OSINT:
tecniche investigative basate sulle fonti aperte su Internet

DFA Open Day 2014
Università degli Studi Milano
05 giugno 2014

Giuseppe Colazzo

- *Laurea specialistica in Economia e management (tesi in Internet Marketing);*
- *Perfezionato in Digital Forensics, Privacy, Cloud e Cyber Warfare;*
- *Specializzato in Computer Forensics and Data Analysis;*
- *EUCIP IT - ENCASE – UFED;*
- *Socio CLUSIT – IISFA;*
- *IT Security Manager;*
- *Componente unità computer forensics and data analysis Guardia di Finanza - Milano;*

Information gathering

raccolta di dati e informazioni non riservati e accessibili a chiunque avendo come fonte i principali social network.
L'obiettivo è quello di possedere quante più informazioni possibili da utilizzare nella fase di intelligence.

Social media information gathering

Cree.py

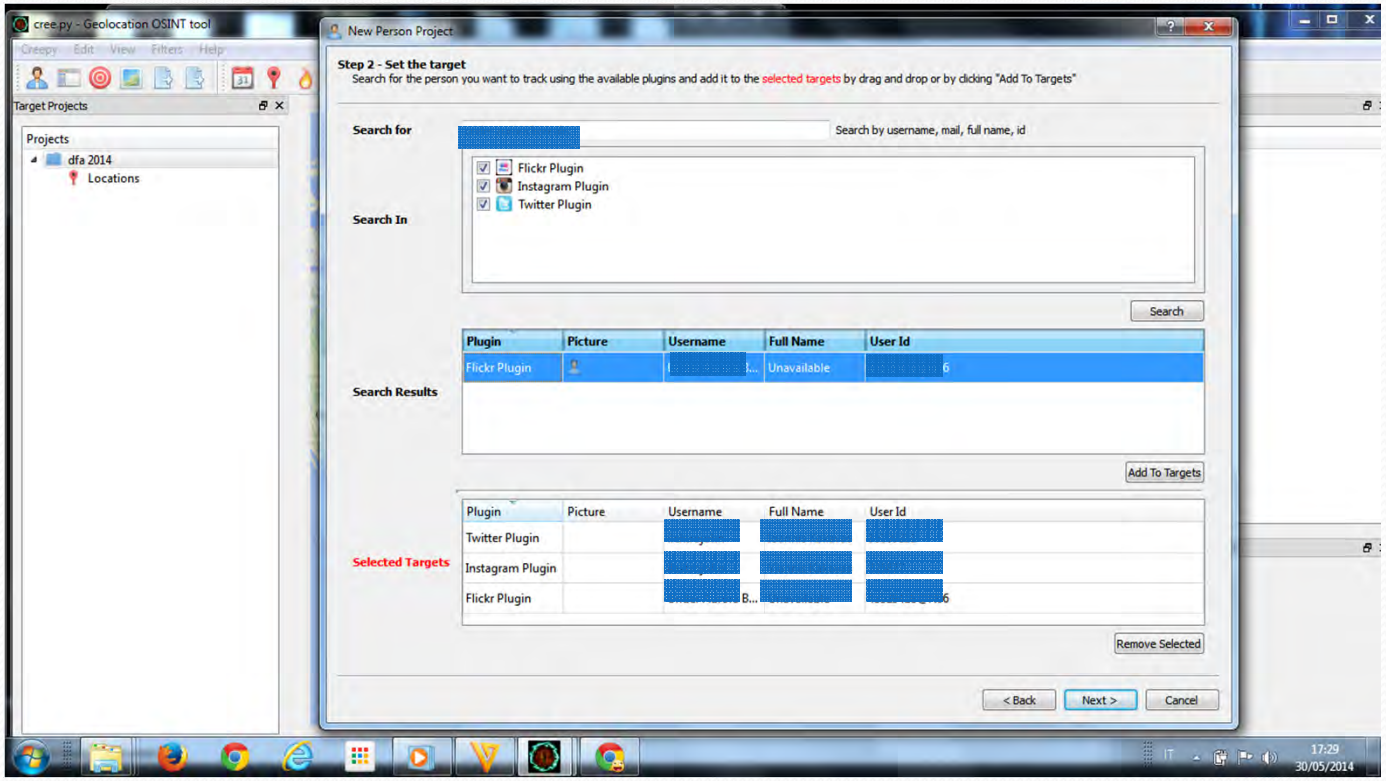
https://ilektrojohn.github.io/creepy/

tool che consente di raccogliere informazioni geolocalizzate da vari social media e esportare i risultati in formato CSV e KML (Google Maps).

