Web Browser Privacy: What Do Browsers Say When They Phone Home?

Additional Material: Content of Network Connections

Note that to save space HTTP headers and parameters with uninteresting content are not shown. Probable ersistent identifiers are highlighted in bold.

I. Google Chrome Connections

A. Connections When Initial Popup Is Displayed

GET https://clients2.google.com/service/update2/crx
Parameters:
os: mac
arch: x64
os_arch: x86_64
nacl_arch: x86−64
prod: chromecrx
prodchannel:
prodversion: 80.0.3987.87
lang: en−GB
acceptformat: crx3
x: id=nmmhkkegccagdldgiimedpiccmgmieda&v=0.0.0.0&installedby=other&uc&ping=r%3D−1%26e%3D1
x: id=pkedcjkdefgpdelpbcmbmeomcjbeemfm&v=0.0.0.0&installedby=other&uc&ping=r%3D−1%26e%3D1
x: id=aapocclcgogkmnckokdopfmhonfmgoek&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x: id=felcaaldnbdncclmgdcncolpebgiejap&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x: id=ghbmnnjooekpmoecnnnilnnbdlolhkhi&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x: id=aohghmighlieiainnegkcijnfilokake&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x: id=apdfllckaahabafndbhieahigkjlhalf&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x: id=blpcfgokakmgnkcojhhkbfbldkacnbeo&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
x:id=pjkljhegncpnkpknbcohdijeoejaedia&v=0.0.0.0&installedby=internal&uc&ping=r%3D−1%26e%3D1
Headers:
x−goog−update−appid: aapocclcgogkmnckokdopfmhonfmgoek, aohghmighlieiainnegkcijnfilokake,apdfllckaahabafndbhieahigkjlhalf, blpcfgokakmgnkcojhhkbfbldkacnbeo,felcaaldnbdncclmgdcncolpebgiejap, ghbmnnjooekpmoecnnnilnnbdlolhkhi,nmmhkkegccagdldgiimedpiccmgmieda, pjkljhegncpnkpknbcohdijeoejaedia,pkedcjkdefgpdelpbcmbmeomcjbeemfm
x−goog−update−updater: chromecrx−80.0.3987.87

Notes:

- *Separate startup of a fresh install of Chome on the same device leads to the same set of identifiers being transmitted by this GET request. They relate to Chrome extensions (namely, in order: Google Wallet, Chrome Cast, Google Slides, Google Sheets, Google Docs Offline, Google Docs, Google Drive, YouTube, Google Mail).*
- *The response is a list of entries one for each id of the following form (the codebase URL for each appid is called later, used to check for updates[1]):*

<app appid="aapocclcgogkmnckokdopfmhonfmgoek" cohort="" cohortname="" status="ok">
<ping status="ok"/>
<updatecheck codebase="https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2DJtnXe8Z7rUJP1q2vfaFufY. . ./extension_0_10_0_0.crx" fp="1.
ee80340a02c0f96a3f9d01e635857d38d7b92444d6102ee29804f559f2eaa7f4" hash_sha256="
ee80340a02c0f96a3f9d01e635857d38d7b92444d6102ee29804f559f2eaa7f4" protected="0" size="23667" status="ok" version="0.10"/>
</app>

[1]See https://developer.chrome.com/apps/autoupdate

POST https://accounts.google.com/ListAccounts?gpsia=1&source=ChromiumBrowser&json=standard

Response is ["gaia.l.a.r",[]] which seems to indicate that the session has not been linked to a Google account (GAIA appears to be an acronym for Google Accounts and ID Administration).

GET https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2DJtnXe8Z7rUJP1q2vfaFufY.../extension_0_10_0_0.crx

Observe that this corresponds to the codebase URL for the extension with appid "aapocclcgogkmnckokdopfmhonfmgoek" (Google Slides). The response is 23667B of content type application/x-chrome-extension.

GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb

The response is 77948B of content of type application/octet-stream. Curiously, this GET and the large response are repeated twice.

GET https://www.gstatic.com/chrome/config/plugins_3/plugins_mac.json

The response is 1814B of content of type application/json which contains entries fo "Adobe Flash Player", "Adobe Shockwave Player" and for several Quicktime plugins.

GET https://www.gstatic.com/autofill/hourly/bins.json

The response is json {"cpan_eligible_bin_wl_regex": ["^4[0−9]{15,18}$"]}

GET https://www.gstatic.com/autofill/weekly/merchants.json

The response is json {"cpan_eligible_merchant_wl": "dump−truck.appspot.com"]. Domain appspot.com is registered to Google.}

B. Connections Made Upon Clicking Initial Popup

GET https://clientservices.googleapis.com/chrome-variations/seed
Parameters:
osname: mac
channel: stable
milestone: 80

The response is 19.84KB of content of type application/x-gzip. The very first GET request to https://clients2.google.com/service/update2/crx is now repeated, with the same response (a list of codebase URLs for 9 Chrome extensions). A GET request is now made to each of these codebase URLs.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . . /extension_0_10_0_0.crx

This corresponds to the extension with appid "aohghmighlieiainnegkcijnfilokake" (Google Docs). The response is 22.73KB of content of type application/x-chrome-extension.

GET https://www.gstatic.com/chrome/intelligence/assist/ranker/models/translate/2017/03/translate_ranker_model_20170329.pb.bin

The response is 2.35KB of content that seems to be related to Google Translate.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_14_2_0_0.crx

This corresponds to the extension with appid "apdfllckaahabafndbhieahigkjlhalf" (Google Drive). The response in 28.97KB of content of type application/x-chrome-extension.

POST https://www.googleapis.com/chromewebstore/v1.1/items/verify

```
{
    "hash": "df7aOTSK6JMuKZRab+neVUanXyyiq4h21H3yLIlHyrQ
=",
    "ids": [
        "aapocclcgogkmnckokdopfmhonfmgoek"
    ],
    "protocol_version": 1
}
```

This seems to be verifying appid "aapocclcgogkmnckokdopfmhonfmgoek" (Google Slides), which was previously fetched while initial popup was displayed. The response is 410B consisting of a sha1 hash and what looks like an extension signature.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_1_2_0_0.crx

This seems to be verifying appid "felcaaldnbdncclmgdcncolpebgiejap" (Google Sheets). The response in 23.09KB of content of type application/x-chrome-extension.

GET
http://redirector.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHR. . .
/8019.1111.0.0_pkedcjkdefgpdelpbcmbmeomcjbeemfm.crx

This corresponds to the extension with appid "pkedcjkdefgpdelpbcmbmeomcjbeemfm" (Chrome Cast). The response is a redirect to http://r5—sn-q0cedn7s.gvt1.com/edgedl/chromewebstore/.

POST https://www.googleapis.com/chromewebstore/v1.1/items/verify
<POST body similar to previous request to https://www.googleapis.com/chromewebstore/v1.1/items/verify>

GET http:
//r5---sn-q0cedn7s.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHR...
/8019.1111.0.0\pkedcjkdefgpdelpbcmbmeomcjbeemfm.crx
Parameters:
cms_redirect: yes
mip: 37.228.245.107
mm: 28
mn: sn−q0cedn7s
ms: nvh
mt: 1581244032
mv: m
mvi: 4
pl: 19
shardbypass: yes

This corresponds to the extension with appid "pkedcjkdefgpdelpbcmbmeomcjbeemfm" (Chrome Cast). The response in 839KB of content of type application/x-chrome-extension.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_8_2_0_0.crx

This corresponds to the extension with appid "pjkljhegncpnkpknbcohdijeoejaedia" (Google Mail). The response in 25.21KB of content of type application/x-chrome-extension.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_0_10_0_0.crx

This corresponds to the extension with appid "aohghmighlieiainnegkcijnfilokake" (Google Docs). The response in 22.73KB of content of type application/x-chrome-extension.

POST https://www.googleapis.com/chromewebstore/v1.1/items/verify
<POST body similar to previous request to https://www.googleapis.com/chromewebstore/v1.1/items/verify>

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_0_10_0_0.crx

This corresponds to the extension with appid "aapocclcgogkmnckokdopfmhonfmgoek" (Google Slides, recently fetched so this seems to be a duplicate fetch). The response in 23.11KB of content of type application/x-chrome-extension.

GET
http://redirector.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHR. . .
/1.0.0.5_nmmhkkegccagdldgiimedpiccmgmieda.crx

This corresponds to the extension with appid "nmmhkkegccagdldgiimedpiccmgmieda" (Google Wallet). The response is a redirect to http://r3—sn-q0cedn7s.gvt1.com/edgedl/chromewebstore/.

GET http://r3—sn-
q0cedn7s.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHR. . .
/1.0.0.5_nmmhkkegccagdldgiimedpiccmgmieda.crx
Parameters: <similar to previous request to gvt1.com>

This corresponds to the extension with appid "nmmhkkegccagdldgiimedpiccmgmieda" (Google Wallet). The response in 293.9KB of content of type application/x-chrome-extension.

POST https://www.googleapis.com/chromewebstore/v1.1/items/verify
<POST body similar to previous request to https://www.googleapis.com/chromewebstore/v1.1/items/verify>

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
g/extension_1_9_0_0.crx

This corresponds to the extension with appid "ghbmnnjooekpmoecnnnilnnbdlolhkhi" (Google Docs Offline). The response in 91.11KB of content of type application/x-chrome-extension.

GET
https://clients2.googleusercontent.com/crx/blobs/QgAAAC6zw0qH2D. . .
/extension_4_2_8_0.crx

This corresponds to the extension with appid "blpcfgokakmgnkcojhhkbfbldkacnbeo" (YouTube). The response in 19.58KB of content of type application/x-chrome-extension.

POST https://www.googleapis.com/chromewebstore/v1.1/items/verify
<POST body similar to previous request to https://www.googleapis.com/chromewebstore/v1.1/items/verify>

GET https://docs.google.com/offline/extension/frame

This response to this call to Google Docs is a redirect to https://accounts.google.com/ServiceLogin

GET https://accounts.google.com/ServiceLogin
Parameters:
service: wise
passive: 1209600
continue: https://docs.google.com/offline/extension/frame?ouid
followup: https://docs.google.com/offline/extension/frame?ouid
ltmpl: homepage
Headers:
x−chrome−id−consistency−request: version=1,client_id
=77185425430.apps.googleusercontent.com, device_id=**90c0f8cc-d49a-4d09-a81c-32b7c0f2aae6**, signin_mode=all_accounts,signout_mode=
show_confirmation

Notes:

- *The client_id is used in OAUTH and is supposed to be the same for all Chrome installs and all users, i.e. its an identifier of the Chrome product*[2] *(confirmed that it remained unchanged across fresh installs).*
- *The device ID is a unique identifier which is tied to your session and should be re-created after signout*[3] *(confirmed that it changed across fresh installs on the same device e.g. changed to* ***aac00742-4b5e-49ed-9526-207077954bec*** *on second install and launch).*
- *The response to this GET request sets a cookie: set-cookie:* ***GAPS=1:-qChrMo1Rv_1fBI0gYpVRkLD_h89hQ:jJRNg2Cs370FK-DG*** *and sends 413KB of HTML/javascript that seems to contain sign-in code for Google Drive. The code has an embedded nonce="QR3bc02y2mU4jgpquGFsGg" and other identifier-like data.*
- *The cookie and the nonce in the response both change on a second fresh install.*

HEAD http://moaytrx/
HEAD http://pcagbumitc/
HEAD http://dohdokiollyud/

These three HEAD requests all fail since they are to invalid domains. It seems they are used to check for DNS hijacking i.e. DNS servers that resolve non-existent domain names to advertising domains[4]*. The next sequence of requests seem to be checking for updates to the extensions.*

POST https://update.googleapis.com/service/update2/json
Parameters:
cup2key=9:2699949029
cup2hreq=36463
a2dd9c89e526c1541e111d3d48bbb34492d1080396fa77c8e65c39fea17
Headers:
x−goog−update−appid: mimojjlkmoijpicakmndhoigimigcmbb, hnimpnehoodheedghdeeijklkeaacbdc, llkgjffcdpffmhiakmfcdcblohccpfmo, gcmjkmgdlgnkkcocmoeiminaijmmjnii, . . .

```
{
    "request": {
        "@os": "mac",
        "@updater": "chrome",
        "acceptformat": "crx2,crx3",
        "app": [
            {
                "appid": "mimojjlkmoijpicakmndhoigimigcmbb",
                "brand": "GGRO",
                "enabled": true,
                "ping": {
                    "r": −2
                },
                "updatecheck": {},
                "version": "0.0.0.0"
            },
            <and similar entries for other appid's listed in x−goog−update−appid header>
        "requestid": "{61f7dcb8−474b−44ac−a0e5−b93a621a549b}",
        "sessionid": "{debfbf76-8eaf-4176-82c6-773d46ca8c57}",
        "updaterversion": "80.0.3987.87"
    }
}
```

The same sessionid value is also used in the POST requests to update.googleapis.com that follow, and so can be used to link these requests to the same browser instance (the requestid value changes between POST requests). Inspection of the Chromium source indicates that cup2key is a randomised value generated by the browser and cup2hreq is a hash of the request body.

GET http://r3—sn-q0cedn7s.gvt1.com/edgedl/release2/chrome_component/AJnAd5fw5FUII. . .
Parmeters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "mimojjlkmoijpicakmndhoigimigcmbb">

GET http://r5—sn-q0cedn7s.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHR. . .
Parameters: <similar to previous request to gvt1.com>

GET http://r4—sn-q0cedn7s.gvt1.com/edgedl/release2/chrome_component/AKXvq. . .
Paameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "hnimpnehoodheedghdeeijklkeaacbdc">

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "gcmjkmgdlgnkkcocmoeiminaijmmjnii">

GET http://r4—sn-q0cedn7s.gvt1.com/edgedl/release2/chrome_component/D9hD-Th6C691. . .
Parameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "hfnkpimlhhgieaddgfemjhofmfblmnib">

GET http://r3—sn-q0cedn7s.gvt1.com/edgedl/release2/chrome_component/V3P1l2hLvLw_7/7_all_sslErrorAssistant.crx
Parameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "giekcmmlnklenlaomppkphknjmnnpneh">

GET http://r2—sn-q0c7rn76.gvt1.com/edgedl/release2/chrome_component/AM334On9dN. . .
Parameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "khaoiebndkojlmppeemjhbpbandiljpe">

GET http://r5—sn-q0cedn7s.gvt1.com/edgedl/release2/Eth6bTe5668ruajuYgrQy. . .
Parameters: <similar to previous request to gvt1.com>

GET http://redirector.gvt1.com/edgedl/release2/XO5hfbcBilKaURwk2jYt6. . .

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "jflookgnkcckhobaglndicnbbgbonegd">

GET http://r4—sn-q0c7rn76.gvt1.com/edgedl/release2/XO5hfbcBilKaURwk. . .
Parameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "bklopemakmnopmghhmccadeonafabnal">

POST https://update.googleapis.com/service/update2/json
Parameters:
<Request body for "appid": "ggkkehgbnfjpeggfpleeakpidbkibbmn">

GET http://redirector.gvt1.com/edgedl/release2/AObXHnCOjk4C. . .

GET http://r2—sn-q0c7rn76.gvt1.com/edgedl/release2/AObXHnCOjk4C. . .
Parameters: <similar to previous request to gvt1.com>

POST https://update.googleapis.com/service/update2/json
<request body for "appid": "ggkkehgbnfjpeggfpleeakpidbkibbmn">

GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Parameters:
$req: ChwKDGdvb2dsZWNocm9tZRIMOD. . .
$ct: application/x−protobuf
key: AIzaSyBOti4mM−6x9WDnZIjIeyEU21OpBXqWBgw

The key value stays the same across fresh installs. As already noted the $req base64 encodes the data described in the safebrowsing API docs. The response is 5.65MB of content of type application/x-protobuf.

[2] See https://groups.google.com/a/chromium.org/forum/#!topic/net-dev/LP6hv0Z7lVA
[3] See footnote 2.
[4] See http://en.wikipedia.org/wiki/DNS_hijacking

C. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar.

GET https://www.google.com/complete/search
Parameters:
q: http://leith.ie/nothingtosee.html
oit: 3
cp: 33
pgcl: 7
gs_rn: 42
psi: akTjeqrWKX4i93lS
sugkey: AIzaSyBOti4mM−6x9WDnZIjIey. . .

Note the value of header sugkey is constant across clean starts and matches the key value used in calls to safebrowsing.googleapis.com (which seems to be the same for all instances of Chrome) but the value of psi changes e.g. to 2ikhow9tFh22zW3O. Response is a fragment of javascript:)] }’[”http://leith.ie/nothingtosee.html”,[],[],[], {”google:clientdata”: {”bpc”:false,”tlw”:true },”google:suggesttype” [],”google:verbatimrelevance”:851}]

GET http://leith.ie/nothingtosee.html

GET http://leith.ie/favicon.ico

D. Connections Made On Re-Open After Close

GET https://www.gstatic.com/autofill/hourly/bins.json

Response is json: {”cpan_eligible_bin_wl_regex”: [”^4[0−]{15,18}$”]}

GET https://www.gstatic.com/autofill/weekly/merchants.json

Response is json:
{”cpan_eligible_merchant_wl”: [”dump−truck.appspot.com”]}

POST https://accounts.google.com/ListAccounts
Headers:
cookie: **GAPS=1:-qChrMo1Rv_1fBI0gYpVRkLD_h89hQ:jJRNg2Cs370FK-DG**

:

Note the cookie sent with the request, this was set during the initial startup of Chrome (see above). Response is json: [”gaia.l.a.r”,[]]

GET https://clientservices.googleapis.com/chrome-variations/seed
Parameters:
osname: mac
channel: stable
milestone: 80

Response is HTTP code 304 (“Not Modified”).

GET https://www.google.com/async/newtab_promos

Response is a curious short fragment of javascript :)]}’ {”update”:{”promos”:{}}}

GET https://www.google.com/async/ddljson

Response is a fragment of javascript :)]}’ {”ddljson”:{}}

GET https://www.google.com/async/newtab_ogb
Headers:
x−client−data:
CIe2yQEIo7bJAQjEtskBCKmdygEIvbDKAQiWtcoBCO21ygEIjrrKARirpMoBGJq6ygE=

Note the x-client-data header. According to Google’s privacy documentation (https://www.google.com/chrome/privacy/whitepaper.html) this is used for field trials. It is observed to change across fresh installs. Response is 39.88KB of application/json content which looks like a fragment of javascript (presumably associated with the set of experiments indicated by the x-client-data header.

POST https://update.googleapis.com/service/update2/json
Parameters:
cup2key=9:3852808952
cup2hreq=
c91c8a6a5f633563d36cbfe0b26a0ddb983ec269df26442c373cee3072011685
Headers:
x−goog−update−appid: aapocclcgogkmnckokdopfmhonfmgoek,aohghmighlieiainnegkcijnfilokake,apdfllckaahabafndbhieahigkjlhalf,blpcfgokakmgnkcojhhkbfbldkacnbeo,felcaaldnbdncclmgdcncolpebgiejap ˜$\ldots$˜
<Plus 2315B of POST data similar to previous requests of this type>

Response is 371B of application/json content, related to extensions, similar to previous such responses

GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb

Response is 76.12KB of application/octet-stream

GET https://ssl.gstatic.com/safebrowsing/csd/client_model_v5_variation_0.pb

Response is 76.12KB of application/octet-stream, a repeat of the previous request and response. This repetition seems to occur on every reopen.

E. Connections Made When Sitting Idle

GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Parameters:
$req: ChwKDGdvb2dsZWNocm9tZRIMODAuMC. . .
$ct: application/x−protobuf
key: AIzaSyBOti4mM−6x9WDnZIjIey. . .
Response is around 1KB of content type application/x-protobuf.

POST https://clients4.google.com/chrome-sync/experimentstatus
Post body:
\x0bgcm_channel
Response is a cryptic string “0000000000 12 04 32 02 08 01 ..2...” of type application/vnd.google.octet-stream-compressible. This request is presumably related to Google’s sync service, even though it has not been enabled.

GET https://clientservices.googleapis.com/chrome-variations/seed
Parameters:
osname: mac
channel: stable
milestone: 80
Response is HTTP code 304 (“Not Modified”). Based on discussions with Chromium developers this seems to be associated with Chrome field trials[5].

