



Sistemi informativi: averne fiducia e trarne valore

**Rome Chapter**

***“OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali”***

Massimiliano Graziani CFE CIFI CFIP CDFP OPSA ACE TCNU

Roma 14/05/2021

# Presentazione relatore

**Massimiliano Graziani** attualmente CEO Cybera Srl e CISO Adora ICT srl

Fondatore, insieme ad altri nel 2005 del capitolo italiano dell'OWASP.

Socio fondatore del capitolo italiano dell' International Information Systems Forensics Association (IISFA), e dell'Osservatorio Nazionale Informatica Forense (ONIF), è in possesso delle seguenti certificazioni internazionali:

- CIFI (Certified Information Forensics Investigator rilasciata da IISFA)
- CFE (Certified Fraud Examiner rilasciata da ACFE)
- ACE (AccessData Certified Examiner rilasciata da AccessData)
- OPSA (OSSTMM Professional Security Analyst rilasciata da ISECOM)
- CIFIP (Certified Forensic Investigation Professional rilasciata da IICFIP)
- CDFP (Certified Digital Forensics Professional rilasciata da IICFIP).



Docente in materia di Digital Forensics Pratica presso Scuola di Polizia Tributaria della Guardia di Finanza (Corso Operativo di Computer Forensics con Logicube Dossier e Falcon), Università La Sapienza Roma (Corso Informatica Giuridica con Aterno), Università LUMSA Roma (Corso Diritto Penale dell'Informatica con Zanotti), Università di Salerno (Convegno La Tecnologia al servizio dell'Indagine Scientifica con De Santis, Cattaneo, Palmieri), Università del Molise (Master Information Security Management – Modulo Computer Forensics con Perrone), Università degli studi Link Campus University di Roma (modulo forensics di vari master, ultimo con Saccone). Docente volontario presso IISFA, OLAF, FF.OO., Consiglio Superiore Magistratura Milano, Ministero Economia e Finanze UCAMP, ISACA Roma e ACFE Italia e Centro Interforze di Formazione Intelligence/GE, Board of Directors ACFE Central.

*Maggiori info sul mio background: [www.cobrasoft.it](http://www.cobrasoft.it)*

OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali. Slide riservate all'evento di ISACA ROMA del 14/05/2021 © 2021 Massimiliano Graziani vietata la riproduzione anche parziale senza l'autorizzazione scritta dell'autore.

# Agenda

---



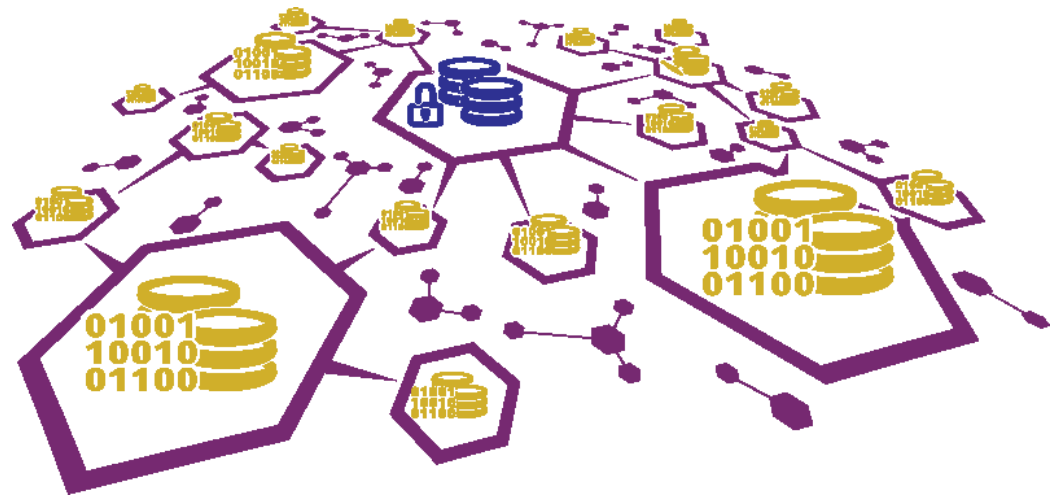
- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A



ATTENZIONE:

QUELLO CHE VEDRETE IN QUESTO SEMINARIO,  
E' MATERIALE A SCOPO EDUCATIVO.  
VI RICORDO CHE EFFETTUARE PORT SCANNING E  
VULNERABILITY ASSESSMENT SENZA ESSERE  
AUTORIZZATI COSTITUISCE UN REATO.

*Open Source INTelligence, acronimo OSINT (in italiano: "Intelligence su fonti aperte"), è quella disciplina dell'intelligence che si occupa della ricerca, raccolta ed analisi di dati e di notizie tratte da fonti aperte.*





*OSINT è un processo di raccolta ed elaborazione di informazioni altamente degradabili...*



...“Un sistema ‘puro’ che non ha bisogno di compromessi oscuri con le fonti, non viola la legge con attività investigative illegali, ma si basa solo sulla capacità tecnica e operativa di trovare le informazioni, la mentalità investigativa, la conoscenza delle tecniche di analisi e correlazione dei dati e infine il lavoro metodico e organizzato di consultazione delle fonti aperte che sono per definizione accessibili a tutti”...

*(tratto da: Leonida Reitano - "Esplorare Internet")*

## Classificazione attività di intelligence:

HUMINT (Human Intelligence - informatori)

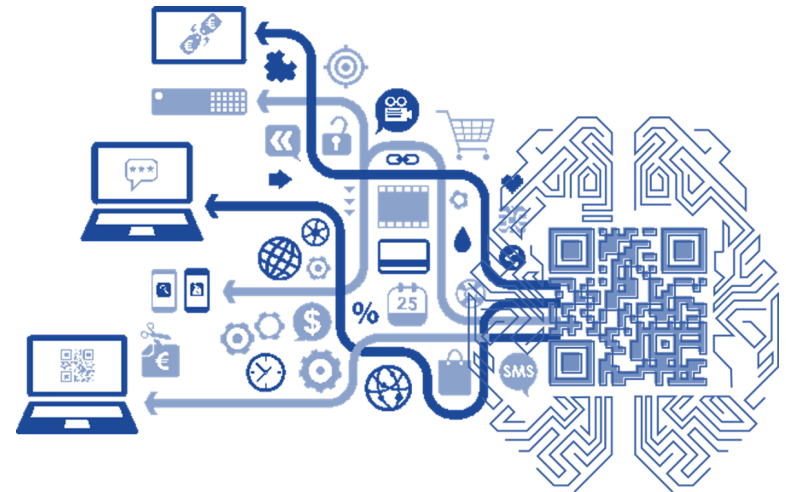
**SIGINT** (Signals Intelligence - intercettazioni) **vediamo subito un esempio!**

GEOINT o IMINT (Image intelligence - immagini satellitari, aerei spia e altri vettori)

OSINT (Open Source intelligence)

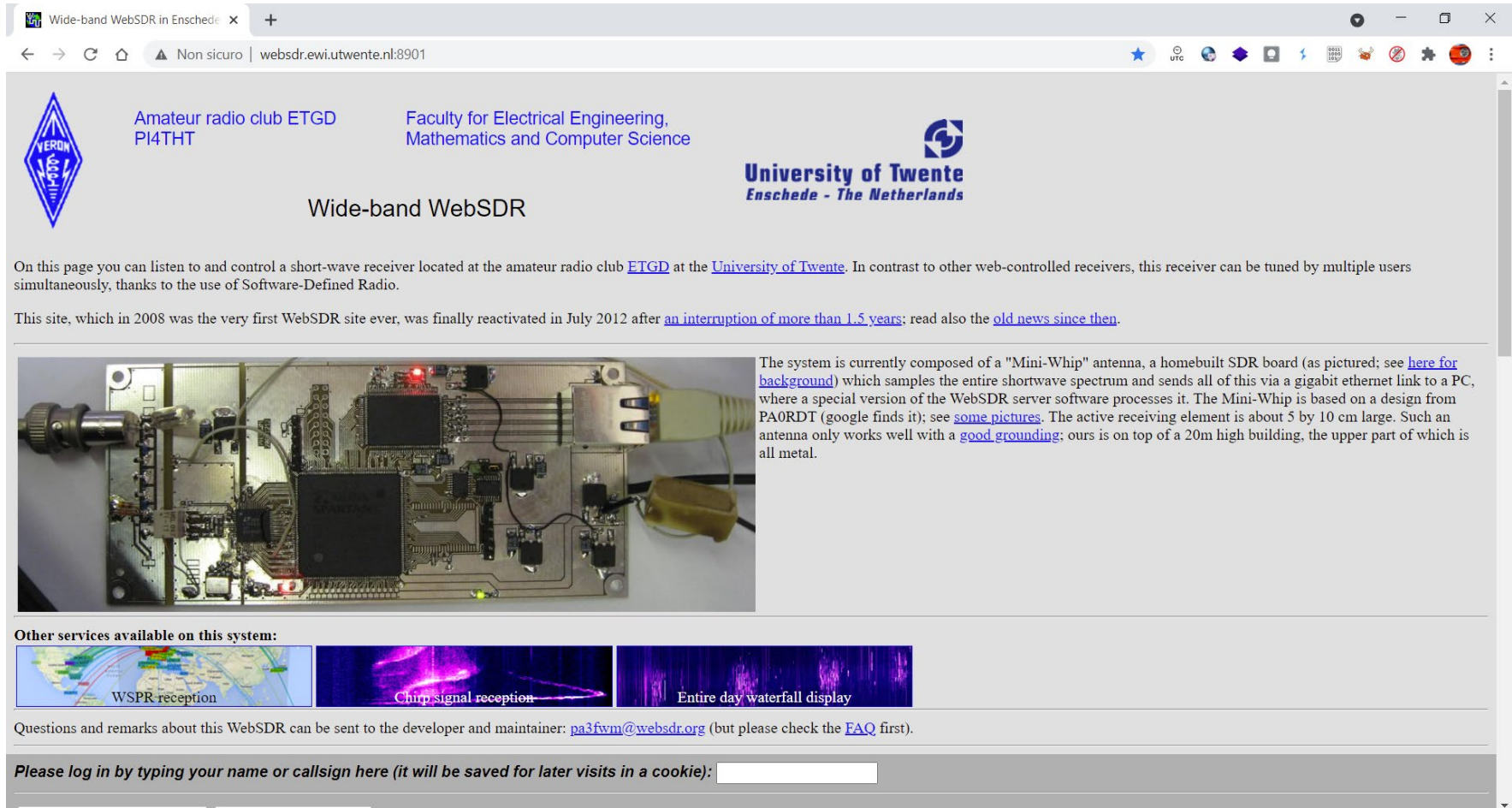
TECHINT (Technical Intelligence)

FININT (Financial Intelligence)





## SIGINT (Signals Intelligence - intercettazioni) vediamo subito un esempio!



The screenshot shows a web browser window with the URL `websdr.ewi.utwente.nl:8901`. The page header includes logos for the amateur radio club ETGD (PI4THT) and the University of Twente. The main heading is "Wide-band WebSDR".

On this page you can listen to and control a short-wave receiver located at the amateur radio club [ETGD](#) at the [University of Twente](#). In contrast to other web-controlled receivers, this receiver can be tuned by multiple users simultaneously, thanks to the use of Software-Defined Radio.

This site, which in 2008 was the very first WebSDR site ever, was finally reactivated in July 2012 after [an interruption of more than 1.5 years](#); read also the [old news since then](#).

The system is currently composed of a "Mini-Whip" antenna, a homebuilt SDR board (as pictured; see [here for background](#)) which samples the entire shortwave spectrum and sends all of this via a gigabit ethernet link to a PC, where a special version of the WebSDR server software processes it. The Mini-Whip is based on a design from PA0RDT (google finds it); see [some pictures](#). The active receiving element is about 5 by 10 cm large. Such an antenna only works well with a [good grounding](#); ours is on top of a 20m high building, the upper part of which is all metal.

**Other services available on this system:**

- WSPR reception
- Chirp signal reception
- Entire day waterfall display

Questions and remarks about this WebSDR can be sent to the developer and maintainer: [pa3fwm@websdr.org](mailto:pa3fwm@websdr.org) (but please check the [FAQ](#) first).

Please log in by typing your name or callsign here (it will be saved for later visits in a cookie):

*DATI PUBBLICI (rendiconti governativi, piani finanziari, dati demografici, notizie stampa, ecc.)*

*MEZZI DI COMUNICAZIONE DI MASSA*

*DATABASE EDITORIALI*

*FILE MULTIMEDIALI*

*DATABASE ISTITUZIONALI*

*trattati con la coscienza di:*

*STRUMENTI DI HACKING (ottenere informazioni sulle identità digitali)*

*AVANZATO USO DEI MOTORI DI RICERCA (usando ad esempio GHDB)*

*UTILIZZO DI PORTALI DI INVESTIGAZIONI ON LINE (informazioni istituzionali su persone fisiche o giuridiche, partecipazioni azionarie/societarie, proprietà immobiliari, ecc.)*

*TECNICHE DI ANALISI INVESTIGATIVA (analizzare e poi rappresentare anche graficamente le informazioni estrapolate)*

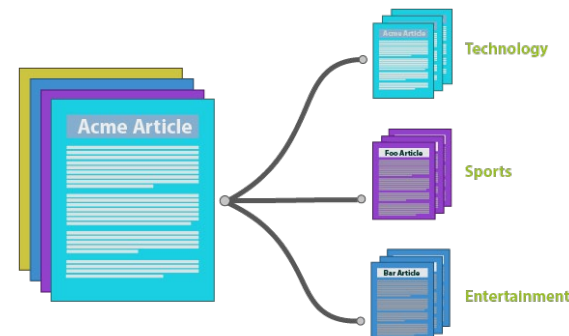
*e capacità di analisi:*

*INDIVIDUAZIONE, VALUTAZIONE, SELEZIONE ED ELABORAZIONE DEI DATI MIRATA AD OTTENERE INFORMAZIONI DI VALORE*

*Circa l'80% delle informazioni di pertinenza investigativa viene raccolta tramite OSINT*

*Circa il 90% delle attività di information gathering si basa su fonti aperte*





## Classificazione delle FONTI:

INFORMAZIONI GENERALI (info provenienti dal web o dai media)

INFORMAZIONI A PAGAMENTO (database commerciali o siti a pagamento)

ESPERTI (interviste e opinioni di esperti, tecnici, specialisti, ecc)

DOCUMENTI “GRAY” (brevetti, report, pubblicazioni ad uso interno, atti di convegni, ecc.)