Social media information gathering

Cree.py

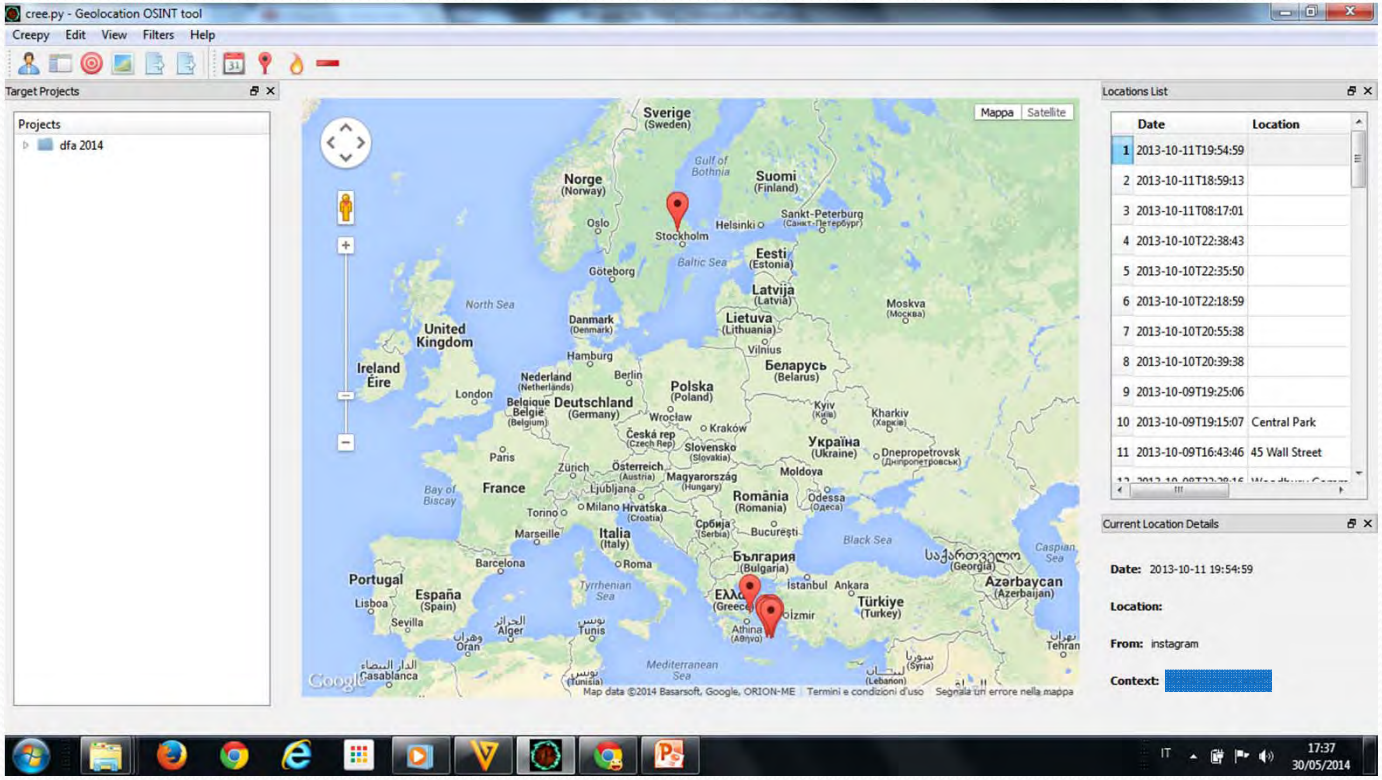
https://ilektrojohn.github.io/creepy/



Social media information gathering

Cree.py

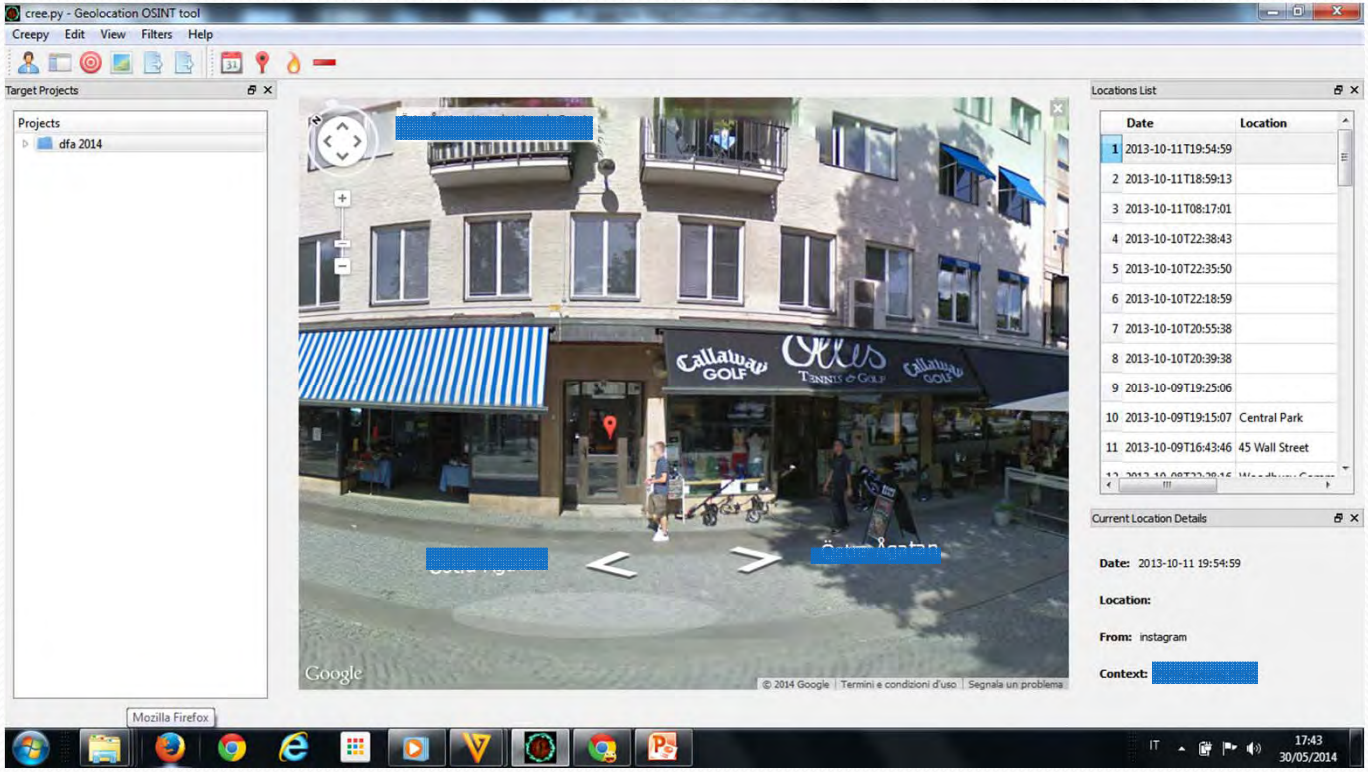
https://ilektrojohn.github.io/creepy/



Social media information gathering

Cree.py

https://ilektrojohn.github.io/creepy/



Social media information gathering

pipl

http://pipl.com

motore di ricerca specializzato nei profili personali.
Il suo algoritmo si basa sull'*identity resolution engine* che raccoglie informazioni su di un soggetto partendo da informazioni di base quali:

- città;
- Email;
- Nome e cognome;
- Nickname;
- Numero telefonico.

Social media information gathering

pipl

http://pipl.com

pipl

Search by Name, Email, Username or Phone

Location (optional)

The most comprehensive people search on the web

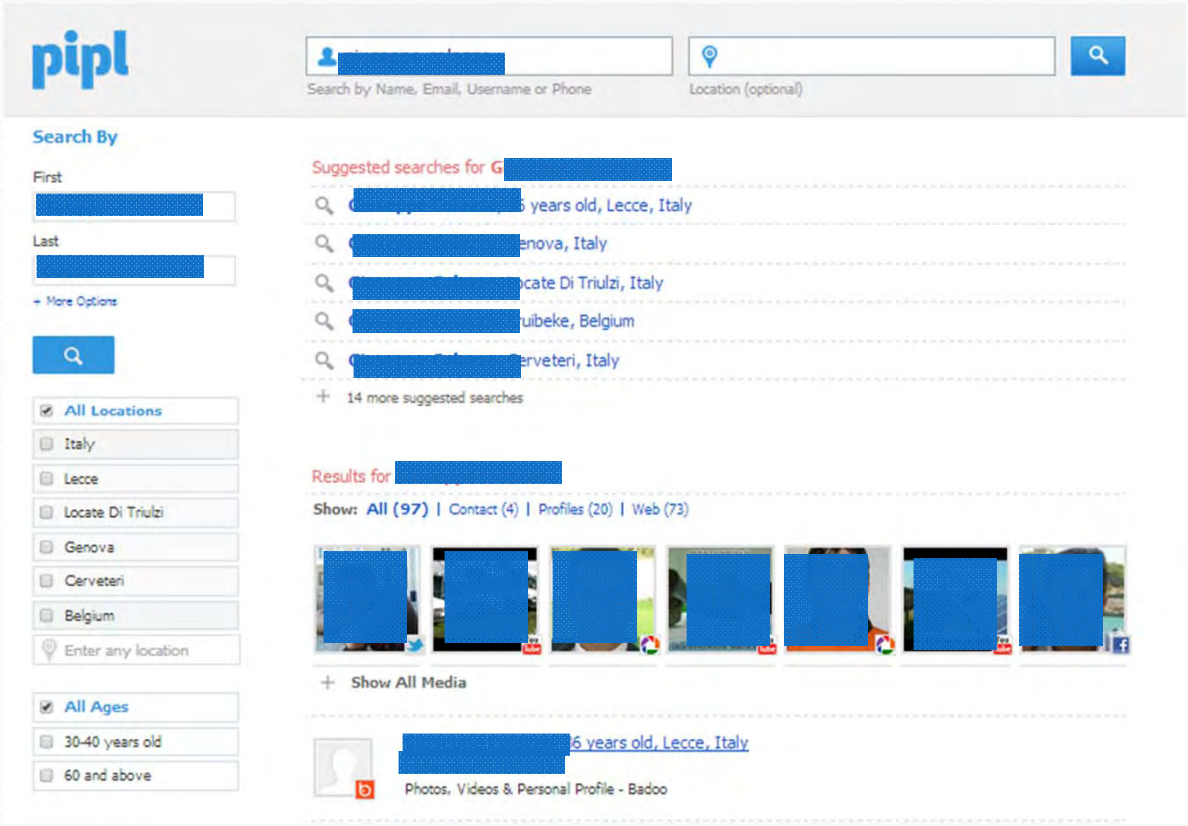
We dive into the deep web to bring you results you won't find in any other search engine then we use a powerful identity resolution engine to identify the person you are looking for.

Terms | Privacy | Directory | Developers | Help | Contact | Business Solutions | © 2006-2014 pipl

Social media information gathering

pipl

http://pipl.com



Social media information gathering

pipl

http://pipl.com

Category	Examples
Personal Profiles	facebook.com pinterest.com last.fm
Professional & Business	linkedin.com spoke.com zoominfo.com
Contact Details	whitepages.com addresses.com anywho.com
Media	picasa.com flickr.com youtube.com
Background Reports	peoplefinders.com intelius.com peoplesmart.com
Public Records	bop.gov archives.com ancestry.com
Publications	uspto.gov portal.acm.org scirus.com
School & Classmates	classmates.com reunion.com schoolbank.nl
Email Address	intelius.com spokeo.com
Web Pages	Default category, for Data-Sources that don't match any of the above categories.

le informazioni vengono categorizzate in base alla natura e alla fonte dei siti in cui vengono reperite.

Fonte: *http://dev.pipl.com/docs/read/search_api/datasources*

Social media information gathering

Social network

FACEBOOK

https://www.facebook.com/directory/people/

Sfoglia per nome

Cerca i tuoi amici per nome in ordine alfabetico. I numeri da 1 a 26 contengono nomi con caratteri non latini.
Nota: qui vengono mostrate solo le persone che vogliono apparire negli elenchi di ricerca pubblici su Facebook. Chiunque può scegliere di non apparire qui, modificando le impostazioni della Privacy delle ricerche. Puoi trovare persone usando la nostra pagina di ricerca persone.

