Web Investigation

L'APPORTO DELLA DIGITAL FORENSICS AL CONTRASTO ALLA VENDITA ONLINE DI SOSTANZE STUPEFACENTI

Dr.ssa Clara Maria Colombini

Digital Forensics Expert – Cyber Intelligence Expert

Docente DCSA - Direzione Centrale Servizi Antidroga, Ministero dell'Interno, Roma

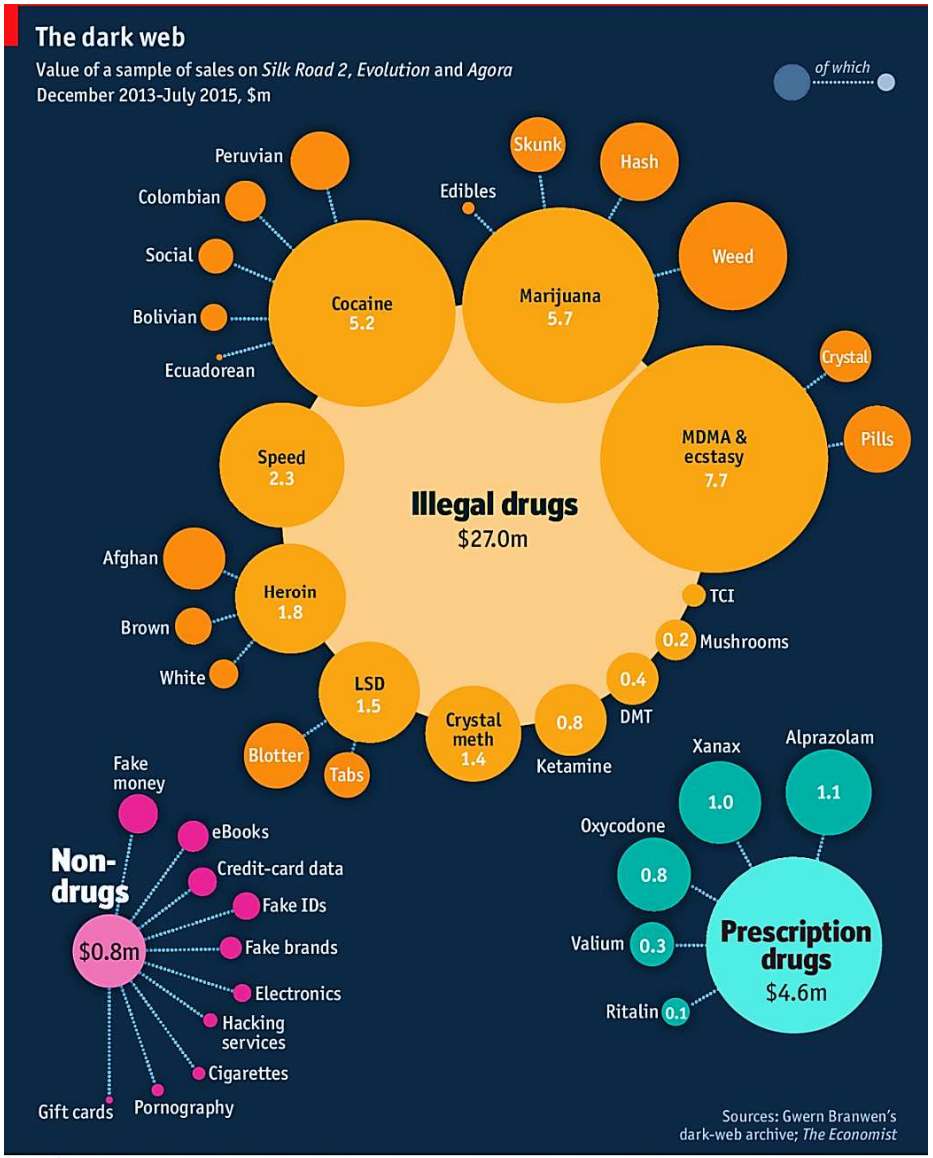
DCSA
Direzione Centrale per i Servizi Antidroga

La Direzione Centrale per i Servizi Antidroga (DCSA) é un organismo interforze composto dalle tre forze di Polizia nazionali (Polizia di Stato, Arma dei Carabinieri e Guardia di Finanza) attraverso il quale il Capo della Polizia attua le direttive emanate dal Ministro dell'Interno in materia di coordinamento e di pianificazione delle forze di polizia per la prevenzione e repressione del traffico illecito di sostanze stupefacenti e psicotrope. Dal 1º luglio 2017 è diretta dal dirigente generale della Polizia di Stato dott. Giuseppe Cucchiara.

LA DCSA:

- coordina le indagini delle forze di polizia sul territorio nazionale ed a livello internazionale;
- si pone come interlocutrice nazionale con i corrispondenti servizi delle polizie estere con contatti diretti o per il tramite dell'O.I.C.P.- INTERPOL e di U.D.E.-EUROPOL;
- utilizza i canali bilaterali attivati a seguito di appositi accordi e la rete degli Esperti e degli Ufficiali di Collegamento antidroga dislocati nei crocevia internazionali della produzione e del traffico illecito;
- è l'unica referente, in Italia ed all'estero, per tutte le operazioni investigative speciali;
- é un servizio nazionale d'intelligence strategica ed operativa nel settore della lotta al traffico delle droghe, operando a beneficio delle forze di polizia e delle dogane;
- cura la formazione specifica del personale di polizia, con l'organizzazione di corsi di specializzazione e di formazione per l'addestramento alle attività di "sottocopertura" e di "sorveglianza", all'analisi criminale e all'informatica;
- in particolare, la sezione operativa «*Drug@Online*» (appartenente al III Servizio) ha il compito di monitorare la rete internet per prevenire e contrastare il commercio illegale di droghe e coordinare le attività di repressione sul territorio nazionale.

LO SCENARIO



LA VENDITA DI SOSTANZE STUPEFACENTI ONLINE E' AUMENTATA ESPONENZIALMENTE NEGLI ULTIMI ANNI

The Economist ha analizzato i dati di 360.00 vendite tra il 2013 e il 2015 su **Agora, Evolution and Silk Road**. (circa 50 milioni di dollari).

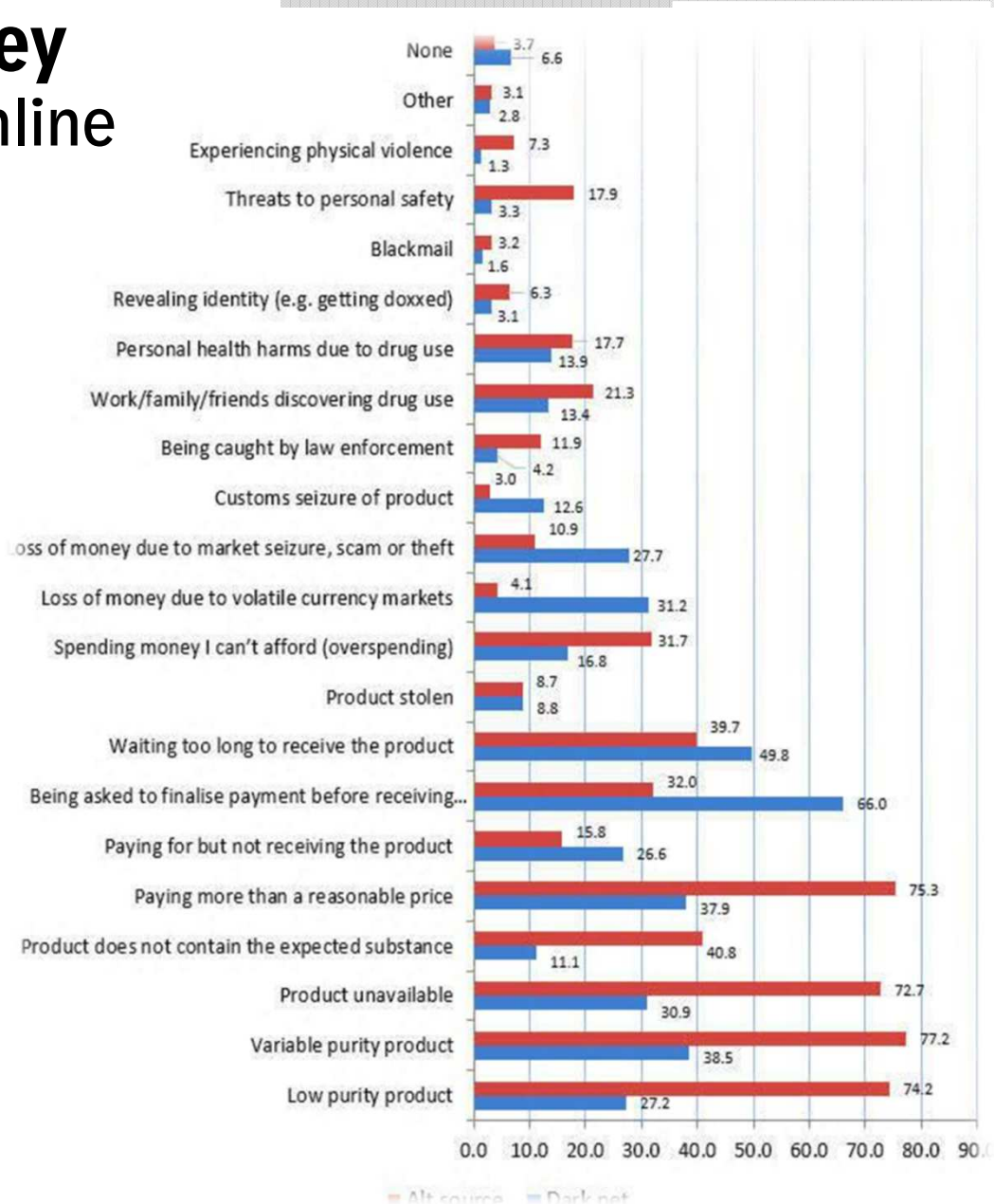
I maggiori ricavi si sono avuti dalla vendita di **MDMA** , mentre la **marijuana** è il prodotto piu' popolare.

