Le attività investigative nel deepweb e nel darkweb

Scuola Superiore della Magistratura – 15 febbraio 2023

Who's the dude

Isp. Davide 'Rebus' Gabrini

GABINETTO REGIONALE POLIZIA SCIENTIFICA PER LA LOMBARDIA
UNITÀ INDAGINI ELETTRONICHE

Precedentemente:

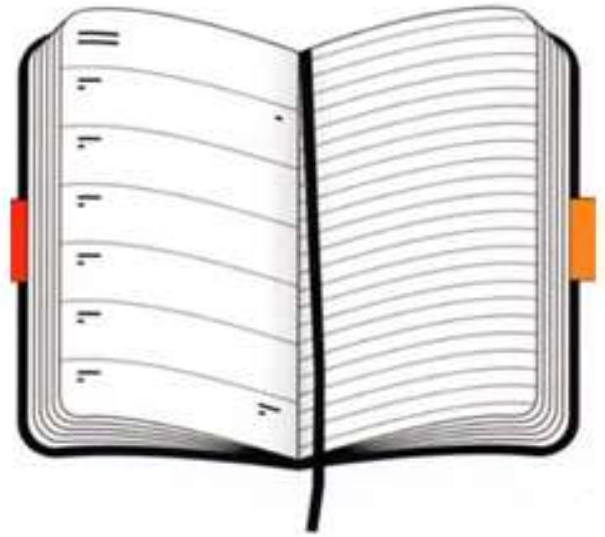
- Squadra Reati Informatici c/o Procura di Milano
- Polizia Postale, Compartimenti di Torino e Milano

Oltre a ciò:

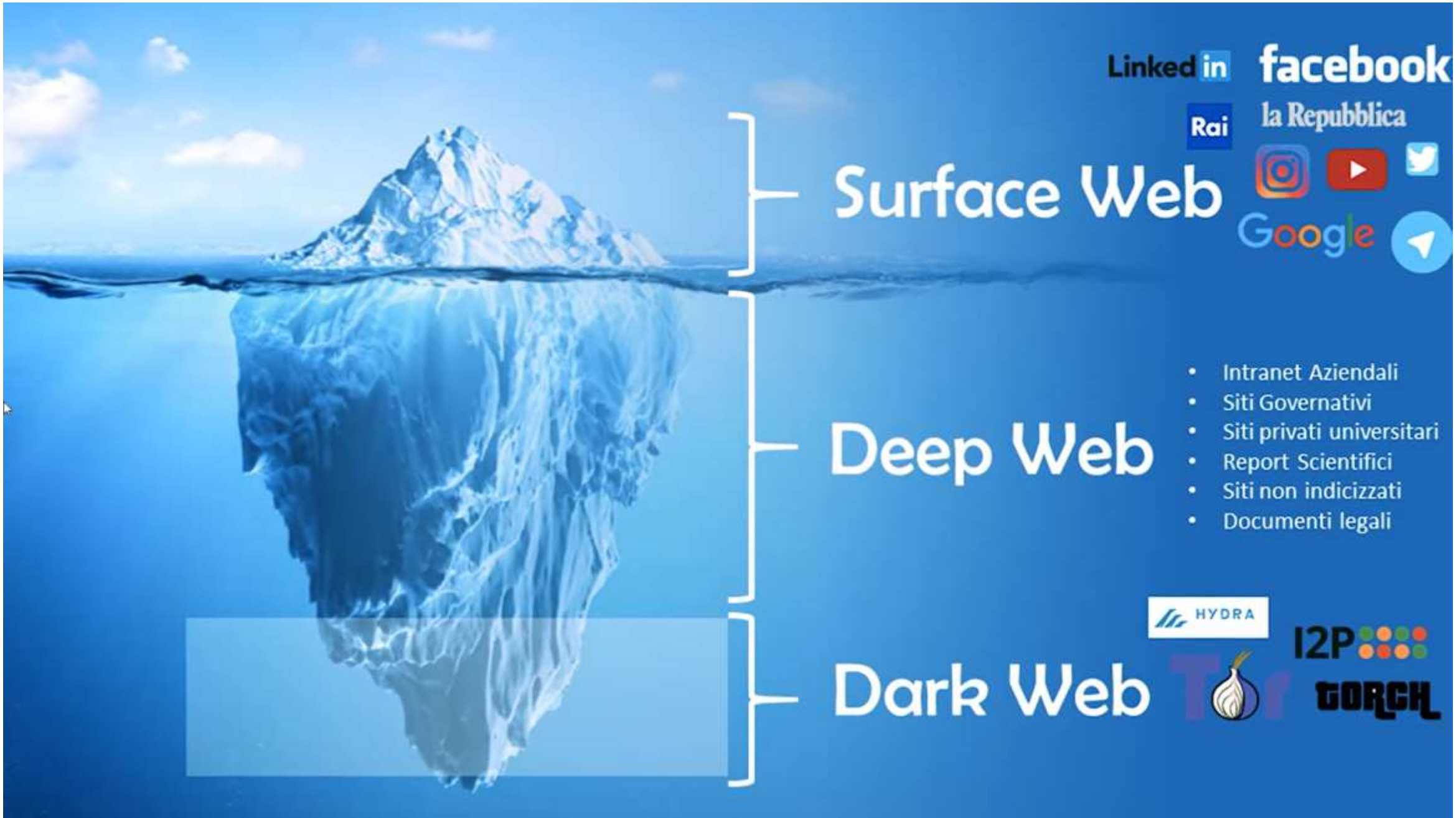
- Professore a contratto in Informatica e Sicurezza Informatica presso il Dipartimento di Giurisprudenza dell'Università degli Studi di Pavia, A.A. 2022/2023
- Collaboratore del Laboratorio di Informatica Forense dell'Università degli Studi di Pavia, afferente al Laboratorio Nazionale di Cybersecurity
- Contributor di Tsurugi Linux, P.M. di Bento
- Socio fondatore di Inclusive Hacker Framework
- Curatore della newsletter Rebus' Digest

