NAVIGAZIONE ANONIMA, DEEP E DARK WEB

Navigare in anonimato è quasi impossibile, perché non si ha il totale controllo delle risorse hardware che si interpongono tra noi ed il server web a cui accediamo e di conseguenza la privacy potrà essere alta ma mai totale.
Le motivazioni per cui la navigazione debba essere anonima possono essere molteplici e non sempre illegali come si potrebbe facilmente intuire. Ad esempio potrebbe esserci la necessità di scambiarsi una mail o dei file, in maniera sicura, senza che essi vengano intercettati, o semplicemente si potrebbe voler navigare in maniera anonima, senza che i propri interessi vengano utilizzati per essere bombardati di offerte di qualsiasi tipo. Purtroppo però l'anonimato è spesso anche sinonimo di attività illegali, ma non per questo deve essere criminalizzato a prescindere.

Possiamo immaginare il mondo di internet diviso nelle seguenti 3 categorie:

- **Clear web o surface web:** la parte indicizzata e presente nei motori di ricerca e nei DNS, è la parte che tutti conosciamo quando navighiamo in rete.
- **Deep web:** contenuti non indicizzati dai motori di ricerca, spesso accessibili mediante autenticazione o URL specifici.
- **Dark web**: l'insieme di reti con siti non indicizzati, a cui è possibile accedere attraverso reti specifiche come Tor.

Finger printing
Come visitiamo un sito WEB si scatenano una serie di eventi che crea una sorta di impronta digitale.
La tracciatura dei nostri interessi è ormai nota, basta andare su youtube e vedere i video consigliati, o navigare e vedere le varie pubblicità apparire che consigliano prodotti legati alle nostre ricerche, e non solo, ma anche al PC che noi usiamo alla nostra età.
Le informazioni che rilasciamo quando visitiamo un sito sono tantissime, con google analytics, è infatti possibile avere informazioni di vario tipo.
La risoluzione dello schermo, i plugin attivi sul browser, la lingua utilizzata dal sistema operativo, la sua versione, il tipo di macchina che stiamo utilizzando e così via.
Ad esempio tramite questo sito: https://panopticlick.eff.org/ si può testare la capacità del nostro browser, di garantire il nostro anonimato.

Cominciamo a trovare la prima maniera per tentare di garantire l'anonimato, e scarichiamo il browser Tor tramite questo link: https://www.torproject.org/



Apriamo una parentesi

Quando si scarica occorre sempre fare il cheksum per evitare che ciò che scarichiamo non contenga potenziali codici dannosi.

Il cheksum MD5 è un algoritmo matematico che restituisce 32 caratteri esadecimali. Il calcolo viene effettuato attraverso una funzione hash di crittografia che può utilizzare vari algoritmi.

I più diffusi sono **MD5, SHA-1 e SHA-2.**

Il cheksum indicato vicino ad un file prima del suo scaricamento, va confrontato con quello calcolato sul file scaricato, in modo da verificare la perfetta corrispondenza, e pertanto essere certi che il download non sia stato corrotto, e che nel file iniziale non sia stato inserito del codice dannoso.

Per calcolare il checksum dopo aver scaricato il file esistono siti online che offrono il servizio di calcolo gratuito come ad esempio http://onlinemd5.com/ oppue esistono programmi anche gratuiti che eseguono la stessa funzione, come ad esempio WinMD5Free https://www.winmd5.com/ , in entrambi i casi viene utilizzato l'algoritmo MD5, per altri algoritmi si trovano in rete diversi siti e software.

Il progetto Tor non è solamente composto dal Browser, ma è un insieme di servers e router che hanno come scopo quello di garantre la navigazione anonima in internet e l'accesso alla Onion Network detta anche DeepWeb. L'acronimo TOR deriva infatti da The Onion Router.

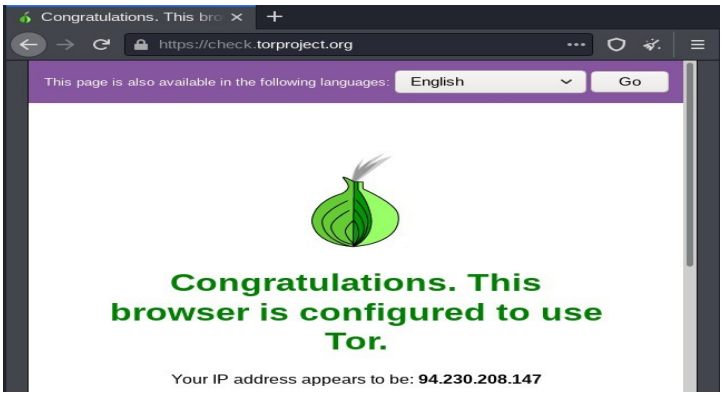
La rete TOR è una rete criptata dentro internet, creata inizialmente dal Naval Research Laboratory statunitense e successivamente presa in gestione da una fondazione no-profit che ha dato seguito il progetto.

I compiti principali sono quelli di rendere privata ed anonima la navigazione verso un sito web, e dare accesso ai servizi nativi e dedicati dentro la rete TOR.

Il nostro PC nel momento in cui utilzza il browser TOR, prima di arrivare al sito richiesto, fa 3 salti entrando nella rete TOR, i dati transitano sul Middle node ed escono dall'Exit node, quest'ultimo è il nodo che manda la richiesta al sito e riceve la sua risposta.

Possiamo scaricare TOR per Windows, Mac o Linux. Una volta lanciato possiamo controllare la sua corretta configurazione digitando sulla barra degli indirizzi check.torproject.org

Nella pagina che si apre, oltre all'informazione relativa alla corretta configurazione, troviamo l'IP con cui usciamo sulla rete internet, possiamo controllare come questo indirizzo sia diverso da quello che otterremmo in un normale browser controllando l'indirizzo di navigazione senza anonimato.



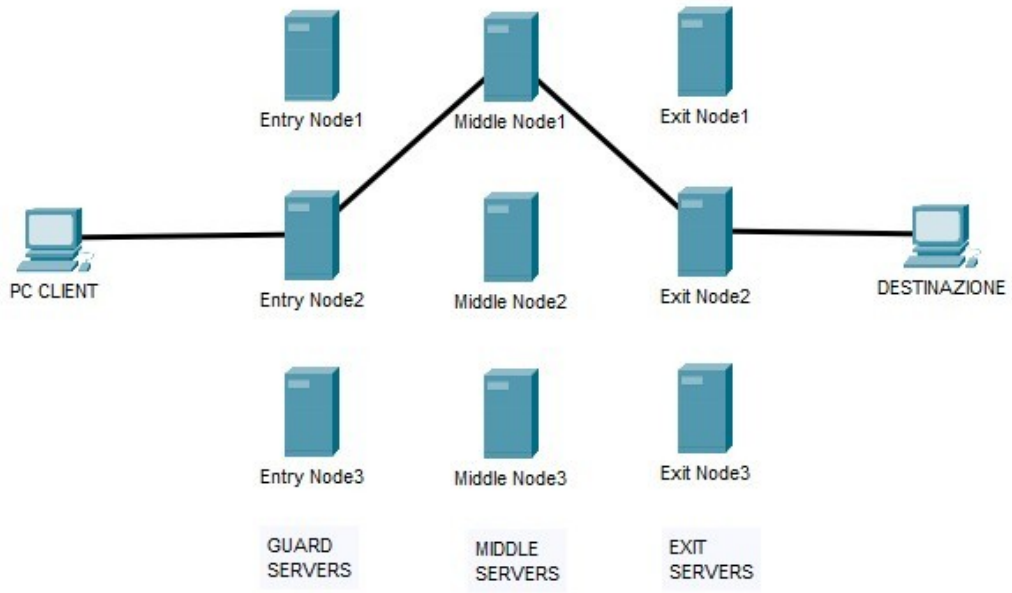


TOR The Onion Router

Letteralmente l'acronimo significa "il router cipolla", ed il significato è più che corretto, in quanto la sua struttura composta da una rete di server, utilizza una crittografia di dati a più strati per accedere a domini nascosti .onion.

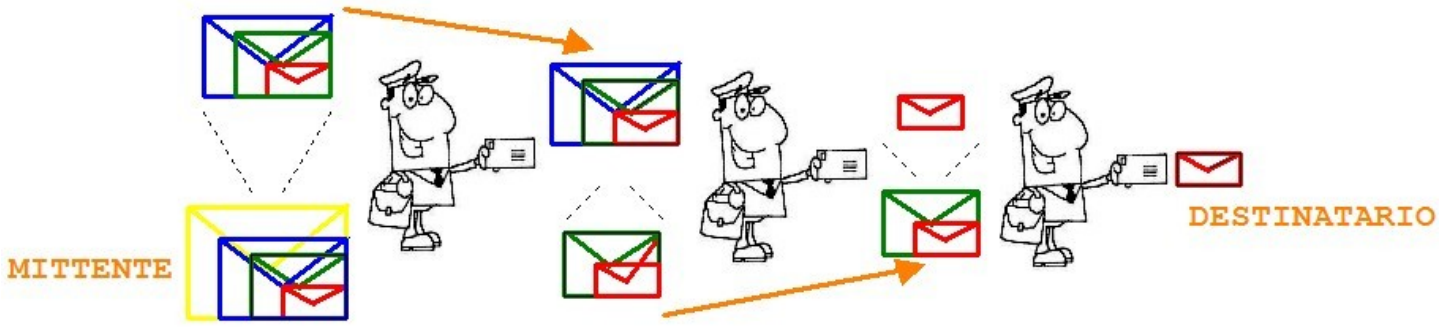
Il suo utilizzo pur se associabile ad attività illecite, è di largo utilizzo anche per attività legali come ad esempio una navigazione anonima finalizzata alla difesa della propria privacy. Non tutti sono infatti contenti di ricevere popup pubblicitari o di visualizzare inserzioni su qualcosa che si è cercato in un motore di ricerca, e tutti hanno l'esigenza di navigare in maniera sicura quando si utilizza la rete per attività di tipo finanziario o commerciale.