Tra i farmaci più venduti l'**oxycodone** e il **diazepam** (Valium).

The Global Drug Survey
Confronto tra la vendita online e quella tradizionale

Motivazioni
per la crescita
dell'acquisto online:

- meno «pericoli» per venditore e cliente
- maggiore qualità dei prodotti
- possibilità di sperimentare nuove droghe
- prezzi più bassi



DI COSA STIAMO PARLANDO?

.....del mercato dei sogni.....

LA VENDITA ONLINE DI SOSTANZE STUPEFACENTI E PSICOTROPE

- I «Black Market» offrono una vasta gamma di sostanze stupefacenti e psicotrope, dalla marijuana fino all'eroina, passando per tutta una serie di droghe sintetiche, senza tralasciare i cosiddetti precursori e i farmaci.
- Il servizio offerto è completo: attraverso Forum dedicati è possibile contattare i venditori o scambiare opinioni sui prodotti e le modalità di invio con altri acquirenti.

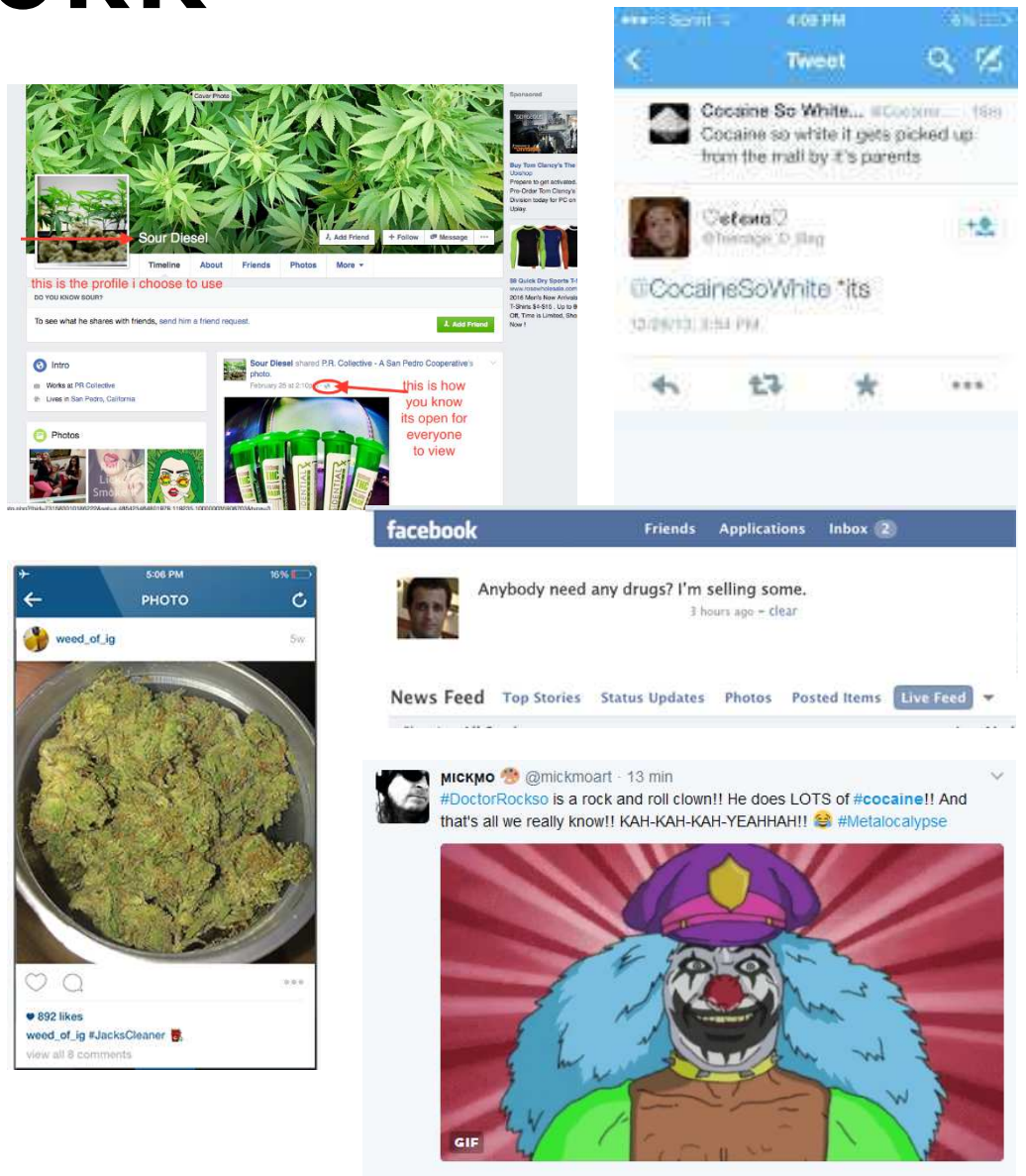
Moneta di scambio sta diventando il **Monero (228 Euro)** acquistabile direttamente presso gli stessi mercati, o meglio presso un «Bitcoin Casino» che farà da tramite per l'acquirente e da «Lavanderia» per il venditore.

NAME	GAMES	PROVABLY FAIR?	DEPOSIT BONUS	CURRENCIES	INTERNATIONAL	VISIT
bitStarz	500	✓	100%	EUR	✓	Visit Site — Bitstarz Review
BitcoinGAMES	7	✓	✗		✓	Visit Site — Bitcoin.com Casino Review
Betchan	400	✓	130%	EU,US,GB	✓	Visit Site — Betchan Casino Review
BetChain	1000+	✓	200%	USD, EUR, RUB, AUD	✓	Visit Site — Betchain Review
LIMOPLAY	600	✓	100%	EUR	✓	Visit Site — Limoplay Review
mBit	900	✓	110%	EUR	✓	Visit Site — mBitcasino Review

I SOCIAL NETWORK

Un altro sviluppo riguarda l'offerta di droga e la condivisione di stupefacenti tramite i social media: **FACEBOOK, TWITTER, INSTAGRAM, WICKR, TELEGRAM, ecc….**

Questo settore è ancora scarsamente conosciuto e difficile da monitorare. Nel complesso, la crescita di mercati delle droghe online e virtuali rappresenta una grande sfida per le politiche per l'applicazione della legge e il controllo degli stupefacenti: il fatto che produttori, fornitori, dettaglianti, servizi di website-hosting e di pagamento possano essere ubicati in paesi diversi rende particolarmente difficile il monitoraggio dei traffici e l'individuazione dei responsabili.



