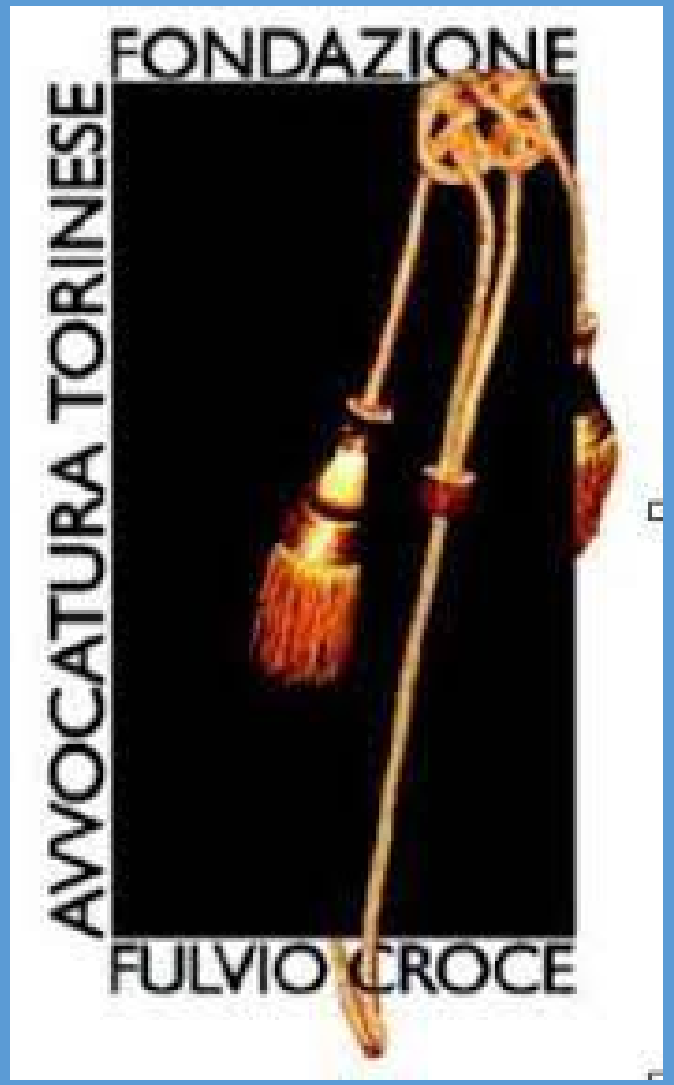
25 OTTOBRE 2023

PHISHING E NUOVI ATTACCHI INFORMATICI

Tecniche e strumenti a disposizione dell'investigatore per l'accertamento del reato



TECNICHE DI ATTACCO

PHISHING & MALWARE

- Il Phishing è una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi-spam di posta elettronica o SMS ingannevoli, apparentemente provenienti da pubbliche amministrazioni, aziende erogatrici di servizi pubblici, istituti finanziari, altre imprese commerciali o persone conosciute.

- Il messaggio normalmente invita ad aprire un link o un allegato malev

- Il pretesto utilizzato dai truffatori per indurre l'utente a cliccare sul link o s
mira ad essere sempre più «credibile»: spesso si utilizza una fattura o un rimb

SITI CLONE

Vengono predisposte pagine web del tutto identiche al sito orginale in modo tale che il truffatore inganni la vittima e lo induca ad inserire I propri codici o credenziali personali per poi appropriarnese.

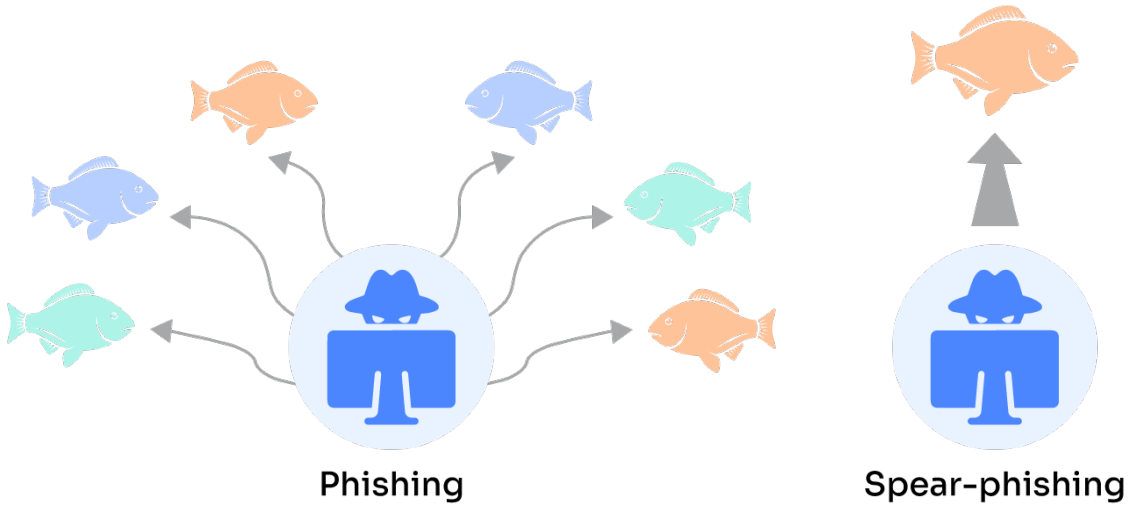
Digitate le credenziali il Sistema le invia a caselle di posta “anonime” o in uno spazio web. La persona non si accorge di nulla perchè spesso viene restituto un generico messaggio di errore o addirittura si viene reindirizzati sul sito orinignale quindi l’utente riprova l’accesso e tutto risulta funzionante.

SPEAR PHISHING

Forma evoluta di Phishing che si concentra sulle abitudini della vittima.

Il truffatore tenta di carpire le abitudini e gli interessi della vittima per cercare di costruire una email o un messaggio da inviargli e che lo induca a fare quello che viene richiesto.

Questa è una tecnica che viene utilizzata anche da chi si occupa di intercettazioni telematiche come attività propedeutica all'installazione del "trojan di stato"



RANSOMWARE

Si tratta di un malware (cryptovirus) che infetta il computer e cifra tutti I file in esso contenuti espandendosi anche su tutte le periferiche esterne collegate sia su porta usb che di rete.

Per ottenere lo “sblocco” dei file, alla vittima vengono lasciate alcune ore per provvedere al pagameto di un riscatto.

Nella maggior parte dei casi vengono fornite istruzioni per acquistare cryptomonete con cui procedere al pagamento dopo il quale viene fornita la chiave di decifratura che pemette di rendere I file nuovamente leggibili.

SMISHING

Trattasi di una variante del phishing realizzata attraverso l'impiego di sms

L'utente generico normalmente pone più attenzione al contenuto di un sms rispetto a quello di un messaggio email.

Per semplice automatismo o distrazione è più facile cliccare il link indicato nel messaggio.

I messaggi-frode spesso vengono messi in coda a messaggi provenienti da oggetti verificati in quanto l'intestazione del messaggio è uguale a quella del mittente conosciuto e lo smartphone lo riconosce e lo pone in coda ai messaggi reali

VISHING

Ulteriore nuova variante realizzata attraverso delle tradizionali chiamate telefoniche

Si viene contattati da soggetti che dicono di operare per conto di gestori telefonici, altri servizi pubblici, banche (in questo caso il chiamante risulta essere il numero del proprio istituto bancario che lo smartphone riconosce e lo mostra a schermo)

L'obiettivo è quello di farsi consegnare i propri dati di accesso e le informazioni personali come i propri dati bancari e costringerti ad eseguire operazioni di trasferimento denaro

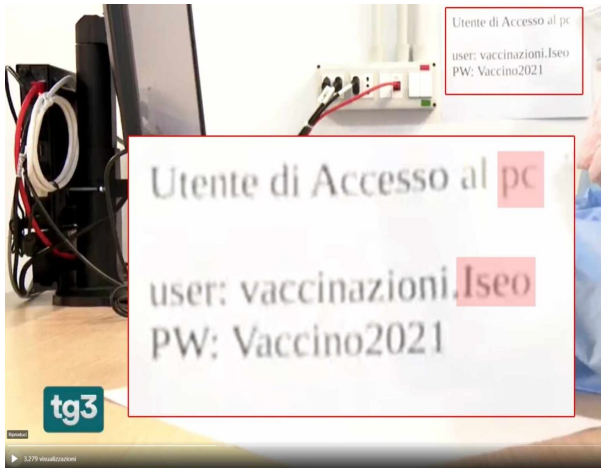
TRUFFA DEL TRADING ONLINE

Tale forma di truffa viene realizzata tramite dapprima un contatto telefonico diretto alla potenziale vittima; il contatto può essere anche sollecitato dalla persona offesa attraverso *banner* presenti sui *social network* più diffusi.

Nella chiamata un presunto *broker* illustra un piano di investimenti sicuro e remunerativo cui aderire tramite delle piattaforme *online* tra cui si segnalano: 'Cyticapital', 'HexoBank', Tradebnp; si precisa peraltro che in diversi casi i broker richiedono all'investitore di attivare sul proprio pc il *software 'anydesk'* per fornire assistenza remota nelle operazioni.

https://open.spotify.com/episode/4WDT0hHhp20Z0S9uINy5Z9?si=FJyYoOSRSyutoUBc2Acp_Q&context=spotify%3Ashow%3A0WHJaWlhK9SlFfZxUkuzjI

C’è bisogno di maggiore **educazione digitale**, gli strumenti digitali sono ormai parte integrante della nostra vita. I servizi indispensabili ormai sono tutti sotto forma digitale ma la stragrande maggioranza delle persone non ha ancora percepito la necessità mettere in atto una maggiore attenzione alla sicurezza digitale.



L’u no è sempre l’anello debole del sistema

- Tutti noi, come utenti digitali, possiamo essere vittime di attacchi di social engineering:
  - l’arte e la scienza del far fare alle persone quel che si desidera
- Affidiamo ai social network e ai vari siti, la maggior parte delle nostre informazioni riservate (foto, chat, documenti)
- Queste informazioni hanno un enorme valore, tutti noi siamo potenzial ne in rete
- Riconoscere i rischi e sapersi difendere è un obbligo