O.D.S. (Open Source Data): Dati grezzi, generici, generati da registrazioni, fotografie, immagini satellitari, in generale tutta la documentazione pubblicata su canali pubblici da fonti non attendibili

O.S.I.F. (Open Source Information): Informazione pubblica che ha subito un processo di filtraggio e convalida, come giornali, libri, comunicazioni e divulgazioni da fonti attendibili

L’O.S.I.N.T. è l’unione di ODS e OSIF, consiste in informazioni filtrate, cercate, selezionate e destinate a soddisfare una specifica richiesta informativa

## A chi interessa?

### Governi

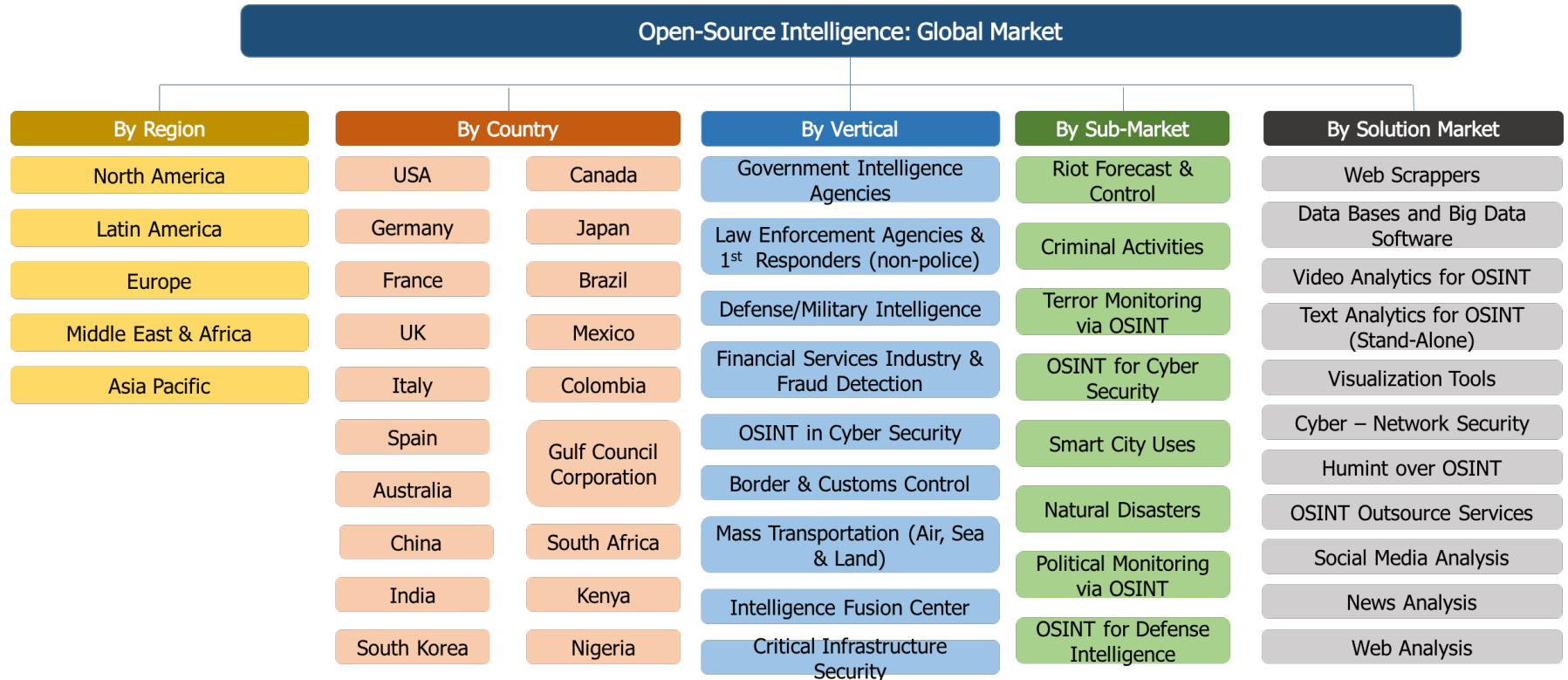
- Agenzie Governative
- Ministeri della difesa
- Forze di Polizia

### Privati

- Aziende
- Consulenti
- Pentester
- Investigatori Privati
- Giornalisti

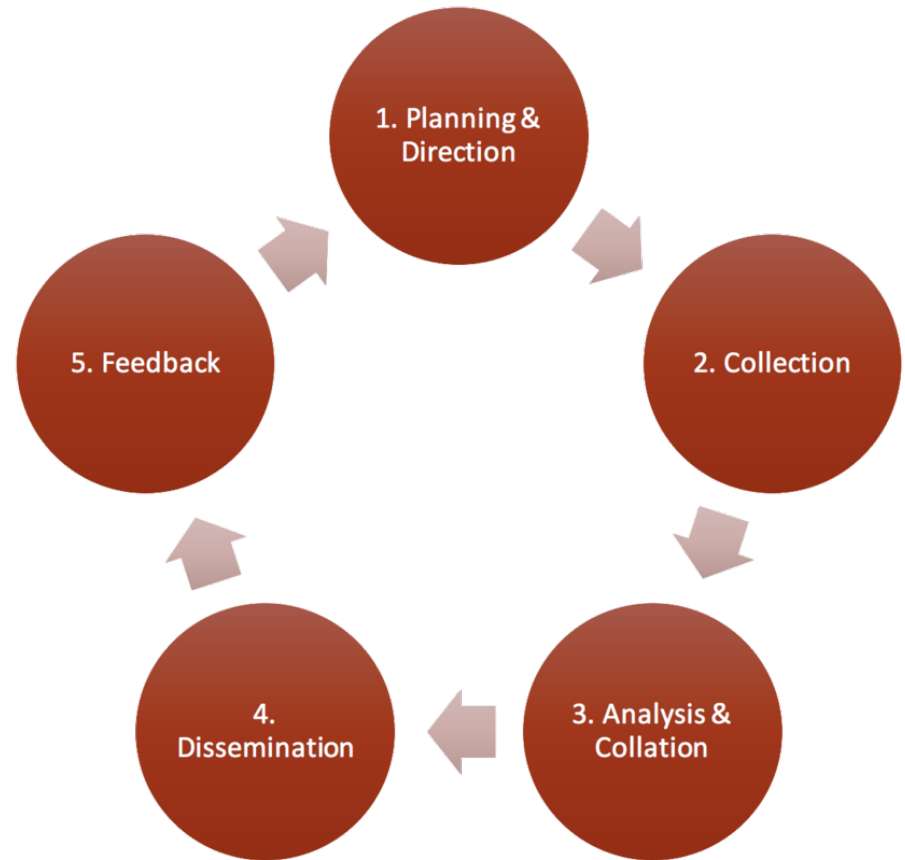
### Organizzazioni Criminali

- Stalking
- Cracking
- Phishing
- Furto d'identità



Le 5 fasi dell'OSINT:

- 1) Planning e Direction (definisco obiettivo e fonti)
- 2) Collection (raccolgo i dati)
- 3) Analysis e Collation (analizzo e confronto)
- 4) Dissemination (diffusione dei report)
- 5) Feedback (misuro il gradimento del cliente)





Operazioni manuali o automatiche?

Manuali:

Raccolta e confronto oneroso, difficilmente “scalabile” ed elevato rischio di “perdere” informazioni

Automatiche:

Potenzialmente molto efficace, facilmente “scalabile” ed integrabile, richiede enormi investimenti, le tecnologie sono in rapida convergenza

# Agenda

---

- Introduzione all'OSINT
- ➔ • Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A



bing YAHOO!  
Google



## SURFACE WEB

Sono i contenuti pubblici indicizzati dai motori di ricerca.



Informazioni  
Accademiche



Risorse  
Governative



Dati Medici



Data Base



Informazioni  
accesso riservato



Informazioni  
Finanziarie



Documenti  
Legali



Contenuti a  
pagamento



Social Media

## DEEP WEB

Sono i contenuti non pubblici che in genere non si trovano con i motori di ricerca. Ad esempio: siti con accesso limitato, siti con file robots.txt che limitano l'indicizzazione dei motori di ricerca, siti a pagamento, ecc. Statisticamente sono 800% più grandi del Surface Web.

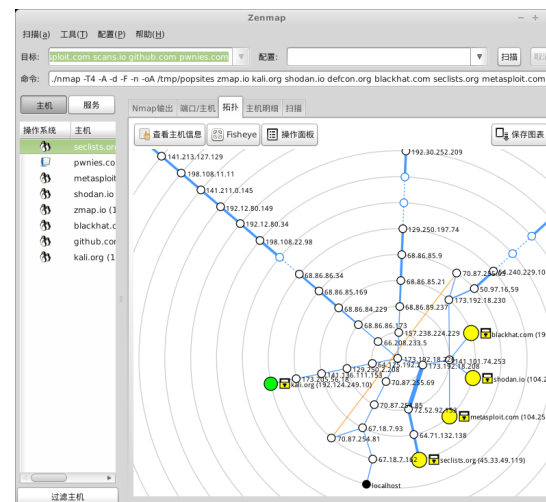
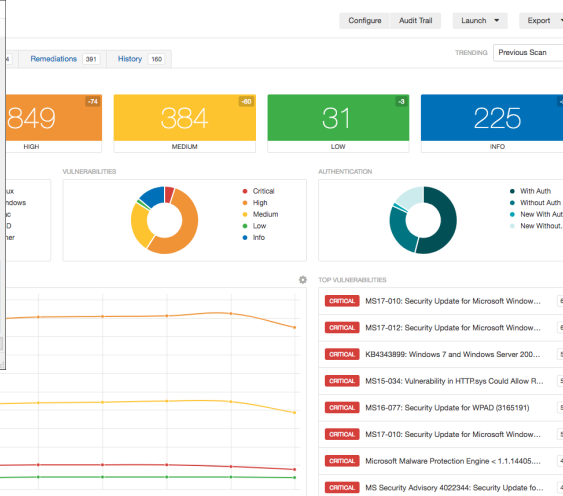
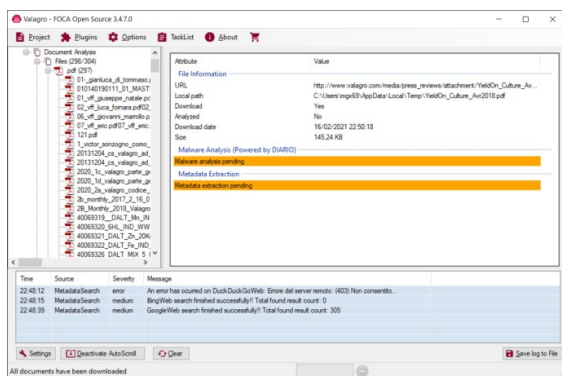


## DARK WEB

Sono contenuti non pubblici che non si trovano con i motori di ricerca che hanno bisogno di speciali software per l'accesso.

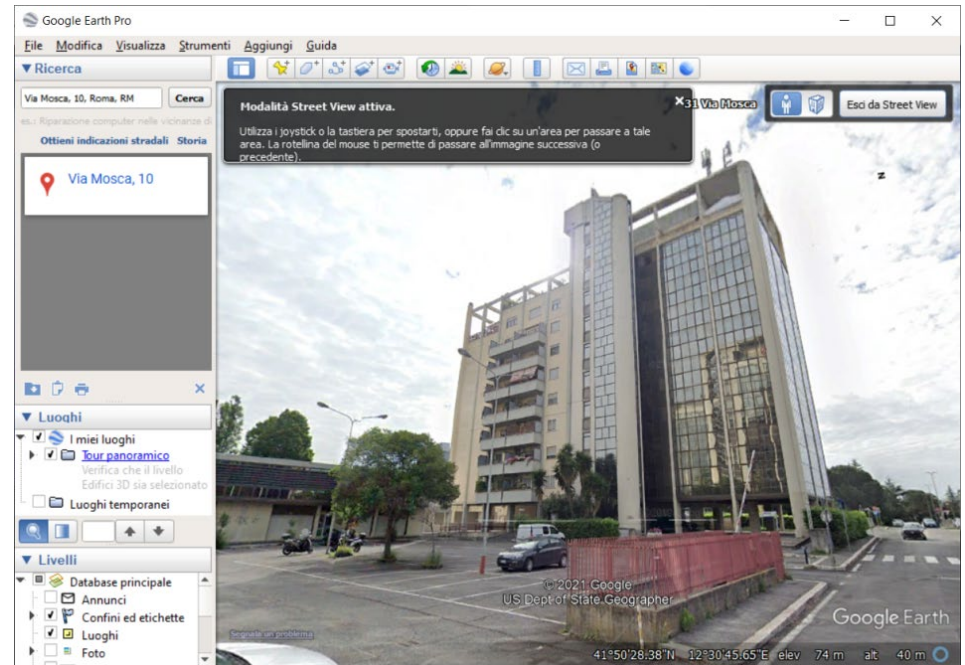
## INFORMATION GATHERING ATTIVA

- Tracing
- Port Scanning (NMAP)
- Scansione dei siti web (esempi: analisi dei robots.txt, ecc.)
- Scansione delle risorse (esempi: ricerche dentro repository FTP, ricerche tramite FOCA, ecc.)
- Rilevamento di configurazioni errate o predefinite (esempi: GHDB, directory listing, ecc.)
- Mappatura delle vulnerabilità (esempi: vulnerability assessment, scansioni con Nessus, scansioni con OpenVAS, ecc.)
- Ricerca Exploit utilizzabili



## INFORMATION GATHERING PASSIVA

- Analisi dei dati della rete (esempio: sniffing con Wireshark, uso di TCPdump, ecc.)
- Motori di ricerca (google, bing, ecc.)
- Social Network (analisi Facebook, LinkedIn, ecc.)
- Analisi header email (manuale oppure on line)
- Crawling (download e analisi contenuto dei siti web)
- Analisi tra entità (esempio: Maltego)
- Analisi di mappe (Google Earth)



CYBER INTELLIGENCE

PASSIVA

OSINT  
Open Source Intelligence, Intercettazioni non invasive, interviste, opinioni, ecc. Non genera nessun traffico di rete.

SEMI PASSIVA

Stealth Intelligence  
Modalità attiva che si svolge sotto la soglia di rilevamento, più costosa, genera un traffico di rete normale.