Le APP per i telefoni cellulari

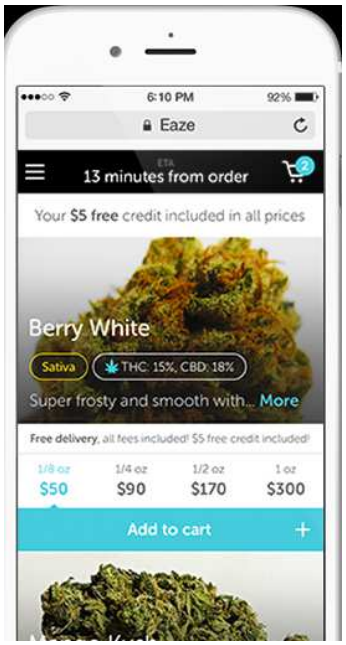
L'ultima frontiera sono le APP per telefoni APPLE e soprattutto ANDROID:

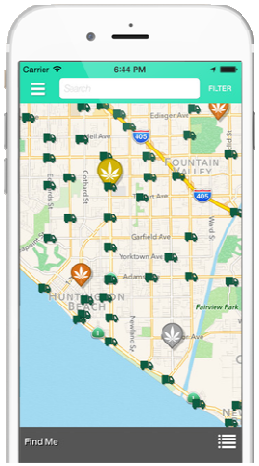
NESTDROP EAZE e NUGG
vendita online

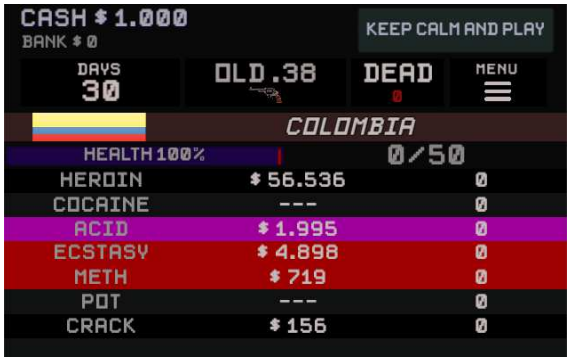
WEEDmaps
mappe ricerca droga

THC Calc – calcola le dosi ottimali
in base ai dati personali
come peso, altezza, età ecc

I'M a Drug Dealer,
Narcotrafficante
le App dello spacciatore







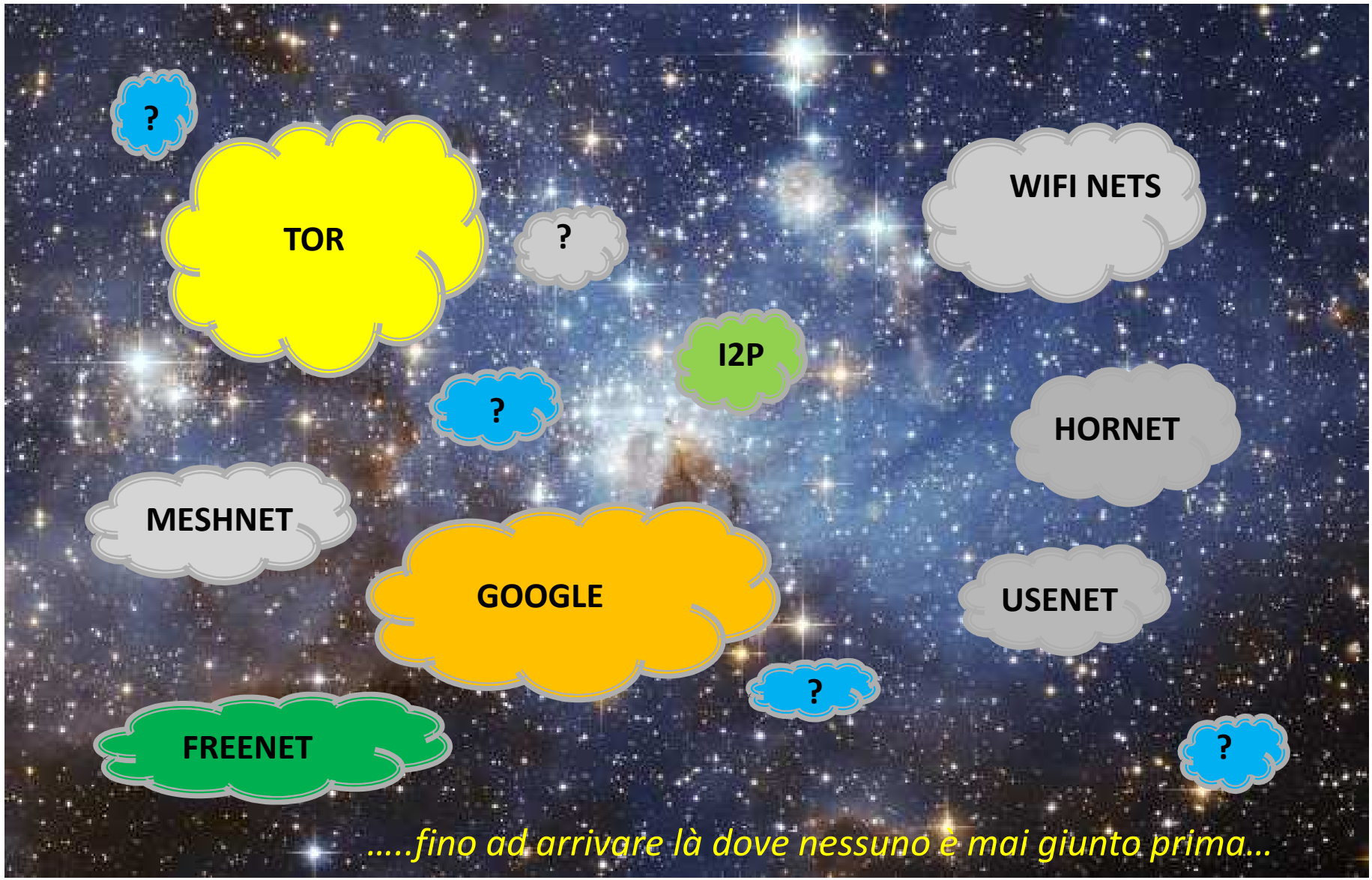
WEB & DEEP WEB

Il Deep Web (Web sommerso o invisibile) è l'insieme delle risorse informative del World Wide Web non raggiunte dai comuni motori di ricerca. I documenti che costituiscono il Deep Web si possono suddividere in:

- *pagine web dinamiche;*
- *pagine web non collegate a nessun'altra;*
- *pagine ad accesso ristretto*;
- *script*: *pagine raggiungibili solo attraverso link;*
- *contenuti non di testo*.

La struttura dell'intero World Wide Web viene spesso paragonata a quella di un iceberg, di cui solo una minima parte sarebbe visibile sopra il pelo dell'acqua.

IL WEB NON HA DIMENSIONI NE' LIVELLI

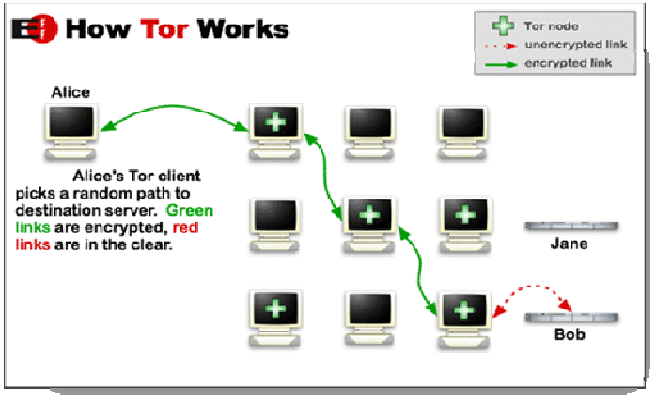


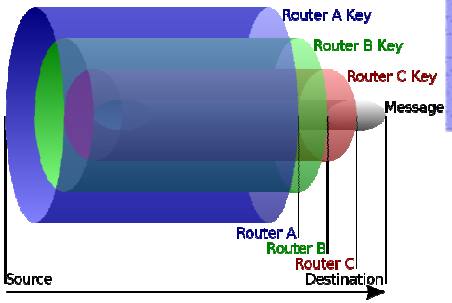
LE DARKNET

Reti virtuali costituite da un gruppo chiuso di utenti per le loro comunicazioni private.