POST https://update.googleapis.com/service/update2/json?cup2key=9:550841509&cup2hreq=37aa51c814ff078593d3638d9a229c5a99221efae418df4e76e281ccd01e1f19
Headers:
x−goog−update−appid: aapocclcgogkmnckokdopfmhonfmgoek,aohghmighlieiainnegkcijnfilokake,apdfllckaahabafndbhieahigkjlhalf,blpcfgokakmgnkcojhhkbfbldkacnbeo,felcaaldnbdncclmgdcncolpebgiejap,ghbmnnjooekpmoecnnnilnnbdlolhkhi,nmmhkkegccagdldgiimedpiccmgmieda,pjkljhegncpnkpknbcohdijeoejaedia,pkedcjkdefgpdelpbcmbmeomcjbeemfm
Response is application/json.

GET http://storage.googleapis.com/update-delta/hfnkpimlhhgieaddgfemjhofmfblmnib/ 5695/5694/f432b1b484e1737ff6d5969a2f775a71a48a4fdd2a92b31f14c8fa70b9682dd6.crxd
Response is 4.36KB of application/octet-stream

This pair of requests seem to be checking for updates to chrome extensions. The POST to update.googleapis.com is similar to requests during the startup of Chrome and contains a request id and a sessionid, but the values seem to change between requests. The response (not shown here) for the extension with appid ”hfnkpimlhhgieaddgfemjhofmfblmnib” has a ”codebase” entry pointing to the storage.googleapis.com URL in the GET request.

[5] See https://cs.chromium.org/chromium/src/base/metrics/field_trial.h

GET https://www.gstatic.com/chrome/config/plugins_3/plugins_mac.json
Response is 1.77KB of application/json relating to Flash, Quicktime etc

F. Connections Generated By Auto-Complete As User Types

Connections generated as user types leith.ie/nothingtosee.html in Chrome browser top bar.

GET https://www.google.com/complete/search
Parameters:
q: l
psi: yl4_OSgxj4pW4MsB
sugkey: AIzaSyBOti4mM−6x9WDnZIjIey. . .
The same psi and sugkey values are repeated in all of the requests below, but to save space are not shown. As noted above, the sugkey value remains constant acrpss fresh installs and seems to be an identifier for Chrome itself. The psi value changes across fresh installs but remains constant across browser restarts. Response is a javascript fragment:
)]}’[”l”,[”lewis burton”,”liverpool”,”love island”,”linkedin”,”littlewoods ”,”lotto”,”lidl”,”laura whitmore”,”lighthouse cinema”,”livescore”,”liverpool fc ”,”lifestyle”,”little women”,”liverpool fixtures”,”leeds united”,”love holidays ”,”lewis capaldi”,”lotto.ie”,”lifestyle sports”,”ladbrokes”],<...>

GET https://www.google.com/complete/search
q: le
Response:
)]}’ [”le”,[”lewis burton”,”leap card”,”leeds united”,”leo varadkar”,”lewis capaldi”,”leinster rugby”,”lewis burton instagram”,”le mans 66”,”leicester”,” leinster vs cheetahs”,”lego”,”league of ireland”,”levis”,”lemon tree”,”lewis burton twitter”,”let it snow”,”leeds”,”leeds fixtures”,”lebron james”,”leeds united news”],<...>

GET https://www.google.com/complete/search
q: leith
Response:
)]}’[”leith”,[”leith”,”leith edinburgh”,”leithreas”,”leith walk”,”leith agency”,”leith restaurants”,”leith to edinburgh city centre”,”leithsceal”,”leith walk edinburgh”,”leith beach”,”leithleasach”,”leitheid”,”leitheoireacht”,” leithead”,”leitrim”,”leith arches”,”leiths how to cook”,”leith chop house”,” leith theatre”,”leith school of art”],<...>

GET https://www.google.com/complete/search
q: leith.
Response:
)]}’[”leith.”,[”leith honda”,”leith toyota”,”leith hill”,”leith bmw”,”leith edinburgh”,”leith theatre”,”leith clothing”,”leith nissan”,”leith acura”,”leith walk”,”leith hill place”,”leith honda raleigh”,”leith mount surgery”,”leith cars”,”leith restaurants”,”leith jeep”,”leith porsche”,”leith academy”,”http:// leith.com”,”http://leith.co.uk”],<...>

GET https://74.125.193.103/complete/search
q: leith.ie
Response:
)]}’[”leith.ie”,[”daft.ie leith east tralee”],,<...>

Plus requests and responses for “leith.ie/”, “leith.ie/n”, “leith.ie/not”, “leith.ie/noth”, “leith.ie/nothing”, “leith.ie/nothingt”, “leith.ie/nothingto”, “leith.ie/nothingtos”, “leith.ie/nothingtosee”, “leith.ie/nothingtosee.”, “leith.ie/nothingtosee.h”, “leith.ie/nothingtosee.ht”, “leith.ie/nothingtosee.htm”, “leith.ie/nothingtosee.html”.

That is, a total of 19 requests.

II. Mozilla Firefox

A. Connections On First Startup

GET http://detectportal.firefox.com/success.txt
GET http://detectportal.firefox.com/success.txt?ipv4
The response to both is "success"

POST https://location.services.mozilla.com6/v1/country?key=7e40f68c-7938-4c5d-9f95-. . .
{}
The key value is observed to remain unchanged across fresh installs. According to the Mozilla Location Services API docs[6] *it is used to regulate API usage. The response to*
json: {"country_code": "IE", "country_name": "Ireland" }

GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=fxmonitor-breaches&bucket=main
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=message-groups&bucket=main
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/fxmonitor-breaches?_expected=1580917139624
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/ changes/records?collection=cfr-fxa&bucket=main
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/fxmonitor-breaches/records?_expected=1580917139624&_sort=-last_modified
GET https://www.mozilla.org/privacy/firefox/
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/cfr-fxa?_expected=1570801254189
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/cfr-fxa/records?_expected=1570801254189&_sort=-last_modified
GET https://content-signature-2.cdn.mozilla.net/chains/remote-settings.content-signature.mozilla.org-2020-03-25-15-04-24.chain
GET https://www.mozilla.org/en-US/privacy/firefox/
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/ms-language-packs/records/cfr-v1-en-US
GET https://firefox.settings.services.mozilla.com/v1/
GET https://www.mozilla.org/media/js/BUNDLES/site.133e404d326d.js
GET https://www.mozilla.org/media/img/placeholder.71a50dbba44c.png
GET https://www.mozilla.org/media/protocol/img/logos/firefox/browser/developer/logo-sm.d3157a6ac671.png
GET https://www.mozilla.org/media/protocol/img/logos/firefox/browser/nightly/logo-sm.751c5555e455.png
GET https://www.mozilla.org/media/protocol/img/logos/firefox/browser/logo-sm.f2523d97cbe0.png
GET https://www.mozilla.org/media/protocol/img/logos/firefox/browser/beta/logo-sm.d1b49e50ffb7.png
GET https://www.mozilla.org/media/protocol/img/logos/firefox/browser/logo-md.f0603b4c28b4.png
GET https://www.mozilla.org/media/css/BUNDLES/privacy_protocol.f4452fb710b7.css
GET https://www.mozilla.org/media/js/BUNDLES/privacy_firefox.7c639bacfbdc.js
GET https://www.mozilla.org/media/js/BUNDLES/common-protocol.7dbe588589cc.js
GET https://www.mozilla.org/media/js/BUNDLES/stub-attribution.4e24eb9b8c65.js
GET https://www.mozilla.org/media/js/BUNDLES/privacy_protocol.ada10ecc4648.js
GET https://www.mozilla.org/media/css/BUNDLES/protocol-core.f0fd276209f6.css

GET https://search.services.mozilla.com/1/firefox/73.0/release/en-US/IE/default/default
The response to json: { "cohort": "nov17−1","interval": 86400,"settings": {"visibleDefaultEngines": ["amazondotcom", "bing","ebay−ie", "google","twitter","wikipedia", "ddg"]}}

GET https://firefox.settings.services.mozilla.com/main-workspace/ms-language-packs/d94084ad-c828-41b8-8ec9-b01d8620245d.ftl
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=cfr&bucket=main
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/cfr?_expected=1581523408218

[6]See https://ichnaea.readthedocs.io/en/latest/api/index.html and https://ichnaea.readthedocs.io/en/latest/api/region.html

GET https://www.mozilla.org/media/protocol/img/logos/firefox/logo-word-hor-sm-high-res.11cb1d47b984.png
GET https://www.mozilla.org/media/protocol/img/icons/social/twitter/white.3dbd28e41ea3.svg
GET https://www.mozilla.org/media/protocol/img/logos/mozilla/white.612a25fa976b.svg
GET https://www.mozilla.org/media/protocol/img/icons/social/instagram/white.7ca00b3abbfd.svg
GET https://www.mozilla.org/media/fonts/Metropolis-Bold.6a80125e795a.woff2
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/cfr/records?_expected=1581523408218&_sort=-last_modified
GET https://www.mozilla.org/media/fonts/Metropolis-Medium.97c97a09cc75.woff2
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=message-groups&bucket=main
GET https://www.mozilla.org/media/fonts/Inter-Bold.0564381b22b2.woff2
GET https://www.mozilla.org/media/fonts/Inter-Regular.d55e957612a3.woff2

POST https://shavar.services.mozilla.com/downloads
Parameters:
client: navclient−auto−ffox
appver: 73.0
pver: 2.2

GET https://www.mozilla.org/media/fonts/Inter-Italic.d6a4e2b82a0b.woff2

Firefox now opens a web socket with push.services.mozilla.com and sends a hello message
GET https://push.services.mozilla.com/
Headers:
Origin: wss://push.services.mozilla.com/
Sec−WebSocket−Protocol: push−notification
Sec−WebSocket−Extensions: permessage−deflate
Sec−WebSocket−Key: E+vT/vB8eaMUr4JSVR0+Jw==
From inspection of the source[7] *the Sec-WebSocket-Key value is set randomly by Firefox. The response has*
header Sec−WebSocket−Accept: 4GeWGLVVQj+xdFk/VjsvO84hf68=
192.168.0.17:59936 -> WebSocket 1 message -> push.services.mozilla.com:443/ {"messageType":"hello","broadcasts":{},"use_webpush":true}
192.168.0.17:62874 <- WebSocket 1 message <- push.services.mozilla.com:443/ {"messageType":"hello","uaid":"**332024d750734458bc95724268a7b163**","status":200,"use_webpush":true,"broadcasts":{}}
Observe that push.services.mozilla.com transmits the uaid value to Firefox over the web socket in its reply to Firefox's hello. This value is included by Firefox in later messages. The value changes between runs of fresh installs of Firefox but persists across restarts.

GET https://snippets.cdn.mozilla.net/6/Firefox/73.0.1/20200217142647/Darwin_x86_64-gcc3/en-US/release/Darwin\%2018.7.0/default/default/

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/undesired-events/1/d7a2197f-8e2a-2f4b-90af-676caa029008
{ "addon_version": "20200207195153",
"event": "ASR_RS_NO_MESSAGES",
"event_context": "message−groups",
"impression_id": "{**f361e385-1630-ed4b-9312-781ebe538aaa**}",
"locale": "en−US",
"message_id": "n/a",
"release_channel": "release",
"version": "73.0"}
Note the impression_id value transmitted by Firefox to incoming.telemetry.mozilla.org. This is repeated in later communication. The value changes between runs of fresh installs of Firefox. According to Firefox documentation[8]*, impression_id is "The unique impression identifier for a specific client."*

GET https://snippets.cdn.mozilla.net/us-west/bundles-

[7]See function WebSocketChannel::SetupRequest() in file netwerk/protocol/websocket/WebSocketChannel.cpp.
[8]See https://github.com/mozilla/activity-stream/blob/master/docs/v2-system-addon/data_dictionary.m

pregen/Firefox/release/en-us/default.json
GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=whats-new-panel\&bucket=main
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/whats-new-panel?_expected=1581008480228
GET https://tracking-protection.cdn.mozilla.net/social-tracking-protection-facebook-digest256/73.0/1578954954
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/whats-new-panel/records?_expected=1582299210040&_sort=-last_modified
GET https://tracking-protection.cdn.mozilla.net/except-flashallow-digest256/1490633678
GET https://tracking-protection.cdn.mozilla.net/allow-flashallow-digest256/1490633678
GET https://tracking-protection.cdn.mozilla.net/social-tracking-protection-linkedin-digest256/73.0/1578954954
GET https://www.mozilla.org/media/img/favicons/mozilla/favicon-196x196.2af054fea211.png
GET https://www.mozilla.org/media/img/favicons/mozilla/favicon.d25d81d39065.ico
GET https://mozilla.org/set_hsts.gif
GET https://tracking-protection.cdn.mozilla.net/google-trackwhite-digest256/1579741547
GET https://tracking-protection.cdn.mozilla.net/analytics-track-digest256/73.0/1581379643
GET https://snippets.cdn.mozilla.net/media/icons/7fb82260-cac3-4e8e-b5e4-549fb24cf640.png
GET https://snippets.cdn.mozilla.net//media/icons/5878847e-a1fb-4204-aad9-09f6cf7f99ee.png
GET https://tracking-protection.cdn.mozilla.net/except-flash-digest256/1494877265
GET https://tracking-protection.cdn.mozilla.net/except-flashsubdoc-digest256/1517935265
GET https://tracking-protection.cdn.mozilla.net/mozstd-trackwhite-digest256/73.0/1582074377
GET https://tracking-protection.cdn.mozilla.net/block-flashsubdoc-digest256/1512160865
GET https://tracking-protection.cdn.mozilla.net/base-fingerprinting-track-digest256/73.0/1581379643

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/onboarding/1/241a596f-0487-254d-a872-a7e95aa7f305

{ ”addon_version”: ”20200207195153”,
”client_id”: ”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
”event”: ”IMPRESSION”,
”id”: ”FIRST_RUN”,
”locale”: ”en−US”,
”message_id”: ”TRAILHEAD_1”,
”source”: ”FIRST_RUN”,
version”: ”73.0”}

Observe the client_id value transmitted to incoming.telemetry.mozilla.org. This is also transmitted in later calls to incoming.telemetry.mozilla.org and persists across browser restarts (although it changes on start of a fresh install of Firefox). The structure of the telemetry payload is as described in the Firefox documenation[9].

GET https://tracking-protection.cdn.mozilla.net/social-track-digest256/73.0/1581543360
GET https://tracking-protection.cdn.mozilla.net/social-tracking-protection-twitter-digest256/73.0/1578954954
GET https://tracking-protection.cdn.mozilla.net/content-track-digest256/73.0/1578954954
GET https://tracking-protection.cdn.mozilla.net/block-flash-digest256/1496263270
GET https://tracking-protection.cdn.mozilla.net/base-cryptomining-track-digest256/73.0/1578954954
GET https://tracking-protection.cdn.mozilla.net/mozplugin-block-digest256/1471849627
GET https://tracking-protection.cdn.mozilla.net/ads-track-digest256/73.0/1581543360

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/undesired-events/1/2f45cc3b-fb9f-a447-bc42-5b8fb10b5b92

{”addon_version”: ”20200207195153”,
”event”: ”ASR_RS_NO_MESSAGES”,
”event_context”: ”message−groups”,
”impression_id”: ”{**f361e385-1630-ed4b-9312-781ebe538aaa**}”,
”locale”: ”en−US”,
”message_id”: ”n/a”,
”release_channel”: ”release”,
”version”: ”73.0”}

Observe that the impression_id value matches that used in the earlier call to incoming.telemetry.mozilla.org

GET https://accounts.firefox.com/metrics-flow
Parameters:
utm_source: activity−stream
utm_campaign: firstrun−release
utm_medium: referral
entrypoint: activity−stream−firstrun
form_type: email
utm_term: trailhead−cards−supercharge
The response is application/json: {”deviceId”: ”f96da5b04d3744cd9095e0b1c28d9bb7”,” flowBeginTime”: 1581668134057, ”flowId”: ”b5dd67a71d31e6ec0. . .”}
Firefox now makes a second (duplicate?) call to accounts.firefox.com:
GET https://accounts.firefox.com/metrics-flow?utm_source=activity-stream&utm_campaign=firstrun-release&utm_medium=referral&entrypoint=activity-stream-firstrun&form_type=email&utm_term=trailhead-cards-supercharge
The response is application/json: {deviceId”: ” e542f56686234976b53e563864f04627”, ”flowBeginTime”: 581668134051, ” flowId”: ”34ebbc4ad32d128c1da060. . .” }
Note the change in the deviceId and flowId values returned by accounts.firefox.com

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/cfr/1/f365cccf-edbe-534f-876a-aca3e7a7b721

{
”addon_version”: ”20200207195153”,
”bucket_id”: ”FXA_ACCOUNTS_BADGE”,
”event”: ”IMPRESSION”,
”impression_id”: ”{**f361e385-1630-ed4b-9312-781ebe538aaa**}”,
”locale”: ”en−US”,
”message_id”: ”n/a”,
”release_channel”: ”release”,
”source”: ”CFR”,
”version”: ”73.0”
}

192.168.0.17:62874 -> WebSocket 1 message -> push.services.mozilla.com:443/ {”messageType”:”broadcast_subscribe”,” broadcasts”:{”remote−settings/monitor_changes”:”\\”0\\””}}
192.168.0.17:62874 <- WebSocket 1 message <- push.services.mozilla.com:443/ {”messageType”:”broadcast”,”broadcasts”:{” remote−settings/monitor_changes”:”\\”1581628381652\\””}}

GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?_expected=%221581628381652%22
GET https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/ addons?_expected=1581545094556

GET https://aus5.mozilla.org/update/3/GMP/73.0/20200207195153/Darwin_x86_64-gcc3/en-US/release/Darwin\%2018.7.0/default/default/update.xml
This seems to be checking for updates to Firefox components, the response is text/xml:

<?xml version=”1.0”?><updates><addons>
<addon id=”gmp−gmpopenh264” URL=”http://ciscobinary. openh264.org/openh264−macosx64−2 e1774ab6dc6c43debb0b5b628bdf122a391d521.zip” hashFunction=”sha512” hashValue=”fc1ddb4b7cff2f27a0f10d. . .” size=”466258” version =”1.8.1.1”/>
<addon id=”gmp−widevinecdm” URL=”https://redirector.gvt1.com /edgedl/widevine−cdm/4.10.1582.2−mac−x64.zip” hashFunction=”sha512” hashValue=”9ad5288a8c6488dc46ff. . .” size=”4270381” version =”4.10.1582.2”/></addons> </updates>

GET https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/ addons/records?_expected=1581545094556&_sort=-last_modified&_since=1580842055124

[9]See https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/data/activation-ping.html

GET https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/plugins

GET http://ciscobinary.openh264.org/openh264-macosx64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip

GET https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/plugins/records?_expected=1581976608692&_sort=-last_modified&_since=1579624011498
GET https://firefox.settings.services.mozilla.com/v1/buckets/security-state/collections/onecrl?_expected=1581628280099
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-skip-urls?_expected=1579735982667
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-skip-urls/records?_expected=1579735982667&_sort=-last_modified&_since=1571936118309

GET https://redirector.gvt1.com/edgedl/widevine-cdm/4.10.1582.2-mac-x64.zip
The response is: moved to https://r3—sn-q0cedn7s.gvt1.com/edgedl/edgedl/widevine-cdm/4.10.1582.2-mac-x64.zip, which is called below.

GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/public-suffix-list?_expected=1575468539758
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/public-suffix-list/records?_expected=1575468539758&_sort=-last_modified
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/hijack-blocklists
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/language-dictionaries
GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/anti-tracking-url-decoration

GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Parmeters:
key: AIzaSyC7jsptDS3am4tPx4r3. . .
$req: ChUKE25hdmNsaWVudC1hdXRvLWZmb3. . .
The key value seems to be the same for all instances of Firefox. The comments for Chrome regarding thge $req value also apply to Firefox. The response is 1KB of application/x-protobuf

GET https://r3—sn-q0cedn7s.gvt1.com/edgedl/widevine-cdm/4.10.1582.2-mac-x64.zip?cms_redirect=yes&mip=37.228.245.107&mm=28&mn=sn-q0cedn7s&ms=nvh&mt=1581668115&mv=m&mvi=2&pl=19&shardbypass=yes

GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/sites-classification
GET https://firefox.settings.services.mozilla.com/v1/buckets/pinning/collections/ pins?_expected=1485794868067
GET https://firefox.settings.services.mozilla.com/v1/buckets/pinning/collections /pins/records?_expected=1485794868067&_sort=-last_modified
GET https://firefox.settings.services.mozilla.com/chains/pinning-preload.content-signature.mozilla.org-2020-03-25-15-04-22.chain
GET https://firefox.settings.services.mozilla.com/v1/buckets/blocklists/collections/ gfx

GET http://detectportal.firefox.com/success.txt
GET http://detectportal.firefox.com/success.txt?ipv4

B. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar (there are no extraneous connections).

