Osint ad Ente di certificazione, Elti

1) Google hacking o Google dork

Query intitle: Elti = Con questa ricerca avanzata di Google ho ottenuto tutti gli HTML, cioè le pagine web, nei quali è presente il nome dell'azienda che ho scelto come target. I primi risultati erano strettamente collegati con Il target.

- **Url sito principale https://www.elti.com**, nel quale si trovano le informazioni fondamentali.

Si tratta del 1 °organismo notificato in Italia che, autorizzato dal Mimit e accreditata da ACCREDIA, dal 1997 opera nel settori delle certificazioni aziendali e professionali, delle verifiche periodiche e della marcatura CE per ascensori.

Queste sono alcune delle **informazioni** contenute nella home del sito:

E.L.T.I. Srl

Organismo Notificato CE 0860

Via Angelo Bargoni, 8 00153 - Roma
+39 06 5833 4362
+39 06 5834 5440
eltisrl@tin.it
eltisrl@**legalmail**.it
P.IVA - C.F. 05384711007

Questi invece sono i **13 servizi**, e quindi i dipartimenti, della Elti:
1) Certificazione Ascensori
2) Verifica Impianti Elettrici
3) Verifica Attrezzature di Lavoro
4) Verifiche Porte e Cancelli Automatici
5) Ispezione Linee Vita
6) Verifica Impianti Fotovoltaici
7) Verifica Acque Potabili
8) Certificazione Energetica (APE)
9) Certificazione Figure Professionali
10) Certificazione Aziendale
11) Dipartimento Imprese
12) Audit on the Supply chain
13) Servizio Personalizzato.

- **Profilo Linkedin Ente**: https://www.linkedin.com/company/eltisrl/?originalSubdomain=it
- **Profilo Fb Ente**: https://www.facebook.com/elti.certificazioni/

- **Alcuni dei Clienti**: Atac, Poste italiane, Bnp Paribas, Inps, Sapienza, Acea, Ansa, Enpam, Aeroporti di Roma, Alenia spazio, Siae, Ministero dell'Interno, Banca d'Italia, Presidenza della Repubblica Italiana.

- **Clienti privati**: tra i quali hanno anche un enorme numero di Amministratori condominiali

Tramite ***Whois*** e **tecniche di Google Dork** ho trovato informazioni sulle **persone legate alla società:**

- **Legale rappresentante**: **Luigi Clementi** che è un Ingegnere civile laureato alla Sapienza di Roma (trovato in Whois, poi cercato sui social e con Google advanced resource). Vive a Frascati, è sposato e ha due figli, Luigi e Enrico Clementi.
  Profilo Fb personale: https://www.facebook.com/eugenio.clementi

- **Dipendente:** Susanna Morelli
  Profilo Fb personale: https://www.facebook.com/susanna.morelli.7

- **Dipendenti fornito dalla Adecco Spa:** esempio Tiziana Carone
  profilo Fb personale https://www.facebook.com/tiziana.castellani.1?locale=it_IT

Utilizzando ***Google advanced research*** ho ottenuto informazioni aggiuntive:

- **Nome completo**: E.L.T.I. S.R.L. (European Lift Testing Italia)
- **Codice ATECO**: 71.20.21
- **Data di costituzione:** 02 Febbraio 1998
- **Numero dipendenti:** 10-24 (Sul Fb della Elti risultano 11-50)
- **Fatturato 2022:** € 10.059.457
- **Utile/perdita 2022:** € 441.550

2) **IP dell' Url dell'hostname "www.elti.it":** 81.88.52.53 (ottenuto con il comando ping www.elti.it)

3) **WHOIS:** per ottenere informazioni sulla registrazione del dominio associato a quell'indirizzo IP.

- **Dominio:** elti.it è stato registrato dalla **Elti Srl (Organizzazione registrante),** il **26 gennaio 2015** alle **ore 16:48:02 (Created).** Il dominio scadrà **l'8 aprile 2024 (Expire date).** Lo **status** del dominio è **"Ok",** cioè attivo e registrato correttamente**.** La Elti Srl ha **sede** a **Roma**, in via Angelo Bargoni, 8**.**

- **Admin** del dominio: è **Luigi Clementi** che ha l'address nella stessa sede della Elti.
- **Contatto tecnico**: Antonio Cocumella, il cui Address è in via Cocumella, 1, Sant'Agnello, 80065 (Na)

- **Registrar:** è la **Register S.p.a.,** il provider che ha fornito alla Elti il servizio di registrazione del dominio. E' un azienda privata che gestisce la compravendita di domini per conto dei registranti, in questo caso Elti, interfacciandosi con il Registry (in Italia, CNR PISA, divisione NIC). In sintesi, ha consentito ad Elti di impostare il proprio dominio sul web.

