

Homework Assignment - Privacy

Cyber Security and Resilience Program

Flita-Vasile Adrian
September 26, 2022

1 What are the required conditions to gather a lawful consent of data processing of a natural person regarding GDPR? What is the difference if the person is a child? Who is a child? What do you need consent for?

1.1 Solving

‘Explicit consent’ is one of the main conditions for processing data of a person. In particular, it must be freely given, specific, affirmative and unambiguous, and able to be withdrawn at any time. Also, In practice, the extra requirements for consent to be ‘explicit’ are likely to be:

- explicit consent must be confirmed in a clear statement (whether oral or written), rather than by any other type of affirmative action;
- it must specify the nature of the special category data;
- it should be separate from any other consents you are seeking.

Explicit consent is the only condition that can apply to a wide range of circumstances, and in some cases may be your only option. If so, you need to make sure that you offer people genuine choice over whether and how you use their data.

You need to be particularly careful if you ask for consent as a condition of your services, or if you are in a position of power over the individual, for example, if you are a public authority or their employer.

The processing of the personal data of a child shall be lawful where the child is at least 16 years old. When a child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Some states provide a lower age like 13 for the consent of the holder of parental responsibility over the child. So in some states you are consider a child until the age of 13 and in other until the age of 16.

So basically any freely given, explicit, informed, and unequivocal expression of the data subject’s intentions through which he or she, by a statement or by a clear affirmative action, expresses approval to the processing of personal data relating to him or her is referred to as consent by the data subject.

2 Why have the data protection agreements between the US and the EU been outlawed? What was the essential difference between the Safe Harbour and Privacy Shield agreements?

2.1 Solving

The decision to share data between US and EU was adopted on 12 July 2016 and allowed the free transfer of data to companies certified in the US under the Privacy Shield. This was so called ”Umbrella Agreement”, the agreement aims to ensure that personal data is protected to a high standard when being transferred by law enforcement authorities (police and criminal justice authorities). It also aims to foster law enforcement cooperation between the EU and the EU countries, on the one hand, and the US on the other. It provides

greater legal certainty and strengthens the rights of the individuals concerned by the transfer of their data.

KEY POINTS

- The agreement complements rules regarding personal data protection in existing EU/EU country-US agreements, and in national laws, that authorise the exchange of information for law enforcement purposes. It establishes a common data protection framework which will also apply to future agreements and national laws in this field.
- The agreement covers all personal data (including names, addresses, criminal records) exchanged between the EU and the US for the purpose of the prevention, detection, investigation and prosecution of criminal offences, including terrorism.

The "Umbrella Agreement" was cancelled because the data were also transferred to companies and they were not only used for law enforcement.

A new EU-US data protection "Umbrella Agreement" has been finalized which once in force will implement a high-level data protection framework to cover the transfer of personal data from the EU to US authorities for the purposes of law enforcement. Although this new agreement relates only to the transfer of information for law enforcement purposes, those issues have been particularly sensitive post-Snowden.

Privacy Shield was designed to replace the old Safe Harbor program, and allow the transfer of data from the European Union to the US. There are a number of key differences between the two certifications:

- New declarations regarding participating in the program.
- New access rights
- Free dispute resolution
- Respond within 45 days
- New closer relationship between the Dept of Commerce and the local DPAs
- Ability to invoke Binding Arbitration
- New rules relating to data integrity and use limitation
- New liabilities related to onward transfer of data
- Data is subject to the principles for its lifetime
- Increased transparency

3 Why is meta data that valuable? Is it possible to encrypt it? (Hint: Gnxr n ybbx ng VCfrp.) Give examples of massive meta data collections by companies and states.

3.1 Solving

Metadata, also known as data that describes other data, is organized reference material that aids in classifying and identifying characteristics of the data it describes. John W. Warren refers to metadata as "both a cosmos and DNA" in *Zen and the Art of Metadata Maintenance*. Metadata summarizes basic information about data, which can make it easier to find, use and reuse particular instances of data.

Simple document file metadata includes things like author, date created, date edited, and file size. Finding a given document is made considerably simpler when one has the option to search for a specific aspect (or elements) of that metadata.

In addition to document files, metadata is used for:

- computer files
- images
- relational databases
- spreadsheets
- videos
- audio files
- web pages

In general, metadata can not be encrypted because is often used for an app or a website to function. Metadata encryption is a developing technology that many apps do not offer. One solution is using a VPN that can block certain metadata such as an IP address from the app. Other than that there is no other example of commercially available metadata encryption.

One popular example of metadata collection is owned by IBM. For the storage devices that are being monitored, asset, capacity, configuration, and performance metadata are gathered and stored. Additionally, diagnostic information is gathered and added to support issues as log packages.

Storage systems, switches, fabrics, and hosts all have associated metadata that describes how they are set up and how they function. On-device data is not accessible or gathered in its actual form.

The metadata that is collected is used for the following tasks:

- To provide and improve services
- To analyze and get insights into storage usage and performance
- To generate charts and present data in IBM® Storage Insights
- To upload logs when support tickets are created or updated
- To enable IBM Support to investigate and close the issues that you might encounter

Other popular collection of metadata NSA collection of phone records of millions of Verizon customers daily. Under a top-secret court order obtained in April, the National Security Agency is now gathering the telephone records of millions of Verizon, one of America's largest telecoms carriers, subscribers in the US. The order, a copy of which was obtained by the Guardian, mandates that Verizon provide the NSA with information on all phone calls in its networks, both within the US and between the US and foreign nations, on a "ongoing, daily basis."

4 Read about the Bleichenbacher, POODLE and DROWN attack on TLS. Describe them in a short, understandable way (1-2 paragraphs per attack). Are these attacks feasible with TLS 1.3? Why? Or why not?

4.1 Solving:

The Bleichenbacher attack explained: This attack is applicable when key-exchange take place using RSA algorithm and the padding used is PKCS1 v1.5.

Be aware that the client selects a random 48-bit number (padded according to the PKCS encoding technique to provide the same order of modulo n) during the creation of a TLS session with an RSA key exchange (2 bytes of the protocol version and 46 random bytes). The entire situation is then brought to public exponentiation. After decryption, the data is checked for alignment on the receiver side; if not, the packet is rejected. After decryption, the receiver checks to see if the plain text data begins with 0x00 02; if not, it is deleted. If 0x00 is not found, the receiver skips all further bytes.