Agenda

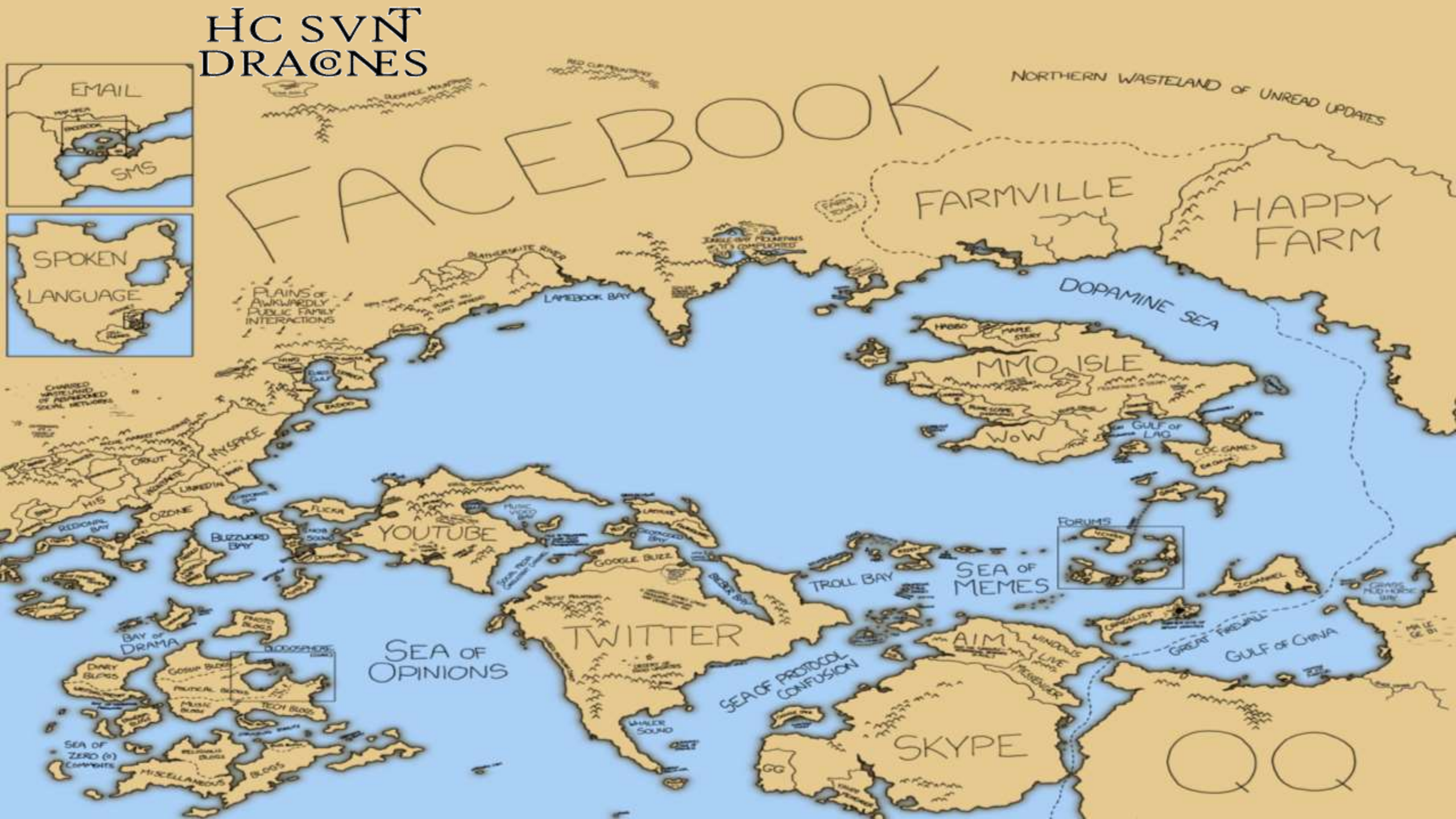
- Definizioni
  - Clearnet
  - Deepweb
  - Darkweb
  - Darknet
- Approcci investigativi
  - Attivi, passivi, ibridi
  - OSINT e cyber intelligence
  - Attacchi di deanonimizzazione



Clear, Deep e Dark web



Come funziona un motore di ricerca


HC SVNT DRACONES
EMAIL
SMS
SPOKEN LANGUAGE
FACEBOOK
NORTHERN WASTELAND OF UNREAD UPDATES
FARMVILLE
HAPPY FARM
DOPAMINE SEA
MMO ISLE
WoW
GULF OF LAG
LAMEBOOK BAY
PLAINS OF AWKWARDLY PUBLIC FAMILY INTERACTIONS
MYSPACE
ORKUT
HI5
XDRIVE
LINKEDIN
BLIZZARD BAY
YOUTUBE
GOOGLE BUZZ
TROLL BAY
SEA OF MEMES
FORUMS
TWITTER
SEA OF OPINIONS
BAY OF DRAMA
SEA OF PROTOCOL CONFUSION
AIM
WINDOWS LIVE MESSENGER
SKYPE
GG
QQ
GULF OF CHINA
GREAT FIREWALL
WHALE SOUND
SEA OF ZERO (0) COMMITS
TECH BLOGS
MISCELLANEOUS BLOGS

Limiti dei crawler convenzionali

- Rispetto del protocollo di esclusione robot (Robots Exclusion Standard)
  - Un file *robots.txt* indica ai crawler dei motori di ricerca a quali URL del sito possono o non possono accedere
- Rispetto del meta tag *noindex*
  - <meta name="robots" content="**noindex, nofollow**" />
- Accesso solo a pagine linkate da altre pagine
- Accesso solo a determinati tipi di contenuto
  - Testo nelle pagine HTML
  - Documenti Office e PDF
  - Immagini e video
- Esclusione dalle aree riservate
  - login, captcha, paywall…
- Tutto ciò che non è indicizzato, tutto ciò che non è raggiungibile è gia deepweb

Investigare nel surface e nel deep web

OSINT: Open Source Intelligence

- Attività di raccolta di informazioni mediante la consultazione di fonti di pubblico accesso, in contrapposizione a fonti segrete o coperte.
- L'OSINT si distingue dalla ricerca perché applica un processo di gestione delle informazioni con lo scopo di creare una specifica conoscenza in supporto a una specifica decisione.

Cyber Intelligence

- Integrando l'OSINT con ulteriori fonti digitali non pubbliche, si possono ottenere risultati più approfonditi e qualificati
  - Banche dati riservate
  - Strumenti di ricerca dedicati
  - Scansioni attive sul target

Modalità

Cyber Intelligence

Attiva	Passiva	Semi-passiva
Proactive Intelligence (ingegneria sociale, attività undercover, exploit, spyware ecc.)	Open Source Intelligence Intercettazioni SIGINT, EMINT, ecc.	Modalità attiva ma sotto la soglia di rilevamento

Aspettative, miti, realtà

- False concezioni sulla cyber intelligence:
  - Tutto è sorvegliato sempre e comunque grazie alle tecnologie avanzate (foto satellitari, videocamere onnipresenti, log…)
  - Si può fare intelligence globale senza muoversi dalla propria scrivania (Echelon…)
  - Tutti i sistemi tecnologici sono vulnerabili, basta saper imporre le mani al modo giusto
- La realtà:
  - La cyber intelligence è un utile supporto ma non una alternativa alle forme di intelligence più tradizionali (agenti sul territorio, social engineering, intercettazioni…)
  - È comunque sorprendente quello che si può ottenere con metodo e con strumenti di pubblico dominio

Strumenti specializzati

- Ottenere di più dai comuni motori di ricerca
  - Google dorks
- Costruire i proprio indici su misura
  - Crawler "spregiudicati"
  - Strumenti di enumerazione
- Consultare banche dati specialistiche/riservate
  - Pipl, Spokeo…
  - Sync.me, TrueCaller…
  - Shodan
  - DomainTools
  - Wiggle
  - Blockchain intelligence

