

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

**Objectif** : Installer et utiliser **Tor Browser** (Navigateur Tor) pour naviguer sur le **dark web** (sites en .onion), protéger votre anonymat, contourner la censure et comprendre les limites de la navigation privée classique.

**Public visé** : Intermédiaire (curieux, journalistes, activistes, ou toute personne souhaitant un anonymat renforcé)

**Temps estimé** : 20 à 30 minutes

**Niveau de difficulté** : ★★☆☆☆ (Facile – l'installation est simple, mais la compréhension des concepts est importante)

**Prérequis** : Une connexion Internet. Avoir lu la fiche N°11 (navigateur privé) est un plus.

### 1. Qu'est-ce que le dark web ? (Clarifications)

#### Les trois couches du web

Couche	Accès	Exemples	Contenu
<b>Web de surface</b> (Surface Web)	Navigateur classique (Chrome, Firefox, Edge)	<a href="https://www.google.com">google.com</a> , <a href="https://www.wikipedia.org">wikipedia.org</a> , le <a href="https://www.monde.fr">monde .fr</a>	Pages indexées par les moteurs de recherche (environ 4-5 % du web total)
<b>Web profond</b> (Deep Web)	Navigateur classique, mais pages non	votre boîte mail, votre espace bancaire, bases de données académiques, pages privées	Contenu accessible mais non référencé (mots de passe requis, formulaires,

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Couche	Accès	Exemples	Contenu
	indexées		etc.) – <b>rien d'illégal en soi</b>
<b>Dark web</b> (Darknet)	Navigateur spécial (Tor Browser, I2P, Freenet)	sites en .onion (Tor), .i2p (I2P)	Sites volontairement cachés, anonymes, non indexés. <b>Certains sont illégaux</b> (marchés de drogue, armes, données volées), d'autres sont légitimes (Whistleblowing, forums de hackers éthiques, services protégés).

**Important** : Le dark web n'est **pas** illégal en soi. Naviguer sur des sites .onion n'est pas un délit. Ce qui est illégal, ce sont les activités que vous y menez (achat de produits interdits, consultation de contenus pédopornographiques, etc.). Tor Browser est un outil **neutre**, comme un couteau de cuisine.

## 2. Qu'est-ce que Tor Browser ?

**Tor** (The Onion Router) est un réseau **anonyme** qui fait passer votre trafic Internet à travers **plusieurs relais** (au moins 3) chiffrés, comme les couches d'un oignon (d'où le nom).

**Tor Browser** est une version modifiée de Firefox, préconfigurée pour :

- **Router tout le trafic via le réseau Tor.**

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

- **Bloquer les traqueurs** (fingerprinting, scripts, cookies tiers).
- **Uniformiser l'empreinte numérique** (tous les utilisateurs de Tor Browser ont la même empreinte, ce qui empêche l'identification individuelle).
- **Effacer toutes les données** à la fermeture (historique, cookies, cache).

### Ce que Tor Browser protège :

Information	Sans Tor	Avec Tor Browser
Adresse IP	Visible par le site web	Masquée (remplacée par celle du dernier relais Tor)
Localisation	Visible (via IP)	Masquée
Historique de navigation	Stocké localement	Effacé à la fermeture
Traqueurs	Présents (cookies tiers, fingerprinting)	Bloqués (sauf si désactivé manuellement)
Site visité	Visible par votre FAI	Le FAI voit que vous utilisez Tor, mais pas quel site vous visitez

### Ce que Tor Browser ne protège pas :

Risque	Explication
Logiciels malveillants	Tor Browser ne vous protège pas si vous téléchargez un virus.
Phishing	Les sites .onion peuvent être faux (usurpation d'identité). Vérifiez les URL.
Déanonymisation par un adversaire puissant	Si un attaquant contrôle plusieurs relais Tor (ou surveille le trafic entrant/sortant), il peut théoriquement corréler les données. Cela reste très difficile et coûteux (agences étatiques uniquement).
Comportement utilisateur	Si vous vous connectez à votre compte Google (ou Facebook) via Tor Browser, vous êtes identifié. Tor cache votre IP, pas votre identité déclarée.

