

Hypertext Transfer Protocol (HTTP): haladó lehetőségek

Jeszenszky Péter
Debreceni Egyetem, Informatikai Kar
jeszenszky.peter@inf.unideb.hu

Utolsó módosítás: 2024. december 4.

Tartalom

- Sütik
- Webes követés
- Eredet
- Kapcsolatkezelés

Süti (1)

- **Süti (*cookie*):**
 - Egy név-érték pár és kapcsolódó metaadatok (attribútumok), melyeket egy eredet szerver egy válasz Set -Cookie fejlécmezőjében küld a felhasználói ágensnek.
 - Az attribútumok segítségével az eredet szerver egy hatáskört határozhat meg a sütihez.
 - A felhasználói ágens a további kérésekben a név-érték párt a Cookie fejlécmezőben küldi vissza az eredet szervernek.
- A jelenleg aktuális specifikáció:
 - Adam Barth. *RFC 6265: HTTP State Management Mechanism*. April 2011. <https://www.rfc-editor.org/rfc/rfc6265>
 - A Cookie és a Set -Cookie és fejlécmezők definiálása.

Sütik (2)

- Felhasználás:
 - Munkamenet kezelés
 - Testreszabás
 - Webes követés (lásd a Referer fejlécmezőt)

Sütik (3)

- Információk sütikről (süti adatbázisok):
 - *CookieSearch* <https://cookiestearch.org/>
 - Példa: YSC
<https://cookiestearch.org/cookies/?cookie-id=YSC>
 - *Open Cookie Database*
<https://github.com/jkwakman/Open-Cookie-Database>
 - Keresés:
<https://jkwakman.github.io/Open-Cookie-Database/open-cookie-database.html>

Sütik (4)

- Példa:

- `curl --http1.1 --head https://www.w3.org/`

```
HTTP/1.1 200 OK
Date: Mon, 02 Dec 2024 15:01:45 GMT
Content-Type: text/html; charset=UTF-8
...
Set-Cookie: __cf_bm=VAdE4lj2Jfo8jwNG9tF...f29a9.L7FoS1dQ;
path=/; expires=Mon, 02-Dec-24 15:31:45 GMT; domain=.w3.org;
HttpOnly; Secure; SameSite=None
...
```

Sütik (5)

- Egy eredet szerver akár több sütit is küldhet egy válaszban:
 - `curl --http1.1 --head https://www.youtube.com/`

```
HTTP/1.1 200 OK
Content-Type: text/html; charset=utf-8
...
Set-Cookie: YSC=XsDxGlmbJ3k; Domain=.youtube.com; Path=/; Secure;
HttpOnly; SameSite=none
Set-Cookie: __Secure-YEC=CgtQV2ZFckdHWDN5YyiBp...IBAREiEgEQ%3D%3D;
Domain=.youtube.com; Expires=Thu, 01-Jan-2026 15:32:16 GMT; Path=/;
Secure; HttpOnly; SameSite=lax
Set-Cookie: VISITOR_PRIVACY_METADATA=CgJIVRIcE...IBAREiEgEQ%3D%3D;
Domain=.youtube.com; Expires=Thu, 01-Jan-2026 15:32:17 GMT; Path=/;
Secure; HttpOnly; SameSite=none
Set-Cookie: VISITOR_INF01_LIVE=; Domain=.youtube.com;
Expires=Tue, 08-Mar-2022 15:32:17 GMT; Path=/; Secure; HttpOnly;
SameSite=none
...
```

Süтик (6)

- Amikor a felhasználói ágens egy Set - Cookie fejlécmezőt kap, eltárolja az attribútumaival együtt.
- A továbbiakban, amikor a felhasználói ágens egy HTTP kérést hajt végre, a Cookie fejlécmezőbe illeszti az alkalmazható, nem lejárt sütiket.
 - Csak a név-érték párokat, az attribútumokat nem!
- Ha a felhasználói ágens egy olyan új sütit kap, melynek neve, valamint Domain és Path attribútuma megegyezik egy már tárolt sütiével, akkor az új sütire cseréli ki a korábbi.

Sütik (7)

- A curl utasítása arra, hogy a kapott sütiket írja egy állományba:
 - `curl --http1.1 https://www.youtube.com/ -c cookies.txt -v -o /dev/null`
 - Lásd: <https://curl.se/docs/http-cookies.html>

Sütik (8)

- Sütik visszaküldése a curl-lel:
 - curl --http1.1
https://www.youtube.com/
-b cookies.txt -v -o /dev/null

```
GET / HTTP/1.1
Host: www.youtube.com
User-Agent: curl/7.81.0
Accept: */*
Cookie: VISITOR_PRIVACY_METADATA=CgJIVRIcE...IBAREiEgHg%3D%3D;
__Secure-YEC=Cgt0Wjc4W...IBAREiEgHg%3D%3D; YSC=J6Cx0kFc5EE
```

Süti attribútumok (1)

- A specifikáció az alábbi attribútumokat definiálja:
 - Expires
 - Max-Age
 - Domain
 - Path
 - Secure
 - HttpOnly

Süti attribútumok (2)

- A süti maximális élettartamát jelző attribútumok:
 - **Expires**: a süti lejáratának dátumát és idejét adja meg.
 - **Max-Age**: azt adja meg, hogy hány másodperc múlva jár le a süti.
- **Perzisztens sütik**nek nevezzük az Expires vagy Max-Age attribútummal rendelkező sütiket, mert ezeket a felhasználói ágens több munkameneten keresztül megtarthatja.
 - Ha egy sütinek Max-Age és Expires attribútuma is van, akkor a Max-Age élvez elsőbbséget az Expires attribútummal szemben.
- Ha egy sütinek nincs Expires és Max-Age attribútuma sem, akkor a felhasználói ágens az aktuális munkamenet végéig tartja meg.
- A szerverek sütiket törölhetnek a felhasználói ágensnek egy olyan új sütit küldve, melynek Expires attribútumának értéke egy múltbeli időpont.