Cerca persone | Cerca

Anne Helmond, May 2009

Persone | Pagine | Luoghi | Argomenti

Latin Character Names

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Non-Latin Character Names

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26

Risultati per A A – azusa sakata nell'elenco Persone

A A - Aamir Hayat
Aamir Hayat - Aashish Tiwari
Aashish Tiwari - Abdalh Alitiba
Abdalh Aljabry - Abdul Shameer Shameer
Abdul Shameer Shameer - Abed Al Amir Wehbe
Abed Al Amoudi - Abishek Akella
Abishek Aki - Abu Alawi
Abu Alawi - Achmad Fai Pule
Achmad Fai Uchiha - Ade Maharani
Ade Maharani - Adelmir Jose Maier

Alex Hennell - Alex Spinato
Alex Spinaze - Alexandre Moises Schuck
Alexandre Moisescot - Alexis Sanchez
Alexis Sanchez - Ali Depil
Ali Deplazes - Ali Shah
Ali Shah - Alicia Jones
Alicia Jones - Aliya S Aliyu
Aliya S Armin - Allieu Sesay
Allieu Sesay - Alvaro Carvalho Carvalho
Alvaro Carvalho Carvalho - Alyssa Vega

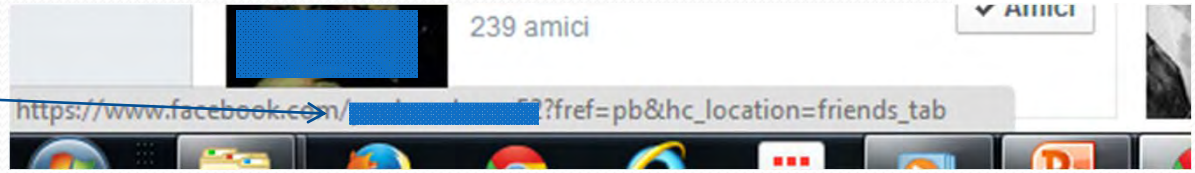
Anirudh Sehgal - Ankita Patel
Ankita Patel - Anna Eriksson
Anna Eriksson - Anna Yushifa
Anna Yushina - Ansar Ancha
Ansar Ancha - Anthony Mcchesney
Anthony Mcchrystal - Antonio Garza Gonzalez
Antonio Garza Gzz - Antony G Velasquez Medina
Antony G Zahs - Apib Kren
Apib Manzoor - Aqoe Xii Cell
Aqoe Xii Chell - Arbin Kulkarni

Social media information gathering

Social network

FACEBOOK Ricerche avanzate

nome.cognome:



per email:	*https://www.facebook.com/search/results.php?q=indirizzo@dominio.com*
foto:	*https://www.facebook.com/nome.cognome/photos*
foto in comune:	*https://www.facebook.com/nome1.cognome1/photos?and=nome2.cognome2*
amici:	*https://www.facebook.com/nome.cognome/friends*
amici in comune:	*https://www.facebook.com/nome1.cognome1/friends?and=nome2.cognome2*
altri parametri:	*about, map, sports, music, movies, tv, books, games, likes, events, groups, …*

Social media information gathering

maltego

https://www.paterva.com

potente tool di *link analysis* che consente di evidenziare le relazioni da diverse entità logiche come:

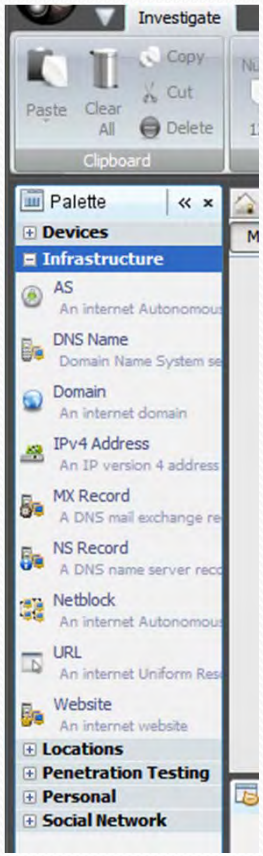
- persone;
- social networks;
- aziende e organizzazioni;
- siti web e email;
- infrastrutture di rete.

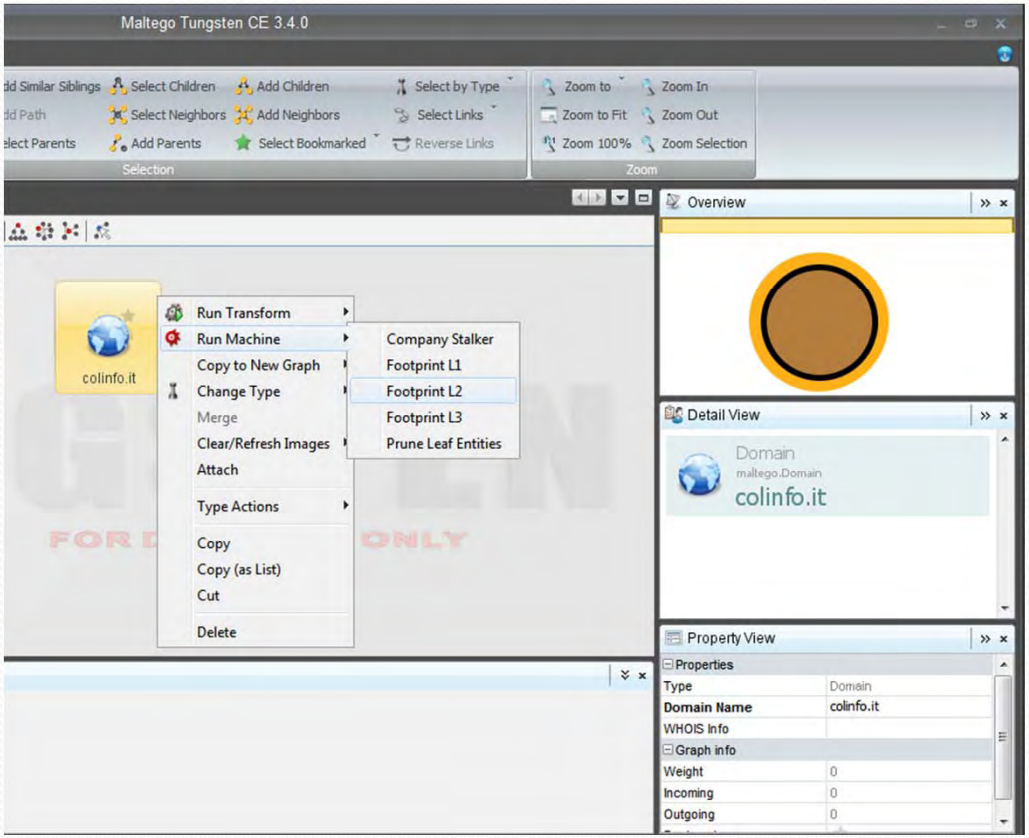
I risultati vengono visualizzati mediante una GUI avanzata che evidenzia i vari tipi di collegamento tra le entità.

Social media information gathering

maltego

https://www.paterva.com

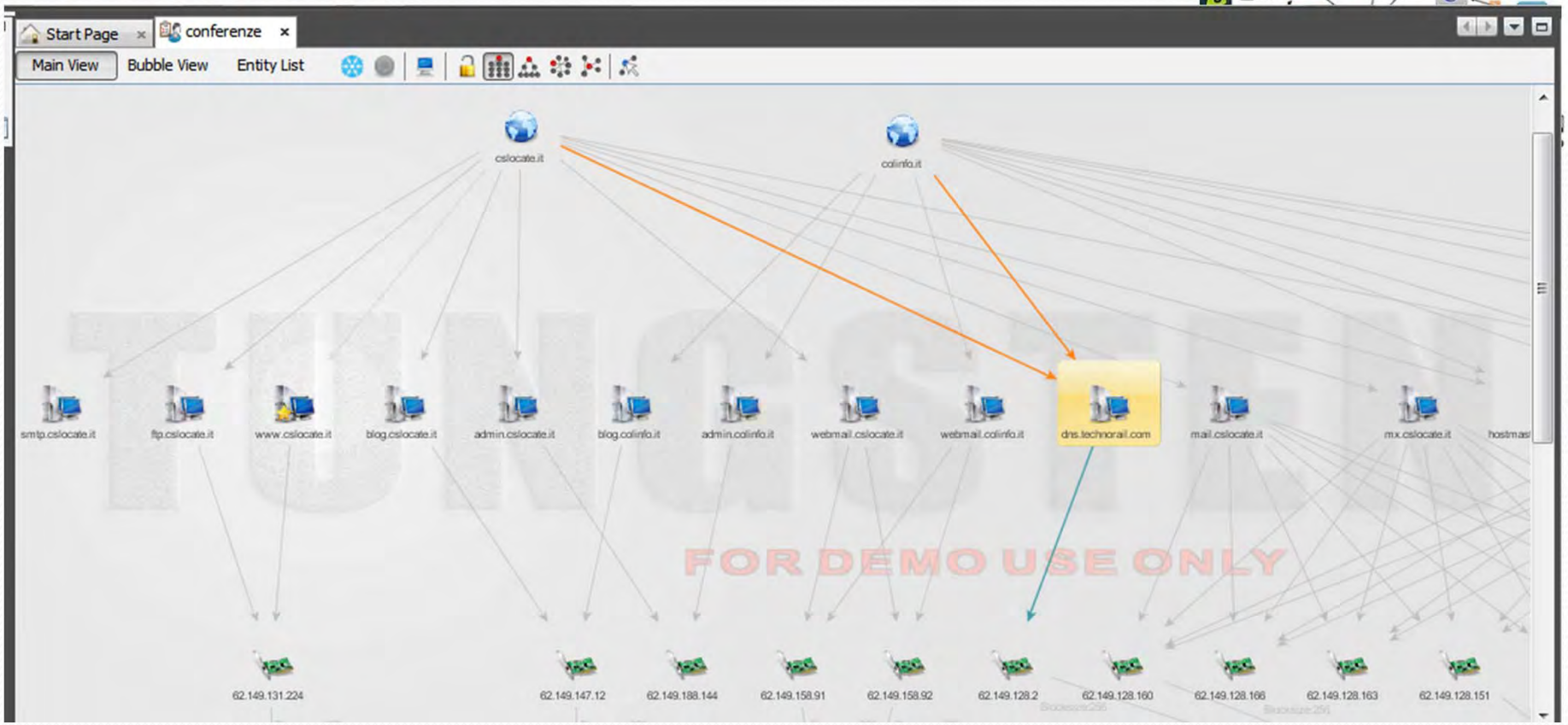




Social media information gathering

maltego

https://www.paterva.com



Geolocalizzazione

server web


www.shutterstock.com

reperire informazioni che consentano di risalire al *provider* che ospita nei propri server il nome di dominio corrispondente ad un sito web.