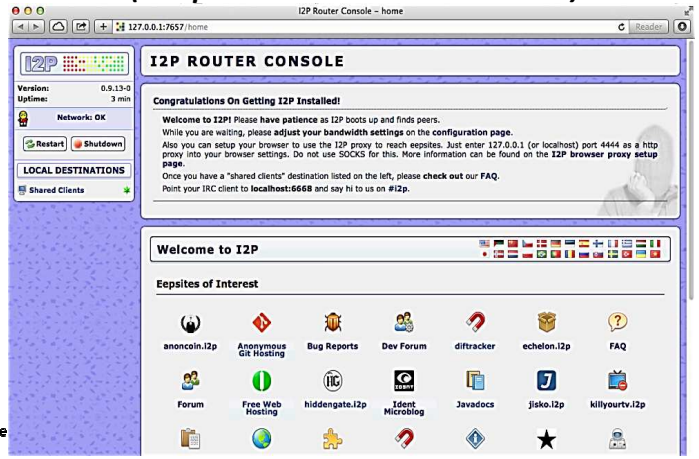
LE PIU CONOSCIUTE (e utilizzate) SONO:

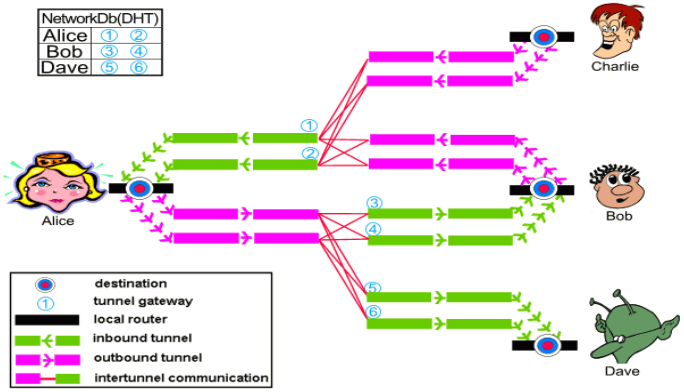
TOR *(The Onion Router)*





I2P *(Impossible To Possible)*





TOR – I2P – USENET – FREENET – HORNET

sono disponibili per PC, MAC, telefoni IOS e Android.

GLI STRUMENTI

NAVIGAZIONE

VPN – virtual provate network **+** **TOR**-the onion router / **I2P**–impossible to possible

ANALISI ONLINE

Google international – *google.com*
GeoSetter – geolocalizzatore di immagini
FacebookForensics – analizzatore dei profili di Facebook
TwitterForensics – analizzatore dei profili Twitter
WayBackMachine – archivio web online: *https://archive.org/web/*
WHOIS – registro dei siti web
HTTRACK – downloader siti web

ANALISI DEI DATI

Analyst/Maltego/Cogito/Palantir/

SENZA DIMENTICARE:

l'analisi del contenuto di memoria di eventuali telefoni cellulari e altri dispositivi digitali

Strumento di analisi: WHOIS

https://www.whois.com/whois/

Riporta tutte le informazioni su un sito web:

- amministratore,
- data creazione
- ultimo aggiornamento
- Indirizzo provider
- ecc.

…. MA NON SEMPRE!

DOMAIN INFORMATION

Domain:	dreammarketdrugs.com
Registrar:	ENOM, INC.
Registration Date:	2015-10-15
Expiration Date:	2017-10-15
Updated Date:	2017-03-08
Status:	clientTransferProhibited
Name Servers:	ada.ns.cloudflare.com eric.ns.cloudflare.com

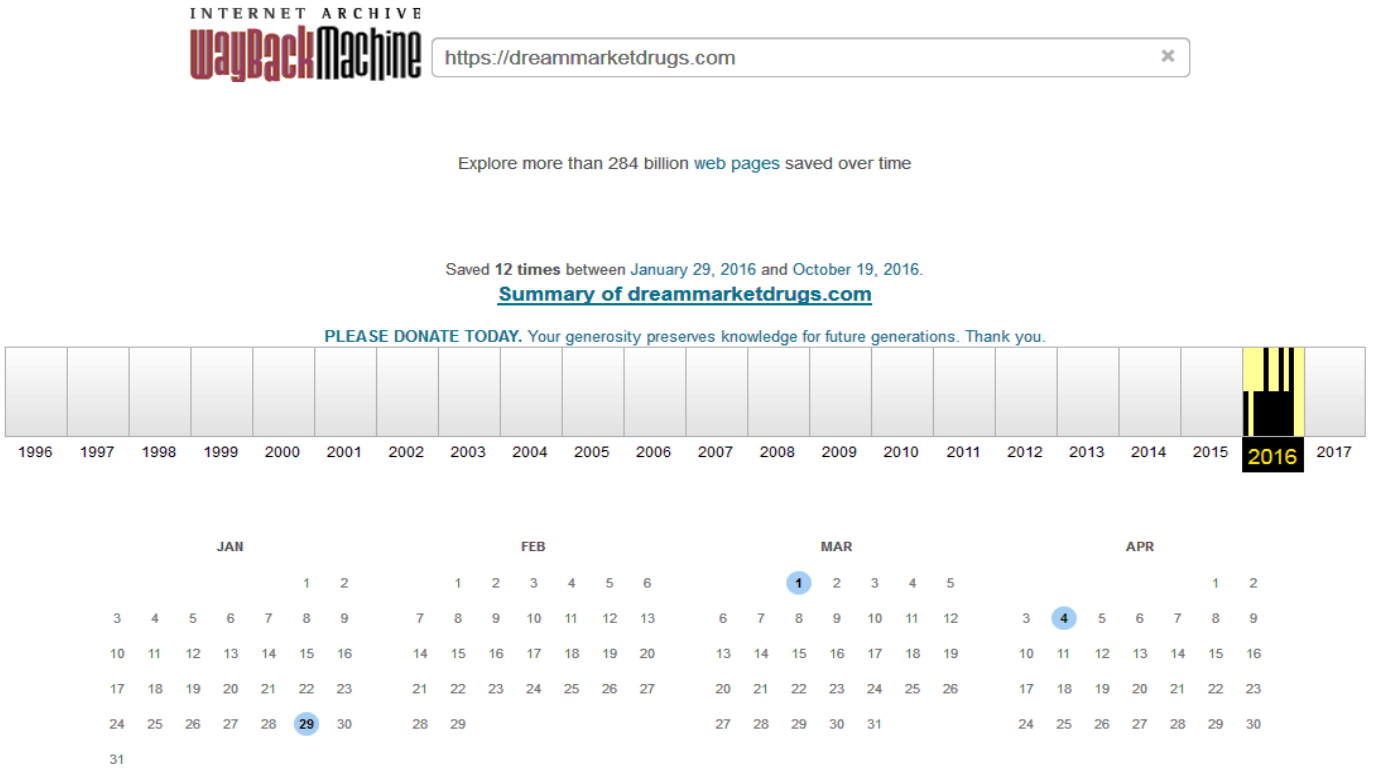
REGISTRANT CONTACT

Name:	WHOISGUARD PROTECTED
Organization:	WHOISGUARD, INC.
Street:	P.O. BOX 0823-03411
City:	PANAMA
State:	PANAMA
Postal Code:	00000
Country:	PA
Phone:	+507.8365503
Fax:	+51.17057182
Email:	B25E97B9BBEA4824A2313F79F76CBD52.PROTECT@WHOISGUARD.COM

