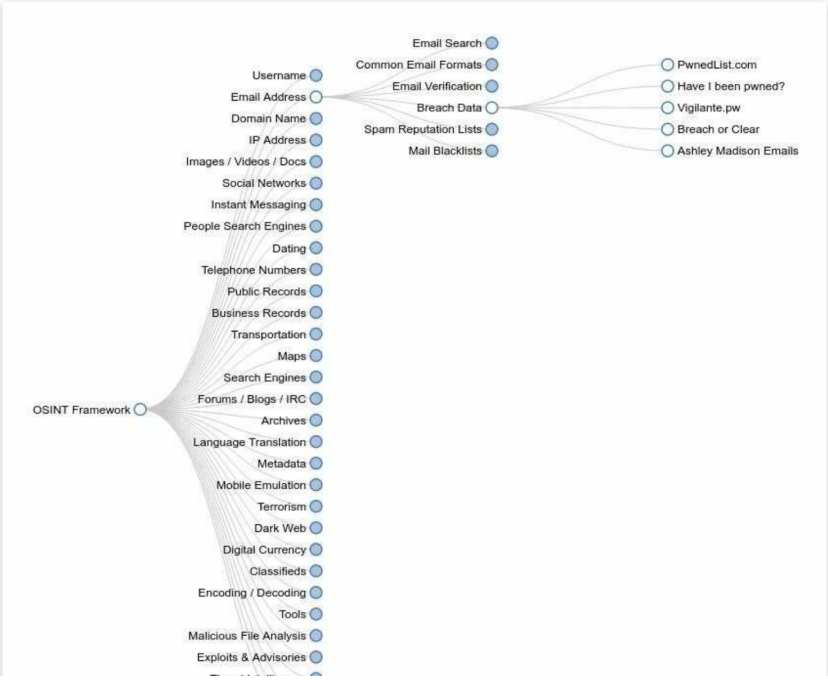
20 Recon and Intel Gathering Tools used by InfoSec Professionals

Important note *before we start: remember that you should never use these tools on external networks/systems without previous authorization. These tools are presented here in order to help IT security researchers and private/public infosec investigators during the first phase of information gathering, which is one of the most important parts of a cybersecurity investigation.*

1. OSINT Framework

While OSINT Framework isn't a tool to be run on your servers, it's a very useful way to get valuable information by querying free search engines, resources, and tools publicly available on the Internet. They are focused on bringing the best links to valuable sources of OSINT data.

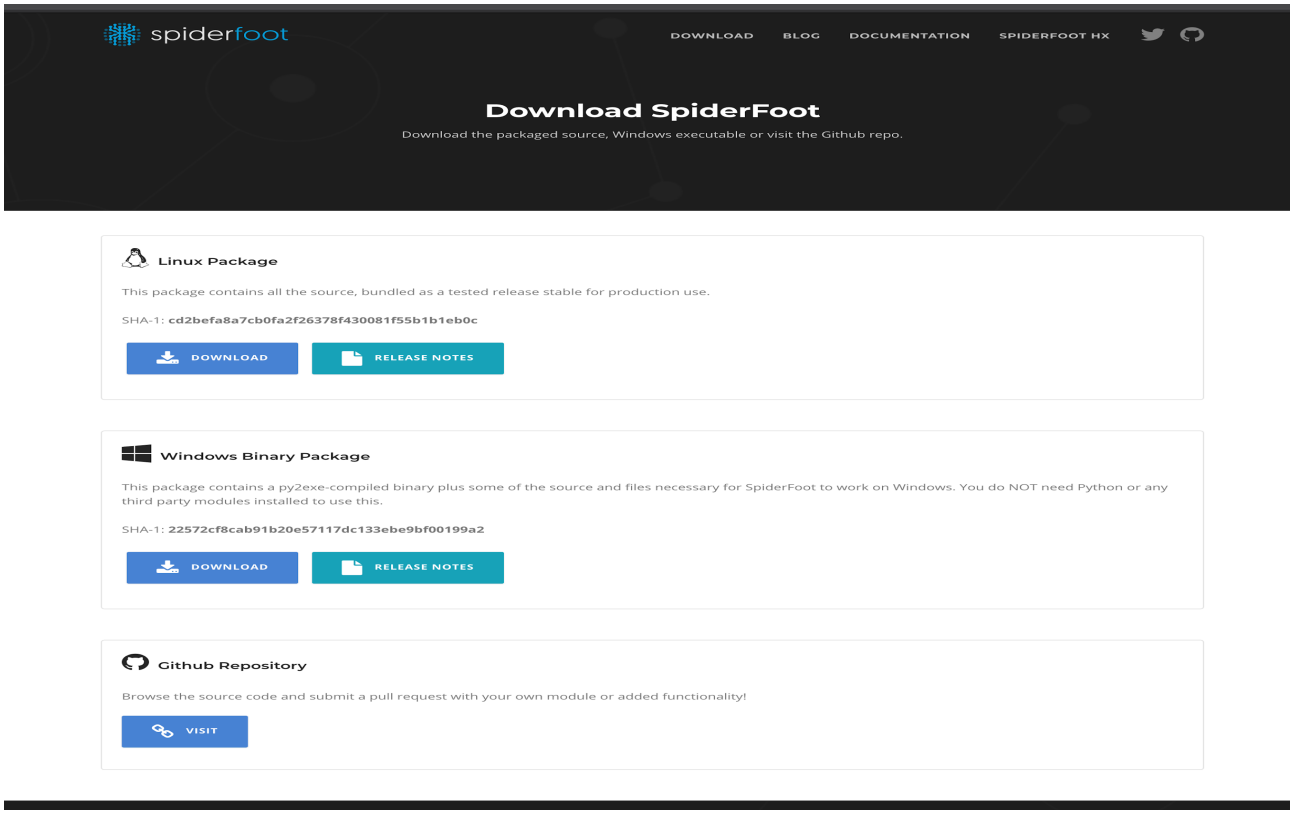
While this web application was originally created focused on IT security, with the time it has evolved and today you can get other kinds of information from other industries as well. Most of the websites it uses to query the information are free, but some may require paying a low fee.

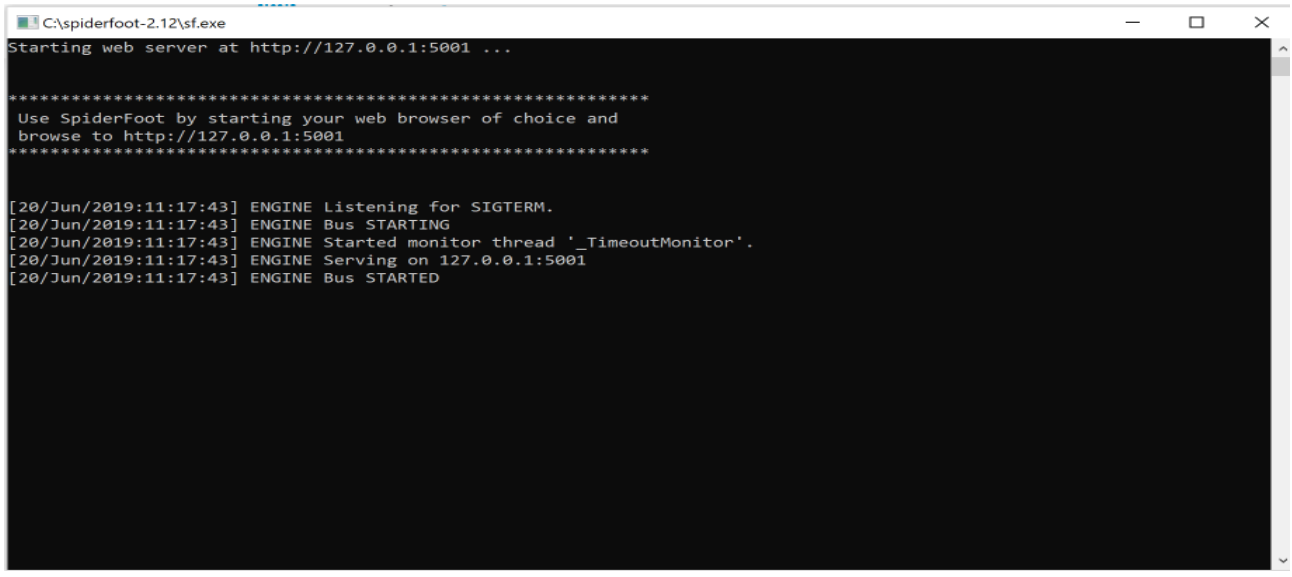


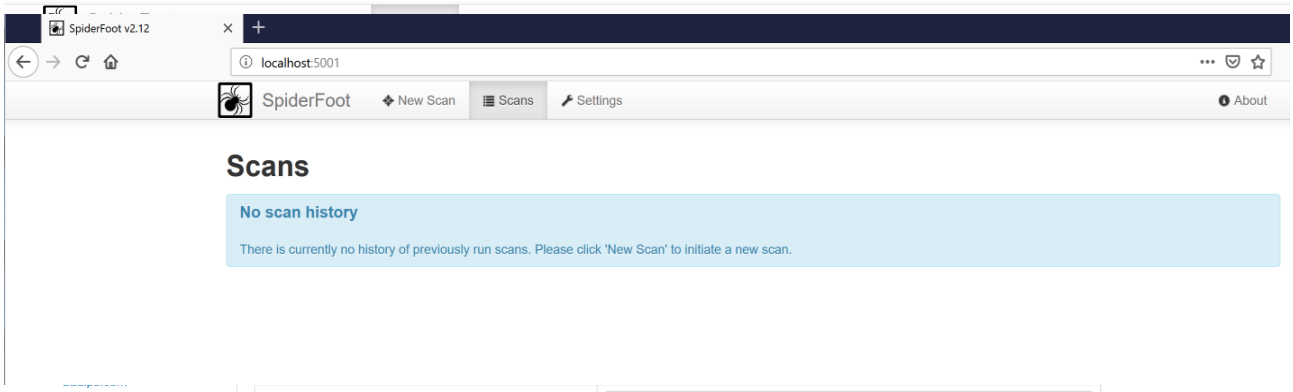
Search...

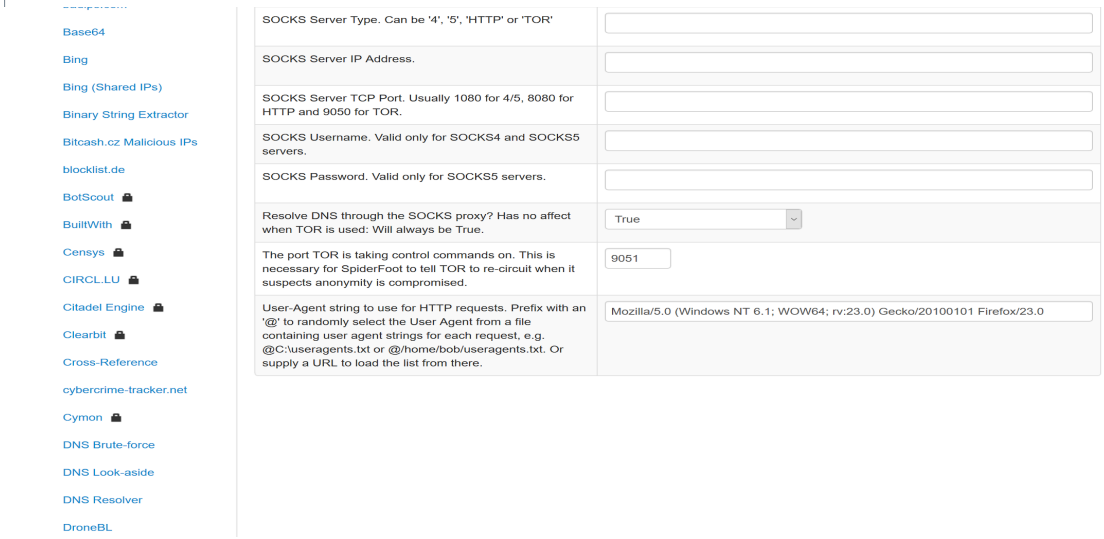
TABLE OF CONTENTS

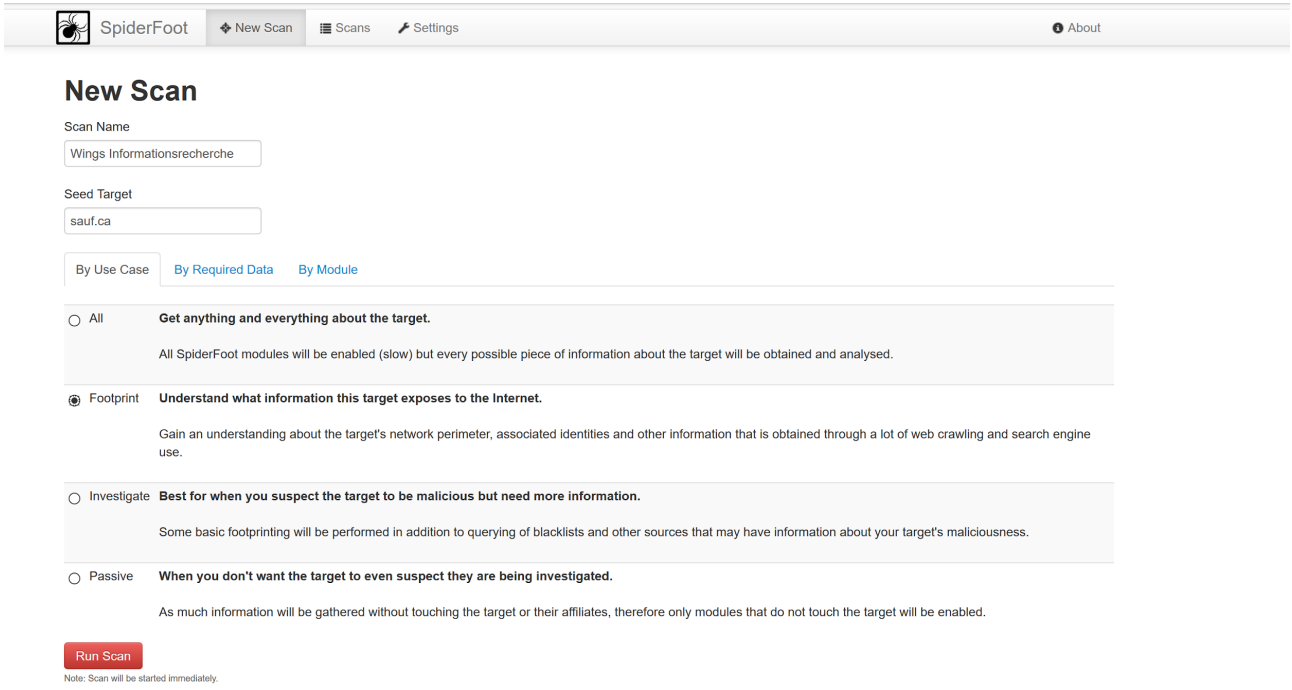
F) Exemplarisch haben sich die Autoren für die Software SpiderFoot entschieden welche hier in Screenshots kurz für sich selbst sprechen kann:

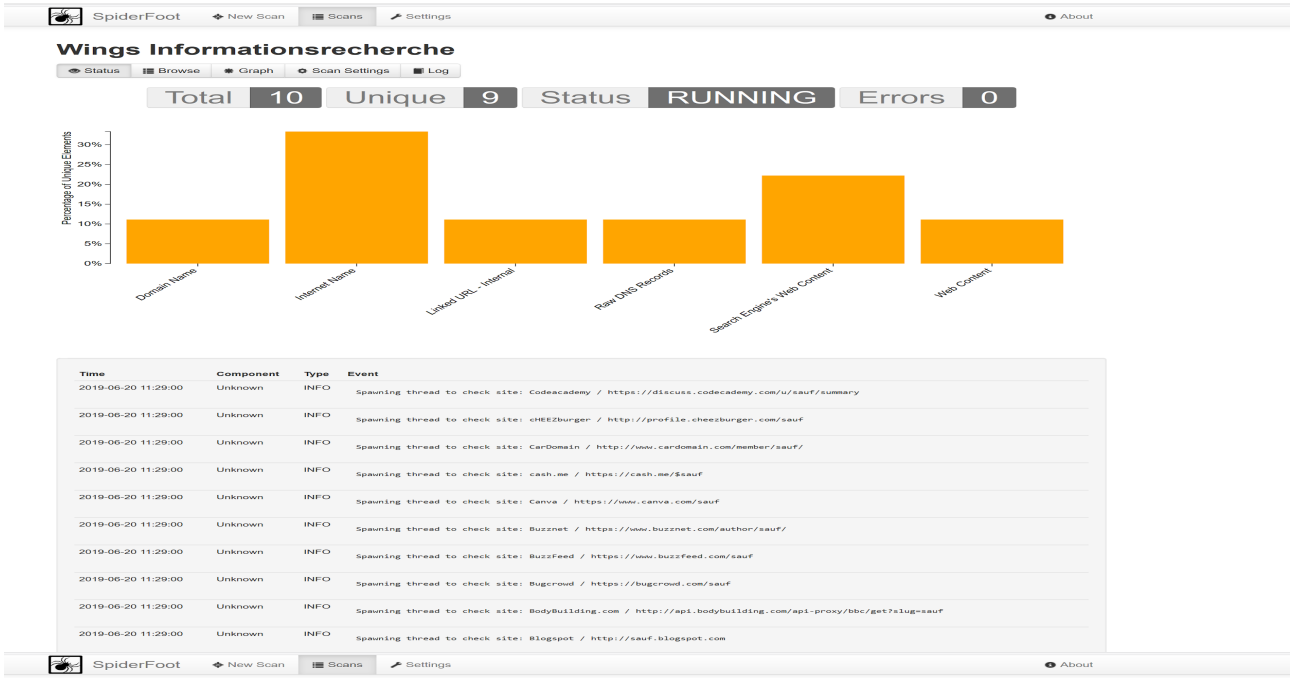




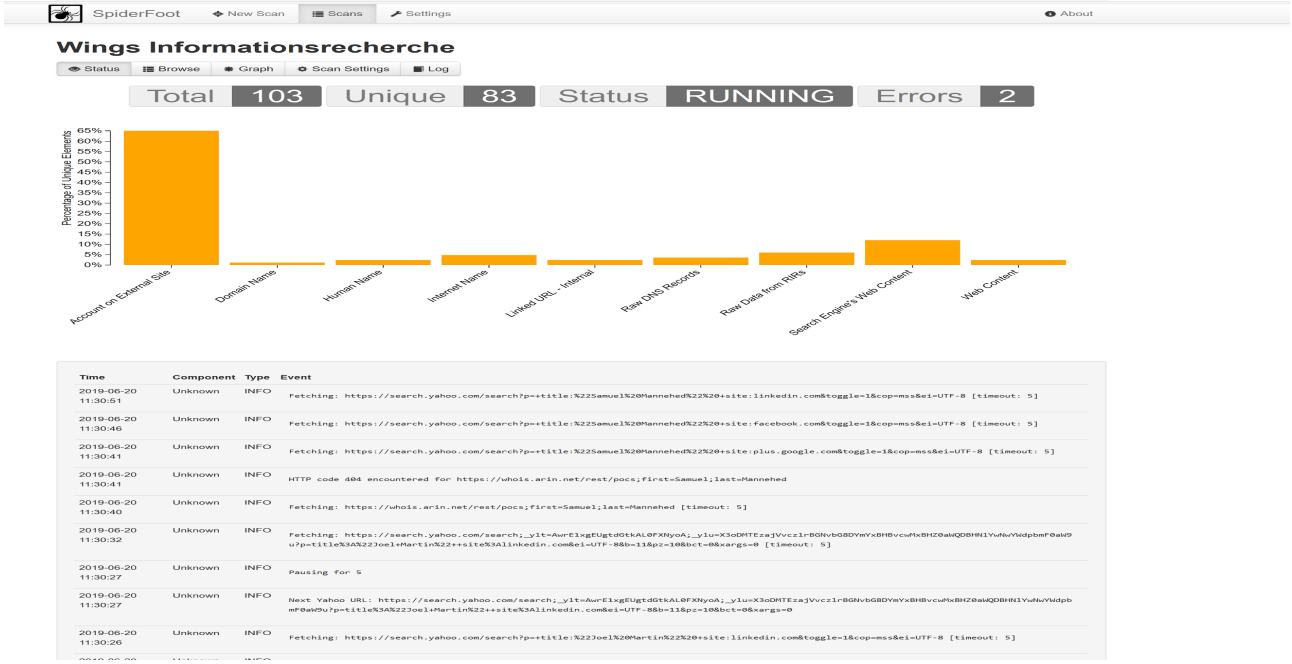

SpiderFoot v2.12
localhost:5001
SpiderFoot
New Scan
Scans
Settings
About
Scans
No scan history
There is currently no history of previously run scans. Please click 'New Scan' to initiate a new scan.


Base64
Bing
Bing (Shared IPs)
Binary String Extractor
Bitcash.cz Malicious IPs
blocklist.de
BotScout
BuiltWith
Censys
CIRCL.LU
Citadel Engine
Clearbit
Cross-Reference
cybercrime-tracker.net
Cymon
DNS Brute-force
DNS Look-aside
DNS Resolver
DroneBL
SOCKS Server Type. Can be '4', '5', 'HTTP' or 'TOR'
SOCKS Server IP Address.
SOCKS Server TCP Port. Usually 1080 for 4/5, 8080 for HTTP and 9050 for TOR.
SOCKS Username. Valid only for SOCKS4 and SOCKS5 servers.
SOCKS Password. Valid only for SOCKS5 servers.
Resolve DNS through the SOCKS proxy? Has no affect when TOR is used: Will always be True.
True
The port TOR is taking control commands on. This is necessary for SpiderFoot to tell TOR to re-circuit when it suspects anonymity is compromised.
9051
User-Agent string to use for HTTP requests. Prefix with an '@' to randomly select the User Agent from a file containing user agent strings for each request, e.g. @C:\useragents.txt or @/home/bob/useragents.txt. Or supply a URL to load the list from there.
Mozilla/5.0 (Windows NT 6.1; WOW64; rv:23.0) Gecko/20100101 Firefox/23.0

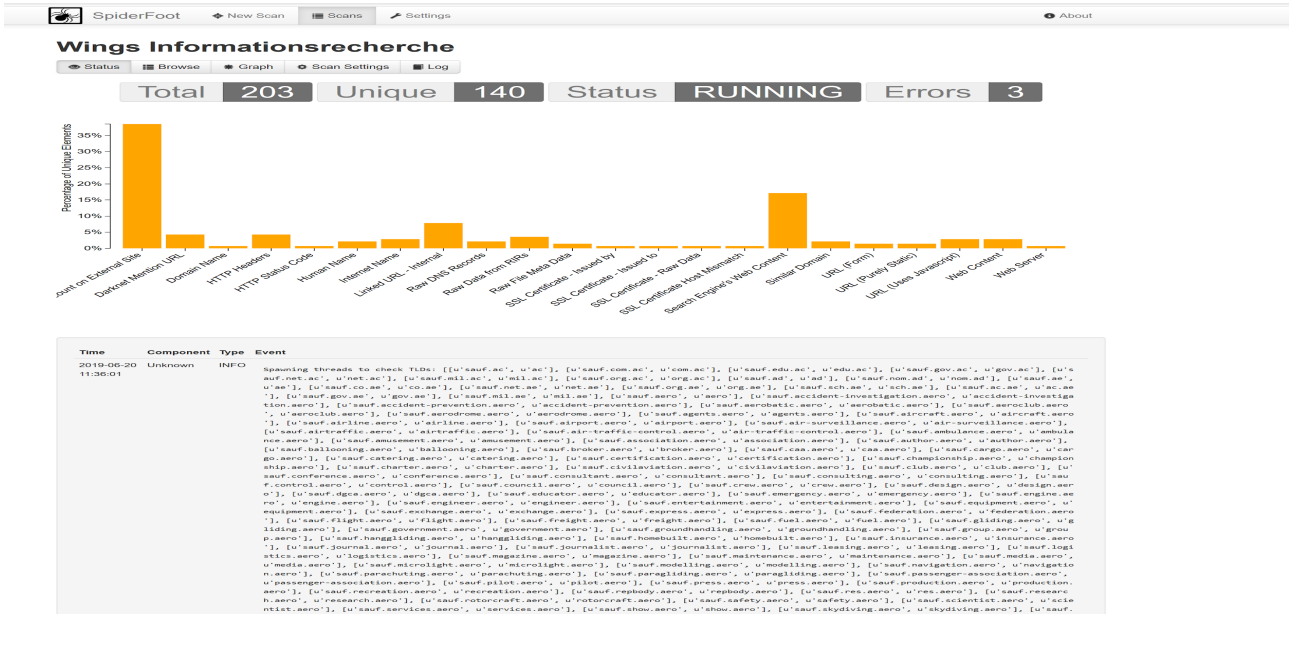

SpiderFoot
New Scan
Scans
Settings
About
New Scan
Scan Name
Wings Informationsrecherche
Seed Target
sauf.ca
By Use Case
By Required Data
By Module
All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.
Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.
Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.
Run Scan
Note: Scan will be started immediately.



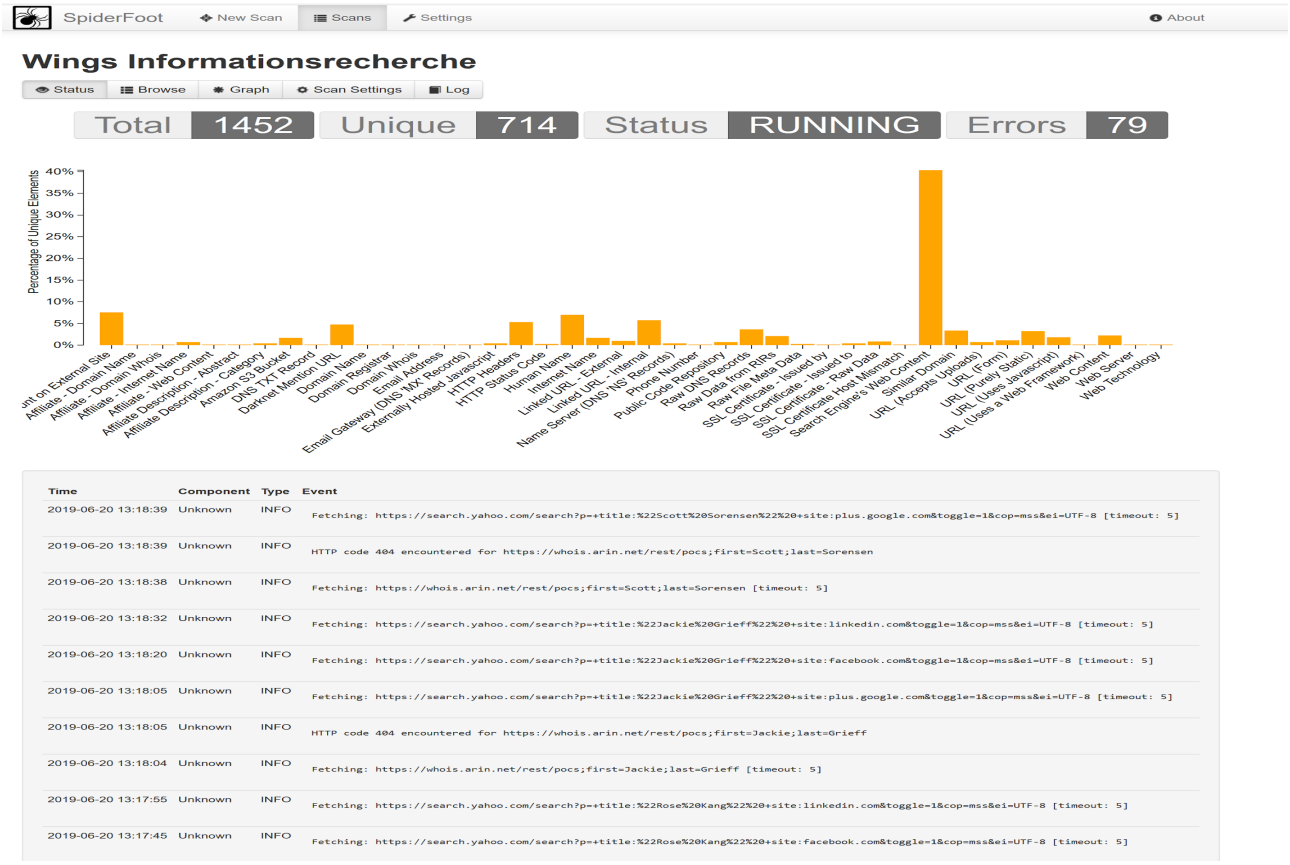
Time	Component	Type	Event
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: Codecademy / https://discuss.codecademy.com/u/sauf/summary
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: cHEEZburger / http://profile.cheezburger.com/sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: CarDomain / http://www.cardomain.com/member/sauf/
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: cash.me / https://cash.me/$sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: Canva / https://www.canva.com/sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: Buzznet / https://www.buzznet.com/author/sauf/
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: BuzzFeed / https://www.buzzfeed.com/sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: Bugcrowd / https://bugcrowd.com/sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: BodyBuilding.com / http://api.bodybuilding.com/api-proxy/bbc/get?slug=sauf
2019-06-20 11:29:00	Unknown	INFO	Spawning thread to check site: Blogspot / http://sauf.blogspot.com