Il traffico dati in una rete TOR, parte dal nostro PC e si immette nel nodo di ingresso Entry Node, per poi raggiungere un Middle Node ed infine uscire verso il sito tramite l'Exit node.



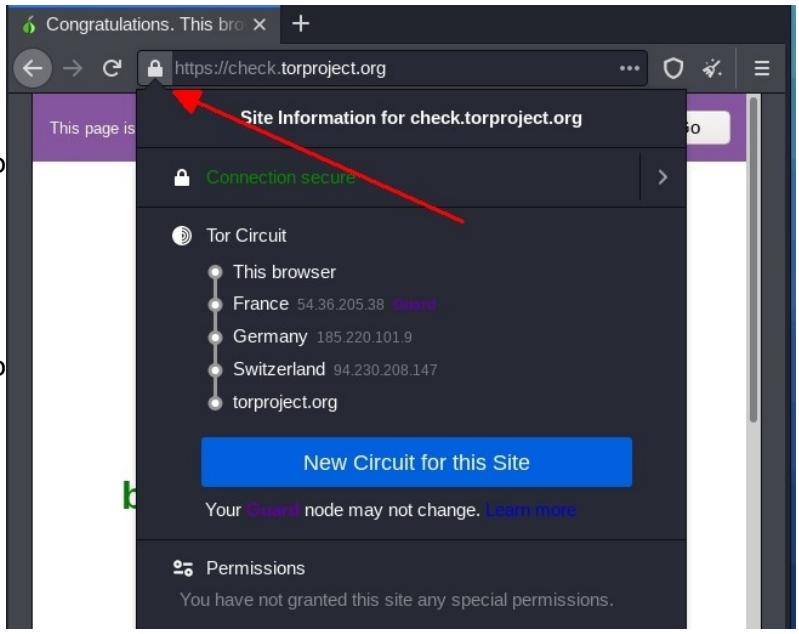
In pratica dal punto di accesso a quello di uscita in una rete TOR, la nostra comunicazione attraverserà dei nodi con diversi livelli di crittografia del messaggio.

In nessuno dei nodi si può avere traccia dell'intero percorso, è come se inviassimo una lettera chiusa in 3 buste. Il primo destinatario aprirà la busta e troverà l'indirizzo a cui spedire la seconda busta, il secondo destinatario aprirà la seconda busta e troverà l'indirizzo a cui spedire la terza, l'ultimo nodo invierà il contenuto al destinatario finale. Nessuno dei destinatari è a conoscenza del contenuto e del percorso completo.

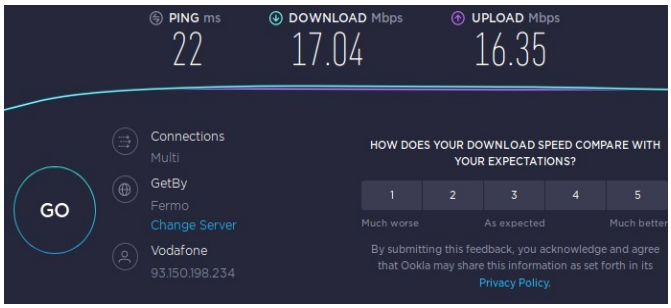


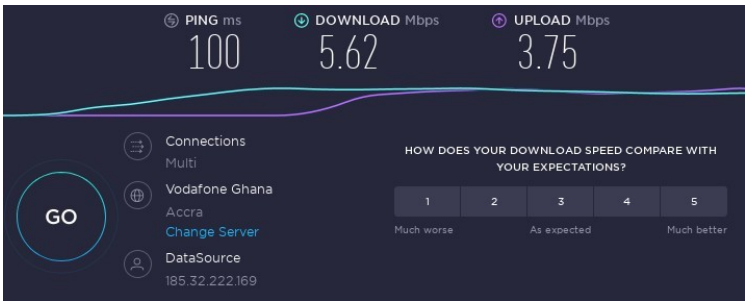
Dal browser possiamo inoltre vedere i 3 nodi utilizzati, cliccando sul lucchetto vicino alla barra degli indirizzi.

Cliccando sul pulsante al centro "New Circuit for this Site", si avranno nodi diversi.



Fermo restando che risulta un buon modo per avere una navigazione sicura, bisogna sempre considerare che determinati siti riescono a tracciare il vero mittente (es. facebook, google) e determinate organizzazioni hanno accesso ai nodi per poter rintracciare gli utenti, come la NSA americana.
Inoltre la sua struttura rende particolarmente lenta la connessione. Se infatti confrontiamo i risultati dello speedtest fatto su un browser normale e sul browser TOR abbiamo quanto segue.

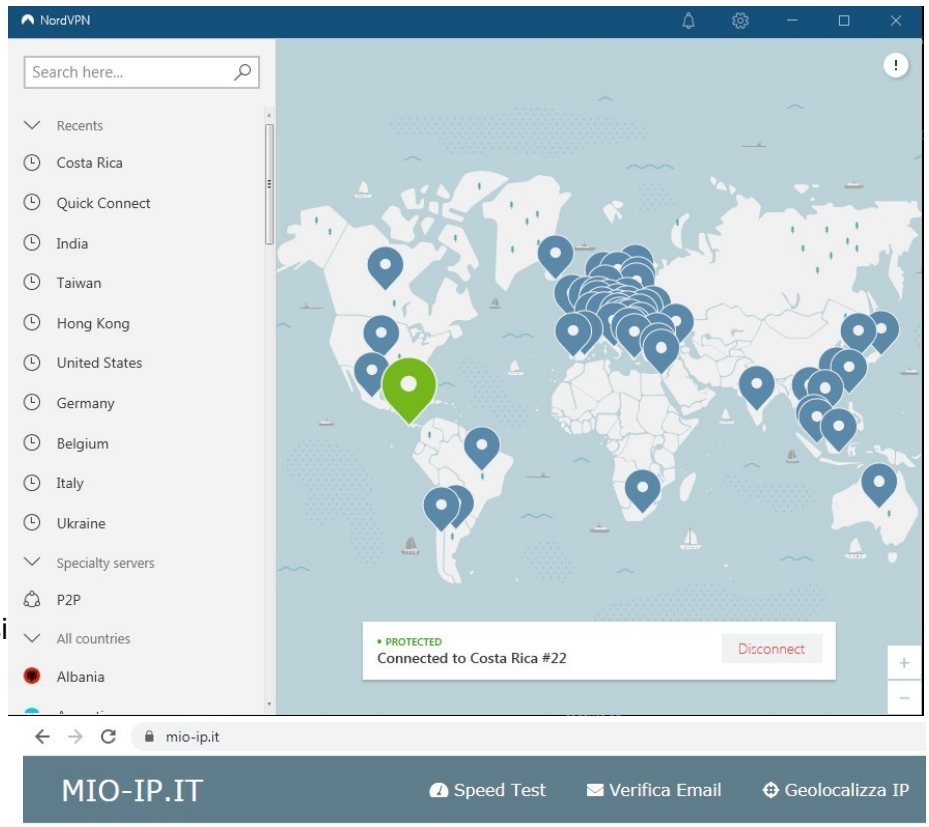


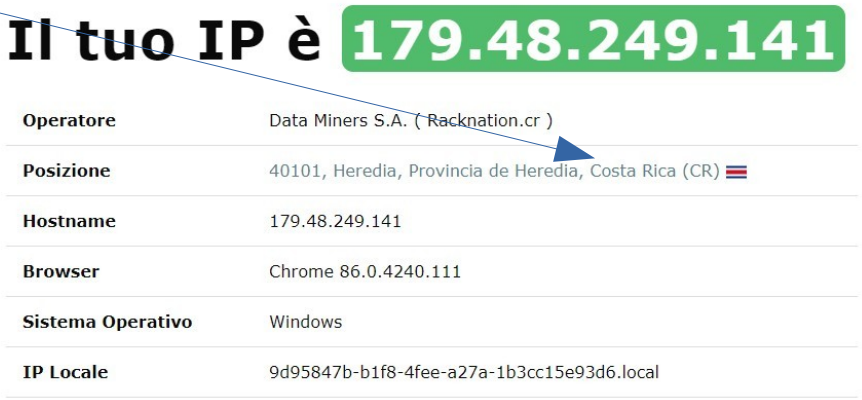


A sinistra uno speedtest con un qualsiasi browser passando tramite una macchina virtuale con Kali Linux, a destra lo stesso speedtest con il TOR browser sempre dentro alla stessa macchina virtuale.
La connessione viene infatti notevolmente rallentata dalla rete TOR, con la sua crittografia a strati.
Un'altro svantaggio è che pur consentento una navigazione anonima, TOR non nasconde il fatto che venga utilizzato.
Si potrebbe confondere TOR con una VPN, la differenza sostanziale è che TOR è una rete logica che opera sopra una rete già esistente e che utilizza dei canali criptati per far viaggiare i dati, invece la VPN è un software che utilizza un canale tra il proprio PC ed un sever remoto posto in una zona geografica che può essere scelta. Anche in questo modo l'indirizzo IP di uscita verso la rete verrebbe modificato.
In entrambi i casi la connessione viene comunque rallentata, in quanto anche nella VPN, come vedremo più avanti, c'è un criptaggio dei dati.

Ad esempio utilizzando la famosa NORDVPN, si possono scegliere diversi server in giro per il mondo, ed una volta che si è stabilita la connessione con il server scelto, è come se fisicamente il nostro PC fosse collegato ad internet in quel paese.

Nell'esempio a destra è stato effettuato il collegamento con un server della Costa Rica e andando sul sito mio-ip.it l'indirizzo pubblico che ci viene assegnato, oltre che essere diverso da quello con cui siamo realmente connessi al nostro provider, è un indirizzo di un server fisicamente collegato in Costa Rica.





VPN sta per Virtual Privat Network, ed è una connessione che instaura un collegamento fisico mediante un tunnel virtuale che sfrutta la rete internet.

Una delle applicazioni più comuni, è quella di consentire il collegamento con una rete aziendale da remoto.

Ma nel nostro caso l'obiettivo è diverso, ed è quello di proteggere la propria privacy e garantire l'anonimato.

Le VPN in via del tutto teorica possono essere di 3 tipi: Trusted, Secure ed Hibryd.