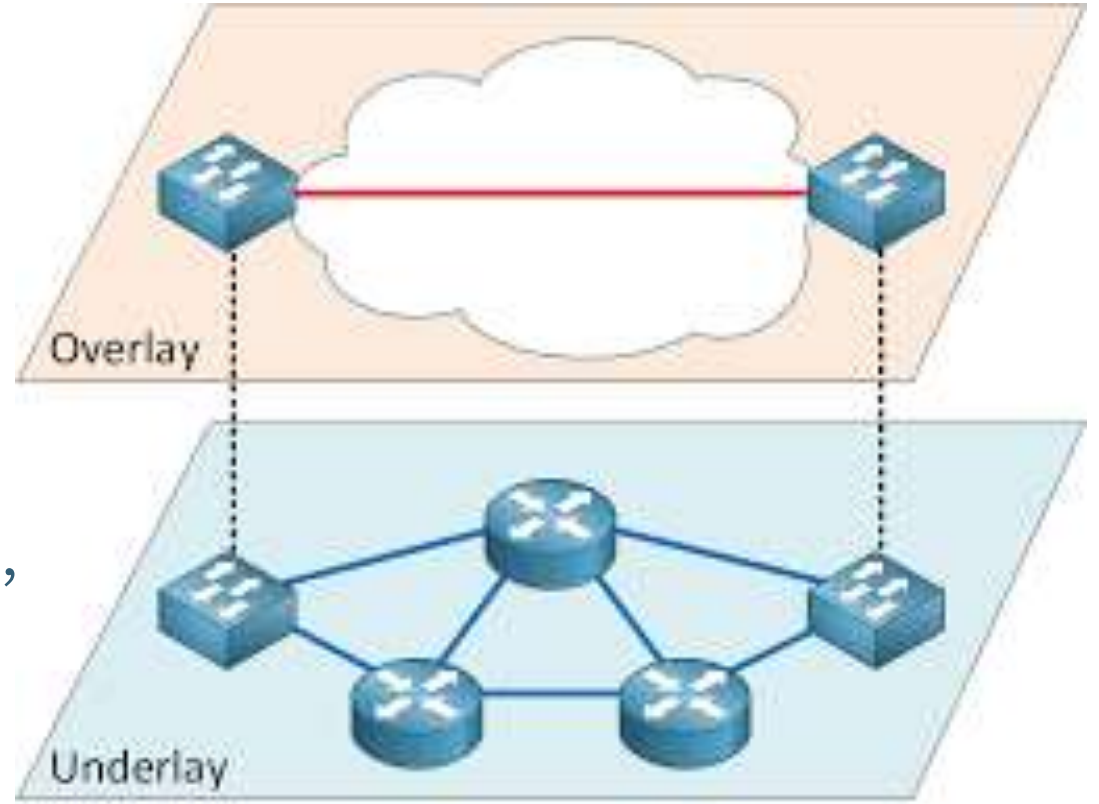
DARK WEB

Dark web, darknet e dark market

- Il dark web è quindi una piccola parte del deep web, a cui si accede con software specifici in particolari configurazioni
- Le darknet sono *overlay network*: reti virtuali cifrate che utilizzano Internet come rete di trasporto

- Una darknet può avere dimensioni globali e accesso pubblico, come **Tor**, **I2P** e **Freenet**

- Oppure essere una piccola rete privata, riservata a utenti che si conoscono e si fidano (friend to friend peer-to-peer), come GigaTribe, RetroShare, OneSwarm



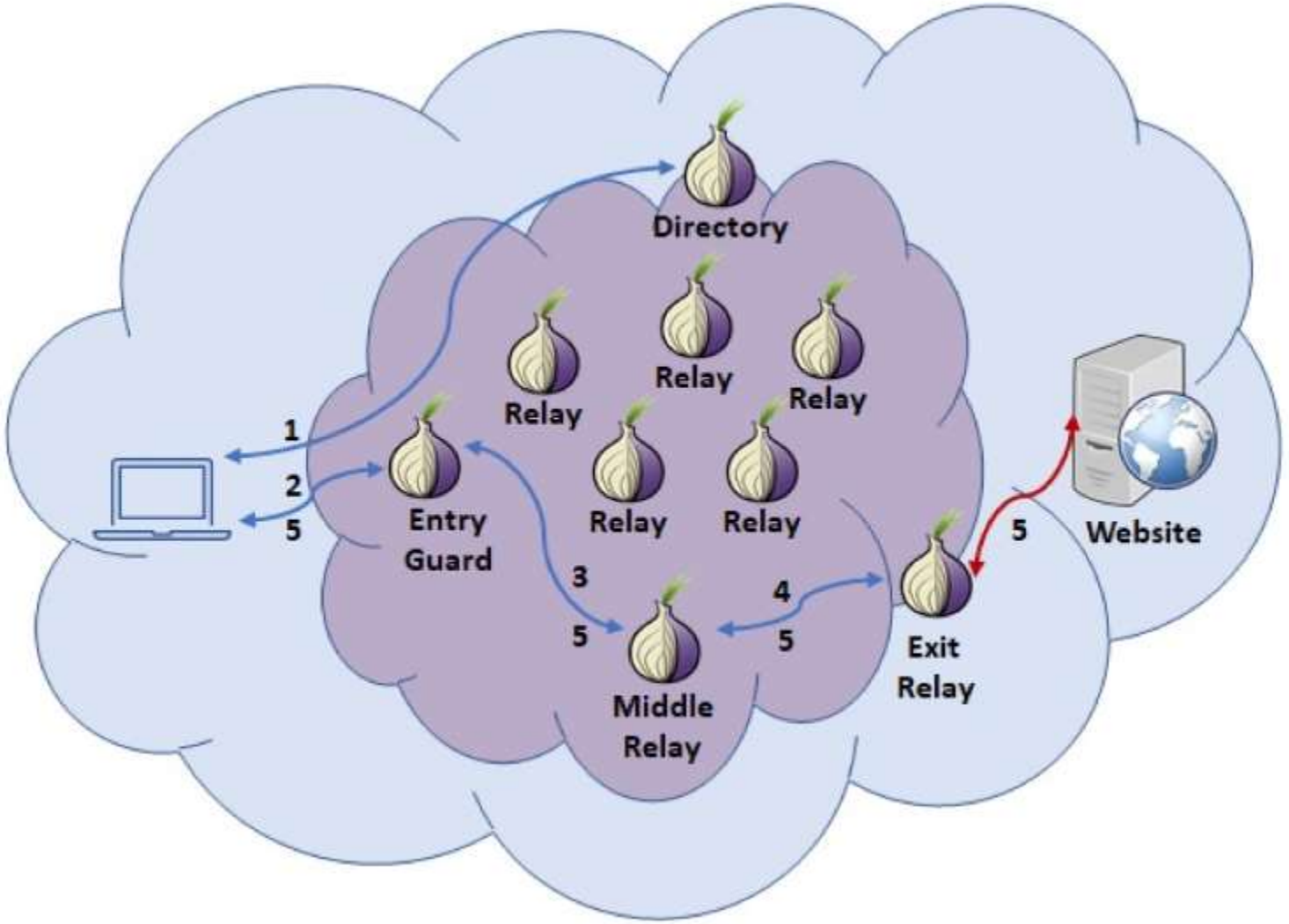
The Onion Router

- Tor è un software libero, disponibile per qualsiasi sistema operativo, che permette l'accesso a una rete virtuale basata su protocolli crittografici
- È concepito per garantire anonimato robusto e resistenza alle intercettazioni
- All'interno della rete Tor è possibile utilizzare qualsiasi protocollo applicativo (chat, mail, VoIP…) ma il più utilizzato è HTTP per la navigazione web
- La principale interfaccia utente è quindi un normale browser web, ma è più comune l'utilizzo di Tor Browser