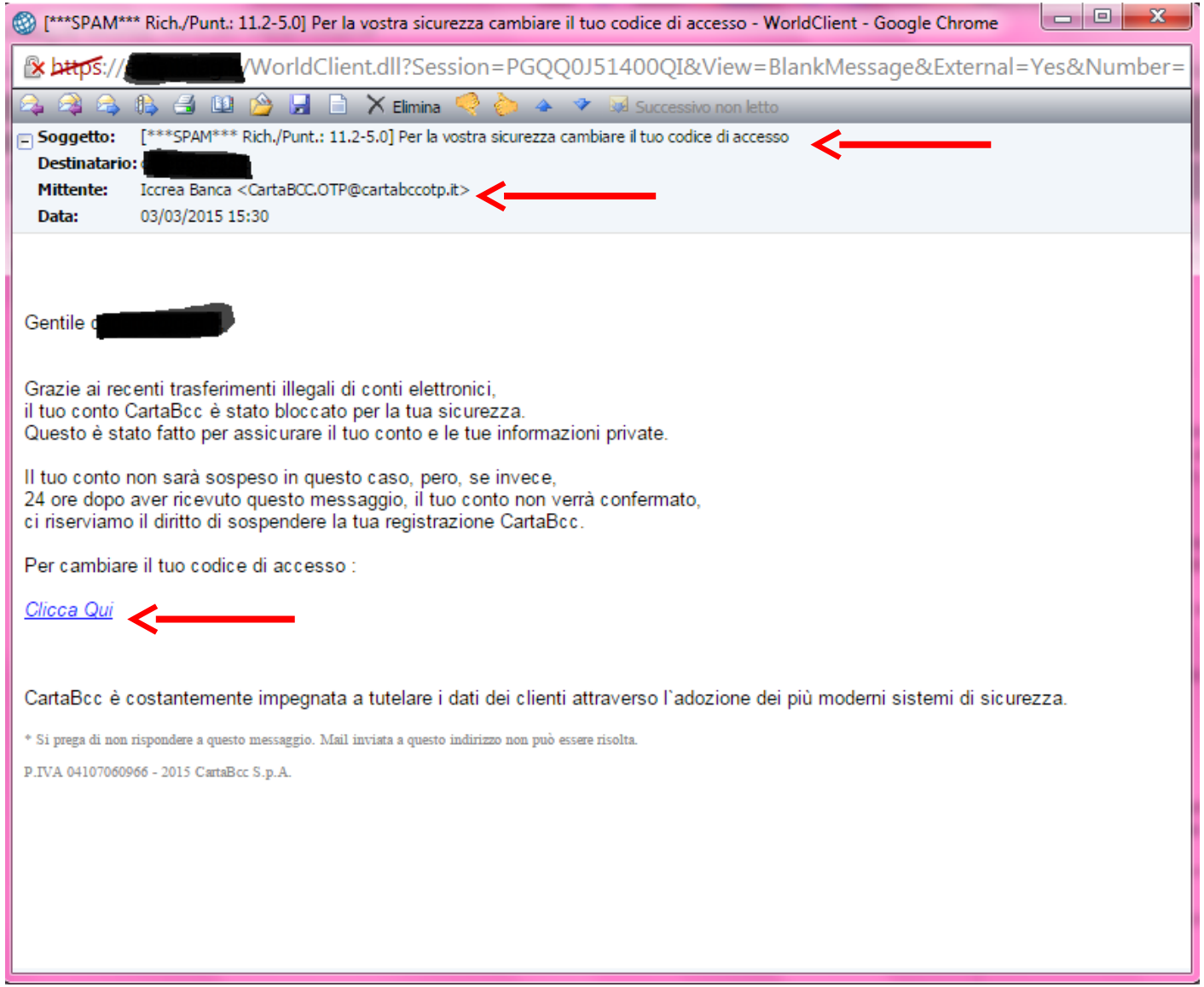
PASSWORD – CHE SCOCCIATURA

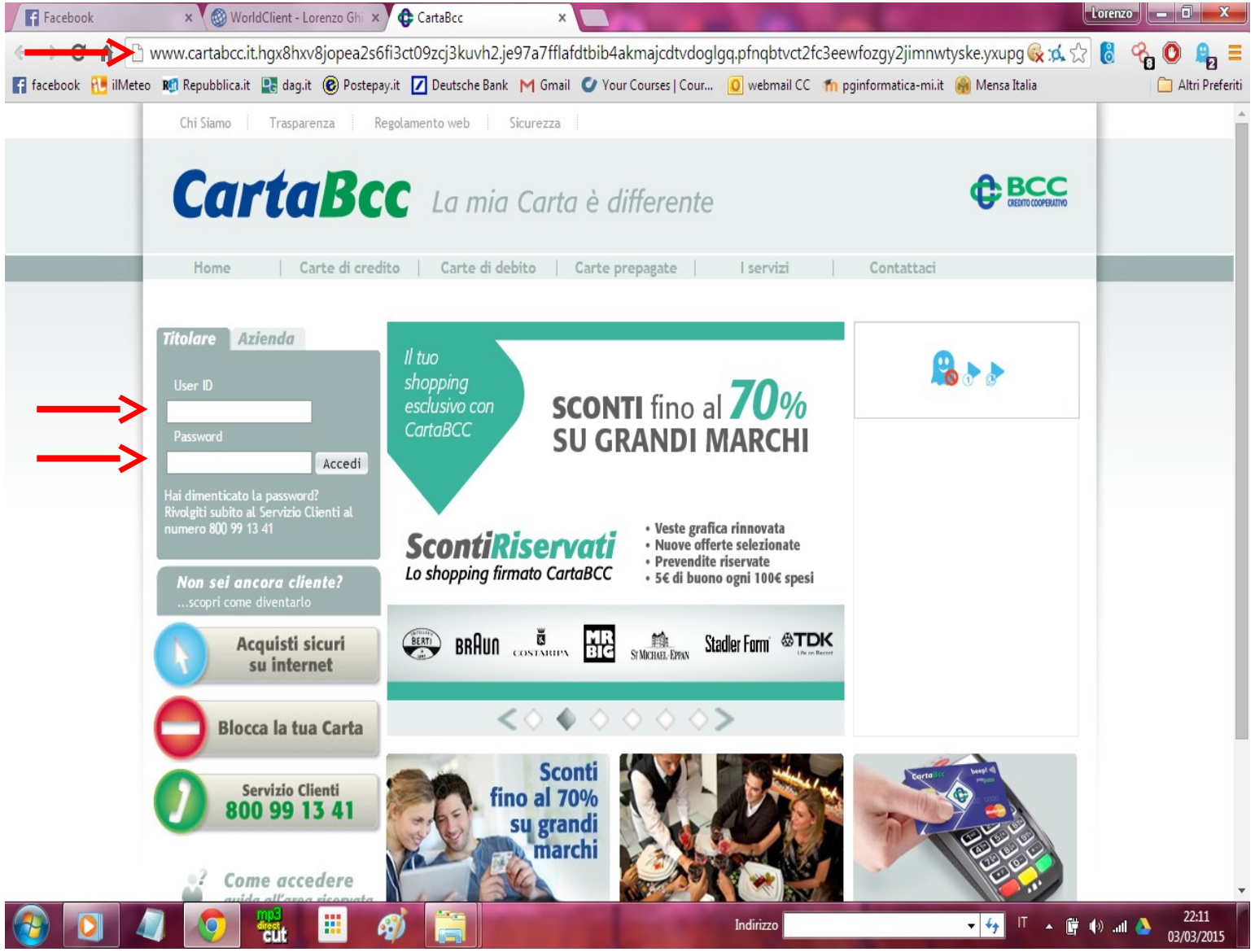
- **Le password sono come le mutande:**
  - Non condividerle
  - Non farle vedere agli altri
  - Ricordati di cambiarle regolarmente

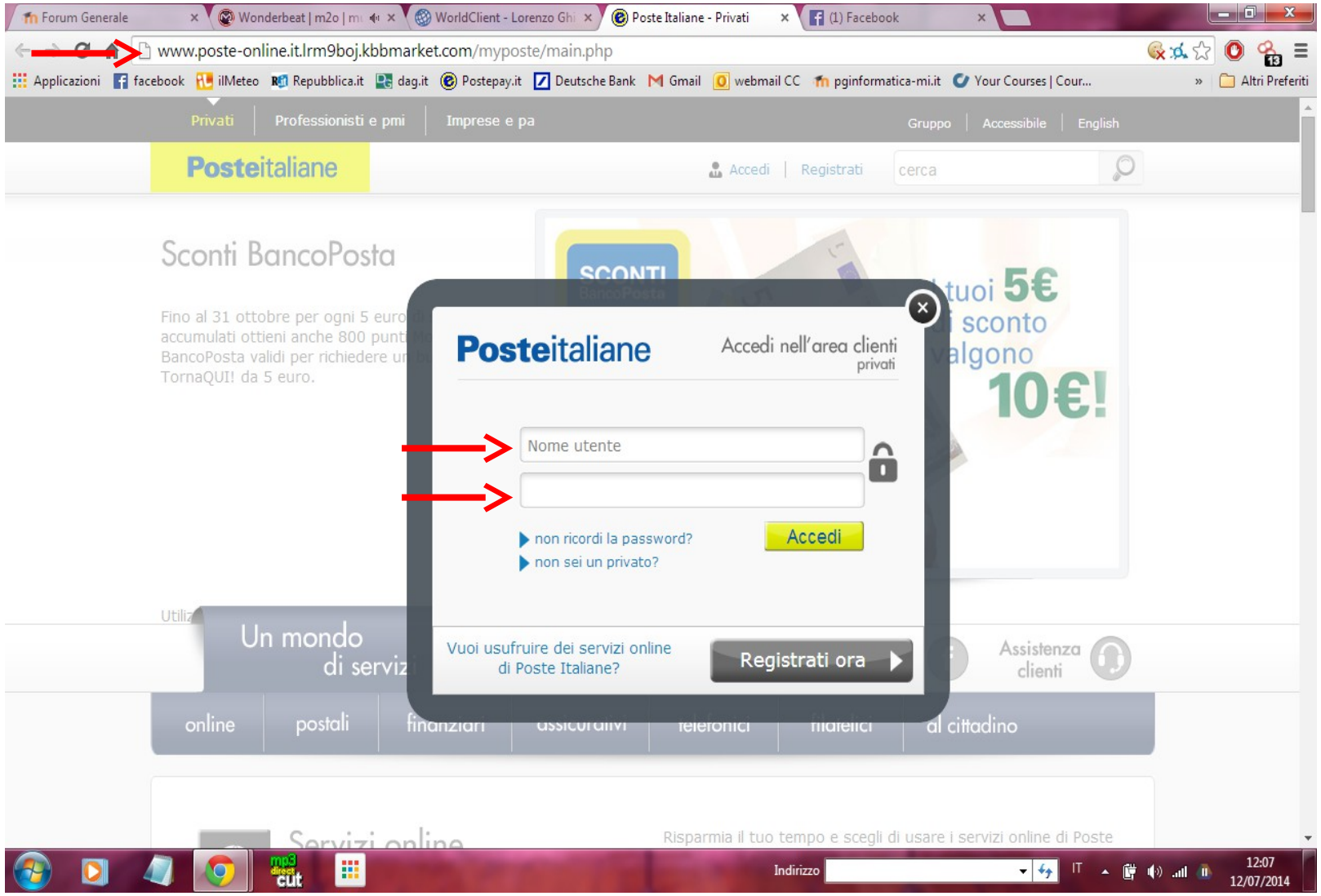
- **Molto importante:**
  - Non usare le stesse su più siti
  - Non scegliere riferimenti personali
  - Non semplici parole comuni

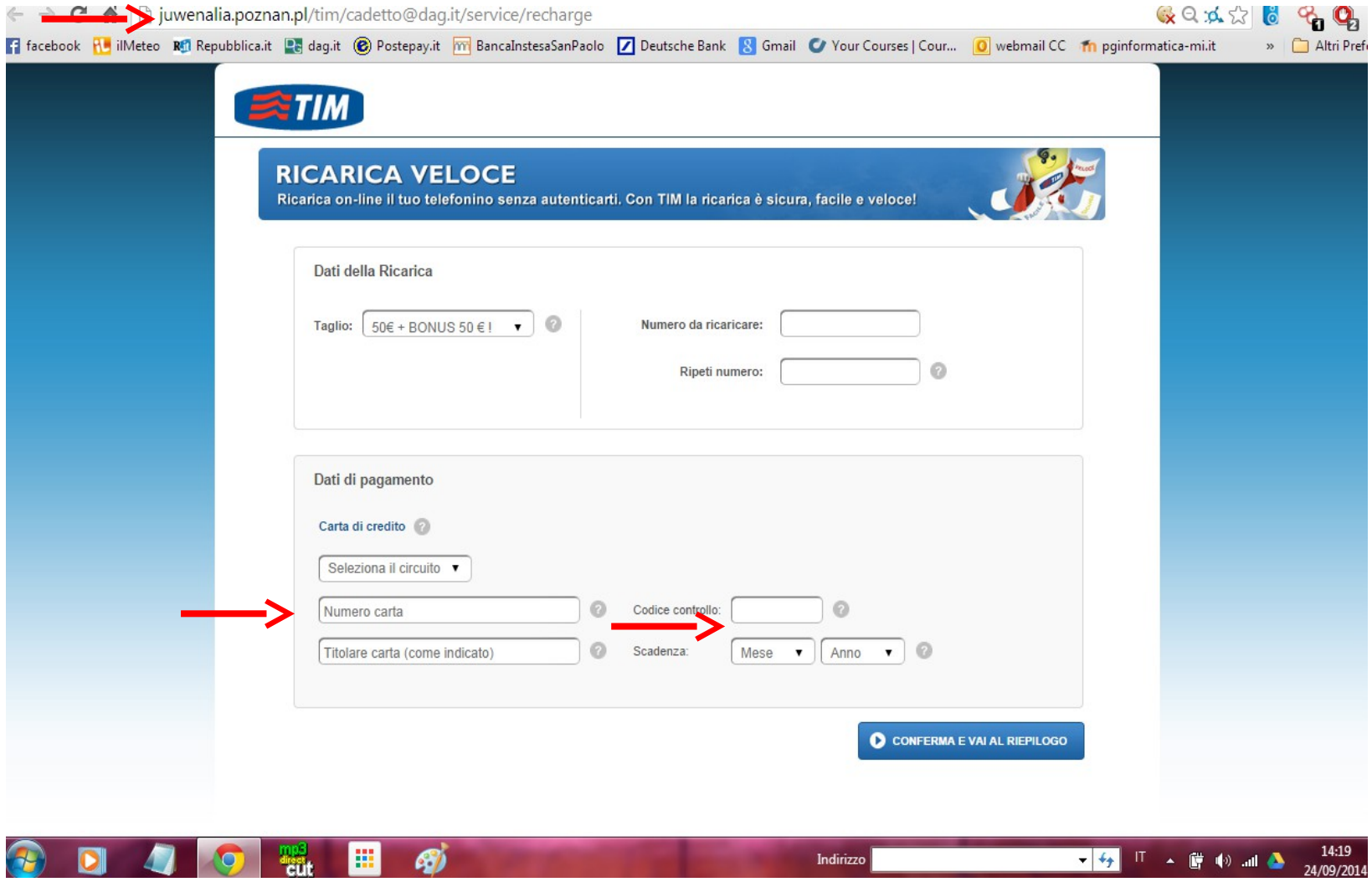
il truffato è **emotivo/irrazionale**

il truffatore è **cognitivo/razionale**


[***SPAM*** Rich./Punt.: 11.2-5.0] Per la vostra sicurezza cambiare il tuo codice di accesso - WorldClient - Google Chrome
https://[redacted]/WorldClient.dll?Session=PGQQ0J51400QI&View=BlankMessage&External=Yes&Number=
Elimina
Successivo non letto
Soggetto: [***SPAM*** Rich./Punt.: 11.2-5.0] Per la vostra sicurezza cambiare il tuo codice di accesso
Destinatario: [redacted]
Mittente: Iccrea Banca <CartaBCC.OTP@cartabccotp.it>
Data: 03/03/2015 15:30
Gentile [redacted]
Grazie ai recenti trasferimenti illegali di conti elettronici,
il tuo conto CartaBcc è stato bloccato per la tua sicurezza.
Questo è stato fatto per assicurare il tuo conto e le tue informazioni private.
Il tuo conto non sarà sospeso in questo caso, pero, se invece,
24 ore dopo aver ricevuto questo messaggio, il tuo conto non verrà confermato,
ci riserviamo il diritto di sospendere la tua registrazione CartaBcc.
Per cambiare il tuo codice di accesso :
Clicca Qui
CartaBcc è costantemente impegnata a tutelare i dati dei clienti attraverso l'adozione dei più moderni sistemi di sicurezza.
* Si prega di non rispondere a questo messaggio. Mail inviata a questo indirizzo non può essere risolta.
P.IVA 04107060966 - 2015 CartaBcc S.p.A.