Süti attribútumok (3)

- **Domain:**

- Meghatározza, hogy a süti mely szervereknek lesz elküldve.
 - Ha például `example.com` az attribútum értéke, akkor a felhasználói ágens a sütit a `Cookie` fejlécmezőbe illeszti, amikor HTTP kéréseket intéz az `example.com` vagy `www.example.com` szerverekhez..
- Ha a szerver kihagyja az attribútumot, akkor a felhasználói ágens csak az eredet szervernek küldi vissza a sütit.
- A felhasználói ágens elutasít minden olyan sütit, melynél az attribútum által meghatározott hatáskör nem tartalmazza az eredet szerveret.
- Biztonsági okokból sok felhasználói ágens úgy van beállítva, hogy elutasítson minden olyan sütit, melynek `Domain` attribútuma egy nyilvános regisztrátor ellenőrzése alatt álló nyilvános utótag, mint például `com`, `co.uk`, ...

- **Path:**

- A süti hatáskörét adott útvonalakra korlátozza.
- Ha a szerver kihagyja az attribútumot, a felhasználói ágens a kért URI útvonal komponensének „könyvtárát” használja alapértelmezett értéként.

Süti attribútumok (4)

- **Secure:**

- A süti hatáskörének biztonságos csatornákra korlátozása.
- Egy Secure attribútummal rendelkező sütit a felhasználói ágens csak akkor tesz bele egy kérésbe, ha annak átvitele biztonságos csatornán keresztül történik.
 - Mivel a süti érzékeny információt tartalmazhat, melynek sima szöveggént történő átvitele kockázatot jelent.

- **HttpOnly:**

- HTTP kérésekre korlátozza a süti hatáskörét.
- Arra utasítja a felhasználói ágenst, hogy ne tegye a sütit elérhetővé kliens oldali API-k (például JavaScript) számára.

Sütik kezelése (1)

- A felhasználói ágenseknek:
 - Törölniük kell a lejárt sütiket.
 - Az aktuális munkamenet végén törölniük kell az összes nem perzisztens sütit.
 - Ajánlott a felhasználók számára lehetővé tenni a tárolt sütik kezelését.
 - Például egy adott időszakban fogadott vagy egy adott tartományhoz kapcsolódó összes süti törlését.
 - Ajánlott a felhasználók számára lehetővé tenni a sütik letiltását.

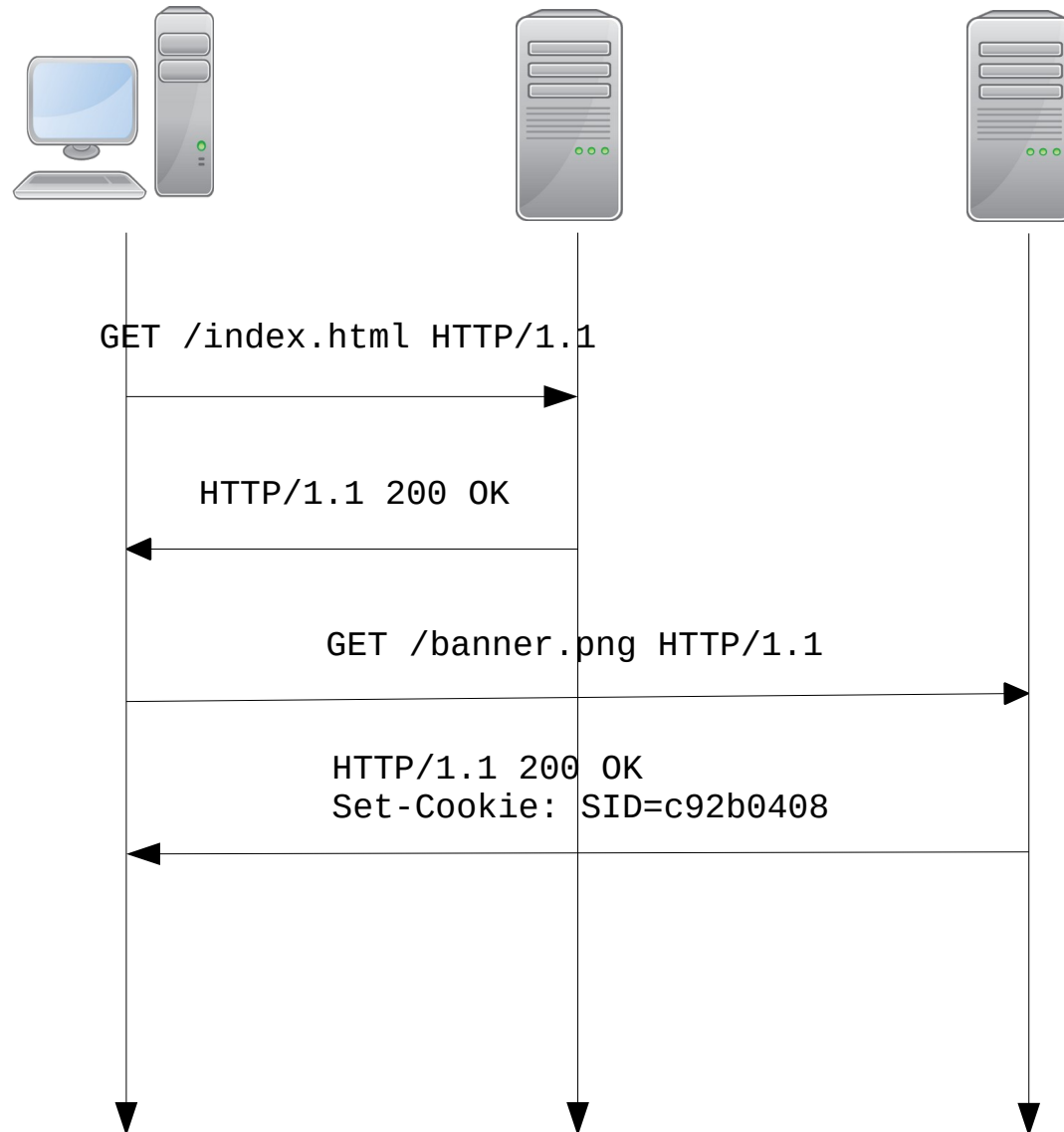
Süti kezelés (2)