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

### 3. À quoi sert Tor Browser (cas d'usage légitimes) ?

Cas d'usage	Explication
<b>Contournement de la censure</b>	Dans les pays où l'accès à certains sites est bloqué (Chine, Russie, Iran, Turquie, etc.), Tor Browser permet d'y accéder.
<b>Protection des lanceurs d'alerte</b>	Les journalistes et lanceurs d'alerte (Edward Snowden, etc.) utilisent Tor pour communiquer anonymement.
<b>Recherche d'informations sensibles</b>	Un citoyen peut rechercher des informations sur des sujets sensibles (maladies, questions intimes) sans que son FAI ou Google ne le sache.
<b>Consultation de sites .onion légitimes</b>	Facebook (facebookcorewwwi.onion), The New York Times, BBC, ProtonMail, Riseup, etc. ont des versions .onion.
<b>Protection des sources journalistiques</b>	Un journaliste peut recevoir des documents anonymement via SecureDrop (système utilisant Tor).
<b>Simple curiosité</b>	Explorer le dark web (sans participer à des activités illégales) est légal et instructif.

**Avertissement : Ne téléchargez pas de fichiers** (surtout des .exe) depuis des sites douteux. **Ne donnez pas d'informations personnelles** (nom, email, mot de passe). **N'utilisez pas Tor Browser** pour des activités illégales.

### 4. Comment faire ? (Pas à pas)

#### Étape 1 : Téléchargez Tor Browser

 **Attention : Téléchargez UNIQUEMENT depuis le site officiel.**

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Site officiel	<a href="https://torproject.org">torproject.org</a> (ou <a href="https://torproject.org/fr">torproject.org/fr</a> pour la version française)
Ne jamais télécharger depuis des sites tiers	Les versions modifiées peuvent contenir des malwares ou des backdoors.

1. Rendez-vous sur [torproject.org](https://torproject.org) .
2. Cliquez sur "**Télécharger Tor Browser**" .
3. Le site détecte automatiquement votre système (Windows, macOS, Linux, Android).
4. Téléchargez le fichier (environ 100 Mo).

**Sur Android** : Tor Browser est disponible via **Google Play** (le projet Tor le certifie) ou **F-Droid** (recherchez "Tor Browser"). Mais préférez **Orbot** + **Orfox** (l'ancien) ou **Tor Browser** directement.

**Sur iOS** : Tor Browser n'existe pas (Apple interdit les navigateurs autres que Safari comme moteur de rendu). Utilisez **Onion Browser** (recommandé par le projet Tor, payant ~1-2 €).

### Étape 2 : Installez Tor Browser

#### Windows / macOS :

- Double-cliquez sur le fichier `.exe` (Windows) ou `.dmg` (macOS).
- Suivez l'assistant d'installation (choisissez la langue, l'emplacement d'installation).
- Une fois installé, lancez Tor Browser (icône oignon).

#### Linux (Ubuntu / Mint) :

*# Extrayez l'archive*

```
tar -xf tor-browser-linux64-xx.x.x.tar.xz
```

*# Lancez le script*

```
cd tor-browser_xx.x.x/
```

```
./start-tor-browser.desktop
```

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

### Étape 3 : Lancez Tor Browser (connexion au réseau Tor)

1. Au premier lancement, une fenêtre "**Connexion au réseau Tor**" s'affiche.
2. Cliquez sur "**Se connecter**" (dans la plupart des pays, pas de configuration supplémentaire).
- Si vous êtes dans un pays censuré (Chine, Russie, Iran, etc.), cochez "**Configurer Tor**" et entrez un pont (bridge) pour contourner la censure.
3. Tor Browser tente de se connecter au réseau (quelques secondes à quelques dizaines de secondes).
4. Une fois connecté, le navigateur s'ouvre (interface basée sur Firefox).