Note that for public key operations, PKCS padded data must always start with 0x00 0x02. Furthermore, RSA is known to have homomorphic multiplication properties. In other words, if you multiply one ciphertext by another, decrypting the resulting value will give you something meaningful. Let's look at this with an example.

Suppose an attacker get the cipher text C which is essentially $[M^e \bmod n]$, attacker doesn't know about M (which is PKCS padded) but he know about public key (e, n) .

$C = M^e \bmod n$ Attacker then multiplies this cipher value with a chosen s . For all failure cases, server must respond something like 'Bad data'. Attacker keep changing value of s and wait until accepted by server.

$C' = C * s^e \bmod n$ which is essentially encryption of $(M * s)$. When server accept this C' that mean C' after decryption start with 0x00 0x02 and C' is a valid encryption for $M*s$ with PKCS padding.

$C' = M * s$ and hence $M = C' \div s$ or $M = C' s^{-1} \bmod n$

$B = 2^8(k-2)$. k is key size in bytes, like in RSA we say 2048 bit (256 bytes). Since first 2 bytes are 0x00 0x02, we are subtracting that. 2^8 is done to show the message in bit representation. When the message is accepted by server, that means.

$2B \leq ms \bmod n < 3B$

$2B$ means 0010k-2 bytes

$3B$ means 0010k-2 bytes

Since we know that if message is accepted first 2 bytes are 0x00 02 and hence the message $ms \bmod n$ is strictly less than when first 2 bytes are 0x00 03. And like that attacker further reduces the boundary by doing binary search until a single value is found.

The POODLE attack explained: The POODLE attack is possible due to several features of the SSL/TLS protocol. The POODLE vulnerability affects cipher suites that include symmetric encryption along with block ciphers such as the AES and DES algorithms. In such cases, the client and server first agree on a private key (private key and public key) that uses asymmetric encryption. All communication is symmetrically encrypted with this key. Block ciphers encrypt data in fixed-length blocks, such as 8 bytes or 16 bytes.

Cipher suites vulnerable to POODLE also use cipher block chaining (CBC mode). This means that each block's value depends on the previous block's value. It is calculated using the logical operation XOR. Also, a random block of data is added at the beginning. This is called

an initialization vector. This is necessary so that the data looks different each time it is encrypted.

1. The attacker tricks the victim's browser into running JavaScript code that lets the attacker perform the attack.
2. The attacker's JavaScript code tricks the user browser into sending multiple legitimate requests to the server. These requests include the session cookie.
3. The JavaScript code modifies the connection URL (adding extra characters) so that the length of the data sent to the server is a multiple of the block size (for example, 8). This means that the last block will contain only padding (see the explanation above).
4. The attacker knows which blocks of data contain the session cookie. For example, the data may have 10 blocks and the attacker knows that the third and fourth blocks contain the session cookie value.
5. The attacker copies the entire third block to the last block and sends it to the server many times, changing something in the connection URL every time so that the MAC is different.
6. After at most 256 times, the message will be accepted. This means that the last byte of the third block, after decryption, will be the number 07, which signifies correct padding.
7. Now the attacker knows the decrypted last byte and they can combine it with previous blocks using XOR operations to obtain the real last byte of the third block.
8. The attacker can then make the connection URL one byte longer and repeat the steps above to get the next piece of the cookie. And then repeat again for the fourth block of data.
9. If the cookie length is 16, the attacker will know the cookie after no more than 4096 requests, which takes at most a few minutes.

The DROWN attack explained: DROWN is a critical vulnerability affecting HTTPS and other services that rely on SSL and TLS, which are part of the cryptographic protocols essential to Internet security. These protocols allow anyone on the Internet to browse her web, use her e-mail, shop online, and send her instant messages without third parties reading the communications

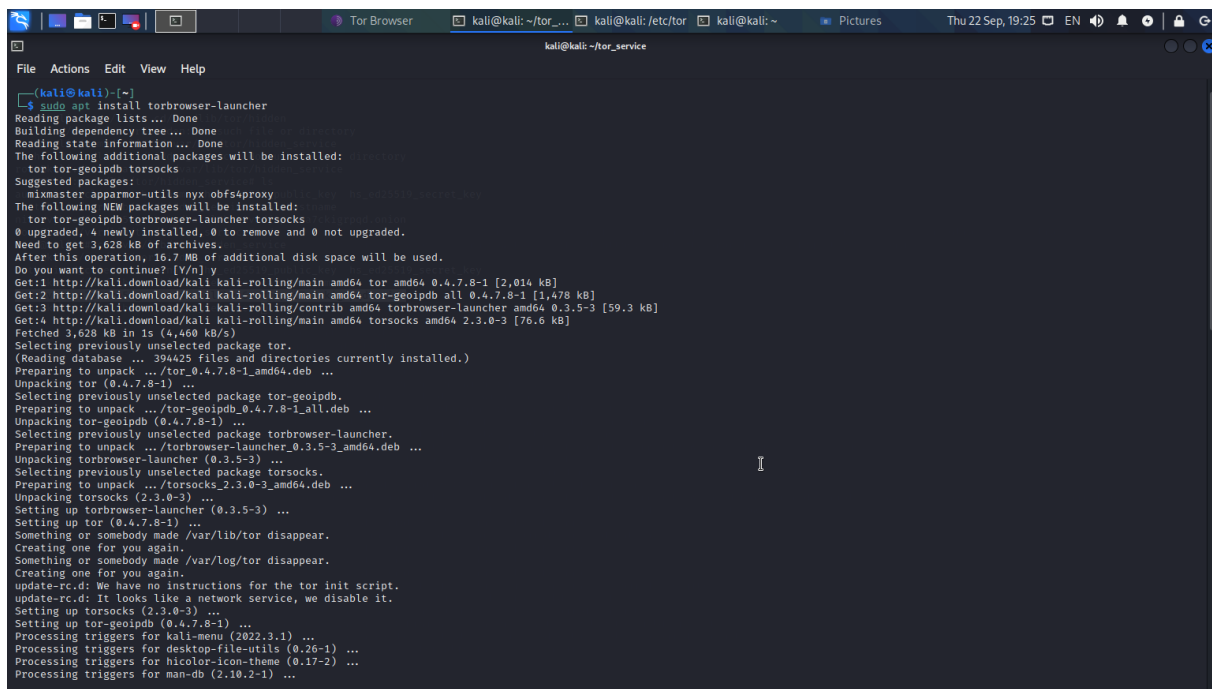
DROWN allows attackers to break encryption and read or steal sensitive communications such as passwords, credit card numbers, trade secrets and financial data. Measurements at the time of publication in March 2016 showed that 33% of all HTTPS servers were vulnerable to attacks. Fortunately, this vulnerability is not very common today. As of 2019, SSL Labs estimates that 1.2% of HTTPS servers are vulnerable.