GET http://leith.ie/nothingtosee.html
GET http://leith.ie/favicon.ico

C. Connections Made On Re-Open After Close

(i) Connections On First Close

POST https://incoming.telemetry.mozilla.org/submit/telemetry/03206176-b1b4-a348-853e-502461c488f7/event/Firefox/73.0/release/20200207195153?v=4
Header:
User−Agent: pingsender/1.0

<...>
”reason”:”shutdown”,<...>
”sessionId”:”**cebba8d1-5a4e-d94a-b137-97979fec8c28**”,”subsessionId”:”af1fc2f8−178d−c046−bef9−1d1dea283453”,<...>
”clientId”:”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
<...>

POST https://incoming.telemetry.mozilla.org/submit/telemetry/97e80a0a-220d-cf44-a6d2-6a8ed320db31/new-profile/Firefox/73.0/release/20200207195153?v=4
Header:
User−Agent: pingsender/1.0

<...>
”clientId”:”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
<...>

POST https://incoming.telemetry.mozilla.org/submit/telemetry/72a4660b-d0f0-3b40-afd2-024d2ffd874e/first-shutdown/Firefox/73.0/release/20200207195153?v=4
Header:
User−Agent: pingsender/1.0

<...mainly histogram data>
”info”:{”reason”:”shutdown”,<...>
”sessionId”:**cebba8d1-5a4e-d94a-b137-97979fec8c28**”,”subsessionId”:”af1fc2f8−178d−c046−bef9−1d1dea283453”,”previousSessionId”:null,”previousSubsessionId”:null,”subsessionCounter”:1,”profileSubsessionCounter”:1,”sessionStartDate”:”2020−02−13T11:00:00.0 00:00”,”subsessionStartDate”:”2020−02−13T11:00:00.0 00:00”,<...>
”clientId”:”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”
<...>

Note that the value of clientId matches that used earlier. The value of sessionId links two of these POSTs, and also the POST on final close (see below). Note alsio the pingsender sender header: these POST requests seem to be sent by a separate helper process after Firefox has closed[10]*. The format of these telemetry messages is as described in Firefox documentation*[11]

(ii) Connections On First Reopen

GET http://detectportal.firefox.com/success.txt
GET http://detectportal.firefox.com/success.txt?ipv4

GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/ changes/records?collection=message-groups&bucket=main
The response is “Not Modified”

GET https://normandy.cdn.mozilla.net/api/v1/
The response is json:
{ ”action−list”: ”https://normandy.cdn.mozilla.net/api/v1/action/”,
”action−signed”: ”https://normandy.cdn.mozilla.net/api/v1/action/signed/”,
”approvalrequest−list”: ”https://normandy.cdn.mozilla.net/api/v1/approval_request/”,
”classify−client”: ”https://classify−client.services.mozilla.com/api/v1/classify_client/”,
”extension−list”: ”https://normandy.cdn.mozilla.net/api/v1/extension/”,
”recipe−list”: ”https://normandy.cdn.mozilla.net/api/v1/recipe/”,
”recipe−signed”: ”https://normandy.cdn.mozilla.net/api/v1/recipe/signed/”,

[10]See https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/internals/pingsender.html
[11]See https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/data/event-ping.html

”reciperevision−list”: ”https://normandy.cdn.mozilla.net/api/v1/recipe_revision/” }
Firefox documentation[12] *indicates that Normandy is used for A/B testing and user surveys.*

GET https://13.224.69.117/v1/buckets/monitor/collections/changes/records?collection=message-groups&bucket=main
The response is “Not Modified”

GET https://classify-client.services.mozilla.com/api/v1/classify_client/
The response is json:
{”country”: ”IE”, ”request_time”: ”2020−02−13T12:02:23.240998153Z”}

GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records?collection=normandy-recipes-capabilities&bucket=main
The response is “Not Modified”

GET https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/normandy-recipes-capabilities?_expected=1581552069173
The response is json

GET https://push.services.mozilla.com/
Header:
Sec−WebSocket−Key: yUXTd3reQB6MzGNVoGNWxQ==

192.168.0.17:59999 -> WebSocket 1 message -> push.services.mozilla.com:443/ {”messageType”:”hello”,”broadcasts”:{”remote−settings/monitor_changes”:”\\”1581628381652\\””},”use_webpush”:true,”uaid”:”**332024d750734458bc95724268a7b163**”}
The uaid value matches that transmitted by push.services.mozilla.com in the previous hello message

GET https://accounts.firefox.com/metrics-flow?utm_source=activity-stream&utm_campaign=firstrun-release&utm_medium=referral&entrypoint=activity-stream-firstrun&form_type=email&utm_term=trailhead-cards-supercharge
The response is json: {”deviceId”: ”a465c8fe6ec340ba8390a6dfe4623ecf”, ”flowBeginTime”: 1581595343622,”flowId”: ”2d9f09a4fa424c91023cf14446e2d05a86a8952ddb2dcbc06aa8966ab84645a7”}

GET https://accounts.firefox.com/metrics-flow?utm_source=activity-stream&utm_campaign=firstrun-release&utm_medium=referral&entrypoint=activity-stream-firstrun&form_type=email&utm_term=trailhead-cards-supercharge
The response is json: {”deviceId”: ”fc7aa2d616f24005adfa0a8fe264119e”,” flowBeginTime”: 1581668302740,”flowId”: ”8f18371d4df7914c0da40e476550f4136687d94f18909c2cf59551f2832d71ba”}

GET https://accounts.firefox.com/metrics-flow?utm_source=activity-stream&utm_campaign=firstrun-release&utm_medium=referral&entrypoint=activity-stream-firstrun&form_type=email&utm_term=trailhead-cards-supercharge
The response is json: {”deviceId”: ”62b00c2cc75f4e0e8d2eb665ce68e4e0”,”flowBeginTime”: 1581668302744,,”flowId”: ”79a8b1a5c6ce2f082ec2a13cb3cdaca07c2dc6d1f1b647ec739995cf5d6587e0”}

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/undesired-events/1/c347eb24-a42f-0948-98b5-857a2c820e07
{ ”addon_version”: ”20200207195153”,
”event”: ”ASR_RS_NO_MESSAGES”,
”event_context”: ”message−groups”,
”impression_id”: ”{**f361e385-1630-ed4b-9312-781ebe538aaa**}”,}

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/undesired-events/1/d78245cb-ae0b-ea48-a569-b33a6452d965
{ ”addon_version”: ”20200207195153”,
”event”: ”ASR_RS_NO_MESSAGES”,
”event_context”: ”message−groups”,
”impression_id”: ”{**f361e385-1630-ed4b-9312-781ebe538aaa**}”,}

The impression_id value in these two POSTs matches that previously transmitted to incoming.telemetry.mozilla.org

[12]See https://mozilla.github.io/normandy/

192.168.0.17:59999 <- WebSocket 1 message <- push.services.mozilla.com:443/ {”messageType”:”hello”,”uaid”:”**332024d750734458bc95724268a7b163**”,”status”:200,”use_webpush”:true,”broadcasts”:{}}

POST https://incoming.telemetry.mozilla.org/submit/messaging-system/onboarding/1/0dca1ff7-332e-6d4c-88e7-1f8477964ecc
{ ”addon_version”: ”20200207195153”,
”client_id”: ”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
”event”: ”IMPRESSION”,
”id”: ”FIRST_RUN”,
”message_id”: ”EXTENDED_TRIPLETS_1”,
”source”: ”FIRST_RUN”,}
Note that the value of clientId matches that used earlier.

POST https://34.212.242.166/submit/messaging-system/cfr/1/5c1489e8-399e-9b40-8d40-eca4f25085a0
{”addon_version”: ”20200207195153”,
”bucket_id”: ”FXA_ACCOUNTS_BADGE”,
”event”: ”IMPRESSION”,
”impression_id”: ”{**f361e385-1630-ed4b-9312-781ebe538aaa**}”,
”source”: ”CFR”,”}
The impression_id value matches that used earlier

GET https://normandy.cdn.mozilla.net/api/v1/
GET https://classify-client.services.mozilla.com/api/v1/classify_client/
The response is json:
{”country”: ”IE”,”request_time”: ”2020−02−13T12:02:51.477863245Z”}

POST https://34.212.242.166/submit/telemetry/259b07c1-3996-ec49-a2a5-74df9397c3dc/main/Firefox/73.0/release/20200207195153?v=4
<...>,
”clientId”: ”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
<...>
The value of clientId matches that used earlier.

GET http://detectportal.firefox.com/success.txt
GET http://detectportal.firefox.com/success.txt?ipv4

GET https://13.224.69.17/update/6/Firefox/73.0/20200207195153/Darwin_x86_64-gcc3/ en-US/release/Darwin%2018.7.0/ISET:SSE4_2,MEM:16384/ default/default/update.xml

(iii) Connections On Final Close

POST https://incoming.telemetry.mozilla.org/submit/telemetry/cdbebd45-af9f-2a40-a6c0-0344065a974f/main/Firefox/73.0/release/20200207195153?v=4
Header:
User−Agent: pingsender/1.0

<mainly histogram data>
”info”:{”reason”:”shutdown”,<...>,
”sessionId”:”93835dcf−6c03−b049−a639−85a95e994099”,
”subsessionId”:”35565be3−8eac−4c40−a86b−045018bbb061”,”previousSessionId”:”**cebba8d1-5a4e-d94a-b137-97979fec8c28**”,”previousSubsessionId”:”af1fc2f8−178d−c046−bef9−1d1dea283453”<...>,
”clientId”:”**0d0214ec-74d8-5640-ae0e-e3dc8952e6aa**”,
<...>
The value of clientId matches that used earlier. The value of previousSessionId also matches the value of sessionId transmitted on previous close event, allowing sessions to be linked. Firefox documentation[13] *says “A session is the time from when Firefox starts until it shuts down”.*

D. Connections Made When Sitting Idle

POST https://shavar.services.mozilla.com/downloads
Parameters:
client: navclient−auto−ffox
appver: 72.0
pver: 2.2

[13]See https://firefox-source-docs.mozilla.org/toolkit/components/telemetry/concepts/sessions.html

Response is : n:3600 .

GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Parameters:
key: AIzaSyC7jsptDS3am4tPx4r. . .
$req: ChUKE25hdmNsaWVud. . .
The key value seems to be the same for all Firefox instances. Response is application/x-protobuf

GET https://firefox.settings.services.mozilla.com/v1/buckets/monitor/collections/changes/records
Parameters:
_since: ”1581552071874”
_expected: ”1581615120425”
Response is application/json, e.g.:


```
{
    ”data”: [
        {
            ”bucket”: ”main”,
            ”collection”: ”normandy−recipes”,
            ”host”: ”firefox.settings.services.mozilla.com”,
            ”id”: ”8da7db1e−dffb−18c9−2efe−0e9d7459a0f4”,
            ”last_modified”: 1581615120425
        },
        {
            ”bucket”: ”main”,
            ”collection”: ”normandy−recipes−capabilities”,
            ”host”: ”firefox.settings.services.mozilla.com”,
            ”id”: ”e9f76a09−1c31−7dce−7c40−8abfbcfb244d”,
            ”last_modified”: 1581615116029
        }
    ]
}
```


Other responses from firefox.settings.services.mozilla.com include:


```
        {
            ”bucket”: ”security−state−preview”,
            ”collection”: ”onecrl”,
            ”host”: ”firefox.settings.services.mozilla.com”,
            ”id”: ”58d1976f−6e75−7728−79da−f4860ed35de5”,
            ”last_modified”: 1581547558126
        },
        {
            ”bucket”: ”blocklists”,
            ”collection”: ”addons”,
            ”host”: ”firefox.settings.services.mozilla.com”,
            ”id”: ”b7f595f9−5fc5−d863−b5dd−e5425dcf427a”,
            ”last_modified”: 1581545094556
        },
        {
```


Normandy is used for A/B testing and user surveys, blocklists are for blocking malware extensions.

E. Connections Generated By Auto-Complete As User Types

Connections generated as user types leith.ie/nothingtosee.html in Firefox top bar.

GET https://www.google.com/complete/search
Parameters:
q: le
Response:
[”le”,[”lewis burton”,”leap card”,”leeds united”,”leo varadkar”,”lewis capaldi”,”leinster rugby”,”lewis burton instagram”,”le mans 66”,”leicester”,” leinster vs cheetahs”]]

GET https://www.google.com/complete/search
q: lei
Response:
[”lei”,[”leinster rugby”,”leinster”,”leicester”,”leinster vs cheetahs”,” leixlip”,”leinster hockey”,”leinster fixtures”,”leisureplex”,”leitrim”,”leicester fixtures”]]

GET https://www.google.com/complete/search
q: leit
Response:
[”leit”,[”leitrim”,”leitrim observer”,”leitrim gaa”,”leitrim county council ”,”leith”,”leitmotif”,”leitrim gaa awards”,”leitrim news”,”leitrim lodge hotel ”,”leitrim hotels”]]

GET https://www.google.com/complete/search
q: leith
Response:
[”leith”,[”leith”,”leith edinburgh”,”leithreas”,”leith agency”,”leith restaurants”,”leith to edinburgh city centre”,”leithsceal”,”leith walk edinburgh”,”leith beach”,”leithleasach”]]

Observe that Firefox is less aggressive and terminates requests after the first word i.e. once the “.” in the URL is typed. This behaviour is consistently observed.

III. Brave

A. Connections On First Startup

GET https://static1.brave.com/autofill/hourly/bins.json
braveservicekey: qjVKcxtUybh8WpKNoQ7...

Notes:
1) *The braveservicekey value is constant across restarts and fresh installs. The cookie value changes across restarts and fresh installs*
2) *Response is to set a cookie: __cfduid=fde00148818268db445781a9c26ef13edb1581679109; domain=.brave.com. This cookie seems to be set byCloudFlare for managing security*[14] *and is not echoed in any of the requests below i.e. it seems to be scrubbed by the Brave browser.*
3) *The response also sends a small fragment of json*

GET https://static1.brave.com/autofill/weekly/merchants.json
Response sets same cookie as before and transmits json:
{"cpan_eligible_merchant_wl": ["dump−truck.appspot.com"] }

GET https://laptop-updates.brave.com/promo/custom-headers
Response is json

PUT https://laptop-updates.brave.com/promo/initialize/nonua
```
{
    "api_key": "fe033168−0ff8−4af6−9a7f−...",
    "platform": "osx",
    "referral_code": "BRV001"
}
```
Response is json: {"download_id": "6a8cc3e0−9dca−404b−8dd5−9043bdfe33d0", "referral_code": "BRV001"}
The value of api_key is constant across fresh installs. The download_id value changes.

GET https://laptop-updates.brave.com/1/usage/brave-core?platform=osx-bc&channel=release&version=1.3.115&daily=true&weekly=true&monthly=true&first=true&woi=2020-02-10&ref=BRV001
Response is json

The content of the following requests, and of the responses, is much the same as the chrome extension update requests made by Chrome. The extensions are different however: cldoidikboihgcjfkhdeidbpclkinee "Brave Tor Client Updater (Mac)", cffkpbalmllkdoenhmdmpbkajipdjfam "Brave Ad Block Updater", afalakplffnnnlkncjhbmahjfjhmlkal "Brave Local Data Files Updater", iobjkiknhhkhkgepehpkpogckaebmhlh "Brave NTP sponsored images", oofiananboodjbbmdelgdommihjbkfag "Brave HTTPS Everywhere Updater", hfnkpimlhhgieaddgfemjhofmfblmnib "Crowd Deny" (Certificate revocation list extension). The brave://components window also lists MEI Preload and Crypto Wallets/ as installed.
Note: The POST requests below contain a sessionid, but this changes between requests (unlike for Chrome calls to update.googleapis.com on startup).
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: cldoidikboihgcjfkhdeidbpclkineef
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: hfnkpimlhhgieaddgfemjhofmfblmnib
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: cffkpbalmllkdoenhmdmpbkajipdjfam
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: afalakplffnnnlkncjhbmahjfjhmlkal
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: iobjkiknhhkhkgepehpkpogckaebmhlh
POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: oofiananboodjbbmdelgdommihjbkfag
POST https://componentupdater.brave.com/service/update2/json
X−Goog−Update−AppId: hfnkpimlhhgieaddgfemjhofmfblmnib
GET https://brave-core-ext.s3.brave.com/release/afalakplffnnnlkncjhbmahjfjhmlkal/extension_1_0_22.crx
GET https://brave-core-ext.s3.brave.com/release/iobjkiknhhkhkgepehpkpogckaebmhlh/extension_1_0_18.crx
GET https://crlsets.brave.com/edgedl/release2/chrome_component/elUSxscyMwF1pK42ZcxFxg_5696/YrJlxQpgdDl87dB9XSR9Ig
POST https://go-updater.brave.com/extensions
POST https://go-updater.brave.com/extensions
POST https://componentupdater.brave.com /service/update2/json
GET https://brave-core-ext.s3.brave.com/release/oofiananboodjbbmdelgdommihjbkfag/extension_1_0_14.crx
GET https://tor.bravesoftware.com/release/cldoidikboihgcjfkhdeidbpclkineef/extension_1_0_8.crx
POST https://go-updater.brave.com/extensions
POST https://go-updater.brave.com/extensions
GET https://199.232.26.217/release/cffkpbalmllkdoenhmdmpbkajipdjfam/extension_1_0_480.crx
POST https://go-updater.brave.com/extensions

GET https://static.brave.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
Response resets the CloudFlare cookie: set−cookie: __cfduid=d463598d9d2e7b03fc122d60a0d6173031581679119

GET https://static.brave.com/safebrowsing/csd/client_model_v5_variation_0.pb
Response is 76.12KB of application/octet-stream

POST https://p3a.brave.com/
Header:
X−Brave−P3A: ?1

CesyWJC+2AQCEkgDLG90aGV...

According to Brave documentation P3A is coarse telemetry data encoded base64. Decoding the above into hex and ASCII gives:
09 eb 32 58 90 be d8 04 02 12 48 03 ,other,osx−bc,1.3.115,release ,207,207,other,1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 41 00 bb a0 63 50 c9 54
There are some details on this content here: https://github.com/brave/brave-browser/wiki/P3A and the Brave brower source code routine GenerateP3AMessage(). No cookie or other identifier is sent with this POST to p3a.brave.com.

GET https://104.28.22.242/chrome/config/plugins_3/plugins_mac.json
Response is 1.67KB of application/json containing flash, quicktime data etc, plus the CloudFlare cookie is reset to:
__cfduid=dfc71a55da0fd0b6f081be5288acecced1581679169

POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: iobjkiknhhkhkgepehpkpogckaebmhlh, cldoidikboihgcjfkhdeidbpclkineef,hfnkpimlhhgieaddgfemjhofmfblmnib, gcmjkmgdlgnkkcocmoeiminaijmmjnii, bklopemakmnopmghhmccadeonafabnal, giekcmmlnklenlaomppkphknjmnnpneh,jflookgnkcckhobaglndicnbbgbonegd, llkgjffcdpffmhiakmfcdcblohccpfmo,khaoiebndkojlmppeemjhbpbandiljpe, aemomkdncapdnfajjbbcbdebjljbpmpj,cffkpbalmllkdoenhmdmpbkajipdjfam, oofiananboodjbbmdelgdommihjbkfag,afalakplffnnnlkncjhbmahjfjhmlkal
Response is 2.0KB application/json

POST https://go-updater.brave.com/extensions
X−Goog−Update−AppId: ggkkehgbnfjpeggfpleeakpidbkibbmn
POST https://componentupdater.brave.com/service/update2/json
X−Goog−Update−AppId: ggkkehgbnfjpeggfpleeakpidbkibbmn
Response is 486B application/json

GET https://redirector.brave.com/edgedl/release2/AObXHnCOjk4CJSdj9hZpiG0_0.5/NgVV6gZZia2sroedLxGb9Q
The request URL is from the codebase value returned by the previous request. Response is 3.69KB application/octet-stream

POST https://go-updater.brave.com/extensions
POST https://componentupdater.brave.com/service/update2/json
Response is 171B application/json

GET https://safebrowsing.brave.com/v4/threatListUpdates:fetch
Parameters:
$req: ChYKCGNoc...
$ct: application/x−protobuf
key: dummytoken
Observe the dummy key value. Decoding $req as a base64 string yields "chromium 80.1.3.115". Response is 5.49MB of application/x-protobuf

[14] See https://support.cloudflare.com/hc/en-us/articles/200170156-Understanding-the-Cloudflare-Cookies

B. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar (there are no extraneous connections).