**Premier lancement** : Lisez l'onglet "**Tor a démarré**" qui explique les bases.

### Étape 4 : Naviguez sur le web normal (surface web) avec Tor

- **Barre d'adresse** : tapez `check.torproject.org` – le site vous confirme que vous utilisez Tor.
- **Recherche** : DuckDuckGo est le moteur de recherche par défaut (privé).
- Vous pouvez naviguer sur n'importe quel site normal ([google.com](https://google.com) , [lemonde.fr](https://lemonde.fr) , etc.) – mais votre FAI ne saura pas que vous visitez ces sites (il saura seulement que vous utilisez Tor).

**Pourquoi utiliser Tor pour le web normal ?** : Pour protéger votre anonymat (votre FAI et Google ne verront pas votre navigation). Mais Tor Browser est **plus lent** qu'un navigateur normal (en raison du routage via plusieurs relais).

### Étape 5 : Accédez aux sites .onion (dark web)

- Les sites `.onion` sont des adresses spéciales (ex: `facebookcorewwwi.onion`).
- **Comment trouver des adresses .onion légitimes ?**

Méthode	Explication
Sites d'information officiels	The New York Times, BBC, ProtonMail, Facebook publient leurs adresses <code>.onion</code> sur leur site normal.

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Méthode	Explication
Wiki index (légitimes)	thehiddenwiki.org (attention : beaucoup de liens morts ou malveillants).
Moteurs de recherche dark web	Ahmia (ahmia.fi) – moteur de recherche indexant des sites .onion légitimes (développé par des militants de la vie privée).

### Exemples de sites .onion légitimes (vérifiés) :

Site	URL .onion (à vérifier sur leur site officiel)
Facebook	facebookcorewwwi.onion
ProtonMail	protonmailrmez3lotccipshtkleetolb73fuirgj7r4o4vfu7ozyd.onion
The New York Times	nytimes3xbfgragh.onion
BBC	bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion
DuckDuckGo	duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion
Riseup	j6om4j2jl7h5b2zw.onion

### Navigation :

- Copiez-collez l'adresse .onion dans la barre d'adresse.
- Attendez que Tor la résolve (quelques secondes).
- Le site s'affiche (souvent basique, pas de JavaScript).

### Étape 6 : Ajustez le niveau de sécurité

Tor Browser a 3 niveaux de sécurité (icône bouclier à droite de la barre d'adresse) :

Niveau	Javascript	Polices	Images	Recommandation
Standard (par défaut)	Activé (certains sites fonctionnent)	Activé	Activées	Pour la navigation générale (surface web)
Plus sûr	Désactivé sur les sites	Désactivé	Bloquées	Pour le dark web (réduit les

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Niveau	Javascript	Polices	Images	Recommandation
	non HTTPS			risques)
<b>Le plus sûr</b>	Désactivé sur tous les sites	Désactivé	Bloquées	Pour les usages sensibles (whistleblowing)

**Recommandation pour le dark web** : Passez en niveau **"Plus sûr"** (désactive JavaScript). Beaucoup de sites .onion ne nécessitent pas JavaScript. Cela réduit les risques de déanonymisation par des scripts malveillants.

### Étape 7 : Fermez Tor Browser (effacement automatique)

- Quand vous fermez Tor Browser, **toutes** vos données sont effacées (historique, cookies, caches, mots de passe).
- La prochaine fois, vous repartez de zéro (nouvelle identité).

**"Nouvelle identité"** : Si vous voulez changer d'identité sans fermer le navigateur, cliquez sur l'icône oignon en haut à gauche → **"Nouvelle identité"** . Tor redémarre, nouvelle IP de sortie, tous les onglets fermés.