Geolocalizzazione

server web

tools:

www.domaintools.com
www.nic.com , www.nic.it
www.tcpiputils.com

Informazioni ottenibili:

- provider;
- IPv4 address;
- Mail server;
- DNS server;
- Registrant;
- Admin contact;
- Tecnical contact.

Domain: colinfo.it
Status: ok
Created: 2011-02-02 23:25:18
Last Update: 2014-02-18 00:44:53
Expire Date: 2015-02-02

Registrant
Name: [redacted]
Organization: [redacted]
ContactID: ARU74374R-870040
Address: [redacted]
[redacted]
MI
IT
Created: 2011-02-02 23:25:17
Last Update: 2011-02-02 23:25:17

Admin Contact
Name: [redacted]
Organization: [redacted]
ContactID: ARU74374R-870040
Address: [redacted]
[redacted]
MI
IT
Created: 2011-02-02 23:25:17
Last Update: 2011-02-02 23:25:17

Technical Contacts
Name: [redacted]
Organization: [redacted]
ContactID: ARU74374R-870040
Address: [redacted]
[redacted]
MI
IT
Created: 2011-02-02 23:25:17
Last Update: 2011-02-02 23:25:17

Registrar
Organization: Aruba s.p.a.
Name: ARUBA-REG
Web: http://www.aruba.it

Network information

DNS server (NS records)	dns.technorail.com (62.149.128.2) dns2.technorail.com (62.149.132.2) dns3.arubadns.net (95.110.220.5) dns4.arubadns.cz (81.2.199.73)
Mail server (MX records)	mx.colinfo.it
IP address (IPv4)	62.149.128.160 62.149.128.163 62.149.128.151 62.149.128.74 62.149.128.157 62.149.128.166 62.149.128.154 62.149.128.72
IP address (IPv6)	
ASN number	31034
ASN name (ISP)	Aruba S.p.A.
IP-range/subnet	62.149.128.0/19 62.149.128.0 - 62.149.159.255
Network tools (IPv4)	Ping 62.149.128.160 Traceroute 62.149.128.160

Geolocalizzazione

e-mail

posizione geografica del client mail dal quale vengono inviate le mail.

dettagli mail →

www.shutterstock.com

Delivered-To: [redacted] Received: by 10.182.158.230 with SMTP id wx6csp2990260bb; Wed, 28 May 2014 10:44:27 -0700 (PDT) X-Received: by 10.194.184.179 with SMTP id ev19mr1323464wjc.85.1401299066651; Wed, 28 May 2014 10:44:26 -0700 (PDT) Return-Path: <[redacted]@tin.it> Received: from smtp2web.tin.it (smtp2web.tin.it. [212.216.176.236]) by mx.google.com with ESMTP id lb4si33621125wjb.84.2014.05.28.10.44.26 for <[redacted]>; Wed, 28 May 2014 10:44:26 -0700 (PDT) Received-SPF: none (google.com: [redacted]@tin.it does not designate permitted sender hosts) client-ip=212.216.176.236; Authentication-Results: mx.google.com; spf=neutral (google.com: [redacted]@tin.it does not designate permitted sender hosts) smtp.mail=[redacted]@tin.it Received: from feu8 (10.192.64.18) by smtp2web.tin.it (8.6.060.28) id 5319830E0162C903 for [redacted]; Wed, 28 May 2014 19:44:26 +0200 **Received: from (93.33.240.153) by webmailvtin.alice.it; Wed, 28 May 2014 19:44:26 +0200**
Message-ID: <14643eeddoa.[redacted]@tin.it>

Received: from (**93.33.240.153**) by webmailvtin.alice.it; Wed, 28 May 2014 19:44:26 +0200

IP address	93.33.240.153
Reverse DNS (PTR record)	93-33-240-153.ip46.fastwebnet.it
DNS server (NS record)	dns2.fastweb.it (213.140.2.21) dns1.fastweb.it (213.140.2.12)

Geolocalizzazione

e-mail

webtool:

www.ip-adress.com/trace_email

www.shutterstock.com

To trace an email using a header, copy and paste the email header below:

```
Delivered-To: [redacted]
Received: by 10.182.158.230 with SMTP id wx6csp299026obb;
        Wed, 28 May 2014 10:44:27 -0700 (PDT)
X-Received: by 10.194.184.179 with SMTP id ev19mr1323464wjc.85.1401299066651;
        Wed, 28 May 2014 10:44:26 -0700 (PDT)
Return-Path: <[redacted]n.it>
Received: from smtp2web.tin.it (smtp2web.tin.it. [212.216.176.236])
        by mx.google.com with ESMTP id lb4si33621125wjb.84.2014.05.28.10.44.26
```

Trace Email Sender | Clear

Geolocalizzazione

e-mail

webtool:

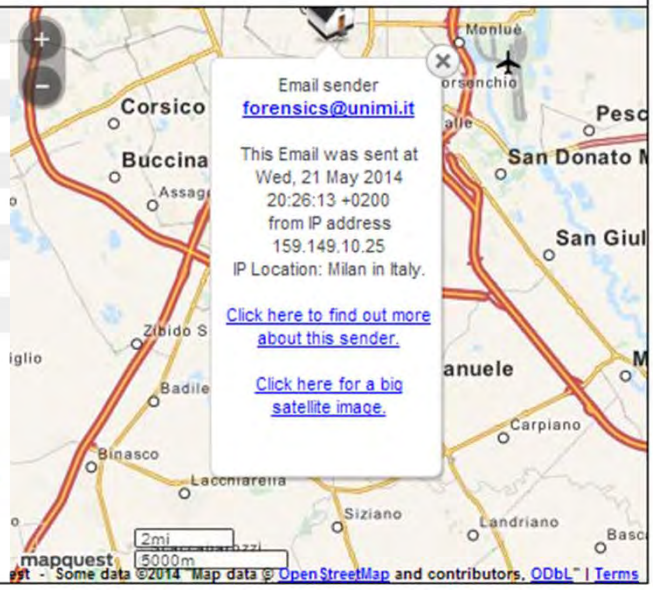
www.ip-adress.com/trace_email

www.shutterstock.com

At Wed, 21 May 2014 20:26:13 +0200, the email sender forensics@unimi.it sent you an email from the IP address **159.149.10.25** located in **Italy, Milan**.

Email Sender:	forensics@unimi.it [more info]
IP address:	159.149.10.25
IP address country:	Italy
IP address state:	Umbria
IP address city:	Milan
IP address latitude:	45.4667
IP address longitude:	9.2000
ISP of this IP:	Universita' di Milano
Organization:	Universita' di Milano
Local Time of this IP country:	2014-05-28 20:57

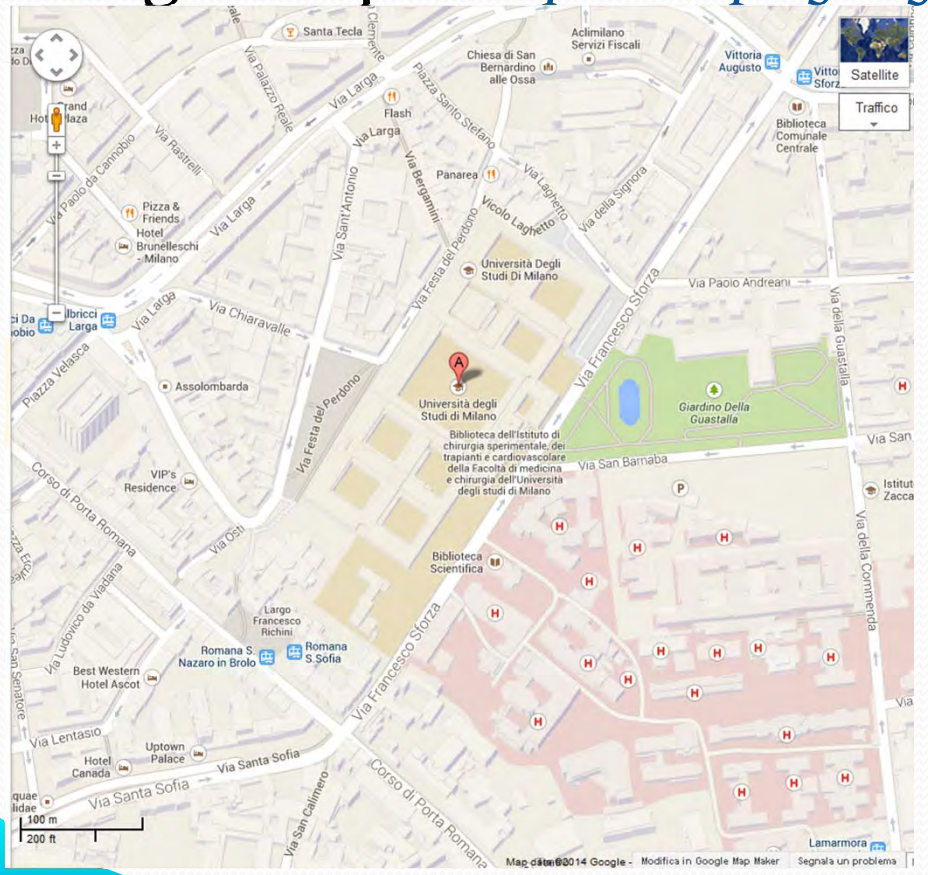
Find out anything about the owner of forensics@unimi.it including address, age and more. Click here.