Strumento di analisi: WAYBACKMACHINE

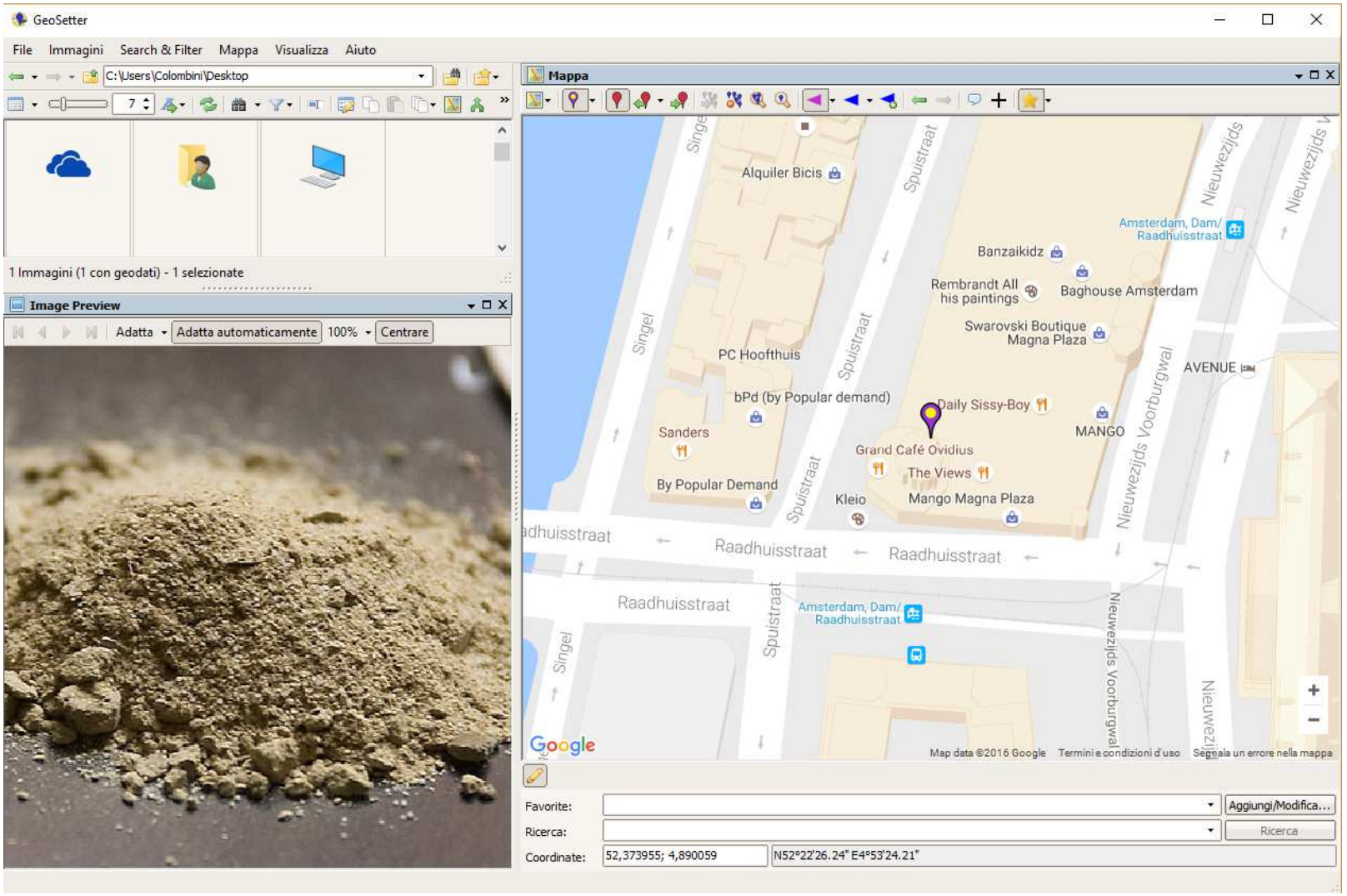
https://archive.org/web/

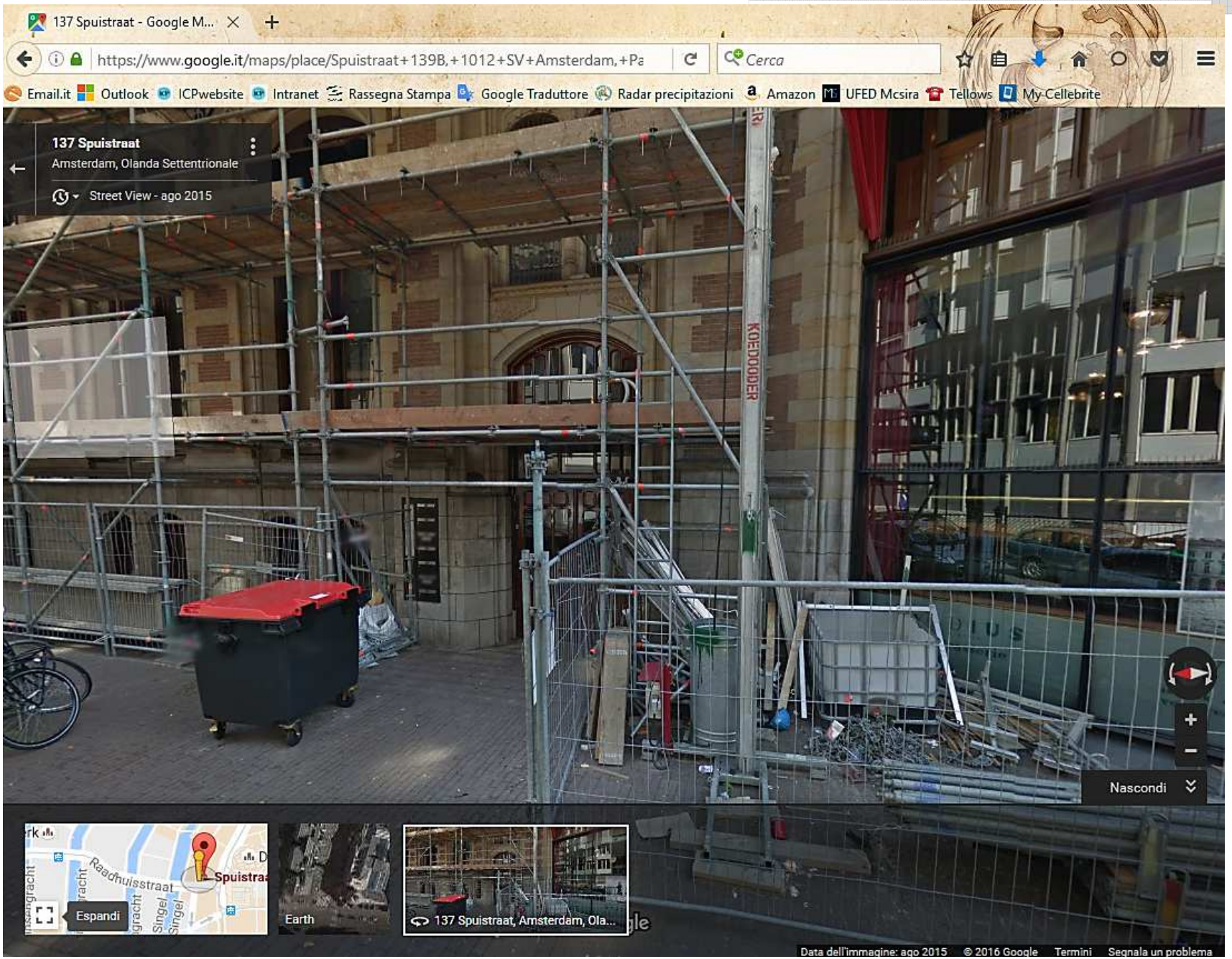
Racconta la «storia» di un sito web raccogliendo screenshot della sua homepage in diversi intervalli nel tempo