Facebook
WorldClient - Lorenzo Gh
CartaBcc
Lorenzo
www.cartabcc.it.hgx8hxv8jopea2s6fi3ct09zcj3kuvh2.je97a7fflafdtbib4akmajcdtvdoglgq.pfnqbtvct2fc3eewfozgy2jimnwtyske.yxupg
facebook
ilMeteo
Repubblica.it
dag.it
Postepay.it
Deutsche Bank
Gmail
Your Courses | Cour...
webmail CC
pginformatica-mi.it
Mensa Italia
Altri Preferiti
Chi Siamo
Trasparenza
Regolamento web
Sicurezza
CartaBcc
La mia Carta è differente
BCC
CREDITO COOPERATIVO
Home
Carte di credito
Carte di debito
Carte prepagate
I servizi
Contattaci
Titolare
Azienda
User ID
Password
Accedi
Hai dimenticato la password?
Rivolgiti subito al Servizio Clienti al numero 800 99 13 41
Non sei ancora cliente?
...scopri come diventarlo
Acquisti sicuri su internet
Blocca la tua Carta
Servizio Clienti
800 99 13 41
Come accedere
Il tuo shopping esclusivo con CartaBCC
SCONTI fino al 70%
SU GRANDI MARCHI
ScontiRiservati
Lo shopping firmato CartaBCC
• Veste grafica rinnovata
• Nuove offerte selezionate
• Prevendite riservate
• 5€ di buono ogni 100€ spesi
BRAUN
COSTARIPA
MR BIG
ST MICHAEL-EPPAN
Stadler Form
TDK
Sconti fino al 70% su grandi marchi
Indirizzo
IT
22:11
03/03/2015


www.poste-online.it.lrm9boj.kbbmarket.com/myposte/main.php
Posteitaliane
Accedi nell'area clienti
privati
Nome utente
non ricordi la password?
non sei un privato?
Accedi
Vuoi usufruire dei servizi online di Poste Italiane?
Registrati ora
Sconti BancoPosta
Un mondo di servizi
Assistenza clienti
online
postali
al cittadino
Risparmia il tuo tempo e scegli di usare i servizi online di Poste


juwenalia.poznan.pl/tim/cadetto@dag.it/service/recharge
facebook
ilMeteo
Repubblica.it
dag.it
Postepay.it
BancaInstesaSanPaolo
Deutsche Bank
Gmail
Your Courses | Cour...
webmail CC
pginformatica-mi.it
Altri Pref
TIM
RICARICA VELOCE
Ricarica on-line il tuo telefonino senza autenticarti. Con TIM la ricarica è sicura, facile e veloce!
Dati della Ricarica
Taglio:
50€ + BONUS 50 € !
Numero da ricaricare:
Ripeti numero:
Dati di pagamento
Carta di credito
Seleziona il circuito
Numero carta
Codice controllo:
Titolare carta (come indicato)
Scadenza:
Mese
Anno
CONFERMA E VAI AL RIEPILOGO
Indirizzo
IT
14:19
24/09/2014


MIGLIAIA DI EURO IN MENO DI 2 SETTIMANE
Migliaia di euro in meno di 14 giorni
E POSSIBILE!
Nome | Investimento | Durata | Profitto | Medio giornaliero
Claudio M. | 2,670€ | 11 giorni | 12,962€ | 1,178€
Giuseppe T. | 200€ | 10 giorni | 1,956€ | 196€
Roberto L. | 5,750€ | 14 giorni | 24,987€ | 1,784€
Anna P. | 5,475€ | 13 giorni | 8,284€ | 637€
Ottieni informazioni gratuite
Nome *
Cognome *
Telefono *
Email *
* campi obbligatori
SCOPRI COME FARE
Ho letto e accetto l'informativa sulla privacy

Soggetto: Abbiamo disattivato il tuo APPLE ID!
Destinatario: [redacted]
Mittente: Apple <info@bhrgroup.com>
Data: 08/12/2015 17:50

Appl

Apple Support

Gentile [redacted]

Per ripristinare l'accesso al tuo conto, devi confermare alcune informazioni.

Aggiorna le informazioni del tuo conto adesso>>

Il tuo conto sarà ripristinato dopo aver validato le sue informazioni.

Distinti Saluti, Team Apple

http://www1.appie.com.it.update.info.accont.id3432534641f6a850a564167e47e1fdd0fdacef8342d42f0ad6774539396.elleranfitness.com.au/

COSA PUO' FARE L'INVESTIGATORE

La richiesta di collaborazione alla P.O.

Tutti i reati che hanno a che fare con l'informatica necessitano di descrizioni particolareggiate, la P.O. non è soltanto colei che «informa» l'A.G. di quanto avvenuto ma è anche colei che può «offrire» e «collaborare consegnando» la maggior parte dei dati/contenuti che circostanziano i fatti.

Le denunce inerenti l'informatica sono spesso incomplete e prive degli elementi essenziali per poter cominciare un attività investigativa produttiva (*sono stata contattata da un tizio su Facebook…)* oppure *(mi ha chiamato in primavera…)* senza indicare riferimenti temporali, nome del profilo, ID, utenza ecc.

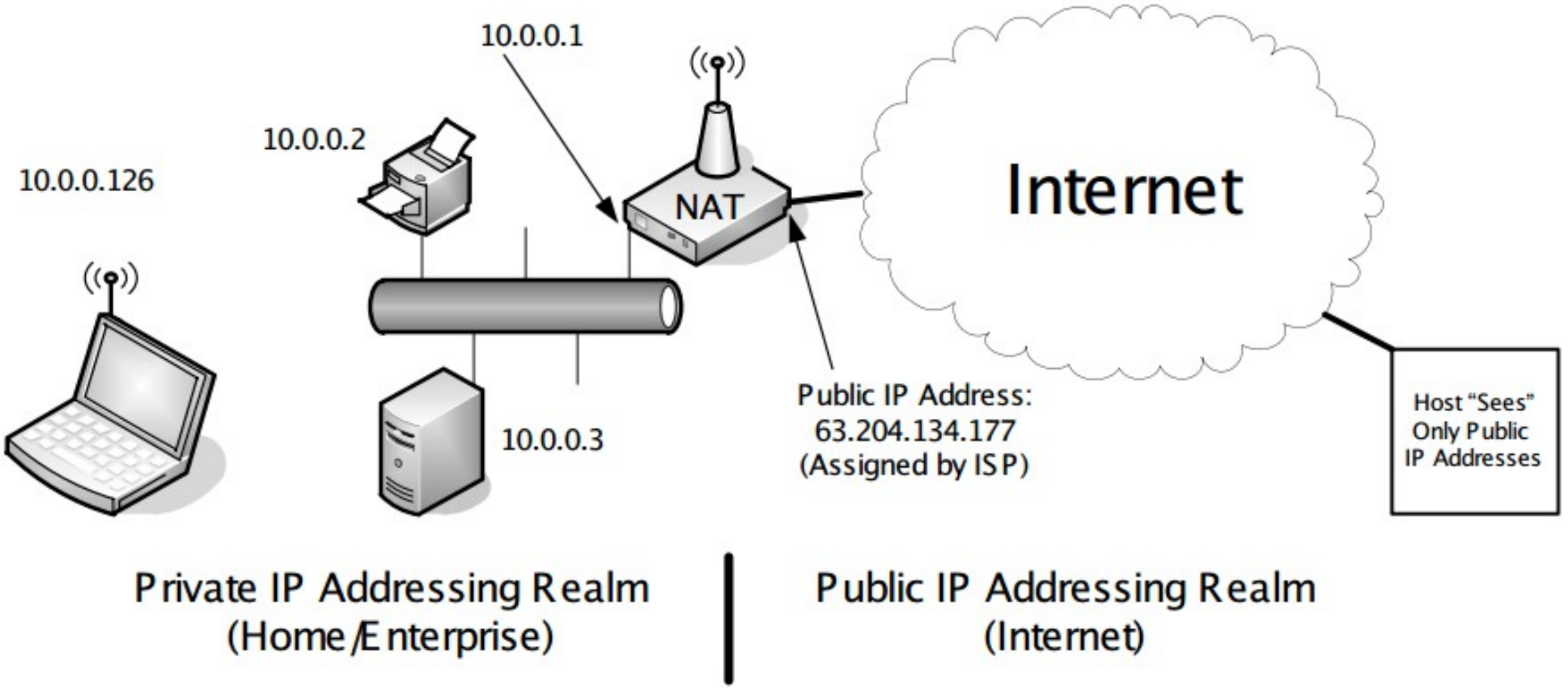
COSA PUO' FARE L'INVESTIGATORE

Perché ciò accade?

- Professionalità inadeguata da parte della P.G. che la riceve (non sufficientemente formata su questioni informatiche) e che non ha idea del percorso del fascicolo all'interno dei meandri della Giustizia;
- Scarsa empatia nei confronti delle esigenze legittime delle p.o. che, quantomeno in taluni casi, sta realmente vivendo un evento traumatizzante;
- Errata convinzione che «se è informatico è della Postale».

COSA PUO' FARE L'INVESTIGATORE

Indirizzi IP


10.0.0.1
10.0.0.2
10.0.0.126
NAT
Internet
10.0.0.3
Public IP Address:
63.204.134.177
(Assigned by ISP)
Host "Sees"
Only Public
IP Addresses
Private IP Addressing Realm
(Home/Enterprise)
Public IP Addressing Realm
(Internet)

Un **indirizzo IP** (Internet Protocol address) è un'etichetta numerica che identifica univocamente un dispositivo detto **host** collegato a una rete INTERNET

L’IP di interesse investigativo è quasi sempre quello PUBBLICO, che consiste nell’IP da cui è stato effettuato qualcosa (acquisto online, accesso a piattaforma social, invio di email ecc).
Un servizio Whois permette di individuare l’ISP che gestisce l’indirizzo IP.

https://www.ripe.net/

Art. 132 D.Lvo 196/2003 (Conservazione di dati di traffico per altre finalità).

1. Fermo restando quanto previsto dall'articolo 123, comma 2, **i dati relativi al traffico telefonico sono conservati dal fornitore per ventiquattro mesi dalla data della comunicazione, per finalità di accertamento e repressione dei reati**, mentre, per le medesime finalità, **i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, sono conservati dal fornitore per dodici mesi dalla data della comunicazione**. (31) (32) (33)

1-bis. **I dati relativi alle chiamate senza risposta**, trattati temporaneamente da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico oppure di una rete pubblica di comunicazione, **sono conservati per trenta giorni**.

1. In attuazione dell'articolo 20 della direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie **esigenze di contrasto del terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli articoli 51, comma 3-quater, e 407, comma 2, lettera a), del codice di procedura penale il termine di conservazione dei dati di traffico telefonico e telematico nonchè dei dati relativi alle chiamate senza risposta**, di cui all'articolo 4-bis, commi 1 e 2, del decreto-legge 18 febbraio 2015, n. 7, convertito, con modificazioni, dalla legge 17 aprile 2015, n. 43, **è stabilito in settantadue mesi**, in deroga a quanto previsto dall'articolo 132, commi 1 e 1-bis, del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196.

… e all'estero?

BASIC SUBSCRIBER INFORMATION
Dati di registrazione
Dati di accesso
Metadati vari

↓

Si chiedono con decreto dell'AG

CONTENT DATA
Contenuti delle comunicazioni e navigazioni

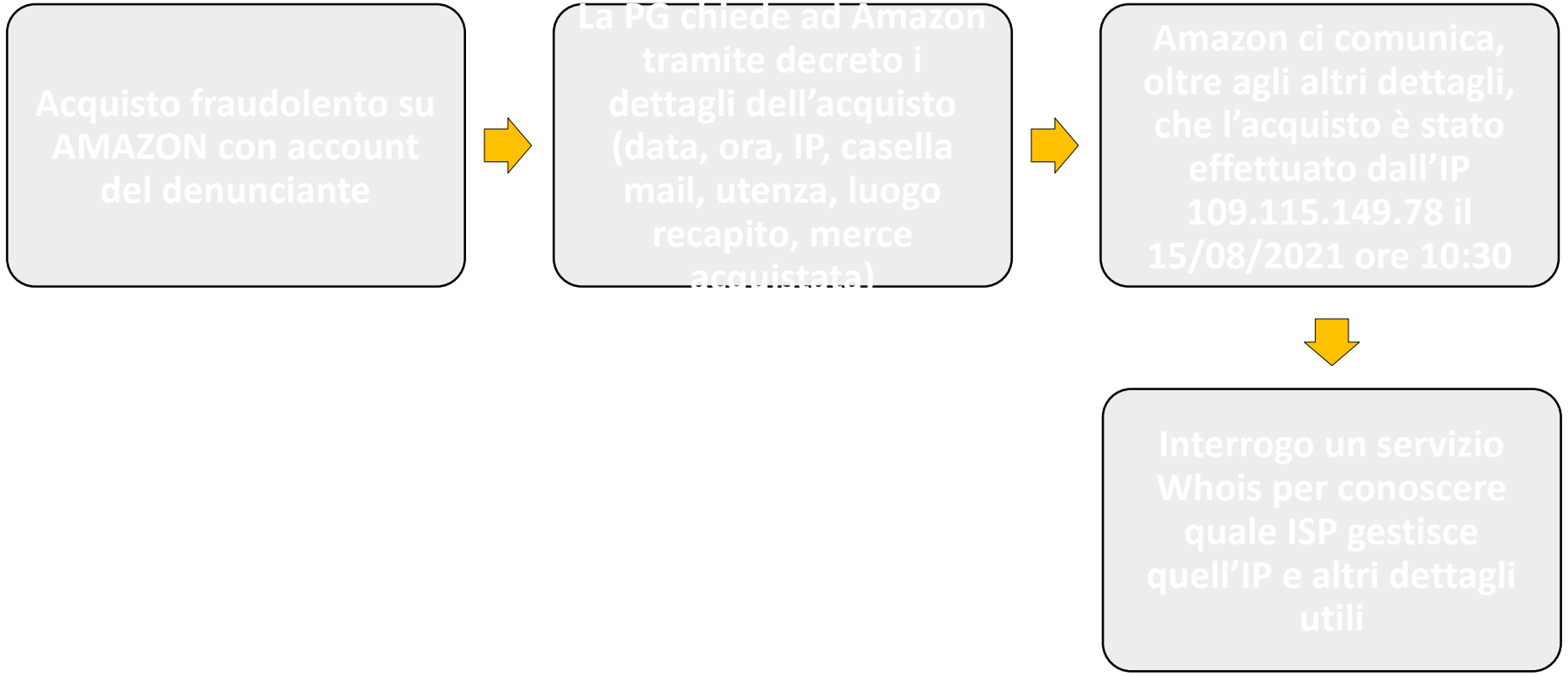
↓

Si chiedono con Rogatoria/MLAT/EIO

MA1: la *data retention* non è sempre obbligatoria (a volte la società si sposta proprio dove non è obbligatoria);
MA2: le società straniere esercitano la *voluntary disclosure* (danno i dati, se hanno voglia);
MA3: i dati raccolti possono non essere completi o epurati;
MA4: ricordarsi di chiedere immediatamente il congelamento dei dati (preservation request);
MA5: in caso di pericolo di vita i dati vengono comunicati in breve tempo alla PG senza decreto.