Geolocalizzazione

coordinate geografiche

Google Maps: *http://maps.google.it*



www.shutterstock.com

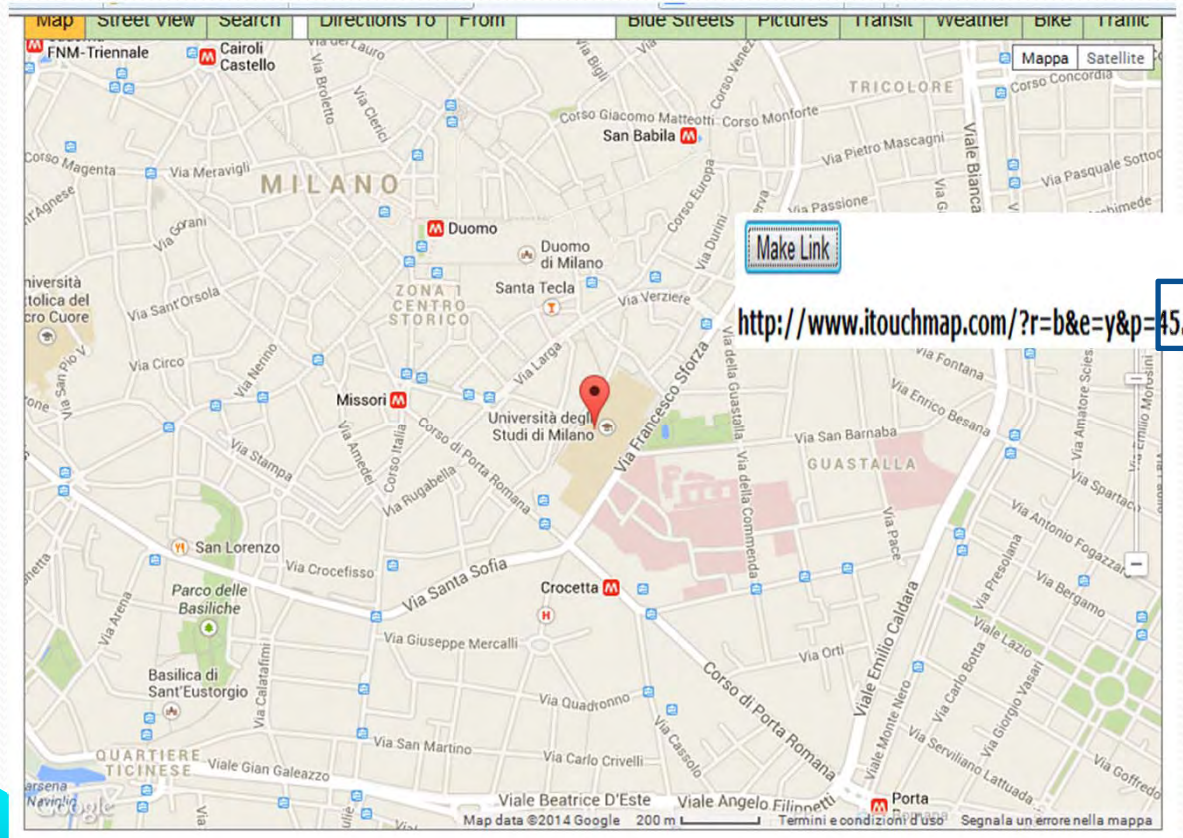
https://maps.google.it/maps?saddr=Universit%C3%A0+degli+Studi+di+Milano,+Via+Festa+del+Perdono,+7,+20122+Milano&hl=it&ie=UTF8&sll=**45.459763,9.194705**&sspn=0.006397,0.009602&geocode=CdVHm-db2V5AFbCqtQIdWEyMACnZdeYtpsaGRzFzj4VyX5D2HQ&mra=mift&t=m&z=17

Geolocalizzazione

coordinate geografiche

iTouchMap: *http://www.itouchmap.com*

www.shutterstock.com



Make Link

http://www.itouchmap.com/?r=b&e=y&p=45.459975,9.19412:0:0 Via Festa del Perdono, 7, 20122 Milano, Italia

Social network


www.shutterstock.com

I più diffusi social network mettono a disposizioni dei tool integrati che restituiscono la posizione degli utenti e/o consentono di effettuare ricerche in base al luogo geografico.
I parametri di ricerca possono includere anche le coordinate geografiche.