ATTIVA

Intelligence Proattiva  
Social engineering, attività sotto copertura, sfruttamento di vulnerabilità, utilizzo di malware, ecc. Genera un traffico di rete anomalo e rilevabile.





## NETWORK INFORMATION GATHERING

- IP
- DNS
- Domini e Whois
- Siti web e web server
- Posta elettronica
- Data Base






## ANALISI DI UN SITO WEB

- Chi ha registrato un dominio
- Chi sta gestendo il sito
- Dove si trova l'hosting
- Domini collegati
- Email e numeri di telefono
- Il passato di un sito web
- ecc.

# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
-  • Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

## NMAP HANDS ON

nmap — Strumento di network exploration e security / port scanner  
znmapp è la versione GUI (con interfaccia grafica) per windows.



```
nmap [ <Tipo di Scansione> ...] [ <Opzioni> ] { <Obiettivo> }
```

Nmap (“Network Mapper”) è uno strumento open-source per l’esplorazione della rete e l’auditing. È stato progettato per scansionare rapidamente reti di grandi dimensioni, ma è indicato anche per l’utilizzo verso singoli host. Nmap usa pacchetti IP "raw" (grezzi, non formattati) in varie modalità per determinare:

- quali host sono disponibili su una rete
- che servizi (nome dell'applicazione e versione) vengono offerti da questi host
- che sistema operativo (e che versione del sistema operativo) è in esecuzione
- che tipo di firewall e packet filters sono usati

Nonostante Nmap sia comunemente usato per audits di sicurezza, molti sistemisti e amministratori di rete lo trovano utile per tutte le attività giornaliere come ad esempio l’inventario delle macchine presenti in rete, per gestire gli aggiornamenti programmati dei servizi e per monitorare gli host o il loro uptime.



## NMAP HANDS ON

L'output di Nmap è un elenco di obiettivi scansionati, con informazioni supplementari per ognuno a seconda delle opzioni usate. Tra queste informazioni è vitale la “tabella delle porte interessanti”. Questa tabella elenca il numero della porta e il protocollo, il nome del servizio e lo stato attuale. Lo stato può essere

- open (aperto)
- filtered (filtrato)
- closed (chiuso)
- unfiltered (non filtrato)



Aperto significa che vi è sulla macchina obiettivo un'applicazione in ascolto su quella porta per connessioni o pacchetti in entrata. Filtrato significa che un firewall, un filtro o qualche altro ostacolo di rete sta bloccando la porta al punto che Nmap non riesce a distinguere tra aperta o chiusa. Le porte chiuse non hanno alcuna applicazione in ascolto, anche se potrebbero aprirsi in ogni momento. Le porte vengono classificate come non filtrate quando rispondono ad una scansione di Nmap, ma non è stato possibile determinare se sono aperte o chiuse. Nmap mostra le combinazioni aperta | filtrata e chiusa | filtrata quando non può determinare quale dei due stati descrive una porta. La tabella delle porte può anche includere dettagli quali le versioni dei software disponibili se è stata usata l'opzione appropriata.

## NMAP HANDS ON

Prima di scansionare un target, Nmap proverà ad inviare un ICMP echo request per verificare che l'host sia "alive".

Questo serve a salvare del tempo quando si scansionano più host, se gli host non sono online non si perderà del tempo inutilmente. Dato che le ICMP request sono spesso bloccate dal firewall, Nmap tenterà di connettersi anche alle porte 80 e 443, visto che spesso queste porte sono aperte. Le opzioni "discovery" di default non sono utili quando si scansionano sistemi messi in sicurezza. Nmap dispone di molti plugin già pronti e la maggior parte delle volte, non ha bisogno di utilizzare parametri particolari, quando è necessario, dispone comunque di moltissime opzioni.

I profili disponibili su ZNMAP sono:

**Intense scan** - Una scansione completa.

Contiene il controllo sul Sistema Operativo utilizzato, sulla versione, sugli script, effettua il traceroute ed è piuttosto aggressiva. Viene considerata una scansione intrusiva.

**Ping scan** - Questa scansione controlla semplicemente se il bersaglio è online, non controlla nessuna porta.

**Quick scan** - È più veloce della scansione regolare grazie a tempistiche aggressive e al fatto che effettua lo scan solo di alcune porte.

**Regular scan** - È la scansione che viene effettuata di base da Nmap, se non modificate alcun parametro. Pingherà il bersaglio e vi restituirà le eventuali porte aperte.

**Slow comprehensive scan** - È la scansione più verbose che include la maggior parte delle opzioni.

## NMAP HANDS ON

Puoi aggiungere dei parametri per modificare il tipo di scansione e aggiungere o rimuovere specifici particolari dai risultati. Cambiare i parametri della scansione, ne varierà l'intrusività.

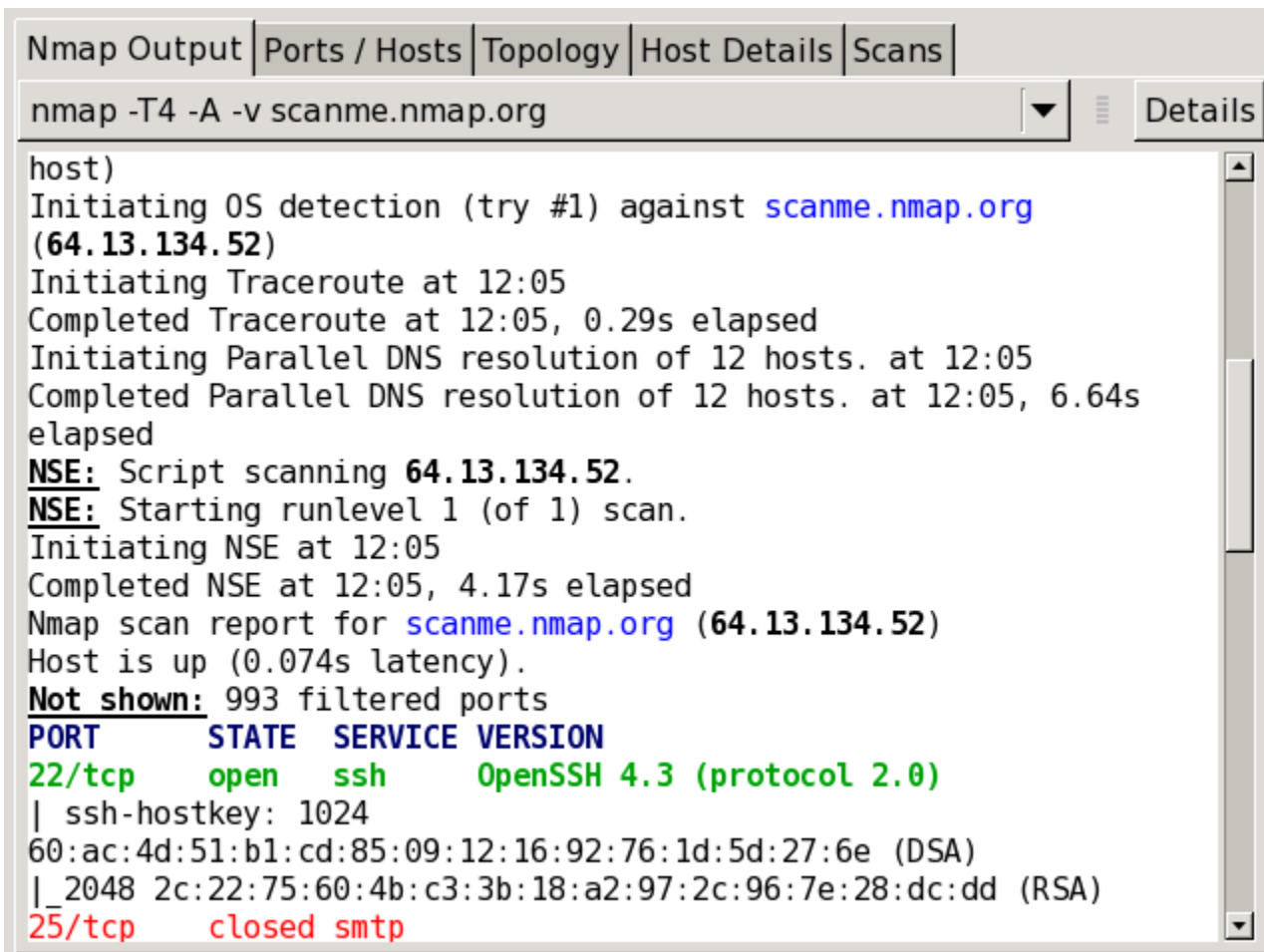
Puoi utilizzare più parametri separati da uno spazio. I parametri vanno inseriti prima del target:

```
nmap <parametro> <parametro> <target>
```

Quando la scansione sarà terminata, vedrete il messaggio: "Nmap done" in cima alla scheda con l'output. Potrai ora controllare i risultati, a seconda del tipo di scansione selezionata. Tutti i risultati saranno elencati nella scheda Nmap Output, ma puoi usare le altre schede per controllare nel dettaglio i risultati specifici.

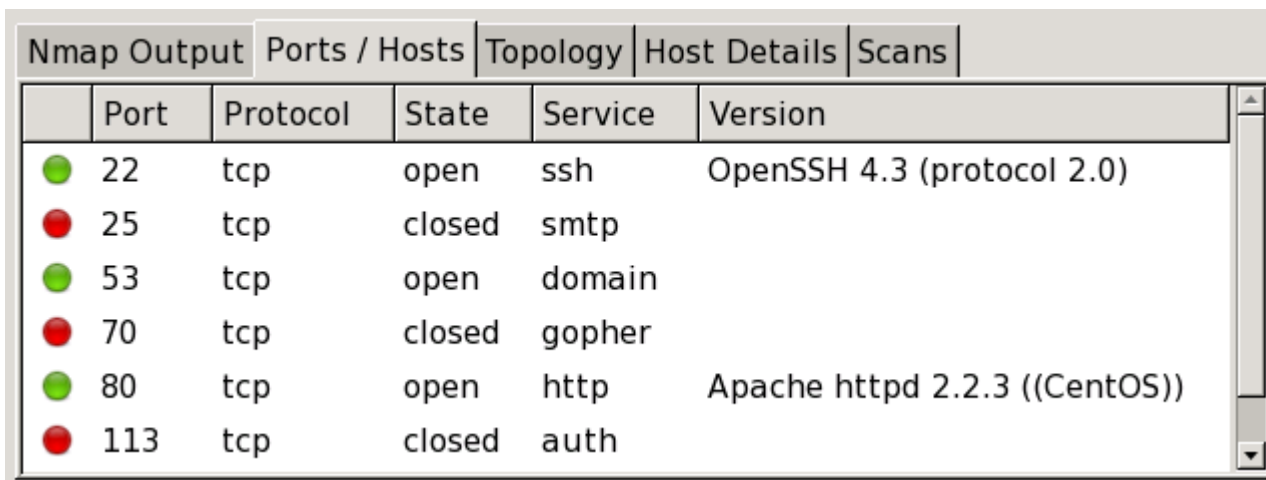
- Ports/Hosts: mostra i risultati elencando le porte e i servizi corrispondenti.
- Topology: mostra il traceroute per la scansione appena effettuata.
- Host Details: Questa scheda mostra tutto ciò che la scansione ha collezionato sul bersaglio durante la scansione.
- Scans: Questa scheda memorizza i comandi usati per lanciare le tue scansioni precedenti per riutilizzarle.

Nella sezione Nmap Output vedrete tutto il dettaglio delle informazioni raccolte dal comando nmap.



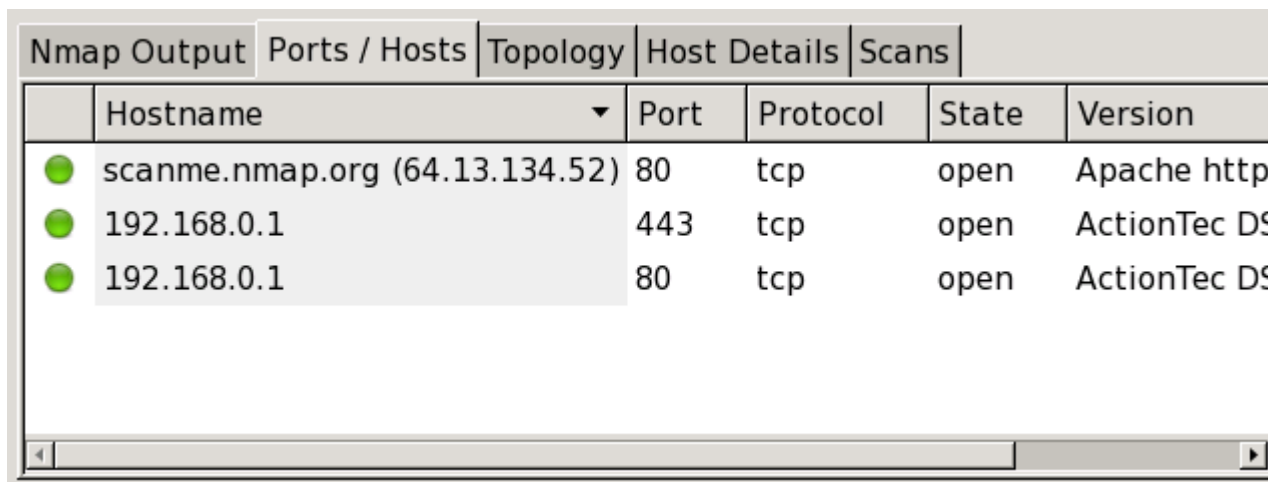
The screenshot shows the Nmap Output window with the following content:

```
Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -T4 -A -v scanme.nmap.org
host)
Initiating OS detection (try #1) against scanme.nmap.org
(64.13.134.52)
Initiating Traceroute at 12:05
Completed Traceroute at 12:05, 0.29s elapsed
Initiating Parallel DNS resolution of 12 hosts. at 12:05
Completed Parallel DNS resolution of 12 hosts. at 12:05, 6.64s
elapsed
NSE: Script scanning 64.13.134.52.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 12:05
Completed NSE at 12:05, 4.17s elapsed
Nmap scan report for scanme.nmap.org (64.13.134.52)
Host is up (0.074s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024
60:ac:4d:51:b1:cd:85:09:12:16:92:76:1d:5d:27:6e (DSA)
|_ 2048 2c:22:75:60:4b:c3:3b:18:a2:97:2c:96:7e:28:dc:dd (RSA)
25/tcp    closed smtp
```