Nel primo caso la VPN Trusted, il tunnel virtuale sfrutta un percorso ben definito di server tra il due punti che si collegano, la sicurezza di questa VPN sta proprio nel controllo del percorso. Nel secondo caso con la VPN Secure, il tunnel virtual non utilizza un percorso definito, ma utilizza i normali percorsi che si creano in una navigazione nel web, il tunnel si stabilisce però utilizzando degli algoritmi di cifratura, garantendo in questo modo la sicurezza del collegamento. Nel terzo caso con la VPN Hibryd, vengono combinati i primi due casi, e cioè un percorso definito dove i dati vengono cifrati.

In una rete VPN i protocolli di sicurezza utilizzati sono svariati, i più conosciuti sono IPSEC, SSL/TLS OpenVPN e SSH.

TOR+VPN

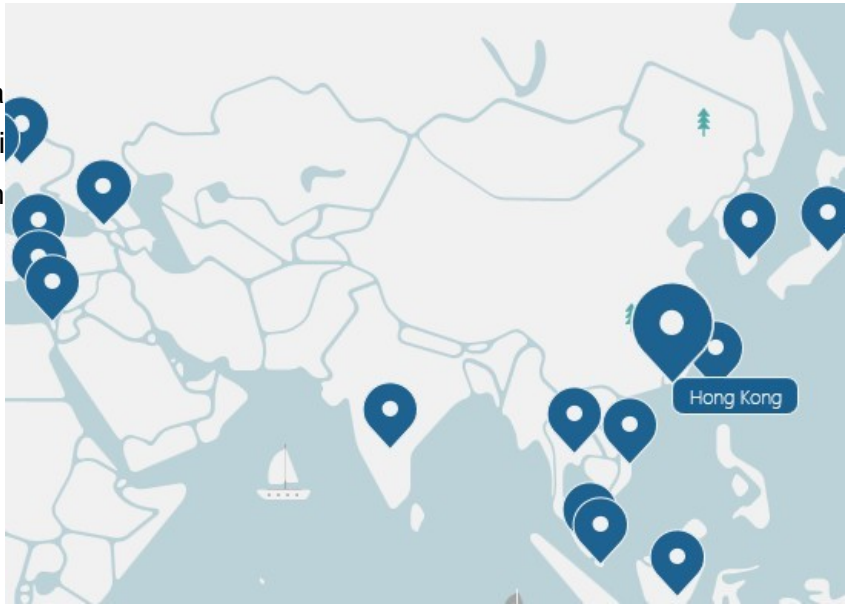
Combinando le due soluzioni e cioè utilizzo del browser TOR con una connessione VPN attiva, facendo attenzione a scegliere una VPN affidabile (perciò mai quelle gratuite) si può avere un alto livello di sicurezza e di anonimato per la propria connessione.

Censura di TOR

Tornando a TOR, uno dei problemi è che può essere riconosciuto e censurato.

In molti paesi con regimi totalitari, come la Cina, l'utilizzo di TOR non viene consentito, perché la navigazione deve essere controllata.

Anche con la VPN avviene la stessa cosa, aprendo NordVPN infatti notiamo che non ci sono server in Cina o in Arabia Saudita.



Il controllo della rete TOR avviene perché i nodi utilizzati visti prima, sono pubblici, e chiunque può contribuire ad aumentare la rete TOR diventando esso stesso un nodo.

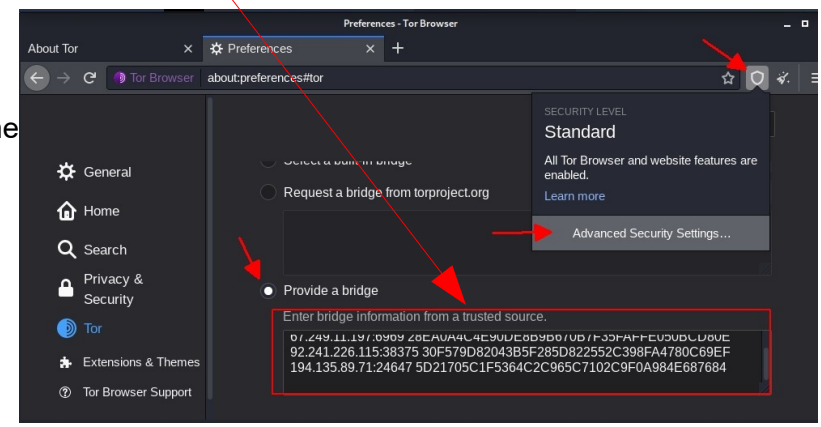
Ciò fa si che questi nodi vengano riconosciuti e pian piano messi in una black list da parte dei service provider, che controllano il primo accesso del nostro PC alla rete.

Una prima soluzione è quella di utilizzare gli Onion Bridges o TOR Bridges, sono nodi praticamente identici agli altri, ma non sono pubblici.

Per fare questo occorre cercare gli indirizzi dei TOR Bridges dal sito https://bridges.torproject.org/bridges e copiare l'elenco dei bridge nell'apposita sezione nella configurazione del browser TOR.

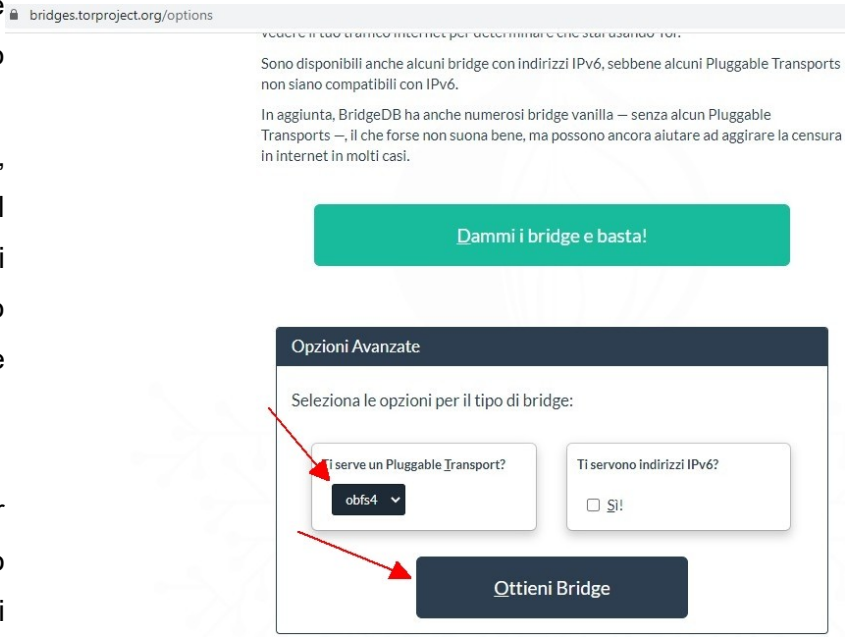


Basta un copia incolla nella sezione evidenziata, e verranno utilizzati i TOR Bridge elencati.



Questo metodo non è sempre risolutivo, in quanto i provider hanno adottato delle soluzioni per bypassare il problema, in pratica tramite delle DPI (Deep Packet Inspection) cioè un'analisi approfondita dei pacchetti, i service provider capisce che stiamo comunque utilizzando una rete TOR, bloccando così il traffico.

TOR mette a disposizione una soluzione utilizzando i pluggable transport che troviamo all'indirizzo https://bridges.torproject.org/options , scegliendo l'algoritmo si clicca poi sul pulsante al centro e si scarica la lista degli indirizzi da copiare ed incollare come fatto precedentemente nelle impostazioni avanzate del browser TOR.



Può accadere che i service provider per evitare la navigazione non consentano l'accesso al sito che contiene gli indirizzi dei TOR bridges, in questo caso si può bypassare il problema cambiando DNS o utilizzare una VPN per accedere al sito passando da altri paesi.

DARK WEB

La premessa fatta sul TOR e sulle VPN è doverosa, per entrare nel dark web.

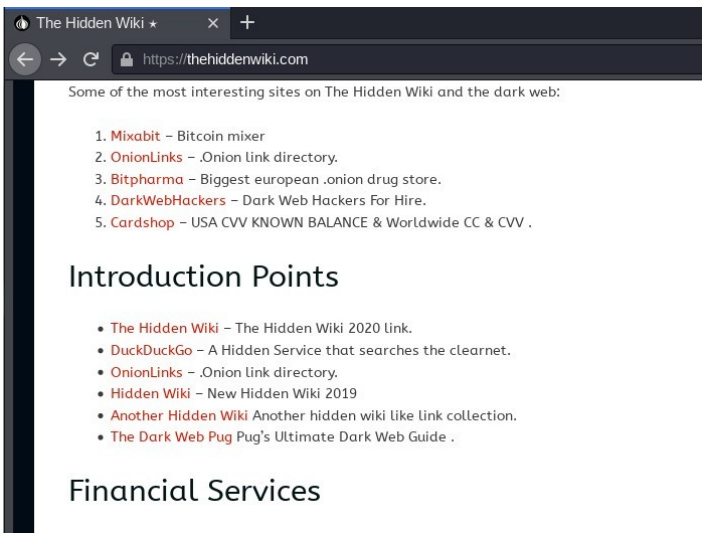
Entrare nel **Dark Web** significa accedere a una porzione nascosta di Internet che richiede software specifici (come Tor) e protocolli dedicati per aggirarsi tra siti non indicizzati e non raggiungibili con i normali browser.

Per chi non conoscesse il funzionameto del DNS, consiglio di leggere a pag.16 del seguente documento: https://danielepostacchini.it/wp-content/uploads/2019/02/Analisi-di-rete_2.pdf

Nel dark web non abbiamo i classici URL che conosciamo come ad esempio www.ebay.it o www.danielepostacchini.it, ma abbiamo degli indirizzi composti da caratteri incomprensibili.

La prima operazione da fare è quella di reperire i link degli indirizzi del dark web, e cioè come già fatto con sopra con i TOR Bridges, accedere ad un sito presente nel normale web, che contiene i link dei siti del dark web appartenenti al mondo TOR. Tutti questi siti hanno estensione .onion e non sono indicizzati nei DNS.

