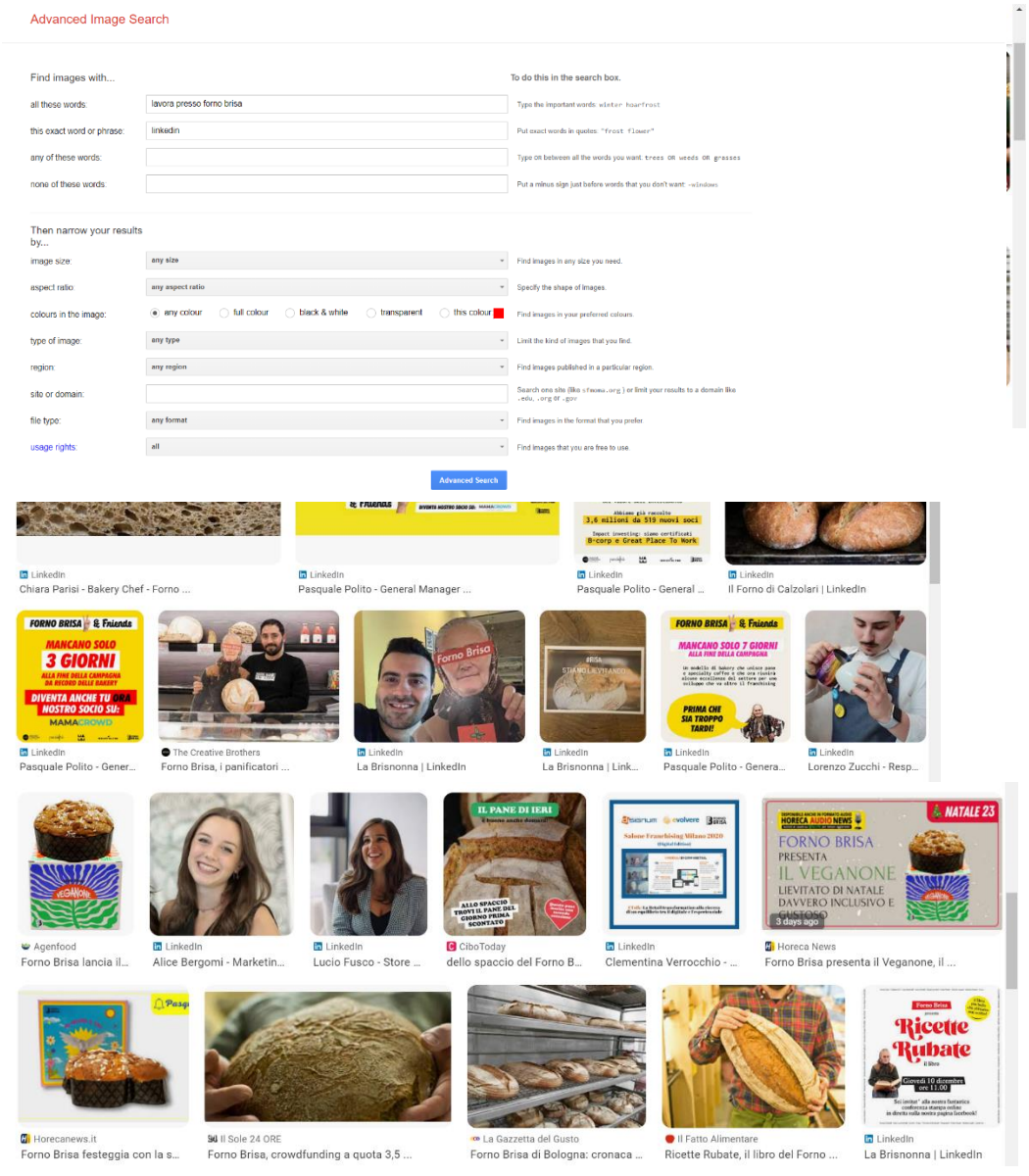
Per questo progetto ho scelto di effettuare l'OSINT su Forno Brisa, una panetteria specifica di Bologna, una bella start-up del territorio.

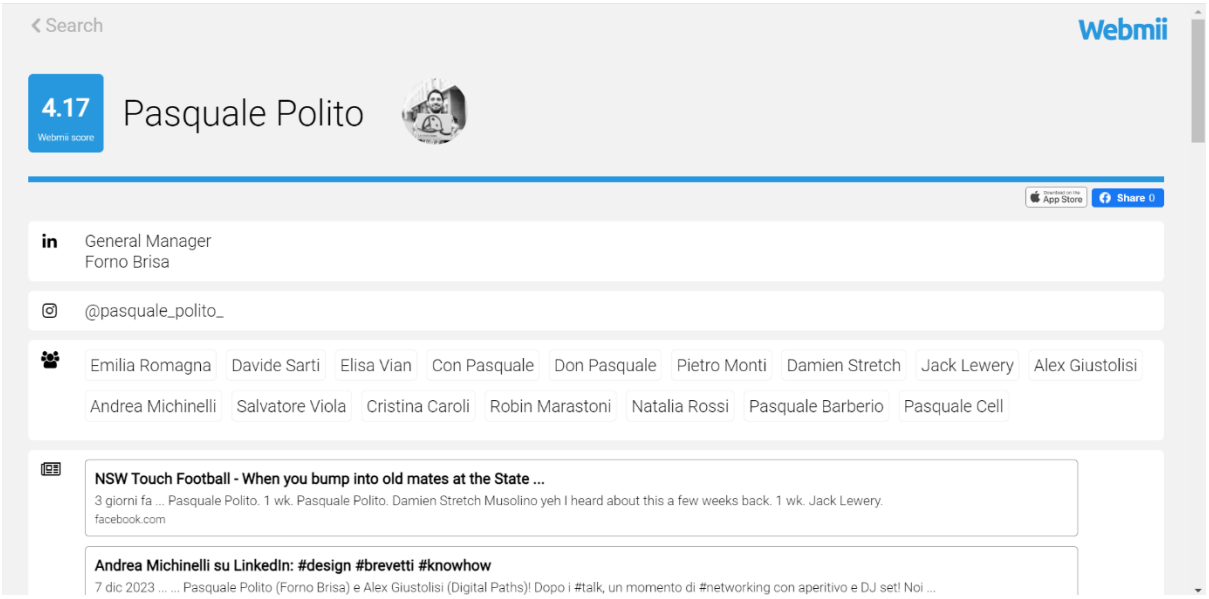
Scrive Il Sole 24 Ore:

Nata nel 2015 a Bologna, sulle ceneri di un ex-forno di quartiere, Forno Brisa è l'idea di quattro ragazzi, capitanati da Pasquale Polito, che decidono di cambiare vita, dedicarsi all'arte della panificazione e sovvertire l'immagine tradizionale del fornaio.
Diventata in breve punto di riferimento per pane, pizze, dolci da forno compresi i lievitati delle feste, oggi l'azienda conta 39 persone di cui 20 donne e 19 uomini (con un'età media sotto i 30 anni).
[…]
Quattro i punti vendita in città e un fatturato 2021 che si è chiuso superando i 2 milioni di euro, ma che – dicono – è in crescita: si aspettano di centrare l'obiettivo 3 milioni per il 2022. Il 49% del pane sfornato proviene dalle farine prodotte in biologico in un'azienda agricola di proprietà in Abruzzo e da campi in filiera diretta.

Il primo step è stato effettuare una ricerca avanzata tramite l'**Advanced Image Search** di Google per trovare più dipendenti possibili, soprattutto quelli di alto livello:



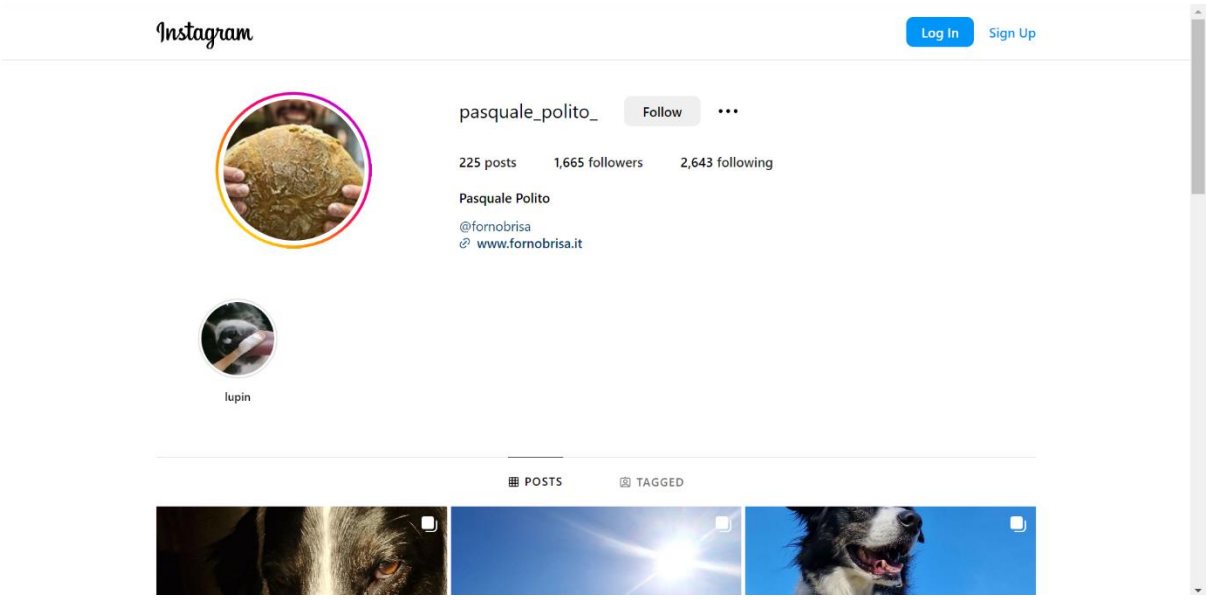
Individuo in particolare Pasquale Polito, già menzionato nell'articolo de Il Sole 24 ore, che da Linkedin risulta essere General manager dell'azienda. Con **Webmii** approfondisco la sua figura:



Il primo nome e cognome nei contatti è Davide Sarti, che scopro essere socio e co-fondatore insieme a Pasquale.

Sempre tramite Google riesco a trovare il profilo Instagram di Pasquale (profilo aperto), mentre purtroppo non riesco a reperire quello di Davide.

https://www.instagram.com/pasquale_polito_/?hl=en



A questo punto mi concentro sul sito, www.fornobrisa.it.

WHOIS

WHOIS è un protocollo di interrogazione utilizzato per ottenere informazioni sui registranti di nomi di dominio, come proprietari, contatti tecnici e dettagli del registrar. In pratica, consente di identificare

chi possiede un dominio o un indirizzo IP specifico. Le informazioni raccolte tramite WHOIS sono utilizzate per vari scopi, tra cui la gestione dei domini, la sicurezza e la risoluzione di problemi legati all'identificazione online. Tuttavia, nel corso degli anni, sono emerse preoccupazioni sulla privacy, portando a limitazioni e regolamentazioni nell'accesso ai dati WHOIS per proteggere le informazioni personali.