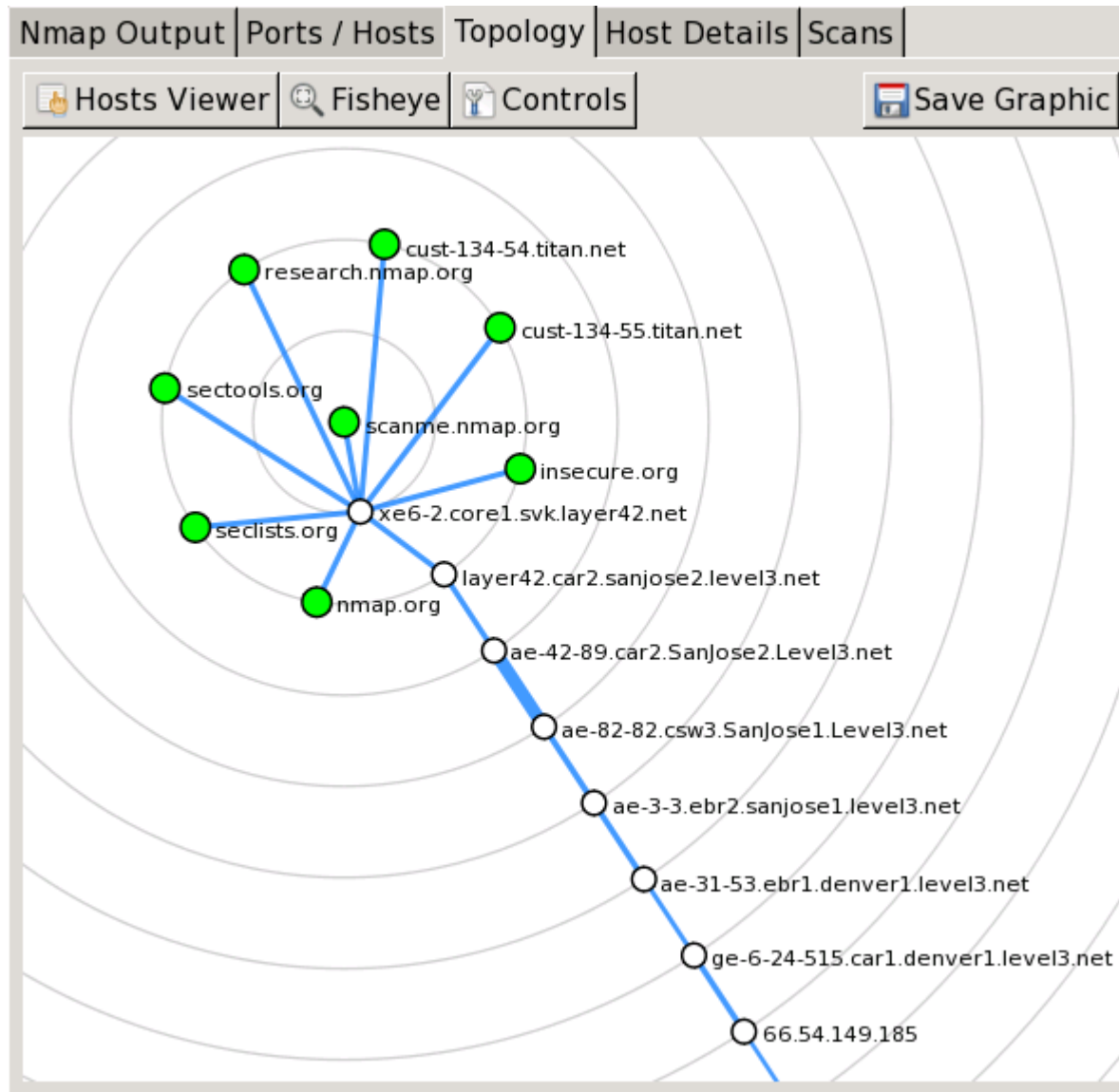
Nmap Output Ports / Hosts Topology Host Details Scans

Port	Protocol	State	Service	Version
22	tcp	open	ssh	OpenSSH 4.3 (protocol 2.0)
25	tcp	closed	smtp	
53	tcp	open	domain	
70	tcp	closed	gopher	
80	tcp	open	http	Apache httpd 2.2.3 ((CentOS))
113	tcp	closed	auth	



Nmap Output Ports / Hosts Topology Host Details Scans

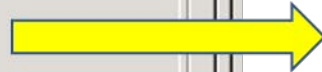
Hostname	Port	Protocol	State	Version
scanme.nmap.org (64.13.134.52)	80	tcp	open	Apache http
192.168.0.1	443	tcp	open	ActionTec DS
192.168.0.1	80	tcp	open	ActionTec DS



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

▼ scanme.nmap.org (64.13.134.52)

- ▶ **Comments**
- ▼ **Host Status**
  - State: up
  - Open ports: 3
  - Filtered ports: 993
  - Closed ports: 4
  - Scanned ports: 1000
  - Up time: 1961342
  - Last boot: Thu Jun 24 19:16:43 2010
- ▼ **Addresses**
  - IPv4: 64.13.134.52
  - IPv6: Not available
  - MAC: Not available
- ▼ **Hostnames**
  - Name - Type: scanme.nmap.org - user



0-2 porte



3-4 porte



5-6 porte

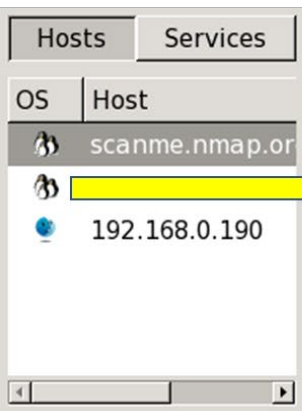
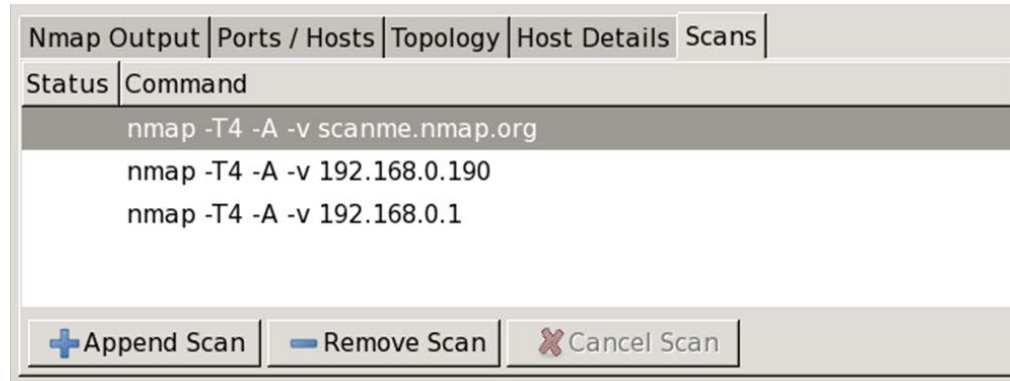


7-8 porte



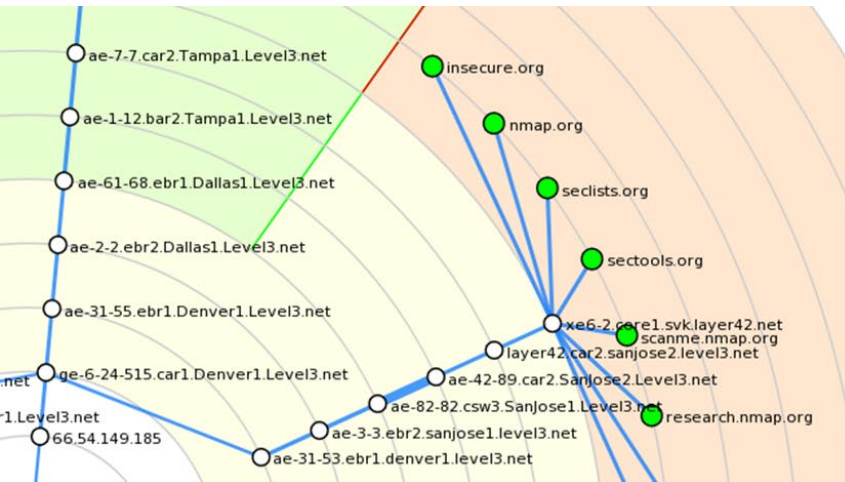
9 + porte

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali





# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



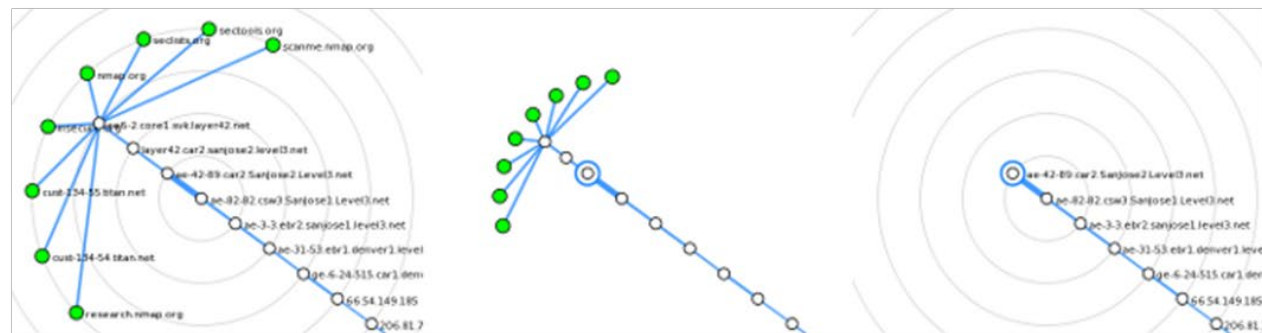
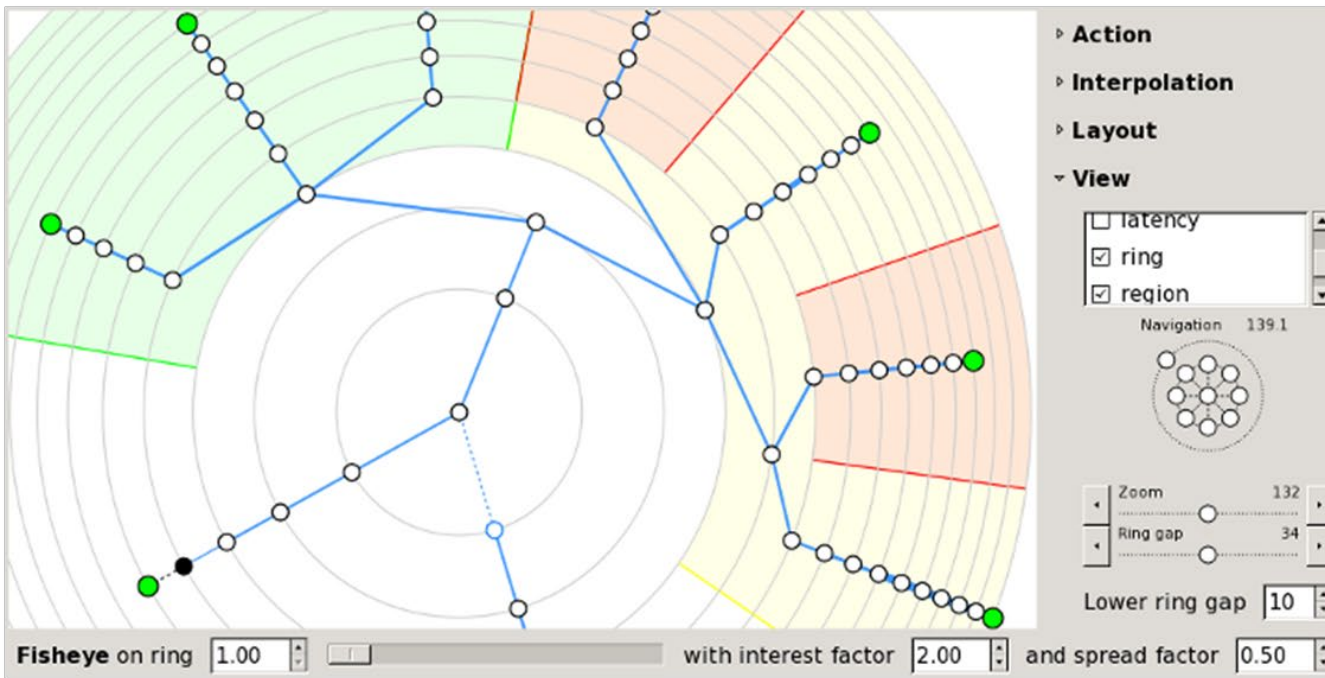
The topology view uses many symbols and color conventions. This section explains what they mean.

- Each regular host in the network is represented by a little circle. The color and size of the circle is determined by the number of open ports on the host. The more open ports, the larger the circle. A white circle represents an intermediate host in a network path that was not port scanned. If a host has fewer than three open ports, it will be green; between three and six open ports, yellow; more than six open ports, red.
- If a host is a router, switch, or wireless access point, it is drawn with a square rather than a circle.
- Network distance is shown as concentric gray rings. Each additional ring signifies one more network hop from the center host.
- Connections between hosts are shown with colored lines. Primary traceroute connections are shown with blue lines. Alternate paths (paths between two hosts where a different path already exists) are drawn in orange. Which path is primary and which paths are alternates is arbitrary and controlled by the order in which paths were recorded. The thickness of a line is proportional to its round-trip time; hosts with a higher RTT have a thicker line. Hosts with no traceroute information are clustered around localhost, connected with a dashed black line.
- If there is no RTT for a hop (a missing traceroute entry), the connection is shown with a blue dashed line and the unknown host that makes the connection is shown with a blue outline.

Some special-purpose hosts may carry one or more icons describing what type of host they are:

- 🔌 A router.
- 🔌 A switch.
- 📶 A wireless access point.
- 🚫 A firewall.
- 🚫 A host with some ports filtered.

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



## NMAP HANDS ON

Overview di alcuni parametri importanti:

**-sS** esegue una scansione SYN stealth, meno rintracciabile di una scansione normale, ma più lenta.

Molti firewall aggiornati possono comunque rilevarla.

**-sn** effettua una scansione di tipo ping. La scansione delle porte verrà disabilitata e vedrete solo se il target è online.

**-O** pratica una scansione sul sistema operativo. La scansione proverà a determinare il sistema operativo utilizzato.

**-A** questo parametro esegue le scansioni più comuni: scansione del sistema operativo, della versione, scan tramite script e traceroute.