GET http://leith.ie/nothingtosee.html
GET http://leith.ie/favicon.ico

C. Connections Made On Re-Open After Close

GET https://static1.brave.com/autofill/hourly/bins.json
braveservicekey: qjVKcxtUybh8WpKNoQ7...

1) *Response is to reset the CloudFlare cookie to: __cfduid=da904267bf31abd2c595d9cf8b5f7a2271581679242*
2) *And sends same json fragment as before.*

GET https://static1.brave.com/autofill/weekly/merchants.json
Response sets same cookie as before and transmits json:
{"cpan_eligible_merchant_wl": ["dump-truck.appspot.com"] }

GET http://leith.ie/favicon.ico
Upon reopen Brave shows the page previously navigated to.

GET https://laptop-updates.brave.com/promo/custom-headers

GET
https://static.brave.com/safebrowsing/csd/client_model_v5_variation_0.pb
Response is 76.12KB application/octet-stream and resets the CloudFlare cookie to: __cfduid=da02a5d909ed582f2b321c5f49bb69ebd1581679251

GET
https://static.brave.com/safebrowsing/csd/client_model_v5_ext_variation_0.pb
Response is a duplicate of previous one. Note that chrome has the same sort of duplication

POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: hfnkpimlhhgieaddgfemjhofmfblmnib
POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: oofiananboodjbbmdelgdommihjbkfag
POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: cldoidikboihgcjfkhdeidbpclkineef
POST https://1go-updater.brave.com/extensions
X-Goog-Update-AppId: cffkpbalmllkdoenhmdmpbkajipdjfam
POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: afalakplffnnnlkncjhbmahjfjhmlkal
POST https://go-updater.brave.comextensions
X-Goog-Update-AppId: iobjkiknhhkhkgepehpkpogckaebmhlh
POST https://go-updater.brave.com/service/update2/json
X-Goog-Update-AppId: hfnkpimlhhgieaddgfemjhofmfblmnib
POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: iobjkiknhhkhkgepehpkpogckaebmhlh,
cldoidikboihgcjfkhdeidbpclkineef,gcmjkmgdlgnkkcocmoeiminaijmmjnii,
llkgjffcdpffmhiakmfcdcblohccpfmo,khaoiebndkojlmppeemjhbpbandiljpe,
giekcmmlnklenlaomppkphknjmnnpneh,
bklopemakmnopmghhmccadeonafabnal,jflookgnkcckhobaglndicnbbgbonegd,
hfnkpimlhhgieaddgfemjhofmfblmnib,aemomkdncapdnfajjbbcbdebjljbpmpj,
oofiananboodjbbmdelgdommihjbkfag,cffkpbalmllkdoenhmdmpbkajipdjfam,
afalakplffnnnlkncjhbmahjfjhmlkal
As already noted, these requests contain a requestid and sessionid but the values change between requests.

POST https://p3a.brave.com/
X-Brave-P3A: ?1
Content-Type: application/base64

Cfv4sUBVhy03EkgDLG90aGVy...

POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: ggkkehgbnfjpeggfpleeakpidbkibbmn
POST https://componentupdater.brave.com/service/update2/json
X-Goog-Update-AppId: ggkkehgbnfjpeggfpleeakpidbkibbmn

D. Connections Made When Sitting Idle

GET https://safebrowsing.brave.com/v4/threatListUpdates:fetch
Host: safebrowsing.brave.com
Parameters:
$req: ChUKCGNocm9ta...
key: dummytoken
Response is application/x-protobuf

POST https://p3a.brave.com/
X-Brave-P3A: ?1
Content-Type: application/base64

Cc7wA/VwhQWxEkgDLG90aGVyLG9zeC1iYywx...
This is uploading coarse telemetry data.

GET
https://updates.bravesoftware.com/sparkle/Brave-Browser/stable/appcast.xml
Response is text/xml with a bunch of software version numbers and URLs. This is checking for Brave updates.

GET https://laptop-updates.brave.com/promo/custom-headers
Response is application/json: [{ "cookieNames": [],"domains": ["coinbase.com","api.coinbase.com"],"expiration": 31536000000,"headers": {"X-Brave-Partner": "coinbase"} <etc>

POST https://go-updater.brave.com/extensions
X-Goog-Update-AppId: cldoidikboihgcjfkhdeidbpclkineef,
hfnkpimlhhgieaddgfemjhofmfblmnib,giekcmmlnklenlaomppkphknjmnnpneh,
bklopemakmnopmghhmccadeonafabnal,llkgjffcdpffmhiakmfcdcblohccpfmo,
jflookgnkcckhobaglndicnbbgbonegd,aemomkdncapdnfajjbbcbdebjljbpmpj,
gcmjkmgdlgnkkcocmoeiminaijmmjnii,khaoiebndkojlmppeemjhbpbandiljpe,
oofiananboodjbbmdelgdommihjbkfag,cffkpbalmllkdoenhmdmpbkajipdjfam,
afalakplffnnnlkncjhbmahjfjhmlkal
The POST request includes a sessionid but the value changes between requests. Response is application/json giving version numbers and URLs. This is checking for updates to chrome extensions.

E. Connections Generated By Auto-Complete As User Types

No connections generated as user types leith.ie/nothingtosee.html in Brave top bar (the auto-complete setting is disabled by default).

IV. Apple Safari

A. Connections On First Startup

GET https://www.icloud.com/
Response is 12.9KB of text/html

GET https://www.apple.com/
Response is 9.82KB of text/html and sets cookies:
set−cookie: geo=IE; path=/; domain=.apple.com
set−cookie: ccl=vap5gNZIyB3y7UIj9eKfIw==; path=/; domain=.apple.com
The value of the ccl cookie is reset by the next call to www.apple.com.

GET https://www.icloud.com/static/touch-icon-pad-retina.png
Response is 404 Not Found
GET https://www.icloud.com/apple-touch-icon-precomposed.png
Response is 404 Not Found
GET https://www.icloud.com/apple-touch-icon.png
Response is 404 Not Found
GET https://www.icloud.com/favicon.ico

GET https://www.icloud.com/
Response is 12.9KB of text/html (duplicate of first request, this is seen consistently)

GET https://www.icloud.com/static/touch-icon-pad-retina.png
Response is 404 Not Found
GET https://www.icloud.com /apple-touch-icon-precomposed.png
Response is 404 Not Found
GET https://www.apple.com/apple-touch-icon-precomposed.png
Response is 404 Not Found and sets cookies:
set−cookie: geo=IE; path=/; domain=.apple.com
set−cookie: ccl=**lx6FLhfAL5+0s30VZQu35Q==**; path=/; domain=.apple.com
The value of the ccl cookie changes across fresh restarts.

GET https://www.icloud.com/apple-touch-icon.png
Response is 404 Not Found
GET https://www.icloud.com/favicon.ico

GET https://www.apple.com/apple-touch-icon.png
Headers:
cookie: ccl=**lx6FLhfAL5+0s30VZQu35Q==**; geo=IE

GET https://www.yahoo.com/
Response sets cookie:
set−cookie: RRC=st=1581777407&cnt=1; expires=Sat, 15−Feb−2020 14:37:17 GMT; path=/; domain=.www.yahoo.com; HttpOnly

GET https://www.bing.com/
Response sets cookies:
set−cookie: SRCHD=AF=NOFORM; domain=.bing.com; expires=Thu, 11−Mar−2021 14:36:47 GMT; path=/
set−cookie: SRCHUID=V=2&GUID=EB49DD6183E84C448C7F2574C4D022C1&dmnchg=1; domain=.bing.com; expires=Thu, 11−Mar−2021 14:36:47 GMT; path=/
set−cookie: SRCHUSR=DOB=20200215; domain=.bing.com; expires=Thu, 11−Mar−2021 14:36:47 GMT; path=/
set−cookie: _SS=SID=25DB8F5829776804323B81292877696F; domain=.bing.com; path=/
set−cookie: ULC=; domain=.bing.com; expires=Fri, 14−Feb−2020 14:36:47 GMT; path=/
set−cookie: _HPVN=CS=eyJQbiI6eyJDbiI6MSwi. . .; domain=.bing.com; expires=Thu, 11−Mar−2021 14:36:47 GMT; path=/
strict−transport−security: max−age=31536000; includeSubDomains; preload
x−msedge−ref: Ref A: 2410E7F3683C47E5975C3BAC6A6D2B9F Ref B: DB3EDGE1617 Ref C: 2020−02−15T14:36:47Z
set−cookie: _EDGE_S=F=1&SID=25DB8F5829776804323B81292877696F; path=/; httponly; domain=bing.com
set−cookie: _EDGE_V=1; path=/; httponly; expires=Thu, 11−Mar−2021 14:36:47 GMT; domain=bing.com
set−cookie: MUID=32561F3ED62A6EEE204E114FD72A6F02; samesite=none; path=/; secure; expires=Thu, 11−Mar−2021 14:36:47 GMT; domain=bing.com
set−cookie: MUIDB=32561F3ED62A6EEE204E114FD72A6F02; path=/; httponly; expires=Thu, 11−Mar−2021 14:36:47 GMT

GET https://ie.yahoo.com/?p=us
Response sets cookies:
set−cookie: GUCS=AT1BOMpq; Max−Age=1800; Domain=.yahoo.com; Path=/; Secure
set−cookie: B=d2skjuhf4g0fv&b=3&s=vl; expires=Sun, 14−Feb−2021 14:36:47 GMT; path=/; domain=.yahoo.com

GET https://guce.yahoo.com/consent
Parameters:
brandType: eu
gcrumb: PUE4ymo
lang: en−IE
done: https://ie.yahoo.com/?p=us

GET https://consent.yahoo.com/collectConsent
Headers:
sessionId: 3_cc−session_85397231−a91a−4dec−bb4e−e5802c169bde

GET https://consent.yahoo.com/apple-touch-icon-precomposed.png
Response is 404 Not Found

GET https://www.bing.com/apple-touch-icon-precomposed.png

GET https://www.google.com/?client=safari&channel=mac_bm
Response sets cookies:
set−cookie: 1P_JAR=2020−02−15−14; expires=Mon, 16−Mar−2020 14:36:48 GMT; path=/; domain=.google.com; Secure
set−cookie: NID=198=WRjk9GEPs0O_rN1. . .; expires=Sun, 16−Aug−2020 14:36:47 GMT; path=/; domain=.google.com; HttpOnly

GET https://consent.yahoo.com/apple-touch-icon.png
Response is 404 Not Found

GET https:// www.google.com/apple-touch-icon-precomposed.png
Response is 404 Not Found

GET https://s.yimg.com/oa/build/images/favicons/yahoo.png

GET https://www.google.com/apple-touch-icon.png
Response is 404 Not Found

GET https://www.google.com/favicon.ico

GET https://www.yahoo.com/
Response sets cookie:
set−cookie: RRC=st=1581777408&cnt=1; expires=Sat, 15−Feb−2020 14:37:18 GMT; path=/; domain=.www.yahoo.com; HttpOnly

GET https://www.google.com/?client=safari&channel=mac_bm
Response sets cookies:
set−cookie: 1P_JAR=2020−02−15−14; expires=Mon, 16−Mar−2020 14:36:48 GMT; path=/; domain=.google.com; Secure
set−cookie: NID=198=q3khY−BI8Dswcw6AgVFTwjKdy6F5SJ. . .; expires=Sun, 16−Aug−2020 14:36:48 GMT; path=/; domain=.google.com; Secure; HttpOnly
set−cookie: CONSENT=WP0.283a07; expires=Fri, 01−Jan−2038 00:00:00 GMT; path=/; domain=.google.com

GET https://ie.yahoo.com/?p=us
Response sets cookies:
set−cookie: GUCS=ASmCmtvr; Max−Age=1800; Domain=.yahoo.com; Path=/; Secure
set−cookie: B=1feq8qtf4g0g0&b=3&s=1f; expires=Sun, 14−Feb−2021 14:36:48 GMT; path=/; domain=.yahoo.com

GET https://guce.yahoo.com/consent
Parameters:
brandType: eu
gcrumb: KYKa2−s
lang: en−IE
done: https://ie.yahoo.com/?p=us

GET https://consent.yahoo.com/collectConsent
Parameters:
sessionId: 3_cc−session_e2a1d62d−07e3−4a43−a4ec−1fc0ebb27cd2
lang: en−IE

inline: false

GET https://consent.yahoo.com/apple-touch-icon-precomposed.png
GET https://consent.yahoo.com/apple-touch-icon.png
GET https://www.google.com/images/branding/product_ios/3x/gsa_ios_60dp.png
GET https://s.yimg.com/oa/build/images/favicons/yahoo.png
GET https://www.wikipedia.org/
Response sets cookies:
set−cookie: WMF−Last−Access=15−Feb−2020;Path=/;HttpOnly; secure;Expires=Wed, 18 Mar 2020 12:00:00 GMT
set−cookie: WMF−Last−Access−Global=15−Feb−2020;Path=/; Domain=.wikipedia.org;HttpOnly;secure;Expires=Wed, 18 Mar 2020 12:00:00 GMT
x−client−ip: 37.228.245.107
set−cookie: GeoIP=IE:L:Dublin:53.33:−6.25:v4; Path=/; secure; Domain=.wikipedia.org
GET https://www.facebook.com/
GET https://www.wikipedia.org /static/apple-touch/wikipedia.png
Response sets cookies:
set−cookie: WMF−Last−Access=15−Feb−2020;Path=/;HttpOnly; secure;Expires=Wed, 18 Mar 2020 12:00:00 GMT
set−cookie: WMF−Last−Access−Global=15−Feb−2020;Path=/; Domain=.wikipedia.org;HttpOnly;secure;Expires=Wed, 18 Mar 2020 12:00:00 GMT
x−client−ip: 37.228.245.107
set−cookie: GeoIP=IE:L:Dublin:53.33:−6.25:v4; Path=/; secure; Domain=.wikipedia.org
Note the GeoIP cookie includes the city plus latitude and longitude.

GET https://www.facebook.com/apple-touch-icon-precomposed.png
GET https://www.weather.com/
Response sets cookies:
set−cookie: speedpin=4G; expires=Sat, 15−Feb−2020 15:06:50 GMT; path=/; domain=.weather.com; secure
set−cookie: ci=TWC−Locale−Group=US&X−Origin−Hint=Prod−IBM−LS&TWC−GeoIP−Country=IE&TWC−Privacy=gdpr; path=/; domain=.weather.com; secure
twc−privacy: gdpr
twc−geoip−latlong: 53.33,−6.25
twc−geoip−country: IE
twc−device−class: desktop
twc−locale−group: US
twc−connection−speed: 4G
twc−ak−req−id: 680bc4a
Note the latitude and longitude in the response.

GET https://twitter.com /
Response sets cookies:
set−cookie: fm=0; Max−Age=0; Expires=Sat, 15 Feb 2020 14:36:50 GMT; Path=/; Domain=.twitter.com; Secure; HTTPOnly
set−cookie: _twitter_sess=BAh7CSIKZmxhc2hJQzon. . .; Path=/; Domain=.twitter.com; Secure; HTTPOnly
set−cookie: personalization_id="v1_HAJmmvmI0ti2idE9L2HO2g==”; Max−Age=63072000; Expires=Mon, 14 Feb 2022 14:36:50 GMT; Path=/; Domain=.twitter.com; Secure
set−cookie: guest_id=v1%3A158177741069714211; Max−Age =63072000; Expires=Mon, 14 Feb 2022 14:36:50 GMT; Path=/; Domain=. twitter.com; Secure
set−cookie: ct0=fae1a04b34452e9bde5e85f54c090f92; Max−Age =21600; Expires=Sat, 15 Feb 2020 20:36:50 GMT; Path=/; Domain=.twitter .com; Secure
GET https://weather.com/
Response sets cookies:
set−cookie: speedpin=4G; expires=Sat, 15−Feb−2020 15:06:50 GMT; path=/; domain=.weather.com; secure
set−cookie: Goto=Redirected; expires=Sat, 15−Feb−2020 14:36:55 GMT; path=/; domain=.weather.com; secure
set−cookie: ci=TWC−Locale−Group=US&X−Origin−Hint=Goto−Prod&TWC−GeoIP−Country=IE&TWC−Privacy=gdpr; path=/; domain=. weather.com; secure
GET https://weather.com/en-IE/weather/today/l/EIXX0014:1:EI
Response sets cookies:
set−cookie: speedpin=4G; expires=Sat, 15−Feb−2020 15:06:51 GMT ; path=/; domain=.weather.com; secure
set−cookie: ci=TWC−Locale−Group=GLS&X−Origin−Hint=Prod−IBM−LS&TWC−GeoIP−Country=IE&TWC−Privacy=gdpr; path=/; domain=.weather.com; secure
GET https://abs.twimg.com /icons/apple-touch-icon-192x192.png
GET https://s.w-x.co/twc_180x180.png
GET https://www.yelp.com /
Response sets cookies:
set−cookie: pid=; Domain=.yelp.com; Max−Age=0; Path=/; expires= Wed, 31−Dec−97 23:59:59 GMT
set−cookie: bse=8975fb19234041cb9045988c692b7de5; Domain=.yelp. com; Path=/; HttpOnly
set−cookie: hl=en_US; Domain=.yelp.com; Max−Age=630720000; Path=/; expires=Fri, 10−Feb−2040 14:36:52 GMT
set−cookie: wdi=1|7BFD7066C9924130|0x1.7920080ff6fb1p+30|9 f37173636172ba0; Domain=.yelp.com; Path=/; Max−Age=630720000; Expires=Fri, 10 Feb 2040 14:36:52 GMT; HttpOnly
GET https://www.tripadvisor.com/
Response sets cookies:
set−cookie: TADCID=lFE_Lkk8Bl− KJaz_ABQCjnFE8vTET66GHuEzPi7KfVt− GbQsyPunvyfz8ziCIcAEoDQbgEPxiluOwcrx24rT_9N4_LieKvqPvQk; Domain=www.tripadvisor.com; Expires=Tue, 12−Feb−2030 14:36:52 GMT ; Path=/; Secure; HttpOnly
set−cookie: TAUnique=%1%enc%3AX9C6wmbSgJsM%2F%2FrX05 . . .; Domain=.tripadvisor.com; Expires=Mon, 14−Feb−2022 14:36:52 GMT; Path=/; HttpOnly
set−cookie: TASession=V2ID.7DB0B55AB8130. . ..37∗HS. recommended∗ES.popularity∗DS.5∗SAS.popularity∗FPS.oldFirst∗FA.1∗DF .0∗TRA.true; Domain=.tripadvisor.com; Path=/
set−cookie: PAC=AGG3R−6Ri3EDIYbjnRLUD. . .; Domain=www. tripadvisor.com; Expires=Mon, 14−Feb−2022 14:36:52 GMT; Path=/; Secure; HttpOnly
set−cookie: SRT=TART_SYNC; Domain=www.tripadvisor.com; Path=/
set−cookie: ServerPool=X; Domain=.tripadvisor.com; Path=/
set−cookie: TAPD=tripadvisor.ie; Domain=.tripadvisor.com; Path=/
set−cookie: PMC=V2∗MS.68∗MD.20200215∗LD.20200215; Domain= www.tripadvisor.com; Expires=Mon, 14−Feb−2022 14:36:52 GMT; Path =/; Secure; HttpOnly
set−cookie: TART=%1%enc%3ADP%2F619OSboK4KhpF%2 FZmeevhe9S6QJQyL2f8. . .; Domain=www.tripadvisor.com; Expires=Thu, 20−Feb−2020 14:36:52 GMT; Path=/; HttpOnly
set−cookie: TATravelInfo=V2∗A.2∗MG.−1∗HP.2∗FL.3∗RS.1; Domain =.tripadvisor.com; Expires=Sat, 29−Feb−2020 14:36:52 GMT; Path=/
set−cookie: TAUD=RDD−1581777412468−2020_02_15; Domain=. tripadvisor.com; Expires=Sat, 29−Feb−2020 14:36:52 GMT; Path=/
set−cookie: ak_bmsc=DD6689196E314F551134. . .; expires=Sat, 15 Feb 2020 16:36:52 GMT; max−age=7200; path=/; domain=.tripadvisor.com ; HttpOnly