## 5. Sécurité et bonnes pratiques sous Tor

Règle	Pourquoi
<b>Ne téléchargez pas de fichiers</b> (sauf depuis des sources absolument fiables)	Les fichiers (.exe, .pdf, .doc) peuvent contenir des malwares ou des scripts qui vous déanonymisent.
<b>Ne maximisez pas la fenêtre</b>	La résolution de votre écran peut être utilisée pour vous identifier (fingerprinting). Laissez la fenêtre à sa taille par défaut.
<b>Ne désactivez pas les paramètres par défaut</b>	Ne touchez pas aux réglages de sécurité (sauf pour passer en niveau "Plus sûr").

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Règle	Pourquoi
<b>N'installez pas d'extensions</b>	Pas de uBlock, pas de LastPass, rien. Les extensions peuvent vous déanonymiser.
<b>N'utilisez pas Tor Browser pour les comptes personnels</b>	Si vous vous connectez à votre Gmail, votre identité est liée à la session Tor (même si votre IP est masquée). Pour l'anonymat, créez des comptes jetables.
<b>Ne désactivez pas JavaScript (sauf si vous passez en niveau "Plus sûr")</b>	Sur le dark web, certains sites malveillants exploitent JS pour révéler votre IP. Passez en niveau "Plus sûr".
<b>Utilisez Tor Browser uniquement pour l'anonymat</b>	Pour la navigation quotidienne (YouTube, Reddit, etc.), préférez Firefox + uBlock Origin (fiche N°11). Tor Browser est trop lent et trop restrictif pour un usage quotidien.

### 6. Limitations de Tor Browser

Limitation	Explication
<b>Lent</b>	Le trafic passe par 3 relais (parfois plus). La latence est élevée. Les vidéos (YouTube) sont impossibles à regarder en streaming.
<b>Certains sites bloquent Tor</b>	De nombreux sites (Cloudflare, Netflix, banques) bloquent les relais de sortie Tor (considérés comme suspects).
<b>Pas de WebRTC</b>	Certaines applications de chat nécessitent WebRTC (désactivé pour protéger votre IP).
<b>Pas de support des DRM (Netflix, etc.)</b>	Impossible de regarder du contenu protégé.
<b>Les .onion peuvent être dangereux</b>	De nombreux sites .onion sont des arnaques, des phishing, ou des malwares. <b>Ne donnez jamais vos informations personnelles</b> (carte bancaire, mot de passe).

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

### 7. Tableau récapitulatif : navigateurs et anonymat

Navigateur	Anonymat	Vitesse	Blocage pub/traqueurs	Idéal pour
Chrome / Edge	✗ Nul	★★★★★	✗	Usage quotidien (si vous acceptez le traçage)
Firefox + uBlock (fiche N°11)	⚠ Bon (contre les traqueurs, mais votre FAI voit tout)	★★★★☆	✓	Usage quotidien, vie privée basique
Brave (fiche N°11)	⚠ Bon (bloqueurs intégrés)	★★★★☆	✓	Usage quotidien, mobile
Tor Browser	✓ Excellent (anonymat fort)	★★★☆☆	✓ (bloqueurs)	Dark web, contournement censure, whistleblowing
LibreWolf (fiche N°11)	⚠ Très bon (mais FAI voit tout)	★★★☆☆	✓	Utilisateurs avancés, vie privée renforcée

### 8. À savoir avant de se lancer

Crainte fréquente	La réalité
"Tor Browser est illégal."	<b>Faux.</b> Tor Browser est <b>légal</b> en France et dans la plupart des démocraties. L'utiliser n'est pas un délit. Ce qui est illégal, ce sont les activités que vous menez (achat de drogues, etc.).
"Mon FAI va me surveiller si"	Les FAI voient que vous utilisez Tor (le protocole est identifiable). Dans certains pays (Chine, Russie), Tor est bloqué ou surveillé. En France,