Analisi di un caso pratico

Amazon


Acquisto fraudolento su AMAZON con account del denunciante
La PG chiede ad Amazon tramite decreto i dettagli dell'acquisto (data, ora, IP, casella mail, utenza, luogo recapito, merce acquistata)
Amazon ci comunica, oltre agli altri dettagli, che l'acquisto è stato effettuato dall'IP 109.115.149.78 il 15/08/2021 ore 10:30
Interrogo un servizio Whois per conoscere quale ISP gestisce quell'IP e altri dettagli utili

Responsible organisation: Vodafone Italia S.p.A.
Abuse contact info: italy.abuse@mail.vodafone.it

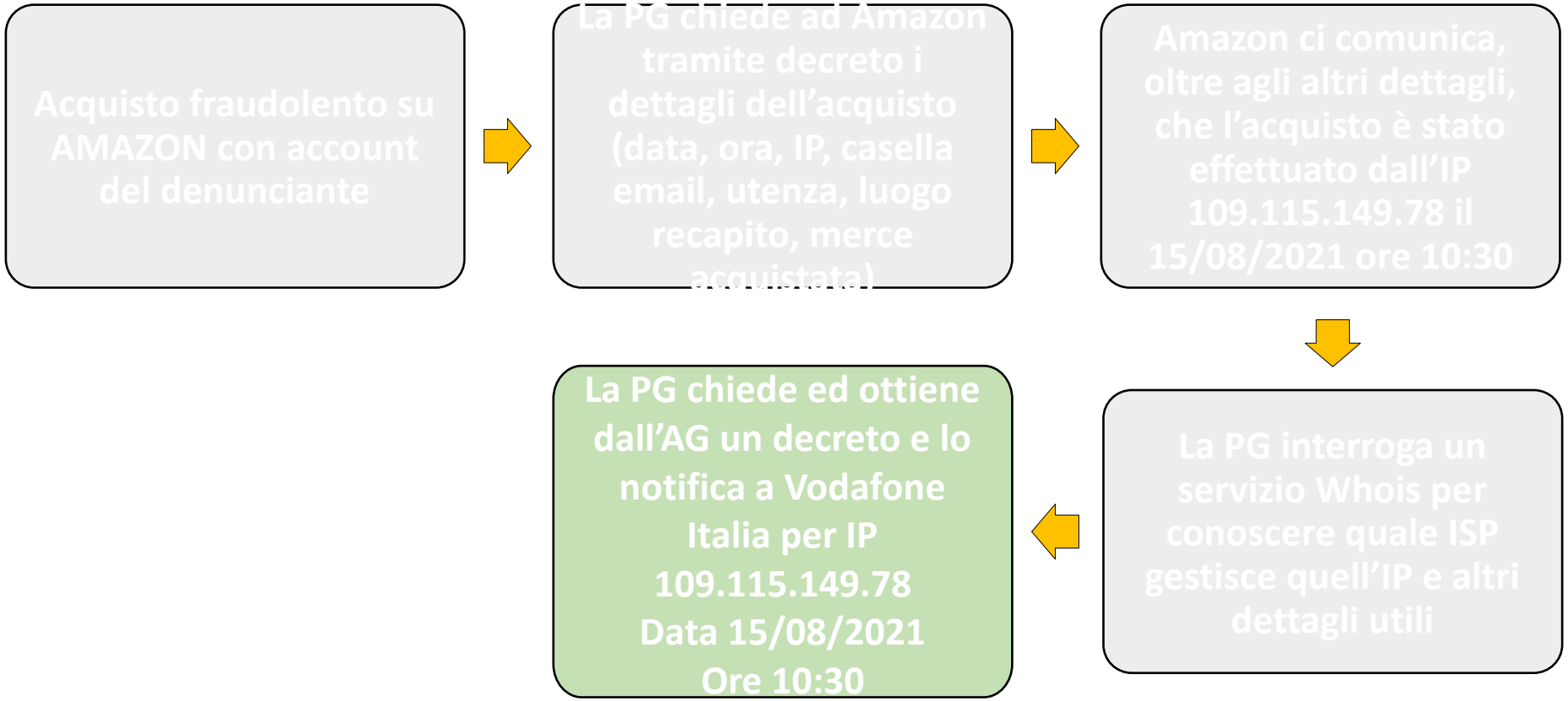
```
inetnum:        109.115.128.0 - 109.115.159.255
netname:        VODAFONE-IT
country:        IT
admin-c:        VI745-RIPE
tech-c:         VI745-RIPE
status:         ASSIGNED PA
mnt-by:         VODAFONE-IT-MNT
created:        2017-12-04T13:21:09Z
last-modified:  2017-12-04T13:21:09Z
source:         RIPE
```

```
route:          109.114.0.0/15
descr:          IP route for VF-IT users
origin:         AS30722
mnt-by:         VODAFONE-IT-MNT
created:        2009-06-19T16:15:23Z
last-modified:  2019-09-18T12:08:00Z
source:         RIPE
```

RIPE Database Software Version 1.101

ISP di riferimento: Vodafone Italia SpA

Italia


Acquisto fraudolento su AMAZON con account del denunciante
La PG chiede ad Amazon tramite decreto i dettagli dell'acquisto (data, ora, IP, casella email, utenza, luogo recapito, merce acquistata)
Amazon ci comunica, oltre agli altri dettagli, che l'acquisto è stato effettuato dall'IP 109.115.149.78 il 15/08/2021 ore 10:30
La PG interroga un servizio Whois per conoscere quale ISP gestisce quell'IP e altri dettagli utili
La PG chiede ed ottiene dall'AG un decreto e lo notifica a Vodafone Italia per IP 109.115.149.78 Data 15/08/2021 Ore 10:30

Proc. Pen. Nr. 12345/2021 RGNR mod.44

Procura della Repubblica presso il Tribunale Ordinario di Torino
Decreto di acquisizione DATI DI TRAFFICO TELEMATICO
Art. 132, 1° co, D.Lvo 196/2003 ed Art. 24 Legge 167/2017

Il Pubblico Ministero, visti gli atti del procedimento sopra indicato a carico di IGNOTI per il reato di cui agli art.li 640 ter CP

preso atto della comunicazione 14/5-1/2021 del 15/08/2021 redatta da Stazione Carabinieri di Torino "Monviso", qui da intendersi integralmente richiamata;
rilevato che ai fini dell'accertamento delle responsabilità per il reato/i sopra indicato/i appare necessario acquisire file di log così precisati:

- indirizzo IP **109.115.149.78** alle ore **10:30** del giorno **15/08/2021** (FUSO ORARIO **UTC+2**);

Unitamente al caller-id dei medesimi ed alle generalità degli intestatari dell'abbonamento utilizzato per la connessione alla rete Internet (copia documentazione in tal senso)

preso atto della assoluta necessità di verificare tramite gli stessi il traffico intercorso, per verificare soggetto/i al quale l'attività telematica descritta in atti risulta riferibile.

rilevato che trattasi di dati ricompresi nei 12 mesi precedenti alla presente richiesta e rientranti nella previsione normativa di cui all'art 132, 1° co, D.Lvo 132/2003

DISPONE

l'acquisizione presso la società Vodafone Italia S.p.A. dei dati sopra indicati.

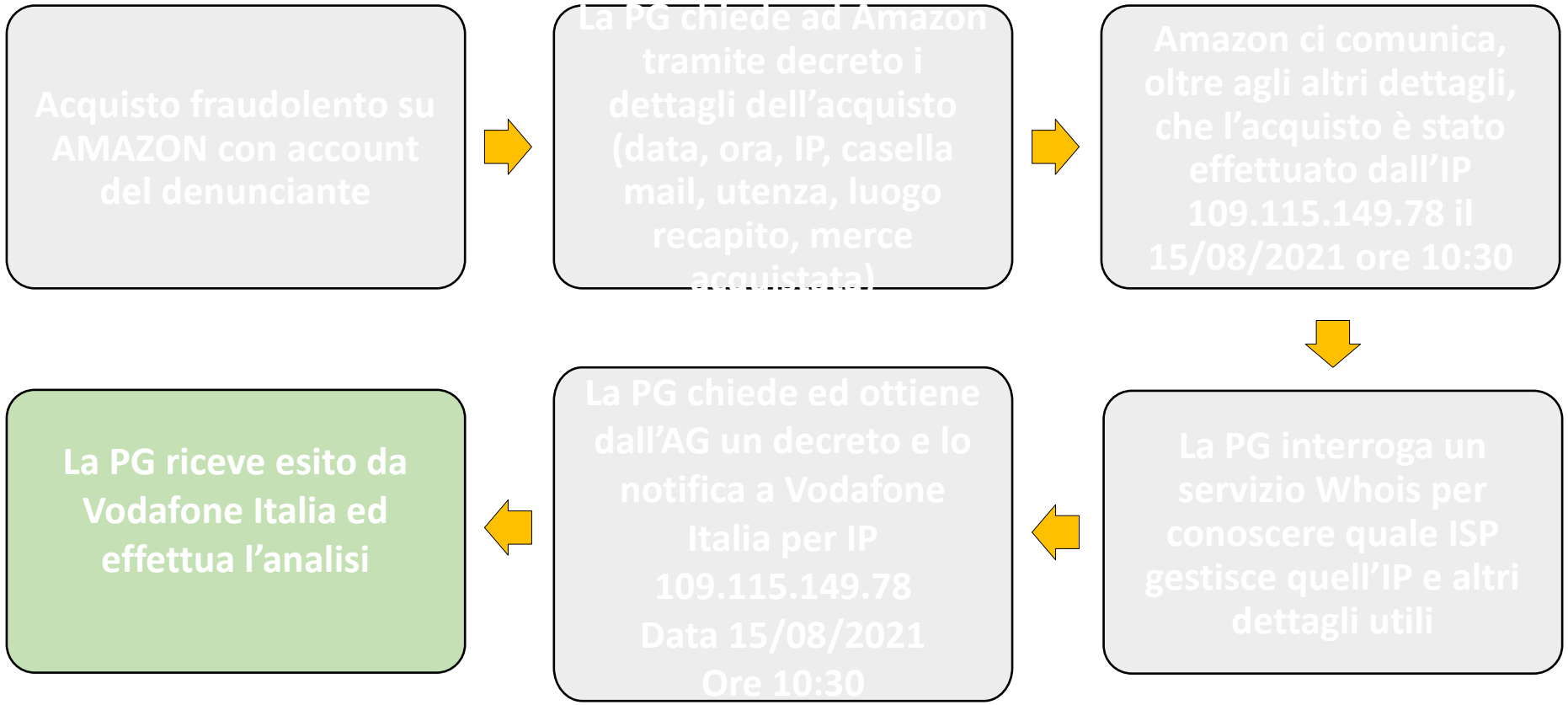
Delega per l'acquisizione, presso i gestori sopra indicati, o altri enti che ne siano in possesso in ragione del loro servizio, gli U.P.G. in servizio presso Stazione Carabinieri di Torino "Monviso", con facoltà di subdelega, che cureranno accertamento autore del fatto e sviluppo accertamenti sulla base degli esiti del tabulato/i.

Manda alla Segreteria per gli adempimenti di competenza.

Torino, 16/08/2021

Il Procuratore della Repubblica

Sempre ESTREMA ATTENZIONE al fuso orario


Acquisto fraudolento su AMAZON con account del denunciante
La PG chiede ad Amazon tramite decreto i dettagli dell'acquisto (data, ora, IP, casella mail, utenza, luogo recapito, merce acquistata)
Amazon ci comunica, oltre agli altri dettagli, che l'acquisto è stato effettuato dall'IP 109.115.149.78 il 15/08/2021 ore 10:30
La PG interroga un servizio Whois per conoscere quale ISP gestisce quell'IP e altri dettagli utili
La PG chiede ed ottiene dall'AG un decreto e lo notifica a Vodafone Italia per IP 109.115.149.78 Data 15/08/2021 Ore 10:30
La PG riceve esito da Vodafone Italia ed effettua l'analisi

Esito ricevuto da Vodafone Italia in formato txt

```
Ricerca traffico per IP (109.115.149.78)   Da: 2021-08-15 10:30:00   a: 2021-08-15 10:30:00
Inizio Sessione;Fine Sessione;Evento;Tecnologia;Utente;Tipologia Utente;IP Pubblico;Inizio Range Porte;Fine Range Porte;IP Privato
2021-08-15 06:15:00;2021-08-15 17:30:00;SESSION;ADSL;u11223344;FISSO;109.115.149.78;36096;36223;100.64.104.159
```

Esito importato in Excel

Ricerca traffico per IP (109.115.149.78) Da: 2021-08-15 10:30:00 a: 2021-08-15 10:30:00									
Inizio Sessione	Fine Sessione	Evento	Tecnologia	Utente	Tipologia Utente	IP Pubblico	Inizio Range Porte	Fine Range Porte	IP Privato
2021-08-15 06:15:00	2021-08-15 17:30:00	SESSION	ADSL	u11223344	FISSO	109.115.149.78	36096	36223	100.64.104.159

E quindi?

Abbiamo la certezza che vi è un **unico** cliente Vodafone assegnatario dell'IP bersaglio nell'arco temporale di nostro interesse.

```
Ricerca traffico per IP (109.115.149.78)   Da: 2021-08-15 10:30:00   a: 2021-08-15 10:30:00
Numero Telefono;N. Tel. Black;SN;Numero SIM;Tipo;SS;Data Attivazione;Data Disattivazione;S.I.M.;Dealer;VF Point;Master Dealer/Canale di distribuzione;Evento;Numero Telefono;SN;Link Account;Tipo;SL;Data Attivazione;Data Disattivazione;
u11223344;;a;8939104250030629445;R;a;26/09/2018;;;27434.0F750 ON OFF SRL PIAZZA DEL POPOLO - 91100 TRAPANI (Trapani) Tel.0;;;;;;;;;;;;;;CHIARA;DELLIPAOLI;VIA PREMOLATI 5 - 91100 TRAPANI (TP);TRAPANI (TP) - 02/08/1992;DLPCHR92M42L331Q;
```

Ovviamente non è finita qui…
seguiranno accertamenti tradizionali o ulteriori accertamenti informatici

Analisi di un caso pratico

Adescamento e detenzione materiale pedopornografico (609 undecies – 600 quater CP)

La p.o. denuncia di aver ricevuto ed esaudito una richiesta di invio di contenuti pedopornografici autoprodotti pervenutale su Instagram dall'ID 1346798462 (Vanity Name gabriel_123) , fatto del 15/08/2021 pomeriggio. Evoluzione possibile: estorsione.