- A felhasználói ágensek korlátokat szabnak a tárolható süti számára és méretére.
- A specifikáció az alábbi minimális képességeket ajánlja:
 - Sütinként legalább 4096 bájt.
 - Tartományonként legalább 50 süti.
 - Összesen legalább 3000 süti.

Sütik: adatvédelmi és biztonsági kérdések (1)

- A sütiket gyakran bírálják azért, mert lehetővé teszik a szerverek számára a felhasználók követését.
- Az úgynevezett **harmadik féltől származó sütik** (*third-party cookies*) különösen problémásak.
 - Egy HTML oldal megjelenítése során egy felhasználói ágens gyakran kér le erőforrásokat más szerverekről.
 - Ezek a harmadik félnek számító szerverek sütiket használhatnak a felhasználó követésére még akkor is, ha a felhasználó közvetlenül soha nem látogatja meg őket.
 - A harmadik féltől származó sütiket *cross-site* sütiknek is nevezik.

Sütik: adatvédelmi és biztonsági kérdések (2)



Süтик: adatvédelmi és biztonsági kérdések (3)

- Hacsak nem biztonságos csatornán (például TLS) keresztül kerülnek küldésre, a Cookie és a Set-Cookie fejlécekben nyílt szöveggként adódnak át az információk.
 - Az ezekben a fejlécekben továbbított érzékeny információk lehallgatható és egy rosszindulatú közvetítő akár módosíthatja is.
- Ajánlott a szerverek számára a sütik tartalmának titkosítása és aláírása a felhasználói ágensnek történő továbbítás során (biztonságos csatorna esetén is).
- Biztonságos csatorna használata esetén a szerverek számára ajánlott a Secure attribútum beállítása minden sütihez.

Sütik: adatvédelmi és biztonsági kérdések (4)

- A jelenleg érvényes EU-s szabályozás:
 - **2002/58/EK**: *Elektronikus hírközlési adatvédelmi irányelv* (2002. július 12.) („ePrivacy irányelv”)
<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32002L0058>
 - **2009/136/EK**: *Az Európai Parlament és a Tanács 2009/136/EK irányelve* (2009. november 25.)
<https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32009L0136>
 - Lásd az 2002/58/EK irányelv 5. cikkének (3) bekezdésének módosítását.
 - Kimondja, hogy süti csak akkor helyezhető el a felhasználó számítógépén, ha ehhez a felhasználó tájékoztatás alapján előzetes hozzájárulását adja!
 - A 29. cikk szerinti adatvédelmi munkacsoport: *2012/4. számú vélemény a sütikhez való hozzájárulás alóli mentességről* (2012. június 7.)
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_hu.pdf

Sütik: adatvédelmi és biztonsági kérdések (5)

- Lásd még:
 - *Cookies, the GDPR, and the ePrivacy Directive*
<https://gdpr.eu/cookies/>
 - *Third-party cookies (MDN)*
https://developer.mozilla.org/en-US/docs/Web/Privacy/Third-party_cookies

Webes követés (1)

- Egy lehetséges definíció:
 - Egy adott felhasználó több különböző kontextuson keresztüli tevékenységével kapcsolatos adatgyűjtés és az ebből a tevékenységből származtatott adatok megőrzése, felhasználása vagy megosztása azon kontextuson kívül, melyben a tevékenység történt.
 - Egy kontextus olyan erőforrások egy összessége, melyek ugyanazon fél ellenőrzése vagy több fél közös ellenőrzése alatt állnak.
- Forrás:
<https://www.w3.org/TR/tracking-dnt/#dfn-tracking>

Webes követés (2)

- Az alábbiakon alapulhat:
 - IP-cím
 - Sütik
 - Az ETag fejlécmező
 - Eszköz ujjlenyomat (operációs rendszer, képernyőfelbontás, telepített betűkészletek, ...)
 - Lásd:
 - *Am I Unique?* <https://amiunique.org/>
 - *Cover Your Tracks* <https://coveryourtracks.eff.org/>
 - ...