This exploit involves a ciphertext attack using an SSLv2 server as a Bleichenbacher oracle. SSLv2 works by encrypting the main secret directly with RSA, and the 40-bit export cipher suite works by encrypting only his 40 bits of the main secret and exposing the remaining 88 bits as plaintext. Did. His SSLv3/TLS-encrypted RSA ciphertext of 48 bytes is "truncated" into 40-bit pieces and used in SSLv2 ClientMasterKey messages. This is treated by the server as her 40-bit fragment of her SSLv2 master secret. ServerVerify messages can be used as oracles using brute force 40-bit encryption.

TLS 1.3 improves on previous versions in several ways, most notably a faster TLS handshake and simpler, more secure cipher suites. Key exchanges with zero round-trip time (0-RTT) further simplify the TLS handshake. These changes, when combined, result in improved performance and increased security. TLS 1.3 requires AEAD bulk encryption rather than block mode ciphers, which have known flaws and vulnerabilities. So TLS 1.3 is immune to most of the known vulnerabilities.

5 Create an onion/hidden service with TOR and try to access it. (e.g.: Webpage with "Hello World"). Document what you did and the outcome. Which browser did you use to access it and why? Can you use any other browser?

5.1 Solving:



```

kali@kali: ~/tor_service
File Actions Edit View Help
(kali@kali)~$ sudo apt install torbrowser-launcher
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  tor tor-geoipdb torsocks
Suggested packages:
  minmaster apparmor-utils nix obfs4proxy
The following NEW packages will be installed:
  tor tor-geoipdb torbrowser-launcher torsocks
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 3,628 kB of archives.
After this operation, 16.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 tor amd64 0.4.7.8-1 [2,014 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 tor-geoipdb all 0.4.7.8-1 [1,478 kB]
Get:3 http://kali.download/kali kali-rolling/contrib amd64 torbrowser-launcher amd64 0.3.5-3 [59.3 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 torsocks amd64 2.3.0-3 [76.6 kB]
Fetched 3,628 kB in 1s (4,460 kB/s)
Selecting previously unselected package tor.
(Reading database ... 394425 files and directories currently installed.)
Preparing to unpack .../tor_0.4.7.8-1_amd64.deb ...
Unpacking tor (0.4.7.8-1) ...
Selecting previously unselected package tor-geoipdb.
Preparing to unpack .../tor-geoipdb_0.4.7.8-1_all.deb ...
Unpacking tor-geoipdb (0.4.7.8-1) ...
Selecting previously unselected package torbrowser-launcher.
Preparing to unpack .../torbrowser-launcher_0.3.5-3_amd64.deb ...
Unpacking torbrowser-launcher (0.3.5-3) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.3.0-3_amd64.deb ...
Unpacking torsocks (2.3.0-3) ...
Setting up torbrowser-launcher (0.3.5-3) ...
Setting up tor (0.4.7.8-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.3.0-3) ...
Setting up tor-geoipdb (0.4.7.8-1) ...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for ncolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.10.2-1) ...

```

First we install the tor browser.

Then we create a new directory named tor service. After that we call the python module http.server on localhost(127.0.0.1) with port 8080 with the following command in the tor service directory:

```

kali@kali: ~/tor_service
File Actions Edit View Help
Preparing to unpack .../tor-geoipdb_0.4.7.8-1_all.deb ...
Unpacking tor-geoipdb (0.4.7.8-1) ...
Selecting previously unselected package torbrowser-launcher.
Preparing to unpack .../torbrowser-launcher_0.3.5-3_amd64.deb ...
Unpacking torbrowser-launcher (0.3.5-3) ...
Selecting previously unselected package torsocks.
Preparing to unpack .../torsocks_2.3.0-3_amd64.deb ...
Unpacking torsocks (2.3.0-3) ...
Setting up torbrowser-launcher (0.3.5-3) ...
Setting up tor (0.4.7.8-1) ...
Something or somebody made /var/lib/tor disappear.
Creating one for you again.
Something or somebody made /var/log/tor disappear.
Creating one for you again.
update-rc.d: We have no instructions for the tor init script.
update-rc.d: It looks like a network service, we disable it.
Setting up torsocks (2.3.0-3) ...
Setting up tor-geoipdb (0.4.7.8-1) ...
Processing triggers for kali-menu (2022.3.1) ...
Processing triggers for desktop-file-utils (0.26-1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for mailcap (3.70+nmui) ...

(kali@kali)-[~]
└─$ mkdir tor_service

(kali@kali)-[~]
└─$ cd tor_service

(kali@kali)-[~/tor_service]
└─$ python3 -m https.server --bind 127.0.0.1 8080
/usr/bin/python3: Error while finding module specification for 'https.server' (ModuleNotFoundError: No module named 'https')

(kali@kali)-[~/tor_service]
└─$ python3 -m http.server --bind 127.0.0.1 8080
Serving HTTP on 127.0.0.1 port 8080 (http://127.0.0.1:8080/) ...

kill
stop
kill
^C
Keyboard interrupt received, exiting.

(kali@kali)-[~/tor_service]
└─$ python3 -m http.server --bind 127.0.0.1 8080
Serving HTTP on 127.0.0.1 port 8080 (http://127.0.0.1:8080/) ...