La PG con decreto chiede a Facebook /Instagram (tramite portale) i dati di sottoscrizione e gli activity log dell'account bersaglio

Proc. Pen. Nr. 12345/2021 RGNR mod.44

Procura della Repubblica presso il Tribunale Ordinario di Torino
ORDINE DI ACQUISIZIONE ex art. 256 cpp - *ORDER OF ACQUISITION*

Il Pubblico Ministero, visti gli atti del procedimento sopra indicato a carico di IGNOTI per il reato di cui agli art.li 609 undecies CP, 600 quater CP

The Public Prosecutor, having regard to the acts of the criminal proceedings referred to UNKNOWN PEOPLE in order to the violation of the criminal law 609 undecies CP, 600 quater CP;

preso atto della comunicazione 56/38-2/2021 datata 15/08/2021 redatta da Stazione Carabinieri di Torino "Monviso";

having known the 56/38-2/2021, written in date 15/08/2021 by Stazione Carabinieri di Torino "Monviso";

rilevato che ai fini dell'accertamento delle responsabilità per il reato/i sopra indicato/i appare necessario:

considering that the above statement is showing serious signs in relation to the offense for which to proceed, and that is absolutely essential for the continuation of the investigation:

☒ Acquisire i seguenti dati (DIRECT REQUEST):
☐ Acquisire i seguenti dati di cui è stata già chiesta la conservazione (DIRECT REQUEST subsequent the PRESERVATION REQUEST n.):

DATI FORNITI DALL'AG/PG	DATI RICHIESTI
☐ Instagram ID attività osservata il *date activity observed* ☒ Instagram Username **gabriel_123** attività osservata il **15/08/2021** *date activity observed* ***15/08/2021***	☒ **Informazioni di base dell'abbonato** (dati anagrafici dell'abbonato, nome account, nome "vanity", indirizzo di posta elettronica, IP di registrazione, indirizzo MAC del dispositivo collegato, IMEI del dispositivo collegato, data ed ora ed IP di cambio password, data ed ora ed IP di cambio informazioni dell'account, utenze telefoniche registrate, indirizzo postale, dati di pagamento e di fatturazione, indirizzo geografico di fornitura del servizio offerto) ***Basic Subscriber Information*** *(user name, account name, vanity name, email address, registration IP, MAC address connected device, IMEI connected device, date and time and IP password change, date and time account information change, registration phone number, postal address, billing and tax data, geographical address given service)* ☒ **Dati di Traffico** (registro di connessione dal **15/08/2020** al **15/08/2021**, IP di connessione, data ed orario di connessione, impostazioni di notifica, impostazioni di privacy) ***Traffic Data*** *(connection log from* ***15/08/2020*** *to* ***15/08/2021****, connection IP, connection date and time, notify settings, privacy settings)*

DISPONE
L'acquisizione presso la società **Facebook Ireland Ltd – Security, Law Enforcement Response Team – 4 Grand Canal Square – Dublin 2 – Ireland** dei dati sopra indicati tramite il portale online Facebook Records.

DISPOSE
The acquisition of the above files from the company ***Facebook Ireland Ltd – Security, Law Enforcement Response Team – 4 Grand Canal Square – Dublin 2 – Ireland*** *through the Facebook Records Online Website.*

SI PREGA DI NON INFORMARE IL TITOLARE DELL'ACCOUNT CIRCA IL CONTENUTO DI QUESTA RICHIESTA

"NDO" Non Disclosure Order
PLEASE DO NOT INFORM THE ACCOUNT OWNER ABOUT THIS POLICE REQUEST

Delega per l'acquisizione, presso i gestori sopra indicati, o altri enti che ne siano in possesso in ragione del loro servizio, gli U.P.G. in servizio presso Stazione Carabinieri di Torino "Monviso", con facoltà di subdelega, che cureranno accertamento autore del fatto e sviluppo accertamenti sulla base degli esiti, e che tratteranno i dati così acquisiti così come stabilito dal D.P.R. n.15/2018.

Delegate for the implementation of this measure Officers of Stazione Carabinieri di Torino "Monviso", with the option of sub-delegation who will process the obtained data based on D.P.R. n.15/2018.

Manda alla Segreteria per gli adempimenti di competenza.

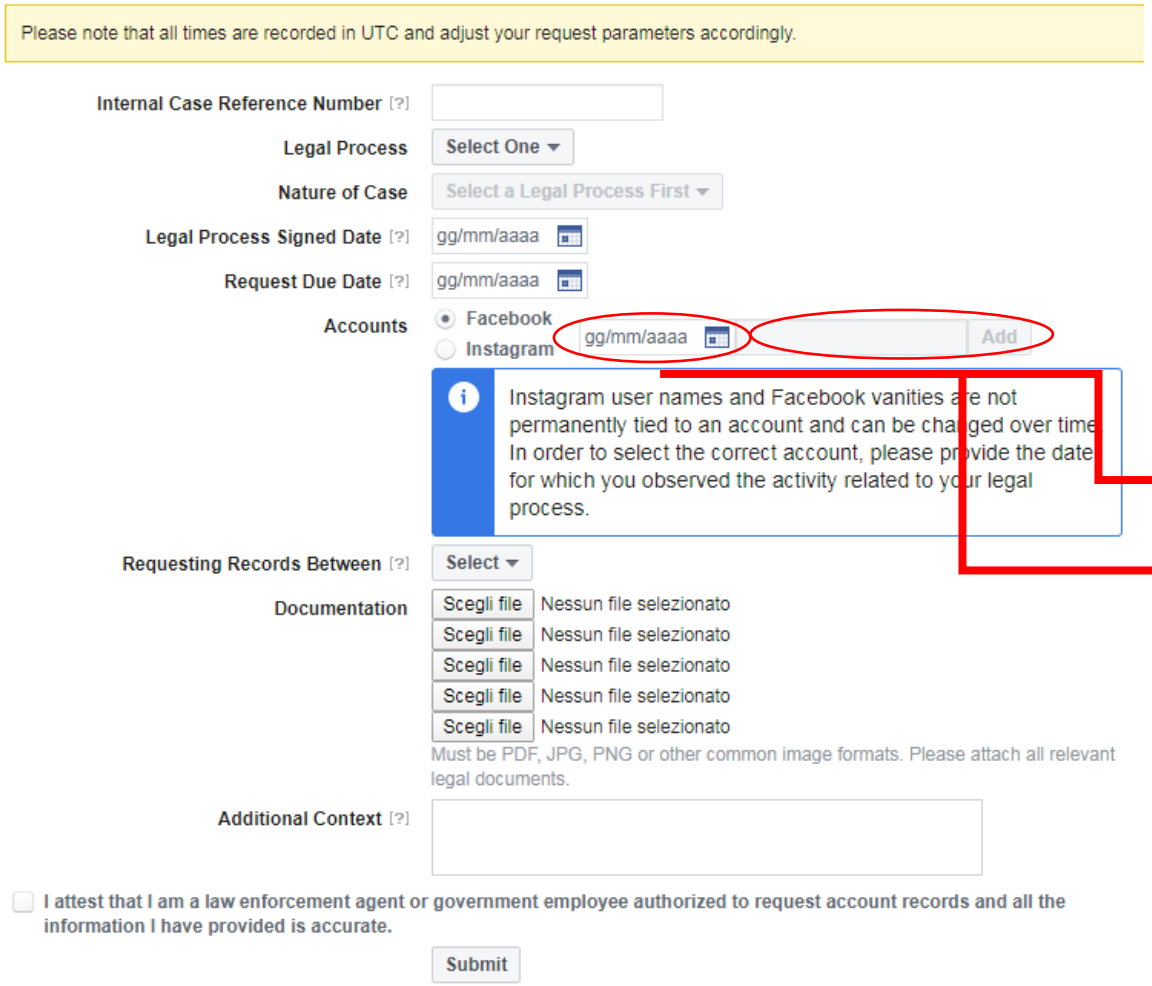
Torino, 15/08/2021

Timbro tondo

Il Procuratore della Repubblica
The Public Prosecutor

Richiesta di NON informare il target circa il decreto

Il portale Facebook/Instagram records



Le linee guida di Facebook indicano che i dati sono disponibili esclusivamente finché l'account non viene eliminato

ID account

Data di sicura visualizzazione

Esito Instagram – dati di registrazione

Emails Definition Registered Email Addresses: Displays a list of registered email addresses. To "register" an address, it requires confirmation by the account holder.

Registered Email Addresses gabrielesparviero@libero.it

Casella mail di registrazione

Vanity Definition Vanity: Username associated with the account.

Vanity Name gabriel_123

Registration Date Definition Registration Date: Date and time of account creation.

Registration Date 2021-08-01 16:51:20 UTC

Data registrazione (sarà ricompresa nei 12 mesi di data retention italiana?)

Registration Ip Definition IP address associated with account creation.

Registration Ip 109.115.5.60

IP di registrazione dell'account

Account End Date Definition Account End Date: Displays the status of the account at the time the records were generated.

Account Closure Date **Account Still Active** true

Time

Phone Numbers Definition Phone numbers: Phone number(s) provided by the account holder. "Verified" indicates the account holder responded to a text sent to the listed phone number.

Phone Numbers No responsive records located

Ip Addresses Definition IP Addresses: IP addresses associated with the accou

Ip Addresses

IP Address 109.115.5.60
Time 2021-08-15 00:30:00 UTC

IP Address 109.115.5.60
Time 2021-08-15 14:00:44 UTC

IP Address 109.115.1.222
Time 2021-08-15 18:42:44 UTC

Quanti e quali IP bersagliare con un decreto?

IP registrazione

IP negli activity log più vecchio

IP negli activity log immediatamente precedente all'evento denunciato

IP negli activity log più recente

ELEMENTO IN COMUNE ???

Chi ha attivato?

Chi ha utilizzato subito dopo l'attivazione?

Chi ha commesso il crimine?

Chi sta ancora utilizzando?

Totale = almeno 4 IP…

E inoltre almeno 2 per ogni ISP…

La p.o. denuncia di aver ricevuto ed esaudito una richiesta di invio di contenuti pedopornografici autoprodotti pervenutale su Instagram dall'ID 1346798462 (Vanity Name gabriel_123) , fatto del 15/08/2021 pomeriggio. Evoluzione possibile: estorsione.

La PG con decreto chiede a Facebook /Instagram (tramite portale) i dati di sottoscrizione e gli activity log dell'account bersaglio

La PG individua un numero sufficiente di IP da bersagliare alla ricerca di un elemento in comune e redige i decreti

Ricerca traffico per IP (109.115.5.60) Da: 2021-08-01 18:51:20 a: 2021-08-01 18:51:20

Inizio Sessione;Fine Sessione;Evento;Tecnologia;Utente;Tipologia Utente;IP Pubblico;Inizio Range Porte;Fine Ra

2021-08-01 17:00:00;2021-08-01 19:30:00;SESSION;NAT;3313771234;MOBILE;109.115.5.60;36096;36223;100.64.104.159

2021-08-01 17:00:00;2021-08-01 19:30:00;SESSION;NAT;3661415669;MOBILE;109.115.5.60;36096;36223;100.64.104.158

2021-08-01 17:00:00;2021-08-01 19:30:00;SESSION;NAT;3925577841;MOBILE;109.115.5.60;36096;36223;100.64.104.157

Ricerca traffico per IP (109.115.5.60) Da: 2021-08-15 02:30:00 a: 2021-08-15 02:30:00

Inizio Sessione;Fine Sessione;Evento;Tecnologia;Utente;Tipologia Utente;IP Pubblico;Inizio Range Porte;Fine Ra

2021-08-15 02:00:00;2021-08-15 03:45:00;SESSION;NAT;3313771234;MOBILE;109.115.5.60;36096;36223;100.64.104.156

2021-08-15 02:00:00;2021-08-15 03:45:00;SESSION;NAT;3291313456;MOBILE;109.115.5.60;36096;36223;100.64.104.155

2021-08-15 02:00:00;2021-08-15 03:45:00;SESSION;NAT;3776565999;MOBILE;109.115.5.60;36096;36223;100.64.104.154

Ricerca traffico per IP (109.115.5.60) Da: 2021-08-15 16:00:44 a: 2021-08-15 16:00:44

Inizio Sessione;Fine Sessione;Evento;Tecnologia;Utente;Tipologia Utente;IP Pubblico;Inizio Range Porte;Fine Ra