Webes követés (3)

- Példa böngésző ujjlenyomat használatára:
 - FingerprintJS (programozási nyelv: TypeScript, licenc: *Business Source License 1.1*)
<https://github.com/fingerprintjs/fingerprintjs>
 - Egy forráskódban rendelkezésre álló (de nem nyílt forrású) böngésző ujjlenyomat könyvtár, mely lekéri a böngésző jellemzőit és azokból egy hasított (*hashed*) látogató azonosítót számít.
 - A sütitől eltérően az ujjlenyomat ugyanaz marad inkognitó/privát módban és a böngésző adatok törlésekor is.
 - Demonstráció:
 - Látogasd meg a Google Chrome-ban a következő oldalt és nyisd meg egy inkognitó ablakban is: <https://fingerprintjs.github.io/fingerprintjs>
 - Ismételd meg a kísérletet a Firefox-ban.

Webes követés (4)

- Statisztikák a követőkről:
 - *Ghostery WhoTracks.me*
<https://www.ghostery.com/whotracksme>
 - *Trackers Rank*
<https://www.ghostery.com/whotracksme/trackers>
 - *Ghostery Tracker Database*
<https://github.com/ghostery/trackerdb>
- További információk:
 - *BrowserLeaks.com* <https://www.browserleaks.com/>

Eredet (1)

- Az eredetek alapvetőek a webes biztonság szempontjából.
- Feltételezhető, hogy megbízik egymásban két olyan aktor a weben, melyeknek ugyanaz az eredete.
- A különböző eredetű aktorokat egymással szemben potenciálisan ellenségesnek tekintjük, elkülöníteni ajánlott őket.
- Lásd: *HTML Living Standard – Loading web pages – Supporting concepts – Origins*
<https://html.spec.whatwg.org/multipage/browsers.html#origin>

Eredet (2)

- Egy erőforrás eredetét az eléréséhez használt URI séma, hoszt és port komponense határozza meg.
- Lásd: *Origin*
<https://developer.mozilla.org/en-US/docs/Glossary/Origin>

Eredet (3)

- Példák azonos eredetekre:
 - <http://example.com/index.html>
 - <http://example.com/docs/>
 - <http://example.com:80/>
- Példák nem azonos eredetekre:
 - <http://example.com/>
 - <http://www.example.com/>
 - <http://example.com:8080/>
 - <https://example.com/>

Eredet (4)

- *Same-origin policy*:
 - Egy azt korlátozó kritikus biztonsági mechanizmus, hogy egy adott eredet által betöltött dokumentum vagy szkript hogyan kerülhet kapcsolatba egy másik eredetű erőforrással.
 - Általában tilos egy adott eredetű kód számára egy másik eredetű kód elérése.
 - Lásd: *Same-origin policy*
https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

Eredet (5)

- *Cross-Origin Resource Sharing (CORS)*:
 - Egy HTTP fejlécmező alapú mechanizmus a cross-origin elérés szabályozásához.
 - Lehetővé teszi a szerverek számára olyan a sajátjától különböző eredetek meghatározását, ahonnan a böngésző számára megengedett tartalom betöltése.
 - Az `Origin` és az `Access-Control-Allow-Origin` fejlécmezők használatán alapul.
 - Lásd:
<https://developer.mozilla.org/en-US/docs/Web/HTTP/CORS>

A Referer fejlécmező (1)

- Lehetővé teszi a felhasználói ágens számára, hogy megadja azt az erőforrást azonosító URI-hivatkozást, melyből a cél URI származik.
 - Lásd:
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referer>
- Példa a használatra:
 - Referer: `https://www.w3.org/`
- Potenciálisan információkat nyújthat a felhasználó böngészési előzményeiről, mely egy biztonsági kockázat.

A Referer fejlécmező (2)

- Nem ajánlott a Referer fejlécmező küldése akkor, ha a hivatkozó erőforrás elérése biztonságos protokollon keresztül történt és a kérés céljának eredete eltér a hivatkozó erőforrásétól, hacsak nem engedi meg kifejezetten a Referer mező küldését a hivatkozó erőforrás.
- Tilos a Referer fejlécmező küldése nem biztonságos HTTP kérésben, ha a mezőértékben jelzett oldal biztonságos protokollon keresztül érkezett.

A Referer fejlécmező használatának szabályozása (1)

- A HTML által biztosított mechanizmus:

- *HTML Living Standard – Link type "noreferrer"*

<https://html.spec.whatwg.org/multipage/semantics.html#link-type-noreferrer>

- Az a elem `rel="noreferrer"` attribútuma.

- Példa:

- `Click here`

- Böngésző támogatás: <https://caniuse.com/rel-noreferrer>

A Referrer fejlécmező használatának szabályozása (2)

- *Referrer Policy* (előzetes W3C javaslattev, 2017. január 26.) <https://www.w3.org/TR/referrer-policy/>
 - Mechanizmus biztosítása, mely révén a dokumentum szerzők szabályozást határozhatnak meg a kliensek számára a Referrer fejlécmező küldésére vonatkozólag.
 - Példa:
 - Referrer-Policy: no-referrer
 - `<meta name="referrer" content="no-referrer"/>`
 - `Click here`
 - Böngésző támogatottság: <https://caniuse.com/referrer-policy>

A Referrer fejlécmező használatának szabályozása (3)