4) **SHODAN:** Inserendo l'indirizzo IP 81.88.52.53 ho trovato informazioni relative al sito www.elti.it

- **Hostnames:** racingforce.com, www.racingforce.com, racingforcegroup.com, www.racingforcegroup.com, lhcp3053.webapps.net

- **Domains:** racingforce.com, racingforcegroup.com, webapps.net

- **ISP: Hosting provider, provider di servizi Internet**. La Register offre anche il servizio di hosting, con il quale ha consentito alla Elti di vedersi assegnato, su un Web server di Register stesso, uno spazio per ospitare la pagina principale del sito web, rendendolo accessibile agli utenti tramite connessione Internet.
- Poiché gli hostnames non erano correlati alla Elti.it, ho approfondito le ricerche scoprendo che Shodan ha scansionato **il Server Web Multitenant** che ospita più siti web di società diverse su uno stesso indirizzo IP, sfruttando il **virtual hosting.**

- **ASN** AS39729 : è il numero di sistema autonomo del Provider, ovvero è il numero univoco che identifica sulla rete Internet il sistema autonomo "Register.it", che è il dominio di **Register S.p.a.**

- **Web Technologies:** si tratta delle tecnologie specifiche usate nella pagina principale del sito web della Elti, tra le quali:

- **CMS: WordPress** è una piattaforma per la creazione di siti web. In altri termini, è un sistema di gestione dei contenuti utilizzato per costruire il sito.
- **Programming Languages: PHP** è il linguaggio di programmazione usato nel Server Multitenant per sviluppare applicazioni Web dinamiche, comunemente associato a WordPress.
- **Database: MySQL** è il database usato dal sito www.elti.it.
- **JavaScript Libraries: 1)** jQuery, libreria utilizzata per semplificare la manipolazione del DOM (*modello a oggetti del documento) e* l'interazione con il browser. *2)* Query Migrate, per mantenere la compatibilità con le vecchie versioni di JQuery durante l'aggiornamento.
- **Page Builders: Elementor** è un plugin (implementazione) di WordPress usato per la costruzione di pagine Complesse con interfaccia drag and drop (esempio Interfaccia grafica utente).
- **Slider Revolution:** viene usato come implementazione di WordPress sia per creare slider statici con più immagini sia per aggiungere elementi interattivi al sito (effetti di transizione, testi dinamici etc)
- **WordPress Themes: Zakra** è un tema di Wordpress utilizzato per la progettazione e presentazione visiva del sito.

- Scansionando Il web Server in ascolto lato client (Elti), vengono indicate:

- **Porte aperte**, 80 (TCP) e 334 (TCP-STL).
- Apache **httpd**: è software (programma) web server, anche detto Apache o httpd, che sta per "**Hypertext Transfer Protocol daemon**", indicando che è un programma che agisce come un demone, rimanendo in ascolto sulle porte 80/443 in background, progettato per gestire le richieste http e https tra i client e il Server stesso.
  Quindi il sito Elti.it si avvale del Server Apache per gestire le richieste HTTP e HTTPS che vengono dagli utenti tramite browser web.
- Status **200 OK**: La risposta del Server indica che le richieste HTTP e HTTPS sono state completate.
  In sintesi, entrambe le porte 80 e 443 indicano che il sito web utilizza il server Apache per gestire il traffico HTTP e HTTPS. La risposta "200 OK" su entrambe le porte indica che le richieste sono state elaborate con

successo, e sulla porta 443, sono presenti dettagli aggiuntivi, come la versione di PHP, il link header per le API di WordPress e il tipo di contenuto.

5) MALTEGO: tramite questo tool ho ottenuto una rappresentazione grafica del sito web e delle informazioni precedentemente raccolte con altre metodologie.