GET https://www.yelp.ie/
Response sets cookies:
set−cookie: pid=; Domain=.yelp.ie; Max−Age=0; Path=/; expires=Wed , 31−Dec−97 23:59:59 GMT
set−cookie: bse=e38264c7d1b54ad79f29343e72f336b8; Domain=.yelp. ie; Path=/; HttpOnly
set−cookie: hl=en_IE; Domain=.yelp.ie; Max−Age=630720000; Path =/; expires=Fri, 10−Feb−2040 14:36:52 GMT
set−cookie: wdi=1|01A93E806AAEAF04|0x1.792008113539cp+30|3 e355a7042e25a94; Domain=.yelp.ie; Path=/; Max−Age=630720000; Expires=Fri, 10 Feb 2040 14:36:52 GMT; HttpOnly
GET https://www.tripadvisor.ie/LangRedirect?auto=3&origin=en_US&pool= X&returnTo=/
Response sets cookies:
set−cookie: TADCID=UcqYzu1e_12GzlADABQCjn. . .; Domain= www.tripadvisor.ie; Expires=Tue, 12−Feb−2030 14:36:52 GMT; Path=/; Secure; HttpOnly
set−cookie: TAUnique=%1%enc%3AGhghyxF3posM%2F%2. . .; Domain=.tripadvisor.ie; Expires=Mon, 14−Feb−2022 14:36:52 GMT; Path =/; HttpOnly
set−cookie: TASession=V2ID.EC9518B53346D29394. . ..recommended ∗ES.popularity∗DS.5∗SAS.popularity∗FPS.oldFirst∗FA.1∗DF.0∗IR.3∗OD. en_US∗TRA.true; Domain=.tripadvisor.ie; Path=/
set−cookie: SRT=TART_SYNC; Domain=www.tripadvisor.ie; Path=/
set−cookie: ServerPool=X; Domain=.tripadvisor.ie; Path=/
set−cookie: TART=%1%enc%3ADP%2F619OSboIuiUH9. . .; Domain= www.tripadvisor.ie; Expires=Thu, 20−Feb−2020 14:36:52 GMT; Path=/; HttpOnly

GET https://www.yelp.ie/dublin

Response sets cookies:
set−cookie: pid=; Domain=.yelp.ie; Max−Age=0; Path=/; expires=Wed, 31−Dec−97 23:59:59 GMT
set−cookie: bse=30ceec001f3b420fa4591f1f1af47d5e; Domain=.yelp.ie; Path=/; HttpOnly
set−cookie: location=%7B%22city%22%3A+%22Dublin%22%2C+%22state%22%3A+%22D%22%2C+%22country%22%3A+%22IE%22%2C+%22latitude%22%3A+53.3458%2C+%22longitude%22%3A+−6.26269%2C+%22max_latitude%22%3A+53.3695%2C+%22min_latitude%22%3A+53.3186%2C+%22max_longitude%22%3A+−6.2129%2C+%22min_longitude%22%3A+−6.3142%2C+%22zip%22%3A+%22%22%2C+%22address1%22%3A+%22%22%2C+%22address2%22%3A+%22%22%2C+%22address3%22%3A+null%2C+%22neighborhood%22%3A+null%2C+%22borough%22%3A+null%2C+%22provenance%22%3A+%22YELP_GEOCODING_ENGINE%22%2C+%22display%22%3A+%22Dublin%22%2C+%22unformatted%22%3A+%22Dublin%22%2C+%22isGoogleHood%22%3A+null%2C+%22usingDefaultZip%22%3A+null%2C+%22accuracy%22%3A+4.0%2C+%22language%22%3A+null%7D; Domain=.yelp.ie; Max−Age=630720000; Path=/; expires=Fri, 10−Feb−2040 14:36:52 GMT
set−cookie: hl=en_IE; Domain=.yelp.ie; Max−Age=630720000; Path=/; expires=Fri, 10−Feb−2040 14:36:53 GMT
set−cookie: wdi=1|90EE1019CEFD06D2|0x1.7920081349f5ap+30|193b796f541f3974; Domain=.yelp.ie; Path=/; Max−Age=630720000; Expires=Fri, 10 Feb 2040 14:36:53 GMT; HttpOnly
Note the city plus latitude and longitude data in the location cookie.

GET https://www.tripadvisor.ie/
Response sets cookies:
set−cookie: TADCID=h2yuJsCTeBZ6vudmABQCj. . .; Domain=www.tripadvisor.ie; Expires=Tue, 12−Feb−2030 14:36:52 GMT; Path=/; Secure; HttpOnly
set−cookie: TAUnique=%1%enc%3AEunuxyLmvzkM%2F%2FrX05Jugo8AQl%2BErAhhpOe8b19AZKV1AOYNre4SJA%3D%3D; Domain=.tripadvisor.ie; Expires=Mon, 14−Feb−2022 14:36:52 GMT; Path=/; HttpOnly
set−cookie: TASSK=enc%3AABaEVB60VD8WdEb. . .; Domain=www.tripadvisor.ie; Expires=Thu, 13−Aug−2020 14:36:53 GMT; Path=/; HttpOnly
set−cookie: TASession=V2ID.D7B5764BD1BDB8. . ..recommended∗ES.popularity∗DS.5∗SAS.popularity∗FPS.oldFirst∗FA.1∗DF.0∗TRA.true; Domain=.tripadvisor.ie; Path=/
set−cookie: PAC=AMUsOJgKEwaxRypNjk628O. . .; Domain=www.tripadvisor.ie; Expires=Mon, 14−Feb−2022 14:36:53 GMT; Path=/; Secure; HttpOnly
set−cookie: SRT=null; Domain=www.tripadvisor.ie; Expires=Thu, 01−Jan−1970 00:00:10 GMT; Path=/
set−cookie: ServerPool=X; Domain=.tripadvisor.ie; Path=/
set−cookie: PMC=V2∗MS.29∗MD.20200215∗LD.20200215; Domain=www.tripadvisor.ie; Expires=Mon, 14−Feb−2022 14:36:53 GMT; Path=/; Secure; HttpOnly
set−cookie: TART=%1%enc%3ADP%2F619OSboJIj. . .; Domain=www.tripadvisor.ie; Expires=Thu, 20−Feb−2020 14:36:53 GMT; Path=/; HttpOnly
set−cookie: TATravelInfo=V2∗A.2∗MG.−1∗HP.2∗FL.3∗RS.1; Domain=.tripadvisor.ie; Expires=Sat, 29−Feb−2020 14:36:53 GMT; Path=/
set−cookie: CM=%1%PremiumMobSess%2C%2C−1%7Ct4b−. . .Domain=.tripadvisor.ie; Expires=Tue, 12−Feb−2030 14:36:53 GMT; Path=/
set−cookie: TAUD=RDD−1581777412978−2020_02_15; Domain=.tripadvisor.ie; Expires=Sat, 29−Feb−2020 14:36:53 GMT; Path=/
set−cookie: TAReturnTo=%1%%2F; Domain=.tripadvisor.ie; Path=/

GET https://www.tripadvisor.ie/apple-touch-icon-precomposed.png
GET https://www.yelp.ie /apple-touch-icon-precomposed.png
GET https://www.yelp.ie/apple-touch-icon.png

The html downloaded from weather.com has quite a few headers of the type <link rel=”preconnect” href=”//trc.taboola.com” crossorigin>. Domains are: s.w-x.co, fonts.googleapis.com, fonts.gstatic.com, www.googletagservices.com, a.tiles.mapbox.com, b.tiles.mapbox.com, c.tiles.mapbox.com, d.tiles.mapbox.com, js-agent.newrelic.com, images.taboola.com.cdn, cdn.taboola.com, trc.taboola.com, securepubads.g.doubleclick.net, sb.scorecardresearch.com, widget.perfectmarket.com, px.moatads.com, z.moatads.com, tpc.googlesyndication.com, cdn.polyfill.io. The html downloaded from www.tripadvisor.ie also has a preconnect link to static.tacdn.com. Safari attempts to connect to all of these preconnect domains, but the connection consistently fails for reasons that are unclear (presumably related to Safari’s caching behaviour since connections to these succeed when e.g. www.weather.com is entered into the browser top bar.

B. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar:

GET https://configuration.apple.com/configurations/pep/config/geo/networkDefaults-osx-10.14.4.plist
Headers:
User−Agent: com.apple.geod/1364.26.4.19.6 CFNetwork/978.1 Darwin/18.7.0 (x86_64)
Response is 2.6KB of text/xml

GET http://leith.ie/nothingtosee.html
GET http://leith.ie/favicon.ico

Note that the connection to configuration.apple.com by process com.apple.geod is consistently observed, although it contains no identifiers and the response seems like a fairly generic xml list of settings. There may also be correlated connections by other processes, in particular by parsecd (a Siri helper daemon which “manages access and data for Siri Suggestions”) but this is less clear.

C. Connections Made On Re-Open After Close

No connections are made by Safari on reopen. However, reopening Safari consistently prompts network connections by nsurlsessiond. Certificate checks reset this connection when mitmproxy is active, preventing direct inspection. However, the output from command “fs_usage -w” identified nsurlsessiond accessing a folder under /var/-folders/.../com.apple.nsurlsessiond/.../. Reopening Safari with mitmproxy disabled consistently creates a new folder under this directory tree containing a number of files including a tasks.plist file. Inspection of this file indicates that the nsurlsessiond is making POST requests to gateway.icloud.com (which DNS maps to CNAME gateway.fe.apple-dns.net) on behalf of com.apple.SafariBookmarksSyncAgent of the following form:

POST https://gateway.icloud.com/ckdatabase/api/client/subscription/retrieve
Headers:
X−CloudKit−ContainerId: com.apple.SafariShared.WBSCloudBookmarksStore
X−CloudKit−UserId: **_9acd71fb10d466**. . .
X−CloudKit−BundleId: com.apple.SafariBookmarksSyncAgent
The X-CloudKit-UserId value remains constant across reopens of Safari and is presumably a persistent identifier.

D. Connections Made When Sitting Idle

GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Headers:
user−agent: SafariSafeBrowsing/15608.4.9.1.3 CFNetwork/1121.1.2 Darwin/19.2.0 (x86_64)
Parameters:
$req: ChcKBlNhZmFyaRINMTU2MDguNC45LjEu. . .
key: AIzaSyANT−dOXDTNxZS4flEI. . .
Previous comments regarding requests to safebrowsing.googleapis.com also apply here.

E. Connections Generated By Auto-Complete As User Types

Connections generated as user types leith.ie/nothingtosee.html in Safari top bar.

GET https://clients1.google.com/complete/search
Parameters:
q: l
Response:
[”l”, [[”lewis burton”, ””,[131]],[”love island”, ””,[131]],[”liverpool ”,””, [131]],[”linkedin”, ””], [”littlewoods”, ””],[”lotto”,””,[131]], [”laura whitmore”, ””,[131]],[”lidl”,””],[”livescore”, ””, [131]],[”lighthouse cinema ”, ””]],{”k”: 1,”q”: ”lEt4xZ4iP9GvFsdKfr4SW_d−ZoI” }]

GET https://api-glb-dub.smoot.apple.com/search
Parameters:
X−Apple−GeoMetadata: SgBQAYABA5gBAKIGByoFCOFJEAA=
X−Apple−UserGuid: **8F00E045-85F3-4C36-9FA4-F2**. . .
X−Apple−GeoSession: 0302623670852399322705352888801992086. . .
User−Agent: parsecd/1.0 (Mac OS X 10.14.6 18G1012) Safari/1
Request body:
24h: 1
ab_seed: 38
alwaysSendTophit: off
calendar: Gregorian Calendar
card: 1
cc: IE
esl: en−GB
geosrc: error.fail
key: quet. . .
locale: en_IE
q: le
sil: MA==
storefront: 143449−2,32
temp: C
time_zone: Europe/Dublin
units: SI
The X-Apple-GeoMetadata, X-Apple-UserGuid and X-Apple-GeoSession values are the repeated in all of the requests below, but to save space are not shown. The value of X-Apple-GeoMetadata remains unchanged across fresh installs in the same location, the X-Apple-UserGuid value changes across fresh installs but remains constant across restarts of Safari. The X-Apple-GeoSession is also observed to remain constant across browser restarts. Note the user agent: the Apple man page says “parsecd manages access and data for Siri Suggestions”. Siri has never been enabled on the device used for these tests. Response:
[{”fbq”: ”eyJ1IjoiOEYwMEUwNDUt. . .”, ”partial_client_ip”: ”37.228.245.0”,”prefix”: ”le”,”query”: ”le”, ”status”: ”NO_RESULTS”}]
Observe that the response includes most of the browser IP address (the last number is zeroed out).

GET https://clients1.google.com/complete/search
Parameters:
q: le
Response:
[”le”,[[”lewisburton”,””,[131]],[”leapcard”,””],[”leedsunited”,””,[131]],[” leovaradkar”,””,[131]],[”lewiscapaldi”,””],[”leinsterrugby”,””],[” lewisburtoninstagram”,””,[131]],[”leinstervscheetahs”,””,[131]],[”lemans66 ”,””],[”leicester”,””]],{”k”:1,”q”:”ksWYWJlOJnAbtTK4Btmpo673qRQ”}]

GET https://api-glb-dub.smoot.apple.com/search
Parameters and request body are as before except the in body the line q: changes to:
q: lei
Response is as above, ”NO_RESULTS”

GET https://clients1.google.com/complete/search?
Parameters:
q: lei
Response:
[”lei”,[[”leinsterrugby”,””],[”leinstervscheetahs”,””,[131]],[”leinster”,””],[” leicester”,””],[”leinsterhockey”,””,[131]],[”leixlip”,””],[”leinsterfixtures ”,””],[”leisureplex”,””,[131]],[”leitrim”,””],[”leicesterfixtures”,””]],{”k”:1,”q ”:”0IInSwuLoU6RTJplHJbrnHDcxQM”}]

Plus requests for “leit”, “leith”, “leith.”, “leith.i”, “leith.ie”, “leith.ie/”, “leith.ie/n”, “leith.ie/no”, “ leith.ie/not”, ‘leith.ie/noth”, “leith.ie/nothi”, “leith.ie/nothin”, “leith.ie/nothing”, “leith.ie/nothingt”, “leith.ie/nothingto”, “leith.ie/nothingtos”, “leith.ie/nothingtose”, “leith.ie/nothingtosee”, “leith.ie/nothingtosee.”, “leith.ie/nothingtosee.h”, “leith.ie/nothingtosee.ht”, “leith.ie/nothingtosee.htm”, “leith.ie/nothingtosee.html”

Requests to clients1.google.com stop shortly after the first word but requests to api-glb-dub.smoot.apple.com continue. The result is 7 requests to clients1.google.com and 25 requests to api-glb-dub.smoot.apple.com, a total of 32 requests

V. Microsoft Edge

A. Connections On First Startup

POST https://nav.smartscreen.microsoft.com/api/browser/edge/actions
Headers:
Authorization: SmartScreenHash eyJhdXRoSWQiOiIyMDM1MT. . .
User−Agent: SmartScreen/281479396982785
Request Body:


```
{
    "identity": {
        "caller": {
            "locale": "en−US"
        },
        "client": {
            "data": {
                "customSettings": "
F95BA787499AB4FA9EFFF472CE383A14",
                "customSynchronousLookupUris": "0",
                "edgeSettings": "1.0−0",
                "synchronousLookupUris": "636976985063396749.rel.
v2",
                "topTraffic":
"17054018593960299740050623419798352937 1"
            },
            "version": "281479396982785"
        },
        "device": {
            "architecture": 9,
            "browser": {
                "internetExplorer": null
            },
            "cloudSku": false,
            "enterprise": {
                "enabled": true,
                "geoId": "",
                "organizationId": "",
                "senseId": ""
            },
            "family": null,
            "locale": "en−US",
            "netJoinStatus": 0,
            "osVersion": "10.14.6.18G1012"
        },
        "user": {
            "locale": "en−US"
        }
    }
}
```


The SmartScreenHash header value and the content of the request body are observed to remain constant across fresh installs. Observe that the user agent value is "SmartScreen". The same "Authorization: SmartScreenHash " header is sent with all requests by this user agent and so to save space is not repeated in the requests below. The response is application/json

GET https://nav.smartscreen.microsoft.com/api/browser/edge/data/settings
Headers:
User−Agent: SmartScreen/281479396982785
The request body is the same a in the previous request. The response is application/octet-stream

POST https://smartscreen-prod.microsoft.com/api/browser/edge/navigate/1
Headers:
User−Agent: SmartScreen/281479396982785
Request Body:


```
<...>
"correlationId": "8cba1194-5f72-4d32-9c73-ab3e381c571a",
<...>
```


The correlationId value changes across fresh installs of Edge. The response is 1.17KB of application/json

GET https://smartscreen-prod.microsoft.com/windows/browser/edge/data/bloomfilter/x
Headers:
User−Agent: SmartScreen/281479396982785
Response is application/octet-stream

GET https://ntp.msn.com/edge/ntp
Parameters:
locale: en−IE
fre: 1
dsp: 1
sp: Bing
startpage: 1
Response is 9.26KB of text/html that sets a cookie:
set−cookie: sptmarket=en−IE||ie|en−ie|en−ie|en; expires=Wed, 16 Feb 2022 16:51:24 GMT; path=/
and includes a x-msedge-ref header:
x−msedge−ref: Ref A: [E8490F80BD18461DBBF1A5D2817DBDF0] Ref B: DB3EDGE1620 Ref C: 2020−02−17T12:10:13Z
The Ref A value in the x-msedge-ref header is echoed back by Edge in subsequent requests and so acts as an identifer that links requests together. The cookie is echoed in requests to ntp.msn.com but to save space is not shown below. The value of Ref A changes across fresh installs and browser restarts.