- *Referrer Policy* (folytatás):
 - A rendelkezésre álló opciók:
<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy>
 - Az alapértelmezés a `strict-origin-when-cross-origin`, ezt használja a Firefox és a Chrome böngésző is.
 - Lásd:
 - Firefox 87 trims HTTP Referrers by default to protect user privacy
<https://blog.mozilla.org/security/2021/03/22/firefox-87-trims-http-referrers-by-default-to-protect-user-privacy/>
 - A new default Referrer-Policy for Chrome – `strict-origin-when-cross-origin`
<https://developer.chrome.com/blog/referrer-policy-new-chrome-default/>
 - További információk: *Referer and Referrer-Policy best practices* <https://web.dev/articles/referrer-best-practices>

Védekezés a követés ellen (1)

- A Referer fejlécmező küldésének tiltása:
 - **Firefox:** lásd a `network.http.sendRefererHeader` opciót (`about:config`)
<https://wiki.mozilla.org/Security/Referrer>
 - **Chromium, Google Chrome:** nem lehetséges (?)
 - **Opera:** nem lehetséges (?)
 - **Chromium-based Microsoft Edge:** nem lehetséges (?)

Védekezés a követés ellen (2)

- Harmadik féltől származó sütik letiltása:
 - A főbb böngészőkben (Chromium, Google Chrome, Chromium-based Microsoft Edge, Firefox, Opera) a felhasználók választhatják a harmadik féltől származó sütik letiltását a privát böngészéskor/inkognitómódban vagy pedig általában.
 - Mivel a harmadik féltől származó sütik letiltása működésképtelenné teheti a webhelyeket, a felhasználók kivételeket tehetnek bizonyos webhelyeknek megengedve a harmadik féltől származó sütik használatát.

Védekezés a követés ellen (3)

- Harmadik féltől származó süтик elfogadásának letiltása:
 - **Firefox:** lásd a `network.cookie.cookieBehavior` opciót (`about:config`)
 - Lásd még: *Third-party cookies and Firefox tracking protection – Disable third-party cookies*
https://support.mozilla.org/en-US/kb/third-party-cookies-firefox-tracking-protection#w_disable-third-party-cookies
 - **Chromium, Google Chrome:** lásd a *Harmadik féltől származó cookie-k letiltása* opciót (`chrome://settings/privacy`)
 - **Opera:** lásd a *Harmadik féltől származó cookie-k letiltása* opciót (`opera://settings/cookies`)
 - **Chromium-alapú Microsoft Edge:** lásd a *Harmadik féltől származó cookie-k letiltása* opciót (`edge://settings/content/cookies`)

Védekezés a követés ellen (4)

- Privát böngészés/inkognitómód:
 - Számos modern böngésző rendelkezik a felhasználó magánszférájának védelmét szolgáló privát böngészési lehetőséggel.
 - Privát böngészési módban a munkamenet végén automatikusan törlésre kerülnek a böngészési információk, úgymint a
 - böngészési előzmények,
 - sütik,
 - gyorsítótárazott tartalmak.

Védekezés a követés ellen (5)

- Privát böngészés/inkognitómód: (folytatás)
 - **Firefox:**
 - *Privát böngészés – internetezés a meglátogatott weboldallal kapcsolatos adatok mentése nélkül*
<https://support.mozilla.org/hu/kb/privat-bongesz-es-internetez-es-meglatogatott-webold>
 - **Chromium, Google Chrome:**
 - *How private browsing works* <https://support.google.com/chrome/?p=incognito>
 - **Opera:**
 - *Opera Help – Security and privacy – Private window*
<https://help.opera.com/en/latest/security-and-privacy/#privateWindow>
 - **Chromium-alapú Microsoft Edge:**
 - *InPrivate-böngészés a Microsoft Edge-ben*
<https://support.microsoft.com/hu-hu/microsoft-edge/inprivate-b%C3%B6ng%C3%A9sz%C3%A9s-a-microsoft-edge-ben-cd2c9a48-0bc4-b98e-5e46-ac40c84e27e2>

Védekezés a követés ellen (6)

- Beépített követés elleni védelem:
 - **Firefox:**
 - *Továbbfejlesztett követés elleni védelem az asztali Firefoxban*
<https://support.mozilla.org/hu/kb/tovabbfejlesztett-kovetes-elleni-vedelem-az-asztal>
 - Lásd: `about:protections`
 - **Chromium-alapú Microsoft Edge:**
 - *Tracking Prevention in Microsoft Edge*
<https://learn.microsoft.com/en-us/microsoft-edge/web-platform/tracking-prevention>
 - See: `edge://settings/privacy`
 - **Safari:**
 - *Tracking Prevention in WebKit* <https://webkit.org/tracking-prevention/>

Védekezés a követés ellen (7)

- Komplex megoldások:
 - *Adblock Plus* (licenc: GPLv3) <https://adblockplus.org/>
<https://gitlab.com/eyeo/extensions/extensions>
 - Támogatott böngészők: Chrome, Firefox, Microsoft Edge, Opera, Safari
 - Lásd az *EasyPrivacy* szűrőt <https://easylist.to/>
 - *Ghostery Browser Extension* (licenc: nem szabad/Mozilla Public License 2.0)
<https://www.ghostery.com/ghostery-ad-blocker>
<https://github.com/ghostery/ghostery-extension>
 - Támogatott böngészők: Chrome, Firefox, Microsoft Edge, Opera, Safari
 - *Privacy Badger* (licenc: GPLv3) <https://privacybadger.org/>
<https://github.com/EFForg/privacybadger>
 - Támogatott böngészők: Chrome, Firefox, Microsoft Edge, Opera
 - *uBlock Origin* (licenc: GPLv3) <https://github.com/gorhill/uBlock>
 - Támogatott böngészők: Chromium, Firefox