Tor | Browser

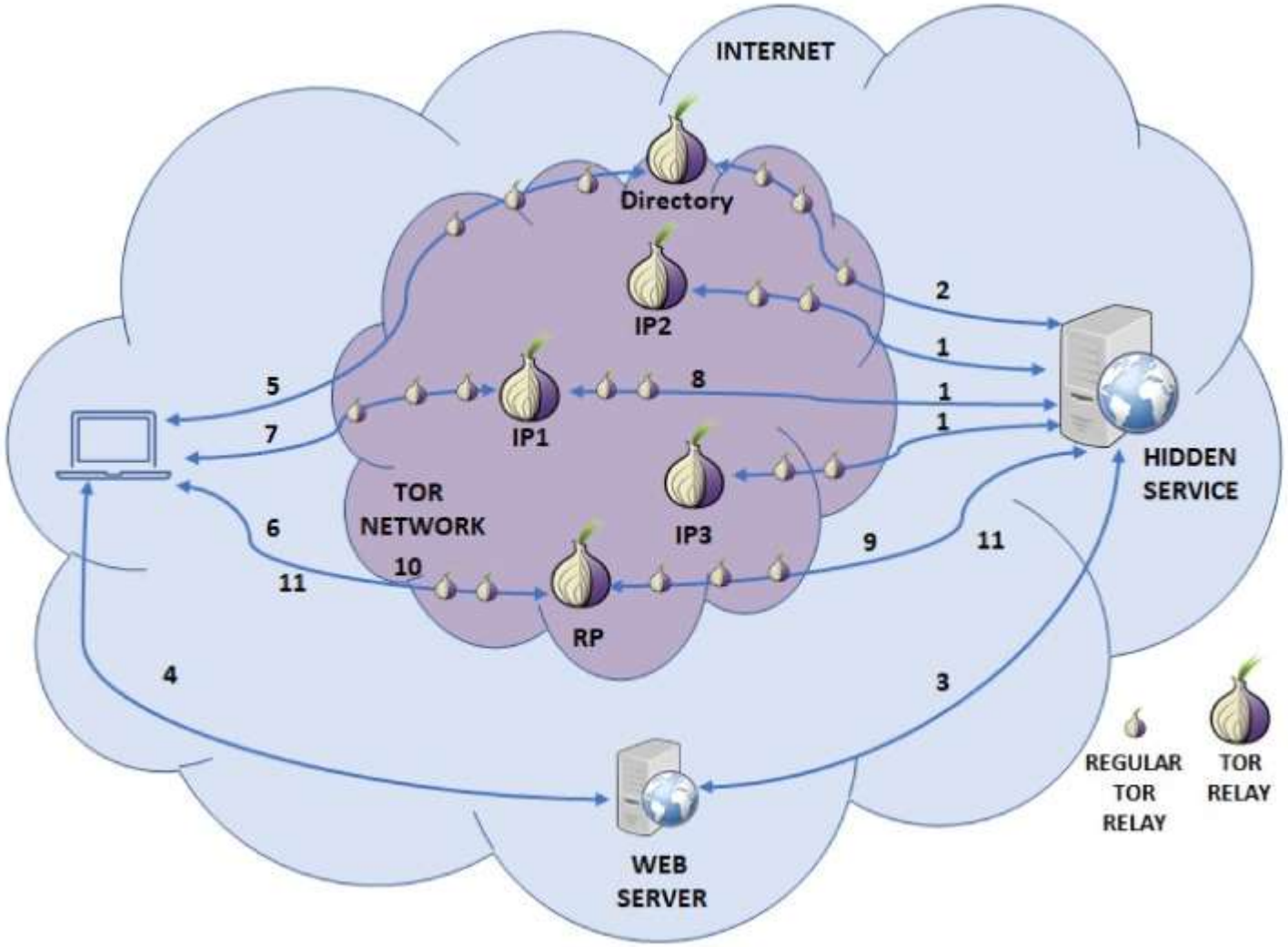
Tor circuit

- La rete è mantenuta da migliaia di nodi messi a disposizione da volontari, che agiscono da relay



Tor hidden service

- Con una procedura complessa, è possibile fornire dei servizi all'interno della rete Tor rimanendo anonimi (hidden service)

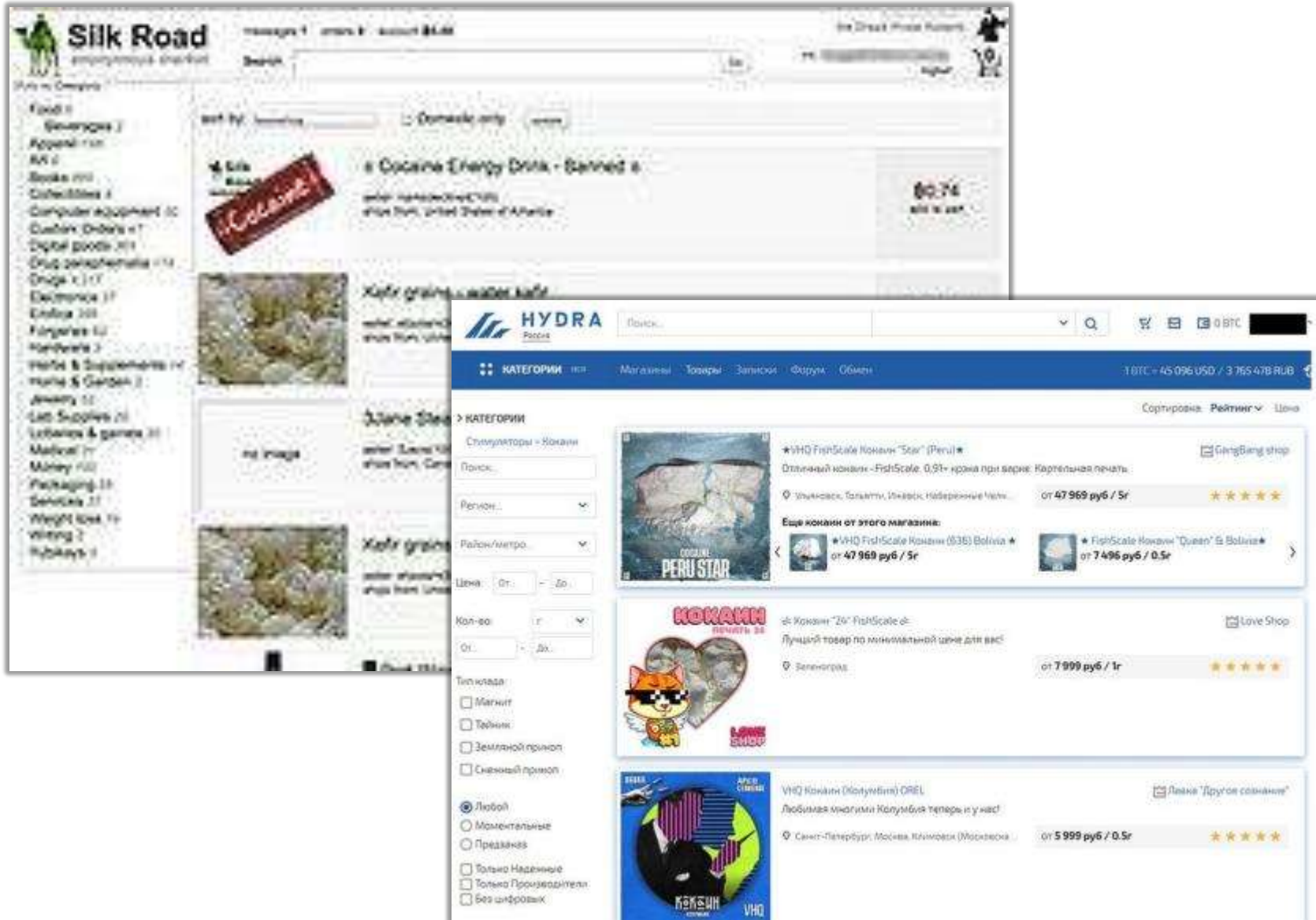


Tor hidden service

- Gli indirizzi URL degli hidden service appartengono al dominio .onion, riservato a Tor e che non può esistere su Internet.
- Gli indirizzi .onion non vengono assegnati, ma sono generati autonomamente dagli utenti stessi, come gli indirizzi Bitcoin
- Si può trovare l'indirizzo onion di un hidden service:
  - in una Dark web directory: pagine web su Tor che pubblicano collegamenti ad altri servizi noti, come The Hidden Wiki o DarkWebLinks
  - tramite Social media: Twitter, Reddit, canali Telegram...
  - tramite condivisione diretta tra utenti
  - da uno dei motori di ricerca esistenti all'interno di Tor
- La possibilità di pubblicare hidden service in completo anonimato ha incoraggiato il proliferare di servizi illegali