GET https://config.edge.skype.com/config/v1/Edge/80.0.361.48
Response is application/json. Edge now downloads javascripts using the following series of requests:
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAC2CIS
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/BBVM2cS
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/BBWdYYX
GET https://assets.msn.com/bundles/v1/edgechromium/latest/telemetry.5b8605afd0db34a32ad8.js
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AACkYoF
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAFFiyC
GET https://assets.msn.com/bundles/v1/edgechromium/latest/oneServiceContentData.8553fa68002d5d3b3416.js
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/BBWiJxo
GET https://assets.msn.com/bundles/v1/edgechromium/latest/msccCookieBanner.3a465857b12066bb8090.js
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAB60Ja
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAC2ECl
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AABH2go
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/BBTdf0j
GET https://assets.msn.com/bundles/v1/edgechromium/latest/telemetry.50f3464b127111c4f24e.js
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAJ7OhE
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAI7UC6
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AACkZFy
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAH691m
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAAI7UC4
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAHQ52l
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AACd7bq
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AACd77X
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAF3amg
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AACd4JC
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAI7DvK
GET https://ntp.msn.com/resolver/api/resolve/v2/configindex/AAHQpX3

POST https://self.events.data.microsoft.com/OneCollector/1.0/
Headers:
APIKey: 7005b72804a64fa4b. . .
SDK−Version: EVT−MacOSX−C++−No−3.2.297.1
Request Body:
)\x033.0I&Microsoft.WebBrowser.SystemInfo.Configq\x80\xb4\xaa\xfc\xaa\xe7\xd9\xd7\x11\xa9"o:**7005b72804a64fa4b2138faab88f877b\xd1\x06\x82\x04\xcb\x15**
\x01i\x05Apple\x89\x0eMacBookPro15,2\x00\xcb\x16
\x01\x00\xcb\x17
\x01I&u:**0B5E1E28-B2E0-5DE9-848D-0368FB**. . .\x00\xcb\x18
\x01\x89\x08Mac OS X\xa9\x0710.14.6\x00\xcb\x19
\x01\xa99M:com.microsoft.edgemac_80.0.361.48_x86_64!Microsoft Edge\xc9\x06\x0b80.0.361.48\x00\xcb\x1f
\x01I Unmeteredi\x05Wired\x00\xcb
\x01)\x1bEVT−MacOSX−C++−No−3.2.297.1I$$**eaf6f216-bca7-a0c9-8b40**. . .
\x01i\x0500:00\x00\xcb%
\x01\x00\xc9<\x06custom\xcbF
\x01−
\x10\x0cAppInfo.ETag\x00\x07Channel0\x00\x91\x08\x00\x0eConnectionTypei\x07Unknown\x00\x04Etag\x00\x0fEventInfo.Level0\x00\x91\x04\x00\x0cPayloadClassi\x0bSYSTEM_INFO\x00\x0b$PayloadGUID

i$2f0dbe5e-a940-4842-8fb3-9b61ed5003ad\x00\x0e PayloadLogType0\x00\x91
\x00\x0fappConsentState0\x00\x00\x0bapp_versioni\x0e80.0.361.48−64\x00 $
client_id0\x00\x91\xba\xa1\xa9\xd4\xef\xc6\xf0\xbc\x04\x00
installSource0\x00\x00\x0cinstall_date0\x00\x91\x80\x9c\xcb\xe4\x0b\x00
pop_sample0\x08\xa8\x00\x00\x00\x00\x00\x00Y@\x00
session_id0\x00\x91\x02\x00 utc_flags0\x00\x91\x80\x80\xc0\x80\x80\x80@\x00\x00\x00
This is a troubling request because the 0B5E1E28-B2E0-5DE9-848D-0368FB... value in the request body is the hardware UUID for the client device (as reported by MacOS System Information), i.e a unique, persistent identifier that can also be used to link across apps. Other notes:

1) *The EVT-MacOSX-C++-No-3.2.297.1 string is present inside the oneds.so library binary packaged with Edge and so presumably is a version number. It is constant across fresh installs.*
2) *The string beginning 7005b72 . . . also forms the first part of the APIkey header value used in the request and is present inside the Microsoft Edge Framework, so presumably it identifies one or more Edge components. It is constant across fresh installs.*
3) *The Microsoft.WebBrowser.SystemInfo.Config block also includes an entry beginning ea f6 f 216 . . .. This is not present in the Edge binary and how this value is calculated is unclear.*
4) *The second block in request body also contains a number of other identifier-like entries, namely the entries PayloadGUID value and client_id. These values are observed to change across fresh installs.*

GET https://otf.msn.com/c.gif
Parameters:
<...>
rid: **e8490f80bd18461dbbf1a5d2817dbdf0**
<...>
clid: **e8490f80bd18461dbbf1a5d2817dbdf0**
<...>
activityId: **e8490f80bd18461dbbf1a5d2817dbdf0**
<...>
Observe that the rid, clid and activityId parameters echo the value returned by the server via the x-msedge-ref header
GET https://www.msn.com/spartan/en-ie/getappanoncookie
OPTIONS https://otf.msn.com/c.gif
GET https://ntp.msn.com/service/graph/actions
Parameters:
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
GET https://ntp.msn.com/service/graph/actions
Parameters:
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
GET https://ntp.msn.com/service/graph/actions
Parameters:
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
GET https://uhf.microsoft.com/_log
GET https://ntp.msn.com/service/graph/actions
Parameters:
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
GET https://ntp.msn.com/service/graph/actions
Parameters:
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
POST https://otf.msn.com/c.gi
Parameters:
<...>
"clid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
"rid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
GET https://assets.msn.com/bundles/v1/edgechromium/latest/settingsDialog.67d7d428c8e08b1b582f.js
GET https://204.79.197.203/edge/ntp/service-worker.js
POST https://otf.msn.com/c.gif
Request body:
<...>
"clid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
"rid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
GET https://assets.msn.com/bundles/v1/edgechromium/latest/welcomeGreeting.c3954f36098492c0aa11.js
POST https://otf.msn.com/c.gif
Request body:
<...>
"clid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
"rid": "**e8490f80bd18461dbbf1a5d2817dbdf0**",
<...>
GET https://otf.msn.com/c.gif
Parameters:
<...>
rid: **e8490f80bd18461dbbf1a5d2817dbdf0**
<...>
clid: **e8490f80bd18461dbbf1a5d2817dbdf0**
<...>
activityId: **E8490F80-BD18-461D-BBF1-A5D2817DBDF0**
<...>
GET https://assets.msn.com/bundles/v1/edgechromium/latest/marketSelector.c6551fbd7fffc43d4eb9.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/oneServiceContentData.8553fa68002d5d3b3416.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/settingsDialog.67d7d428c8e08b1b582f.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/msccCookieBanner.3a465857b12066bb8090.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/telemetryEdgeChromium.50f3464b127111c4f24e.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/telemetry.5b8605afd0db34a32ad8.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/weather-data-connector.1f99f41ebed76cfd3c5a.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest/welcomeGreeting.c3954f36098492c0aa11.js
GET https://assets.msn.com/bundles/v1/edgechromium/latest//content/view/v1/weathersummary/en-ie/53.3481,-6.2483
GET https://assets.msn.com/bundles/v1/edgechromium/latest/welcomeGreeting.c3954f36098492c0aa11.js

GET https://arc.msn.com/v4/api/selection
Parameters:
placement: **88000216**
<...>
The response is json which includes values:
ASID=**DA50B3ECE6E34DC38D6C6FCB7E935971**
DS_EVTID=**DA50B3ECE6E34DC38D6C6FCB7E935971**
plus other values echoed in the next request.

GET https://arc.msn.com/v3/Delivery/Events/Impression
Parameters:
PID: 425122471
TID: 700336220
CID: 128000000001812869
BID: 1112554955
PG: IRIS000001.0000000216
TPID: 425122471
REQASID:
ASID: **DA50B3ECE6E34DC38D6C6FCB7E935971**
SLOT:
REQT: 20200217T121018
<...>
DS_EVTID: **DA50B3ECE6E34DC38D6C6FCB7E935971**
PG: IRIS000001.0000000216
UNID: **88000216**
MAP_TID: 71E62249−D4D7−4C67−9526−515F5742A15E
NCT: 1
ASID: DA50B3ECE6E34DC38D6C6FCB7E935971
<...>
CIP: 37.228.245.107

<...>

GET https://edge.microsoft.com/abusiveadblocking/api/v1/blocklist
GET https://config.edge.skype.com/config/v1/Edge/80.0.361.48

The next sequence of requests have similar content to those used by Chrome and other browsers to check for updates to extensions
POST https://edge.microsoft.com/componentupdater/api/v1/update
Headers:
x−microsoft−update−appid: oankkpibpaokgecfckkdkgaoafllipag, gcmjkmgdlgnkkcocmoeiminaijmmjnii,ojblfafjmiikbkepnnolpgbbhejhlcim, jbfaflocpnkhbgcijpkiafdpbjkedane
Parameters:
cup2key: 3:2477908307
cup2hreq: 9ceca690972036a90...
:authority:
content−length: 890
Request body:

```
{
    "request": {
        "@os": "mac",
        "@updater": "msedge",
        "acceptformat": "crx2,crx3",
        "app": [
            {
                "appid": "oankkpibpaokgecfckkdkgaoafllipag",
                "enabled": true,
                "ping": {
                    "r": −2
                },
                "updatecheck": {},
                "version": "0.0.0.0"
            },
```

<...>
GET http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/d7203b19-7bfa-4ff0-8b10-48509b0b7960?P1=1581978793&P2=402&P3=2&P4=i9IO...
POST https://edge.microsoft.com/componentupdater/api/v1/update
GET http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/7154ce99-f4f6-4086-a0a3-312335bcb7e3?P1=1582023475&P2=402&P3=2&P4=KUsntB...
POST https://edge.microsoft.com/componentupdater/api/v1/update
GET http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/a6152d02-e3fe-4b93-87db-40ab08d1e089?P1=1582024897&P2=402&P3=2&P4=B9hDtoK...
POST https://edge.microsoft.com/componentupdater/api/v1/update
GET http://msedge.b.tlu.dl.delivery.mp.microsoft.com/filestreamingservice/files/892b761b-f7d2-4172-adc4-f092b3993e8a?P1=1582023473&P2=402&P3=2&P4=g1ZlSTLw...
POST https://edge.microsoft.com8/componentupdater/api/v1/update

GET https://edge.microsoft.com/extensionrevocation/v1/threatListUpdates:fetch
Parameters:
req: ChcKCGNocm9ta!...
ct: application/x−protobuf
key: d414dd4f9db345fa8003...
This request is similar to those to Google's Safe Browsing API. The response is 8290KB of application/x-protobuf

B. Clicking on "Get Started" Button

GET https:// ris.api.iris.microsoft.com/v1/a/click
Parameters:
<...>
CID: 128000000001812449
PID: 425122451
<...>
ASID: **DA50B3ECE6E34DC38D6C6FCB7E935971**
REQT: **20200217T121018**
<...>
DS_EVTID: **DA50B3ECE6E34DC38D6C6FCB7E935971**
<...>
Observe that the ASID and DS_EVTID are the same as previously, allowing these requests to be linked

GET https://go.microsoft.com/fwlink/
Parameters:
linkid: 2108500
Response is 302 Moved Temporarily to https://microsoftedgewelcome.microsoft.com/
GET https://microsoftedgewelcome.microsoft.com/
Response sets cookies:
set−cookie: sessionid=s%3ALctoQ2Elzu9LAOhL8W399_ZVBE4yJhlZ.5AHpKiEt3IE3PL5dsIKENEFWQFipTLhW7pMIjRUWdS4; Path=/; HttpOnly
set−cookie: ARRAffinity=85c0eee69a1f47b36cea7f0c1fee0879ce24e8896995f12054676e1f93b058a2;Path=/;HttpOnly;Domain=microsoftedgewelcome.microsoft.com
The value of the ARRAffinity cookie is the same across fresh installs, the sessionid cookie value changes

GET https://microsoftedgewelcome.microsoft.com/en-gb/
Headers:
cookie: sessionid=s%3ALctoQ2Elzu9LAOhL8W399_ZVBE4yJhlZ.5AHpKiEt3IE3PL5dsIKENEFWQFipTLhW7pMIjRUWdS4; ARRAffinity=85c0eee69a1f47b36cea7f0c1fee0879ce24e8896995f12054676e1f93b058a2

GET https://edgewelcomecdn.microsoft.com/site/dd0a2ef15896ce9012a7.css
GET https://edgewelcomecdn.microsoft.com/site/8ceec26c7fdd22959222.js
GET https://edgewelcomecdn.microsoft.com/site/11dd992623a245531a2e.js
GET https://edgewelcomecdn.microsoft.com/site/28f1fe2f84946d7d6302.js
GET https://edgewelcomecdn.microsoft.com/site/04d132fcac13433150ce.js
GET https://edgewelcomecdn.microsoft.com/site/3961ebffc82a2a519bdf.css
GET https://edgewelcomecdn.microsoft.com/site/502e75aac5b94f8e50f5.css
GET https://edgewelcomecdn.microsoft.com/site/5f8d0624467c92445c8d.js
GET https://edgewelcomecdn.microsoft.com/site/f59f237e760575632314.js
GET https://az725175.vo.msecnd.net/scripts/jsll-4.js
GET https://edgewelcomecdn.microsoft.com/site/img/f57da5f.png
GET https://edgewelcomecdn.microsoft.com/site/img/6e1b70e.png
GET https://mem.gfx.ms/meversion?partner=MSEdgeWelcome&market=en-gb&uhf=1
GET https://edgewelcomecdn.microsoft.com/site/img/ce5bc2c.svg
GET https://edgewelcomecdn.microsoft.com/site/img/3d4b9d7.svg
GET https://edgewelcomecdn.microsoft.com/site/img/2c44299.svg
GET https://edgewelcomecdn.microsoft.com/site/img/4851850.svg
GET https://edgewelcomecdn.microsoft.com/site/img/9d5b9e4.svg
GET https://edgewelcomecdn.microsoft.com/site/img/7de43e5.png
GET https://edgewelcomecdn.microsoft.com/site/img/032eff5.png
GET https://edgewelcomecdn.microsoft.com/site/fonts/36397a3.woff2
GET https://edgewelcomecdn.microsoft.com/site/fonts/dd6a59e.woff2
GET https://edgewelcomecdn.microsoft.com/site/fonts/6e75a94.woff2
GET https://edgewelcomecdn.microsoft.com/site/a24b1e59a34e4fa5d12b.js
GET https://uhf.microsoft.com/_log?o=mscc&s=Microsoft.OneRenderFramework.Core&m=show&nv=aspnet-3.1.3&sv=0.1.2
GET https://edgewelcomecdn.microsoft.com/site/c9072fee7ec76312ffde.js
GET https://edgewelcomecdn.microsoft.com/site/7e92a13793cb8704a2e3.js

GET https://web.vortex.data.microsoft.com/collect/v1/t.js
Parameters:
<...>
−impressionGuid: '59d59183−cd90−4787−ab0c−8328d0b20e75'
<...>
The response sets cookies:
Set−Cookie: MC1=GUID=**da7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000;Domain=.microsoft.com;Expires=Tue, 16 Feb 2021 12:12:24 GMT;Path=/;Secure;SameSite=None
Set−Cookie: MS0=dc42e1616b0e434e9bef71d2da20f061;Domain=.microsoft.com;Expires=Mon, 17 Feb 2020 12:42:24 GMT;Path=/;Secure;SameSite=None
and includes javascript with the cookie value embedded:
document.cookie="MSFPC=GUID=**da7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000;expires=Tue,

POST https://web.vortex.data.microsoft.com/collect/v1
Cookie: MC1=GUID=**dda7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000; MS0=dc42e1616b0e434e9bef71d2da20f061
Parameters:
$mscomCookies: false
ext−javascript−msfpc: 'GUID=

da7d27b6947c48b8abd43591e780322d&HASH=da7d&LV=202002&V=4&LU=1581941544000'

GET https://www.microsoft.com/store/buy/cartcount
cookie: MC1=GUID=**da7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000; MS0=dc42e1616b0e434e9bef71d2da20f061
Embedding the cookie in javascript uploaded to Edge, allows cross-domain sharing of the cookie and this can be seen here: the cookie set by vortex.data.microsoft.com is now shared with www.microsoft.com.

C. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar.

GET https://www.bing.com/qbox
Parameters
query: http://leith.ie/nothingtosee.html
language: en−GB
PC: U531
pt: EdgBox
cvid: 93e34a2400f048398b57850cd2926aff
ig: 2926dba55de04765821ac674ec80196c
oit: 3
cp: 33
pgcl: 4
The response sets cookies:
set−cookie: SRCHD=AF=NOFORM; domain=.bing.com; expires=Sat, 13−Mar−2021 12:13:04 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUID=V=2&GUID=AD5BCE0A898742268E4DCAC4EB9C24DA&dmnchg=1; domain=.bing.com; expires=Sat, 13−Mar−2021 12:13:04 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUSR=DOB=20200217; domain=.bing.com; expires=Sat, 13−Mar−2021 12:13:04 GMT; path=/; secure; SameSite=None
set−cookie: _SS=SID=1E9FAB0EE8876D5E334CA57DE9876C6D; domain=.bing.com; path=/; secure; SameSite=None
and returns json:

```
[
    "http://leith.ie/nothingtosee.html",
    [],
    [],
    [],
    {
        "google:clientdata": {
            "bcp": false,
            "phi": 0,
            "tlw": false
        },
        "google:suggestdetail": [],
        "google:suggestrelevance": [],
        "google:suggesttype": [],
        "google:verbatimrelevance": 871
    }
]
```

POST https://web.vortex.data.microsoft.com/collect/v1
Headers:
Origin: https://microsoftedgewelcome.microsoft.com
Cookie: MC1=GUID=**da7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000; MS0=dc42e1616b0e434e9bef71d2da20f061
Parameters:
$mscomCookies: false
ext−javascript−msfpc: 'GUID=**da7d27b6947c48b8abd43591e780322d**&HASH=da7d&LV=202002&V=4&LU=1581941544000'

GET http://leith.ie/nothingtosee.html
GET http://leith.ie/favicon.ico

POST https://nav.smartscreen.microsoft.com/api/browser/edge/navigate/1
Request Body:
<...>
"correlationId": "fc69e97f−0fd0−4677−9368−be0dd05e2612",
<...>
GET https://smartscreen-prod.microsoft.com/windows/browser/edge/data/bloomfilter/x?pushCert=false
User−Agent: SmartScreen/281479396982785

D. Connections Made On Re-Open After Close

POST https://nav.smartscreen.microsoft.com/api/browser/edge/actions
POST https://nav.smartscreen.microsoft.com/api/browser/edge/navigate/1
Request Body:
<...>
"correlationId": "8a0f0ec2−085e−4af8−8c67−4d8bbf095fb6",
<...>

GET https://ntp.msn.com/edge/ntp
Parameters:
locale: en−IE
fre: 1
dsp: 1
sp: Bing
startpage: 1
Response includes header:
x−msedge−ref: Ref A: **45047DC6B72A4D7E99A0327B27D5B92D** Ref B: DB3EDGE1216 Ref C: 2020−02−17T12:13:47Z
The Ref A value is now echoed back by the browser in subsequent requests

GET https://smartscreen-prod.microsoft.com/windows/browser/edge/data/bloomfilter/x
GET https://config.edge.skype.com/config/v1/Edge/80.0.361.48
GET https://www.msn.com/spartan/en-ie/getappanoncookie
GET https://otf.msn.com6/c.gif
Parameters:
<...>
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
OPTIONS https://otf.msn.com/c.gif
GET https://ntp.msn.com/service/graph/actions
Parameters:
apiKey: 0QfOX3Vn51YCz. . .
activityId: **45047DC6-B72A-4D7E-99A0-327B27D5B92D**
<...>
OPTIONS https://otf.msn.com/c.gif
GET https://204.79.197.203/service/graph/actions
:authority: ntp.msn.com
user−agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.87 Safari/537.36 Edg/80.0.361.48
cookie: sptmarket=en−IE||ie|en−ie|en−ie|en
Parameters:
apiKey: 0QfOX3Vn51YC. . .
activityId: **45047DC6-B72A-4D7E-99A0-327B27D5B92D**
<...>
GET https://otf.msn.com/c.gif
Parameters:
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
GET https://ntp.msn.com/service/graph/actions
Parameters
apiKey: 0QfOX3Vn51YCz. . .
activityId: **45047DC6-B72A-4D7E-99A0-327B27D5B92D**
<...>
GET https://ntp.msn.com/service/graph/actions
Parameters:
apiKey: 0QfOX3Vn51YCzitbLaRkTTBadtWpgTN8NZLW0C1SEM
activityId: **45047DC6-B72A-4D7E-99A0-327B27D5B92D**
<...>
GET https://ntp.msn.com/service/graph/actions

Headers:
cookie: sptmarket=en−IE||ie|en−ie|en−ie|en
Parameters:
apiKey: 0QfOX3Vn51YCz. . .
activityId: **45047DC6-B72A-4D7E-99A0-327B27D5B92D**
<...>
GET https://uhf.microsoft.com/_log
Headers:
cookie: MC1=GUID=da7d27b6947c48b8abd43591e780322d&HASH=da7d&LV=202002&V=4&LU=1581941544000; MS0=dc42e1616b0e434e9bef71d2da20f061
GET https://otf.msn.com/c.gif
Parameters:
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>

POST https://otf.msn.com/c.gif
Parameters:
<...>
”clid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
”rid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>

POST https://otf.msn.com/c.gif
Parameters:
<...>
”clid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
”rid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>

GET https://otf.msn.com/c.gif
Parameters:
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>

POST https://otf.msn.com/c.gif
Parameters:
<...>
”clid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
”rid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”
<...>
GET https://otf.msn.com/c.gif
Parameters:
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
POST https://otf.msn.com/c.gif
Parameters:
<...>
”clid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
”rid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
POST https://otf.msn.com/c.gif
Parameters:
<...>
”clid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
”rid”: ”**45047dc6b72a4d7e99a0327b27d5b92d**”,
<...>
GET https://otf.msn.com6/c.gif
Parameters:
rid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
clid: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
activityId: **45047dc6b72a4d7e99a0327b27d5b92d**
<...>
GET https://ntp.msn.com/edge/ntp/service-worker.js
POST https://edge.microsoft.com/componentupdater/api/v1/update
Headers:
x−microsoft−update−appid: gcmjkmgdlgnkkcocmoeiminaijmmjnii,oankkpibpaokgecfckkdkgaoafllipag,ojblfafjmiikbkepnnolpgbbhejhlcim,jbfaflocpnkhbgcijpkiafdpbjkedane
Response:

```
{
    ”request”: {
        ”@os”: ”mac”,
        ”@updater”: ”msedge”,
        ”acceptformat”: ”crx2,crx3”,
        ”app”: [
            {
                ”appid”: ”gcmjkmgdlgnkkcocmoeiminaijmmjnii”,
                ”enabled”: true,
```

<...>
The request and response are similar to other requests for browser extension updates by Chrome etc.