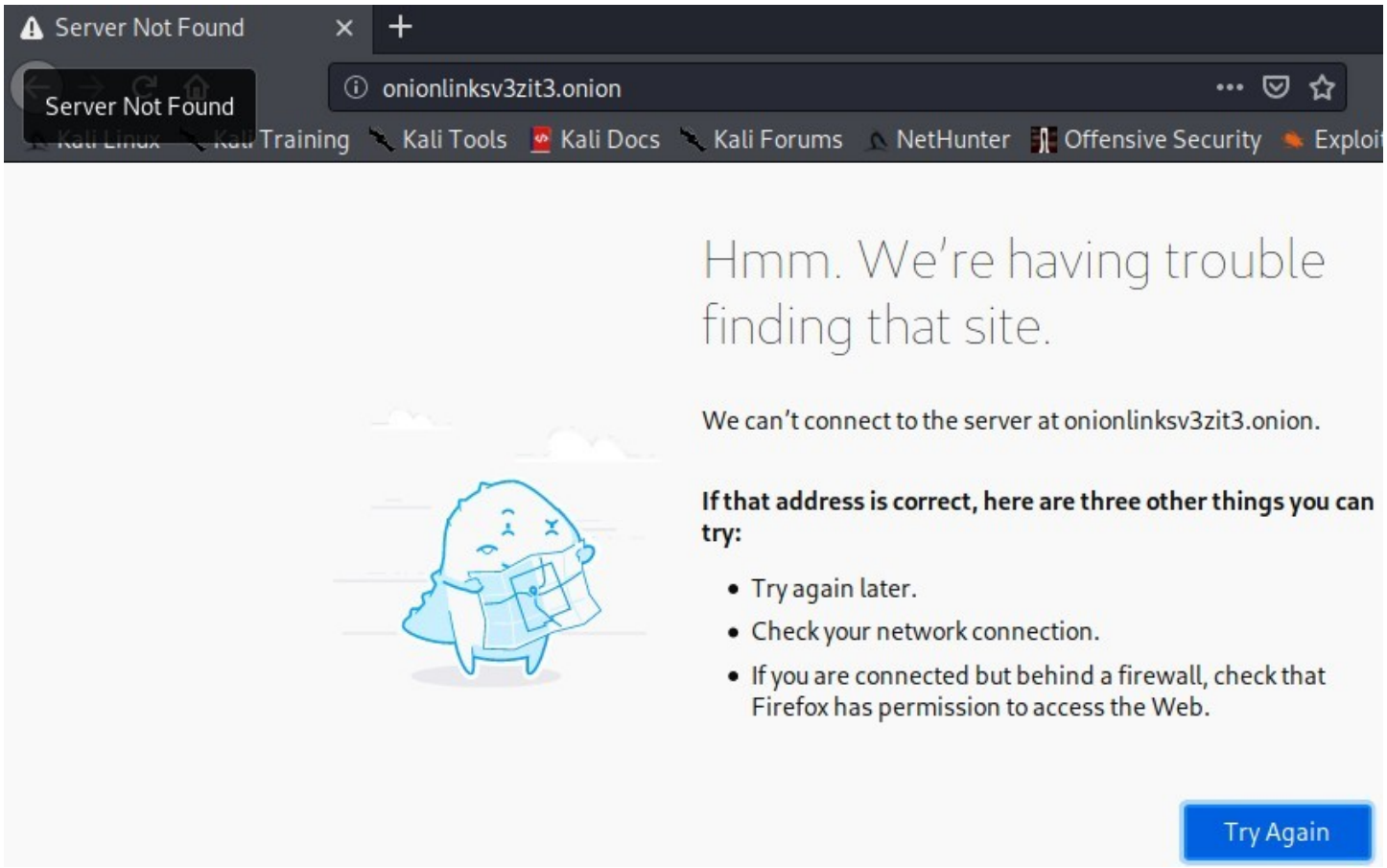
Una pagina web che ci permette di entrare nel dark web è ad esempio la seguente: https://thehiddenwiki.com

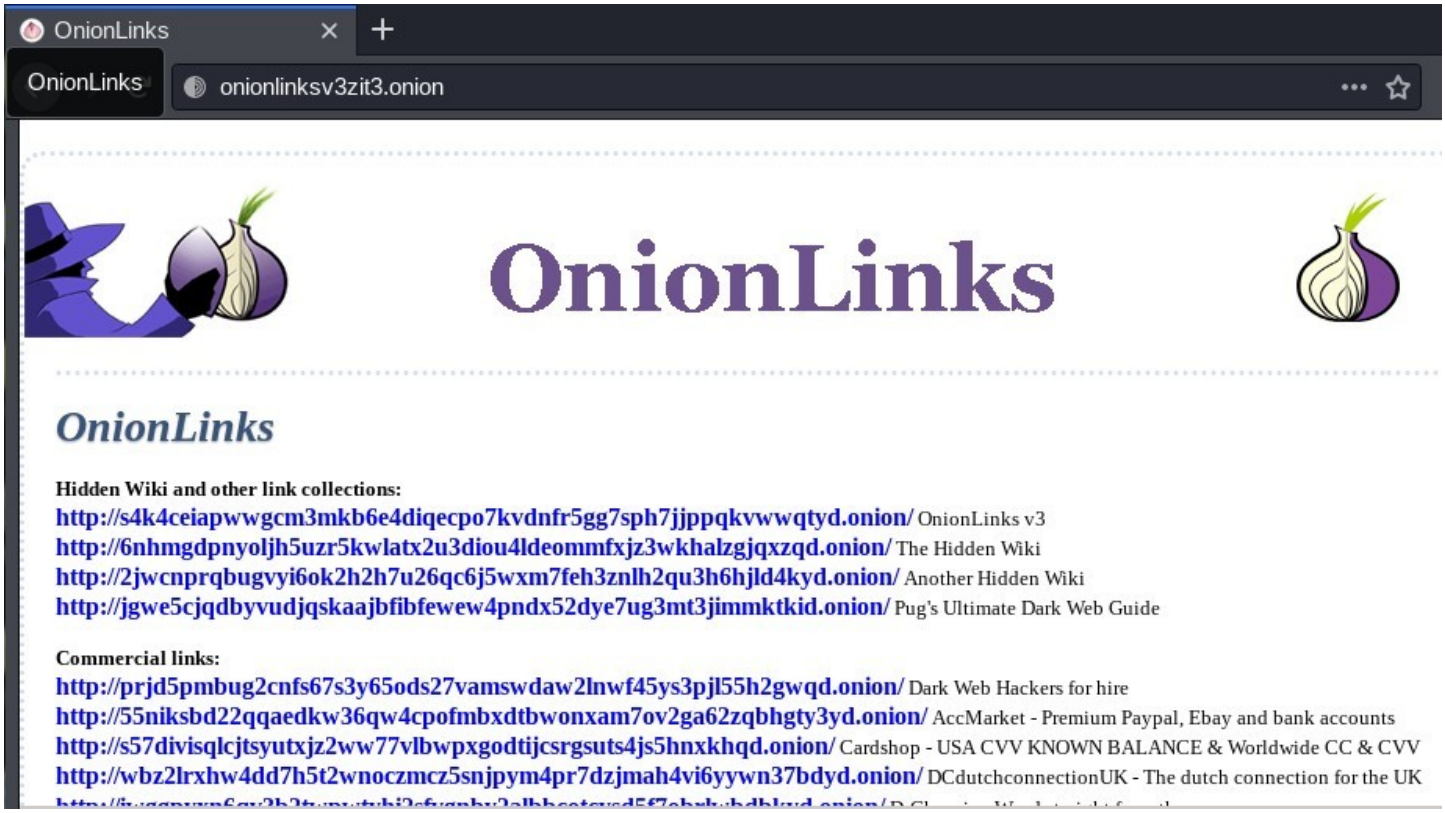


Cliccando su uno dei link potremo accedere ad un sito .onion.

Ma potremo farlo solo utilizzando il browser TOR, perché questi indirizzi non sono presenti nei normali DNS, pertanto facendo la stessa operazione con un browser diverso non riusciremo a raggiungere il sito.

Proviamo ad esempio a cliccare su “OnionLinks”, una pagina che contiene l’elenco di vari siti del dark web. Nelle due seguenti immagini ci sarà il risultato, la prima con un browser normale e la seconda con TOR.

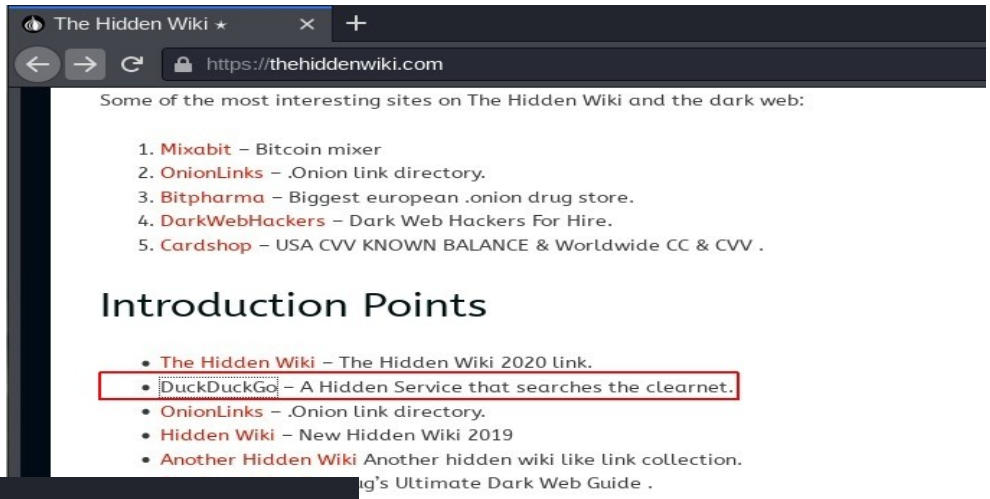


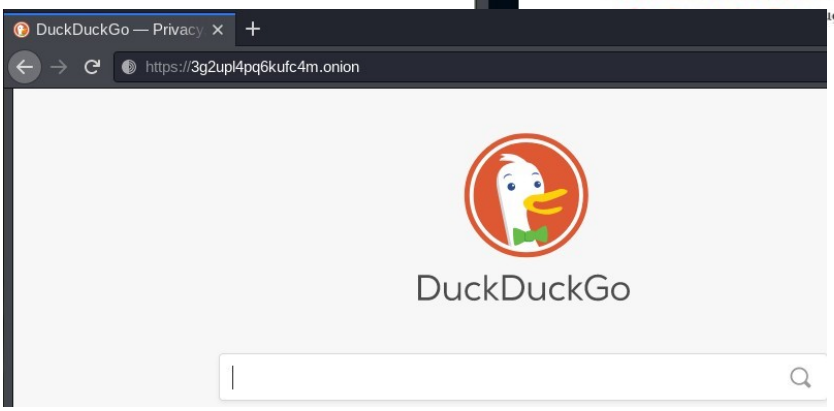


Come si può notare l’indirizzo nella barra degli indirizzi è lo stesso in entrambi i casi http://onionlinksv3zit3.onion/ ma un normale browser prova a risolvere l’indirizzo trovando il DNS, cosa che in questo caso non risulta possibile perché nel DNS non è presente questo sito.