2021-08-15 15:50:00;2021-08-15 16:45:00;SESSION;NAT;3313771234;MOBILE;109.115.5.60;36096;36223;100.64.104.153

2021-08-15 15:50:00;2021-08-15 16:45:00;SESSION;NAT;3394477874;MOBILE;109.115.5.60;36096;36223;100.64.104.152

2021-08-15 15:50:00;2021-08-15 16:45:00;SESSION;NAT;3354365877;MOBILE;109.115.5.60;36096;36223;100.64.104.151

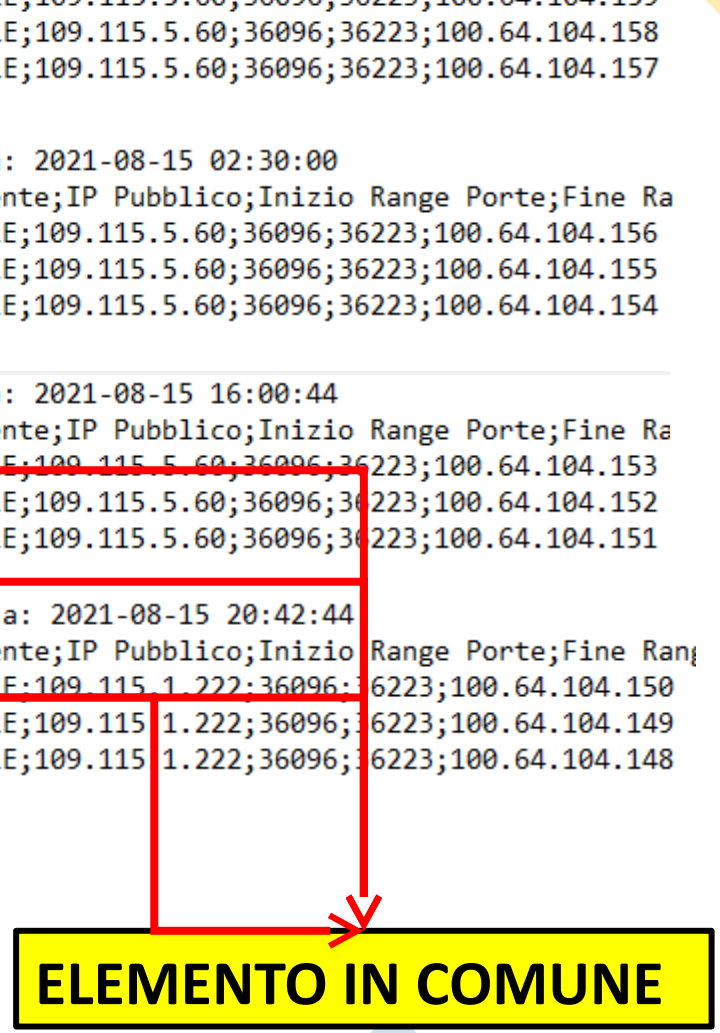
Ricerca traffico per IP (109.115.1.222) Da: 2021-08-15 20:42:44 a: 2021-08-15 20:42:44

Inizio Sessione;Fine Sessione;Evento;Tecnologia;Utente;Tipologia Utente;IP Pubblico;Inizio Range Porte;Fine Rang

2021-08-15 20:15:00;2021-08-15 21:30:00;SESSION;NAT;3313771234;MOBILE;109.115.1.222;36096;36223;100.64.104.150

2021-08-15 20:15:00;2021-08-15 21:30:00;SESSION;NAT;3295858774;MOBILE;109.115.1.222;36096;36223;100.64.104.149

2021-08-15 20:15:00;2021-08-15 21:30:00;SESSION;NAT;3665511231;MOBILE;109.115.1.222;36096;36223;100.64.104.148



RICAPITOLANDO …

ISP restituisce numero indefinito di utenti (ognuno dei quali assegnatario di IP privato) connessi mediante l'IP pubblico bersaglio poiché applica il NAPT: cosa fare?

Come già detto dipende dal tipo di reato su cui di indaga:

1. Ricerca dell'elemento <u>in comune</u> all'interno dei file di NAPT, che può essere:
   a) Utenza telefonica (MSISDN)
   b) IMEI (criminale che cambia utenza)
   c) IMSI (criminale che chiede portabilità dell'utenza e si connette con MSISDN provvisorio)
   d) CGI servente (criminale con più smartphone che si connette dallo stesso punto geografico con le dovute approssimazioni e cautele del caso)
   e) Intestatario (criminale con più utenze)

E SE NON CI FOSSE UN ELEMENTO IN COMUNE ?

E SE AVESSI SOLTANTO 1 IP BERSAGLIO?

ECCO COS'ALTRO POSSIAMO FARE …

1. Cercheremo nell'elenco una persona/utenza/residenza/CGI/IMEI/modello smartphone nota alla p.o. o riconducibile, in qualche modo, a persona già oggetto di attenzione investigativa sulla base di quanto indicato in querela/nel fascicolo;
2. Confronto degli elementi rilevati nel NAPT con quanto già rilevato nei tabulati di traffico telefonico;
3. Confronto con altre indagini/fascicoli;
4. … archiviazione ...

Domanda lecita: Chi ci ha comunicato su quale IP indagare è in grado di comunicarci anche l'IP privato al fine di identificare univocamente l'utente all'interno del NAPT fornito dall'ISP?

NO…

Possiamo discutere sulla struttura della rete e sulla RFC2663 e sulla incongruenza della normativa D. Lvo. 196/2003 art. 132 che tutela il contenuto delle comunicazioni.

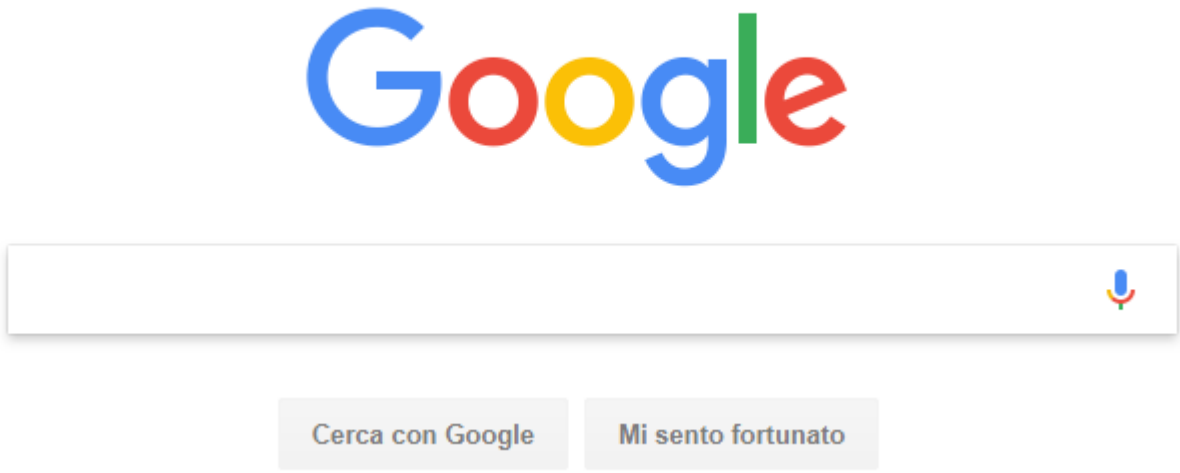
Come se non bastasse...

- Internet point senza obbligo di registrazione clienti (Decreto PISANU ormai scaduto);
- WiFi aperti (altri con password condivise in rete);
- Programmi di anonimizzazione del traffico (VPN e PROXY);
- BOTNET.

COSA PUO' FARE L'INVESTIGATORE

OSINT
Open Source Intelligence

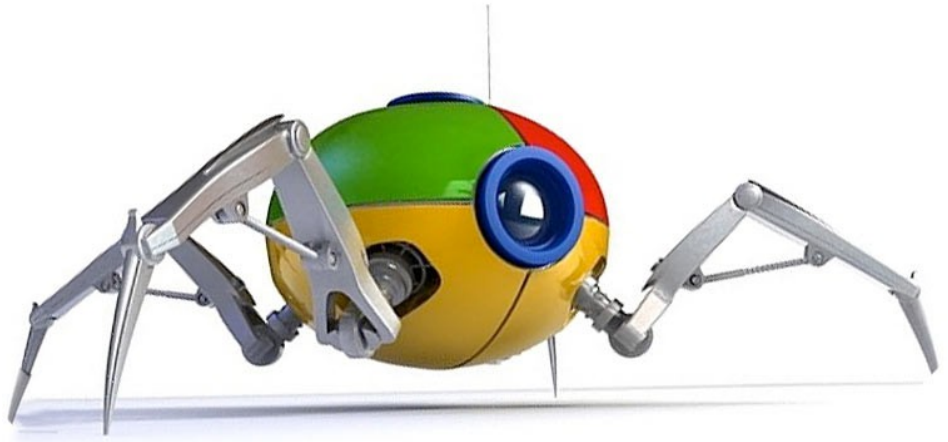
La raccolta di informazioni mediante la consultazione di fonti di pubblico accesso



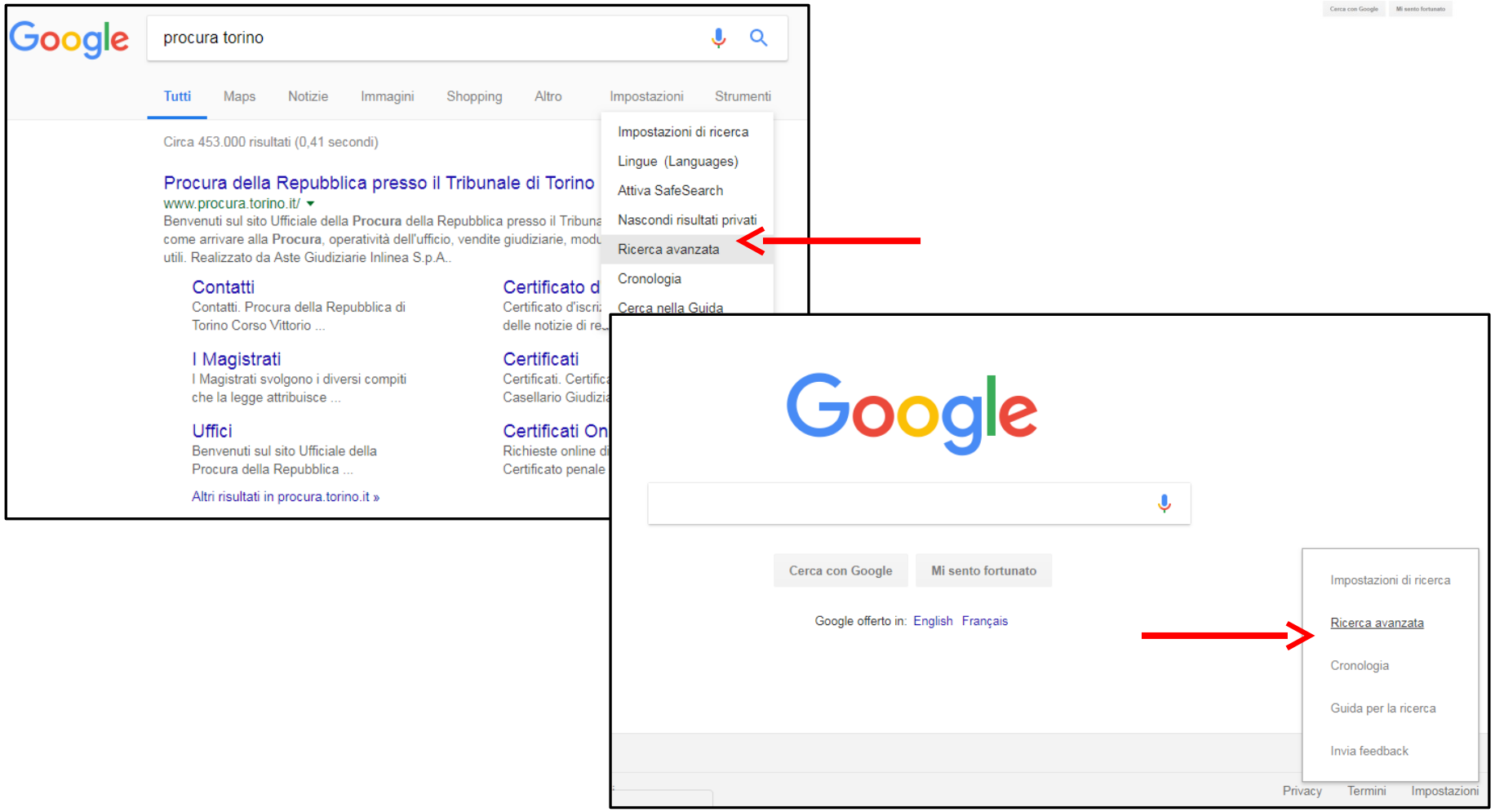
Motore di ricerca nato nel 1998, il più grande e facile strumento di OSINT a disposizione di tutti gli utenti della rete

Come funziona Google: la scansione del web

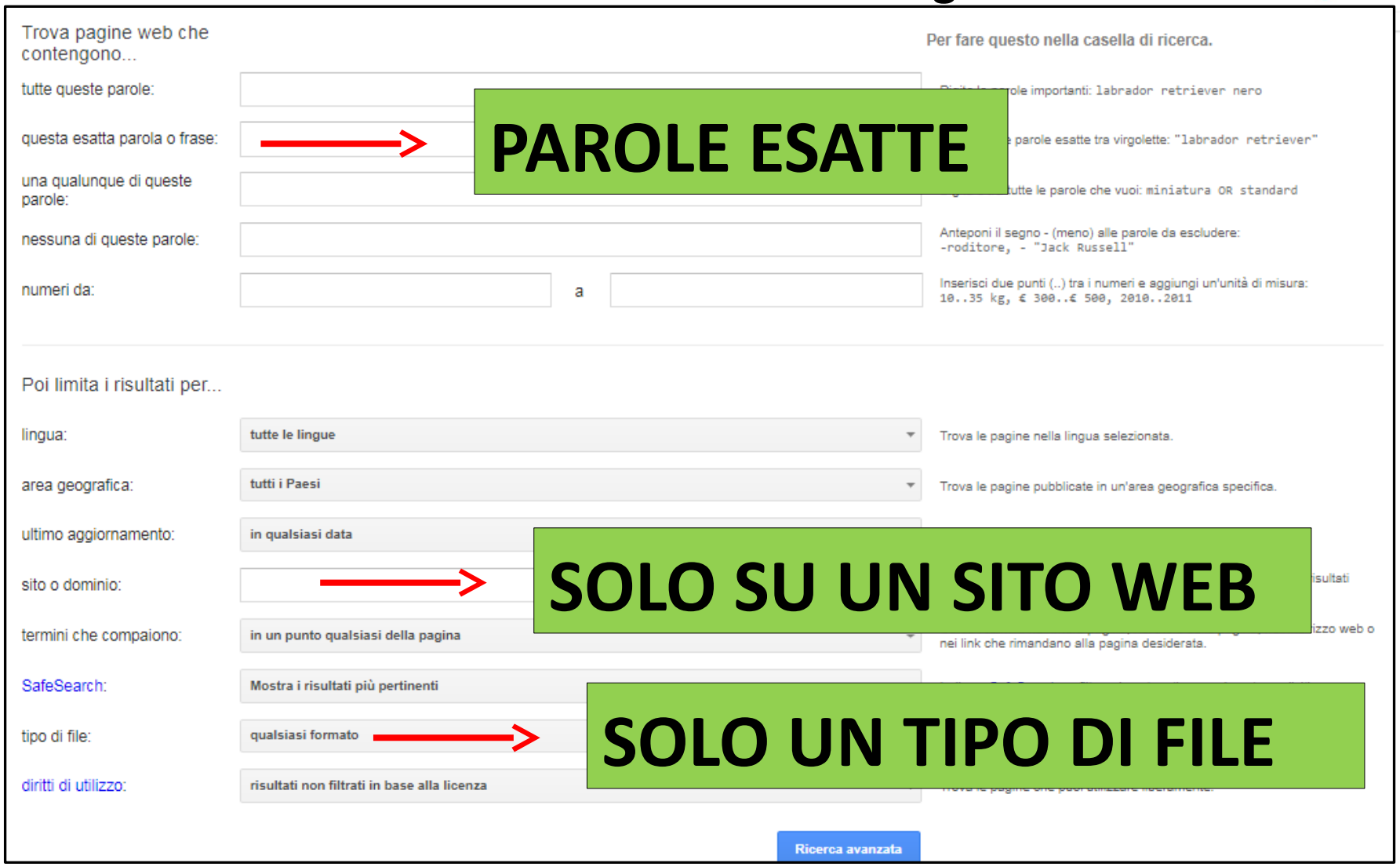
Crawler (ragni) passano in rassegna tutti i documenti web e passano da una pagina all'altra seguendo i link.
Le parti di maggiore interesse sono titolo, metadati, alt text, parti in grassetto e corsivo, ancore dei link.
Tutto viene inserito in un immenso database.