Dark market

- Dal 2011 sono divenuti noti alle cronache nomi come
  - SilkRoad
  - Agora
  - Utopia
  - Babylon
  - TheRealDeal
  - AlphaBay
  - DreamMarket
  - WallStreetMarket
  - Hydra…



Dark market

French World Market

Boutique PGP À propos

Nos Produits (8)

Pass Sanitaire 3 doses FRANCE
Digital
Livraison: 72h
Vendeur Vérifié: FrenchPass
Note:
150.00€

Passe-Partout Vigik de Facteur

Physique
Livraison: 48h
Vendeur Vérifié: KYC
Note:
95.00€

Compte Paypal Piraté d'une valeur de 1000€ à 3000€
Digital
Livraison: 24h
Vendeur Vérifié: Artyum
Note:
300.00€

Fausse Carte d'identité par Archibal

Physique
Livraison: 2 semaines
Vendeur Vérifié: Archibal
Note:
460.00€

Clés PTT T10 & F10 de Facteur

Physique
Livraison: 48h
Vendeur Vérifié: KYC
Note:
30.00€

Gorilla Glue : 5 grammes

Physique
Livraison: 1 semaine
Vendeur Vérifié: Marseille
Note:
35.00€

MDMA / XTC - 259 mg : 10 cachets

Physique
Livraison: 1 semaine
Vendeur Vérifié: RedBull
Note:
46.00€

Pistolet à Blanc modifié et Fonctionnel (tire en 7.65)
PAS D'IMAGE DISPONIBLE
Physique
Livraison: 2 semaines
Vendeur Vérifié: Bidouilleur10
Note:
600.00€

Description

Dark market


Top 25 darknet markets and fraud shops by revenue, 2022
Blue = Drug market, Orange = Fraud shop
$600.0 M
$400.0 M
$200.0 M
$0.0 M
Hydra Marketplace
Mega Darknet Market
Blacksprut Market
OMG!OMG! Market
Brian Dumps
ASAP Market
MG555
Unicc
Solaris market
Benumb Shop
World Market
Bankomat.cc
Bypass Shop
Matanga market
Abacus Market
HGN store
Incognito market
XNova.ltd
Yalelodge
Basetools - Trustcvv
Easydeals
Approved Credit Card
Flugsvamp 4.0
Russian Market
Exploit.in Escrow
© Chainalysis

Hydra

Bundeskriminalamt

GENERALSTAATSANWALTSCHAFT FRANKFURT AM MAIN
ZIT

HESSEN

Die Plattform und der kriminelle Inhalt wurden beschlagnahmt
durch das Bundeskriminalamt unter Sachleitung der
Generalstaatsanwaltschaft Frankfurt am Main
im Rahmen einer international koordinierten Operation.

The platform and the criminal content have been seized
by the Federal Criminal Police Office (BKA) on behalf of
Attorney General's Office in Frankfurt am Main
in the course of an international coordinated law enforcement operation.

Платформа и криминальное содержимое конфискованы
Федеральной уголовной полицией под управлением
Генеральной прокуратуры Франкфурта на Майне
в рамках международно согласованной операции.

Underground economy

- Secondo un recente report di Chainalysis, nel 2022 i mercati darknet hanno registrato una drastica diminuzione delle entrate rispetto al 2021:
- Il fatturato totale del settore cade da 3,1 a 1,5 miliardi di dollari
- La maggior parte dei guadagni sono stati generati da darkmarket convenzionali incentrati sulle droghe
- Hydra Market è stato il market con i guadagni più alti nel 2022, ma è stato chiuso lo scorso aprile in un'operazione congiunta organizzata da Usa e Germania.
- La chiusura di questo market ha provocato un calo dell'intero settore, ma i tre mercati con i guadagni più alti, Mega Darknet, Blacksprut e OMG! hanno cercato di attirare gli ex utenti e venditori di Hydra.