**-F** è il parametro abilita la modalità veloce, ma riduce il numero di porte scansionate.

**-v** mostrerà più informazioni nei risultati, rendendoli più semplici da leggere e interpretare.

**-vv** oppure **-v -v** come sopra ma con maggiori dettagli.

**-PO** diciamo a Nmap di non pingare l'host bersaglio, utile se sappiamo che l'host è up.

**-PT** pinga sulla porta 80 con un TCP Ack invece che con ICMP.

**-T0** oppure **-T Paranoid** è la modalità più prudente, in grado di eludere anche gli IDS, esegue lo scan in modo seriale ed aspetta almeno 5 minuti tra uno scan e l'altro, da T1 a T4 impiega sempre meno tempo con T5 viaggia alla massima velocità, rischia di perdere pacchetti e di far crashare il TARGET

## NMAP HANDS ON

Il range di sistemi da scansionare possono essere scritti con wildcard:

`nmap 192.168.1.1,2,3` scansiona i primi 3 IP della stessa subnet

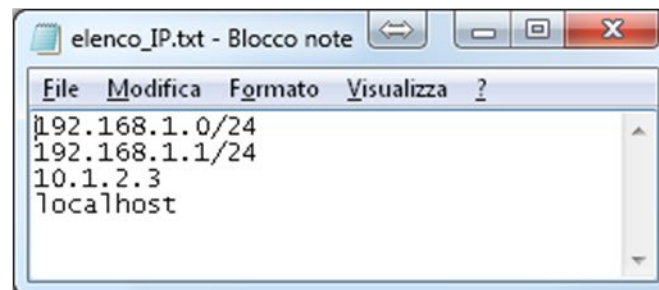
`nmap 192.168.1.1-20` scansiona i primi 20 IP della stessa subnet

`nmap 192.168.1.*` scansiona tutta la subnet

`nmap 192.168.1.0/24` scansiona tutta la subnet

`nmap 192.168.1.0/24 --exclude 192.168.1.5` esclude un indirizzo

`nmap -iL /mgx/desktop/elenco_IP.txt`



## NMAP HANDS ON

```
nmap -A 192.168.1.254 --  
nmap -v -A 192.168.1.1 | -> Rilevazione del Sistema Operativo  
nmap -A -iL /mgx/desktop/elenco_IP.txt --
```

nmap -sA 192.168.1.254 Rilevazione di un sistema filtrato da un firewall

nmap -PN 192.168.1.1 Rilevazione di un sistema protetto da un firewall

nmap --packet-trace 192.168.1.1 Visualizza tutti i pacchetti inviati e ricevuti

nmap -sV 192.168.1.1 Rileva e visualizza la versione del servizio rilevato

nmap -PS 192.168.1.1 Se un firewall blocca ICMP potete usare TCP Syn

nmap -PA 192.168.1.1 Se un firewall blocca ICMP potete usare TCP Ack

nmap -f 192.168.1.1 Frammenta i pacchetti per eludere il firewall

## NMAP HANDS ON

### Firewall evasion con IP spoofing

Sintassi “nmap -n -Ddecoy-ip1,decoy-ip2,il\_tuo\_ip,decoy-ip3,decoy-ip4 TARGET”

```
nmap -n -D192.168.1.5,10.5.1.2,172.1.2.4,3.4.2.1 192.168.1.5
```

### Firewall evasion con MAC address spoofing

Sintassi “nmap --spooof-mac MAC-ADDRESS-HERE TARGET”

```
nmap -v -sT -PN --spooof-mac 0 192.168.1.1 Con 0 il MAC viene generato in modo causale
```

NESSUS



Nessus possiede un archivio di oltre 100.000 plugin. Ognuno con particolari compiti di

- host discovery
- vulnerability identification
- flaws exploitability
- compliance checks
- configuration auditing

Il prodotto si aggiorna continuamente per coprire le molteplici nuove vulnerabilità che vengono scoperte, non esiste un prodotto che vanta la stessa esperienza ed efficacia di Nessus nel mercato!

L'utente di Nessus dispone di un Support Portal dove può accedere a tutti i servizi professionali, messi a disposizione da Tenable.





# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



# Foca

OPEN SOURCE

The screenshot displays the Foca OSINT tool interface with three main windows:

- IPNetInfo:** Shows a table with columns: Order, IP Address, Status, Country, Network Name, Owner Name, From IP. The first entry is: Order 1, IP Address 151.99.23.22, Status Succeed, Country Italy, Network Name INTERBUSINESS, Owner Name Telecom Italia SPA, From IP 151.99.23.0.
- DomainHostingView:** Shows details for domain 'adora-ic.com'. Tech State/Province: REDACTED FOR PRIVACY. Tech Postal Code: REDACTED FOR PRIVACY. Tech Country: REDACTED FOR PRIVACY. Tech Phone: REDACTED FOR PRIVACY. Tech Phone Ext: REDACTED FOR PRIVACY. Tech Fax: REDACTED FOR PRIVACY. Tech Fax Ext: REDACTED FOR PRIVACY. Tech Email: 2lrvrnx75fh77zxwhzfxk.o-w-o.info. Name Server: dns200.anycast.me. Name Server: ns200.anycast.me. DNSSEC: signedDelegation. URL of the ICANN WHOIS Data Problem Reporting System: <http://wdprs.internic.net/>. Last update of WHOIS database: 2020-05-25T07:55:25.0Z <<<. For more information on Whois status codes, please visit <https://icann.org/ipp>.
- DNSDataView:** Shows a table with columns: Record, Domain, Record Type, Host Name, IP Address, More Data, Section, TTL. Records include: cybers.it NS dns1.lanubadn.net (94.177.216.253), cybers.it NS dns2.lanubadn.net (94.177.216.153), cybers.it NS dns2.techhosted.com (93.110.136.8), cybers.it NS dns1.lanubadn.cz (81.2.216.125), cybers.it MX mx.cybers.it (62.148.126.74), cybers.it A cybers.it (31.11.34.64), cybers.it CNAME, and cybers.it SOA dns2.techhosted.com (94.177.216.153).


The screenshot shows the Maltego website homepage. At the top, there is a navigation bar with the Maltego logo on the left and menu items: SOLUTIONS, PRODUCTS, PRICING, RESOURCES, DATA SOURCES, ABOUT US, BUY ONLINE, and GET QUOTE. The main content area has a dark blue background. On the left, a large white text block reads "INTEL 471 DATA BUNDLES & WEBINAR!". Below this, a paragraph of text describes the availability of Intel 471 data bundles and mentions a webinar with Robert McArdle from TrendMicro on May 26. Two yellow buttons are positioned below the text: "REGISTER NOW" and "MORE ABOUT DATA BUNDLES". On the right side, a diagram shows a central white person icon at the top, with lines radiating outwards to several grey person icons below. Two of these grey icons are highlighted with orange borders. In the bottom right corner, there are logos for MALTEGO, INTEL471, and TREND MICRO, along with a yellow circular button that says "Get a demo" with a play icon. A vertical "Feedback" button is also visible on the far right edge. At the bottom left, there is a row of seven white circles, with the second one from the left being yellow. A white circular button with a downward arrow is located at the bottom center.

## LA BACCHETTA MAGICA OSINT... ma solo con trasformate a pagamento...

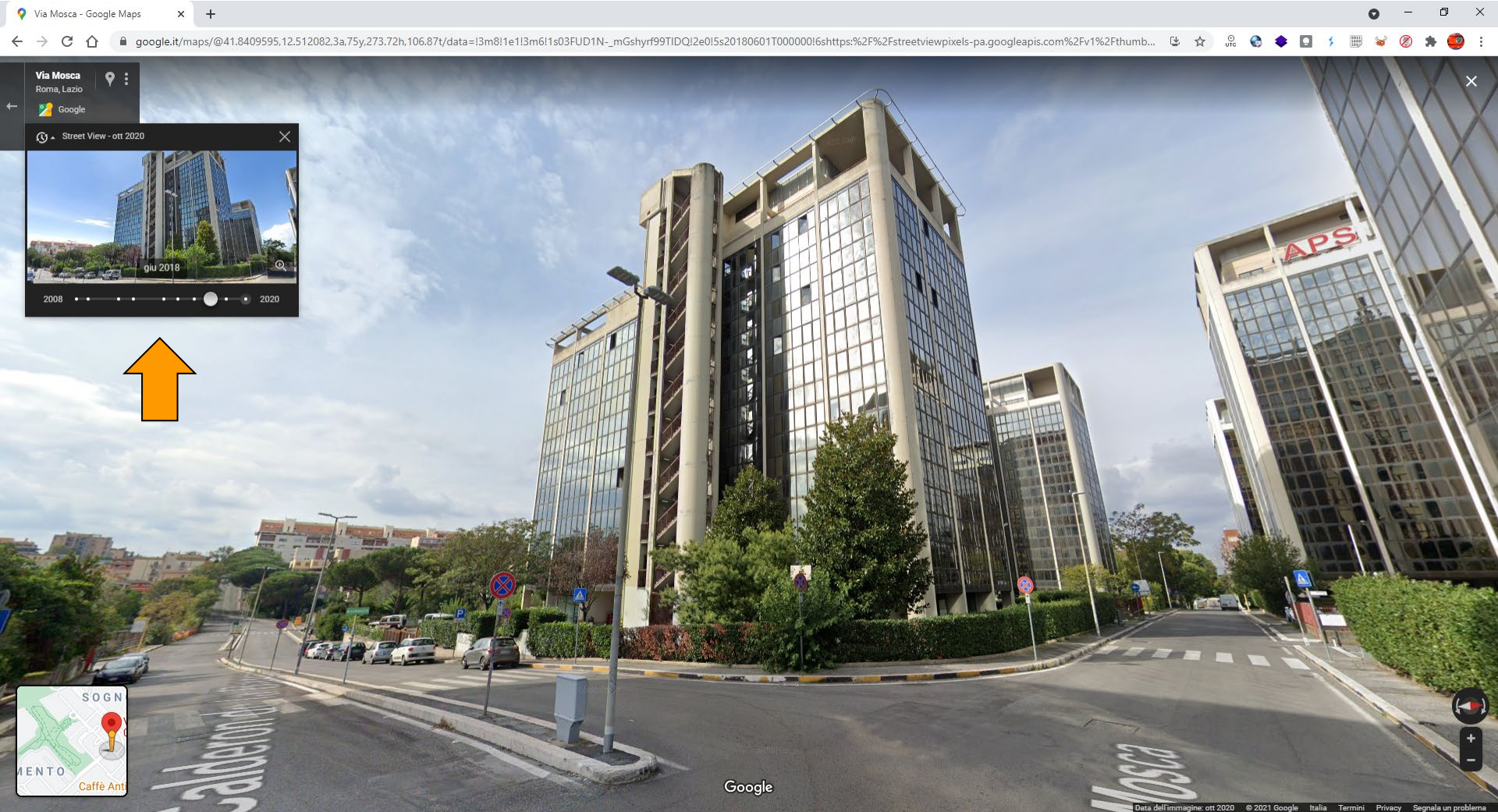
The screenshot displays the Maltego One 4.2.15 - Pro interface. The top menu includes Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import | Export, and Windows. The main area is the Maltego Transform Hub, which shows 59 Hub items total and 11 Hub items installed (1357 Transforms). The interface includes a search bar, filter options (Data Categories, Pricing, Useful for Teams), and a grid of transform partners such as Standard Transforms, CaseFile Entities, AliasDB, ATT&CK - MISP, Blockchain.info (Bitcoin), and CipherTrace (Large Bundle).

# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
-  • Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



## Contenuti di siti rimossi o modificati (i **testimoni virtuali**)

- web.archive.org
- Whois plus (whois.domaintools.com, who.is)
- Reverse whois (reversewhois.io)
- Many tools (yougetsignal.com)
- spamhaus.org (rosko)
- esplorare i certificati SSL
- messaggi di errore con banner parlanti
- web-sniffer.net
- siteliner.com (copie di siti web)  
come scoprire se i contenuti del sito sono copiati da altri
- copia **cache** social network cache: <https://www.facebook.com/ACMilan/>



# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali

Wayback Machine

Non sicuro | web.archive.org/web/\*/%20mgx.net

INTERNET ARCHIVE WEB BOOKS VIDEO AUDIO SOFTWARE IMAGES

SIGN UP | LOG IN | UPLOAD

ABOUT BLOG PROJECTS HELP DONATE CONTACT JOBS VOLUNTEER PEOPLE

INTERNET ARCHIVE Explore more than 566 billion web pages saved over time

DONATE WayBackMachine

mgx.net Results: 50 100 500

Calendar · Collections <sup>beta</sup> · Changes <sup>beta</sup> · Summary · Site Map

Saved 176 times between December 6, 1998 and April 11, 2021.