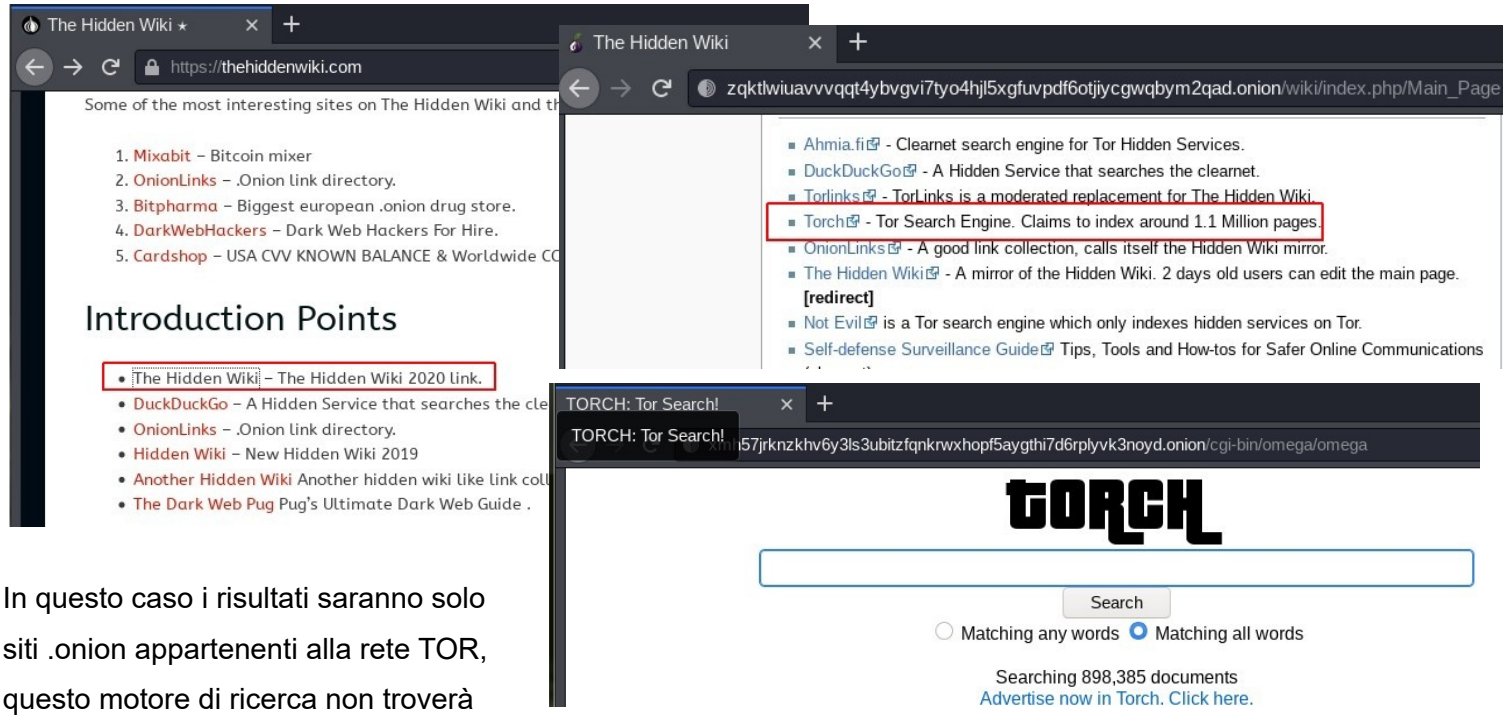
E così per tutti gli altri siti .onion, è come se dovessimo rintracciare l'indirizzo di una persona dall'elenco telefonico, se non è presente in elenco non possiamo ovviamente rintracciarla. I domini .onion sono pertanto disponibili solo dentro la rete TOR.

Il motore di ricerca che si può utilizzare nella rete TOR, è duckduckgo.com, con questo motore di ricerca non usciamo dalla rete TOR e non rischiamo di diventare visibili.





Ci sono anche motori di ricerca che lavorano solo sul dark web, partendo dalla pagina thehiddenwiki.com accediamo al link thehiddenwiki, e poi su torch.



In questo caso i risultati saranno solo siti .onion appartenenti alla rete TOR, questo motore di ricerca non troverà nessun sito appartenente alla classica rete web.

Torch non è l'unico motore di ricerca, tornando nella pagina thehiddenwiki sotto a torch troviamo NotEvil, che è un altro motore di ricerca dedicato solo alla rete TOR.

Da questo momento in poi, ci sono due problemi principali, uno è relativo alla sicurezza, ed il secondo è un problema etico.

Per essere più chiari è come se si entrasse in un mondo parallelo dove tutto è lecito, è ovvio che l'illegalità prolifera in determinati ambienti, pertanto il primo problema è la sicurezza personale. Il vostro PC pur se nascosto al mondo esterno non lo è in questo mondo parallelo, dove malintenzionati ed hacker potrebbero utilizzare qualche falla di sicurezza per entrare nella vostra macchina. Un po' come quando si va in una zona dove la percentuale degli scippi e dei furti è alta, la prima cosa da fare è tenere stretto il portafoglio.
In questo caso i consigli da seguire sono i seguenti:

1. Non utilizzare solamente TOR, ma anche una valida e sicura VPN, perciò non quelle gratuite ma quelle a pagamento (nulla viene regalato senza un motivo).

2. Possibilmente utilizzare un sistema operativo Linux, ancora meglio un sistema operativo Linux su macchina virtuale dentro una macchina con Linux. A pag.16 del seguente tutorial, viene descritto come istallare virtual box sulla macchina host, con Kali Linux sulla macchina virtuale.
   https://danielepostacchini.it/wp-content/uploads/2019/02/Analisi_reti_1.pdf

3. Coprire la webcam con un pezzetto di scotch, o chiuderla con l'apposito sportellino.

4. Modificare il percorso dei nodi di TOR durante la navigazione.

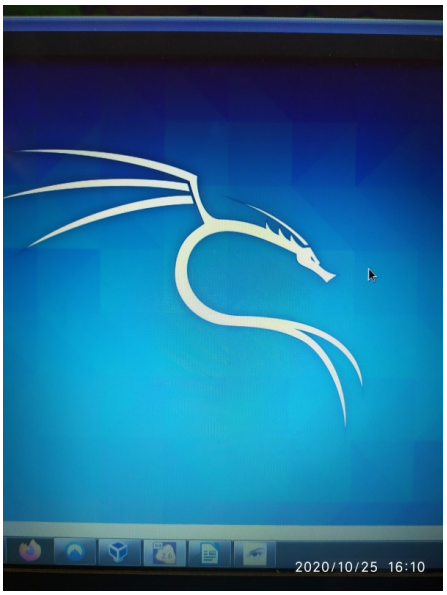
Insomma usare le massime precauzioni e la massima attenzione, soprattutto se ci si accorge di essere entrati in siti dove è meglio non essere. E da qui il secondo problema di carattere etico.
Purtroppo in un mondo senza controllo, si può avere l'anonimato e la privacy, ma si ha anche una proliferazione di contenuti illegali.
Anche involontariamente ci si può trovare in siti dove la tentazione di chiamare la polizia postale è molto alta, ma sicuramente gli stessi posti vengono monitorati dalle forze dell'ordine, e sicuramente è un arduo compito anche per loro.
Non si può restare indifferenti nel sapere che esistono sul serio siti dove si commercia di tutto, ed è triste vedere a che livello di miseria può arrivare la mente umana, per questo ho menzionato un probema di carattere etico, perché usare il dark web significa anche poter incappare, magari per un'eccessiva curiosità, in simili contenuti.
Per questo motivo anche solo realizzare questo tutorial può essere fonte di riflessione sull'opportunità di far conoscere o meno il modo di accedere a simili contenuti. Diciamo però che visto che il dark web è una realtà, spiegare correttamente il suo funzionamento, i suoi rischi ma anche i suoi vantaggi, potrebbe aiutare a fruire in maniera legale di questa struttura.

Si calcola che le dimensioni del materiale disponibile nel deep e dark web sia almeno 500 volte superiore di quello disponibile nel web normale, definito anche mondo sommerso. Cerchiamo perciò di vedere cosa potremmo cercare ed utilizzare in maniera del tutto lecita e legale.