POST https://self.events.data.microsoft.com/OneCollector/1.0/
Parameters:
APIKey: 7005b72804a64fa4b2138. . .
SDK−Version: EVT−MacOSX−C++−No−3.2.297.1
Request Body:
\x033.0I&Microsoft.WebBrowser.SystemInfo.Configq\x80\xfc\x9f\xa3\xdf\xe8\xd9\xd7\x11\xa9”o:7005b72804a64fa4b2138faab88f877b\xd1\x06\x82\x04\xcb\x15
\x01i\x05Apple\x89\x0eMacBookPro15,2\x00\xcb\x16
\x01\x00\xcb\x17
\x01I&u:**0B5E1E28-B2E0-5DE9-848D-0368F**. . .\x00\xcb\x18
\x01\x89\x08Mac OS X\xa9\x0710.14.6\x00\xcb\x19
\x01\xa99M:com.microsoft.edgemac_80.0.361.48_x86_64 Microsoft Edge\xc9\x06\x0b80.0.361.48\x00\xcb\x1f
\x01I Unmeteredi\x05Wired\x00\xcb
\x01)\x1bEVT−MacOSX−C++−No−3.2.297.1I$a5f18c07−24cf−9556−9987−3e3815fd0914q\x02\x89$afb5a3dc−c3b5−b9d3−3170−c20f81fb6592\x00\xcb
\x01i\x0500:00\x00\xcb%
\x01\x00\xc9<\x06custom\xcbF
\x01−
\x10\x0cAppInfo.ETag\x00\x07Channel0\x00\x91\x08\x00\x0eConnectionTypei\x04WiFi\x00\x04Etag\x00\x0fEventInfo.Level0\x00\x91\x04\x00\x0cPayloadClassi\x0bSYSTEM_INFO\x00\x0b{PayloadGUID **i$67870410-95cc-41ab-bce2-3de3d5e0cea2\x00\x0e**PayloadLogType0\x00\x91
\x00\x0fappConsentState0\x00\x00\x0bapp_versioni\x0e80.0.361.48−64\x00 client_id **0\x00\x91\xb8\xcb\xa5\x88\xc0\xdc\xc1\xcf\xd2\x01\x00**
installSource0\x00\x00\x0cinstall_date0\x00\x91\x80\x81\xd4\xe4\x0b\x00
pop_sample0\x08\xa8\x00\x00\x00\x00\x00\x00Y@\x00
session_id0\x00\x91\x02\x00 utc_flags0\x00\x91\x80\x80\xc0\x80\x80\x80@\x00\x00\x00\x00
As in the previous POST to self.events.data.microsoft.com the request body contains the hardware UUID of the client device together with a number of other identifier-like values.

E. Connections Made When Sitting Idle

GET https://config.edge.skype.com/config/v1/Edge/80.0.361.48
Parameters:
enabledomainactions: 1
osname: mac
channel: stable
osver: 10.15.2
osarch: x86_64
uma: 0
mngd: 0
This seems to checking for updates to Edge itself. Response is usually 304 Not Modified

There seem to be two main request types made to edge.microsoft.com, as follows:
GET
https://edge.microsoft.com/extensionrevocation/v1/threatListUpdates:fetch
Parameters:
req: ChcKCGNocm9taXVtEgs3...
key: d414dd4f9db345fa8003...
This seems to be a call to a safe browsing API. Response is application/x-protobuf

POST https://edge.microsoft.com/componentupdater/api/v1/update
Headers:
x−microsoft−update−appid: bgieaagdibllmkdbmgagfgfonoaepegi, oankkpibpaokgecfckkdkgaoafllipag,gcmjkmgdlgnkkcocmoeiminaijmmjnii, ojblfafjmiikbkepnnolpgbbhejhlcim,jbfaflocpnkhbgcijpkiafdpbjkedane
Parameters:
cup2key: 3:1394258492
cup2hreq: 4
c380d719b819ca8a98e99d243fd2f0d054342beb920afcacfff073f7dfff373
This request seems to be checking for updates to browser extensions, using a similar API to Chrome etc. If there is an update, this seems to be downloaded from msedge.b.tlu.dl.delivery.mp.microsoft.com.

There seem to be two main request types made to smartscreen-prod.microsoft.com when the browser is idle, as follows:
POST https://smartscreen-prod.microsoft.com/windows/browser/edge/actions
Request Body:


```
{
    "config": {
        "device": {
            "appControl": {
                "level": "anywhere"
            },
            "appReputation": {
                "enforcedByPolicy": false,
                "level": "warn"
            },
            "pua": null
        },
        "user": {
            "uriReputation": {
                "enforcedByPolicy": false,
                "level": "warn"
            }
        }
    },
    "identity": {
        "caller": {
            "locale": "en−us"
        },
        "client": {
            "data": {
                "customSettings": "
F95BA787499AB4FA9EFFF472CE383A14",
                "customSynchronousLookupUris": "0",
                "edgeSettings": "1.0−5
abfbe7cfad552badaf691e9fc66d8038f212a9bdd7839199adb04a83e146ec6",
                "synchronousLookupUris": "637172430419439753",
                "topTraffic":
"319729430708873239333501969648228053463"
            },
            "version": "281479396851715"
        },
        "device": {
            "architecture": 9,
            "browser": {
                "internetExplorer": null
            },
            "cloudSku": false,
            "enterprise": null,
            "family": null,
            "locale": "en−us",
            "netJoinStatus": 0,
            "osVersion": "10.15.2.19C57"
        },
        "user": {
            "locale": "en−us"
        }
    }
}
```


The response is application/json. The value of customSettings in the request body is observed to stay constant across fresh installs, so does not seem to act as an identifier of the browser instance. The values of the edgeSettings and topTraffic fields are observed to change and whether theyt might act as identifiers is unclear.

GET https://smartscreen-prod.microsoft.com/windows/browser/edge/data/bloomfilter/x?pushCert=false
The response is application/octet-stream

F. Connections Generated By Auto-Complete As User Types

Connections generated as user types leith.ie/nothingtosee.html in the browser top bar.

GET https://www.bing.com/qbox
Parameters:
query: l
language: en−GB
PC: U531
pt: EdgBox
cvid: **870fc01328ae43118b7c06b24ff982e5**
ig: 76ccc01509bb45acba5782944b30ebee
oit: 1
cp: 1
pgcl: 4
Response sets cookies:
set−cookie: SRCHD=AF=NOFORM; domain=.bing.com; expires=Sat, 13−Mar−2021 14:46:59 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUID=V=2&GUID=5A4AEFE3F98B4D90BBDCACDEC73E4E3E&dmnchg=1; domain=.bing.com; expires=Sat, 13−Mar−2021 14:46:59 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUSR=DOB=20200217; domain=.bing.com; expires=Sat, 13−Mar−2021 14:46:59 GMT; path=/; secure; SameSite=None
set−cookie: _SS=SID=2E1AE47AABA36AD61FE9EA09AA086B50; domain=.bing.com; path=/; secure; SameSite=None
and returns json:
["l",["linkedin","linkedinlogin","lanebryant","lego","landsend","lakers","lastpass","lowe's","lululemon","lol","lisinopril","lebronjames","lizzo","lamborghini"],
<...>

GET https://www.bing.com/qbox
query: le
language: en−GB
PC: U531
pt: EdgBox
cvid: **870fc01328ae43118b7c06b24ff982e5**
ig: 4b4bf0b40b034dec9d4a0ecf85a6b8f7
oit: 1
cp: 2
pgcl: 4
Response sets cookies:
set−cookie: SRCHD=AF=NOFORM; domain=.bing.com; expires=Sat, 13−Mar−2021 14:47:00 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUID=V=2&GUID=57E6102FC042474496E4E3F89660EAF9&dmnchg=1; domain=.bing.com; expires=Sat, 13−Mar−2021 14:47:00 GMT; path=/; secure; SameSite=None
set−cookie: SRCHUSR=DOB=20200217; domain=.bing.com; expires=Sat, 13−Mar−2021 14:47:00 GMT; path=/; secure; SameSite=None
set−cookie: _SS=SID=347E80CBFE796B4029A28EB8FFD26A06; domain=.bing.com; path=/; secure; SameSite=None
and returns json:
["le",["lego","lebronjames","lenovo","letgo","leagueoflegends","leopard","lexus","lexapro","levothyroxine","lendingclub","legalzoom","legostarwars","letitgo","legacy","leonardodicaprio"
<...>

Plus requests for "leit", "leith", "leith.", "leith.i", "leith.ie", "leith.ie/", "leith.ie/n", "leith.ie/no", " leith.ie/not", 'leith.ie/noth", "leith.ie/nothi",

“leith.ie/nothin”, “leith.ie/nothing”, “leith.ie/nothingt”, “leith.ie/nothingto”, “leith.ie/nothingtos”, “leith.ie/nothingtose”, “leith.ie/nothingtosee”, “leith.ie/nothingtosee.”, “leith.ie/nothingtosee.h”, “leith.ie/nothingtosee.ht”, “leith.ie/nothingtosee.htm”, “leith.ie/nothingtosee.html”

A total of 25 requests.

Based on discussions with Microsoft the cvid value is an ephemeral identifier that changes between search sessions, i.e. after the user presses enter in the top bar.

After navigating to https://leith.ie/nothingtosee.html Edge then makes the following additional requests:

POST https://web.vortex.data.microsoft.com/collect/v1
Headers:
Cookie: MC1=GUID=f8608be5ec5347d99b3a2c674ff4f7b2&HASH=f860&LV=202002&V=4&LU=1581950694904; MS0=1a79bcd73509431bb5d4f14818154399
Parameters:
$mscomCookies: false
ext−javascript−msfpc: ’GUID=f8608be5ec5347d99b3a2c674ff4f7b2&HASH=f860&LV=202002&V=4&LU=1581950694904’
The cookie value is set by the call to web.vortex.data.microsoft.com when microsoftedgewelcome.microsoft.com finished loading, and so allows calls to web.vortex.data.microsoft.com to be linked (note that the cookie value here is different from above since the data here is collected from a fresh install of Edge, with the URL entered immediately after clicking the “GetStarted” button). Based on discussions with Microsoft this request is made upon first navigating away from the welcome page and is not repeated when navigating to subsequent pages.

POST https://nav.smartscreen.microsoft.com/api/browser/edge/navigate/1
Headers:
User−Agent: SmartScreen/281479396982785
Request body:

```
<...>
    ”correlationId”: ”5f530f2a−e381−4f9f−8bc8−f54ac70e8fa5”,
    ”destination”: {
        ”ip”: null,
        ”uri”: ”http://leith.ie/nothingtosee.html”
    },
<...>
```

Observe that in addition to sending the typed URL to www.bing.com, once the page is displayed the URL is also transmitted to nav.smartscreen.microsoft.com (Microsoft’s phishing/malware protection service) and presumably logged.

VI. Yandex Browser

A. Connections On First Startup

GET https://browser.yandex.com/wallpapers/api/desktop/new-albums?partnerId=
Headers:
Cookie: ys=ybzcc.int#def_bro.0
Response is application/json

GET https://api.browser.yandex.com/wprotate/get
Headers:
cookie: ys=ybzcc.int
The value of this cookie is constant across fresh installs and across different devices and so presumably is tied to the browser version rather than to a particulatr browser instance. Response is application/json

GET https://bro-bg-store.s3.yandex.net/f820515b-04cb-4aed-8a3c-50816cb8e3b2.webm

GET https://sba.yandex.net/v4/threatListUpdates:fetch
Parameters:
$req: ChkKB2Jyb21pdW0SDjc...
$ct: application/x−protobuf
key: 01521754e0283a...
This seems to a call to the Safe Browsing API, or similar. Response is application/x-protobuf

GET https://yastatic.net/s3/bro-bg-store/0baffecb-0407-41b7-94cf-73baf39c9aa8.jpg
GET https://sba.cdn.yandex.net/csd/client_model_v5_variation_0.pb
GET https://sba.cdn.yandex.net/csd/client_model_v5_ext_variation_0.pb
GET https://api.browser.yandex.ru/sba/cp
GET https://yandex.ru/prefetch.txt
Headers:
cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0
Note that at this point no cookies have been set by server responses and so these values are presumably generated by the browser itself. The value of the yp cookie changes across fresh installs and so acts an an identifier of the browser instance.

Response sets cookie:
set−cookie: i=**wafLP9GWR**...; Expires=Thu, 14−Feb−2030 19:28:22 GMT; Domain=.yandex.ru; Path=/; Secure; HttpOnly; SameSite=None
The value of this cookie changes across fresh installs and so acts as an identifier of the browser instance.

GET https:// mail.yandex.ru/prefetch.txt
Headers:
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**...

GET https://yastatic.net/s3/home/fonts/ys/1/prefetch.txt
GET https://yastatic.net/s3/web4static/_/v2/cmmv5ByveliklEGiDrfh64srLVc.js
GET https://yastatic.net/s3/web4static/_/v2/ffij9uH3QVDe-sa5jzJ3iLwvyso.js
GET https://yastatic.net/s3/web4static/_/v2/kikhcb107KEIYqQLbJTMaHe7qb8.js
GET https://browser.yandex.ru/wallpapers/api/rotate/266
Headers:
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**...
GET https://yastat.net/s3/home/fonts/ys/1/text-bold.woff2
GET https://yastatic.net/s3/bro-bg-store/cd354bdb-c311-4c2f-95b3-c2e5f9277643.jpg
GET https://yastat.net/s3/home/fonts/ys/1/text-medium.woff2
GET https://yastat.net/s3/home/fonts/ys/1/text-regular.woff2
GET https://yastatic.net/jquery/1.12.4/jquery.min.js
GET https://yastatic.net/mail/_/0378065f40bc06d8acef-0.js
GET https://yastatic.net/mail/_/0ffc9e9cbecac628607f-bootstrap.js
GET https://yastatic.net/mail/_/14ad933e5a316e460eb0-28.js
GET https://yastatic.net/mail/_/22b6327274706526d3b1-2.js
GET https://yastatic.net/mail/_/36f22d17f61cf6e2d4a4-36.js
GET https://yastatic.net/mail/_/5b7f81734de837933134-14.js
GET https://yastatic.net/mail/_/60a02cbe437c0fe55c25-3.js
GET https://yastatic.net/mail/_/678ba6173f5bce429064-39.js
GET https://yastatic.net/mail/_/8d52d97f8eefa03cad42-6.js
GET https://yastatic.net/mail/_/94e15b97112f0d3e45af-35.js
GET https://yastatic.net/mail/_/a47415a84486d3ee580e-4.js
GET https://yastatic.net/mail/_/boot-c464e222e41f1a2b5fd455d26b96c791.css
GET https://yastatic.net/mail/_/ceae4ba7a3efb1977266-30.js
GET https://yastatic.net/mail/_/de8cf1d58e33faf0abb8-33.js
GET https://yastatic.net/mail/_/e2ae158219487d2771da-1.js
GET https://yastatic.net/mail/_/ee57c82c8edc27ff405f-9.js
GET https://yastatic.net/mail/_/f9594b8e69a4e25804fd-7.js
GET https://yastatic.net/mail/_/fdf4db889928bc6f574e-12.js
GET https://yastatic.net/mail/_/left-43b7b2293ee8df1d7430e279239fc02c.css
GET https://yastatic.net/mail/_/mail-7d03b31ce69af45097f182b71a71d36d.css
POST https://sync.browser.yandex.net/sync/experimentstatus
GET https://storage.ape.yandex.net/get/browser/web_components/plugins_mac.json
GET https://yastatic.net/mail/_/messages-ebfcc9c22362868cd7a91fbadf3e73f0.css
GET https://yastatic.net/mail/_/nanoislands-1f6155334ce223a68d7de2d256418d72.css
GET https://yastatic.net/mail/_/old-55d8b5f85e4eafeb05c926a2943d0508.css
GET https://yastatic.net/mail/_/theme-colorful-62c19cc96561bc01702bffe7fe1b82af.css
GET https://yastatic.net/mail/_/theme-seasons-c16e4d592d4811cef9759b46ffa003f3.css
GET https://yastatic.net/mail/_/theme-weather-03a68fe3288f5a01c364a9c67246e08c.css
GET https://yastatic.net/nearest.js
GET https://yastatic.net/s3/home/fonts/ys/1/text-bold.woff2
GET https://yastatic.net/s3/home/fonts/ys/1/text-medium.woff2
GET https://yastatic.net/s3/home/fonts/ys/1/text-regular.woff2

B. Clicking on "Yandex Search" Button

GET https://browser.yandex.ru/welcome
Headers:
X−Yandex−UI: C3788EAE5EA242B9BB915DFC...
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**...
The value of the X-Yandex-UI header is constant across fresh installs and across devices, so is presumably tied to the browser version rather than to a particular browser instance or device.
GET https://api.browser.yandex.com/ntp/widgets
Headers:
cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0
GET https://api.browser.yandex.ru/content/get/experiments/browser.proto
GET https://api.browser.yandex.com/ntp/widgets?
Headers:
cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0
GET https://pages.browser.yandex.ru/zen_error_iframe.html
Headers:
cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**...
GET https://yastatic.net/s3/home/yabro/notification/ether_opacity.svg
GET https://yastatic.net/s3/home/yabro/notification/desk-notif-card__stream_icon_play.svg
GET https://yastatic.net/s3/home/yabro/notification/ether_icon.svg
GET https://yastatic.net/s3/zen-lib/2.203.0/zenlib-desktop/loader.legacy.bundle.js
GET https://yastatic.net/s3/home/yabro/notification/desk-notif-card__stream_icon_dot.svg
GET https://browser.yandex.ru/activation/metrika/
Headers:
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0
Response sets cookie:
Set−Cookie: yandexuid=**2527063231581967889**; Domain=.yandex.com; Path=/; Expires=Sun, 17 Feb 2030 19:31:29 GMT
The value of the yandexuid cookie changes across fresh installs and so acts as an identifier of the browser instance.

GET https://yastatic.net/s3/zen-lib/2.203.0/zenlib-desktop/app.css
GET https://collections.yandex.ru/collections/api/v0.1/recent-timestamp
Headers:
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**...
GET https://browser.yandex.ru/welcome/
Headers:
X−Yandex−UI: C3788EAE5EA242B9BB915DFC...

Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**. . .
Response sets cookie:
Headers:
Set−Cookie: yandexuid=**641582481581967889**; Domain=.yandex.ru; Path=/; Expires=Sun, 17 Feb 2030 19:31:29 GMT
A different value of the yandexuid cookie is set for domain yandex.ru (the previous value is for domain yandex.com).