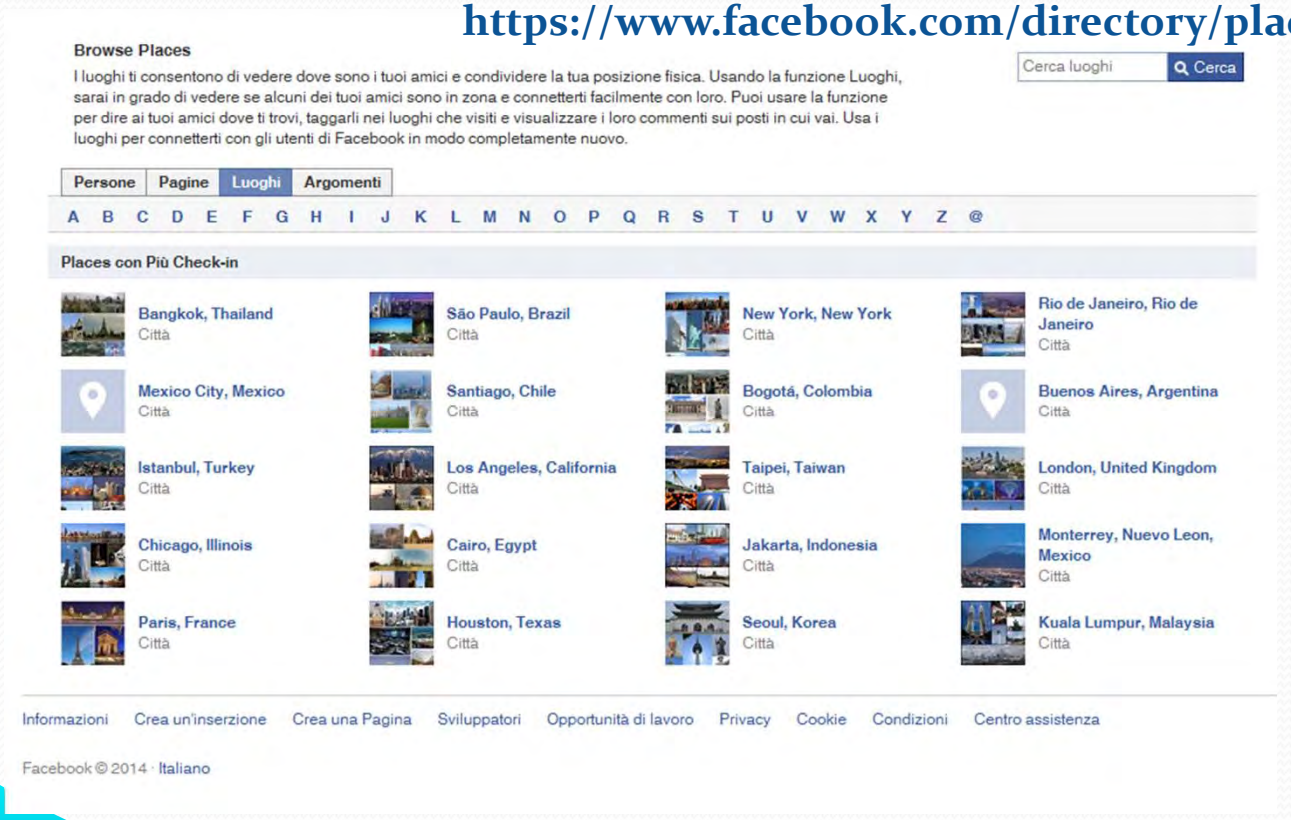
Geolocalizzazione

Social network

FACEBOOK

https://www.facebook.com/directory/places/

www.shutterstock.com

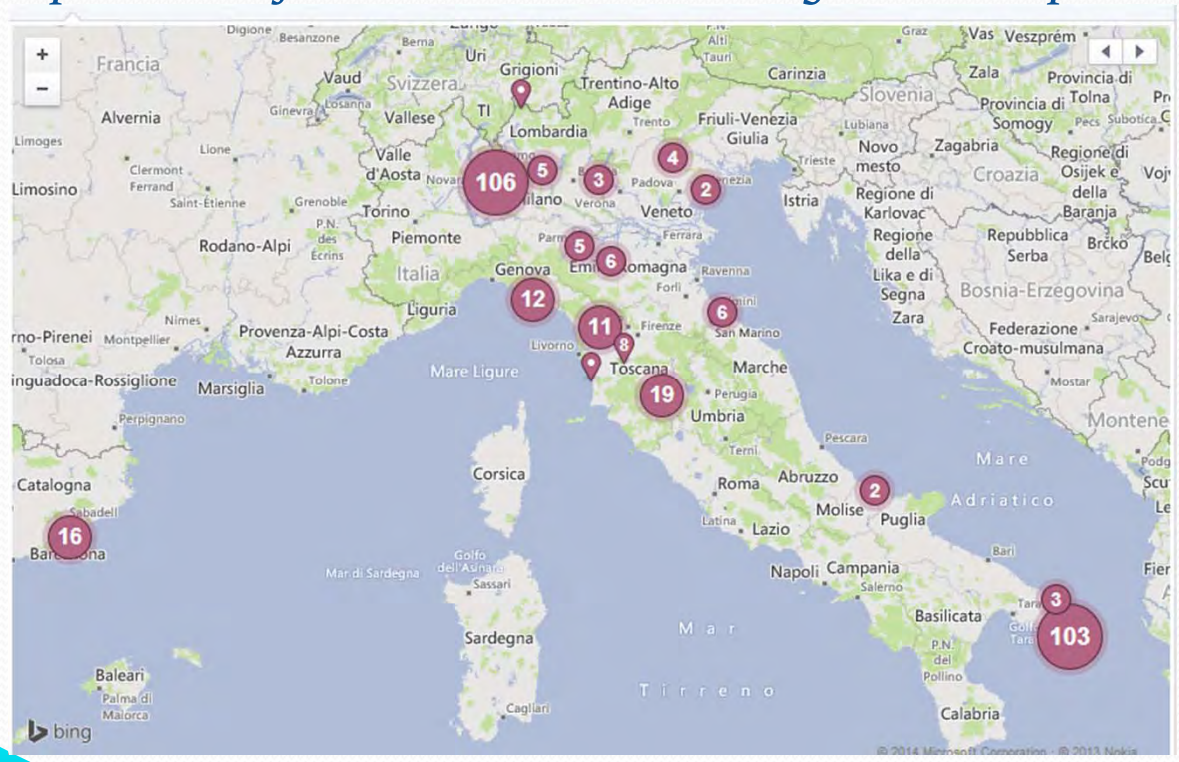


Geolocalizzazione

Social network

FACEBOOK

https://www.facebook.com/nome.cognome/map

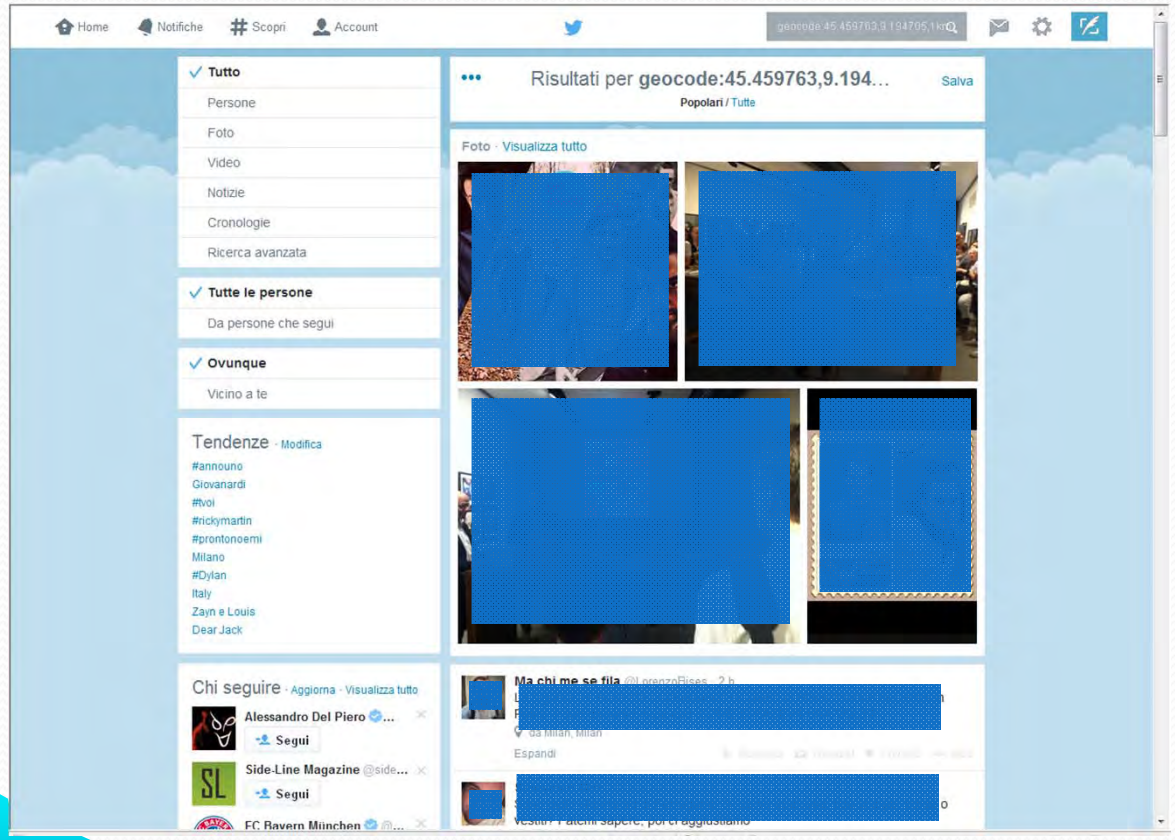


www.shutterstock.com

Geolocalizzazione

Social network

TWITTER



www.shutterstock.com

geocode:45.459763,9.194705,1km

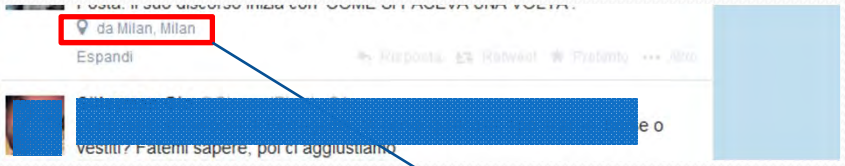
Geolocalizzazione

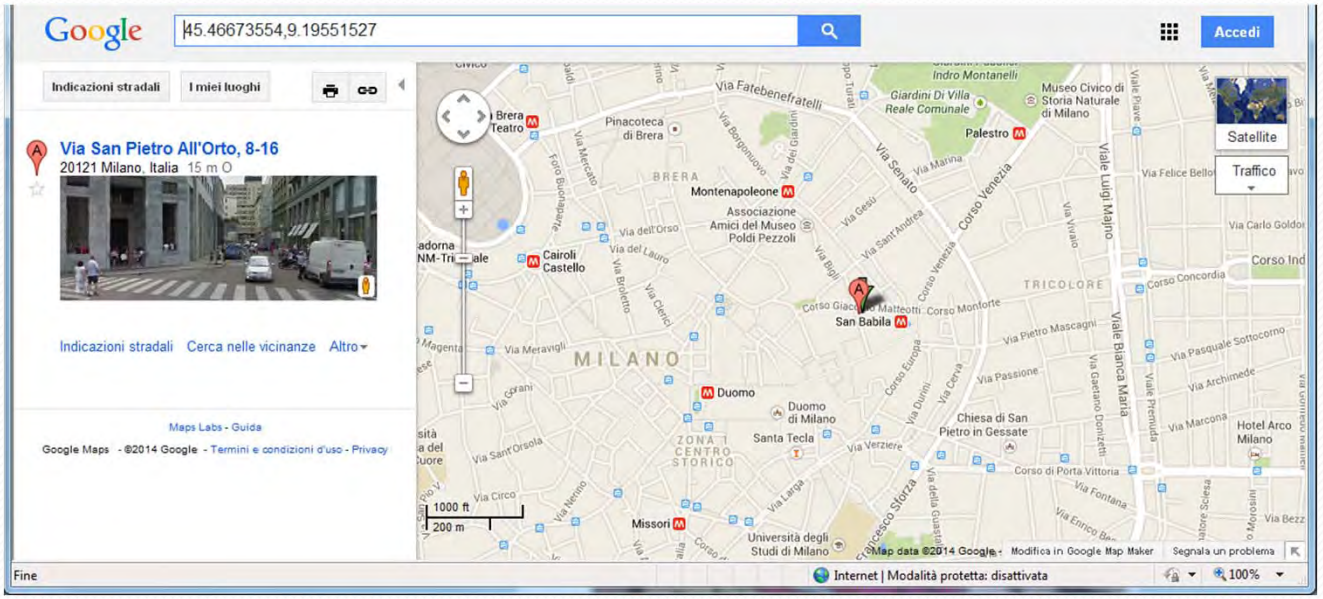
Social network

TWITTER

geocode:45.459763,9.194705,1km

www.shutterstock.com

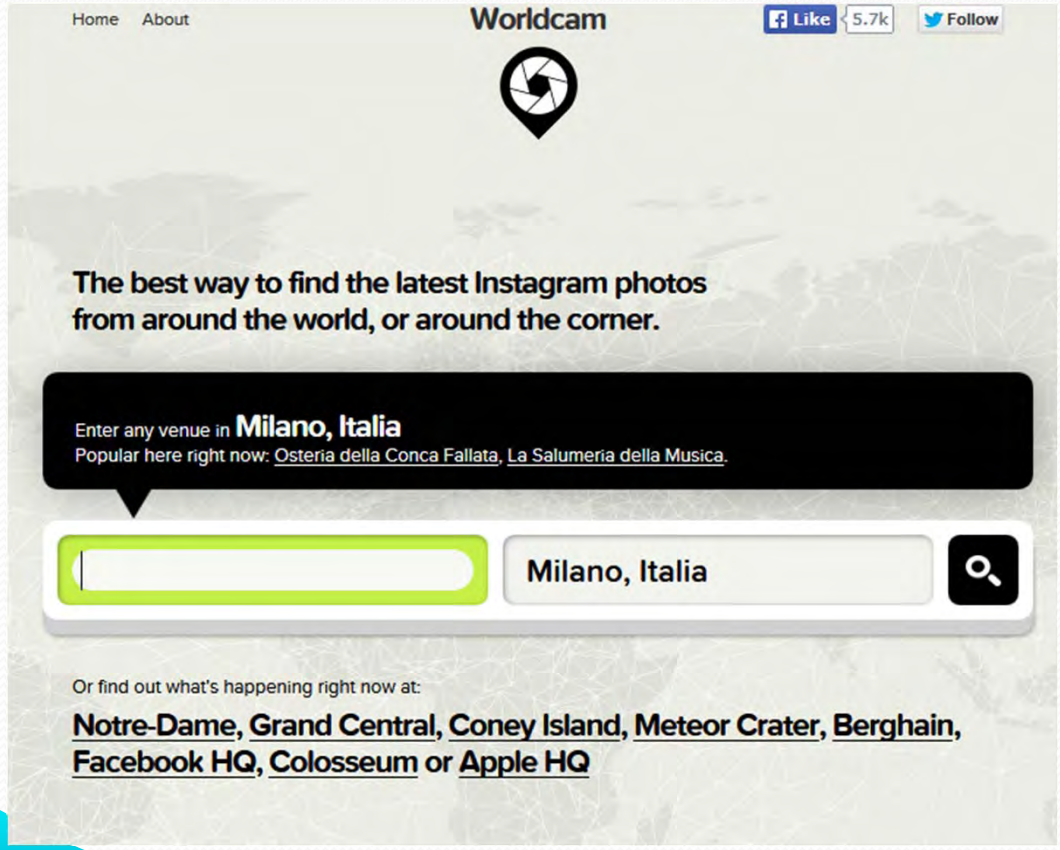




Geolocalizzazione

Social network

INSTAGRAM: *http://worldc.am*



www.shutterstock.com

Geolocalizzazione

immagini

Dati EXIF


www.shutterstock.com