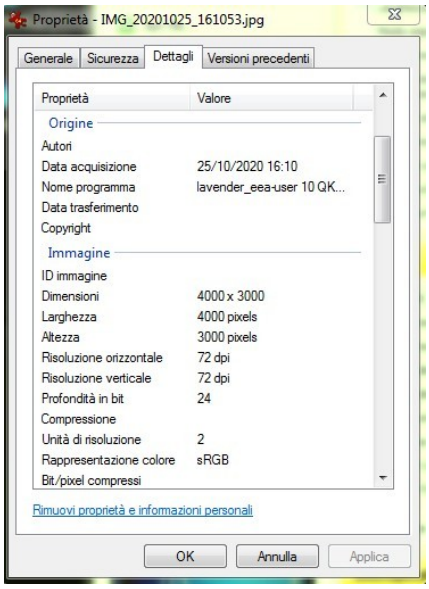
CONDIVISIONE DI FILE NEL DARK WEB

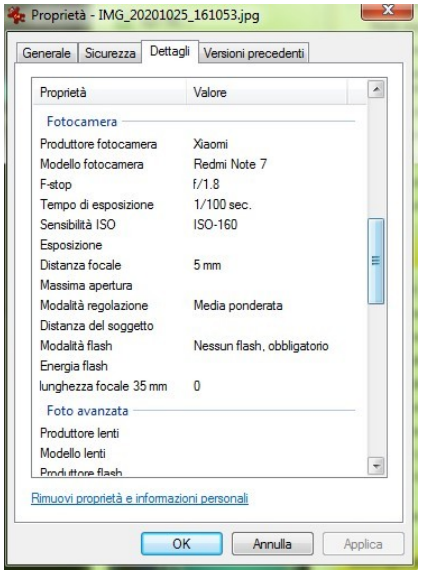
Uno dei problemi principali di internet, è la possibilità di scambiarsi dei file in assoluta sicurezza.
Innanzitutto bisogna sapere che un file non solo contiene i dati strettamente legati al contenuto del file. Facciamo un esempio se facciamo una foto con il telefonino, il file non conterrà solo i dati relativi ai pixel che compongono l'immagine, ma conterrà tante altre informazioni.

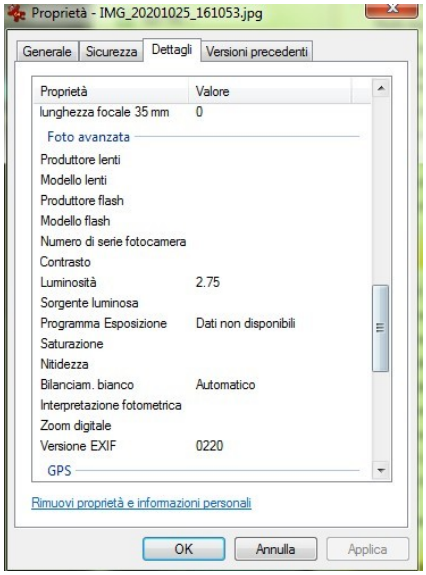
Proviamo a scattare un'immagine con il nostro telefonino e salviamola sul nostro PC.
E' una semplice foto dello sfondo della mia macchina virtuale con Kali Linux, ma se dovessi inviare questa foto a qualcuno, insieme ad essa invierei i suoi metadati.



I metadati sono una quantità variabile di informazioni allegati a qualsiasi file. Nell'esempio della foto, facendo click con il pulsante destro sul file, andando poi su "proprietà" e cliccando su "dettagli", avrò le seguenti informazioni.

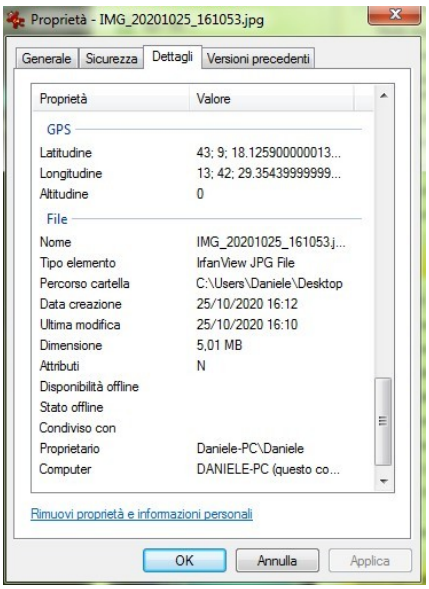






In pratica oltre alla foto vengono inviati informazioni sul tipo di fotocamera o dispositivo, risoluzione, data e ora, e spesso anche le coordinate GPS dove è stata scattata la foto.

Ci sono dei software con cui si possono avere maggiori informazioni uno dei tanti free, è PhotoME, ed in quel caso i metadati estrapolati dall'immagine sono davvero tanti, come vediamo nella pagina successiva.



JPEG | Immagine | Info-Miniatura | Fotocamera | GPS | Interoperability

Riepilogo

Nome File: C:\Users\Daniele\Desktop\IMG_20201025_161053.jpg
Tipo File: JPEG
Dimensione File: 5.138 KB
Data di creazione: 25/10/2020 16:10
Ultima modifica: 25/10/2020 16:10

Costruttore: Xiaomi
Modello: Redmi Note 7
Software: lavender_eea-user 10 QKQ1.190910.002 V11.0.1.0

Dimensione: 4000 x 3000 px (12 MP, 4:3)
Distanza focale: 4.74 mm
Diaframma: F1.8
Tempo d'esposizione: 1/100"
Sensibilità ISO: 160/23°
Programma: Esposizione automatica
Modo Esposizione: Media centrale ponderata
Bilanciamento Bianco: Auto
Flash: Flash non emesso, modalità flash forzata

Località: N43.155035, 13.708154

JPEG

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
Application Segment 1 (Exif)	0x00000006	E1	APP1	UNDEFINED(12099)
Define Quantization Table	<Dati binari>	DB	DQT	UNDEFINED(130)
Start of Frame	<Dati binari>	C0	SOF0	UNDEFINED(15)
Encoder	Unknown encoding software or device	C0	SOF[Encoder]	UNDEFINED(15)
Encoder Signature	F3235A7D187D083B7B7EAD949653F730:221111	C0	SOF[EncoderSignat...	UNDEFINED(15)
Color Mode	RGB color	C0	SOF[Colors]	UNDEFINED(15)
Subsampling ratio of Y to C	YCbCr4:2:0	C0	SOF[Subsampling]	UNDEFINED(15)
Encoding Process	Baseline DCT, Huffman coding	C0	SOF[n]	UNDEFINED(15)
Bits per Sample	8 bps	C0	SOF[P]	UNDEFINED(15)
Image Height	3000 px	C0	SOF[Y]	UNDEFINED(15)
Image Width	4000 px	C0	SOF[X]	UNDEFINED(15)
Number of image components in frame	3 comp.	C0	SOF[Nf]	UNDEFINED(15)
Define Huffman Table	<Dati binari>	C4	DHT	UNDEFINED(416)

Immagine

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
Modello Fotocamera	Redmi Note 7	0110	Model	ASCII(13)
Software	lavender_eea-user 10 QKQ1.190910.002 V11.0.1.0.QFGEUXM release-keys	0131	Software	ASCII(68)
Orientamento dell'immagine	90° senso antiorario (destra/alto)	0112	Orientation	SHORT
Data e ora di modifica del file	2020-10-25 16:10:53	0132	DateTime	ASCII(20)
Posizionamento Y e C	Centrato	0213	YCbCrPositioning	SHORT
Puntatore IFD Exif	0x0000010E	8769	ExifIFDPointer	LONG
Unità di risoluzione in X e Y	pollici	0128	ResolutionUnit	SHORT
Puntatore IFD GPS	0x00000B61	8825	GPSIFDPointer	LONG
Risoluzione orizzontale immagine	72 dpi	011A	XResolution	RATIONAL
Risoluzione verticale immagine	72 dpi	011B	YResolution	RATIONAL
Costruttore	Xiaomi	010F	Make	ASCII(7)

Info-Miniatura

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
Offset to JPEG SOI	0x00000CA7	0201	JPEGInterchangeFormat	LONG
Orientamento dell'immagine	90° senso antiorario (destra/alto)	0112	Orientation	SHORT
Bytes dei dati JPEG	8854 bytes	0202	JPEGInterchangeForm...	LONG
Schema compressione	JPEG (vecchio stile)	0103	Compression	SHORT
Unità di risoluzione in X e Y	pollici	0128	ResolutionUnit	SHORT
Risoluzione orizzontale immagine	72 dpi	011A	XResolution	RATIONAL
Risoluzione verticale immagine	72 dpi	011B	YResolution	RATIONAL

Fotocamera

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
???	118, 75, 110, 165, 158, 120, 54, 111, 15, 123, 144, 76, 49, 155, 115, 32, ...	9AAA		BYTE(2048)
Sensibilità ISO	160/23°	8827	ISOSpeedRatings	SHORT
Programma esposizione	Non definito	8822	ExposureProgram	SHORT
Numero F	F1.8	829D	FNumber	RATIONAL
Tempo di esposizione	1/100"	829A	ExposureTime	RATIONAL
???	{"mirror":false,"?sensor_type":"rear","Hdr":"off","OpMode":32769,"AIScene":0}	9999		ASCII(78)
Metodo di misurazione esposimetrica	0	A217	SensingMethod	SHORT
???	0	8895		SHORT
???	494145	9292		ASCII(7)
???	494145	9291		ASCII(7)
???	494145	9290		ASCII(7)
Lunghezza focale obiettivo	4.74 mm	920A	FocalLength	RATIONAL
Flash	Flash non emesso, modalità flash forzata	9209	Flash	SHORT
Modalità misurazione esposimetrica	Media centrale ponderata	9207	MeteringMode	SHORT
Tipo di cattura scena	Standard	A406	SceneCaptureType	SHORT
Interoperability IFD Pointer	0x00000B43	A005	InteroperabilityIFDPointer	LONG
Lunghezza focale in 35 mm	Unknown	A405	FocalLengthIn35mmFilm	SHORT
Data e ora di creazione dei dati digitali	2020-10-25 16:10:53	9004	DateTimeDigitized	ASCII(20)
Altezza immagine	3000 px	A003	PixelYDimension	LONG
Bilanciamento del Bianco	Auto	A403	WhiteBalance	SHORT
Data e ora di creazione dei dati originali	2020-10-25 16:10:53	9003	DateTimeOriginal	ASCII(20)
Luminosità	2.75 (6.7 fL)	9203	BrightnessValue	SRATIONAL
Larghezza immagine	4000 px	A002	PixelXDimension	LONG
Modo esposizione	Esposizione automatica	A402	ExposureMode	SHORT
Diaframma	1.69 Av (F1.8)	9202	ApertureValue	RATIONAL
Significato di ogni componente	YCbCr	9101	ComponentsConfiguration	UNDEFINED(4)
Spazio colore	sRGB	A001	ColorSpace	SHORT
Tipo scena	Immagine fotografata direttamente	A301	SceneType	UNDEFINED(1)