```

After the port is functional we create index.html file in the same directory. In the tor configuration directory using the path /etc/tor/ we uncomment the lines HiddenServiceDir and HiddenServicePort and also the port is changed to 8080. Tor service is started with the command `sudo tor`.

```

kali@kali: /etc/tor
File Actions Edit View Help
(kali@kali)-[~]
└─$ cd tor_service

(kali@kali)-[~/tor_service]
└─$ touch index.html

(kali@kali)-[~/tor_service]
└─$ ls
index.html

(kali@kali)-[~/tor_service]
└─$ nano index.html

(kali@kali)-[~/tor_service]
└─$ sudo apt install tor
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
tor is already the newest version (0.4.7.8-1).
tor set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

(kali@kali)-[~/tor_service]
└─$ whereis tor
tor: /usr/bin/tor /usr/sbin/tor /etc/tor /usr/share/tor /usr/share/man/man1/tor.1.gz

(kali@kali)-[~/tor_service]
└─$ cd /etc/tor

(kali@kali)-[/etc/tor]
└─$ ls
torrc  torsocks.conf

(kali@kali)-[/etc/tor]
└─$ sudo nano torrc

(kali@kali)-[/etc/tor]
└─$ sudo tor
Sep 22 18:08:43.826 [notice] Tor 0.4.7.8 running on Linux with Libevent 2.1.12-stable, OpenSSL 3.0.4, Zlib 1.2.11, Liblzma 5.2.5, Libzstd 1.5.2 and Glibc 2.33 as libc.
Sep 22 18:08:43.826 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://support.torproject.org/faq/staying-anonymous/
Sep 22 18:08:43.829 [notice] Read configuration file "/etc/tor/torrc".
Sep 22 18:08:43.829 [notice] Opening Socks listener on 127.0.0.1:9050
Sep 22 18:08:43.829 [notice] Opened Socks listener connection (ready) on 127.0.0.1:9050
Sep 22 18:08:43.800 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
Sep 22 18:08:43.800 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
Sep 22 18:08:43.800 [warn] You are running Tor as root. You don't need to, and you probably shouldn't.
Sep 22 18:08:43.800 [notice] Bootstrapped 0% (starting): Starting

```

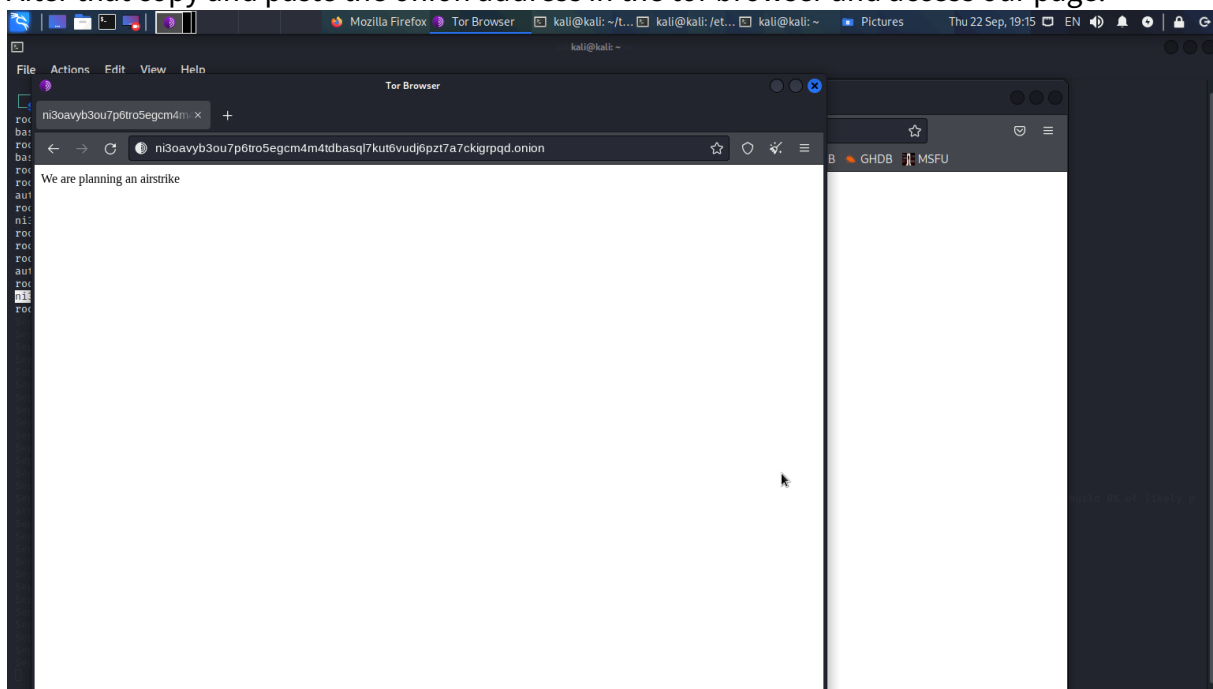
We use the **sudo su** command to find our onion address. Which is situated under the path /var/lib/tor/hidden service then access the file **hostname**


```

kali@kali:~$ sudo su
root@kali:/home/kali# cd /var/lib/tor/hidden
bash: cd /var/lib/tor/hidden: No such file or directory
root@kali:/home/kali# cd /var/lib/tor/hidden_service
bash: cd /var/lib/tor/hidden_service: No such file or directory
root@kali:/home/kali# cd /var/lib/tor/hidden_service
root@kali:/var/lib/tor/hidden_service# ls
authorized_clients  hostname  hs_ed25519_public_key  hs_ed25519_secret_key
root@kali:/var/lib/tor/hidden_service# cat hostname
ni3oavb3ou7p6tro5egcm4m4tdbasq17kut6vudj6pzt7a7ckigrpqd.onion
root@kali:/var/lib/tor/hidden_service# cd
root@kali:~$ cd /var/lib/tor/hidden_service
root@kali:/var/lib/tor/hidden_service# ls
authorized_clients  hostname  hs_ed25519_public_key  hs_ed25519_secret_key
root@kali:/var/lib/tor/hidden_service# cat hostname
ni3oavb3ou7p6tro5egcm4m4tdbasq17kut6vudj6pzt7a7ckigrpqd.onion
root@kali:/var/lib/tor/hidden_service#

```

After that copy and paste the onion address in the tor browser and access our page.



6 Shortly describe the differences between the various bridge types.

6.1 Solving:

Bridge relays are Tor relays that are not listed in the public Tor directory. This means that an ISP or government trying to block access to the Tor network cannot simply block all bridges. Bridges are useful for Tor users under oppressive regimes or those who need an extra layer of security for fear of someone detecting that they are connecting to a public Tor relay IP address. A bridge is just a normal relay with a slightly different configuration.