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Crainte fréquente	La réalité
j'utilise Tor."	aucun problème.
"Je suis totalement anonyme avec Tor Browser."	<b>Non.</b> Tor Browser vous protège de la plupart des menaces, mais pas de toutes. Si vous vous connectez à votre compte Google, votre anonymat est brisé. Si un logiciel malveillant exploite une faille, votre IP peut être révélée. Pour un anonymat quasi-total, combinez Tor Browser + Tails (système d'exploitation amnésique) sur une clé USB.
"Tor Browser est trop lent, c'est normal ?"	Oui. La latence est élevée. Ne l'utilisez pas pour le streaming ou les téléchargements lourds.
"Puis-je utiliser Tor Browser avec un VPN ?"	C'est <b>déconseillé</b> (sauf cas spécifiques). Le VPN ajoute une couche, mais peut casser l'anonymat (le VPN vous identifie). L'équipe Tor recommande Tor Browser <b>seul</b> . Si vous êtes dans un pays censuré, utilisez des <b>bridges</b> (configurés dans Tor Browser).
"J'ai peur de tomber sur des contenus illégaux."	Ne cliquez pas sur des liens suspects. Utilisez des moteurs comme Ahmia (filtre les sites illégaux). Si vous tombez accidentellement sur un contenu illégal (ex: photo d'enfant), fermez immédiatement le navigateur (et signalez-le si vous le souhaitez). Votre simple visite (sans téléchargement) n'est généralement pas poursuivie (mais la loi varie selon les pays).

### 9. Challenge 7 jours (découverte du dark web)

**Challenge :** Pendant 7 jours, utilisez Tor Browser pour explorer le dark web (uniquement des sites légitimes).

**Jour 1 :** Téléchargez et installez Tor Browser. Lancez-le. Vérifiez votre IP sur [check.torproject.org](https://check.torproject.org) – elle doit être différente de votre IP réelle.

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

**Jour 2 :** Naviguez sur des sites normaux ( [lemonde.fr](http://lemonde.fr) , [wikipedia.org](http://wikipedia.org) ) avec Tor Browser. Comparez la vitesse avec Firefox.

**Jour 3 :** Connectez-vous au site Facebook [.onion](http://facebookcorewwwi.onion) ([facebookcorewwwi.onion](http://facebookcorewwwi.onion)). Créez un compte jetable (ou connectez-vous si vous acceptez de perdre l'anonymat).

**Jour 4 :** Utilisez le moteur de recherche **Ahmia** ([ahmia.fi](http://ahmia.fi)) pour trouver des sites [.onion](http://.onion) légitimes (ex: DuckDuckGo, ProtonMail, BBC).

**Jour 5 :** Passez le niveau de sécurité à "**Plus sûr**" (désactive JavaScript). Visitez un site [.onion](http://.onion). Remarquez que certains sites se cassent (ceux qui dépendent de JS).

**Jour 6 :** Utilisez la fonction "**Nouvelle identité**". Vérifiez que votre IP (sur [check.torproject.org](http://check.torproject.org)) a changé.

**Jour 7 :** (Optionnel) Installez **Tails** (système d'exploitation) sur une clé USB – étape suivante pour l'anonymat extrême.

### À la fin :

- Vous comprenez les bases de Tor et du dark web.
- Vous savez utiliser Tor Browser en sécurité (niveau de sécurité, bonnes pratiques).
- Vous avez constaté les limites (lenteur, sites cassés).

## 10. Alternatives et approfondissements

Si vous avez besoin de...	Essayez plutôt...
Un niveau d'anonymat plus fort (ordinateur dédié)	<b>Tails</b> ( <a href="http://tails.net">tails.net</a> ) : système d'exploitation amnésique (clé USB) qui route <b>tout</b> le trafic via Tor, n'écrit rien sur le disque dur.
Un navigateur plus léger (pour mobiles)	<b>Orbot</b> (Android) + <b>Orfox</b> (obsolète, remplacé par Tor Browser).