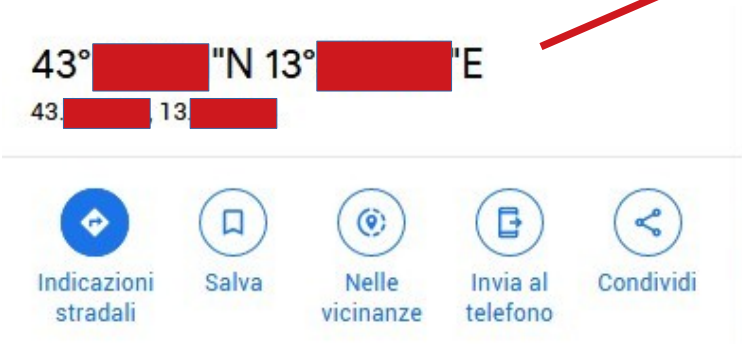
GPS

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
Latitudine Nord o Sud	Latitudine Nord	0001	GPSLatitudeRef	ASCII(2)
Latitudine	43° 09' 18.1259"	0002	GPSLatitude	RATIONAL(3)
Longitudine Est o Ovest	Longitudine Est	0003	GPSLongitudeRef	ASCII(2)
Longitudine	13° 42' 29.3544"	0004	GPSLongitude	RATIONAL(3)
Riferimento Altitudine	Livello del mare	0005	GPSAltitudeRef	BYTE
Altitudine	0 m	0006	GPSAltitude	RATIONAL
Ora GPS (orologio atomico)	15:10:29 UTC	0007	GPSTimeStamp	RATIONAL(3)
Name of GPS processing method	CELLID	001B	GPSProcessingMethod	UNDEFINED(15)
GPS date	2020-10-25 UTC	001D	GPSDateStamp	ASCII(11)

E dulcis in fundo, la posizione con tanto di pulsante per essere visualizzata su maps.

GPS

Campo	Valore	ID-Tag	Nome del Tag	Formato Dati
Latitudine Nord o Sud	Latitudine Nord	0001	GPSLatitudeRef	ASCII(2)
Latitudine	43° [redacted]	0002	GPSLatitude	RATIONAL(3)
Longitudine Est o Ovest	Longitudine Est	0003	GPSLongitudeRef	ASCII(2)
Longitudine	13° [redacted]	0004	GPSLongitude	RATIONAL(3)
Riferimento Altitudine	Livello del mare	0005	GPSAltitudeRef	BYTE
Altitudine	0 m	0006	GPSAltitude	RATIONAL
Ora GPS (orologio atomico)	15:10:29 UTC	0007	GPSTimeStamp	RATIONAL(3)
Name of GPS processing method	CELLID	001B	GPSProcessingMethod	UNDEFINED(15)
GPS date	2020-10-25 UTC	001D	GPSDateStamp	ASCII(11)





Credo di aver reso l'idea, ed i metadati sono contenuti in ogni tipo di file, compresi i documenti in word o pdf.

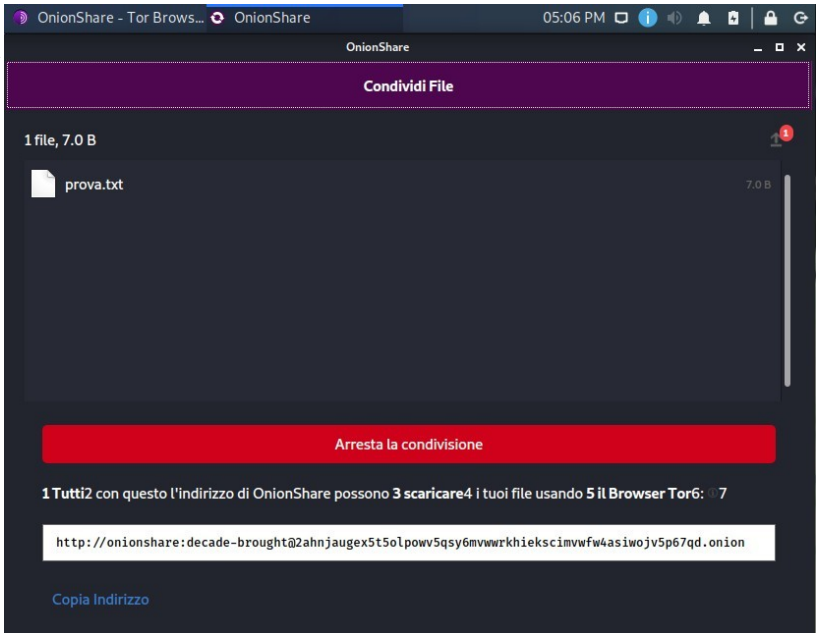
Viene da se l'inutilità di cercare di mantenere l'anonimato nella navigazione, se poi inviamo file contenenti tutte queste informazioni. Pertanto la prima cosa da fare (e questo vale in ogni caso non solo nel dark web) è di togliere tutti i metadati relativi alle informazioni più sensibili.
Per fare questo esistono diversi programmi che possiamo reperire in rete, digitiamo ad esempio "come eliminare i metadati" e sicuramente il buon Aranzulla o qualcun'altro ci saprà dare le indicazioni più aggiornate.

Una volta ripulito il file o i file dai metadati, per condividere un file utilizzando il dark web, possiamo installare il software onionshare, dal sito onionshare.org

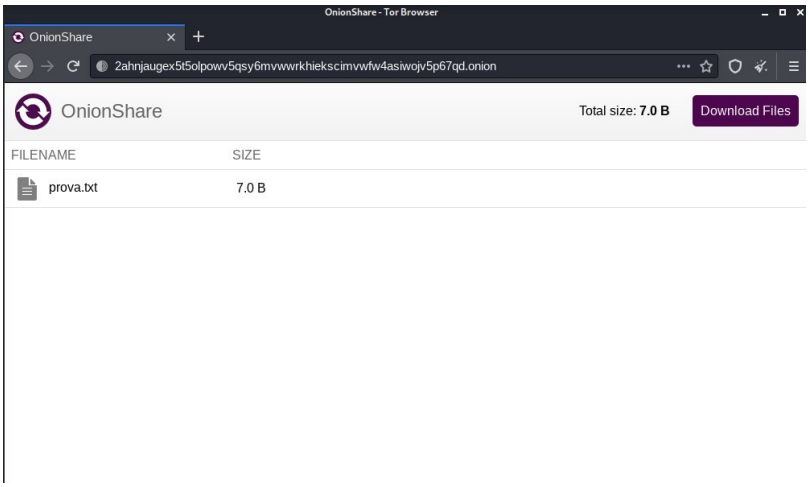


Il software è disponibile per Windows, Mac e Linux, in quest'ultimo caso, ad esempio su Ubuntu o su Kali, potrebbe essere installato da terminale con il comando: *sudo apt-get install onionshare*

Una volta installato, il software si connette alla rete TOR e mediante la sua interfaccia semplice ed intuitiva, permette il caricamento di uno o più file.
In basso ci sarà un pulsante verde "inizia la condivisione" e cliccando su di esso apparirà la schermata di fianco con il link che potrà essere inviato al destinatario.

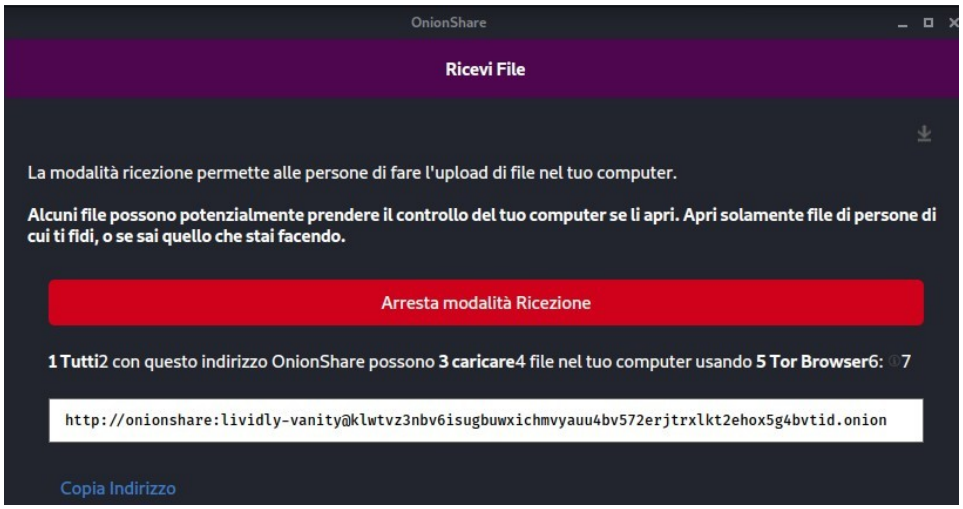


Il destinatario ricevuto il link può scaricare il file copiando il link nel uo browser TOR o utilizzando lo stesso programma onionshare.

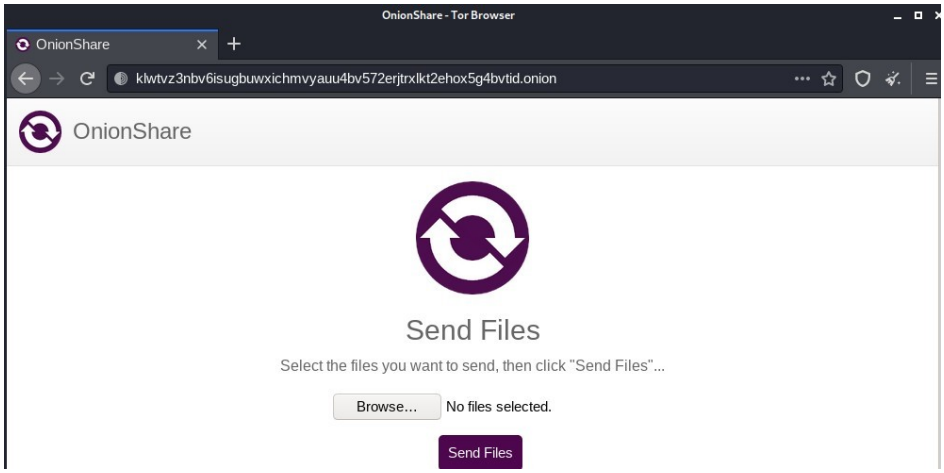


Il file sarà disponibile fino a quanto non arresteremo la sua condivisione con il pulsante rosso nella schermata.