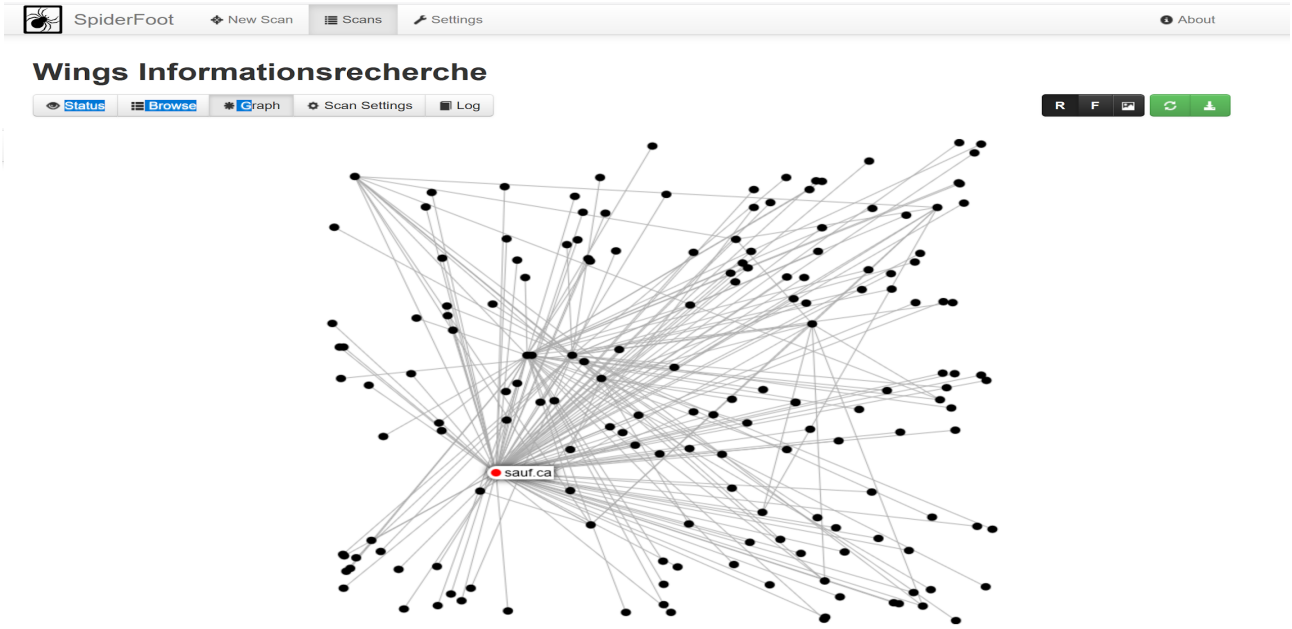


Time	Component	Type	Event
2019-06-20 11:30:51	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Samuel%20Mannehed%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 11:30:46	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Samuel%20Mannehed%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 11:30:41	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Samuel%20Mannehed%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 11:30:41	Unknown	INFO	HTTP code 404 encountered for https://whois.arin.net/rest/pocs;first=Samuel;last=Mannehed
2019-06-20 11:30:40	Unknown	INFO	Fetching: https://whois.arin.net/rest/pocs;first=Samuel;last=Mannehed [timeout: 5]
2019-06-20 11:30:32	Unknown	INFO	Fetching: https://search.yahoo.com/search;_ylt=AwrElxgfUgtdOtkAL0FXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbGBDYmYxBHBvcwMxBHZ0aWQDBHNlYwNvYWdpbmF0aW9u?p=title%3A%22Joel+Martin%22++site%3Alinkedin.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0 [timeout: 5]
2019-06-20 11:30:27	Unknown	INFO	Pausing for 5
2019-06-20 11:30:27	Unknown	INFO	Next Yahoo URL: https://search.yahoo.com/search;_ylt=AwrElxgfUgtdGtkAL0FXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbGBDYmYxBHBvcwMxBHZ0aWQDBHNlYwNvYWdpbmF0aW9u?p=title%3A%22Joel+Martin%22++site%3Alinkedin.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0
2019-06-20 11:30:26	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Joel%20Martin%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]

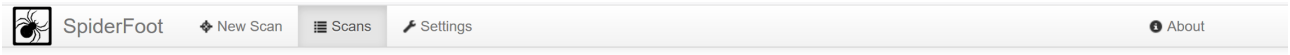


Time	Component	Type	Event
2019-06-20 11:36:01	Unknown	INFO	Spawning threads to check TLDs: [[u'sauf.ac', u'ac'], [u'sauf.com.ac', u'com.ac'], [u'sauf.edu.ac', u'edu.ac'], [u'sauf.gov.ac', u'gov.ac'], [u'sauf.net.ac', u'net.ac'], [u'sauf.mil.ac', u'mil.ac'], [u'sauf.org.ac', u'org.ac'], [u'sauf.ad', u'ad'], [u'sauf.nom.ad', u'nom.ad'], [u'sauf.ae', u'ae'], [u'sauf.co.ae', u'co.ae'], [u'sauf.net.ae', u'net.ae'], [u'sauf.org.ae', u'org.ae'], [u'sauf.sch.ae', u'sch.ae'], [u'sauf.ac.ae', u'ac.ae'], [u'sauf.gov.ae', u'gov.ae'], [u'sauf.mil.ae', u'mil.ae'], [u'sauf.aero', u'aero'], [u'sauf.accident-investigation.aero', u'accident-investigation.aero'], [u'sauf.accident-prevention.aero', u'accident-prevention.aero'], [u'sauf.aerobatic.aero', u'aerobatic.aero'], [u'sauf.aeroclub.aero', u'aeroclub.aero'], [u'sauf.aerodrome.aero', u'aerodrome.aero'], [u'sauf.agents.aero', u'agents.aero'], [u'sauf.aircraft.aero', u'aircraft.aero'], [u'sauf.airline.aero', u'airline.aero'], [u'sauf.airport.aero', u'airport.aero'], [u'sauf.air-surveillance.aero', u'air-surveillance.aero'], [u'sauf.air-traffic.aero', u'air-traffic.aero'], [u'sauf.air-traffic-control.aero', u'air-traffic-control.aero'], [u'sauf.ambulance.aero', u'ambulance.aero'], [u'sauf.amusement.aero', u'amusement.aero'], [u'sauf.association.aero', u'association.aero'], [u'sauf.author.aero', u'author.aero'], [u'sauf.ballooning.aero', u'ballooning.aero'], [u'sauf.broker.aero', u'broker.aero'], [u'sauf.caa.aero', u'caa.aero'], [u'sauf.cargo.aero', u'cargo.aero'], [u'sauf.catering.aero', u'catering.aero'], [u'sauf.certification.aero', u'certification.aero'], [u'sauf.championship.aero', u'championship.aero'], [u'sauf.charter.aero', u'charter.aero'], [u'sauf.civilaviation.aero', u'civilaviation.aero'], [u'sauf.club.aero', u'club.aero'], [u'sauf.conference.aero', u'conference.aero'], [u'sauf.consultant.aero', u'consultant.aero'], [u'sauf.consulting.aero', u'consulting.aero'], [u'sauf.control.aero', u'control.aero'], [u'sauf.council.aero', u'council.aero'], [u'sauf.crew.aero', u'crew.aero'], [u'sauf.design.aero', u'design.aero'], [u'sauf.dgca.aero', u'dgca.aero'], [u'sauf.educator.aero', u'educator.aero'], [u'sauf.emergency.aero', u'emergency.aero'], [u'sauf.engine.aero', u'engine.aero'], [u'sauf.engineer.aero', u'engineer.aero'], [u'sauf.entertainment.aero', u'entertainment.aero'], [u'sauf.equipment.aero', u'equipment.aero'], [u'sauf.exchange.aero', u'exchange.aero'], [u'sauf.express.aero', u'express.aero'], [u'sauf.federation.aero', u'federation.aero'], [u'sauf.flight.aero', u'flight.aero'], [u'sauf.freight.aero', u'freight.aero'], [u'sauf.fuel.aero', u'fuel.aero'], [u'sauf.gliding.aero', u'gliding.aero'], [u'sauf.government.aero', u'government.aero'], [u'sauf.groundhandling.aero', u'groundhandling.aero'], [u'sauf.group.aero', u'group.aero'], [u'sauf.hanggliding.aero', u'hanggliding.aero'], [u'sauf.homebuilt.aero', u'homebuilt.aero'], [u'sauf.insurance.aero', u'insurance.aero'], [u'sauf.journal.aero', u'journal.aero'], [u'sauf.journalist.aero', u'journalist.aero'], [u'sauf.leasing.aero', u'leasing.aero'], [u'sauf.logistics.aero', u'logistics.aero'], [u'sauf.magazine.aero', u'magazine.aero'], [u'sauf.maintenance.aero', u'maintenance.aero'], [u'sauf.media.aero', u'media.aero'], [u'sauf.microlight.aero', u'microlight.aero'], [u'sauf.modelling.aero', u'modelling.aero'], [u'sauf.navigation.aero', u'navigation.aero'], [u'sauf.parachuting.aero', u'parachuting.aero'], [u'sauf.paragliding.aero', u'paragliding.aero'], [u'sauf.passenger-association.aero', u'passenger-association.aero'], [u'sauf.pilot.aero', u'pilot.aero'], [u'sauf.press.aero', u'press.aero'], [u'sauf.production.aero', u'production.aero'], [u'sauf.recreation.aero', u'recreation.aero'], [u'sauf.repbody.aero', u'repbody.aero'], [u'sauf.res.aero', u'res.aero'], [u'sauf.research.aero', u'research.aero'], [u'sauf.rotorcraft.aero', u'rotorcraft.aero'], [u'sauf.safety.aero', u'safety.aero'], [u'sauf.scientist.aero', u'scientist.aero'], [u'sauf.services.aero', u'services.aero'], [u'sauf.show.aero', u'show.aero'], [u'sauf.skydiving.aero', u'skydiving.aero'], [u'sauf.


SpiderFoot
New Scan
Scans
Settings
About
Wings Informationsrecherche
Status
Browse
Graph
Scan Settings
Log
Total 1452
Unique 714
Status RUNNING
Errors 79
Percentage of Unique Elements
40%
35%
30%
25%
20%
15%
10%
5%
0%
Affiliate - Domain Name
Affiliate - Domain Whois
Affiliate - Internet Name
Affiliate - Web Content
Affiliate Description - Abstract
Affiliate Description - Category
Amazon S3 Bucket
DNS TXT Record
Darknet Mention URL
Domain Name
Domain Registrar
Domain Whois
Email Address
Email Gateway (DNS 'MX' Records)
Externally Hosted Javascript
HTTP Headers
HTTP Status Code
Human Name
Internet Name
Linked URL - External
Linked URL - Internal
Name Server (DNS 'NS' Records)
Phone Number
Public Code Repository
Raw DNS Records
Raw Data from RIRs
Raw File Meta Data
SSL Certificate - Issued by
SSL Certificate - Issued to
SSL Certificate - Raw Data
SSL Certificate Host Mismatch
Search Engine's Web Content
Similar Domain
URL (Accepts Uploads)
URL (Form)
URL (Purely Static)
URL (Uses Javascript)
URL (Uses a Web Framework)
Web Content
Web Server
Web Technology
Time Component Type Event
2019-06-20 13:18:39 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Scott%20Sorensen%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:39 Unknown INFO HTTP code 404 encountered for https://whois.arin.net/rest/pocs;first=Scott;last=Sorensen
2019-06-20 13:18:38 Unknown INFO Fetching: https://whois.arin.net/rest/pocs;first=Scott;last=Sorensen [timeout: 5]
2019-06-20 13:18:32 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:20 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:05 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:05 Unknown INFO HTTP code 404 encountered for https://whois.arin.net/rest/pocs;first=Jackie;last=Grieff
2019-06-20 13:18:04 Unknown INFO Fetching: https://whois.arin.net/rest/pocs;first=Jackie;last=Grieff [timeout: 5]
2019-06-20 13:17:55 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Rose%20Kang%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:17:45 Unknown INFO Fetching: https://search.yahoo.com/search?p=+title:%22Rose%20Kang%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]



Raw Data from RIRs	15	15	2019-06-20 12:50:35
Raw File Meta Data	2	4	2019-06-20 11:35:57
SSL Certificate - Issued by	1	17	2019-06-20 13:15:23
SSL Certificate - Issued to	3	17	2019-06-20 13:15:23
SSL Certificate - Raw Data	6	17	2019-06-20 13:15:23
SSL Certificate Host Mismatch	1	12	2019-06-20 13:15:23