Anche nell'output di Whois compare il nome di Davide Sarti, ma non c'è purtroppo nessun contatto (mail o telefono).

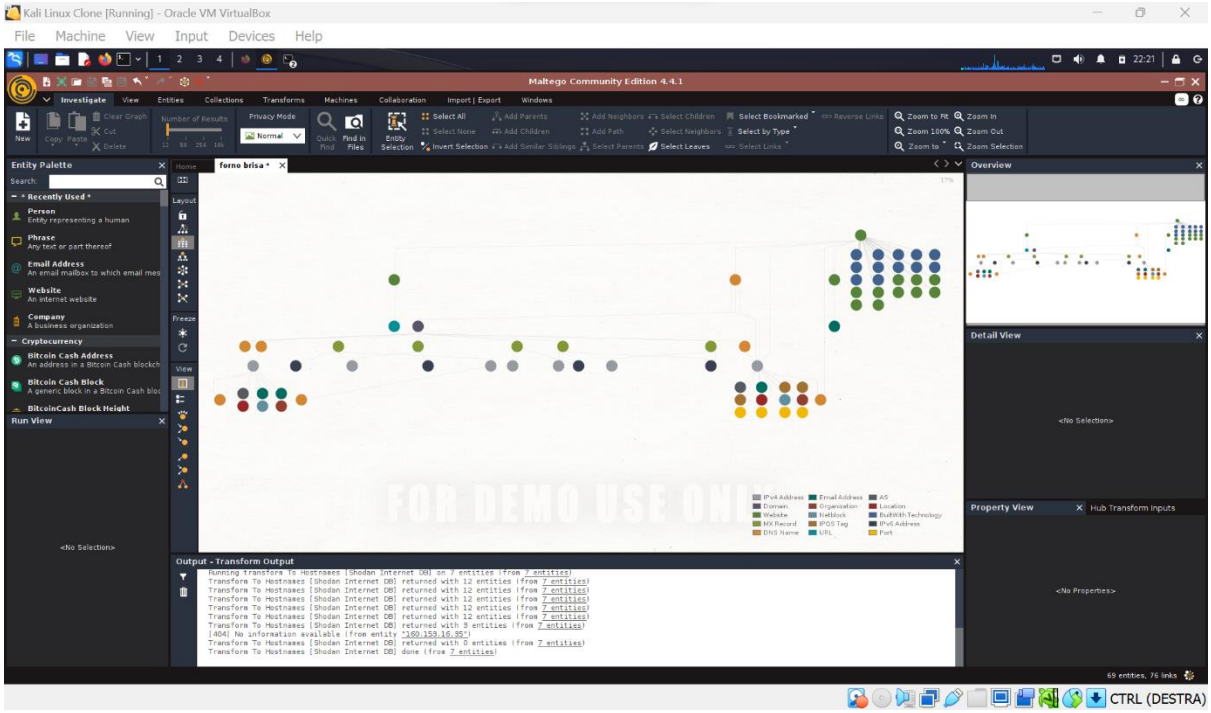
Scopriamo che il dominio è in scadenza il 9/09/24 ed è registrato tramite www.1api.net: queste informazioni potrebbero essere utilizzate da malintenzionati per simulare problemi con la registrazione o il rinnovo della stessa, in un tentativo di phishing.

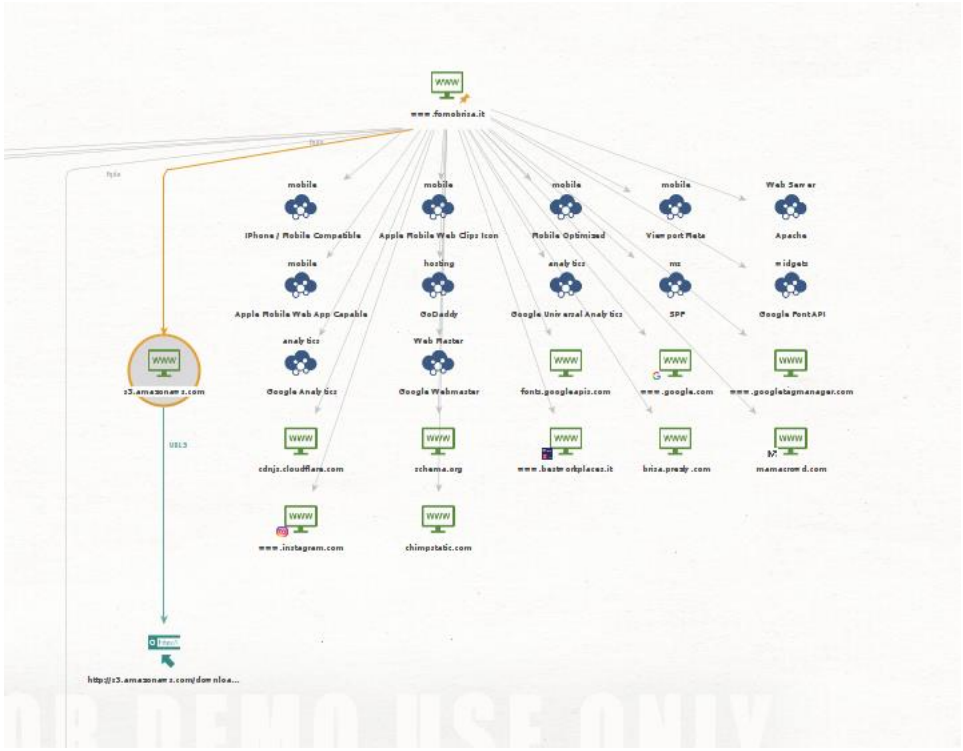
È inoltre presente l'informazione DNSSEC: yes.
DNSSEC è un'estensione del sistema DNS che garantisce autenticità e integrità delle informazioni DNS. Nel contesto WHOIS, indicare DNSSEC per un dominio significa che quel dominio utilizza misure di sicurezza per prevenire manipolazioni o falsificazioni dei suoi record DNS. Essenzialmente, è un meccanismo di sicurezza per rafforzare la validità delle informazioni associate a un dominio.