JAN	FEB	MAR	APR
	1 2	1 2 3 4 5 6	
3 4 5 6 7 8 9	7 8 9 10 11 12 13	7 8 9 10 11 12 13	1 2 3
10 11 12 13 14 15 16	14 15 16 17 18 19 20	14 15 16 17 18 19 20	4 5 6 7 8 9 10
17 18 19 20 21 22 23	21 22 23 24 25 26 27	21 22 23 24 25 26 27	11 12 13 14 15 16 17
24 25 26 27 28 29 30	28	28 29 30 31	18 19 20 21 22 23 24
31			25 26 27 28 29 30

## Social network

- [site:www.facebook.com cybera](https://www.facebook.com/cybera)
- [site:www.facebook.com "Mario Rossi" \(Immagini\)](https://www.facebook.com/MarioRossi)
- [site:www.linkedin.com "Mario Rossi" \(Immagini\)](https://www.linkedin.com/MarioRossi)
- <https://independent.academia.edu/>
- <https://core.ac.uk/>
- <https://onemilliontweetmap.com/>
- <https://www.tweeplers.com/map/>
- <https://www.hashatit.com/hashtags/etna>

## Biblioteche internazionali

- <https://www.loc.gov/search/?in=&q=graziani&new=true&st=>
- <https://www.loc.gov/resource/sn83030272/1908-02-02/ed-1/?st=gallery>

## Mappe della conoscenza

- <https://openknowledgemaps.org/>

## Mappe arricchite

<http://metrocosm.com/disputed-territories-map.html>

<https://www.healthmap.org/en/>

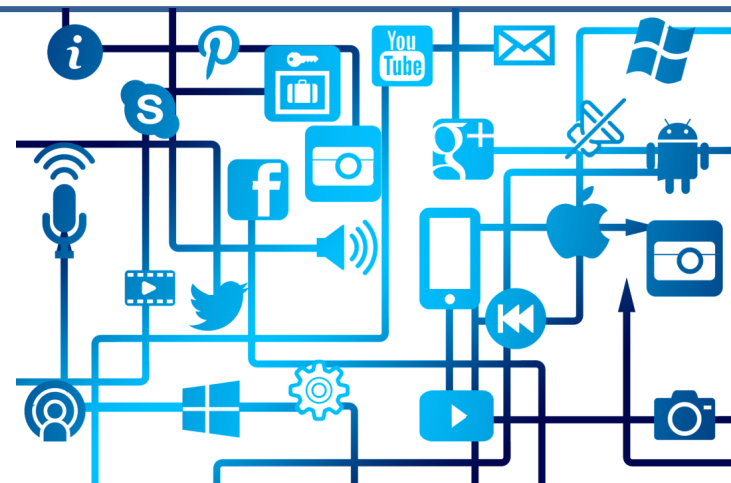
<https://www.marinetraffic.com/en/ais/home/centerx:10.5/centery:42.0/zoom:4>

<https://www.flightradar24.com/43.15,12.11/6>

<https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map>

<https://acleddata.com/dashboard/#/dashboard>

<https://newspapermap.com/#38.13456,14.89197,8z>





*Vediamoli direttamente, non serve prendere appunti perché nelle slide on line troverete la solita sezione:*

*SITOGRAFIA con tutti gli URL aggiornati*

*Vediamo prima come si analizzano alcuni dati pubblici come l'header della email e le pagine celate nel robots.txt*

*GHDB: Directory Listing e altro di riservato in rete*

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



**BLACKLISTING** isn't the **ONLY** email delivery issue [LEARN MORE](#)

## SPF and DKIM Information

dmarc:iqons.biz

Hide

Solve Email Delivery Problems

[Feedback](#) [Contact](#) [Terms & Conditions](#) [Site Map](#) [API](#) [Privacy](#)

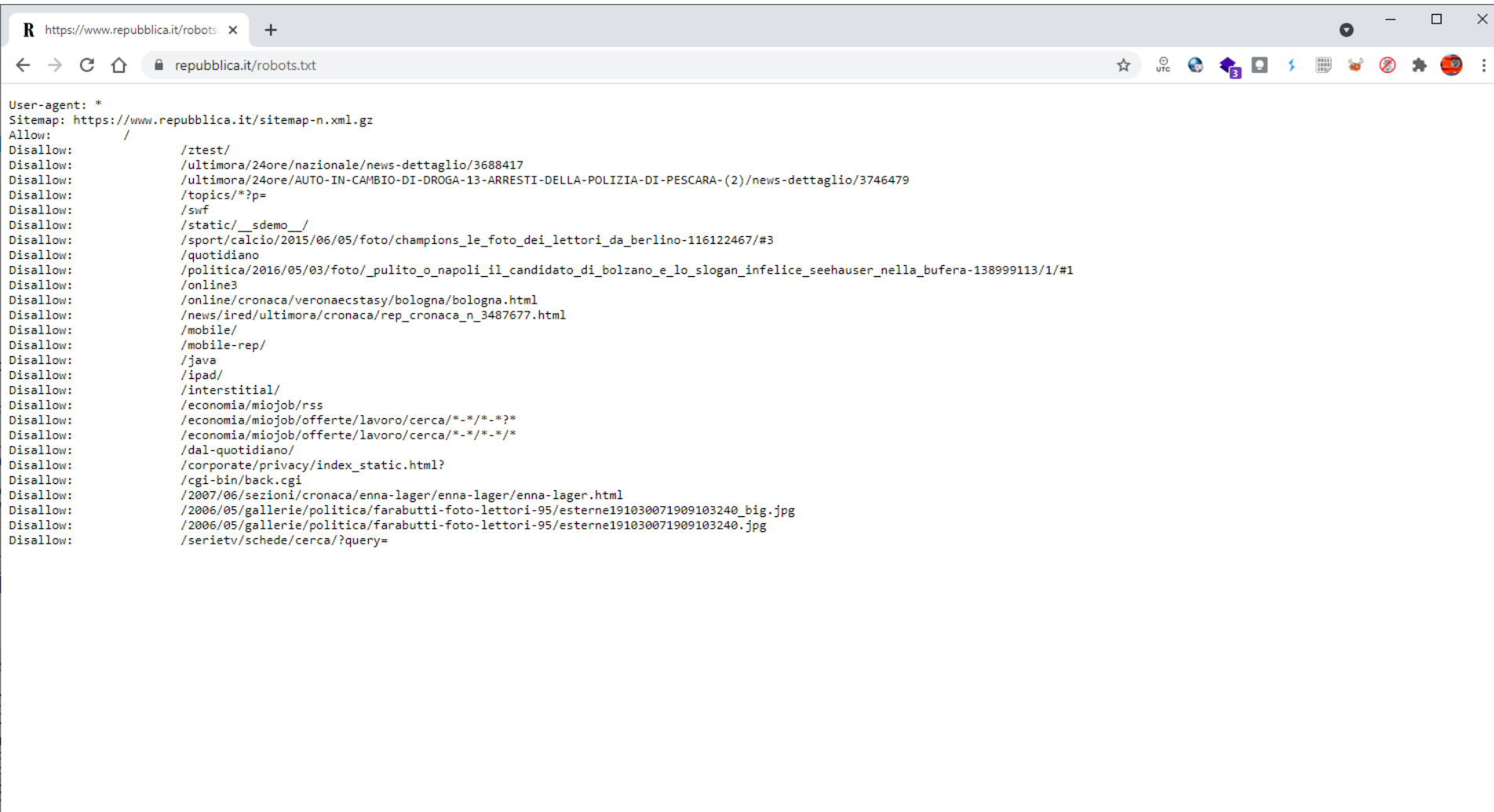
Your IP is: 93.47.1.121

Phone: (888)-MXTOOLBOX / (888)-888-8852 | [feedback@mxtoolbox.com](mailto:feedback@mxtoolbox.com)

© Copyright 2004-2021, MXToolBox, Inc. All rights reserved

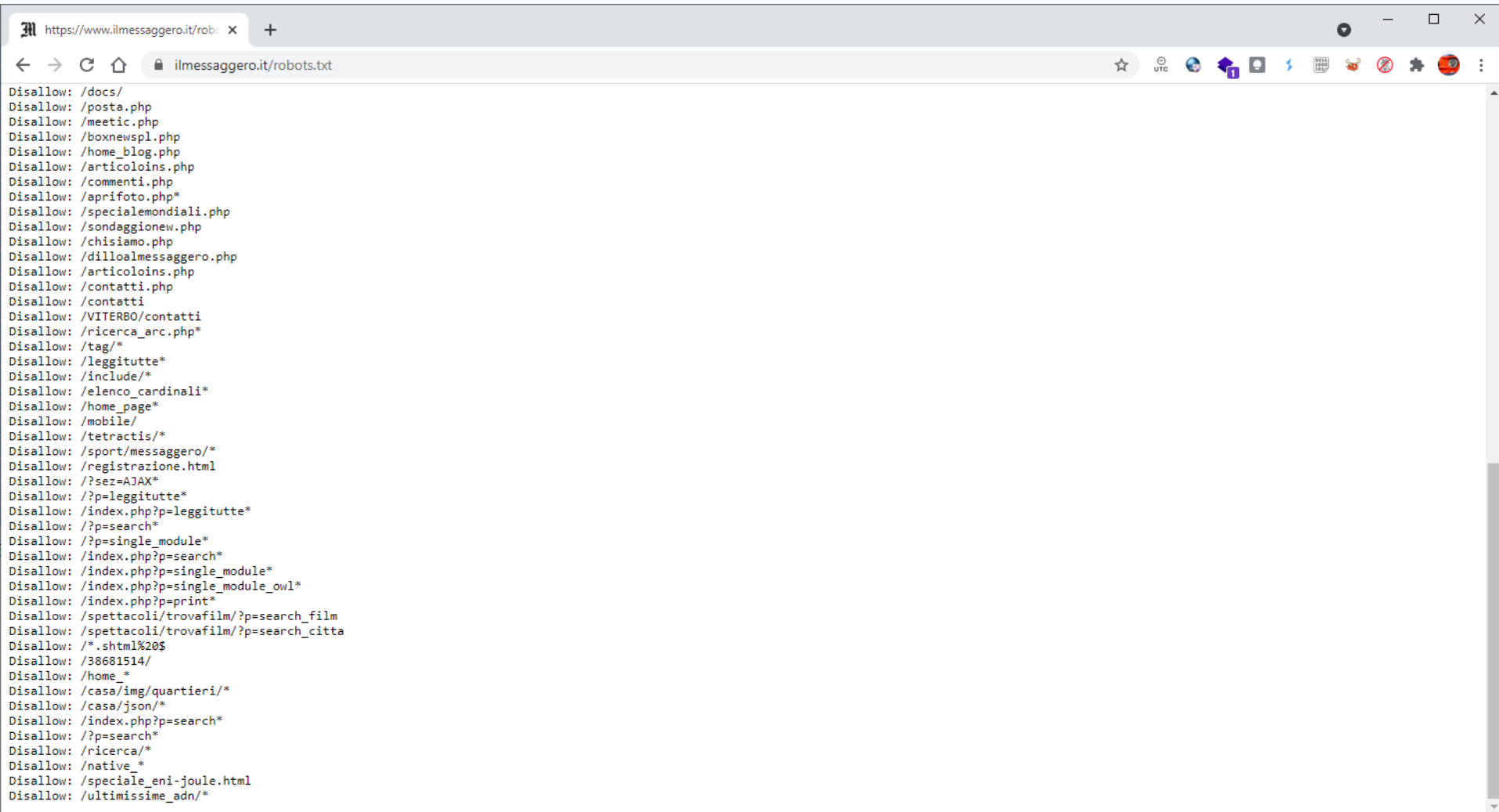


# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



```
User-agent: *
Sitemap: https://www.repubblica.it/sitemap-n.xml.gz
Allow: /
Disallow: /ztest/
Disallow: /ultimora/24ore/nazionale/news-dettaglio/3688417
Disallow: /ultimora/24ore/AUTO-IN-CAMBIO-DI-DROGA-13-ARRESTI-DELLA-POLIZIA-DI-PESCARA-(2)/news-dettaglio/3746479
Disallow: /topics/*?p=
Disallow: /swf
Disallow: /static/_sdemo_/
Disallow: /sport/calcio/2015/06/05/foto/champions_le_foto_dei_lettori_da_berlino-116122467/#3
Disallow: /quotidiano
Disallow: /politica/2016/05/03/foto/_pulito_o_napoli_il_candidato_di_bolzano_e_lo_slogan_infelice_seehauser_nella_bufer-138999113/1/#1
Disallow: /online3
Disallow: /online/cronaca/veronaecstasy/bologna/bologna.html
Disallow: /news/ired/ultimora/cronaca/rep_cronaca_n_3487677.html
Disallow: /mobile/
Disallow: /mobile-rep/
Disallow: /java
Disallow: /ipad/
Disallow: /interstitial/
Disallow: /economia/miojob/rss
Disallow: /economia/miojob/offerte/lavoro/cerca/*-/*-*?
Disallow: /economia/miojob/offerte/lavoro/cerca/*-/*-*/*
Disallow: /dal-quotidiano/
Disallow: /corporate/privacy/index_static.html?
Disallow: /cgi-bin/back.cgi
Disallow: /2007/06/sezioni/cronaca/enna-lager/enna-lager/enna-lager.html
Disallow: /2006/05/gallerie/politica/farabutti-foto-lettori-95/esterne191030071909103240_big.jpg
Disallow: /2006/05/gallerie/politica/farabutti-foto-lettori-95/esterne191030071909103240.jpg
Disallow: /serietv/schede/cerca/?query=
```

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



```
Disallow: /docs/
Disallow: /posta.php
Disallow: /meetic.php
Disallow: /boxnewspl.php
Disallow: /home_blog.php
Disallow: /articoloins.php
Disallow: /commenti.php
Disallow: /aprifoto.php*
Disallow: /specialemondiali.php
Disallow: /sondaggionew.php
Disallow: /chisiamo.php
Disallow: /dilloalmessaggero.php
Disallow: /articoloins.php
Disallow: /contatti.php
Disallow: /contatti
Disallow: /VITERBO/contatti
Disallow: /ricerca_arc.php*
Disallow: /tag/*
Disallow: /leggitutte*
Disallow: /include/*
Disallow: /elenco_cardinali*
Disallow: /home_page*
Disallow: /mobile/
Disallow: /tetractis/*
Disallow: /sport/messaggero/*
Disallow: /registrazione.html
Disallow: /?sez=AJAX*
Disallow: /?p=leggitutte*
Disallow: /index.php?p=leggitutte*
Disallow: /?p=search*
Disallow: /?p=single_module*
Disallow: /index.php?p=search*
Disallow: /index.php?p=single_module*
Disallow: /index.php?p=single_module_owl*
Disallow: /index.php?p=print*
Disallow: /spettacoli/trovafilm/?p=search_film
Disallow: /spettacoli/trovafilm/?p=search_citta
Disallow: /*.shtml%20$
Disallow: /38681514/
Disallow: /home_*
Disallow: /casa/img/quartieri/*
Disallow: /casa/json/*
Disallow: /index.php?p=search*
Disallow: /?p=search*
Disallow: /ricerca/*
Disallow: /native_*
Disallow: /speciale_eni-joule.html
Disallow: /ultimissime_adn/*
```