Because bridge addresses are not public, you will need to request them yourself. You have a few options:

- Visit <https://bridges.torproject.org/> and follow the instructions, or
- Email bridges@torproject.org from a Gmail, or Riseup email address
- Use Moat to fetch bridges from within Tor Browser.

Obfs4 and meek-azure are the most common used type of bridges, nowadays Snowflake bridges are becoming more popular.

7 Create an email address in the I2P network. Also create a PGP key pair and publish the correct part of it. Share the onion address with a partner (encrypted) and let him access it. Is it necessary to publish the key to multiple key server? Why (not)? Document your way of creating the email address, the key pair (where did you publish it), and the created emails, as well as the access of the partners browser.

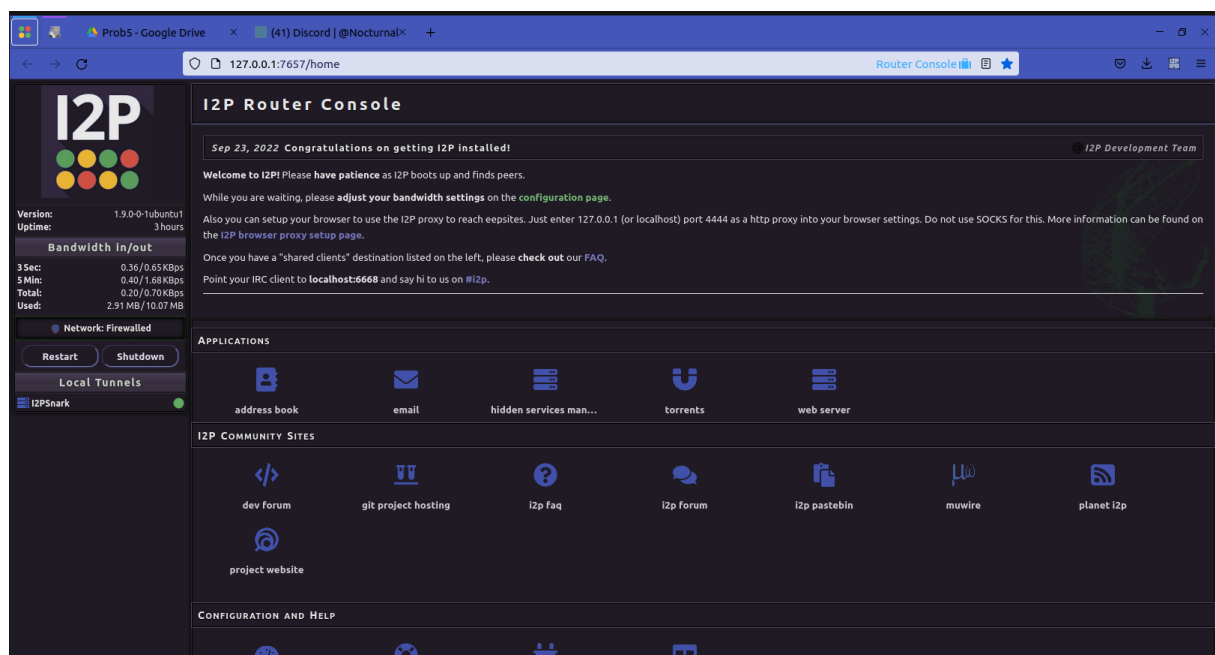
7.1 Solving:

First we install the I2P using two commands:

sudo apt-add-repository ppa:i2p-maintainers/i2p

sudo apt-get install i2p

We start the I2P using the command **i2prouter start**. After that we setup the browser using the add on I2P In Private Browsing. After that we access the URL **127.0.0.1:7657**. Finish the set-up then we click on the "Mail" section



PGP Key Pair

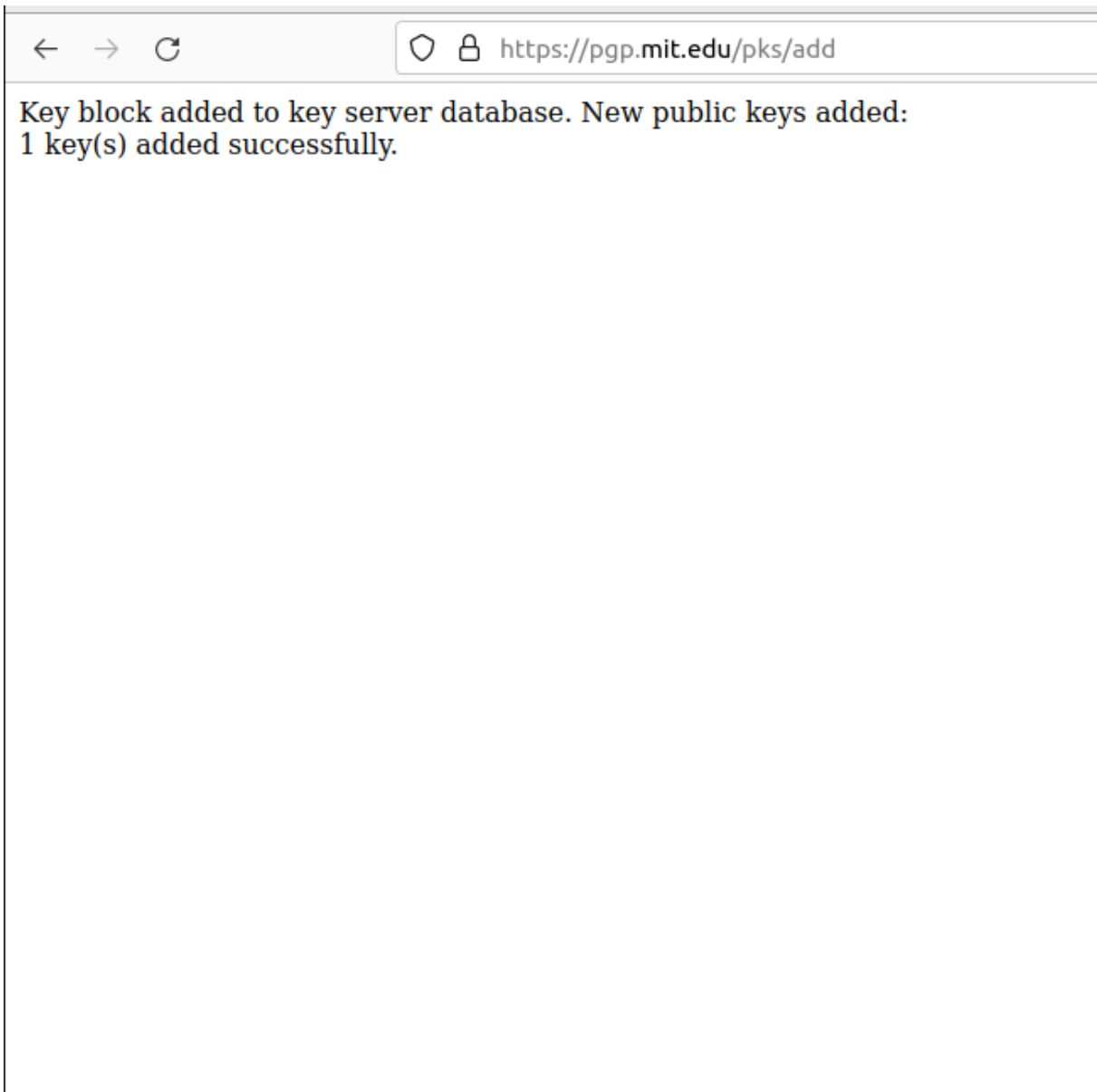
Create a PGP key pair using the command **gpg -gen-key**.

```
student@studend-server:~$ gpg -k
/home/student/.gnupg/pubring.kbx
-----
pub   rsa3072 2022-09-23 [SC] [expires: 2024-09-22]
       34AB167AB8B629379AB5B4171CA90BC0DC4FD1B2
uid           [ultimate] Flita Adrian <cr221504@fhstp.ac.at>
sub   rsa3072 2022-09-23 [E] [expires: 2024-09-22]
sub   rsa3072 2022-09-23 [E]
```