INVESTIGARE NEL DARK WEB

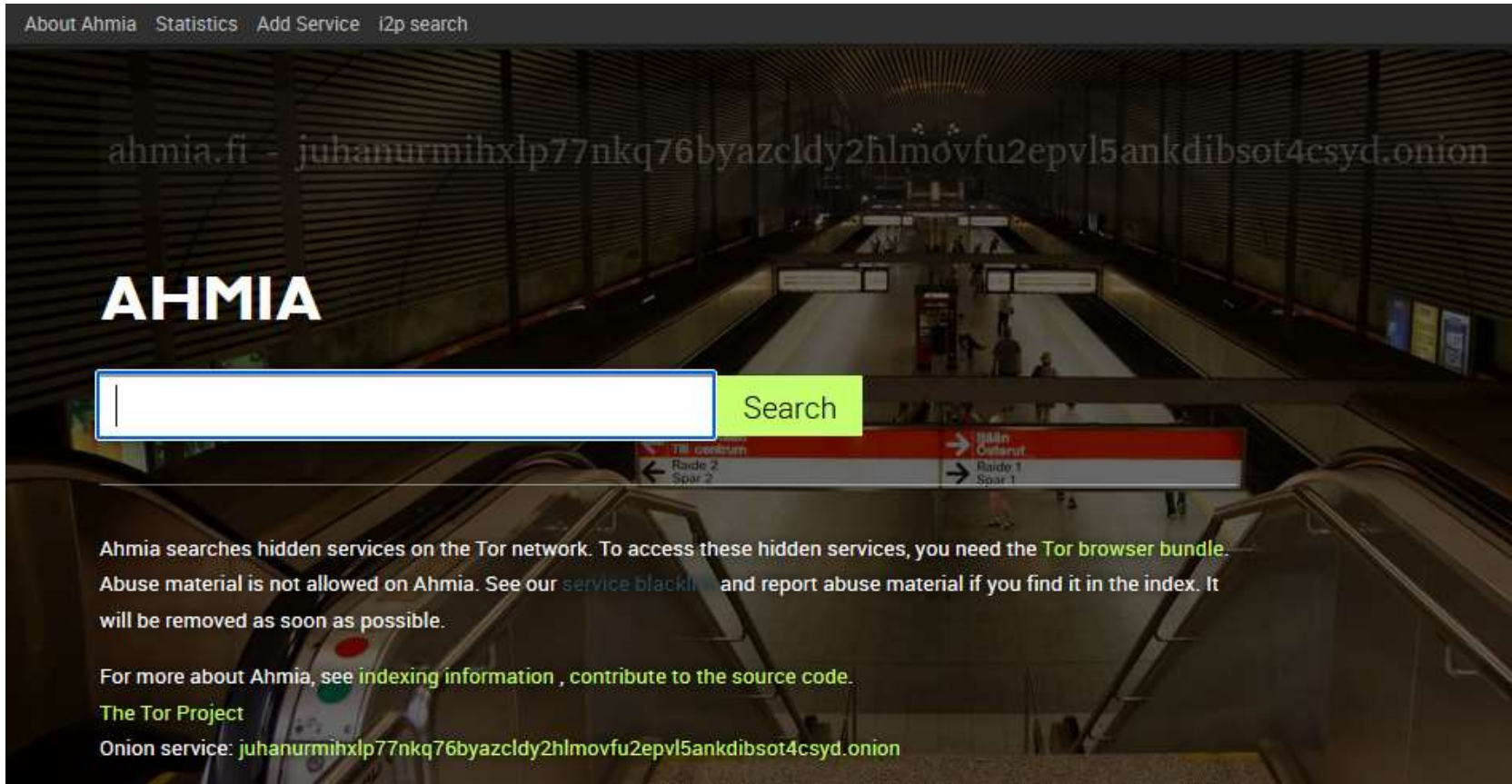
Strumenti di accesso e ricerca: Tor2web

- Tor2web è una rete di server proxy HTTP (forniti da volontati) utilizzata per l'accesso ai contenuti dei Tor Hidden Services attraverso un normale browser web.
- Progettato nel 2008 da Aaron Swartz e Virgil Griffith, è oggi parte del progetto GlobaLeaks ed è mantenuto dal Centro Studi Hermes per la Trasparenza ed i Diritti Umani Digitali.
- Per visitare un hidden service tor da clearnet, basta sostituire nell'indirizzo .onion con .onion.to o .onion.city o .onion.cab o .onion.direct o qualsiasi alttro dominio reso disponibile dagli operatori volontari di Tor2web

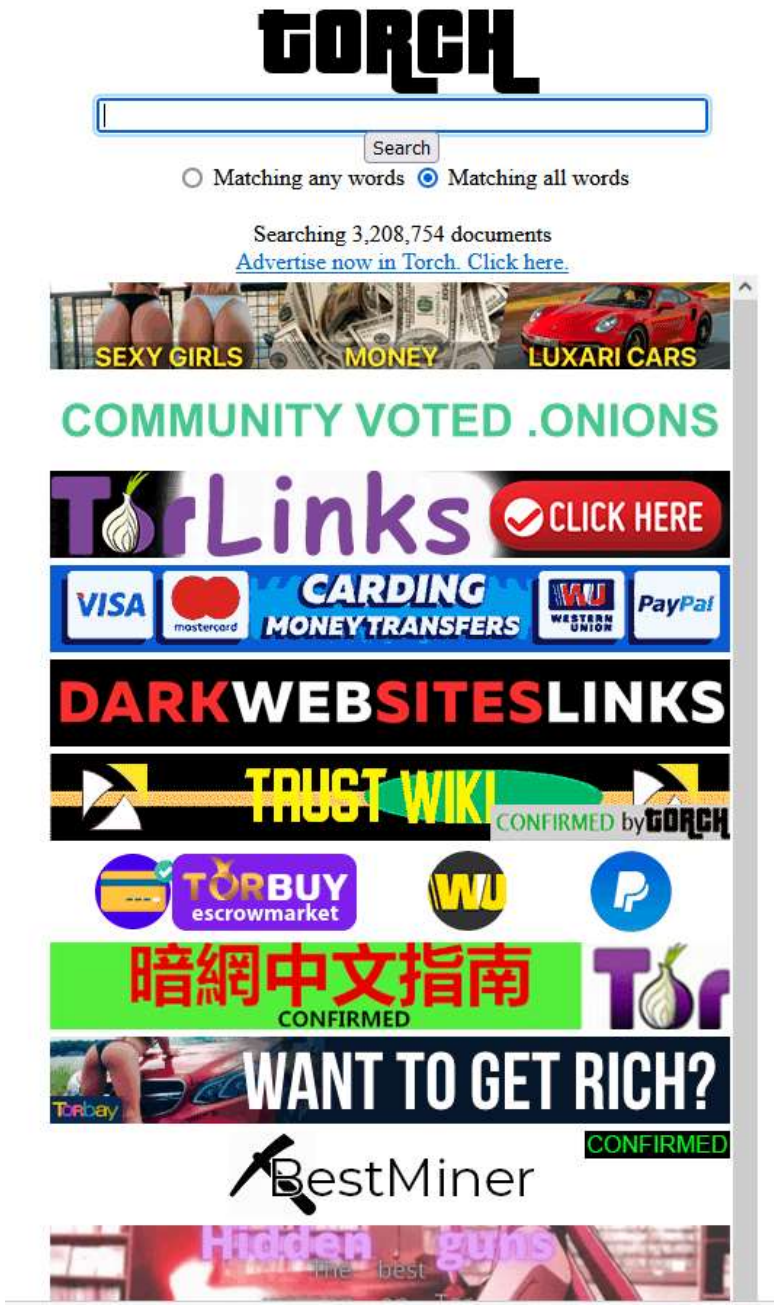
TOR2WEB

Strumenti di accesso e ricerca: Ahmia

- Ahmia è un motore di ricerca basato su software open source, creato e mantenuto dal ricercatore di sicurezza Juha Nurmi
- Il suo scopo è indicizzare e rendere raggiungibili gli hidden service di Tor
- Offre un'interfaccia su clearnet e servizi di ricerca anche sulla rete I2p
- Applica delle policy di filtraggio e blacklist per contenuti CSA e rispetta le direttive robot.txt

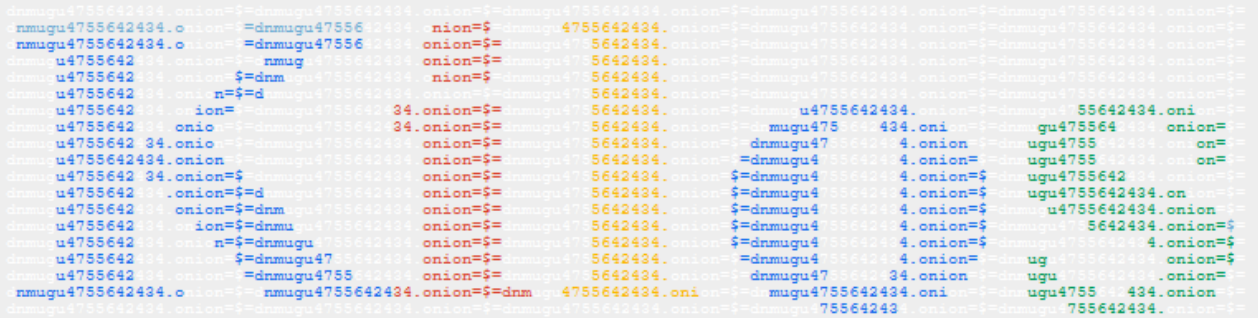


Torch


TORCH
Search
Matching any words
Matching all words
Searching 3,208,754 documents
Advertise now in Torch. Click here.
SEXY GIRLS
MONEY
LUXARI CARS
COMMUNITY VOTED .ONIONS
TorLinks
CLICK HERE
VISA
mastercard
CARDING
MONEY TRANSFERS
WESTERN UNION
PayPal
DARKWEBSITESLINKS
TRUST WIKI
CONFIRMED by TORCH
TORBUY
escrowmarket
WU
暗網中文指南
CONFIRMED
Tor
WANT TO GET RICH?
CONFIRMED
BestMiner
Hidden
guns