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Si vous avez besoin de...	Essayez plutôt...
<b>Contourner la censure (sans Tor)</b>	Utilisez un <b>VPN</b> (Proton VPN, Mullvad – fiches N°4, N°5) ou un <b>bridge</b> Tor.
<b>Le dark web sans navigateur (API)</b>	<b>Torsocks</b> (forcer une application à utiliser Tor).
<b>Le réseau I2P</b> (alternative à Tor)	<b>I2P</b> (geti2p.net) – anonymat basé sur une infrastructure différente (plus adaptée au partage de fichiers).
<b>Naviguer de façon privée sans dark web</b>	<b>Firefox + uBlock Origin</b> (fiche N°11) ou <b>Brave</b> (fiche N°11).

### 11. En résumé (ce que vous gagnez)

Action	Bénéfice
Installer <b>Tor Browser</b>	Naviguer anonymement (IP masquée, localisation cachée, traqueurs bloqués)
Accéder aux <b>sites .onion</b>	Découvrir le dark web (légal), consulter des services anonymes (SecureDrop, Facebook onion, etc.)
Contourner la <b>censure</b> (bridges)	Accéder à Internet librement depuis les pays censurés (Chine, Russie, Iran, Turquie)
Utiliser le niveau " <b>Plus sûr</b> "	Désactiver JavaScript – réduire les risques de déanonymisation
Utiliser <b>Tails</b> (optionnel)	Anonymat extrême – système d'exploitation complet sur clé USB, sans laisser de traces

### Conclusion générale

Si vous êtes...	Choisissez...
<b>Un citoyen lambda (vie)</b>	<b>Firefox + uBlock Origin</b> (fiche N°11) – pas besoin de Tor pour

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

Si vous êtes...	Choisissez...
privée quotidienne)	la navigation normale. Tor est trop lent.
Un journaliste / lanceur d'alerte	<b>Tor Browser</b> (ou <b>Tails</b> + Tor Browser) – pour protéger vos sources et votre identité.
Un voyageur dans un pays censuré	<b>Tor Browser</b> avec <b>bridges</b> (ou <b>VPN</b> si Tor est bloqué).
Un curieux (découvrir le dark web)	<b>Tor Browser</b> (ne téléchargez rien, ne donnez pas d'infos persos).
Un militant / activiste	<b>Tails</b> (clé USB) + <b>Tor Browser</b> – pour un anonymat quasi total.

### À retenir absolument :

- **Le dark web n'est pas que le "web criminel"**. Il existe de nombreux sites légitimes (Facebook, ProtonMail, BBC, etc.) qui protègent leur accès via .onion.
- **Tor Browser = anonymat, pas sécurité absolue**. Ne téléchargez pas de fichiers. Ne désactivez pas les paramètres de sécurité.
- **Tor Browser est lent**. Ne l'utilisez pas pour YouTube ou Netflix.
- **Utilisez Tor Browser dans un but légal**. L'anonymat est un droit, pas un privilège.
- **Pour un anonymat quasi-parfait** : Tails (clé USB) + Tor Browser (avec niveau de sécurité "Plus sûr") + aucun compte personnel connecté.

### Test final :

1. Téléchargez Tor Browser depuis [torproject.org](https://torproject.org).
2. Lancez-le, connectez-vous au réseau Tor.
3. Rendez-vous sur [check.torproject.org](https://check.torproject.org). Vous devez voir : "You are using Tor. Your IP address appears to be: xx.xx.xx.xx" (une IP qui n'est pas la vôtre).
4. Rendez-vous sur [facebookcorewwi.onion](https://facebookcorewwi.onion). Le site Facebook doit s'afficher (version texte, sans JS).
5. (Optionnel) Rendez-vous sur [duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion](https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion) (DuckDuckGo .onion).
6. Fermez Tor Browser. Rouvrez-le. Votre historique doit être vide.

## Fiche Pratique N°27 : Naviguez légalement sur le dark web avec Tor Browser – Découvrez l'anonymat fort et les sites .onion V1.0

7. Si tout fonctionne : **vous avez les bases de Tor** ✓