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali

Google Hacking Database (GHDE) x +

exploit-db.com/google-hacking-database

## EXPLOIT DATABASE

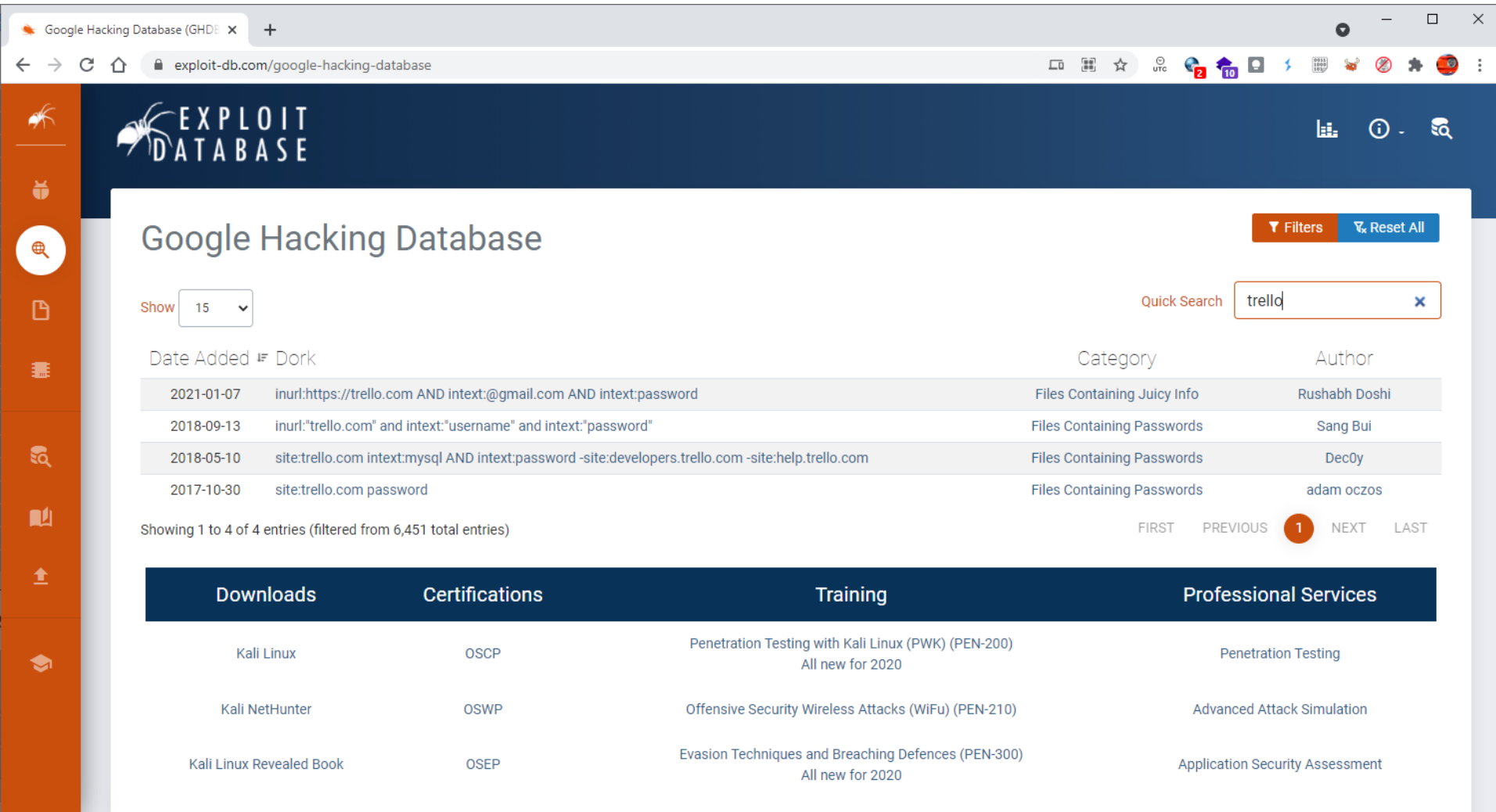
### Google Hacking Database

Filters Reset All

Show 15 Quick Search

Date Added	Dork	Category	Author
2021-05-18	"Cisco Systems, Inc. All Rights Reserved." -cisco.com filetype:jsp	Web Server Detection	J. Igor Melo
2021-05-18	intitle:"Gargoyle Router Management Utility" intext:"Enter Admin Password"	Pages Containing Login Portals	J. Igor Melo
2021-05-18	intitle:"Yealink" inurl:"servlet?m="	Various Online Devices	J. Igor Melo
2021-05-18	intitle:"Device(" intext:"ActiveX Mode (For IE Browser)"	Various Online Devices	J. Igor Melo
2021-05-18	intitle:"OpenWrt - LuCI" intext:"Powered by LuCI   OpenWrt"	Pages Containing Login Portals	Mugdha Peter Bansode
2021-05-18	intitle:HP LASERJET PRO MFP inurl:/SSI/index.htm	Various Online Devices	Anmol K Sachan
2021-05-18	filetype:axd inurl:/elmah.axd	Web Server Detection	Prajwal Khante
2021-05-18	"Saferoads VMS" "login"	Pages Containing Login Portals	Strontium
2021-05-14	"Name" "Password" intitle:"LANCOM 1790VA"	Various Online Devices	J. Igor Melo
2021-05-14	intext:clave inurl:admin.php	Pages Containing Login Portals	Aniket Prabhakar
2021-05-14	inurl:/PRESENTATION/PSWD	Various Online Devices	Anmol K Sachan
2021-05-14	intitle:"Teampass" intext:"Server Time"	Pages Containing Login Portals	J. Igor Melo
2021-05-14	intitle:"Login" intext:"(Moka pot)" inurl:"login.php"	Pages Containing Login Portals	J. Igor Melo
2021-05-14	intitle:series "Note: It is recommended to communicate via HTTPS for entering an administrator password."	Various Online Devices	Anmol K Sachan

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



The screenshot shows the Exploit Database website interface. The search bar contains the query 'trello'. The results table displays four entries with their respective dates, search queries, categories, and authors.

Date Added	Dork	Category	Author
2021-01-07	<code>inurl:https://trello.com AND intext:@gmail.com AND intext:password</code>	Files Containing Juicy Info	Rushabh Doshi
2018-09-13	<code>inurl:"trello.com" and intext:"username" and intext:"password"</code>	Files Containing Passwords	Sang Bui
2018-05-10	<code>site:trello.com intext:mysql AND intext:password -site:developers.trello.com -site:help.trello.com</code>	Files Containing Passwords	Dec0y
2017-10-30	<code>site:trello.com password</code>	Files Containing Passwords	adam oczos

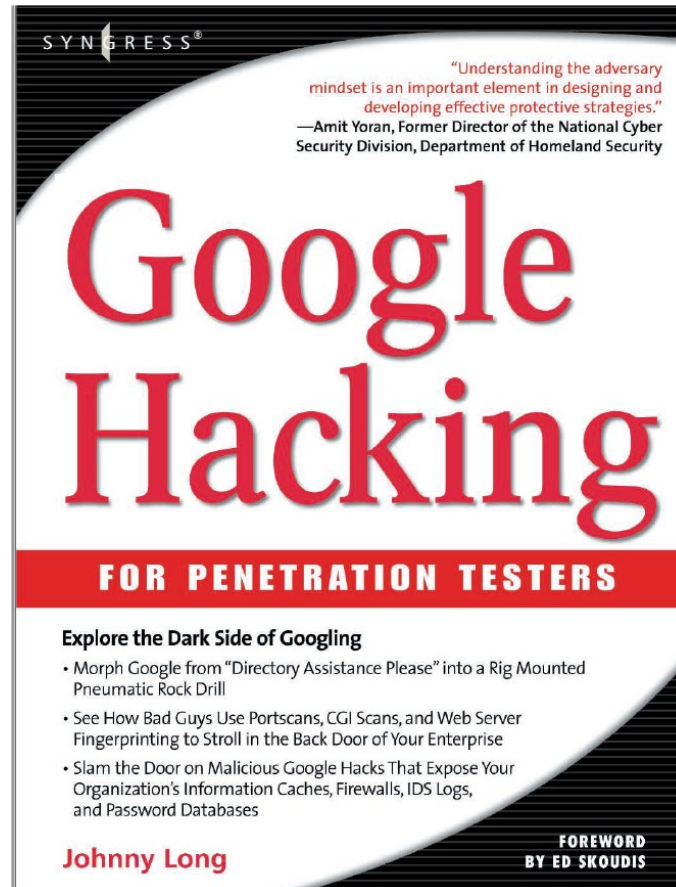
Showing 1 to 4 of 4 entries (filtered from 6,451 total entries)

Navigation: FIRST PREVIOUS 1 NEXT LAST

Downloads	Certifications	Training	Professional Services
Kali Linux	OSCP	Penetration Testing with Kali Linux (PWK) (PEN-200) All new for 2020	Penetration Testing
Kali NetHunter	OSWP	Offensive Security Wireless Attacks (WiFu) (PEN-210)	Advanced Attack Simulation
Kali Linux Revealed Book	OSEP	Evasion Techniques and Breaching Defences (PEN-300) All new for 2020	Application Security Assessment




Google Hacking for penetration testers filetype:pdf



# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
-  • Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A



# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali

Miglior servizio VPN. Sicurezza

nordvpn.com/it/

Il tuo indirizzo IP: 93.471.121 · ISP: Fastweb · Il tuo stato: **Non protetto**

**NordVPN** | Prezzi | Caratteristiche | Server | Cos'è una VPN? | App VPN | Blog | VPN aziendale | **Ottieni NordVPN** | Supporto | Accedi

## La migliore offerta qualità-prezzo: risparmi il 65%

Proteggi le tue attività online. A soli €3.30 al mese.

Offerta a tempo limitato: 65% di sconto sul piano di 2 anni  
00 : 09 : 37 : 24

**Approfitta dell'offerta**

✓ Garanzia soddisfatti o rimborsati di 30 giorni

Questo sito web utilizza i cookie. Per saperne di più, visita la nostra [Informativa sui cookie](#).

**Accetta**

Tor Project | Anonymity Online x +

torproject.org

Tor [Donate Now](#)

[About](#) [Documentation](#) [Support](#) [Community](#) [Blog](#) [Donate](#)

English (en) [Download Tor Browser](#) ↓

# Browse Privately. Explore Freely.

Defend yourself against tracking and surveillance. Circumvent censorship.

[Download Tor Browser](#) ↓

Info su Tor

Tor Browser

Inserisci un indirizzo o avvia una ricerca

Prima volta in Tor Browser? Cominciamo.

Tor Browser 10.0.16  
[Vedi il Changelog](#)

# Naviga. Privatamente.

Sei pronto per l'esperienza di navigazione più privata al mondo.

Cerca con DuckDuckGo


L'utilizzo di Tor è gratuito grazie alle donazioni fatte da persone come te. [Dona Adesso »](#)

Ottieni le ultime info da Tor direttamente nella tua casella di posta elettronica. [Registrati alle Tor News. »](#)

Il Tor Project è una organizzazione non-profit allo scopo di avanzare i diritti e le libertà umane creando e distribuendo software libero con tecnologie per la privacy e l'anonimato, supportando la loro disponibilità e utilizzo senza restrizioni e avanzandone la loro comprensione scientifica e popolare. [Unisciti a noi »](#)

# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
-  • Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A

La distro linux BUSCADOR non è più supportata: eccone una nuova disponibile



About ▾ Initiatives ▾ Supporters ▾ Blog ▾ Shop

Get Involved

## Trace Labs OSINT VM

### Crowdsourced OSINT to Find Missing Persons


The Trace Labs team created a specialized OSINT VM specifically to bring together the most effective OSINT tools and customized scripts we saw being used during our Search Party CTF's. Inspired by the infamous Buscador VM, the Trace Labs OSINT VM was built in a similar way, to enable OSINT investigators participating in the Trace Labs Search Party CTF's a quick way to get started and have access to the most popular OSINT tools and scripts all neatly packaged under one roof.

Download OVA

## See It In Action

# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
-  • Un giro sul Dark Web
- Q&A




ATTENZIONE:

QUELLO CHE VEDRETE IN QUESTO SEMINARIO,  
E' MATERIALE A SCOPO EDUCATIVO.

VI RICORDO CHE EFFETTUARE ACQUISTI SU DARK WEB DI DROGA,  
ARMI, E SERVIZI ILLEGALI, COME ANCHE NAVIGARE E SCARICARE  
CONTENUTI PEDOPORNOGRAFICI COSTITUISCE UN REATO.

## DARK WEB entriamo nella tana del bianconiglio...

[View this email in your browser](#)



BETTER INVESTIGATIONS.

### Your Dark Web Report Is Ready

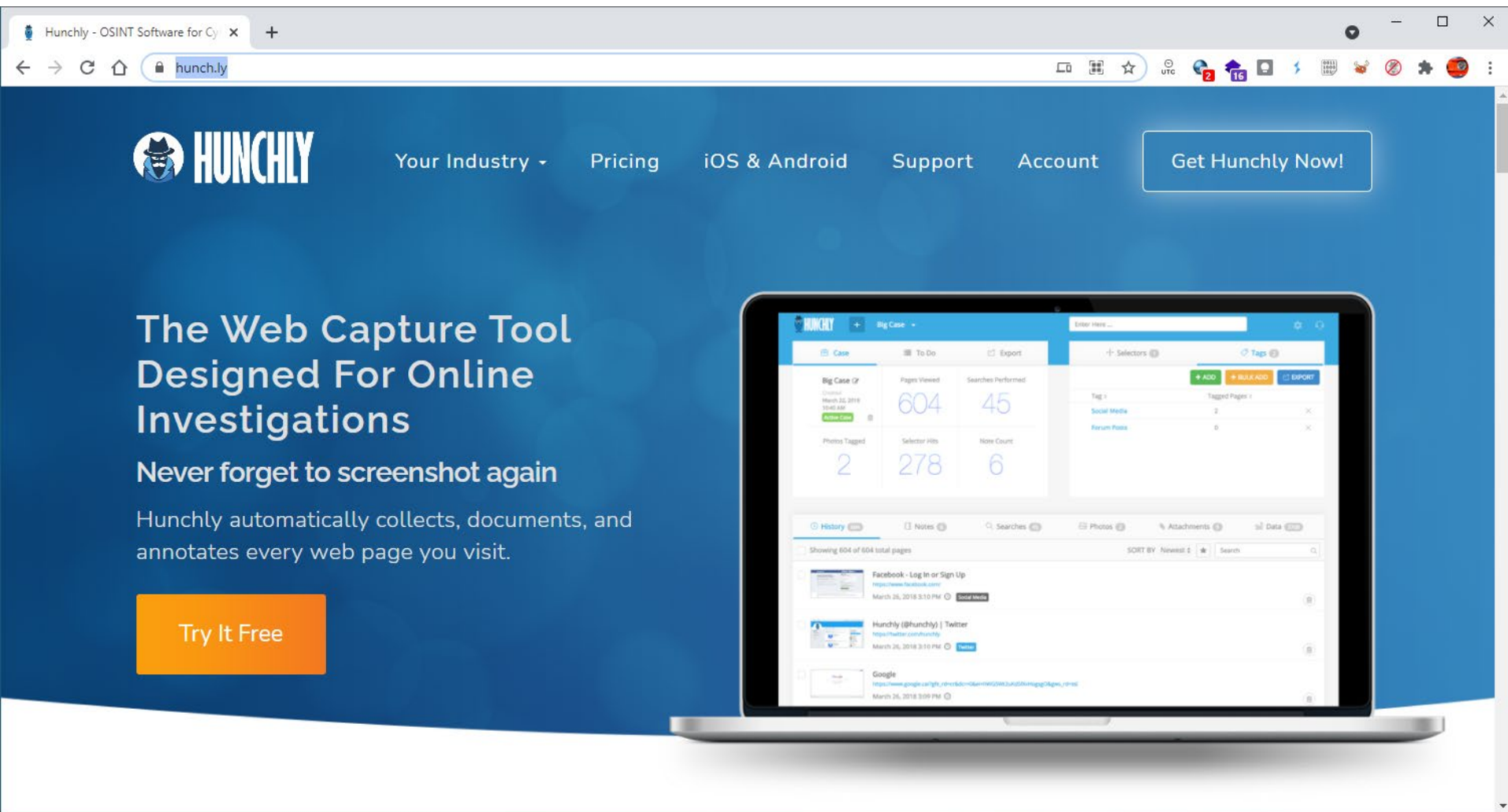
The newest hidden services list is ready for you to download from Dropbox.  
Click the button below to access it.