Kilos

- Motore di ricerca specializzato in dark markets



2,011,949 searches served since 29 Nov, 2020

7,956 vendors 122,812 listings 1,461,954 reviews 876,601 forum posts

If you can remember your phone number, you can remember our URL! DNM ugu (475) 564-2434
— *Message from staff*

Search query

Minimum price | Maximum price | Display currency

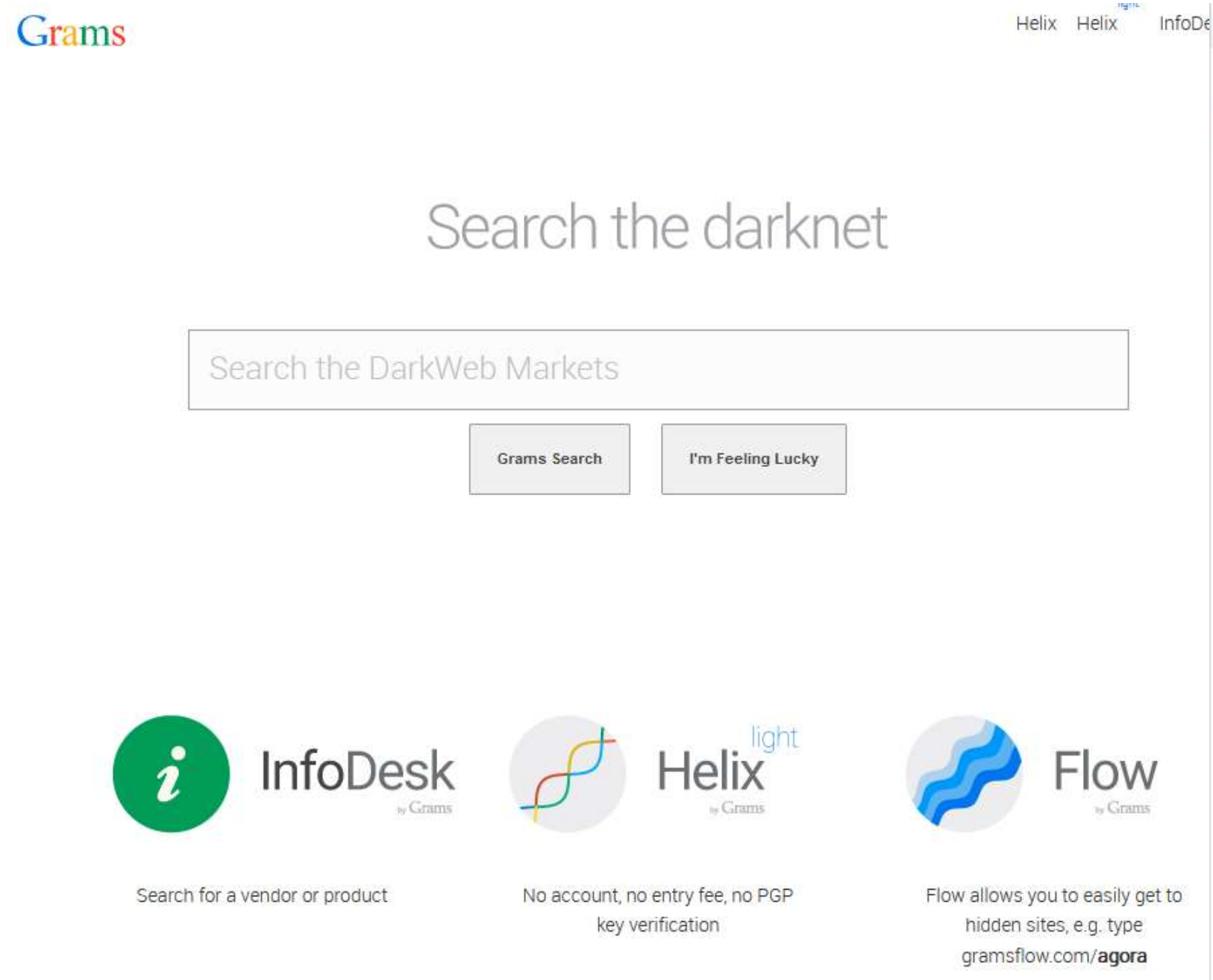
Relevance | Market

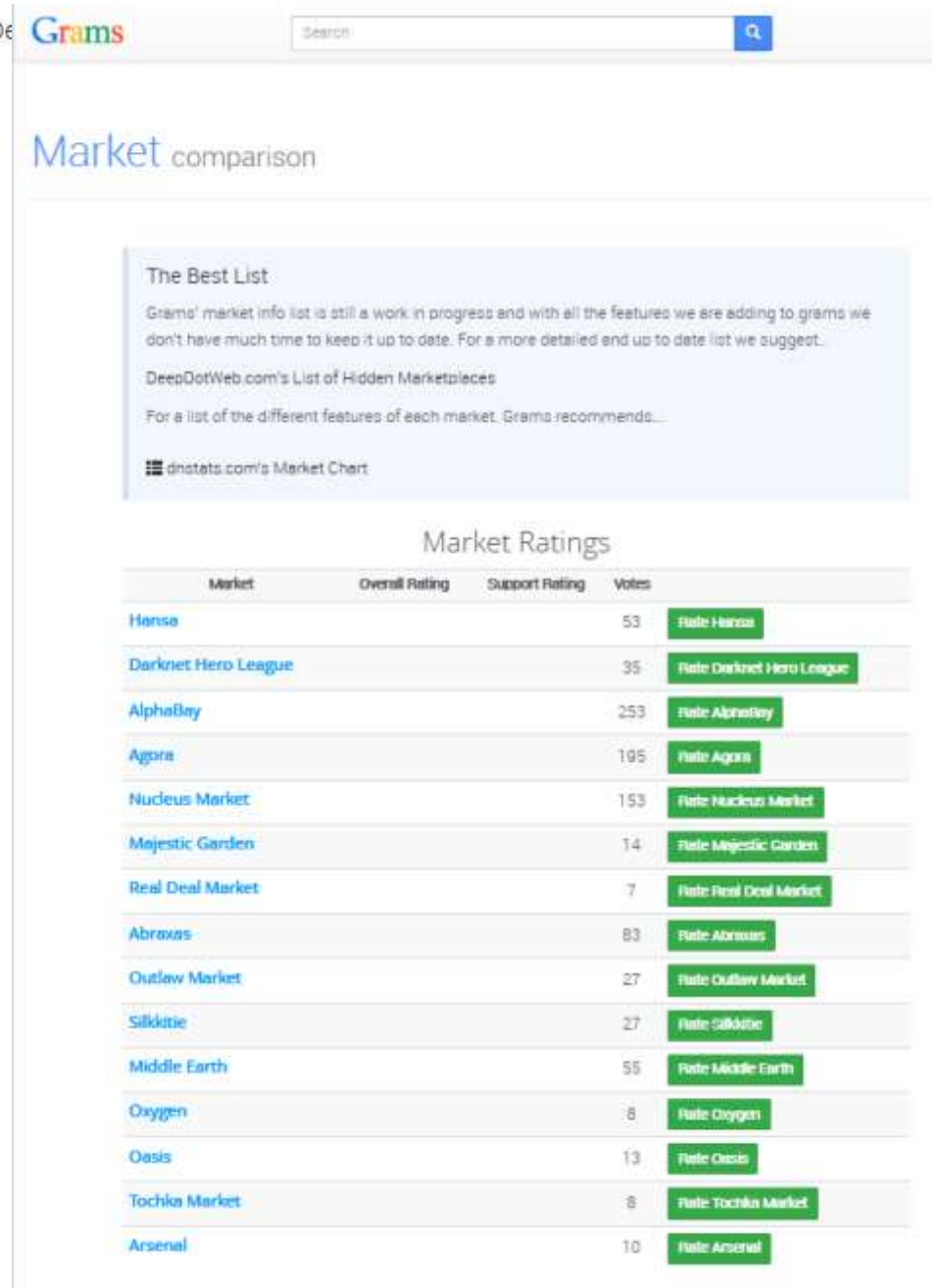
Shipping origin | Shipping destination | Product class - any