After that we export the key using the command **gpg -armor -output 'Flita Adrian'-pub-sub.asc -export 'Flita Adrian'**

- Upload the public key to MIT PGP Key Server

-



- Search and download colleague's public key.

- Import that public key to your machine with: **gpg --import marwin-pub.asc**

```
pub  rsa3072 2022-09-23 [SC] [expires: 2024-09-22]
     BA9516C50E13821108E506DCA9835C49BF863B32
uid          [ unknown] marwin <cr221525@fhstp.ac.at>
sub  rsa3072 2022-09-23 [E] [expires: 2024-09-22]
```

- Save your .onion address to a text file and encrypt it with your colleague's public key: **gpg --encrypt --sign --armor -r marwin onionaddress.txt**
- The resulting file is onionaddress.asc

Send this encrypted file via I2P mail to your colleague to decrypt and access the tor site from a tor enabled browser.

From: tiger6987 <tiger6987@mail.i2p>

To: moonlight6942@mail.i2p

Cc:

Bcc:

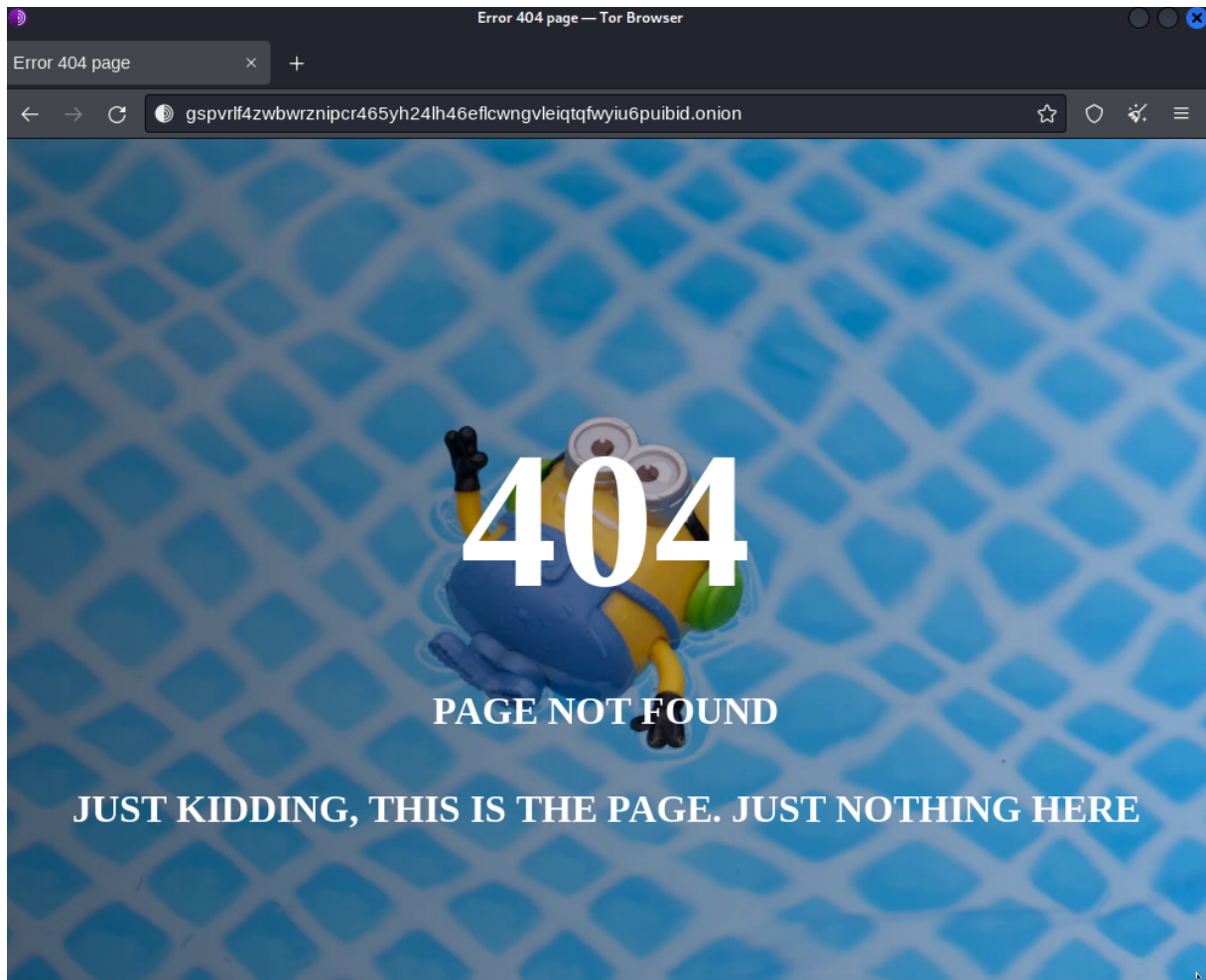
Subject:

Add Attachment: onion_adress.asc

You can also decrypt your colleague's key yo visit his tor address.

```
gpg --decrypt marwin_onion4adrian.txt.asc > marwinonion.txt
```

The result:

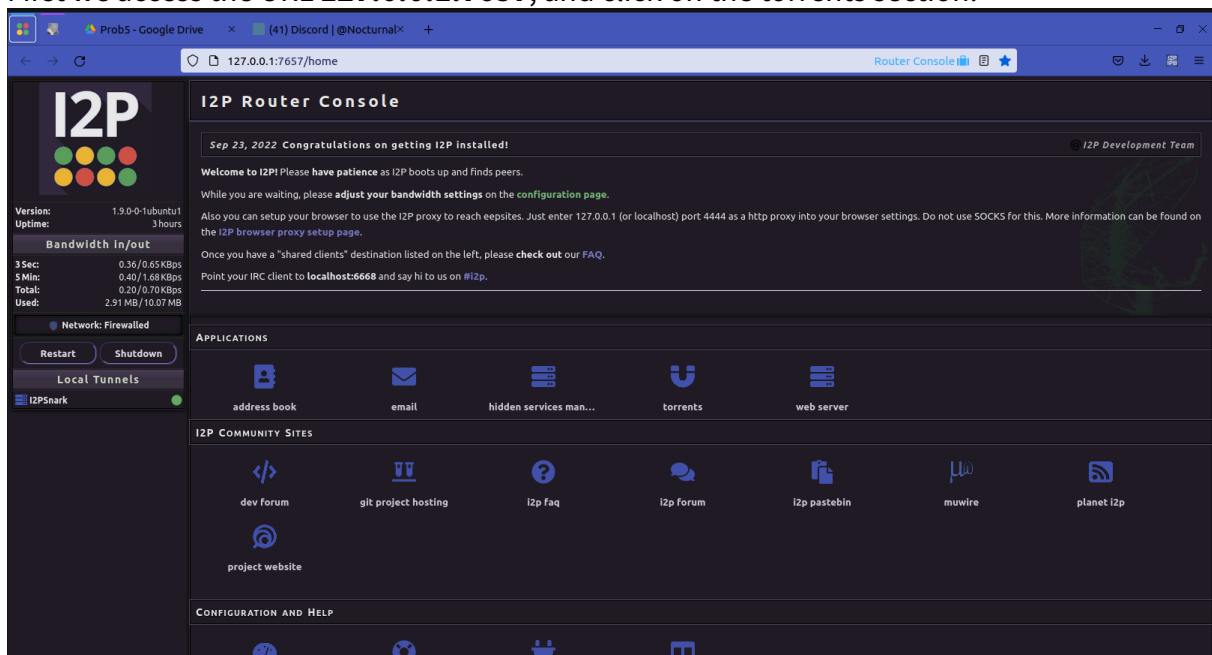


It is not necessary to publish your public key into multiple keyserver if the individual you are sending it to, knows on which server the keys can be found.

8 Create a torrent for the I2P network and send the address to a colleague. Are there any differences to clearnet torrents? Does torrenting over Tor work? Why (not)? Why may it still be a bad idea? What is the difference to the I2P network?

8.1 Solving:

First we access the URL **127.0.0.1:7657**, and click on the torrents section.



Torrents are uploaded to the built-in anonymous Bittorrent client I2PSNARK in the i2psnark subdirectory of the ip2 directory. Torrents are deleted when data is deleted from this directory. You start the torrent and then you share the magnet link with a colleague.

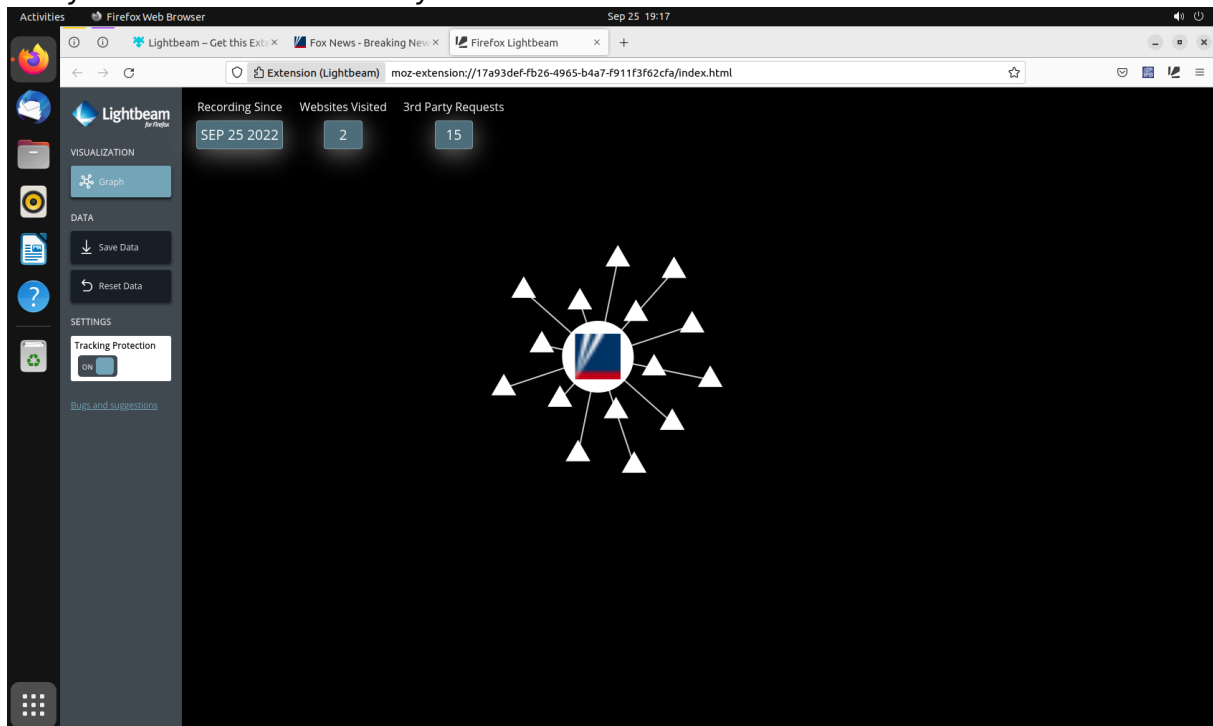
I2P networks are only available to users on the network. Other users cannot access it. Using clearnet torrent will show your IP address to all peers broadcasting the data you are streaming. A simple solution could be using a VPN SERVICE, but we do not have the certainty it is trustworthy.