[Download Report for Monday, February 15, 2021](#)

[Report Archives](#)



# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali



The image shows a browser window displaying the Hunchly website. The browser's address bar shows "hunch.ly". The website has a blue header with the Hunchly logo (a cat wearing a hat) and navigation links: "Your Industry", "Pricing", "iOS & Android", "Support", and "Account". A prominent "Get Hunchly Now!" button is on the right. The main content area features the headline "The Web Capture Tool Designed For Online Investigations" and the sub-headline "Never forget to screenshot again". Below this, it states "Hunchly automatically collects, documents, and annotates every web page you visit." and includes a "Try It Free" button.

The laptop screen displays the Hunchly software interface. It shows a "Big Case" dashboard with the following statistics:

Big Case ID	Pages Viewed	Searches Performed
Created: March 22, 2019 10:48 AM	604	45

Additional statistics shown:

Photos Tagged	Selector Hits	Note Count
2	278	6

The interface also includes a "Selectors" panel with "Social Media" (2 hits) and "Forum Posts" (0 hits). A "History" section at the bottom lists captured pages, including "Facebook - Log In or Sign Up" and "Hunchly (@hunchly) | Twitter".

# OSINT pratico con tool gratuiti o quasi... ossia come si fanno le investigazioni da fonti non convenzionali

The screenshot displays a web browser window with several tabs: 'Info su Tor', 'Check your IP address', 'Store', and 'THIS HIDDEN SITE HAS BEEN...'. The address bar shows the URL: `chemspansi5ouwybtrylkfq3ehjfcac7ea7kt23hk7b6g3qvx2tyd.onion/list_catlistings.php?parent=10`. The website header includes the 'ChemSpain' logo, navigation links for 'Online store' and 'About', and a shopping cart icon showing 'EUR 0'. A blue banner below the header reads 'CATEGORIES'. The main content area features three product listings, each with a 'New!' starburst:

- 500 Xanax Bars 3MG**: 500 Xanax bars of 3mg. Price: 550 EUR. Buy button.
- 1000 Xanax Bars 3MG**: 1000 Xanax bars of 3mg. Price: 980 EUR. Buy button.
- 100gr Alprazolam HCL**: 100gr of pure Alprazolam H... Price: 1000 EUR. Buy button.

Below these are two more product images, also marked 'New!'. On the right side, there is a 'ChemSpain Market' sidebar with a 'Categories' list:

- All (18)
- GBL (3)
- RC's (4)
- Benzos (5)
- GHB (3)
- Bulk orders (2)
- Travels (1)

Info su Tor | Check your | Store | THIS HIDDEN SI | Counterfeit | Black Ma X | Hire a killer, hitn

← → ↻ 🔒 weaponscrzmjlddczhs5dhestbh4m4iyo62dzng3tppatajl4vpmid.onion/shop.php

**BLACK MARKET**

**Desert Eagle 357 Mag GOLD TIGER STRIPE**

1 - 2 - 3

**Remington Defense XM110 SASS 308**

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

**Barrett M107A1 20" CQ FDE 50 BMG QDL Suppressor**

1 - 2 - 3 - 4 - 5 - 6 - 7 - 8 - 9 - 10 - 11

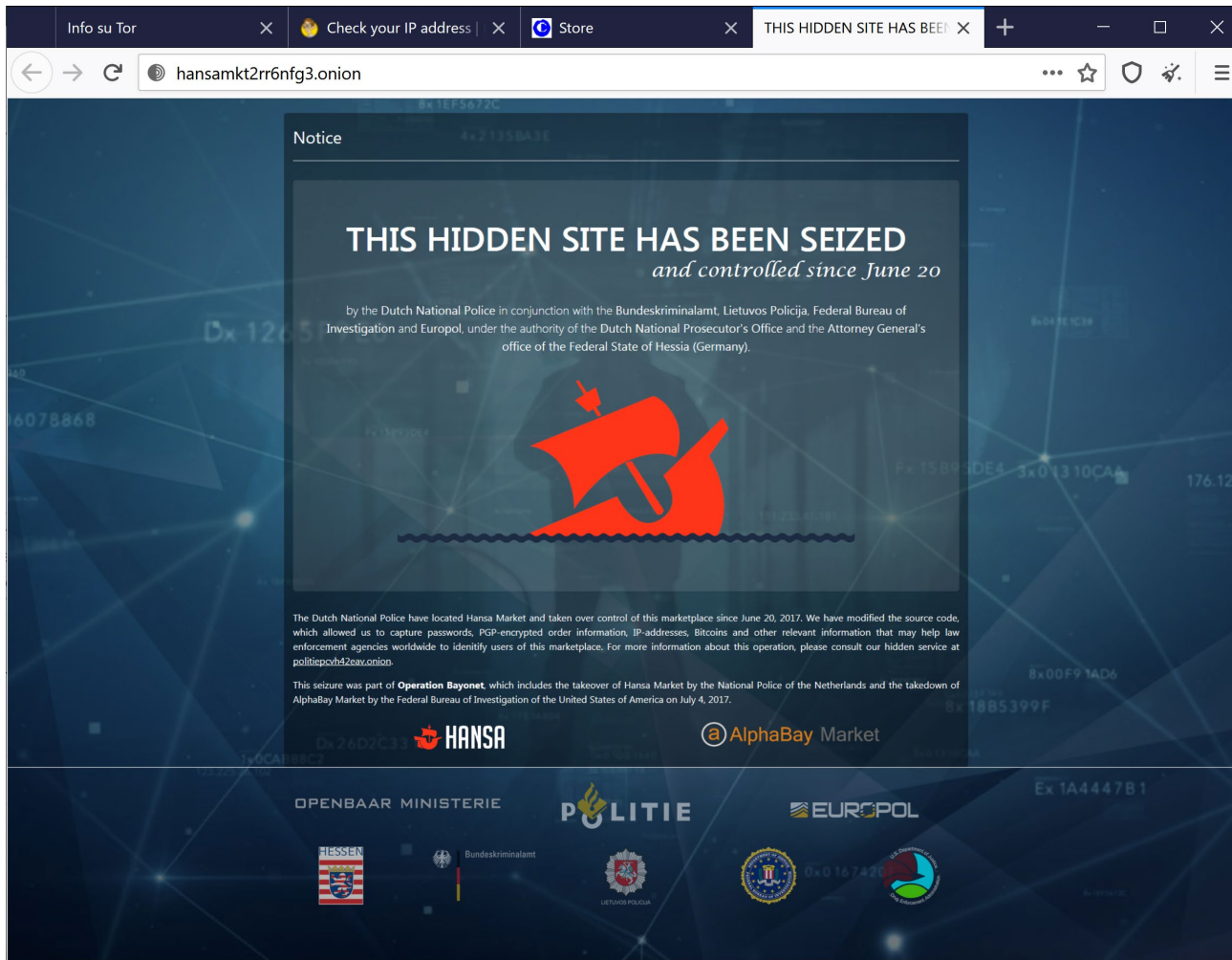
**Features:**  
Manufacturer: Magnum Research  
Model: Desearth Eagle 357

This rifle was one of the designs that Remington Defense submitted for the Military SASS trials. This is a very nice unfired .308/7.62 Nato AR-10 style rifle

It has the upgraded muzzle brake which gives you less recoil, and enables you to stay on target for faster, more accurate follow up shots.

The screenshot shows a browser window with the following elements:

- Browser tabs: Info su Tor, Check your IP, Store, THIS HIDDEN SITE, Counterfeit, Black Market, Hire a killer, Hitman for hire, real contract murders w
- Address bar: marak2kjeehrao5s.onion
- Header navigation: [Mara Salvatrucha](#), [Support](#), [Buyer](#), [Vendor](#), [Video](#), [Create escrow](#), [Login](#)
- Main text area (dark background):
  - Paragraph 1: Welcome to the Mara Salvatrucha marketplace for hire killers all over the world. It is a well known branch of gang engaged in contract killings through the Dark Network. We are doing business in many areas like the USA, Europe, China, etc. Everywhere. We can kill your sacrifice, kidnap, beat up, rape or burn, etc. Just contact us as need.
  - Paragraph 2: No need to ask us whether we can kill your sacrifice or not, whether we can do it in this city or this place, whether we are a very strong guy, etc. We can do it and we can do it everywhere. Just give us information about job and sacrifice. questions.
  - Paragraph 3: Several years we are available on the Darknet. This is an easy and secure way to offer our services for customers. If you are a weak human and you are not able to kill or beat up your hated man you can ask us to do it instead. If you are a strong man with killing or fighting skills you can ask us to do the job to stay safe and not to go to jail. A new members all over the world. You can also join us and work with us if you are skilled enough.
  - Paragraph 4: We have many businesses outside the Darknet but this business also makes money. Why should we abandon doing a lot of illegal things, unlike the normal internet. Also to keep in touch with customers and members even



# Agenda

---

- Introduzione all'OSINT
- Surface Web, Deep Web e Dark Web
- Strumenti OSINT
- Siti Web OSINT
- Investigare sotto copertura, VPN e TOR
- Buscador è morto, nasce Trace Labs VM
- Un giro sul Dark Web
- Q&A





## Sessione domande e risposte

# Sitografia in ordine di apparizione 1

<http://www.websdr.org/> portale che raccoglie tutti i serve dei radioamatori mondiali, potete ascoltare tutte le frequenze disponibili da diverse antenne posizionate in tutto il mondo!

<https://www.google.it/earth/versions/#download-pro> per scaricare Google Earth Pro

<https://nmap.org/> sito dove è possibile scaricare nmap anche per Windows

<https://www.tenable.com/products/nessus>

<https://github.com/ElevenPaths/FOCA> sito dove è possibile scaricare FOCA, richiede SQL Server

[https://www.nirsoft.net/utils/dns\\_records\\_viewer.html](https://www.nirsoft.net/utils/dns_records_viewer.html) sito dove è possibile scaricare DNS Data View

[https://www.nirsoft.net/utils/domain\\_hosting\\_view.html](https://www.nirsoft.net/utils/domain_hosting_view.html) sito dove è possibile scaricare Domain Hosting View

<https://www.nirsoft.net/utils/ipnetinfo.html> sito dove è possibile scaricare IP Net Info, vedere altri tool a piacere

<https://www.repubblica.it/robots.txt> esempio di disallow su robots.txt

<https://www.ilmessaggero.it/robots.txt> altro esempio di disallow su robots.txt

<https://www.maltego.com/> tool specifico OSINT professionale

<https://www.exploit-db.com/google-hacking-database> ricerche pronte per argomenti

<https://www.google.com/search?q=Google+Hacking+for+penetration+testers+filetype%3Apdf>

<https://nordvpn.com/it> migliore VPN per garantire anonimato su internet

<https://www.torproject.org/> sito dove scaricate TOR Browser per navigare il Dark Web

<https://www.tracelabs.org/initiatives/osint-vm> macchina virtuale Linux con tool OSINT ready to go

<https://www.learnallthethings.net/blog/2020/7/23/rage-against-the-virtual-machines>

<https://www.hunch.ly/> sito dove abbonarsi per elenco siti attivi su darkweb



# Sitografia siti web OSINT

## Social network

[site:www.facebook.com cybera](https://www.facebook.com/cybera)

[site:www.facebook.com “Mario Rossi” \(Immagini\)](https://www.facebook.com/MarioRossi)

[site:www.linkedin.com “Mario Rossi” \(Immagini\)](https://www.linkedin.com/MarioRossi)

<https://independent.academia.edu/>

<https://core.ac.uk/>

<https://onemilliontweetmap.com/>

<https://www.tweeplers.com/map/>

<https://www.hashatit.com/hashtags/etna>

## Biblioteche internazionali

<https://www.loc.gov/search/?in=&q=graziani&new=true&st=>

<https://www.loc.gov/resource/sn83030272/1908-02-02/ed-1/?st=gallery>

## Mappe della conoscenza

<https://openknowledgemaps.org/>

## Mappe arricchite

<http://metrocosm.com/disputed-territories-map.html>

<https://www.healthmap.org/en/>

<https://www.marinetraffic.com/en/ais/home/centerx:10.5/centery:42.0/zoom:4>

<https://www.flightradar24.com/43.15,12.11/6>

<https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map>

<https://acleddata.com/dashboard/#/dashboard>

<https://newspapermap.com/#38.13456,14.89197,8z>

massimiliano.graziani@cybera.it

*Dubbi, altre domande? Desiderate approfondimenti riguardo gli argomenti trattati? Scrivetemi, rispondo sempre a tutti!*

*Grazie...*



*Era il 6 giugno 2018 mentre ero relatore al Security Summit di Roma, non rispondevo al cellulare e non potevo soccorrere mio padre, colto da un infarto, mentre tutti mi chiamavano...*

*Tra sensi di colpa e rimorso per non essere arrivato in tempo per vederlo ancora vivo, per l'ultima volta...*

*...per questo dedico a Giuseppe, mio padre, ogni attività di divulgazione e condivisione accademica, perseguendo i valori che mi ha trasmesso: umiltà, generosità e sacrificio.*

*Grazie di tutto papà.*