Wings Informationsrecherche

Status | Browse | Graph | Scan Settings | Log

Time	Component	Type	Event
2019-06-20 13:19:46	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Nathan%20Azhderian%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:19:41	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Nathan%20Azhderian%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:19:34	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Nathan%20Azhderian%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:19:34	Unknown	INFO	HTTP code 404 encountered for https://whois.arin.net/rest/pocs;first=Nathan;last=Azhderian
2019-06-20 13:19:33	Unknown	INFO	Fetching: https://whois.arin.net/rest/pocs;first=Nathan;last=Azhderian [timeout: 5]
2019-06-20 13:19:26	Unknown	INFO	Fetching: https://search.yahoo.com/search;_ylt=A0geKLyIawtdpWoA0xRXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwYWdpbmF0aW9u?p=title%3A%22Scott+Sorensen%22++site%3Alinkedin.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0 [timeout: 5]
2019-06-20 13:19:20	Unknown	INFO	Pausing for 6
2019-06-20 13:19:20	Unknown	INFO	Next Yahoo URL: https://search.yahoo.com/search;_ylt=A0geKLyIawtdpWoA0xRXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwYWdpbmF0aW9u?p=title%3A%22Scott+Sorensen%22++site%3Alinkedin.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0
2019-06-20 13:19:18	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Scott%20Sorensen%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:19:07	Unknown	INFO	Fetching: https://search.yahoo.com/search;_ylt=AwrJ61NwawtdcscABwtXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwYWdpbmF0aW9u?p=title%3A%22Scott+Sorensen%22++site%3Afacebook.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0 [timeout: 5]
2019-06-20 13:18:56	Unknown	INFO	Pausing for 11
2019-06-20 13:18:56	Unknown	INFO	Next Yahoo URL: https://search.yahoo.com/search;_ylt=AwrJ61NwawtdcscABwtXNyoA;_ylu=X3oDMTEzajVvczlrBGNvbG8DYmYxBHBvcwMxBHZ0aWQDBHNlYwNwYWdpbmF0aW9u?p=title%3A%22Scott+Sorensen%22++site%3Afacebook.com&ei=UTF-8&b=11&pz=10&bct=0&xargs=0
2019-06-20 13:18:55	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Scott%20Sorensen%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:39	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Scott%20Sorensen%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:39	Unknown	INFO	HTTP code 404 encountered for https://whois.arin.net/rest/pocs;first=Scott;last=Sorensen
2019-06-20 13:18:38	Unknown	INFO	Fetching: https://whois.arin.net/rest/pocs;first=Scott;last=Sorensen [timeout: 5]
2019-06-20 13:18:32	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:linkedin.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:20	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:facebook.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]
2019-06-20 13:18:05	Unknown	INFO	Fetching: https://search.yahoo.com/search?p=+title:%22Jackie%20Grieff%22%20+site:plus.google.com&toggle=1&cop=mss&ei=UTF-8 [timeout: 5]

3. Versuch mit Google-Abfragen die vorangegangenen Infos zu finden

Aus der vorherigen Footprinting-Recherche (mit Hilfe von Tools) konnten zusammengefasst folgende Informationen gewonnen werden:

DNS-Informationen

egal welche subdomain man eingibt, man landet bei sauf.ca

IP-Adresse

176.9.123.245

Provider

Hetzner

Offene Ports

22 ssh
80 http
443 https

Software Versionen

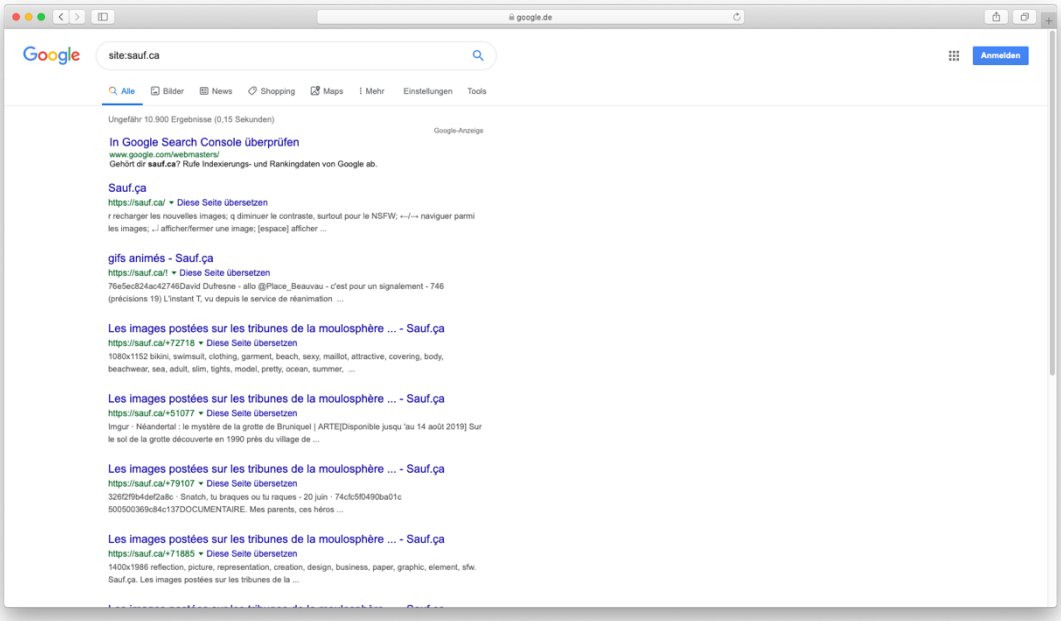
Apache Webserver Version 2.4.38 als LINUX/UNIX Version mit einkompiliertem OpenSSL Version 1.1.1b
OpenSSH Server Version 7.9 (Protokollnummer 2.0)

Nun soll versucht werden diese Information per Google-Abfragen zu finden:
Ausgangssituation für diese Abfragen ist natürlich, dass man lediglich die URL der Seite hat.

DNS-Informationen:

Hierfür wird eine Abfrage gemacht um mögliche Subdomains zu finden.

Abfrage: site:sauf.ca
Ergebnisse: ca. 10.900



Das Ergebnis von ungefähr 10.900 Ergebnissen spricht für sich. Hierbei ist aber zu beachten, dass es sich hierbei nie um eine Subdomain handelt, sondern immer nur um Kategorien der Website selbst, die nichtssagend sind (Format: sauf.ca/XXXX).

In diesem Fall lassen sich also nicht die vorangegangen Infos per Footprinting-tools herausfinden.

IP-Adresse:

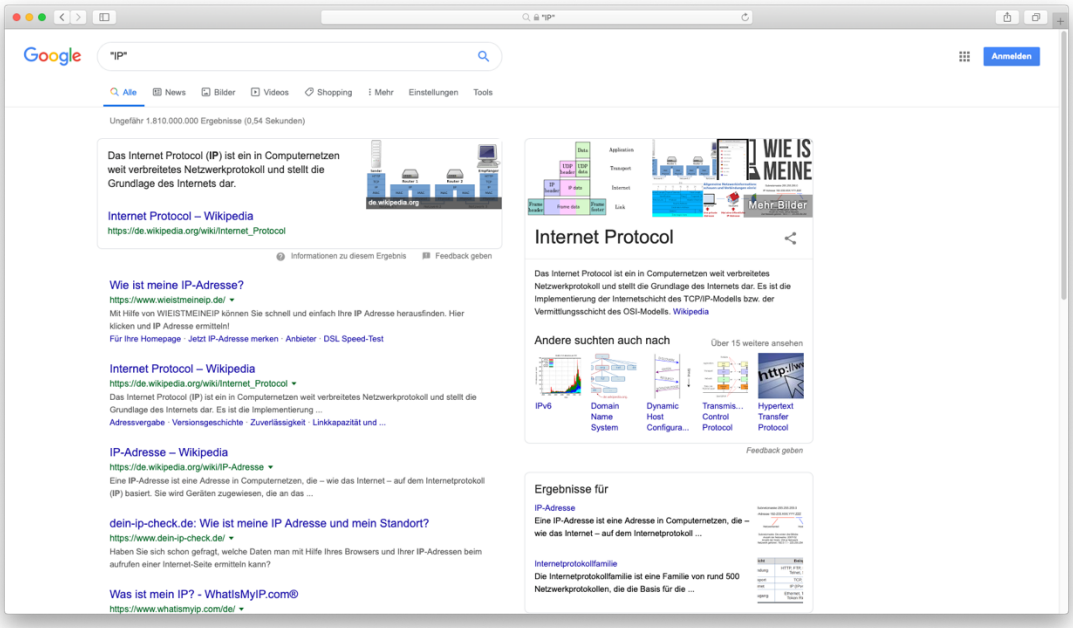
Hierfür wird eine Abfrage gemacht um die IP-Adresse des Servers zu finden.

Da man nichts über den Server weiß, kann man nur auf gut Glück nach der IP-Adresse suchen, in dem man alle indexierten Seiten durchsucht ob im Titel, Text oder in der URL der Begriff IP vorkommt.

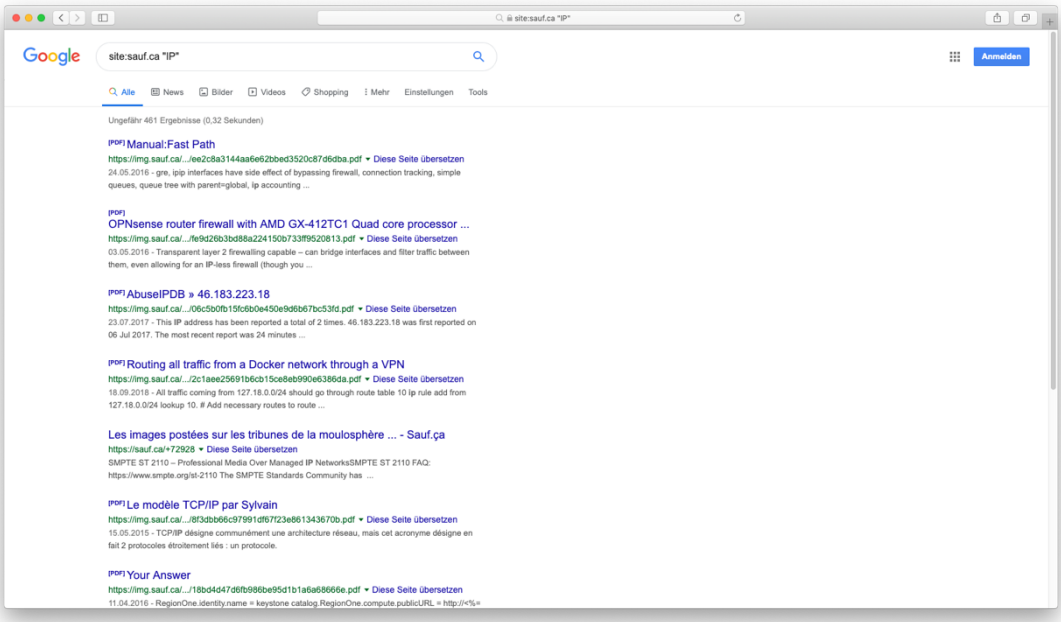
Allgemeine Abfrage: "IP"
Ergebnisse: ca. 1.810.000.000

“Sauf.ca”-Abfrage: site:sauf.ca "IP"
Ergebnisse: ca. 461

Allgemeine Abfrage:



„Sauf.ca“-Abfrage



Bei den gelieferten Seiten handelt es sich wieder nur um hochgeladene Dateien. Dies bringt uns also wieder nicht weiter.

In diesem Fall lassen sich also nicht die vorangegangen Infos per Footprinting-tools herausfinden.

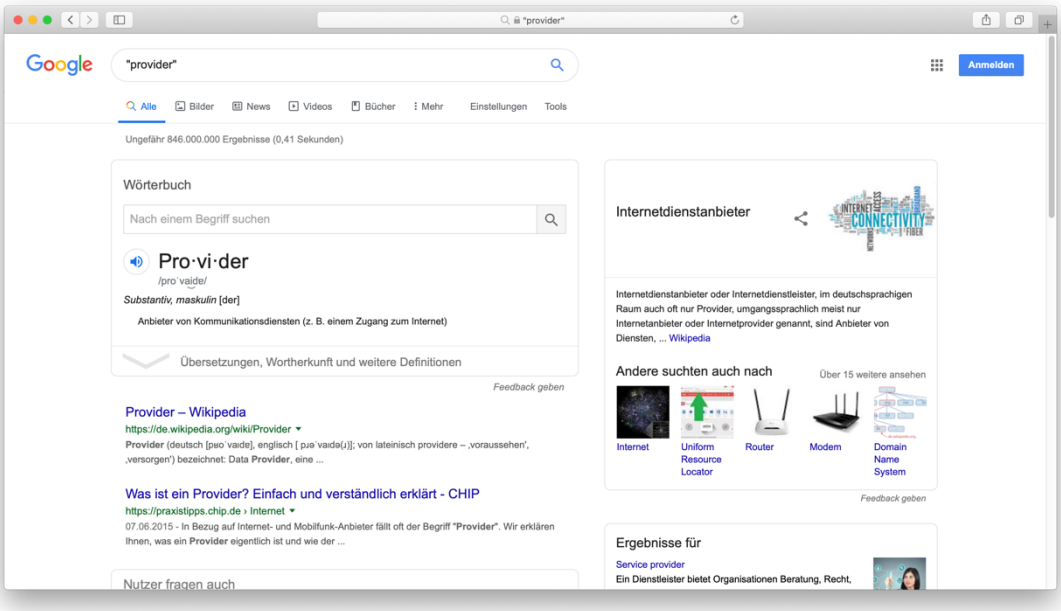
Provider:

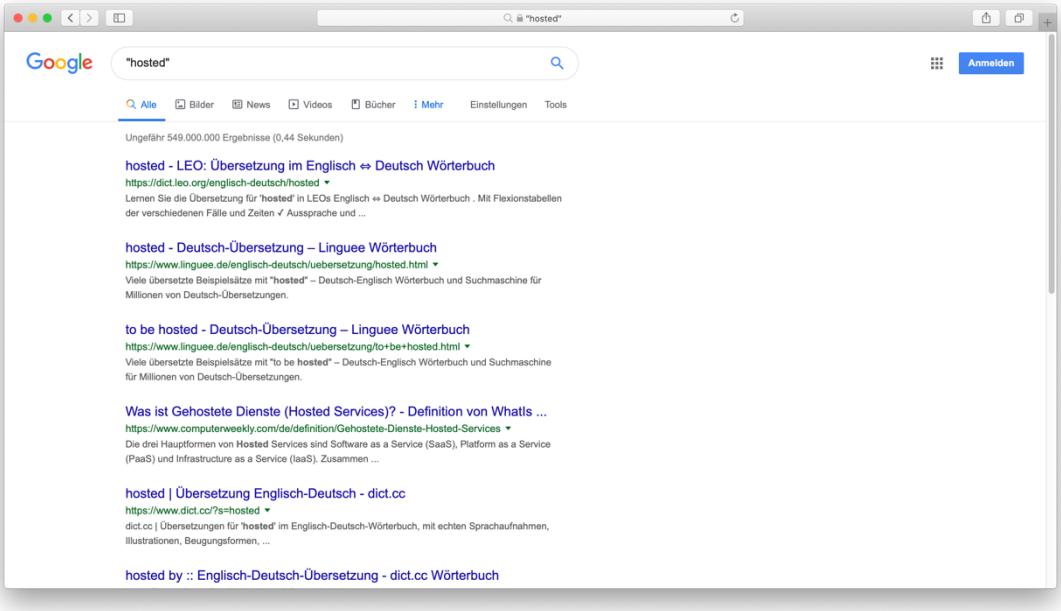
Hierfür wird eine Abfrage gemacht um den Provider des Servers zu finden.
Wie bereits bei der vorherigen Abfrage muss man hier auf gut Glück suchen.