MALTEGO

A questo punto creiamo un nuovo schema su **Maltego**. Il nostro nodo zero sarà proprio www.fornobrisa.it.

Dopo vari transform, lo schema risulterà come segue. Vediamo le sue parti nel dettaglio.



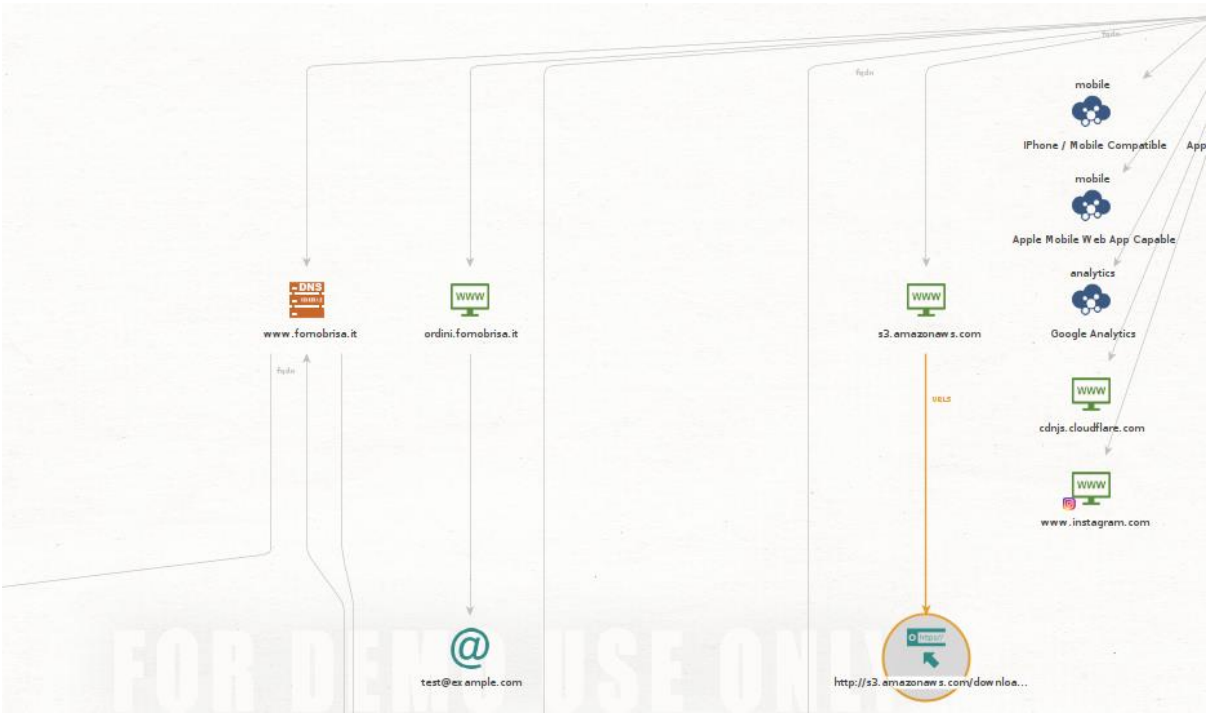


Tramite il trasform Built With, scopriamo le diverse tecnologie con cui è stato creato il sito. Fra gli elementi più interessanti spiccano:

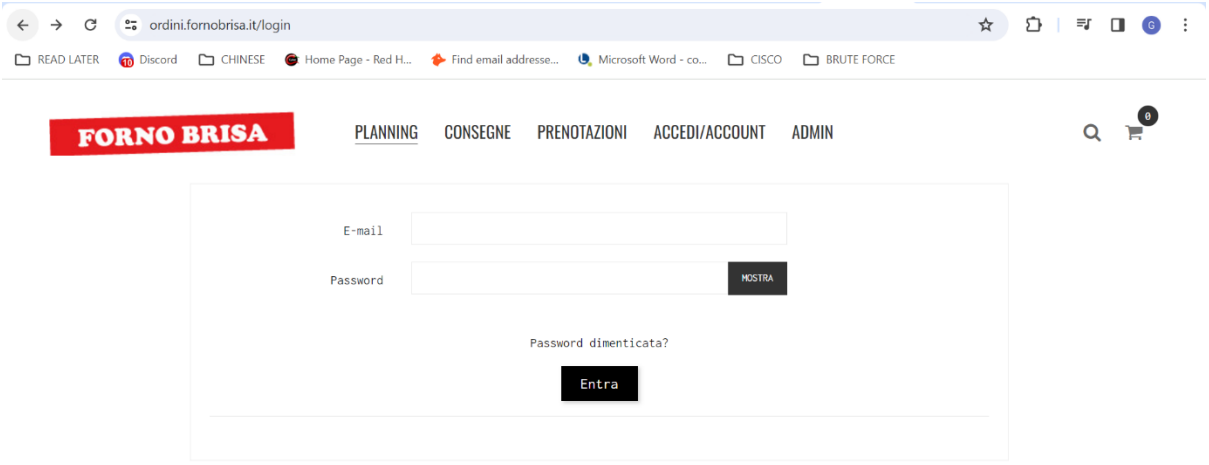
- Il Web Server è Apache. Apache è un popolare server web open-source utilizzato per ospitare siti web. Fornisce la capacità di servire pagine web su Internet, gestire richieste HTTP e supportare linguaggi di programmazione come PHP e Perl;
- L'hosting è di GoDaddy;
- Viene utilizzato il record SPF per verificare l'autenticità e la provenienza delle email, riducendo il rischio di email fraudolente o spam.