☐ Accepts BTC ☐ Accepts BCH ☐ Accepts LTC ☐ Accepts XMR

Search the darknet markets

Grams


Grams
Helix
Helix
InfoDe
Search the darknet
Search the DarkWeb Markets
Grams Search
I'm Feeling Lucky
InfoDesk
by Grams
Search for a vendor or product
Helix light
by Grams
No account, no entry fee, no PGP key verification
Flow
by Grams
Flow allows you to easily get to hidden sites, e.g. type gramsflow.com/agora

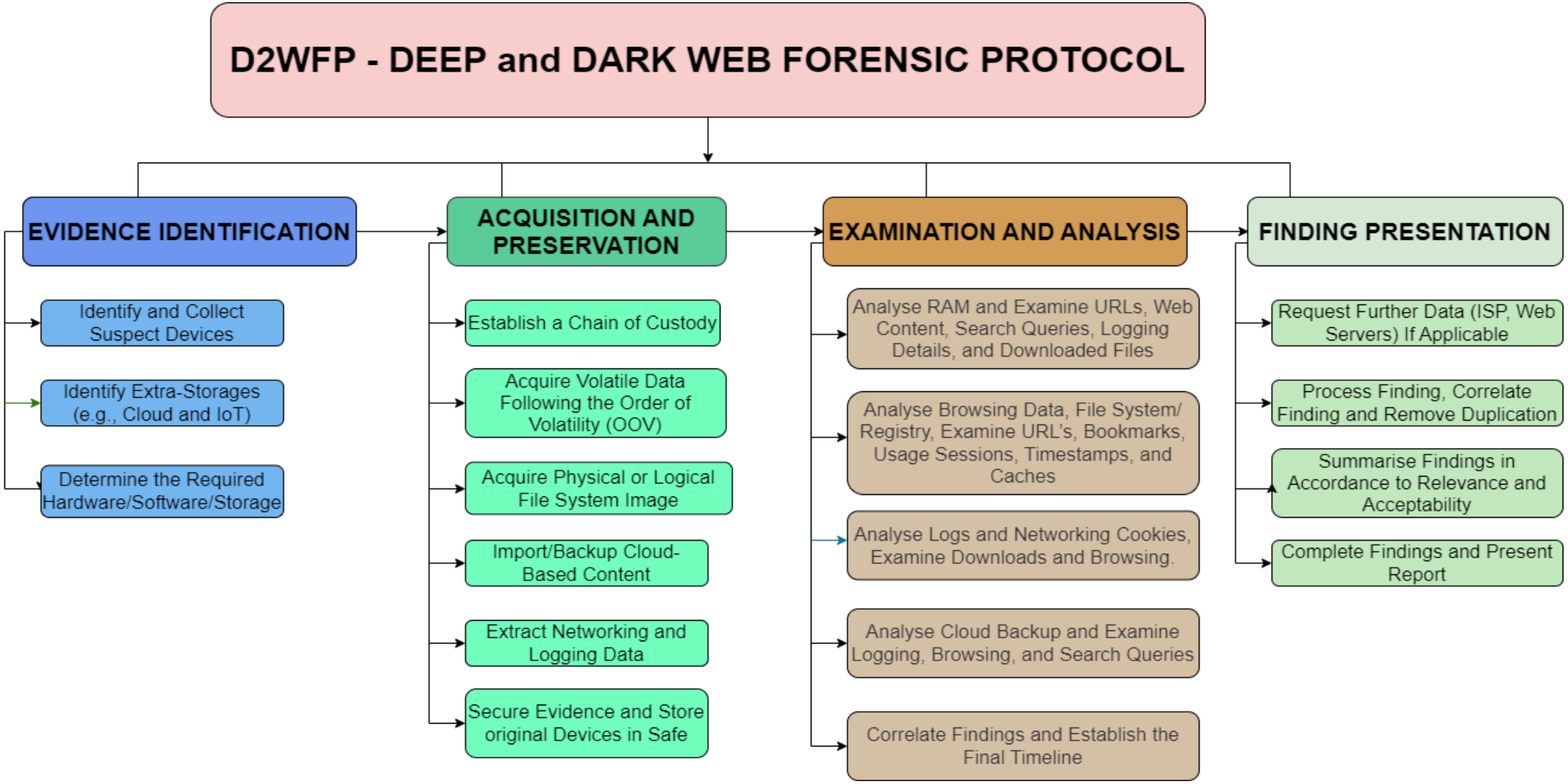

Grams
Search
Market comparison
The Best List
Grams' market info list is still a work in progress and with all the features we are adding to grams we don't have much time to keep it up to date. For a more detailed and up to date list we suggest.
DeepDotWeb.com's List of Hidden Marketplaces
For a list of the different features of each market, Grams recommends...
dnstats.com's Market Chart
Market Ratings
Market
Overall Rating
Support Rating
Votes
Hansa 53 Rate Hansa
Darknet Hero League 35 Rate Darknet Hero League
AlphaBay 253 Rate AlphaBay
Agora 195 Rate Agora
Nucleus Market 153 Rate Nucleus Market
Majestic Garden 14 Rate Majestic Garden
Real Deal Market 7 Rate Real Deal Market
Abraxas 83 Rate Abraxas
Outlaw Market 27 Rate Outlaw Market
Silkkitie 27 Rate Silkkitie
Middle Earth 55 Rate Middle Earth
Oxygen 8 Rate Oxygen
Oasis 13 Rate Oasis
Tochka Market 8 Rate Tochka Market
Arsenal 10 Rate Arsenal

DEANONIMIZZAZIONE

Deanonimizzazione utenti darknet

Deep and Dark Web Forensics Protocol

- Il modello D2WFP integra diversi metodi di digital forensics per individuare artefatti correlati all'uso di dark web



Teniamoci in contatto...

Isp. **Davide Rebus Gabrini**

Gabinetto Regionale Polizia Scientifica per la Lombardia
Unità Indagini Elettroniche

Contatti personali:

e-mail: davide.gabrini@poliziadistato.it

GPG Public Key: www.tipiloschi.net/rebus.asc
KeyID: 0x176560F7

facebook.com/gabrini

twitter.com/therebus

it.linkedin.com/in/rebus