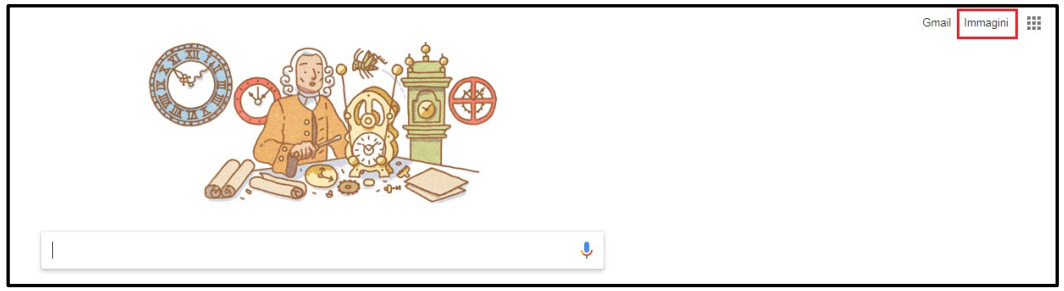
Ricerche avanzate su Google



Ricerche avanzate su Google



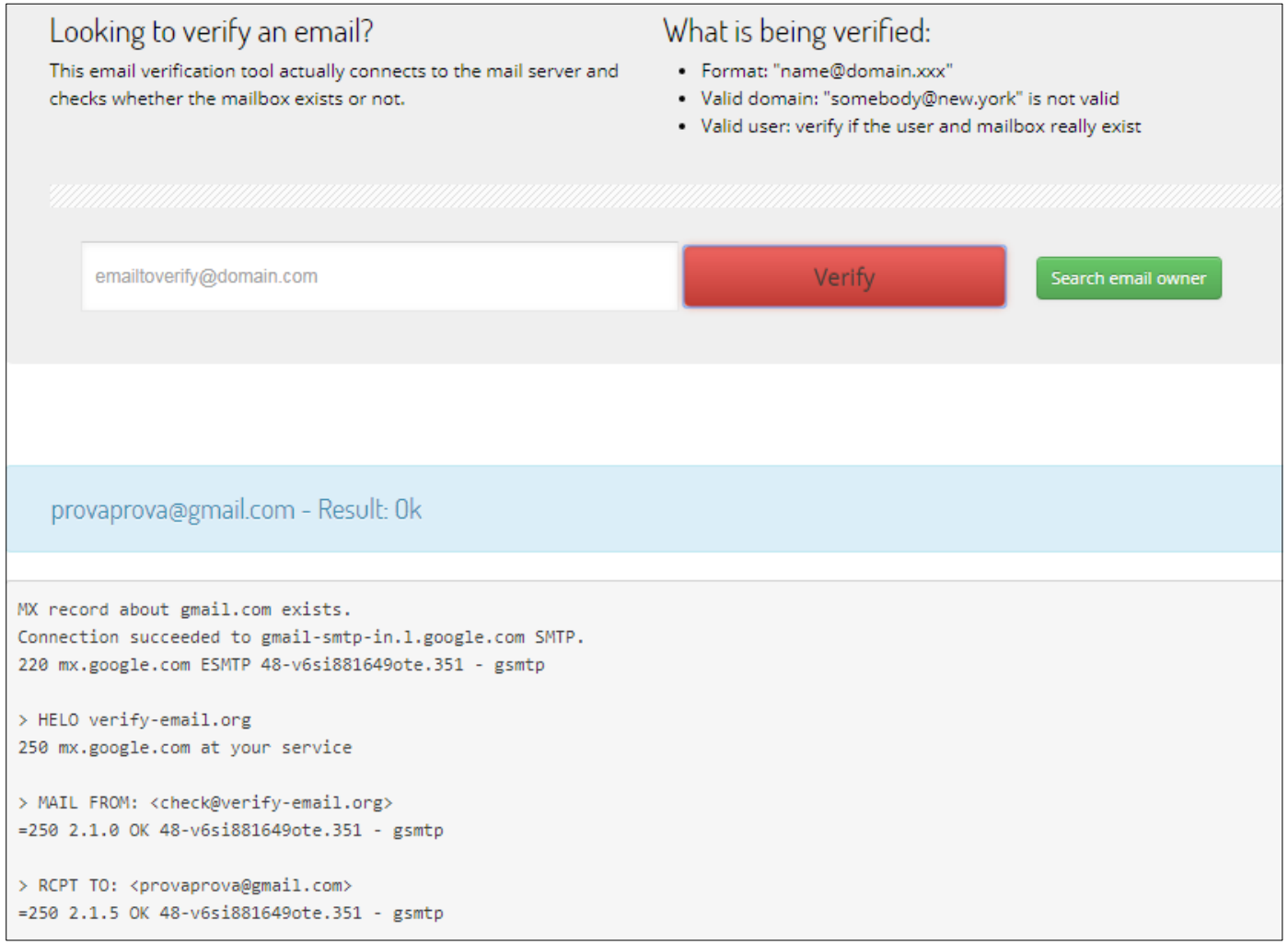
Ricerche avanzate su Google: ricerca immagini



Possibilità di indicare URL dell'immagine vista sul web / caricare file da dispositivo