I dispositivi fotografici di ultima generazione (tra cui smartphone) sono dotati di GPS che consentono di aggiungere i dati geo referenziali alle immagini acquisite (latitudine e longitudine).

Geolocalizzazione

immagini

Dati EXIF


www.shutterstock.com

Alcuni tools permettono di estrarre queste informazioni e di rappresentarle su mappe (Google Maps):

- *EXIF Viewer per Google Chrome*
- *Fastone;*
- *Exif-Viewer.*
- *www.regex.info/exif.cgi*

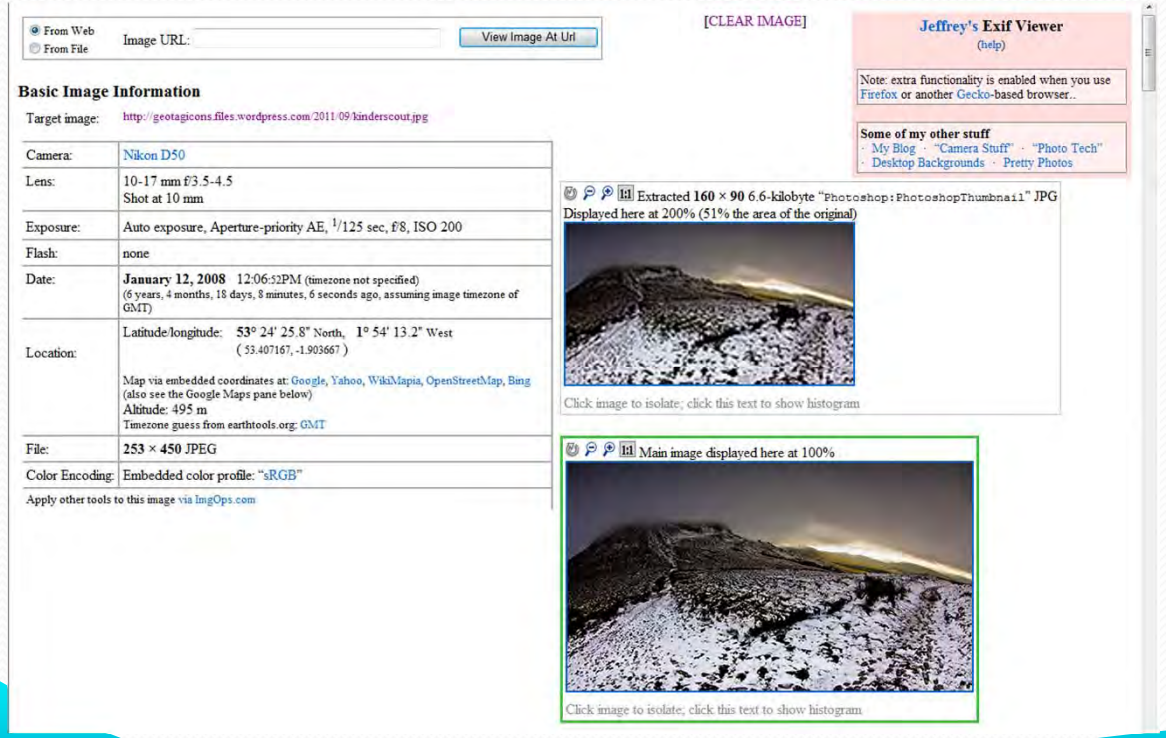
Geolocalizzazione

immagini

Dati EXIF

www.regex.info/exif.cgi

www.shutterstock.com



Geolocalizzazione

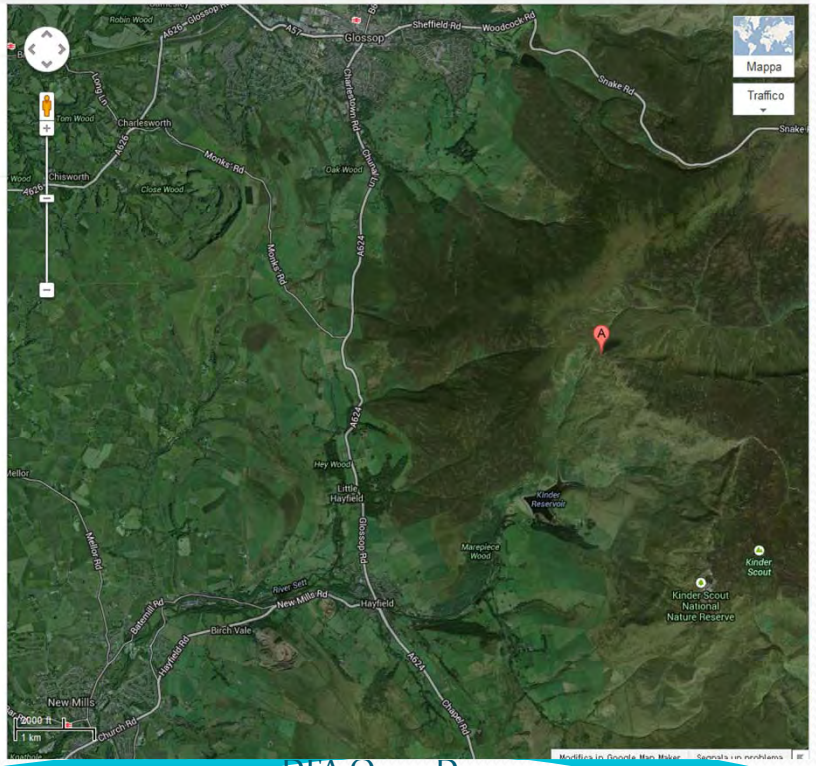
immagini

Dati EXIF

www.regex.info/exif.cgi

	GMT)
Location:	Latitude/longitude: 53° 24' 25.8" North, 1° 54' 13.2" West (53.407167, -1.903667) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 495 m Timezone guess from earthtools.org: GMT