GET https://yastatic.net/s3/zen-lib/2.203.0/zenlib-desktop/app.chromium.en.bundle.js
GET https://browser.yandex.ru/welcome-update/r/data-collection/
Headers:
Cookie: yp=**1613503686.cld.2112413**; ys=ybzcc.int#def_bro.0; yandexuid=**2527063231581967889**

GET https://browser.yandex.ru/welcome-update/r/data-collection/
Headers:
X−Yandex−UI: C3788EAE5EA242B9BB915DFC...
Cookie: ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**. . .; yandexuid=**641582481581967889**; yp=**1613503891.cld.2112413**

GET https://yastatic.net/s3/distribution/stardust/react-welcomes/v1.4.2/build/data-collection.build.css
GET https://yastatic.net/s3/distribution/stardust/react-welcomes/v1.4.2/build/vendor.js
GET https://yastatic.net/s3/distribution/stardust/react-welcomes/v1.4.2/build/data-collection.build.js
GET https://yastatic.net/ravenjs/3.15.0/raven.min.js
GET https://mc.yandex.ru/metrika/watch.js
Headers:
Cookie: ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**. . .; yandexuid=**641582481581967889**; yp=**1613503891.cld.2112413**

GET https://yastatic.net/islands/_/TR2STky64Ra69XlYzqKN7cnjYfQ.woff2
POST https://mc.yandex.ru/watch/3/1
Headers:
Cookie: ys=ybzcc.int#def_bro.0; i=**wafLP9GWR**. . .; yandexuid=**641582481581967889**; yp=**1613503891.cld.2112413**
Parameters:
browser−info: ti:10:fu:2:v:1808:rqnl:1:st:1581967892:u:
Response sets cookies:
Set−Cookie: yp=**1613503891.cld.2112413**; Expires=Thu, 14−Feb−2030 19:31:32 GMT; Domain=.yandex.ru; Path=/; SameSite=None; Secure
Set−Cookie: i=**MUder0bCuVZNQQNZM1**. . .; Expires=Tue, 16−Feb−2021 19:31:32 GMT; Domain=.yandex.ru; Path=/; Secure; HttpOnly; SameSite=None
Set−Cookie: yandexuid=**641582481581967889**; Expires=Tue, 16−Feb−2021 19:31:32 GMT; Domain=.yandex.ru; Path=/; SameSite=None; Secure
Set−Cookie: yuidss=**641582481581967889**; Expires=Tue, 16−Feb−2021 19:31:32 GMT; Domain=.yandex.ru; Path=/; SameSite=None; Secure
Set−Cookie: ymex=**1613503892.yrts.158**. . .; Expires=Tue, 16−Feb−2021 19:31:32 GMT; Domain=.yandex.ru; Path=/;
The value of the yuidss cookie is set to match yandexuid. The value of i the cookie is reset but since the original value was sent with the request the server can link these values together. The value of ymex changes across fresh installs

GET https://yastatic.net/islands/_/KRBKbh7904nwfw8-FzDelXRpZ9o.woff2
GET https://yastatic.net/q/global-notifications/cc/_lego-cc.en.js
GET https://api.browser.yandex.ru/sba/cp
GET https://soft.export.yandex.ru/status.xml
Parameters:
client_id: **169682930770929...**
machine_id: **5D40DBFECB. . .0000000109**
ui: C3788EAE−5EA2−42B9−BB91−5DFC95...
The machine_id value remains the same across fresh installs but changes on different devices. It seems to be a persistent identifier derived from the device hardware, namely via the GetMachineIdImpl() function in Chromium[15] *which generates a 49 byte value with the first 40 bytes being an SHA1 hash of the MAC address of the device primary network interface and the device serial number, the next 8 bytes are the 64 bit integer representation of the value 1 and the last byte is a checksum. The client_id value changes across fresh installs of the browser and so acts as an identifier of the browser instance. The ui value matches that of the X-Yandex-UI header (with the addition of hyphens).*

GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/ntp/get/
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/update-info/browser/int/mac-int.rss
Parameters:
uid: C3788EAE−5EA2−42B9−BB91−5DFC95D6B728

GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/installstats/send/dtype=stred/pid=457/cid=72992/path=extended_stat/vars=-action=setup,-brand_id=int_custo,-partner_id=,-stage=complete,-ui=**C3788EAE_5EA2_42B9_BB91_5DFC95D6B728**,-ver=/*
GEThttps://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard3/blist?lang=en-US
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://api.browser.yandex.com/dashboard/get_scales
GET https://storage.mds.yandex.net/get-browser/52018/dashboard/bNtiXT1XAHlQf9YhwxIL6w.svg
GET https://storage.mds.yandex.net/get-browser/42135/dashboard/5IpzbjCQiHJThK5TM-dChw.svg
GET https://storage.mds.yandex.net/get-browser/42135/dashboard/oXIrv5nAtnhFzQm8LKOnug.svg
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/Mv0QPDdhEgBBJb0oUQ9PpQ.svg
GET https://storage.mds.yandex.net/get-browser/38105/dashboard/NXyiFChT_Azu4lr8Y_9QlQ.png
GET https://storage.mds.yandex.net/get-browser/38105/dashboard/BgasWHG2ZKV8KSdyCUn1vA.svg
GET https://storage.mds.yandex.net/get-browser/42135/dashboard/cE5CdH_3gF0FB195e_1P3Q.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/8mrBjFJl7GnyaiHOZ8gcuw.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/qWbY4sb57IisDirI9aj8dQ.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/RvEzoIth7FzSsPgRrxtwhw.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/Xh8tBJDt7wk7onp0j_-YOA.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/kzQqp3I6GeUEpSxgtpILVw.png
GET https://storage.mds.yandex.net/get-browser/42135/dashboard/oqHiQPhcgilssE67FRY4Bw.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/JfKP9pPE01-X_wcLzunJmg.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/3-mHyBXjNSeus4elDDQxmw.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/iWY48ZaXHzOEzVglihP0OQ.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/58GpaXl0oKnTGiDVMBwGXw.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/dGETMu-afRcsiQyKsx6yzA.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/XdGDk2ayzlT4ZzCNJiCObg.png
GET https://storage.mds.yandex.net/get-browser/67255/dashboard/KCGrGNGyLa2g1a7VZ3fEhQ.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/QCym8dE7Y0jv1gSATamLsg.png
GET https://storage.mds.yandex.net/get-browser/38105/dashboard/AOHW6pEqlzzh1103pvH--A.png
GET https://storage.mds.yandex.net/get-browser/68995/dashboard/3FwKFwFaMVXVQ8otU7f8IQ.png

[15] See files rlz/lib/machine_id.cc and rlz/mac/lib/machine_id_mac.cc in the Chromium source.

GET https:
//yastatic.net/s3/bro-bg-store/a8ac881f-99a7-4782-8088-4730a3736e75.jpg
GET https:
//yastatic.net/s3/bro-bg-store/116cb7d6-6791-42da-b1c7-ebdf07771ef5.jpg

GET https://strm.yandex.ru/vh-browser-converted/vod-content/
15120286228192265404_169_768p.webm
Headers
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D

GET https://browser.yandex.ru/wallpapers/api/rotate/266
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D

GET https://yastatic.net/s3/bro-bg-store/81771fa3-81de-4a66-98a3-
a84bf376f4a6.jpg

GET https://strm.yandex.ru/vh-browser-converted/vod-content/
15120286228192265404_169_1080p.webm
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D

GET https://soft.export.yandex.ru/status.xml
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**. . .
ui: C3788EAE−5EA2−42B9−BB91−5DFC95D6B728
yandexuid: **641582481581967889**

GET https://zen.yandex.ru/yabro/index.html
Host: zen.yandex.ru
GET https://zen.yandex.ru/yabro/index.html
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D

GET https://yastatic.net/s3/zen-
lib/2.263.9/yabro/maintenance.chromium.ru.bundle.js
GET https://yastatic.net/s3/zen-lib/2.263.9/yabro/client-
errors.chromium.ru.bundle.js
GET https://yastatic.net/s3/zen-lib/2.263.9/yabro/custo-page-scrollbar.js
:authority: yastatic.net
GET https://yastatic.net/s3/zen-lib/2.263.9/loader/loader.chromium.bundle.js
GET https://yastatic.net/s3/zen-lib/2.263.9/yabro/yabro.css
:authority: yastatic.net
GET
https://yastatic.net/s3/zen-lib/2.263.9/yabro/yabro.chromium.en.bundle.js
GET https://yastatic.net/s3/zen-lib/favicons3/favicon-32x32.png
:authority: yastatic.net
GET https:// zen.yandex.ru/api/v3/launcher/export
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
Parameters:
clid: 2271310
rnd: 1581967955371

GET https:// zen.yandex.ru/yabro/service-worker.js
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=
MUder0bCuVZNQQNZM1. . .; yuidss=**641582481581967889**; ymex=
1613503892.yrts.158. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced
=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22
eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D

GET https://yastatic.net/s3/home/fonts/ys/1/text-light.woff2
GET https://9bro-bg-store.s3.yandex.net/f820515b-04cb-4aed-8a3c-
50816cb8e3b2.webm

GET https:// sba.yandex.net/v4/threatListUpdates:fetch
Parameters:
$req: ChkKB2Jyb21pdW0SDj. . .
key: 01521754e0283a. . .

GET https://api.browser.yandex.net/configs/all_zip
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**. . .

POST https:// api.browser.yandex.com2/cupdate/get
Headers:
x−goog−update−appid: gnlefjfipbnlnkcohfkoollpigihdaek
Request Body:
<...>
"machine_id": "**35D40DBFECB**. . .",
<...>
GET https://download.cdn.yandex.net/browser/crx3/hat/20_02_05_01.crx
GET https://cache-default01h.cdn.yandex.net/download.cdn.yandex.net/
browser/crx3/hat/20_02_05_01.crx
POST https://update.googleapis.com/service/update2/json
Headers:
x−goog−update−appid: hfnkpimlhhgieaddgfemjhofmfblmnib,
oimompecagnajdejgnnjijobebaeigek,hnimpnehoodheedghdeeijklkeaacbdc
GET http://redirector.gvt1.com/edgedl/release2/chrome_component/
AMYfeLjqMD0L3c1. . .
GET http://r3---sn-q0c7rn76.gvt1.com/edgedl/release2/chrome_component/
AMYfeLjqMD0L3c1xsk. . .
GET http://redirector.gvt1.com/edgedl/chromewebstore/
L2Nocm9tZV9leHRlbnNpb. . ./4.10.1582.2_
oimompecagnajdejgnnjijobebaeigek.crx
GET http://r4---sn-q0cedn7s.gvt1.com/edgedl/chromewebstore/
L2Nocm9tZV9leHRlbnNpb24. . ./4.10.1582.2_
oimompecagnajdejgnnjijobebaeigek.crx
GET http:
//redirector.gvt1.com/edgedl/chromewebstore/L2Nocm9tZV9leHRlbn. . ./0.
57.44.2492_hnimpnehoodheedghdeeijklkeaacbdc.crx
GET http://r5---sn-q0c7rn76.gvt1.com/edgedl/chromewebstore/
L2Nocm9tZV9leHRlbn. . ./0.57.44.2492_
hnimpnehoodheedghdeeijklkeaacbdc.crx
POST https:// api.browser.yandex.com2/cupdate/get
Headers:
x−goog−update−appid: igomlkonjcmjlliglfnjfhkgmjpbeoel,
hhhgobidkfmmjogmggpheegjclbdcegm,gadfhegkcccmeaogagbbdbggopjgopio,
lilcnlfdlljcegdcinbbmdekbepkpibp,dgfcbhdmmlbdndoheeodpplamagnocli,
nbpjjkkldnniojjnhnfefnndlpplpnhb,pjmljaobnjdafibmlnhbfpfiflmlnieg,
hnkogepebjcohfmmiiklndhgkahmdeja,fbiljjabopogcepmmdjfedmahiccablo,
lglcjdpfhlnihglnecghdhgjgfipjafb,gnlefjfipbnlnkcohfkoollpigihdaek,
lkbinnfaehilihednohobmmflcndblof

GET
https://download.cdn.yandex.net/browser/crx3/flash/mac/32_00_00_293.crx
GEThttps://cache-default02h.cdn.yandex.net/download.cdn.yandex.net/
browser/crx3/flash/mac/32_00_00_293.crx
GEThttp://storage.mds.yandex.net/get-browser-components/2809972/
1581931188/crx3/yablocker2/20_02_17_00.crx
GEThttps://storage.mds.yandex.net/browser/crx3/https_ew/20_02_17_00.crx
GET https://storage.mds.yandex.net/download.cdn.yandex.net/browser/crx3/
https_ew/20_02_17_00.crx
GET
https://storage.mds.yandex.net/browser/crx3/pupo_blacklist/19_06_13_00.crx
GET https://cache-default04h.cdn.yandex.net/download.cdn.yandex.net/
browser/crx3/pupo_blacklist/19_06_13_00.crx
GET https:
//storage.mds.yandex.net/browser/crx3/payments_autofill/19_09_12_00.crx
GET https://cache-default04h.cdn.yandex.net/download.cdn.yandex.net/
browser/crx3/payments_autofill/19_09_12_00.crx
GET
https://storage.mds.yandex.net/browser/crx3/internal_promo/19_06_12_00.crx
GET https://storage.mds.yandex.net/download.cdn.yandex.net/browser/crx3/
internal_promo/19_06_12_00.crx
GET https://storage.mds.yandex.net/browser/crx3/suggest_catboost_model_

tag_model_19_7_3_14/19_07_03_14.crx
GET https://storage.mds.yandex.net/download.cdn.yandex.net/browser/crx3/suggest_catboost_model_tag_model_19_7_3_14/19_07_03_14.crx
GET https://sba.yandex.net/v4/fullHashes:find
$req: ChkKB2Jyb...
key: 01521754e0283a...
Response sets cookie:
set−cookie: ys=def_bro.0#wprid.1581968154007023−722466846943183734043660−man1−4421#ybzcc.int; path=/; domain=.yandex.ru; Secure; SameSite=None

GET https://yandex.ru/search/pre
cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
GET https://yandex.ru/favicon.ico
cookie: yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D; ys=**def_bro.0\#wprid.15819**...

GET https://yastatic.net/jquery/2.1.4/jquery.min.js
GET https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch
Parameters:
$req: ChMKBlNhZmFya...
key: AIzaSyANT−dOXDTNxZS4flEImFNycnoe...
GET https://yastatic.net/react/16.8.4/react-with-dom-and-polyfills.min.js
GET https://yastatic.net/s3/web4static/_/v2/198f549e44583ac78470.js
GET https://yastatic.net/lego/_/pDu9OWAQKB0s2J9IojKpiS_Eho.ico
GET https://178.154.131.216/s3/web4static/_/v2/ffij9uH3QVDe-sa5jzJ3iLwvyso.js
GET https://collections.yandex.ru/collections/api/v0.1/recent-timestamp
Cookie: yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D; ys=**def_bro.0#wprid.15819**...
GET https://api.browser.yandex.com/store/crx/v1/featured?locale=en-US
cookie: ys=ybzcc.int#def_bro.0; yandexuid=**2527063231581967889**; yp=1613503890.cld.2112413
GET https://sba.yandex.net/v4/threatListUpdates:fetch
Parameters:
$req: ChkKB2Jyb21pd...
key: 01521754e0283a...
GET https://api.browser.yandex.com2/configs/url_symbols
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https://api.browser.yandex.com2/configs/api_pool
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https://api.browser.yandex.com2/configs/wlpconf
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https:// api.browser.yandex.com2/configs/pushblocker
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https://api.browser.yandex.com2/configs/rewrite_list
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https://api.browser.yandex.com2/configs/forced_update
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...
GET https:// api.browser.yandex.com2/configs/replace
Parameters:
client_id: **169682930770929...**
machine_id: **35D40DBFECB**...

C. Connecting to A Plain Web Page

Connections made after pasting URL http://leith.ie/nothingtosee.html into browser top bar.

GET https://yandex.ru/suggest/suggest-browser
Headers:
cookie: yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D; ys=**def_bro.0#wprid.15819**...
Parameters:
part: http://leith.ie/nothingtosee.html
Response is json:
["http://leith.ie/nothingtosee.html",[],[],[],{"endings":[],"freqs":[],"google:suggesttype":[],"suggestions":[],"types":[],"yandex:answer":[]}]

GET http:// leith.ie/nothingtosee.html
GET http:// leith.ie/favicon.ico

POST https://translate.yandex.net/api/v1/tr.json/detect?srv=yabrowser&request_id=392952917
Request Body:
text: Boring test page

D. Connections Made On Re-Open After Close

GET https://api.browser.yandex.com2/ntp/widgets
cookie: ys=ybzcc.int#def_bro.0; yandexuid=**2527063231581967889**; yp=1613503890.cld.2112413

GET https://api.browser.yandex.com2/ntp/widgets
cookie: ys=ybzcc.int#def_bro.0; yandexuid=**2527063231581967889**; yp=1613503890.cld.2112413

GET https://yastatic.net/s3/bro-bg-store/7191a300-20f2-4d26-a46d-32042025be2d.jpg
GET https://api.browser.yandex.com2/content/get/experiments/browser.proto?osname=mac&channel=stable&milestone=79

GET http://leith.ie/favicon.ico

POST https://translate.yandex.net/api/v1/tr.json/detect?srv=yabrowser&request_id=3746020779
Request Body:
text: Boring test page

GET https://87.250.250.29/collections/api/v0.1/recent-timestamp
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
GET https://en.yandex.ru/api/v3/launcher/export
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
GET https://zen.yandex.ru/yabro/service-worker.js
Cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**...; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**...; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
GET https://api.browser.yandex.com2/ntp/get/
GET https://api.browser.yandex.com2/dashboard3/blist
GET https://sba.cdn.yandex.net/csd/client_model_v5_variation_0.pb
GET https://sba.cdn.yandex.net/csd/client_model_v5_ext_variation_0.pb
GET https://api.browser.yandex.com2/sba/cp

GET https://sba.yandex.net/v4/fullHashes:find
Parameters:
$req: ChkKB2Jyb21pd...

key: 01521754e0283a. . .

GET https://yandex.ru/search/pre
cookie: ys=ybzcc.int#def_bro.0; yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**. . .; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
GET https://yandex.ru/favicon.ico
cookie: yandexuid=**641582481581967889**; i=**MUder0bCuVZNQQNZM1**. . .; yuidss=**641582481581967889**; ymex=**1613503892.yrts.158**. . .; yp=**1613503892.cld.2112413**; _ym_wasSynced=%7B%22time%22%3A1581967892462%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D; ys=def_bro.0#wprid.1581968397331789−317736487288352848558371−man1−3559#ybzcc.int
GET https://yastatic.net/lego/_/pDu9OWAQKB0s2J9IojKpiS_Eho.ico
GET https://yastatic.net/s3/web4static/_/v2/ffij9uH3QVDe-sa5jzJ3iLwvyso.js
GET https://yastatic.net/s3/web4static/_/v2/198f549e44583ac78470.js
GET https://yastatic.net/jquery/2.1.4/jquery.min.js
GET https://yastatic.net/react/16.8.4/react-with-dom-and-polyfills.min.js

E. Connections Made When Sitting Idle

GET https://collections.yandex.ru/collections/api/v0.1/recent-timestamp
Headers:
Cookie: yandexuid=3986319101581581555; ys=def_bro.0#wprid.1581581555512961−782102994689863191094638−man1−3697#ybzcc.int; yp=1613117556.cld.2112413; i=JbWvwJqmKHWCapakVh11NEw9JXeJhA5eJ5+lxc187kdjCmiKLFJvQpAZeDmjOx4vKPpotLJnicSRYeOkAVYCP0t5Ws8=
Parameters:
source_name: yabrowser
source_version: 20.2.0.1145
ui: desktop

Several types of request are made to api.browser.yandex.net including:
GET https://api.browser.yandex.net/configs/mining_whitelist
GET https://api.browser.yandex.net/configs/known_antivirus
GET https://api.browser.yandex.net/configs/ua_change
All of these requests transmit the following values:
Parameters:
brandID: int
client_id: 9034088184062436259
machine_id: BF92A2637943257838D2D659797C6F099BA6B11500000001EF

Two types of request are made to api.browser.yandex.com including:
GET https://api.browser.yandex.com/store/crx/v1/thumbnails
GET https://api.browser.yandex.com/store/crx/v1/showcase
These requests transmit the following header values:
Headers:
x−yauuid: eb69d31827654cd8882e761a92a90dab
cookie: yp=1613117289.cld.2112413; ys=ybzcc.int#def_bro.0

POST https://sync.browser.yandex.net/sync/experimentstatus
Request Body:
\x0bgcm_channel

GET https://sba.yandex.net/v4/threatListUpdates:fetch
Parameters:
$req: ChkKB2Jyb21pdW0SDjc5L. . .
$ct: application/x−protobuf
key: 01521754e0283a825c33. . .

F. Connections Generated By Auto-Complete As User Types

Connections generated as user types leith.ie/nothingtosee.html in the browser top bar.

GET https://yandex.ru/suggest/suggest-browser
Headers:
cookie: ys=ybzcc.int#def_bro.0; yandexuid=4216748441582013902; i=d60gum1z2MMq1IV0. . .; yuidss=4216748441582013902; ymex=1613549905.cld.2112413; _ym_wasSynced=%7B%22time%22%3A1582013905086%2C%22params%22%3A%7B%22eu%22%3A1%7D%2C%22bkParams%22%3A%7B%7D%7D
Parameters:
part: l
<...>
The cookies are sent with every request. The valus of the cookies differ from those in the traces above because the autocomplete test here was carried out with as fresh browser install. The response is json:
["l",["logitech","lottery.ie","logitechunifyingsoftware","liepainiekiem.lv","livetv.sx","laptitvonline??????????????????","list","laptop","lottoie","livetvsx"],<...>

Plus requests for every subsequent letter typed: "'le", "lei", "leit", "leith", "leith.", "leith.i", "leith.ie", "leith.ie/", "leith.ie/n", "leith.ie/no", "leith.ie/not", 'leith.ie/noth", "leith.ie/nothi", "leith.ie/nothin", "leith.ie/nothing", "leith.ie/nothingt", "leith.ie/nothingto", "leith.ie/nothingtos", "leith.ie/nothingtose", "leith.ie/nothingtosee", "leith.ie/nothingtosee.", "leith.ie/nothingtosee.h", "leith.ie/nothingtosee.ht", "leith.ie/nothingtosee.htm", "leith.ie/nothingtosee.html"

A total of 26 requests.

After navigating to leith.ie/nothingtosee.html the browser then makes the following two additional requests:

GET https://yandex.ru/ugcpub/iznanka
Parameters:
text: leith.ie
POST https://translate.yandex.net/api/v1/tr.json/detect
Parameters:
text: Boring test page
The first request transmits the domain visited and the second send the page content (presumably for translation)