Se invece approfondiamo i link esterni, emerge chimpstatic che è legato a Mailchimp. Da cui deduciamo che è in uso Mailchimp, piattaforma leader per il marketing via email, specialmente utilizzata da piccole e medie imprese. Molto interessante anche il link a s3.amazonaws.com: Amazon S3 è un servizio di archiviazione cloud di Amazon Web Services (AWS). "s3.amazonaws.com" è l'indirizzo per accedere ai dati archiviati su S3, dove i dati vengono conservati in "bucket" virtuali.

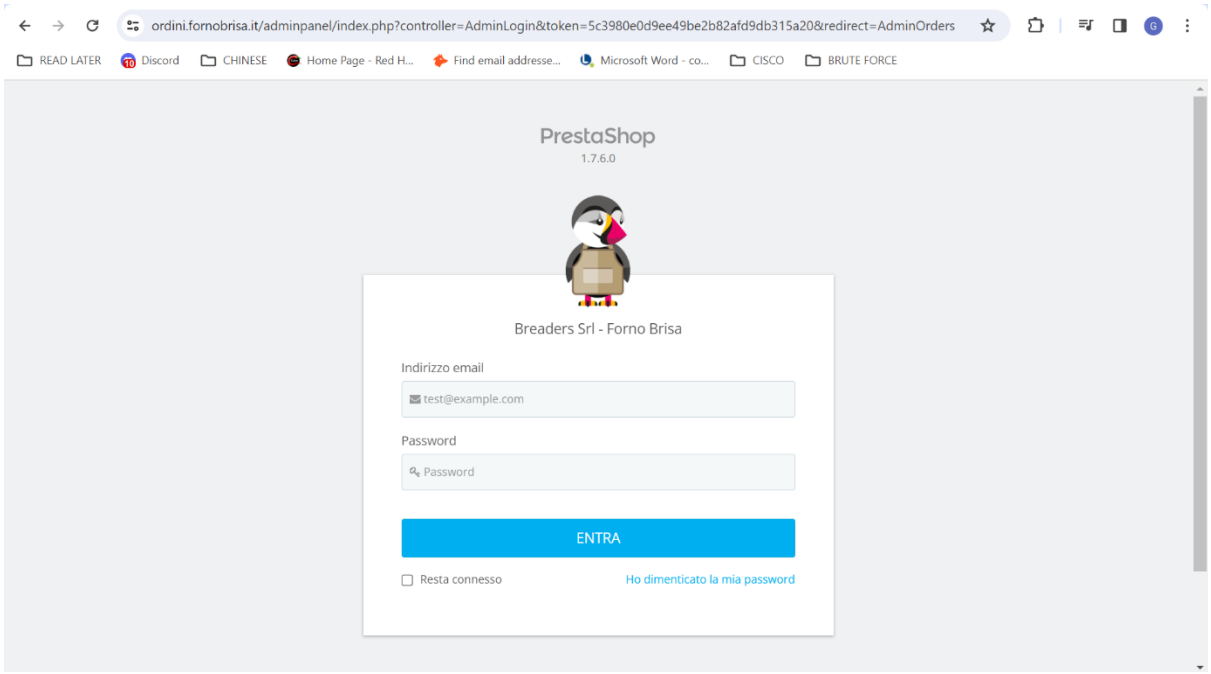
Spostandoci verso sinistra nello schema, troviamo un altro indirizzo: ordini.fornobrisa.it.



Lo visitiamo e sembra proprio un sito che non dovrebbe essere visibile o accessibile al pubblico:



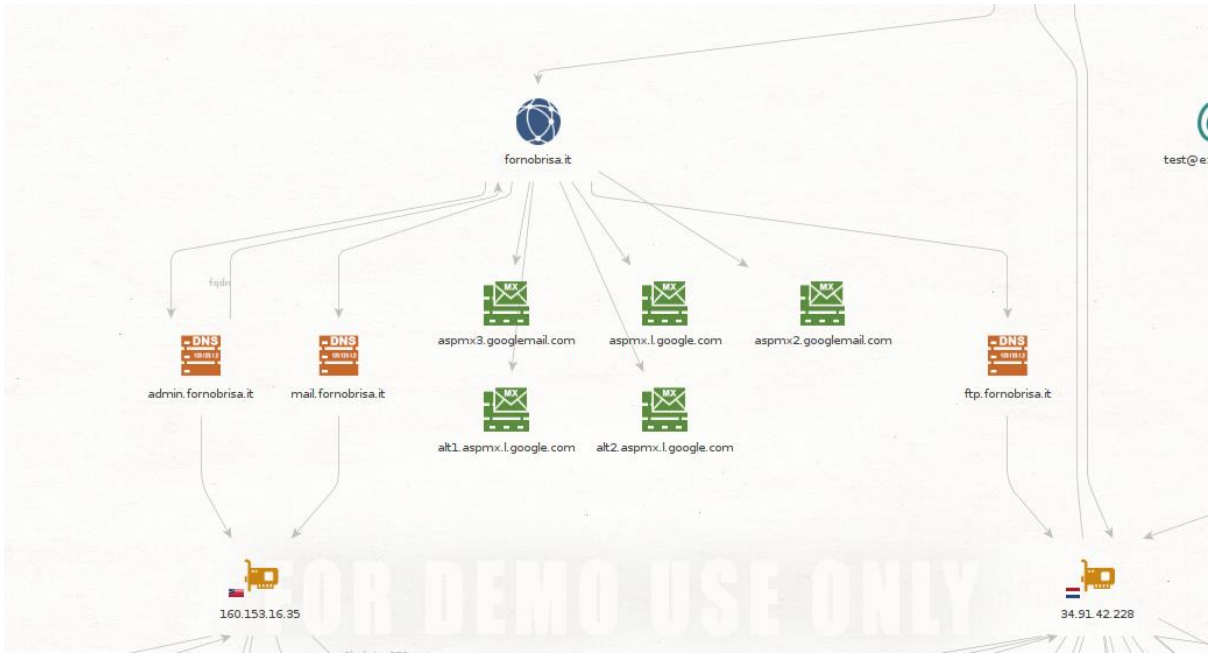
Di particolare interesse la tab ADMIN, che rimanda ad una finestra di login PrestaShop:



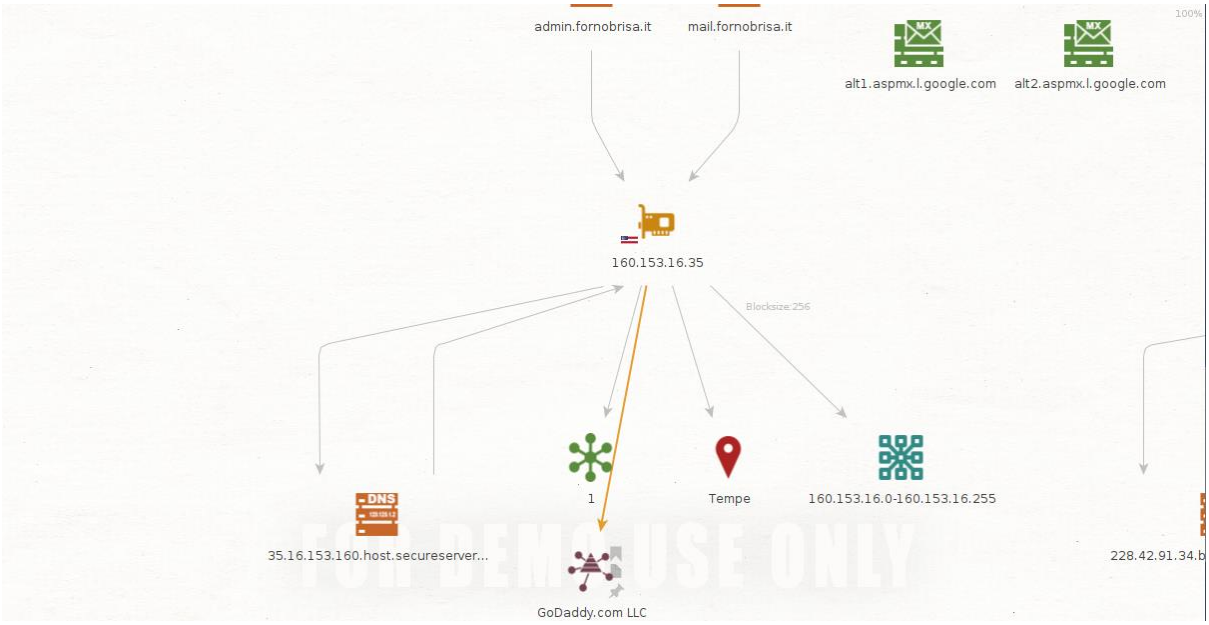
PrestaShop è una piattaforma open-source per e-commerce. Permette di creare negozi online personalizzati, gestire prodotti, ordini, pagamenti e altri aspetti del commercio elettronico.

Questa tab potrebbe prestarsi ad attacchi Brute Force, se non adeguatamente protetta.

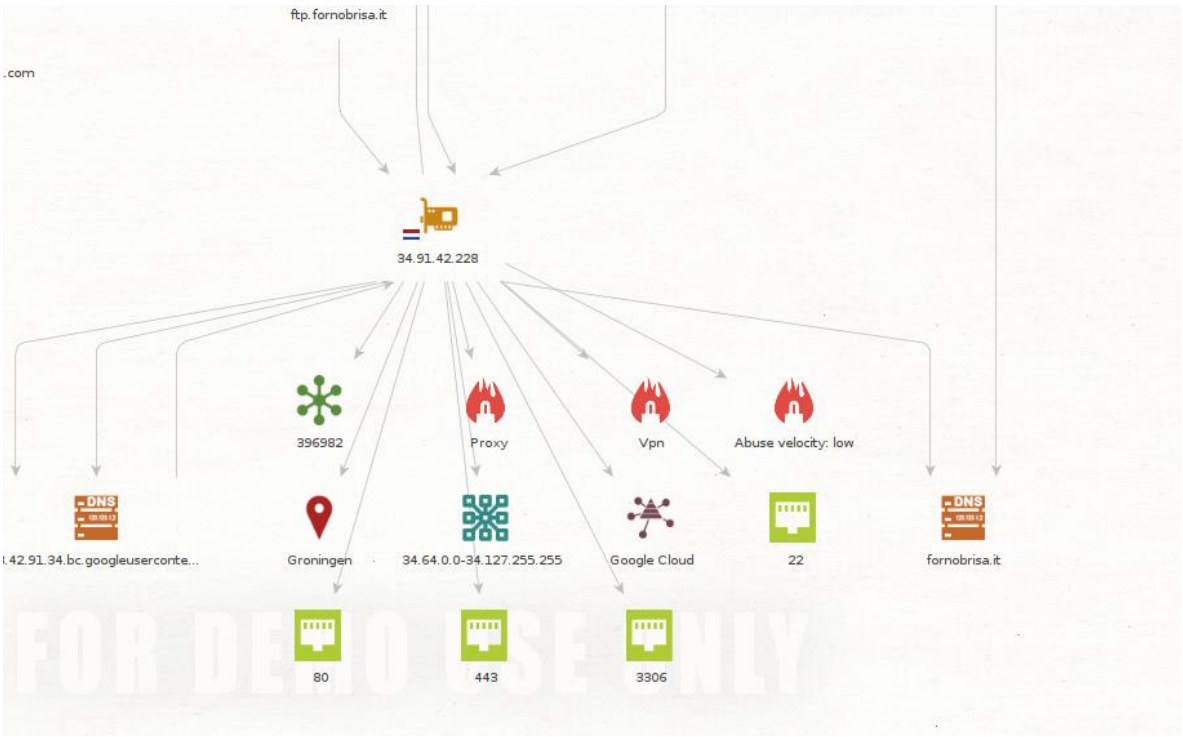
Spostandoci a sinistra nello schema di Maltego, dal dominio fornobrisa.it riusciamo a ricavare ben 3 DNS: admin.fornobrisa.it e mail.fornobrisa.it e ftp fornobrisa.it:



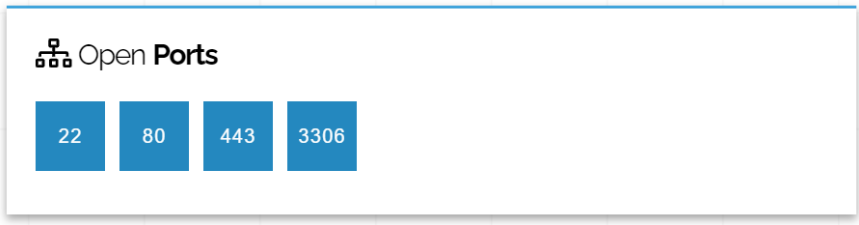
I primi due sono collegati ad un IP che, a parte essere collegato ad un netblock (blocco di indirizzi IP consecutivi in una particolare rete), non offre spunti particolarmente interessanti. Interrogato su questo indirizzo, **Shodan** non dà alcun risultato.



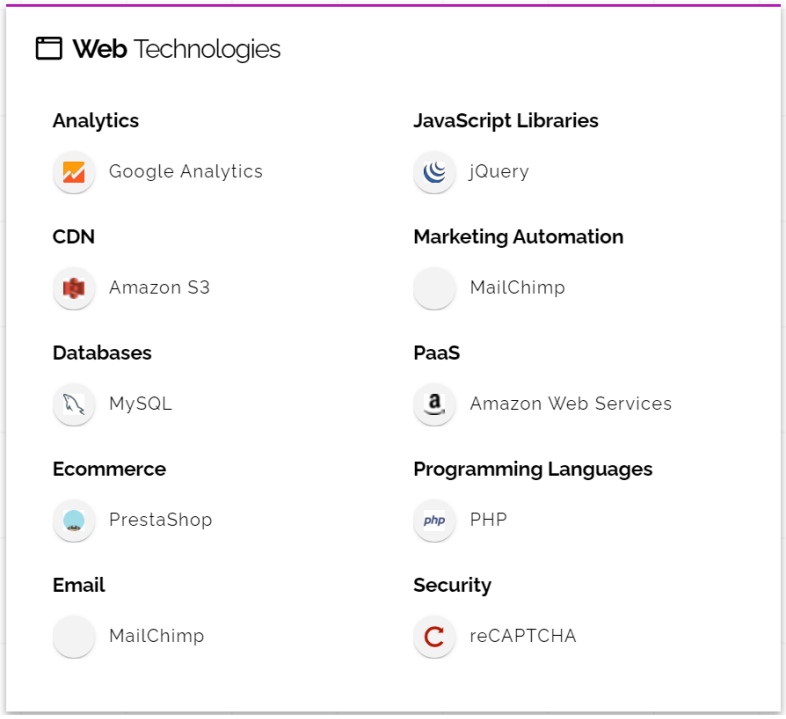
L'IP legato a ftp.fornobrisa.it, invece, oltre al proxy e alla VPN presenta 4 porte che andiamo ad approfondire con **Shodan**.



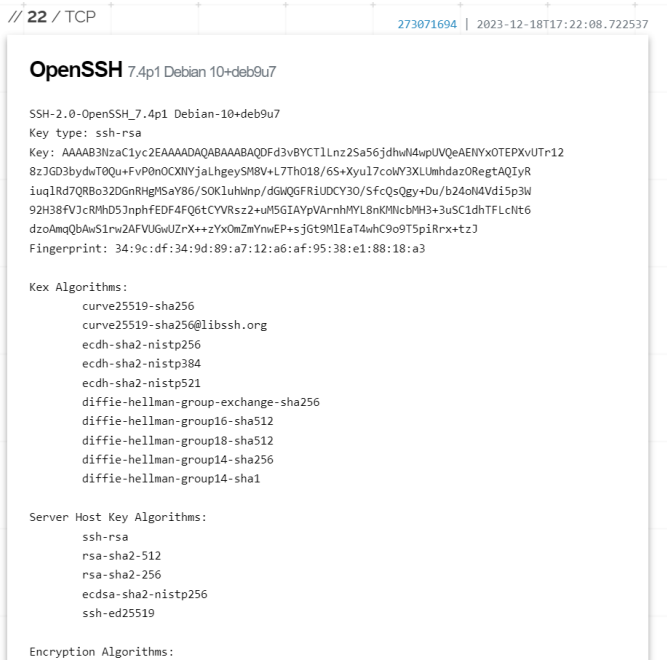
Da **Shodan**:



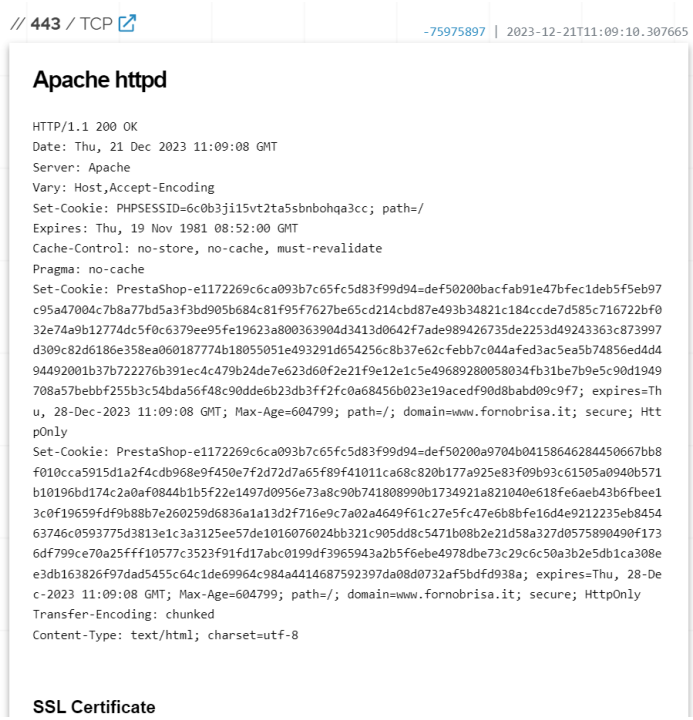
Troviamo riconfermate inoltre le informazioni già reperite prima:



Sulla porta 22, troviamo il servizio SSH. SSH è un protocollo crittografico utilizzato per l'accesso sicuro a server e dispositivi remoti su una rete.
Configurando e permettendo l'accesso SSH su una porta (la porta 22 è quella standard), gli amministratori di sistema possono connettersi in modo sicuro al server per gestire, configurare o eseguire operazioni sul sistema remoto utilizzando comandi SSH. Tuttavia, è essenziale mantenere la sicurezza configurando correttamente SSH, come disabilitando l'accesso root remoto, utilizzando autenticazione a due fattori e limitando l'accesso solo a indirizzi IP autorizzati, per proteggere il server da potenziali minacce o attacchi.

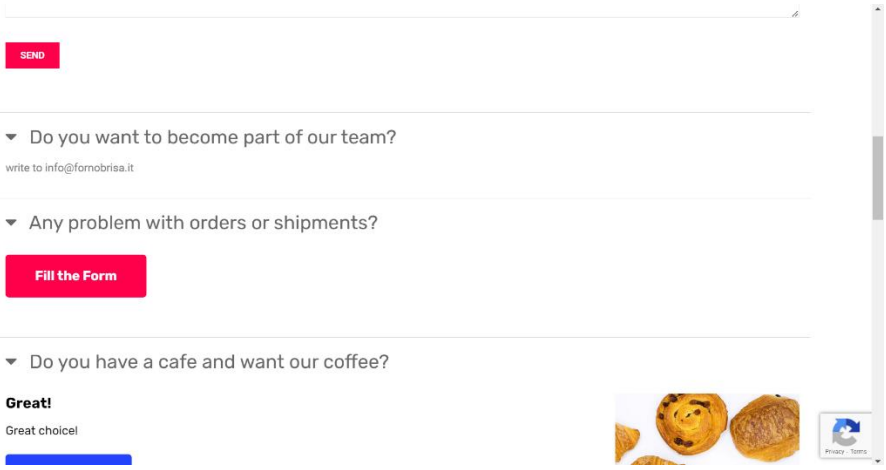


La porta 80 è la porta standard per il traffico HTTP non cifrato.
La porta 443 è la porta standard per il traffico HTTPS, che è HTTP cifrato con SSL/TLS per garantire la sicurezza delle comunicazioni. Apache HTTP Server è uno dei server web più popolari e utilizzati al mondo. Configurando Apache per ascoltare su queste porte, il server è pronto a gestire richieste web non cifrate (porta 80) e richieste web cifrate (porta 443) per fornire contenuti web agli utenti attraverso protocolli HTTP o HTTPS, rispettivamente.



Sulla porta 3306, infine, è in esecuzione MySQL, un popolare sistema di gestione di database. Se MySQL sulla porta 3306 è configurato in modo errato o non sicuro potrebbe essere esposto a tentativi di accesso:

Arrivata a questo punto, non ho però ancora nessun contatto mail o cellulare (ho solo il numero fisso di Forno Brisa). Dopo una lunga ricerca riesco a reperire questo indirizzo mail sul sito:



Come immaginavo, la mail è @fornobrisa.it. Quando provo però a lanciare questo dominio su **theHarvester**, non ottengo alcun risultato:

Nonostante numerose ricerche e approfondimenti, non ho trovato alcuna informazione su indirizzi mail dell'azienda. L'informazione potrebbe essere ben protetta oppure posso supporre che i fondatori utilizzino una mail che non termina in @fornobrisa.it, essendo comunque l'azienda ancora piccola e non avendo dei veri e propri reparti interni.