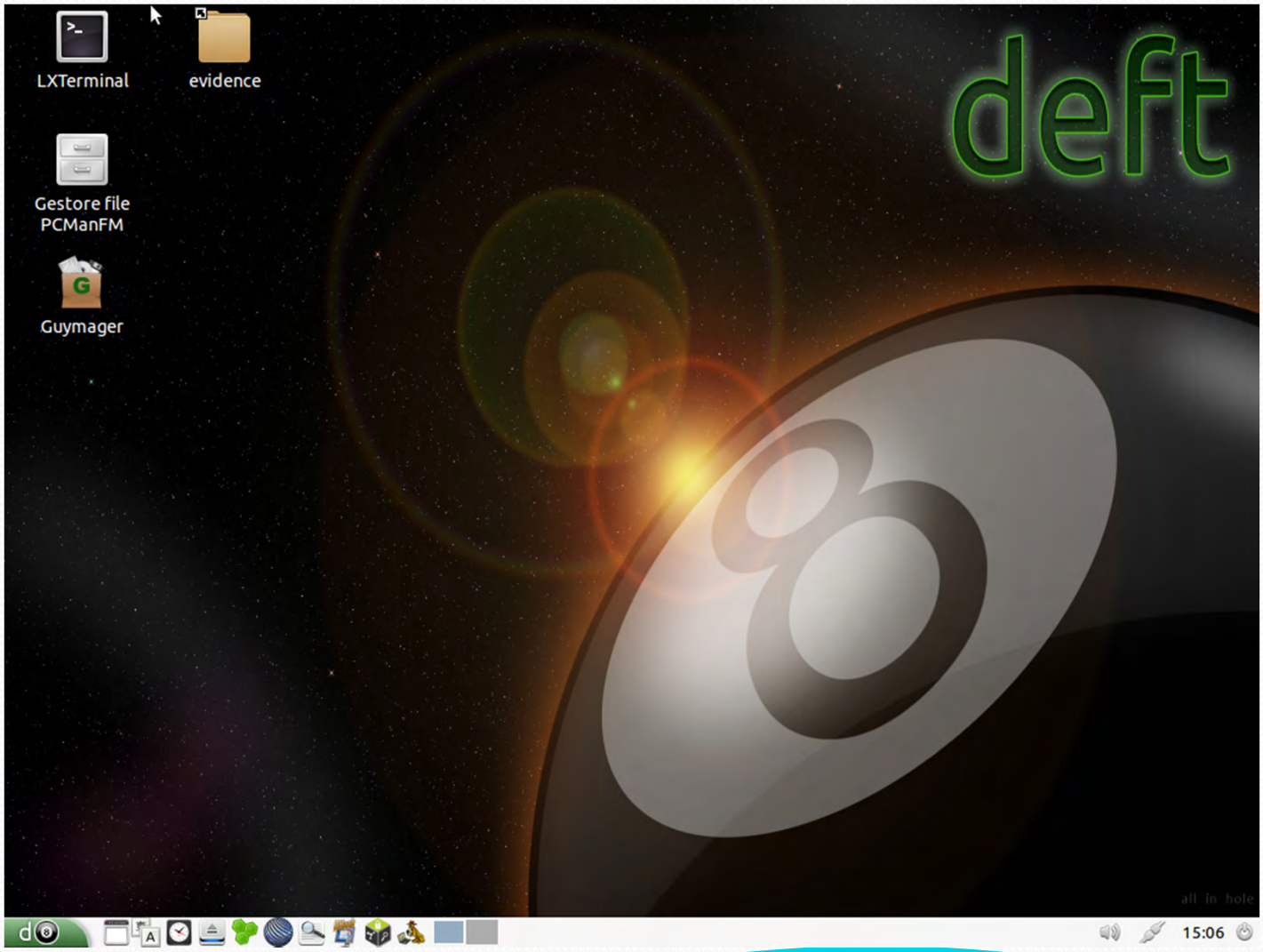
www.shutterstock.com



Forensics toolkit

Deft 8.1

http://www.deftlinux.net



Forensics toolkit

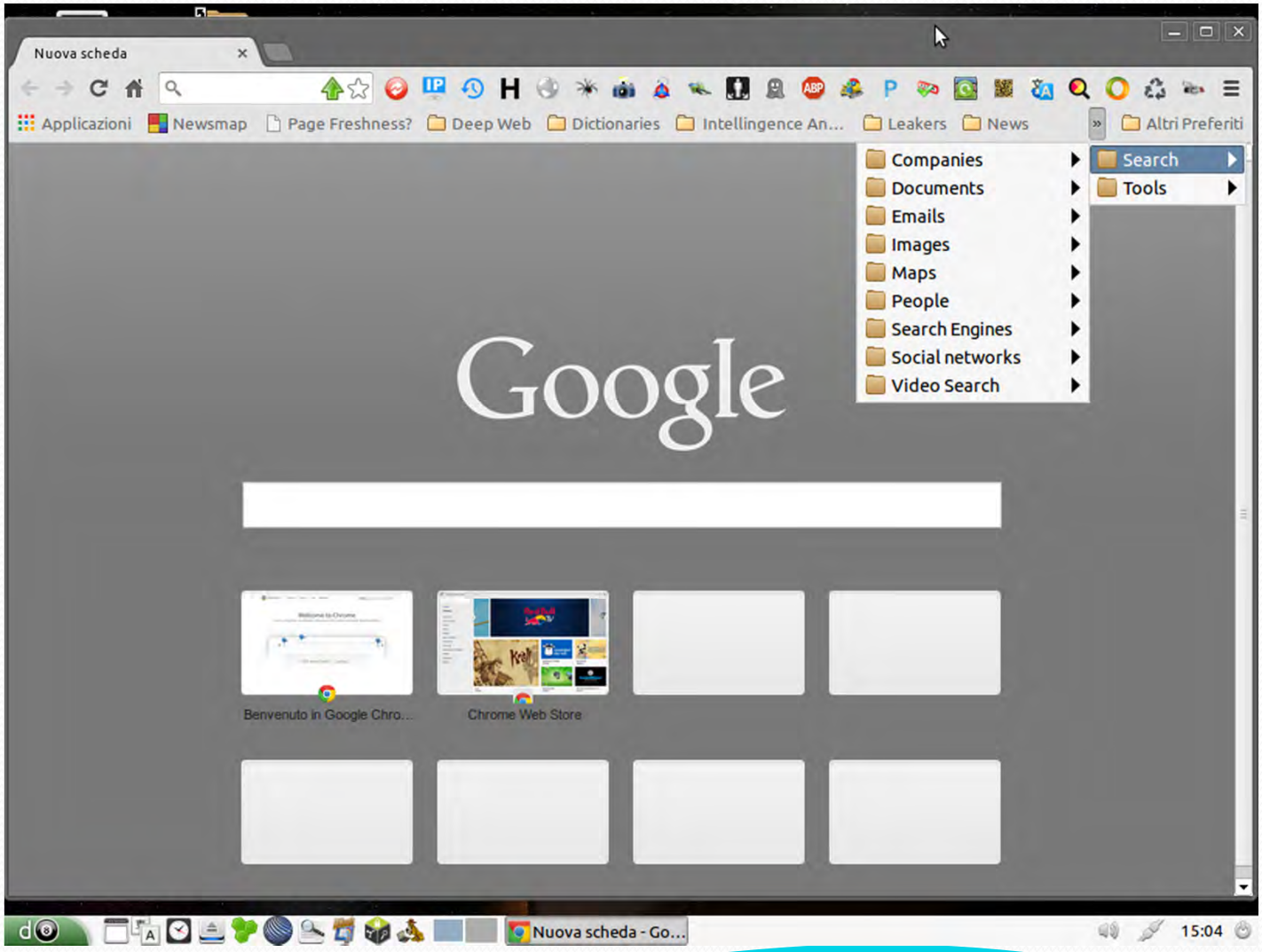
Deft 8.1

http://www.deftlinux.net

Forensics toolkit

Deft 8.1

http://www.deftlinux.net



OSINT…

Giuseppe Colazzo

khcola@gmail.com

www.linkedin.it/in/colazzog

Grazie per l'attenzione…