Védekezés a követés ellen (8)

- A magánszféra védelmére koncentrááló böngészők:
 - Brave: a Chromium-on alapuló szabad és nyílt forrású böngésző, mely a magánszféra védelmét helyezi a középpontba.
 - Fejlesztő: Brave Software, Inc.
 - Webhely: <https://brave.com/>
 - Tároló: <https://github.com/brave/brave-browser>
 - Programozási nyelv: C++, Swift, TypeScript
 - Licenc: Mozilla Public License 2.0
 - Platform: Android, iOS, Linux, macOS, Windows

Védekezés a követés ellen (9)

- Google Chrome:
 - A Google azt tervezte, hogy tesztelési célból a felhasználók 1%-ánál korlátozza a harmadik féltől származó sütik használatát, és 2024 harmadik negyedévére ez minden felhasználó számára elérhető lesz.
 - Lásd:
 - Chris Mills. *Saying goodbye to third-party cookies in 2024*. December 8, 2023. <https://developer.mozilla.org/en-US/blog/goodbye-third-party-cookies/>
 - *Third-party cookies restricted by default for 1% of Chrome users*. January 4, 2024. <https://developers.google.com/privacy-sandbox/blog/cookie-countdown-2024jan>
 - Később a Google úgy döntött, hogy mégsem így tesz, hanem inkább egy más megközelítést követ.
 - Lásd: Anthony Chavez. *A new path for Privacy Sandbox on the web*. July 22, 2024. <https://privacysandbox.com/news/privacy-sandbox-update/>

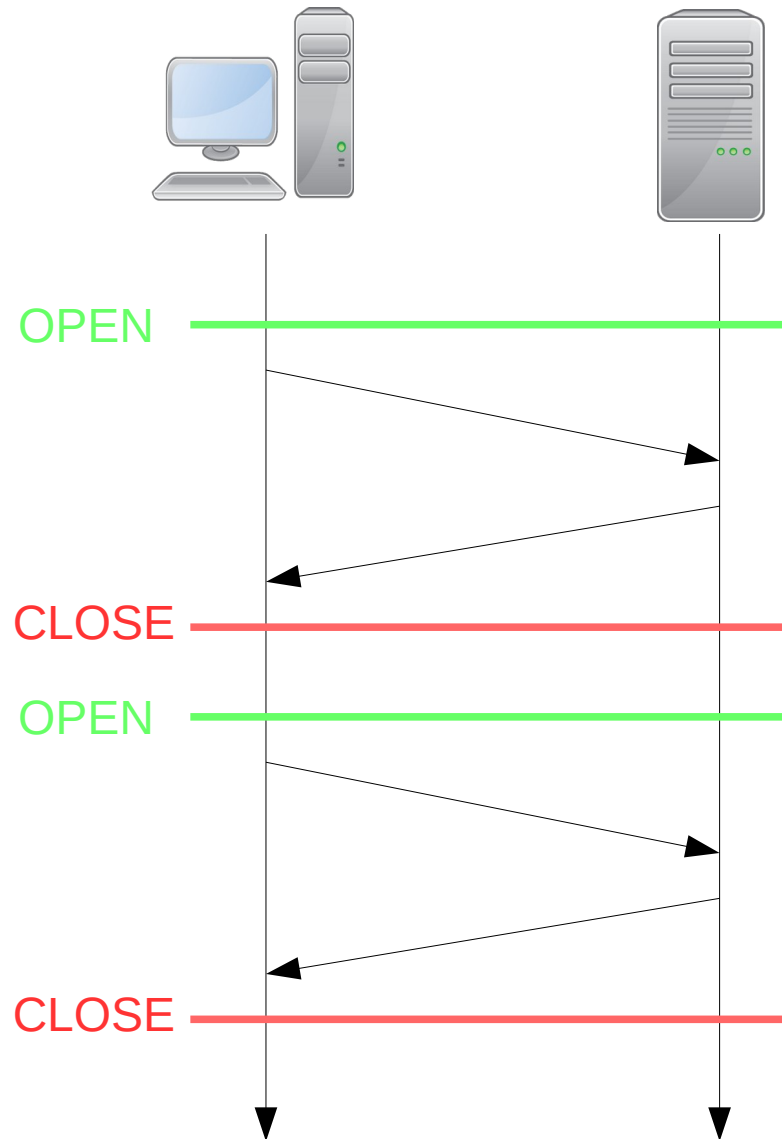
Védekezés a követés ellen (10)

- További információk:
 - *PrivacyTools* <https://www.privacytools.io/>

Böngészők összehasonlítása

- *Can I use...* – *Browser comparison*
<https://caniuse.com/ciu/comparison>
<https://github.com/Fyrd/caniuse>
- *Comparison of Web Browsers*
https://eylenburg.github.io/browser_comparison.htm
- *PrivacyTests.org* <https://privacytests.org/>