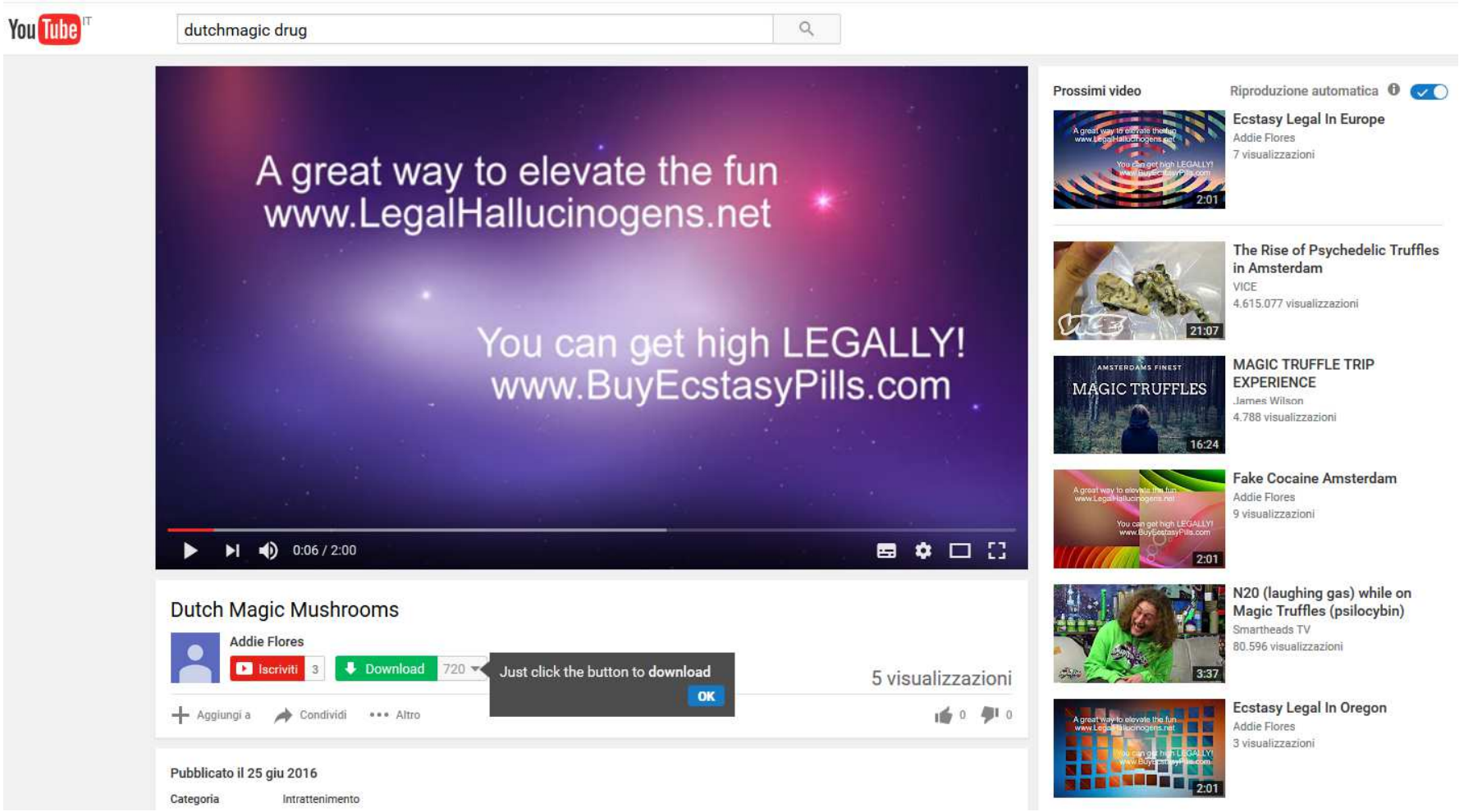
Geosetter

www.geosetter.de




137 Spuistraat - Google M...
https://www.google.it/maps/place/Spuistraat+139B,+1012+SV+Amsterdam,+Pa
Cerca
Email.it
Outlook
ICPwebsite
Intranet
Rassegna Stampa
Google Traduttore
Radar precipitazioni
Amazon
UFED Mcsira
Tellows
My-Cellebrite
137 Spuistraat
Amsterdam, Olanda Settentrionale
Street View - ago 2015
KOEDOODER
Nascondi
Espandi
Raadhuisstraat
Earth
137 Spuistraat, Amsterdam, Ola...
Data dell'immagine: ago 2015
© 2016 Google
Termini
Segnala un problema

Non dimenticate YOUTUBE !!!

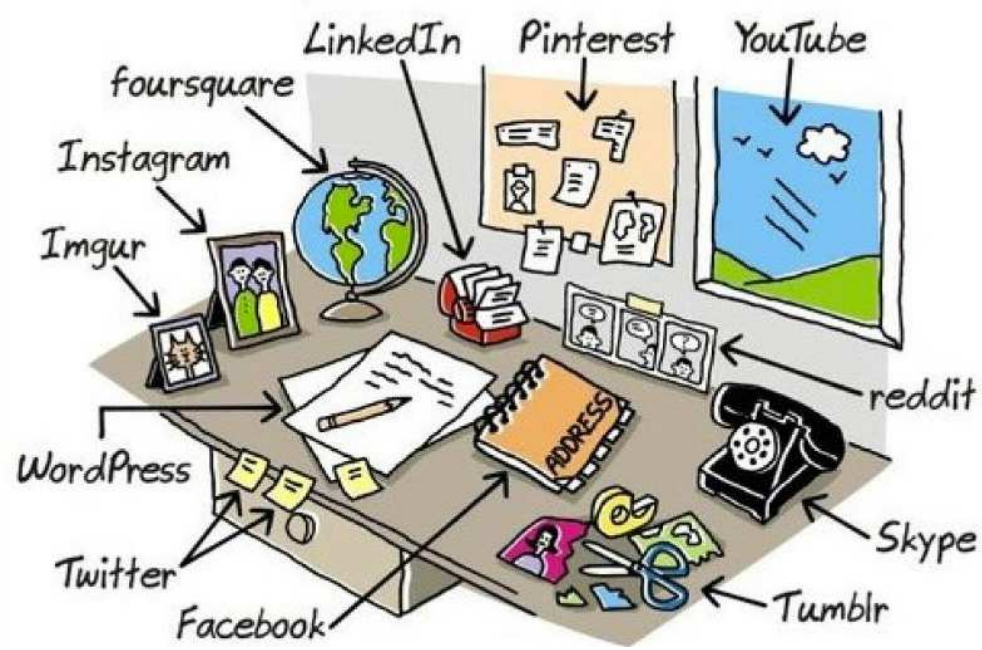


IL PROBLEMA DELLA RICERCA NEL WEB

il problema non consiste nel trovare l'informazione,
ma nel riuscire a trovare quella giusta, in un oceano
di informazioni senza controllo in continuo mutamento.

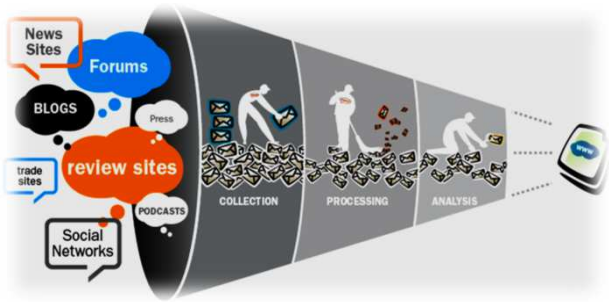
L'OSINT (Open Source Intelligence) ci viene in soccorso applicando al WEB il suo metodo di gestione dei suoi due soggetti primari:

La fonte
L'informazione



CICLO DI INTELLIGENCE INVESTIGATIVO APPLICATO AL WEB

- ***Planning:*** pianificazione dell'obiettivo;
- ***Collection***: ricerca di specifiche pagine web e raccolta di dati coerenti;
- ***Processing***: selezione e valutazione dei dati rilevanti (indicatori);
- ***Production***: estrapolazione ed interpretazione delle informazioni in relazione all'obiettivo prefissato.



La procedura si svolge per raffinamenti successivi, ripetendo il ciclo ogni qualvolta si presentano nuovi dati o nuove informazioni.

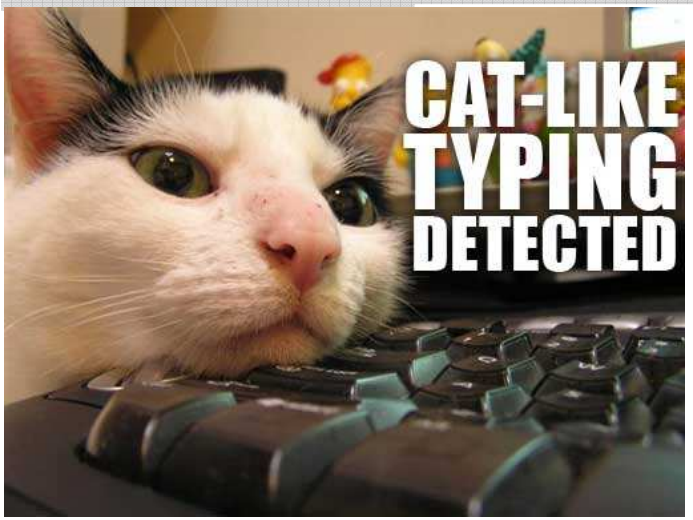
VALUTAZIONE DELLE FONTI

Particolare attenzione va posta nella valutazione dell'attendibilità delle fonti online, (forum, wiki, blog, social, ecc.), fase più delicata che è stata basata sui seguenti requisiti:

- **accuratezza** delle informazioni;
- capacità di mantenere le **informazioni aggiornate**;
- **attendibilità e autorità** del sito stesso;
- **rilevanza** delle informazioni contenute.

Su questo modello si selezionano, tramite il confronto delle informazioni offerte, una serie di siti considerati «attendibili» a cui fare riferimento, ma senza mai dimenticare che nel Web nascono continuamente nuove fonti.