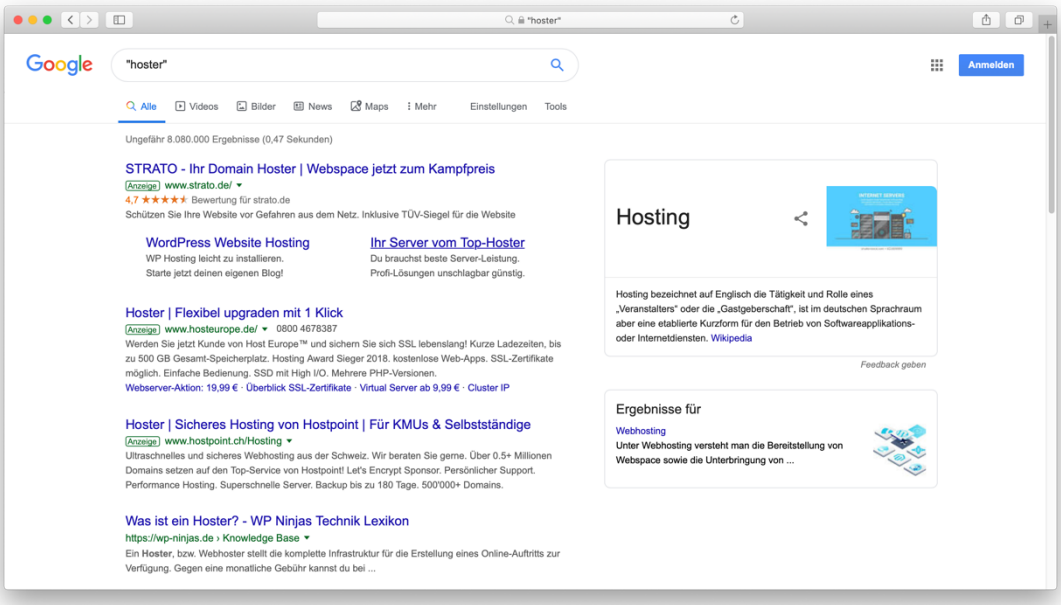
Allgemeine Abfrage: "provider"
Ergebnisse: ca. 846.000.000
Allgemeine Abfrage: "hosted"
Ergebnisse: ca. 549.000.000
Allgemeine Abfrage: "hoster"
Ergebnisse: ca. 808.000.000

“Sauf.ca”-Abfrage: site:sauf.ca "provider"
Ergebnisse: ca. 177
“Sauf.ca”-Abfrage: site:sauf.ca "hosted"
Ergebnisse: ca. 468
“Sauf.ca”-Abfrage: site:sauf.ca "hoster"
Ergebnisse: ca. 4

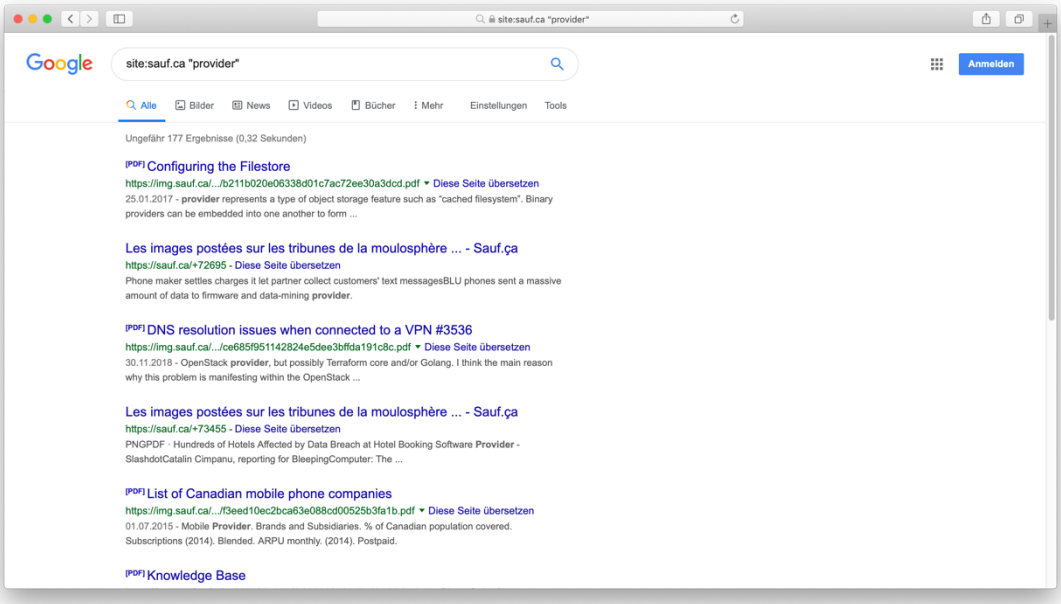
Allgemeine Abfragen

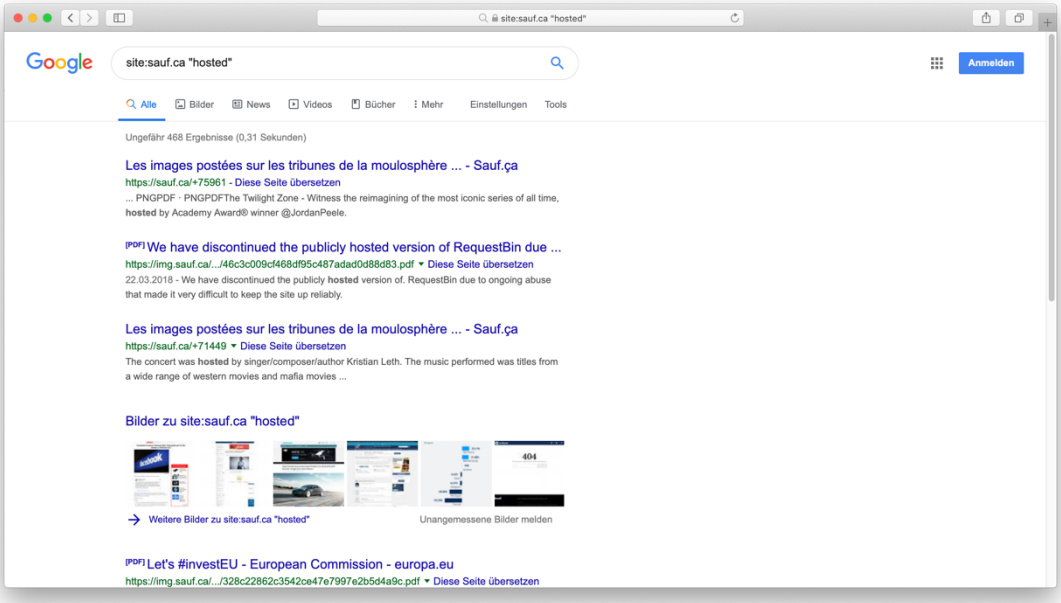


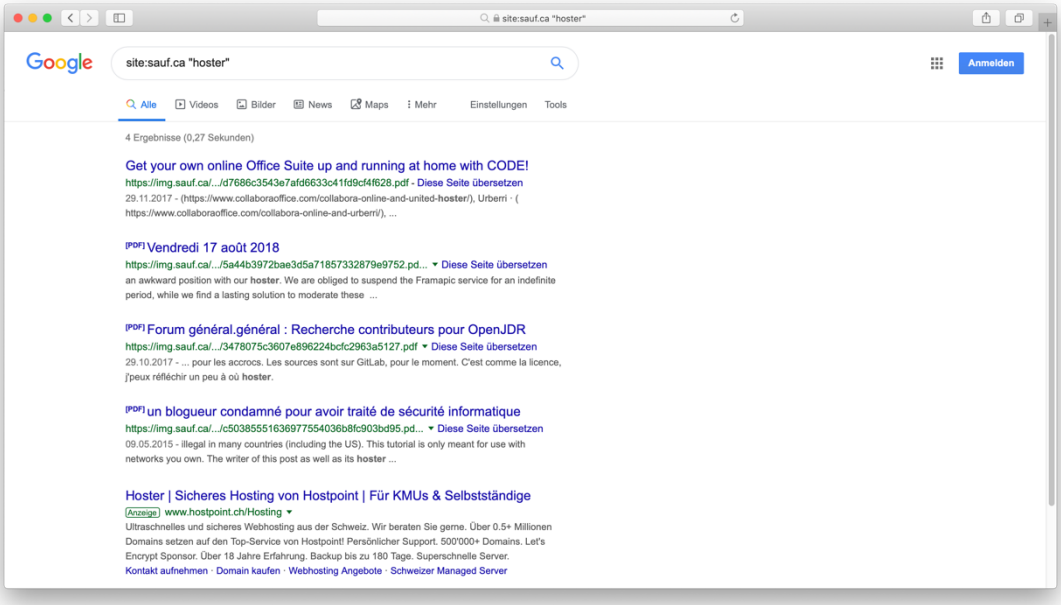

"hosted"
Google
"hosted"
Anmelden
Alle Bilder News Videos Bücher Mehr Einstellungen Tools
Ungefähr 549.000.000 Ergebnisse (0,44 Sekunden)
hosted - LEO: Übersetzung im Englisch ⇔ Deutsch Wörterbuch
https://dict.leo.org/englisch-deutsch/hosted
Lernen Sie die Übersetzung für 'hosted' in LEOs Englisch ⇔ Deutsch Wörterbuch . Mit Flexionstabellen der verschiedenen Fälle und Zeiten ✓ Aussprache und ...
hosted - Deutsch-Übersetzung – Linguee Wörterbuch
https://www.linguee.de/englisch-deutsch/uebersetzung/hosted.html
Viele übersetzte Beispielsätze mit "hosted" – Deutsch-Englisch Wörterbuch und Suchmaschine für Millionen von Deutsch-Übersetzungen.
to be hosted - Deutsch-Übersetzung – Linguee Wörterbuch
https://www.linguee.de/englisch-deutsch/uebersetzung/to+be+hosted.html
Viele übersetzte Beispielsätze mit "to be hosted" – Deutsch-Englisch Wörterbuch und Suchmaschine für Millionen von Deutsch-Übersetzungen.
Was ist Gehostete Dienste (Hosted Services)? - Definition von WhatIs ...
https://www.computerweekly.com/de/definition/Gehostete-Dienste-Hosted-Services
Die drei Hauptformen von Hosted Services sind Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS). Zusammen ...
hosted | Übersetzung Englisch-Deutsch - dict.cc
https://www.dict.cc/?s=hosted
dict.cc | Übersetzungen für 'hosted' im Englisch-Deutsch-Wörterbuch, mit echten Sprachaufnahmen, Illustrationen, Beugungsformen, ...
hosted by :: Englisch-Deutsch-Übersetzung - dict.cc Wörterbuch


"hoster"
Google
"hoster"
Anmelden
Alle Videos Bilder News Maps Mehr Einstellungen Tools
Ungefähr 8.080.000 Ergebnisse (0,47 Sekunden)
STRATO - Ihr Domain Hoster | Webspace jetzt zum Kampfpreis
Anzeige www.strato.de/
4,7 ★★★★★ Bewertung für strato.de
Schützen Sie Ihre Website vor Gefahren aus dem Netz. Inklusive TÜV-Siegel für die Website
WordPress Website Hosting
WP Hosting leicht zu installieren.
Starte jetzt deinen eigenen Blog!
Ihr Server vom Top-Hoster
Du brauchst beste Server-Leistung.
Profi-Lösungen unschlagbar günstig.
Hoster | Flexibel upgraden mit 1 Klick
Anzeige www.hosteurope.de/ 0800 4678387
Werden Sie jetzt Kunde von Host Europe™ und sichern Sie sich SSL lebenslang! Kurze Ladezeiten, bis zu 500 GB Gesamt-Speicherplatz. Hosting Award Sieger 2018. kostenlose Web-Apps. SSL-Zertifikate möglich. Einfache Bedienung. SSD mit High I/O. Mehrere PHP-Versionen.
Webserver-Aktion: 19,99 € · Überblick SSL-Zertifikate · Virtual Server ab 9,99 € · Cluster IP
Hoster | Sicheres Hosting von Hostpoint | Für KMUs & Selbstständige
Anzeige www.hostpoint.ch/Hosting
Ultraschnelles und sicheres Webhosting aus der Schweiz. Wir beraten Sie gerne. Über 0.5+ Millionen Domains setzen auf den Top-Service von Hostpoint! Let's Encrypt Sponsor. Persönlicher Support. Performance Hosting. Superschnelle Server. Backup bis zu 180 Tage. 500'000+ Domains.
Was ist ein Hoster? - WP Ninjas Technik Lexikon
https://wp-ninjas.de › Knowledge Base
Ein Hoster, bzw. Webhoster stellt die komplette Infrastruktur für die Erstellung eines Online-Auftritts zur Verfügung. Gegen eine monatliche Gebühr kannst du bei ...
Hosting
Hosting bezeichnet auf Englisch die Tätigkeit und Rolle eines „Veranstalters“ oder die „Gastgeberschaft“, ist im deutschen Sprachraum aber eine etablierte Kurzform für den Betrieb von Softwareapplikations- oder Internetdiensten. Wikipedia
Feedback geben
Ergebnisse für
Webhosting
Unter Webhosting versteht man die Bereitstellung von Webspace sowie die Unterbringung von ...