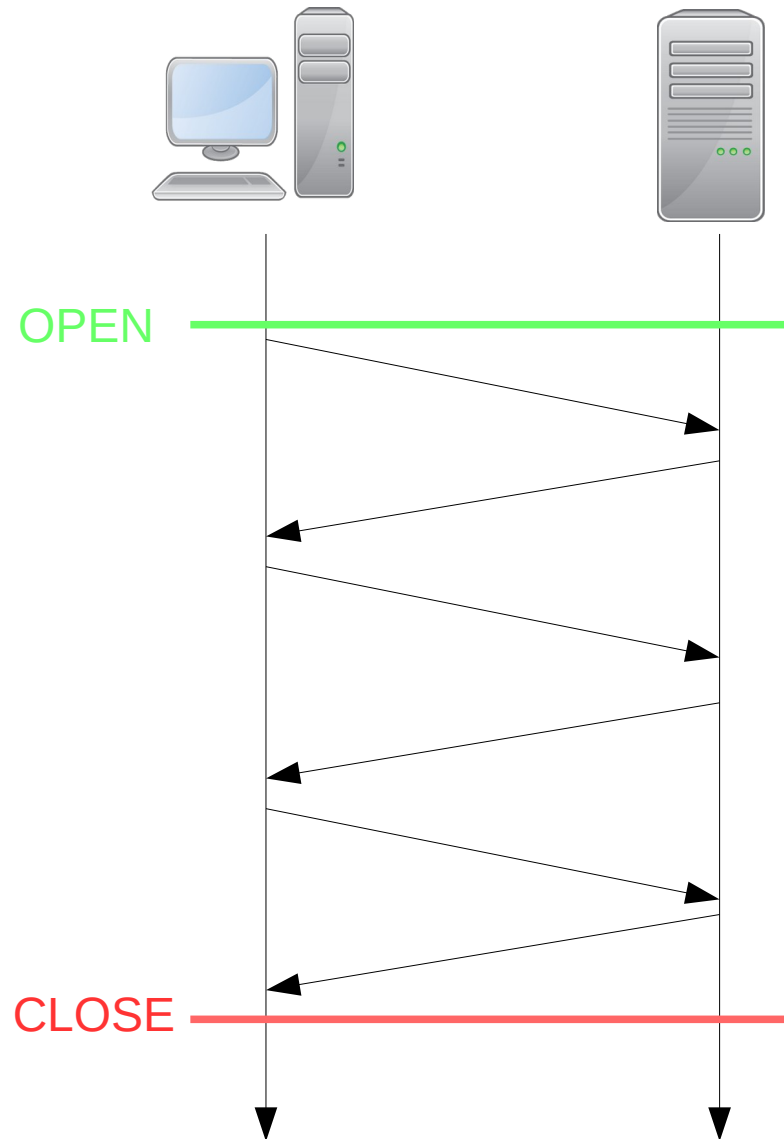
HTTP/1.0 kapcsolatkezelés



Perzisztens kapcsolatok (1)

- A HTTP/1.1 vezette be.
- Lehetővé teszi több kérés és válasz átvitelét egyetlen TCP kapcsolaton át.
- A HTTP/1.1 alapértelmezetten perzisztens kapcsolatokat használ.

Perzisztens kapcsolatok (2)



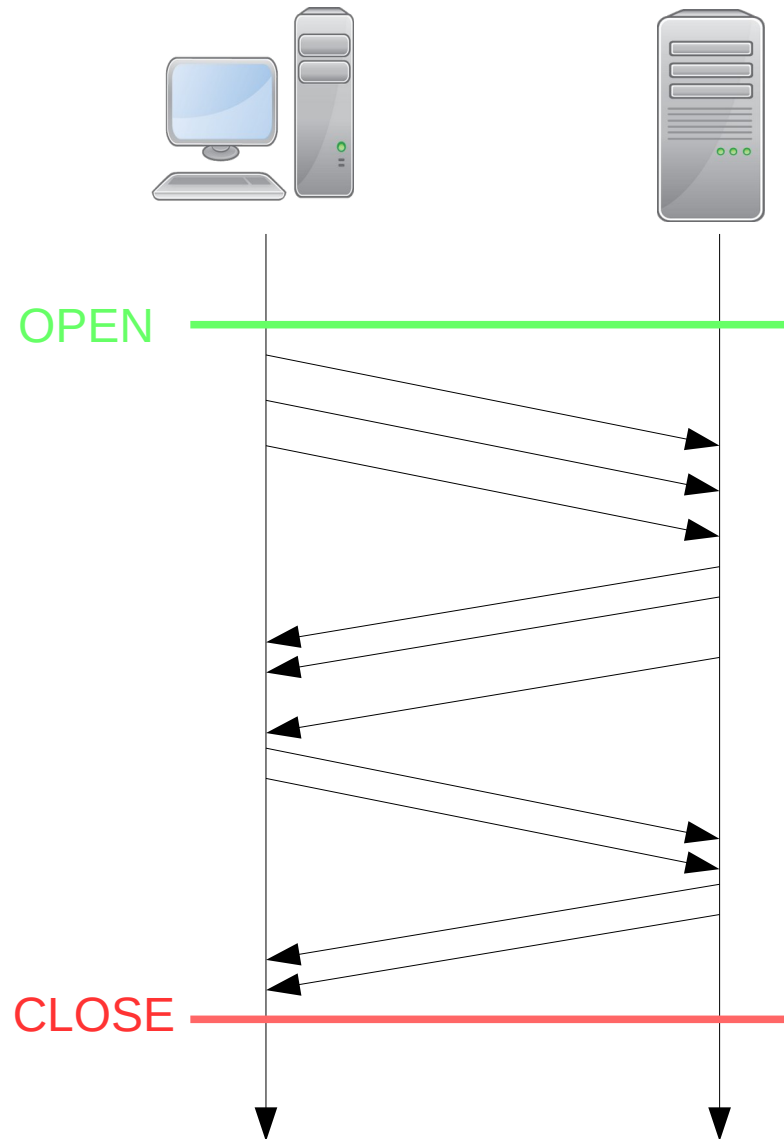
Kapcsolatkezelés: kapcsolati beállítások

- A `Connection` fejlécmező lehetővé teszi a küldő számára az aktuális kapcsolatra vonatkozó vezérlő beállítások megadását.
 - A mezőérték kisbetű-nagybetű érzéketlen opciók listája.