WEB PROFILING



PROFILAZIONE DEI DATI

- modellazione e classificazione
- Associazione/deviazione/ricorrenze
- analisi dei path
- modellazione sequenziale
- comparazione di stringhe

ESTRAZIONE DI INFORMAZIONI CARATTERIZZANTI DA CHAT, FORUM, BLOG, COME:

- nickname, espressioni idiomatiche,
  errori di ortografia e battitura;
- analisi della timeline delle conversazioni;
- estrapolazione delle interconnessioni fra utenti diversi;
- analisi della frequenza delle conversazioni;
- Analisi della geolocalizzazione delle foto;
- altre informazioni caratterizzanti estrapolabili dai testi, come riferimenti a cose, persone, luoghi ecc.

ANALISI DELLA STRUTTURAZIONE DEL CODICE
(analisi dei listati) e delle funzioni implementate per la rilevazione di commenti, firme ecc. caratterizzanti il programmatore.

ANALISI BLACK MARKET

- LOGIN AL SITO
- 1° RICOGNIZIONE VISIVA
- CREAZIONE DI UNA CARTELLA CON LA MEDESIMA STRUTTURA DEL SITO:
  - Homepage
  - Forum
  - Venditori
  - Supporto
  - Ordini
  - Prodotti
  - Servizi
  - Organizzazione di vendita
  - Modalità di spedizione
  - Links esterni
  - Ecc…
- SALVATAGGIO DI TUTTE LE PAGINE DI INTERESSE NELLE RISPETTIVE SOTTO-CARTELLE PER LA SUCCESSIVA ANALISI OFF-LINE.

CHI-DOVE-COME-QUANDO-PERCHE’

RISULTATO:

- la tipologia di utente a cui vuole rivolgersi (**CHI**)
- la struttura e le funzionalità offerte (blog, chat, forum, archivi documentali, transazioni ecc.) (**COME**)
- la struttura dei link interni e soprattutto esterni (**DOVE**)
- la timeline della vita del sito e la sua evoluzione (**QUANDO**)
- gli scopi che si prefigge (**PERCHE’)**

L'INDAGINE SOTTO COPERTURA

parola d'ordine: non improvvisare

Il Web sembra anonimo ma non lo è: senza le opportune precauzioni ogni connessione è tracciabile e identificabile

Sono possibili:
attacchi informatici
invio di malware
tentativi di intrusione
allo scopo
di rivelare
la nostra identità

…..e perché no, sottrarre qualche dato da vendere….

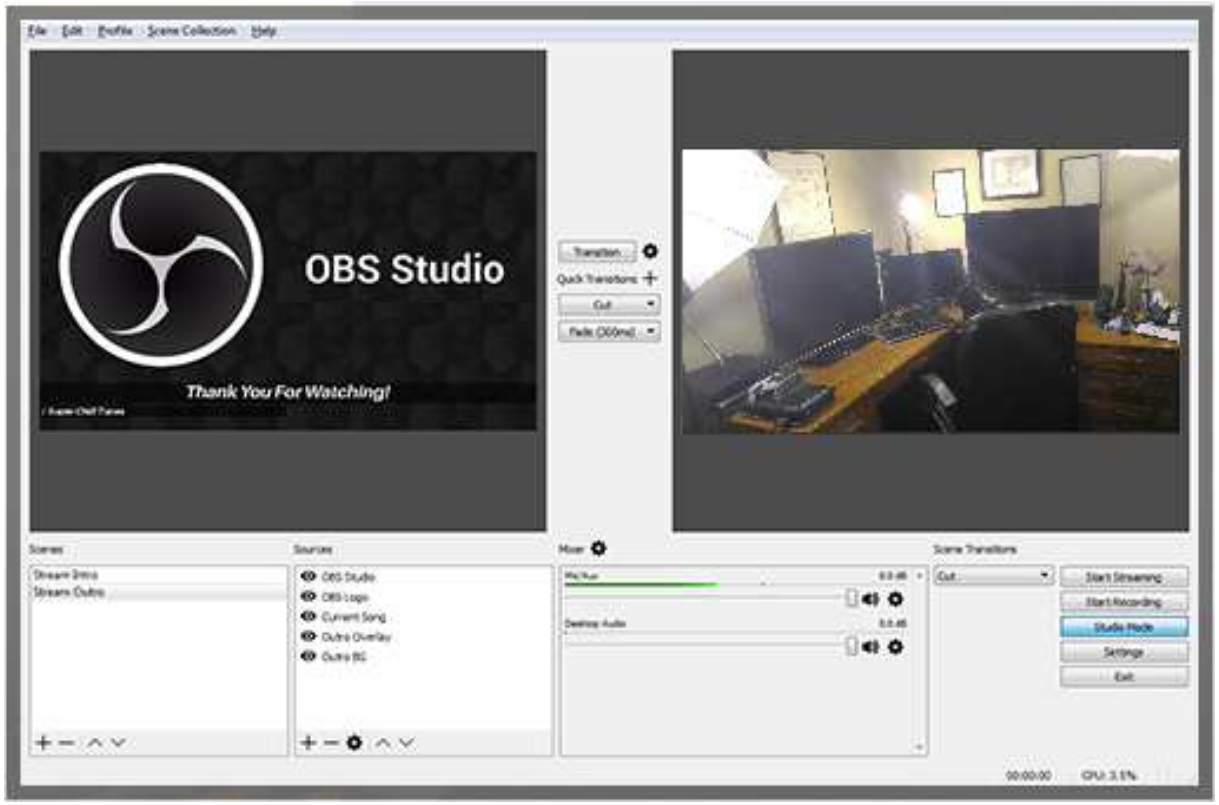
PRECAUZIONI PER MANTENERE L'ANONIMATO

- **Non** utilizzare il proprio PC o quello collegato alla rete interna dell'ufficio.
- **Non** utilizzare connessioni WIFI condivise o pubbliche.
- **Non** utilizzare WIFI pubbliche.
- **Scollegare** la webcam e il microfono.
- **Utilizzare** un programma di wiping sulla macchina utilizzata per «ripulirla» periodicamente da eventuali malware.
- **Avviare sempre una VPN** (Virtual Private Network) per nascondere il proprio IP.
- **Utilizzare sempre TOR** per la navigazione e mantenerlo aggiornato.
- **Utilizzare un account email ANONIMO** .onion
- **Utilizzare una chiave PGP** con l'email .onion
- **Costruire una o più false identità** sui Social Network e/o Forum che si vogliono indagare (consigliato Facebook)

Prima di prendere contatto e' indispensabile imparare la «*lingua scritta*» del web studiando le conversazioni nei forum dei black market per imparare il linguaggio e l'approccio della comunità in cui ci si intende infiltrare

LA CONOSCENZA DELLA LINGUA INGLESE E' INDISPENSABILE

REGISTRAZIONE SCHERMO PC

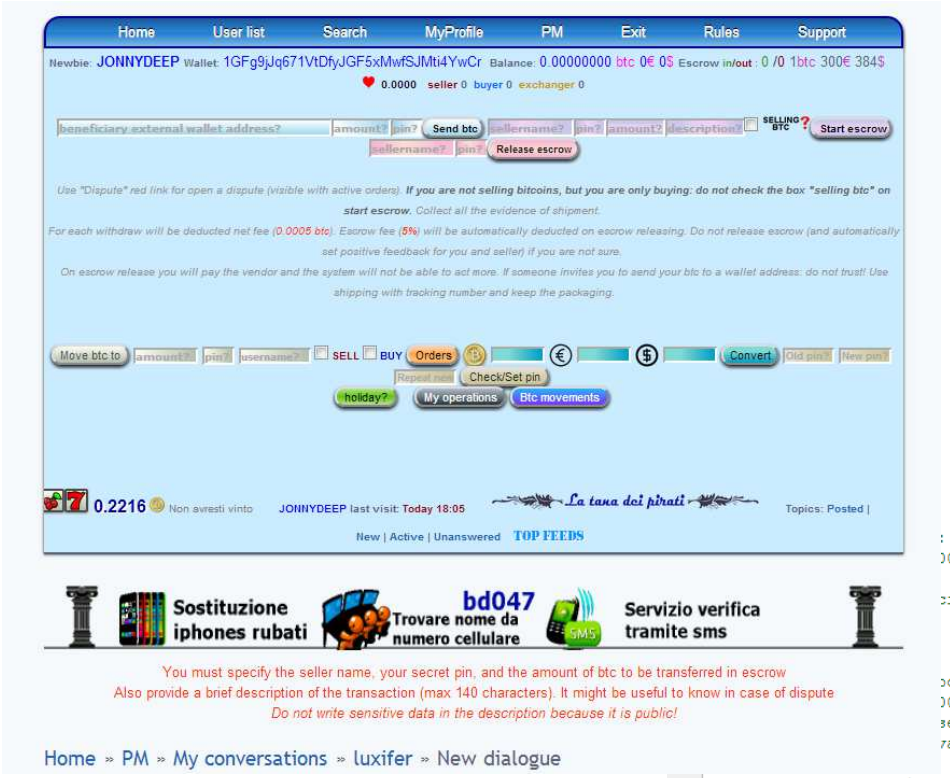


OBS Studio è un software gratuito che permette di registrare qualsiasi azione compiuta sul PC.