„Sauf.ca“-Abfragen







Wie man anhand der Screenshots sehen kann, wird wieder eine riesige Menge an Seiten geliefert und hier ebenfalls nur auf irgendwelche hochgeladen Dateien verweist, sodass sich hier nichts verwertbares finden lässt.

In diesem Fall lassen sich also nicht die vorangegangen Infos per Footprinting-tools herausfinden.

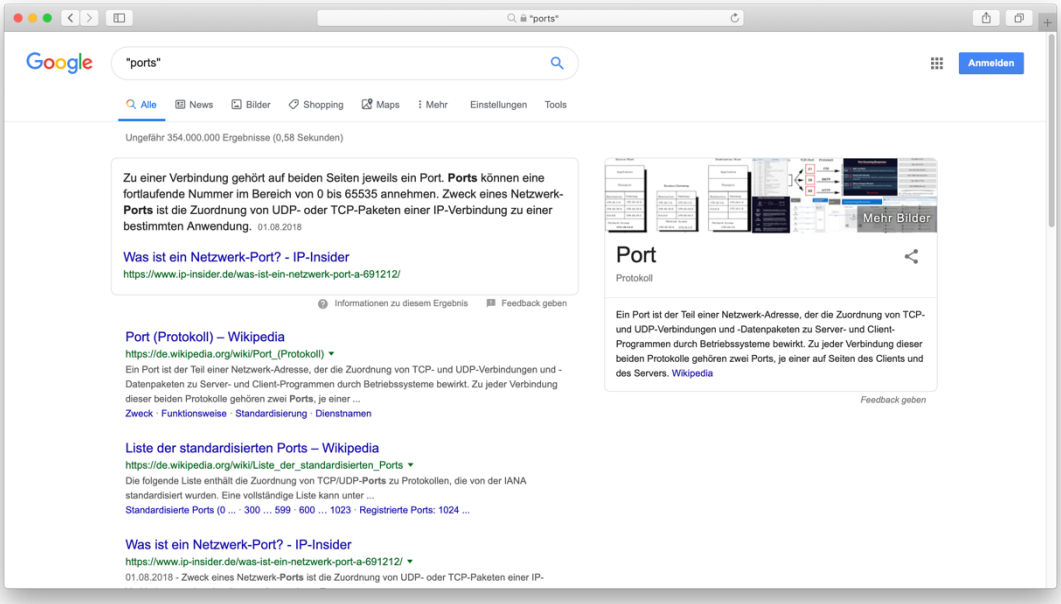
Offene Ports:

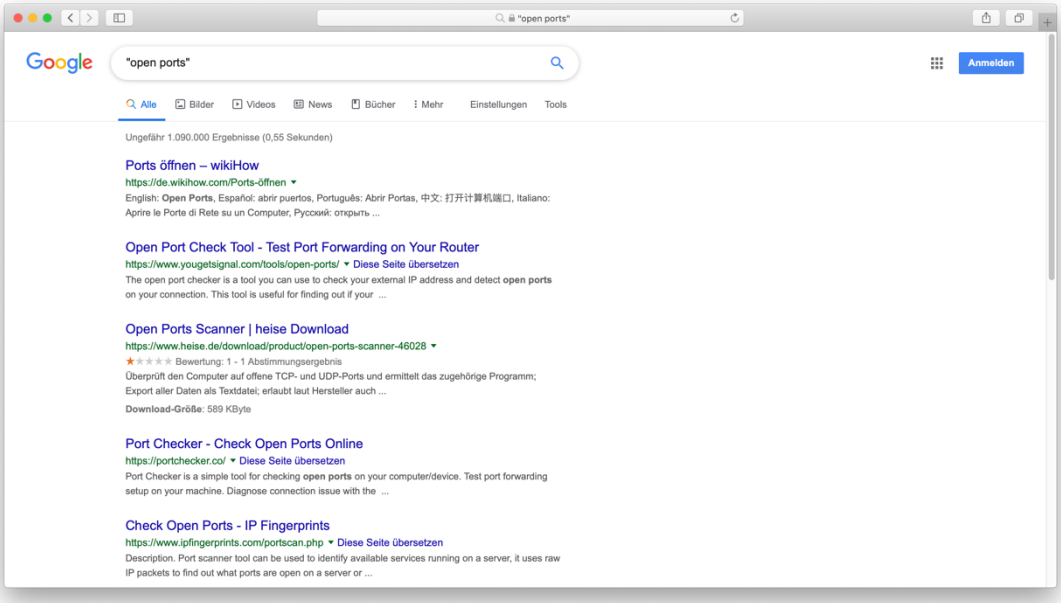
Hierfür wird eine Abfrage gemacht um offene Ports des Servers zu finden.

Allgemeine Abfrage: "ports"
Ergebnisse: ca. 354.000.000
Allgemeine Abfrage: "open ports"
Ergebnisse: ca. 1.090.000

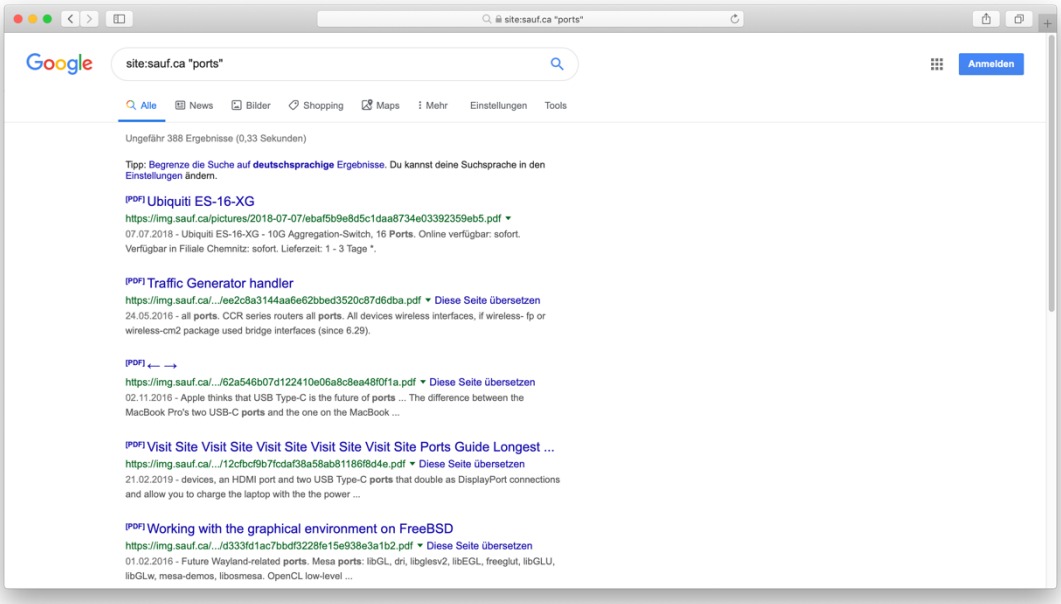
“Sauf.ca”-Abfrage: site:sauf.ca "ports"
Ergebnisse: ca. 388
“Sauf.ca”-Abfrage: site:sauf.ca "open ports"
Ergebnisse: ca. 3

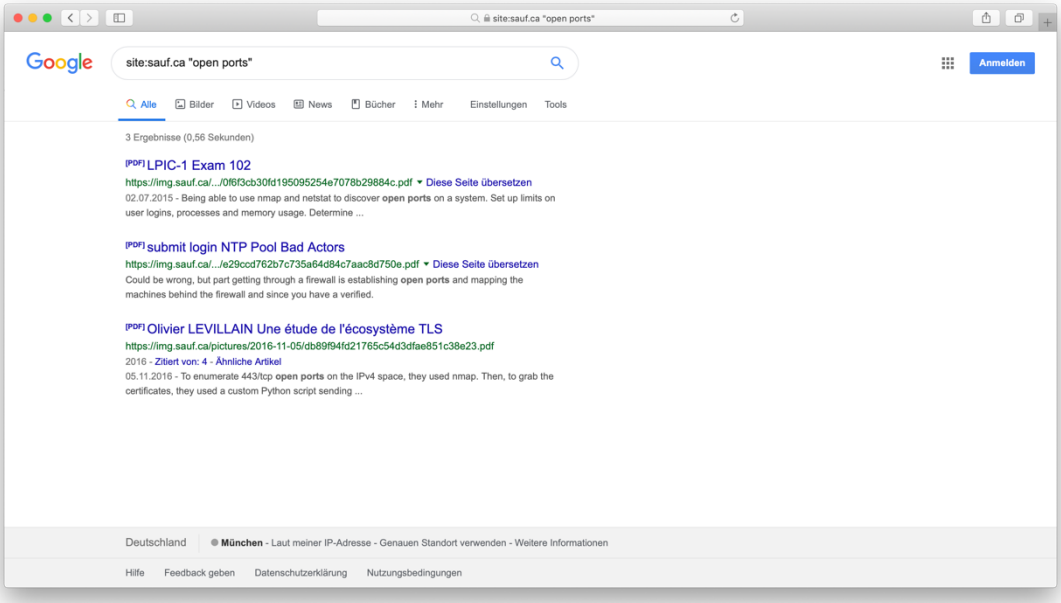
Allgemeine Abfragen:





„Sauf.ca“-Abfragen





Obwohl bei einer Abfrage nur drei Ergebnisse geliefert werden, bringen uns diese nicht weiter, da es wieder nur hochgeladene Dateien sind.

In diesem Fall lassen sich also nicht die vorangegangen Infos per Footprinting-tools herausfinden.

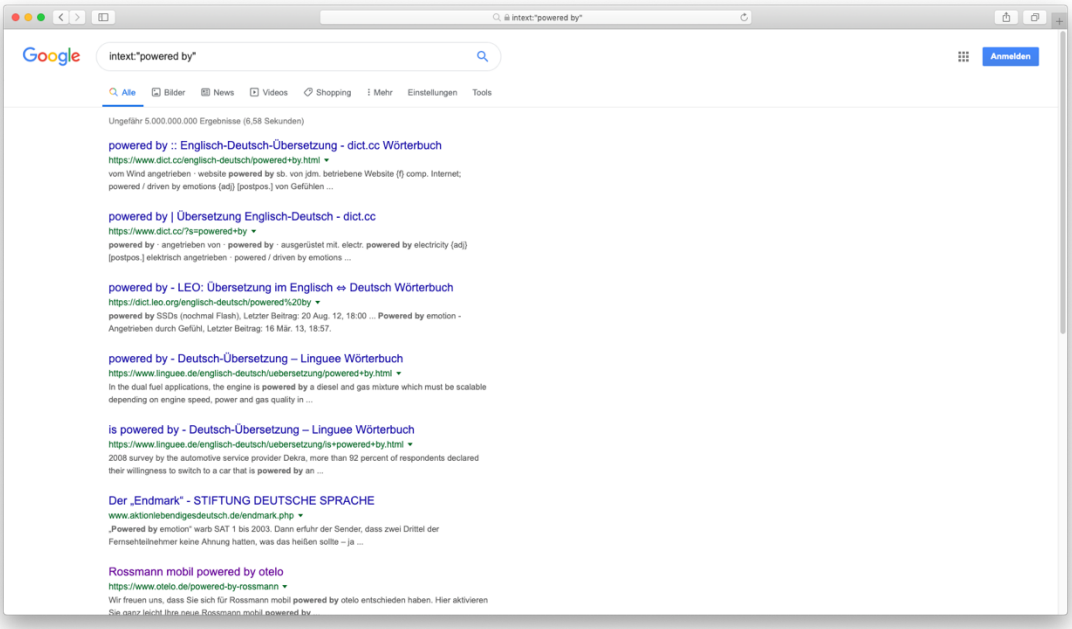
Software Versionen:

Bei so gut wie jedem Softwareanbieter wird ein „powered by XXXX“ im Text erwähnt. Ist diese Seite öffentlich zugänglich, so lässt sich leicht herausfinden um was für einen Server und welche Version es sich handelt.

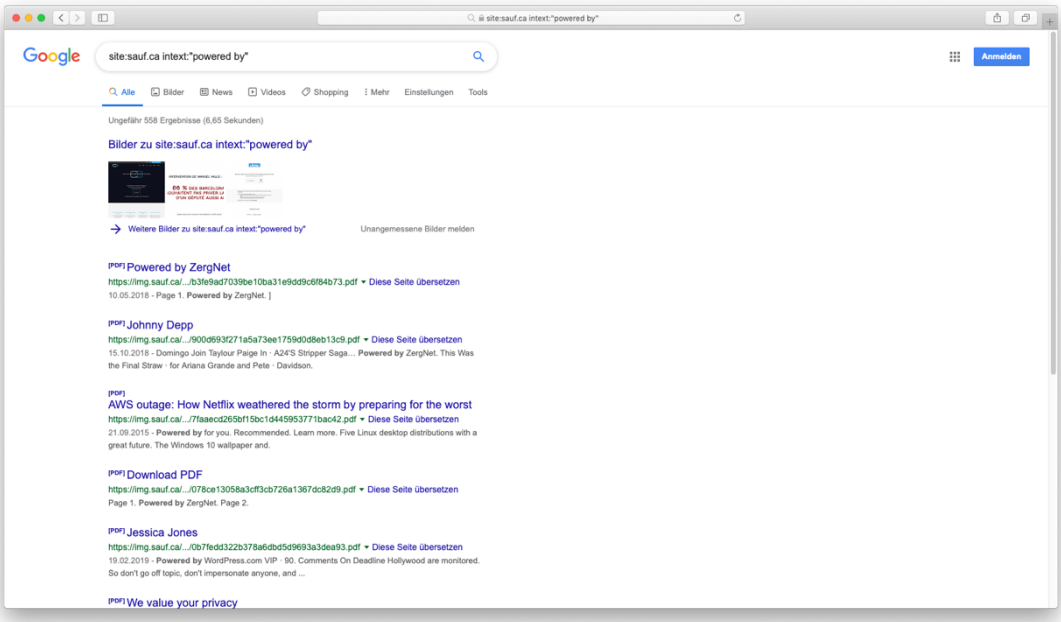
Allgemeine Abfrage: intext:"powered by"
Ergebnisse: ca. 5.000.000

“Sauf.ca”-Abfrage: site:sauf.ca intext:"powered by"
Ergebnisse: ca. 558

Allgemeine Abfrage:



„Sauf.ca“-Abfrage



Es lassen sich zwar Ergebnisse finden, diese sind aber in keinster Weise zufriedenstellend. Zum einen handelt es sich nur um hochgeladene Objekte, die nichts mit dem eigentlichen Server zu tun haben und zum anderen wird eine unübersichtliche Anzahl an Ergebnissen zurückgeliefert.