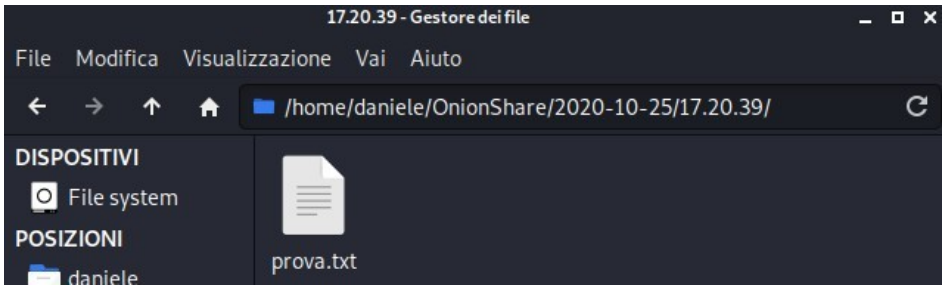
In maniera del tutto analoga, tramite onion share posso anche ricevere file, attivando la funzione ricevi file e non trasmetti file.
Anche in questo caso dovremo inviare il link a chi dovrà spedirci il file.



Dall'altra parte con il browser TOR verranno selezionati i file con il pulsante, ed inviati con "sent files".



In questo modo si crea un canale diretto e ciò che viene inviato lo troveremo nella cartella di download di onionshare.
Il canale rimane attivo fino a quanto non si arresta la modalità di ricezione.



E' consigliabile comunque lavorare da entrambi i lati con onionshare.

EMAIL ANONIME E SICURE

Uno dei problemi quando si accede a dei servizi o a delle pagine web, è quello di dover fornire la nostra email, per essere poi bombardati di pubblicità o altro. Se andate nella casella SPAM della vostra webmail, vi accorgerete che è sempre piena di posta inutile di ogni genere, ed oltre a questo a volte nella cartella ci vanno anche email che ci interessano, perché erroneamente classificate come SPAM.

Il dark web potrebbe aiutarci a diffondere la nostra email, solo nei casi in cui sia strettamente indispensabile, e solo in quei siti che non utilizzano la nostra email per fini pubblicitari.

Volendo accedere all'area riservata di un sito, ad esempio di un quotidiano di informazione, ci viene chiesto di registrarci con una mail.

In questo caso possiamo anche agire al di fuori del dark web, ad esempio nel il sito http://guerrillamail.com/ possiamo aprire e gestire temporaneamente una mail per usufruire dei servizi del sito e chiudere la mail quando non ne avremo più bisogno. Utilizzando il sito in oggetto tramite TOR avremo inoltre un maggiore grado di sicurezza in quanto la nostra navigazione nella rete web è comunque anonima.

Un'altra esigenza è invece quella di avere una mail permanente, ma anonima.

Sempre rimanendo nel surface web, cioè la rete normale, ci sono dei siti che offrono il servizio di email gratuita e criptata, ad esempio www.tutanota.com, o www.protonmail.com.

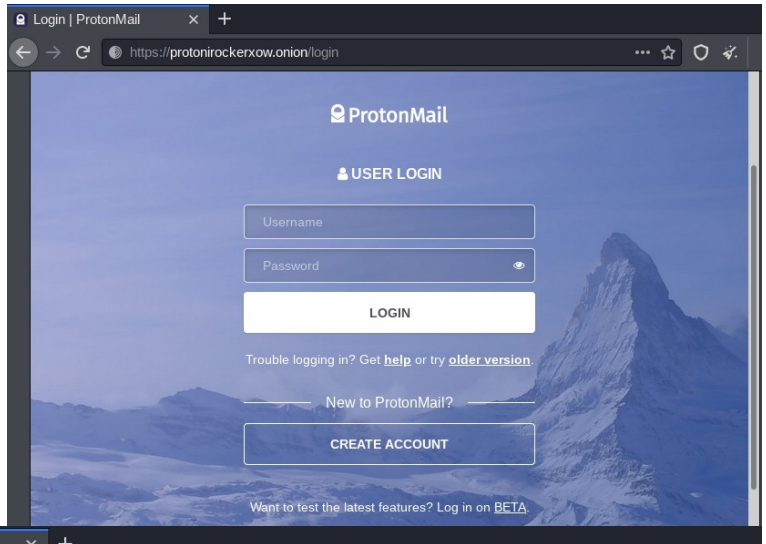
In entrambi i casi ci si può iscrivere e creare una email permanente, all'atto dell'iscrizione possiamo notare che a differenza di altri, vengono richieste pochissime informazioni, ed in entrambi i casi c'è possibilità di installare un client. Nel caso di Protonmail inoltre c'è la possibilità di usufruire di una buona VPN, ovviamente a pagamento.

Anche nel dark web ci sono diversi servizi relativi alle email, ad esempio lo stesso protonmail menzionato prima è presente nel dark web, in questo caso il dominio sarà .onion e l'indirizzo è il seguente:

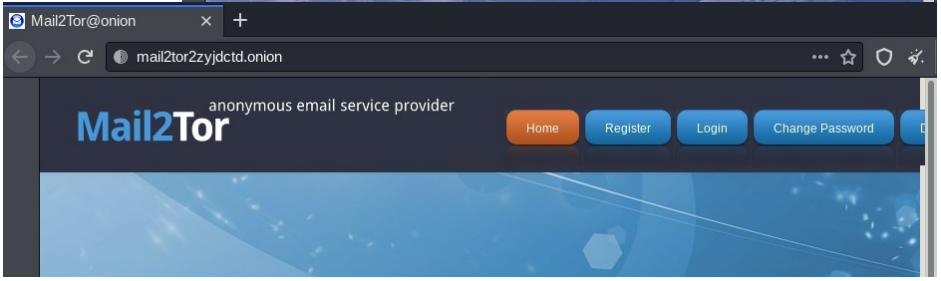
https://protonirockerxow.onion

A questo punto possiamo registrarci scegliendo il nostro indirizzo con dominio protonmail.

Una volta registrati, avremo la possibilità di inviare email al surface web, da dark web.



Un altro servizio che però consente lo scambio di email solo su piattaforma TOR, e cioè solo nel dark web, è mail2tor.



Il link onion di questo servizio, possiamo trovarlo con il motore di ricerca duckduckgo all'interno del browser TOR. Ed anche in questo caso occorre registrarsi e creare la propria mail. In questo caso operando solo al termine del dark web, avremo la massima sicurezza.

Conclusioni

Utilizzare il dark web, è oggi l'unica possibilità di avere un buon livello di anonimato, in questa rete nascosta troviamo inoltre molti servizi e contenuti, ma non dobbiamo dimenticare che i rischi relativi all'anonimato e alla sicurezza sono ancor più grandi che nel classico web.

Come ho già consigliato potrebbe essere un valido strumento insieme ad un'adeguata VPN, da utilizzare con una macchina virtuale con ambiente Linux.

Di seguito qualche immagine estratta dalla pagina di presentazione del dark web thehiddenwiki

Introduction Points

- Ahmia.fi - Clearnet search engine for Tor Hidden Services.
- DuckDuckGo - A Hidden Service that searches the clearnet.
- Torlinks - TorLinks is a moderated replacement for The Hidden Wiki.
- Torch - Tor Search Engine. Claims to index around 1.1 Million pages.
- OnionLinks - A good link collection, calls itself the Hidden Wiki mirror.
- The Hidden Wiki - A mirror of the Hidden Wiki. 2 days old users can edit the main page. **[redirect]**
- Not Evil is a Tor search engine which only indexes hidden services on Tor.
- Self-defense Surveillance Guide Tips, Tools and How-tos for Safer Online Communications (clearnet).

Email / Messaging

See also: The compendium of clear net Email providers.

- secMail.pro - Complete mail service that allows you to send and receive mails without violating your privacy.
- Mail2Tor - Mail2Tor is a free anonymous e-mail service made to protect your privacy.
- Elude.in - Elude.in is a privacy based email service and a Bitcoin/Monero exchange.
- TorBox - This is a hidden mailbox service only accessible from TOR without connection with public internet.
- BitMessage - Connects bitmessage and e-mail services. Registration only available using the clearweb link.
- Protonmail - Swiss based e-mail service, encrypts e-mails locally on your browser. Free and paid accounts.
- TorGuerrillaMail - Disposable Temporary E-Mail Address.

Books

- Example rendezvous points page - Thomas Paine's *Common Sense* and *The Federalist papers*.
- Traum library mirror - 60GB of Russian and English books. A mirror of the latest Traum ISO. Covers, search and downloads in FB2, HTML and plain TXT.
- ParaZite - Collection of forbidden files and howto's (pdf, txt, etc.).
- Jotunbane's Reading Club "All your ebooks belong to us!".
- Liberated Books and Papers A small collection of hard to find books.
- Clockwise Library A collection of art and science books.
- The Last of PAPYREFB2 A collection of mostly Spanish books.
- Paul Dreyer's eBook Library - DRM-Free Growing eBook Library, mostly in ePub format.
- BB Compendium - A collection of chemistry, drugs, explosives, fireworks, pyrotechnics, science, and weapons related documents.
- The Incorrect Library - 1100 books (and counting...) Beautifully prepared in E-Pub format, with a focus on publishing politically incorrect books.
- Comic Book Library - Collection of comic books, largely independent.
- The Library A collection of hard to find books.
- Bible - several links for downloading versions of the Bible.
- Libraries A more complete list.