Tor is used for anonymity and it could be slow when it comes to downloading content. Torrenting requires you to use your real IP address, and Tor doesn't support UDP connections, so you can't use Tor to remain anonymous.

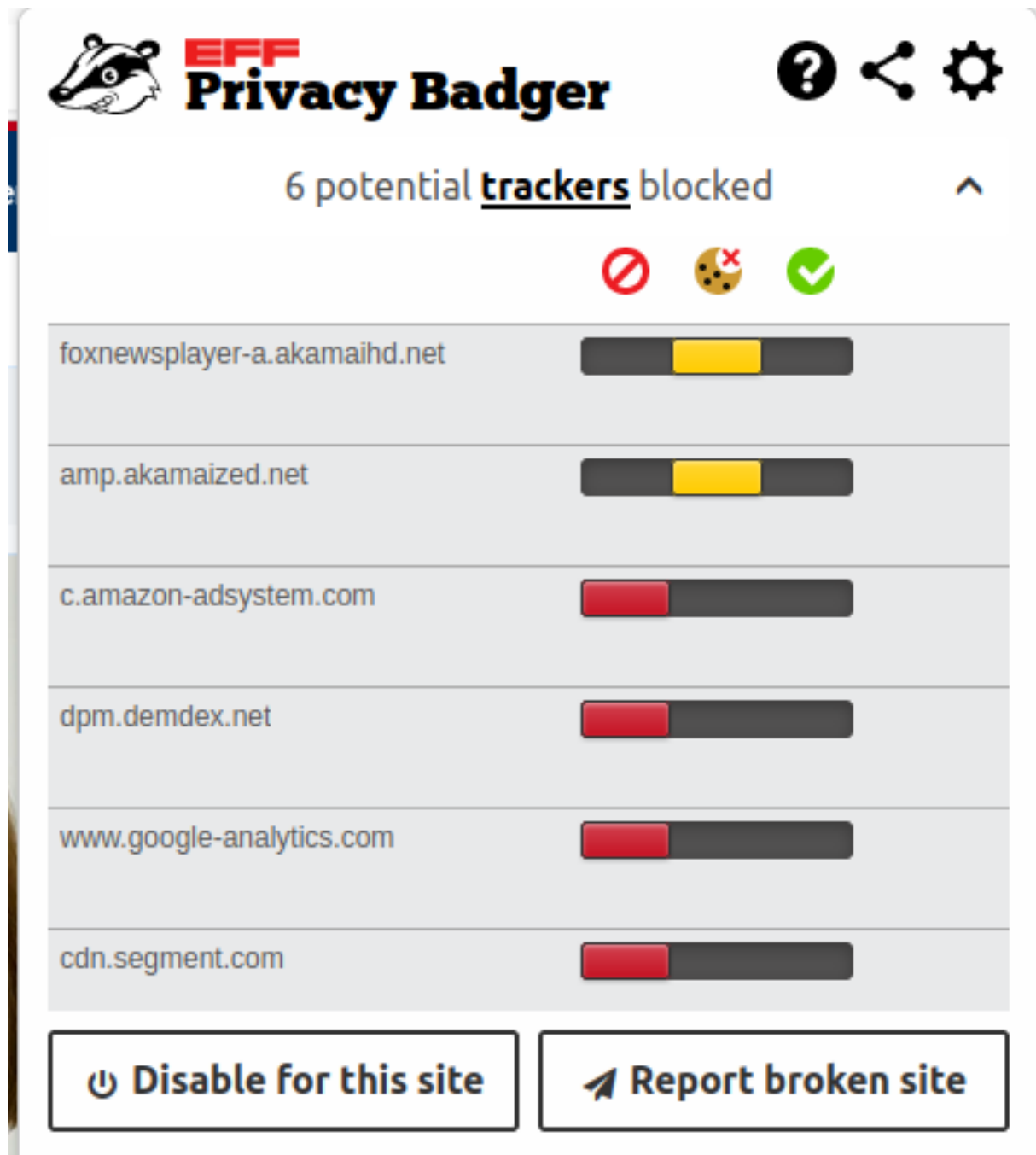
9 Install the add-on Lightbeam for Mozilla Firefox and visit your favorite news site. Document who is (visible) tracking your visit. Reset the data and additionally install the add-on privacy badger. Can you see a difference?

9.1 Solving:

After installing Lightbeam I visited Foxnews.com. With the help of this add on we can see how many trackers are active while you visit this website.



The second step is installing Privacy Badger and then resetting the data on Lightbeam. It is shown that the number of tracker is reduced.



The image shows the EFF Privacy Badger interface. At the top, the EFF Privacy Badger logo is displayed, along with icons for help, share, and settings. Below the logo, it states "6 potential trackers blocked". There are three status icons: a red circle with a slash, a cookie icon with a red 'x', and a green checkmark. A list of trackers is shown, each with a corresponding status bar. The trackers listed are foxnewsplayer-a.akamaihd.net, amp.akamaized.net, c.amazon-adsystem.com, dpm.demdex.net, www.google-analytics.com, and cdn.segment.com. The first two trackers have yellow status bars, while the others have red status bars. At the bottom, there are two buttons: "Disable for this site" and "Report broken site".

Tracker	Status
foxnewsplayer-a.akamaihd.net	Blocked (Yellow)
amp.akamaized.net	Blocked (Yellow)
c.amazon-adsystem.com	Blocked (Red)
dpm.demdex.net	Blocked (Red)
www.google-analytics.com	Blocked (Red)
cdn.segment.com	Blocked (Red)

[Disable for this site](#) [Report broken site](#)