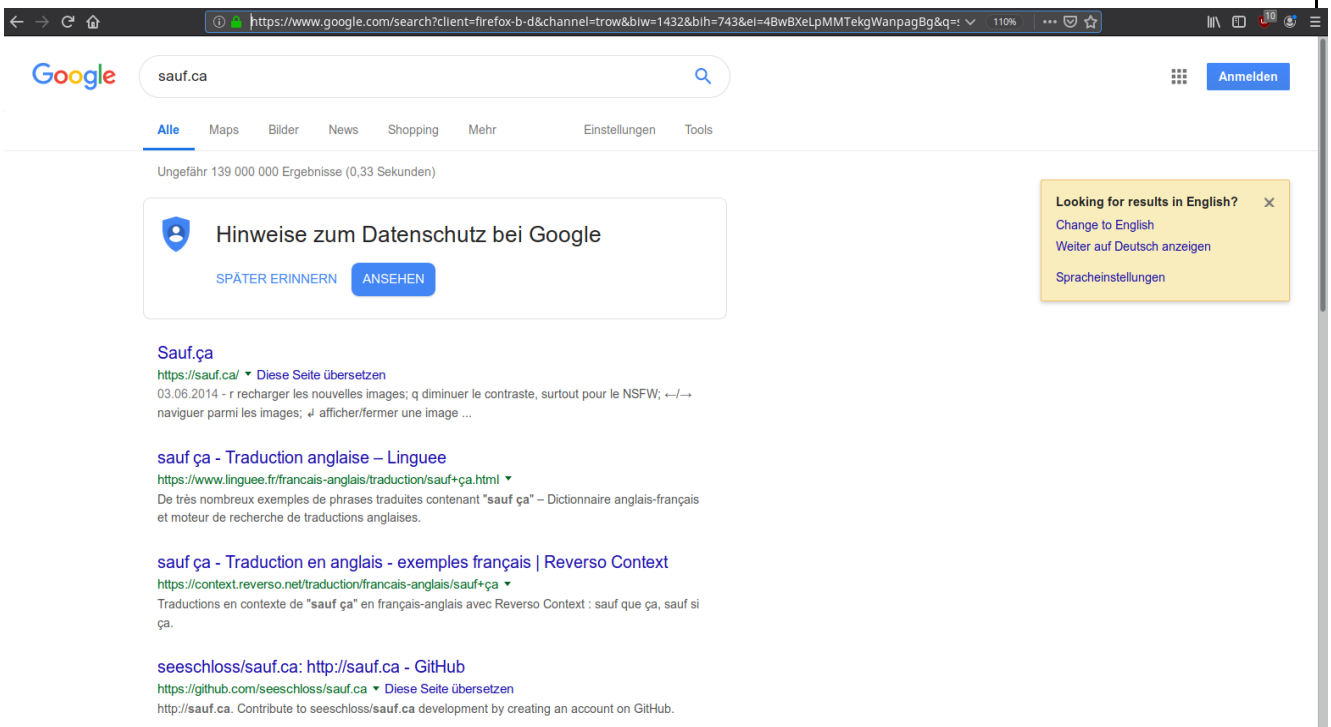
In diesem Fall lassen sich also nicht die vorangegangen Infos per Footprinting-tools herausfinden.

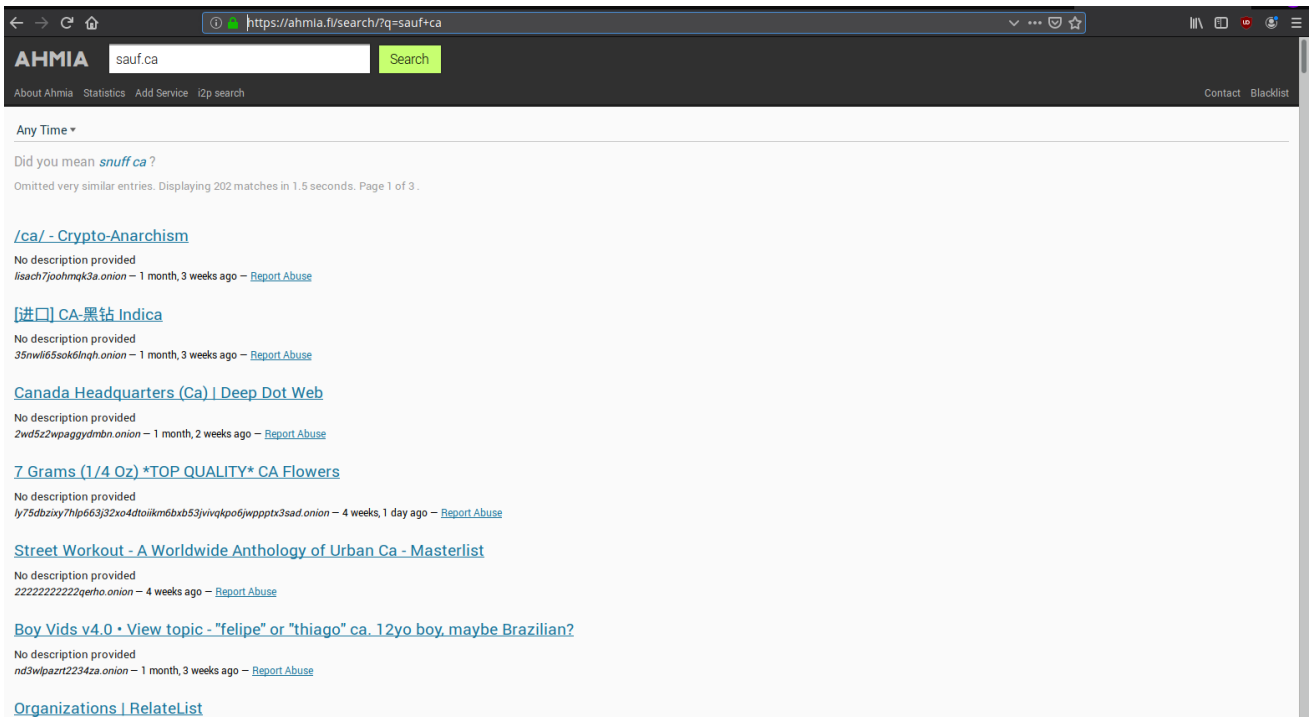
Abschließend lässt sich sagen, dass man zwar viele Informationen über eine Website herausfinden könnte, dies aber natürlich voraussetzt, dass der betroffene Server hinter der Website öffentlich zugänglich ist. Ist dies nicht der Fall und es lässt sich kein Zugriff darauf ermöglichen, wird es sehr schwer an die Informationen heranzukommen.

Analyse und Dokumentation der Seite “sauf.ca”

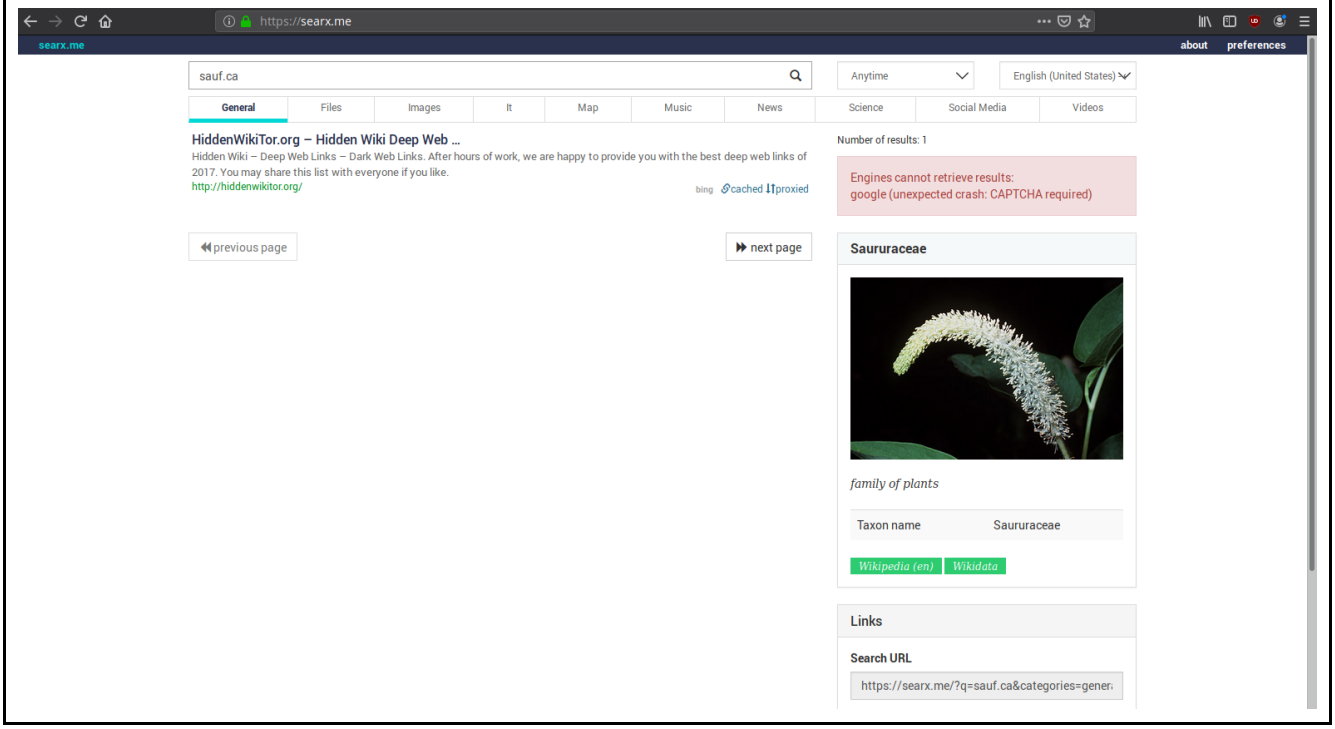
zu 4. Analyse der URL durch Abfragen in diversen Suchmaschinen im Dark Web

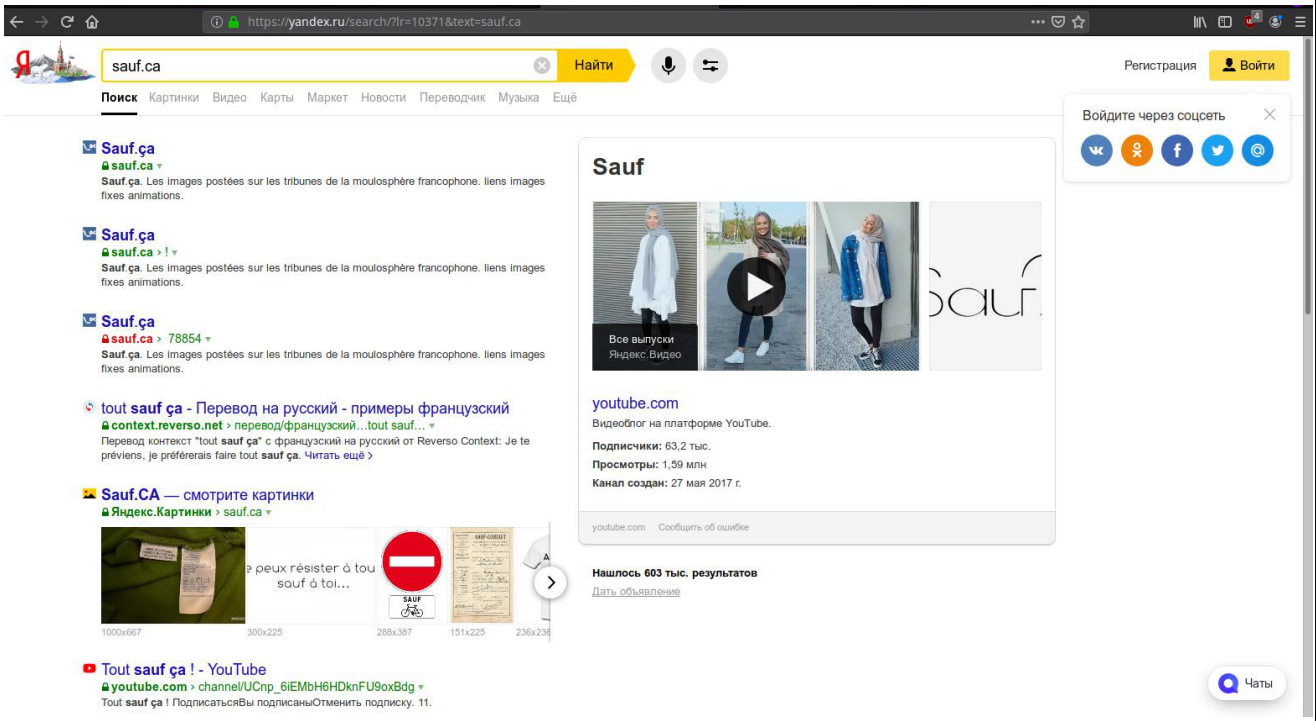
Datum der Recherche	verwendete Suchmaschine	verwendete Suchparameter / IP / etc.	Ergebnis der Suche (Screenshot)
12.06.2019 19:10:00 +0200	google.com	ohne / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	Screenshot (siehe unten)
12.06.2019 19:29:00 +0200	ahmia.fi	ohne / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	Screenshot (siehe unten)