Molto utile per produrre fonti di prova per il Tribunale.

LE INDAGINI:

Qualche risultato..



L'importanza dell'analisi del codice HTML

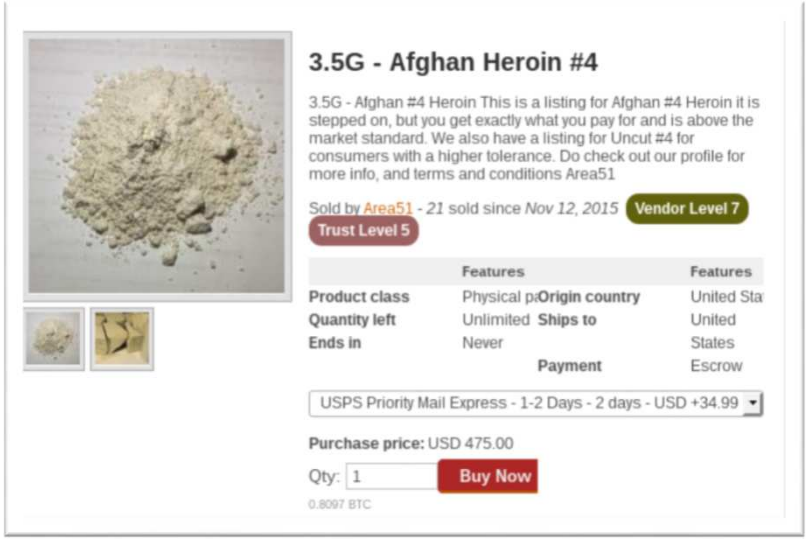
```
: block;margin: -2px 0;">
)000><i>Assicuratevi di ricordare il pin e di aver cambiato quello di default prima di

:ile aiutarvi. Ricordate che i logins non cambiati dal 29 Gennaio sono insicuri</i>


ock;margin: -2px 0;">
)000><i><strong>Gli utenti sono invitati al prelievo dei loro fondi. Non fate ordini ne
ser.
vate presto per permettere il reset dei wallet<br style="display: block;margin: -2px
```

```
122 Dopo tutto ritornerà alla norma. Prima di prelevare assicuratevi che l' url sia
123 </i><font size=2
    color=#000999>&#98;&#97;&#98;&#121;&#108;&#111;&#110;&#120;&#106;&#114;&#116;&#100;&#121;&#111;&#109;&#121;&#
    46;&#111;&#110;&#105;&#111;&#110;
124 </strong></font></font>
125 -->
126
127 <!--
128 <br style="display: block;margin: -2px 0;">
129 <font size=2 color=#ff0000><i><strong>Siete invitati a reimpostare le immagini ed i prezzi nei vostri topics.
    E non lasciate topics obsoleti.
130 Avete a disposizione 6 prodotti/pezzature per topic
131 <br style="display: block;margin: -2px 0;">
132 Chi non provvede entro le ore 24 del 13 ottobre o comunque al primo accesso non ottempera...verrà bandito dal
    forum per 2 settimane
133 </i></strong></font>
134 -->
135
136 <!--
137 <br style="display: block;margin: -2px 0;">
138 4023610901407776 03/19 salvatore uccellatore, fiscale CCLSVT70H08C351V <--- SCAM
139 -->
140
141 <!--</i></strong></font>-->
142
```

BABYLON

2016

I venditori di ALPHABAY ***AREA51*** e ***DARKAPOLLO*** sono stati identificati da un agente DEA sotto copertura
L'errore di **AREA51** e **DARKAPOLLO** è stato quella di inserire nella loro chiave pubblica l'email ***Adashc31@gmail.com***, che ha fatto risalire ai loro profili Facebook, Twitter ed Instagram tramite il nick "***Adashc31***".
La ricerca ha portato ad un unico individuo di nome ***Ahmed Farook***, residente a Brooklyn, New York.



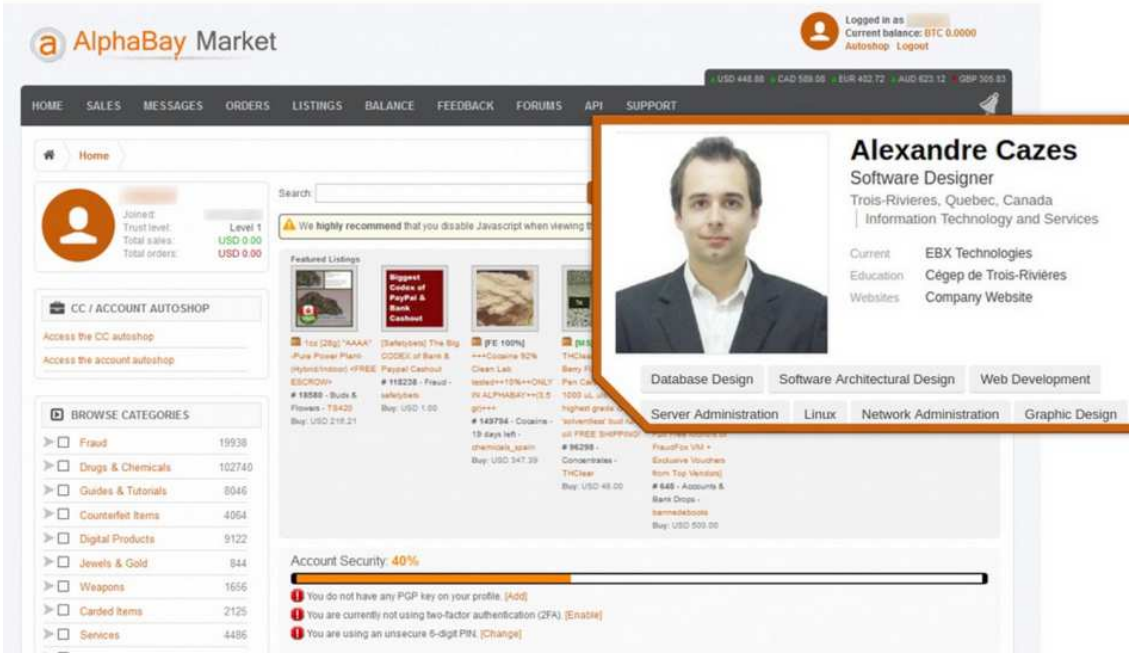
OPERAZIONE ALPHABAY

LUGLIO 2017 - FBI, Dea e polizia olandese, col sostegno di Europol, hanno smantellato, in due operazioni, AlphaBay e Hansa, vere e proprie dorsali dell'economia criminale sommersa sul Deep Web, per il commercio online di oltre 350mila prodotti illeciti.

Viene arrestato l'amministratore del sito, Alexandre Cazes "Alpha02".
Una settimana dopo sembra si sia tolto la vita all'interno di un carcere Tailandese.

Gli investigatori hanno avuto accesso alle chiavi private / **Wallet**, dei quali hanno ottenuto la password per decifrare le chiavi private e poter firmare le transazioni verso gli indirizzi istituzionali di Bitcoin, Ethereum, Zcash e Monero per diversi milioni di Euro.

Sembra che i wallet non fossero criptati.



I Black Market come banche

spariti 12 milioni di Bitcoin

"Potete vedere Alphabay come una banca: mentre permettiamo alle persone di depositare e ritirare a piacimento, i farmaci sono solo un prodotto per attirare il cliente. I soldi depositati nei portafogli non restano lì freddi: investiamo in svariate cose in forma anonima, guadagniamo con quegli investimenti, assicurandoci sempre il 100 per cento della riserva".

È facile a questo punto vedere delle analogie sulla nascita e morte di numerosi market, dietro ai quali vi sarebbe la volontà di **intascare moneta elettronica prima che le forze dell'ordine facciano il loro lavoro**.

Grazie per l'attezione