Kapcsolatkezelés: csővezetékezés (1)

- Egy perzisztens kapcsolatokat támogató kliens „csővezetékezheti” a kérései, azaz egymás után több kérést is küldhet anélkül, hogy megvárná a válaszokat.
- Egy szerver csővezetékezett kérések egy sorozatát párhuzamosan is feldolgozhatja, ha minden kérés metódusa biztonságos, de a megfelelő válaszokat ugyanabban a sorrendben kell, hogy elküldje, melyben a kéréseket fogadta.

Kapcsolatkezelés: csővezetékezés (2)



Kapcsolatkezelés: csővezetékezés (3)

- Ha a kapcsolat még azelőtt lezárul, hogy egy kéréseket csővezetékező kliens az összes választ megkapná, akkor megpróbálhatja ismét a megválaszolatlan kéréseket.
- Idempotens kérések próbálhatók újra automatikusan kapcsolati hiba után.

Kapcsolatkezelés: csővezetékezés (4)

- Böngésző támogatás:
 - **Firefox**: támogatott, de alapértelmezésben ki van kapcsolva.
 - Lásd a `network.http.pipelining` opciót (`about:config`).
 - **Chromium, Google Chrome**: eltávolították az engedélyezésre szolgáló opciót.
 - Lásd:
<https://www.chromium.org/developers/design-documents/network-stack/http-pipelining>
 - **Opera**: nem támogatott
 - **Chromium-based Microsoft Edge**: nem támogatott

Kapcsolatkezelés: csővezetékezés (5)

- Elméletileg a teljesítmény javítható több HTTP kérés ugyanabba a TCP üzenetbe történő csomagolásával is.
- Feleslegessé teszi egy jobb mechanizmus, a HTTP/2 által használt multiplexelés.

- Lásd: *Connection management in HTTP/1.x – HTTP pipelining*

https://developer.mozilla.org/en-US/docs/Web/HTTP/Connection_management_in_HTTP_1.x#http_pipelining

Kapcsolatkezelés: kapcsolat lezárása

- Kapcsolat explicit lezárása:
 - A `Connection` fejlécmező biztosít egy `close` opciót, mellyel a küldő jelezheti, hogy az aktuális kérés/válasz befejezése után lezárásra kerül a kapcsolat.
 - Kérésekben és válaszokban is használható.
 - Példa:
 - `Connection: close`
- Időtúllépés:
 - A szerverek általában van valamiféle várakozási ideje, melyen túl nem tartanak fenn tovább egy inaktív kapcsolatot.

Kapcsolatkezelés: egyidejű kapcsolatok (1)

- A legtöbb szervert úgy tervezték, hogy képes legyen sok ezer egyidejű kapcsolatot fenntartani.
- A legtöbb kliens több kapcsolatot tart fenn párhuzamosan, egy szerverhez akár többet is.
 - Jellemzően a **sor eleji blokkolás** (*head-of-line blocking*) problémájának elkerüléséhez használnak több kapcsolatot.

Kapcsolatkezelés: egyidejű kapcsolatok (2)

- A HTTP korábbi kiadásai egy korlátot határoztak meg az egy kliens által egy adott szerverhez egyidejűleg fenntartható kapcsolatok számára.
 - RFC 2616: a kapcsolatok maximális száma 2.
- Ez sok alkalmazáshoz célszerűtlennek bizonyult, ezért a HTTP/1.1 nem ír elő konkrét korlátot, hanem helyette azt javasolja a klienseknek, hogy legyenek óvatosak, amikor több kapcsolat nyitnak.
 - Minden egyes kapcsolat a szerver erőforrásait fogyasztja és a szerver megtagadhatja a kéréseket, ha egy kliens túl sok kapcsolatot nyit meg.

Kapcsolatkezelés: egyidejű kapcsolatok (3)

- Korlátok a kapcsolatok számára:
 - **Firefox:** lásd az alábbi opciókat (about : config):
 - `network.http.max-connections` (alapértelmezett érték: 900)
 - `network.http.max-persistent-connections-per-proxy` (alapértelmezett érték: 32)
 - `network.http.max-persistent-connections-per-server` (alapértelmezett érték: 6)
 - **Chromium, Google Chrome:** a Firefox fenti opcióinál adott alapértelmezett értékek használata rögzített módon
 - Lásd:
<https://www.chromium.org/developers/design-documents/network-stack/#connection-management>
 - **Chromium-alapú Microsoft Edge:**
<https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/issues#queued-or-stalled-requests>

További ajánlott irodalom

- *MDN Web Docs – HTTP*
<https://developer.mozilla.org/docs/Web/HTTP>
- Ilya Grigorik, *High Performance Browser Networking*. O'Reilly, 2013. <https://hpbn.co/>