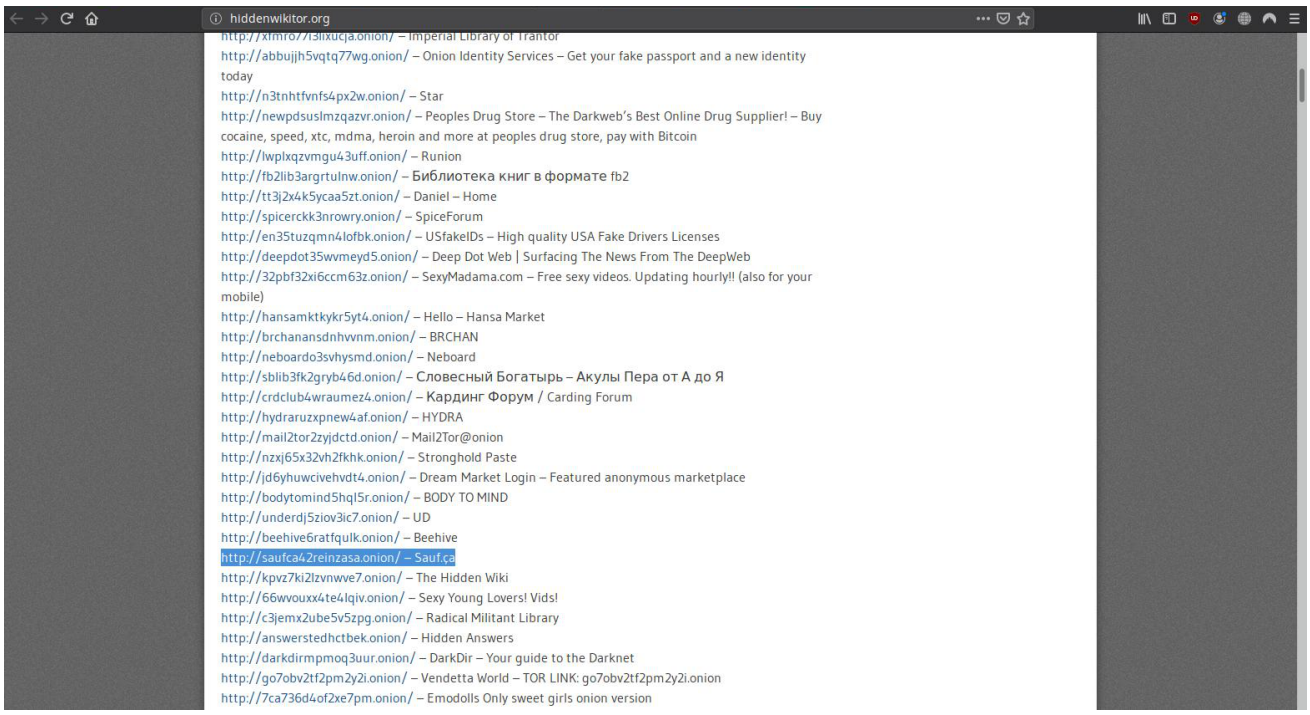




12.06.2019 19:35:00 +0200	searx.me	ohne / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	Screenshot (siehe unten)

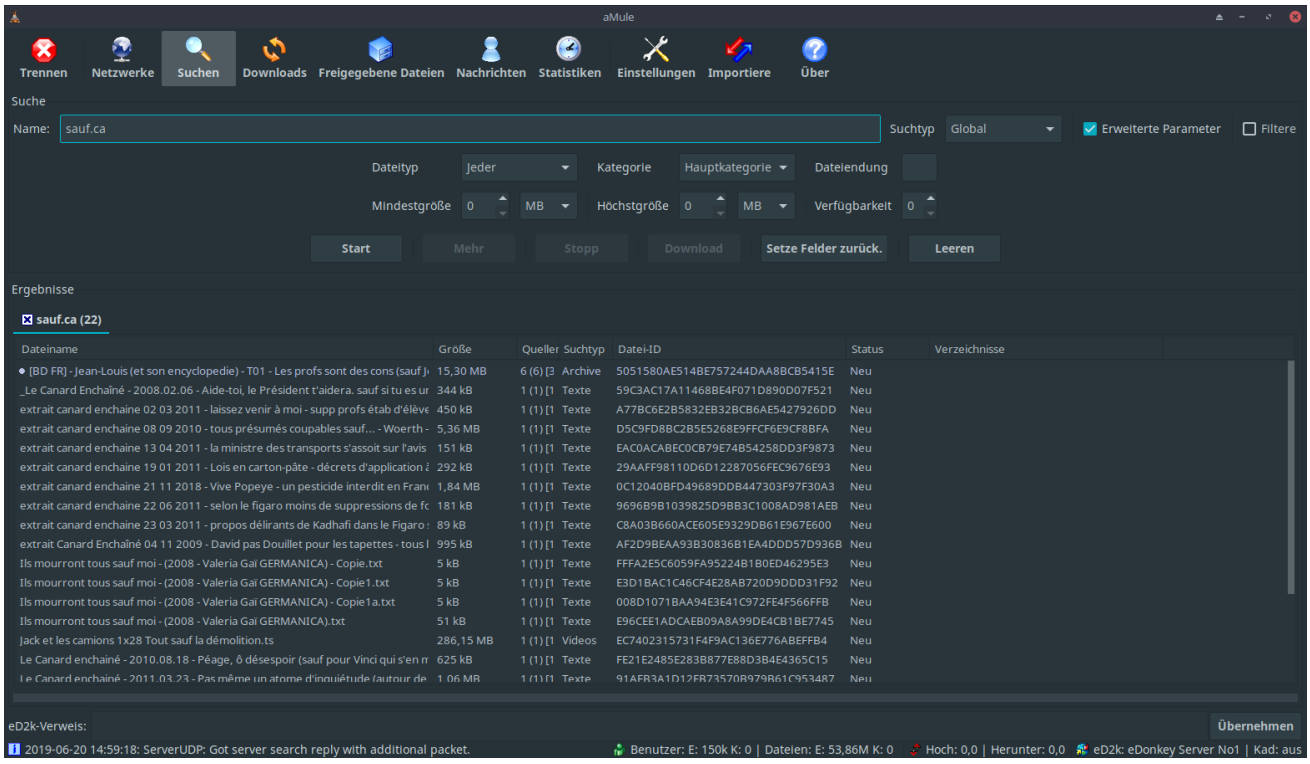


12.06.2019 19:39:00 +0200	yandex.ru	ohne / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	Screenshot (siehe unten)
			
12.06.2019 19:48:00 +0200	hiddenwikitor.org	ohne / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	Screenshot (siehe unten)



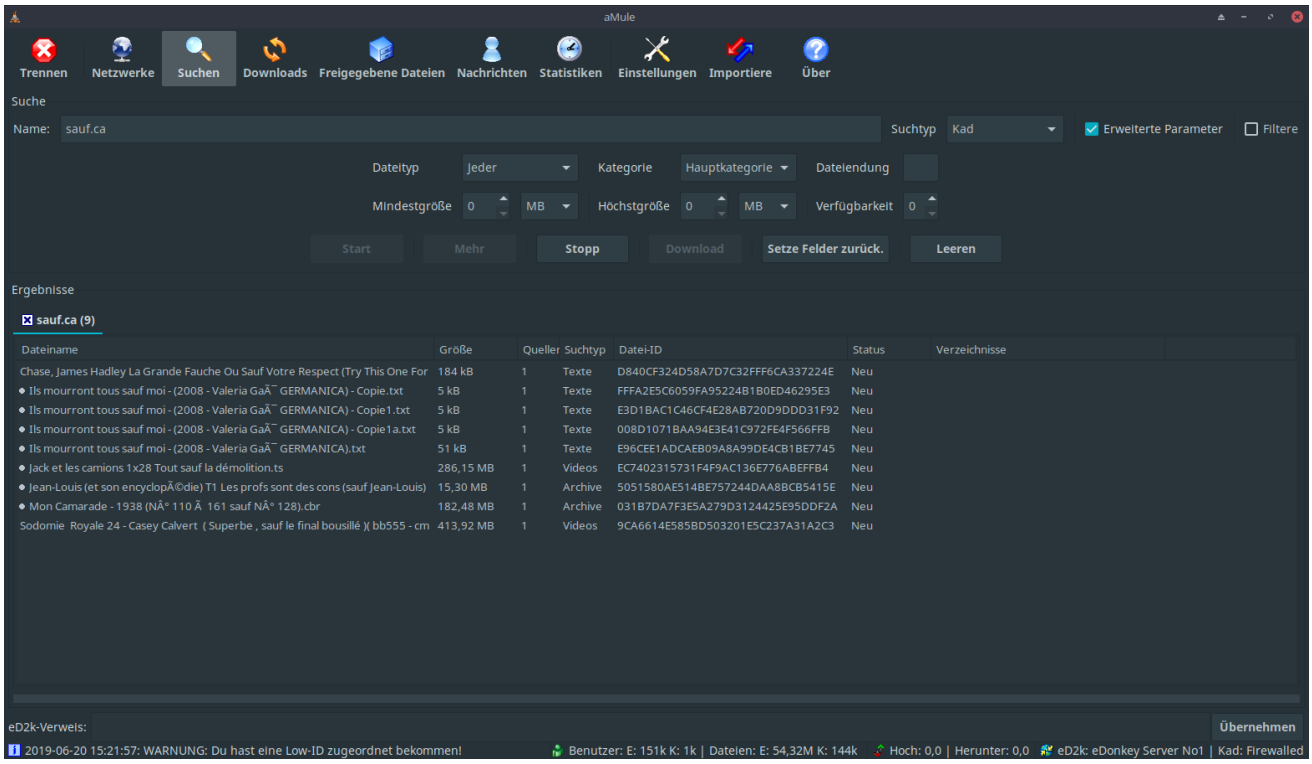
12.06.2019 19:59:00 +0200	github.com	sauf.ca / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	https://github.com/seeschloss/sauf.ca/commits?author=seeschloss https://github.com/seeschloss Keine weiteren Daten zum Ersteller “Seeschloss” vorhanden. Standort evtl. Region Port-aux-Français Erstelldatum: 26.05.2014
16.06.2019 14:01:00 +0200	benefito.com	sauf.ca / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	http://sauf.ca.benefito.com/ Zugriffstatistiken der Webseite

16.06.2019 14:08:00 +0200	easycounter.com	sauf.ca / 77.119.130.58 / TOR-Browser “Linux Firefox 67.0 privater Modus”	https://www.easycounter.com/report/sauf.ca
19.06.2019 15:17:50 +0200	aMule	sauf.ca (Global)	Screenshot (siehe unten)



mehrere Textdateien, Archive, Videos im weiteren Kontext gefunden

19.06.2019 15:19:10 +0200	aMule	sauf.ca (KAD)	Screenshot (siehe unten)



Teilergebnis der globalen Suche

besondere gefundene Informationen:

Dateien online:

https://sauf.ca/feeds/all.tsv Tabelle mit Informationen

http://sauf.ca/?tut_tut nicht öffentliche Webseite mit div. Links

zu 5. Dokumentation der Recherche im Dark-Web

Für die Analyse im Dark-Web wurde der TOR-Browser in seiner aktuellen Version 8.5.1 64 bit für Linux verwendet.

Die Spiegelung der Webseite erfolgte durch das Programm “WebHTTrack Website Copier” am 13.06.2019 bis 04:18 Uhr.
Die gesammelte Datenmenge beläuft sich auf etwa 4.2 GB mit einer Directorytiefe von 10 und einer Linktiefe von 5.
Es wurden hierbei 709 Dateien gespeichert.
Eine Analyse der “index.html” wurde gem. Aufgabenstellung nicht durchgeführt.
Es befinden sich weiterhin diverse Logdateien in Textform zur Analyse im gespeicherten Datenbestand.

Die Recherche bzgl. des Seitennamens im Dark-Web ergab, dass die Webseite in unterschiedlichen Foren gespeichert und als Informationsquelle gelistet ist. Offensichtlich wurden auf der Webseite nicht-öffentliche Informationen im Quelltext der HTML-Seiten abgelegt, die nicht direkt auf einem Browser angezeigt werden.
Konkrete Hinweise auf den Betreiber der Webseite gibt es im öffentlichen Bereich nicht. Es wird davon ausgegangen, dass der Betreiber der Seite anonym bleiben möchte und eine gewisse Expertise dahingehend besitzt.
Augenscheinlich wird zumindest gegen eine Impressumspflicht verstoßen.

Eine strafrechtliche Bewertung des Inhaltes wurde jedoch nicht durchgeführt.
Es handelte sich dabei um Textnachrichten.
Weiterhin sind diverse Links zu externen Inhalten auf der Startseite vorhanden.
Eine strafrechtliche Relevanz der Verlinkungen wurde nicht geprüft.
Es handelt sich augenscheinlich um Links zu Videodateien, Textdateien und Webseiten mit thematischer Relevanz für den Ersteller in Form einer Linksammlung.
Ein Impressum ist auf der Seite oder auch im Quelltext nicht vorhanden.
Konkrete Hinweise auf den Ersteller der Seite gibt es nicht.
Dieser ist vermutlich dem deutsch-französichen Sprachraum zuzuordnen.
Auch im verborgenen Quelltext gibt es keine Hinweise auf den Autor.
Eine IP-Recherche ergab, dass die URL in Panama registriert wurde.
Der Dateninhalt verweist jedoch auf einen Provider in Deutschland:

Domain: sauf.ca **IP-Adresse:** 176.9.123.245 **Provider:** Hetzner Online AG
(Quelle: utrace.de)

Abschließend wurde das für Sharing-Zwecke übliche aMule-Netzwerk (Kademlia und eDonkey) auf Hinweise der Seite durchsucht (siehe Tabelle “Screenshots”). Dabei wurden Ergebnisse erzielt, die auf geringe Sharing-Aktivitäten schließen lassen.
Es konnten 21 Textdateien, 4 Archivdateien und 2 Videos mit Relevanz gefunden werden.
Eine nähere Analyse der einzelnen Dateien wurde nicht durchgeführt.

Als Zwischenergebnis lässt sich darstellen, dass im versteckten Bereich des Internet diverse Hinweise auf das Rechercheziel vorhanden sind. Der Betreiber der Webseite konnte jedoch auf diesem Wege nicht ausfindig gemacht werden. Hier wäre eine Anfrage beim Provider zielführend.
Auch auf die Nutzer der Webseite gibt es keine weiteren Hinweise. Die Seite wird nach Zugriffstatistik benefito.com überwiegend aus Frankreich (45,9 %) und USA (18,0%) aufgerufen.
Es erfolgen dazu 4- bis 8-Tausend Aufrufe pro Monat.
Damit ist die Seite nicht mehr als unbekannt einzustufen.