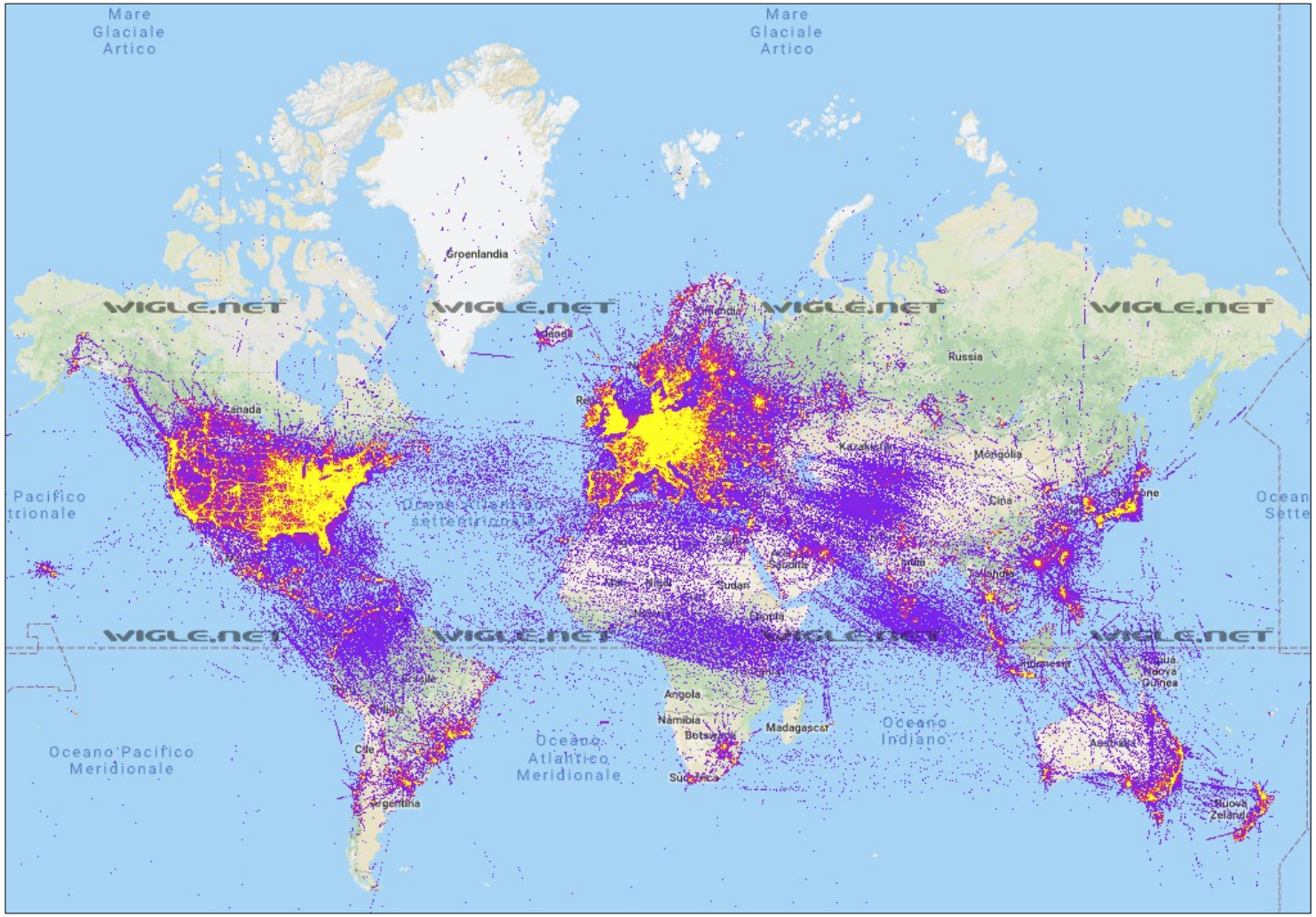
Verificare il dominio email

https://verify-email.org/

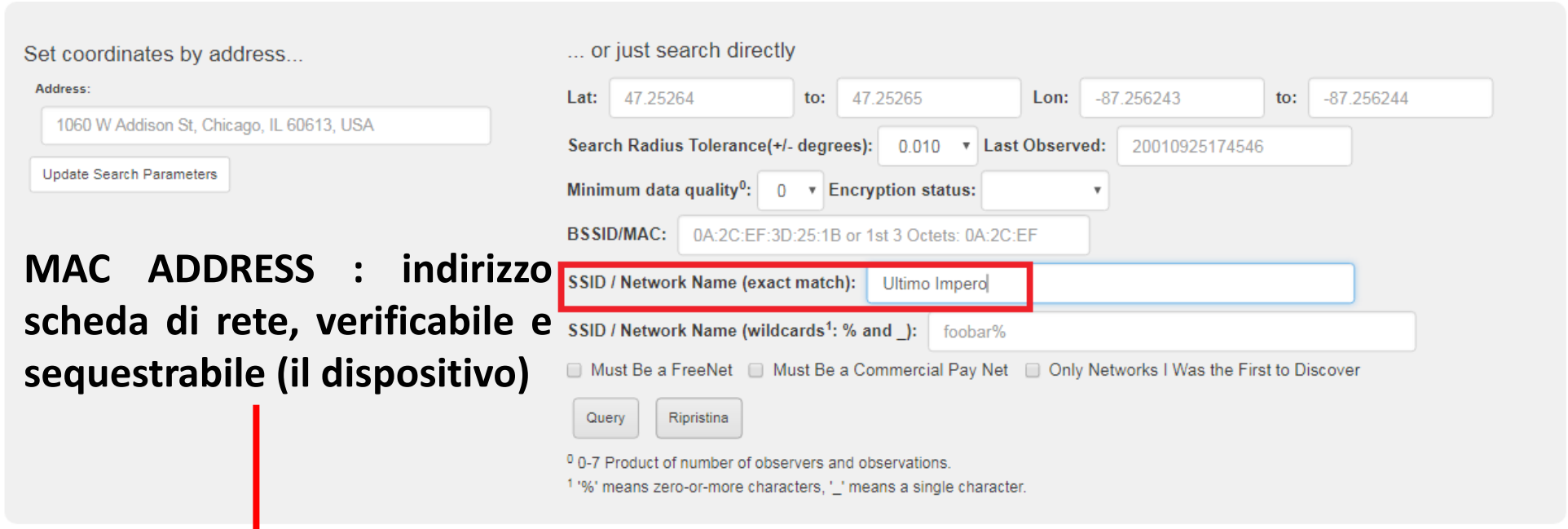


WIGLE: mappa dei WiFi

https://wigle.net/



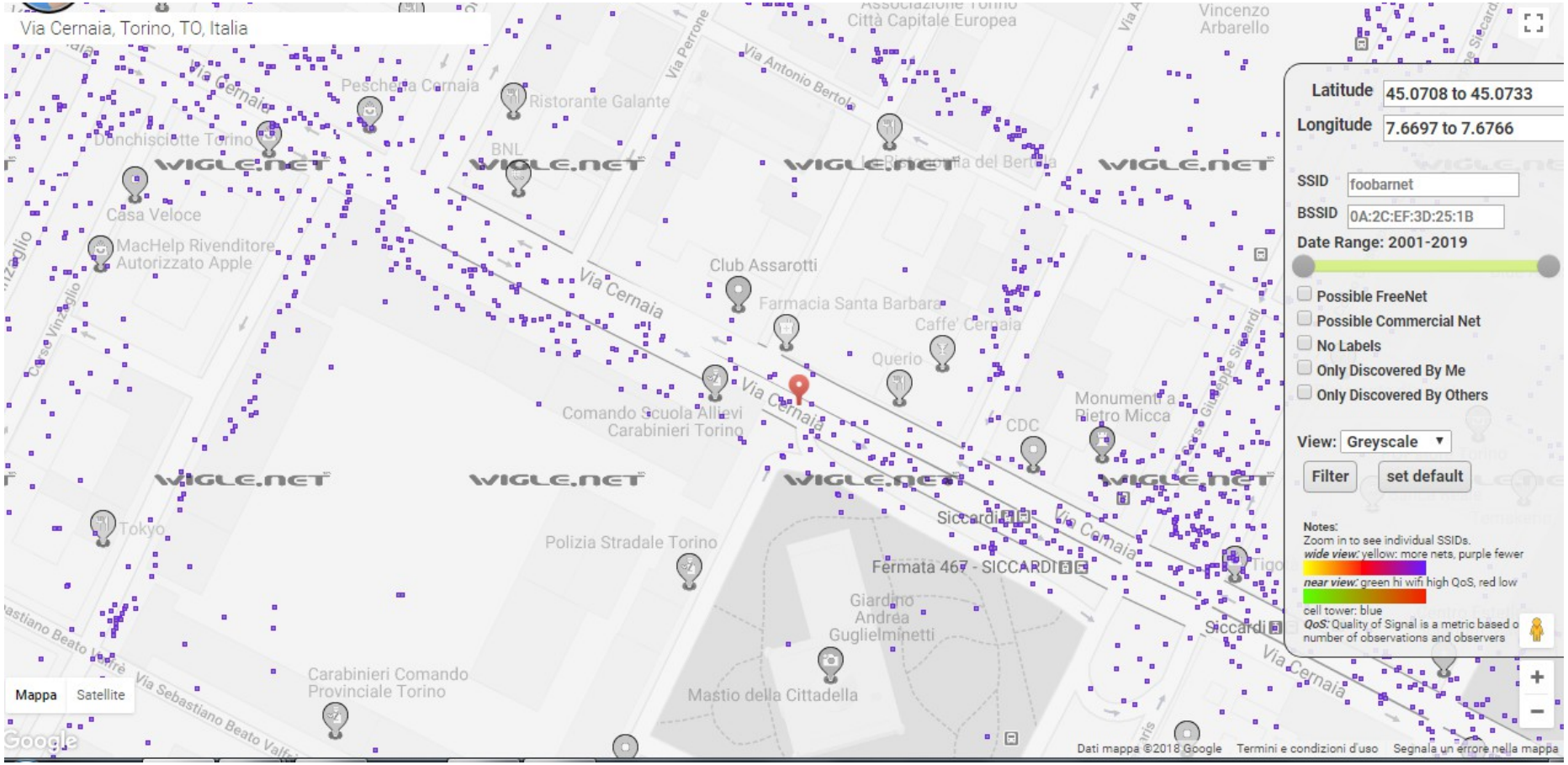
WIGLE : Conoscendo il SSID di un WiFi → localizzarlo su mappa



MAC ADDRESS : indirizzo scheda di rete, verificabile e sequestrabile (il dispositivo)

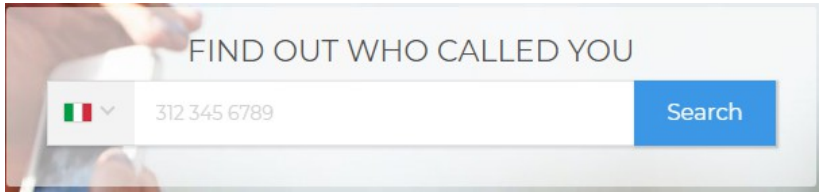
Map	Net ID	SSID	Name	Type	First Seen	Most Recently	Crypto	Est. Lat	Est. Long	Channel
map	9C:97:26:41:CF:07	Ultimo Impero		infra	2014-06-28T14:00:00.000Z	2016-09-16T00:00:00.000Z	WPA	45.04891586	7.65631676	11
map	08:6A:0A:5E:CE:7E	Ultimo Impero		infra	2017-06-14T08:00:00.000Z	2018-02-01T08:00:00.000Z	WPA	45.04895401	7.65632677	1

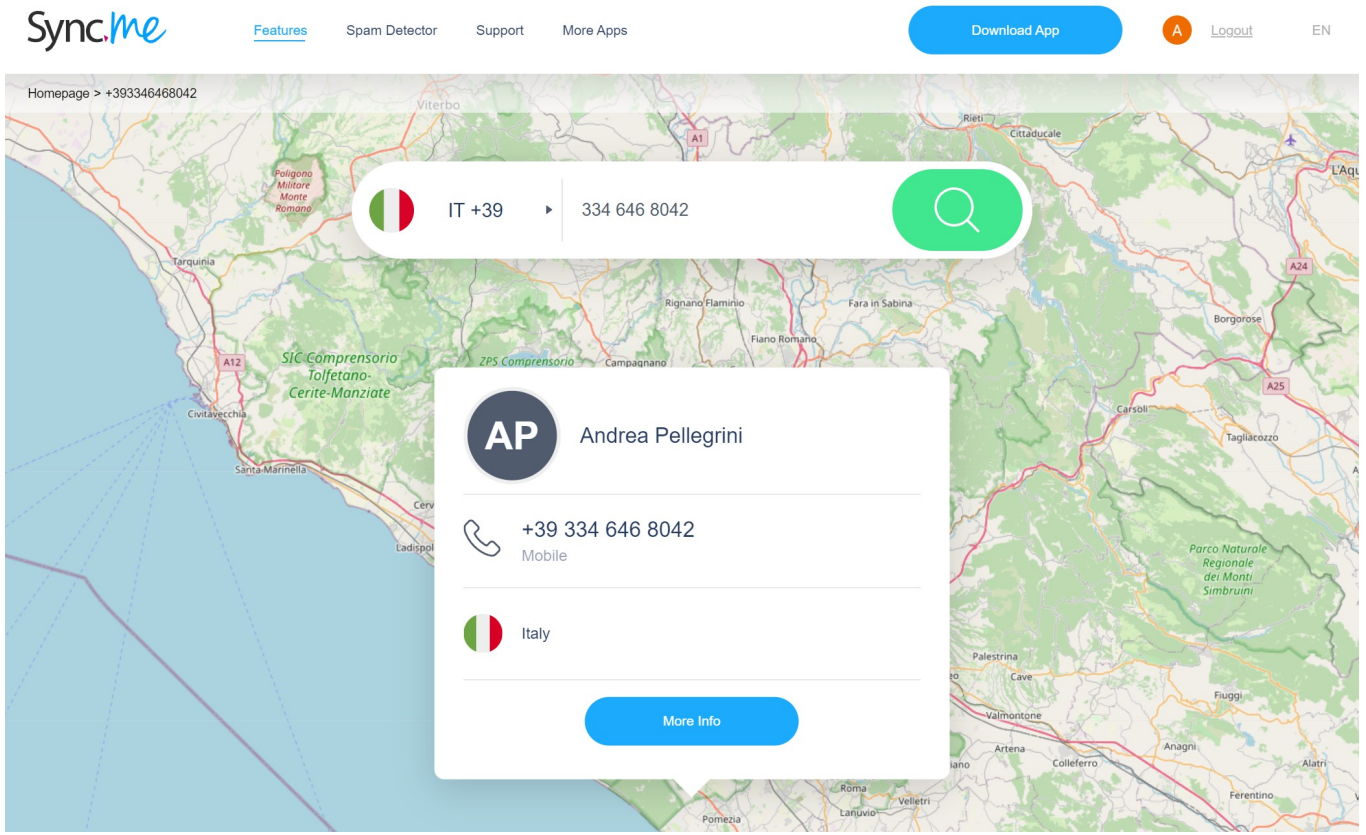
WIGLE: Navigazione su mappa



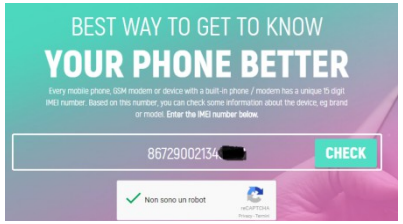
Ricerca per numero telefonico

https://sync.me



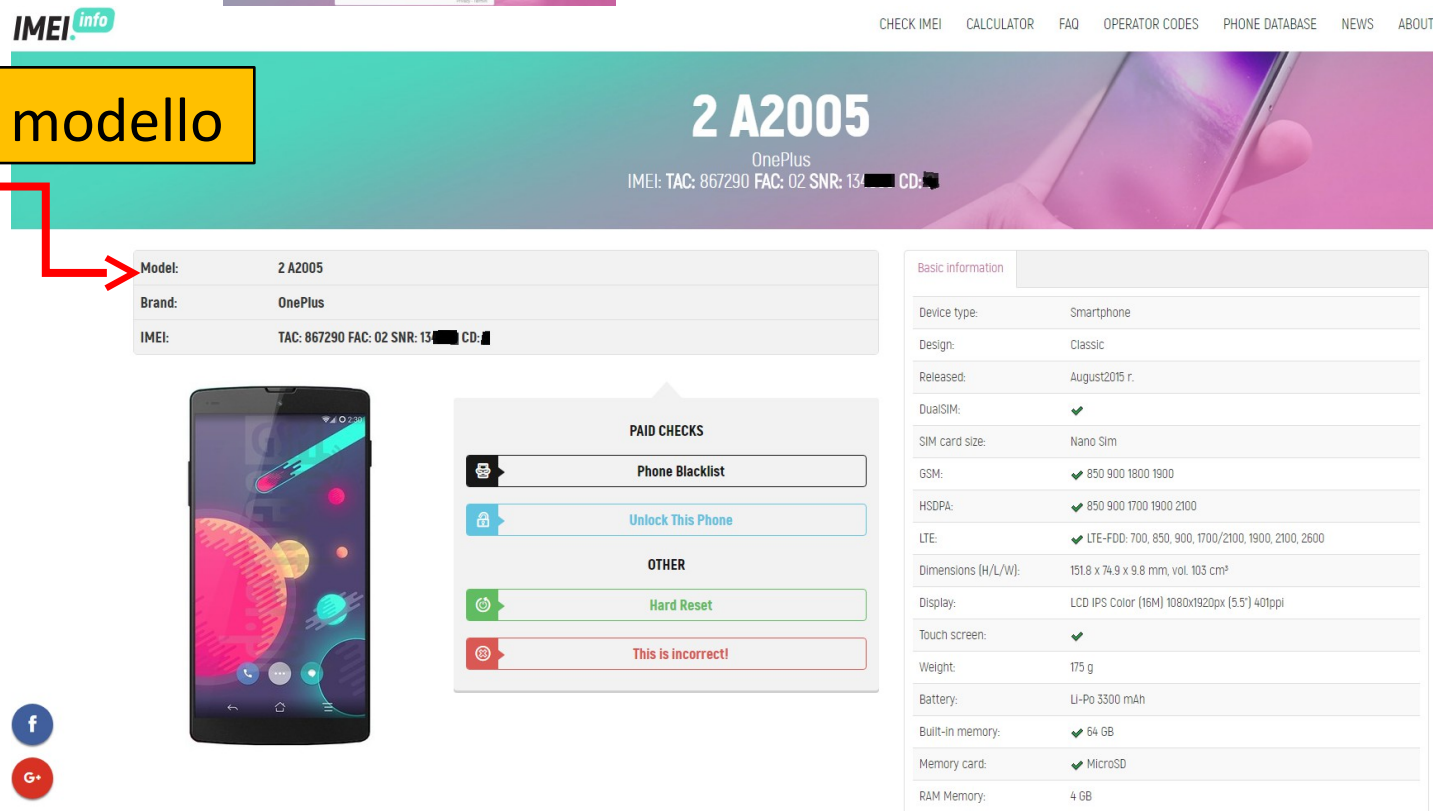


IMEI Check: quale smartphone compare nei tabulati?
Cosa cercare durante la perquisizione?



https://www.imei.info

Marca e modello



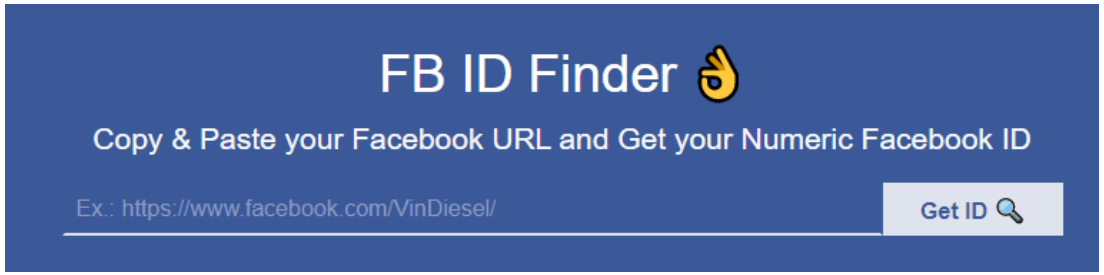
Facebook

Casella mail di registrazione

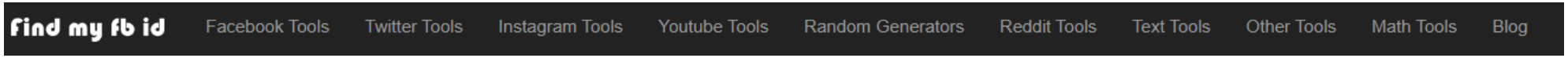
Vanity name (alfanumerico)
ID (numerico)

Questo non è un ID !!!

Servizi online per individuare ID



https://findfb.id/



https://findmyfbid.in/

ID dei profili serve per le future richieste ai portali

... Restituiscono ID anche di (alcuni) profili disattivati ...

BUON POMERIGGIO