

## 1. Goal:

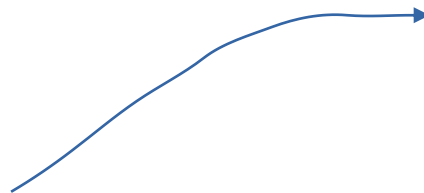
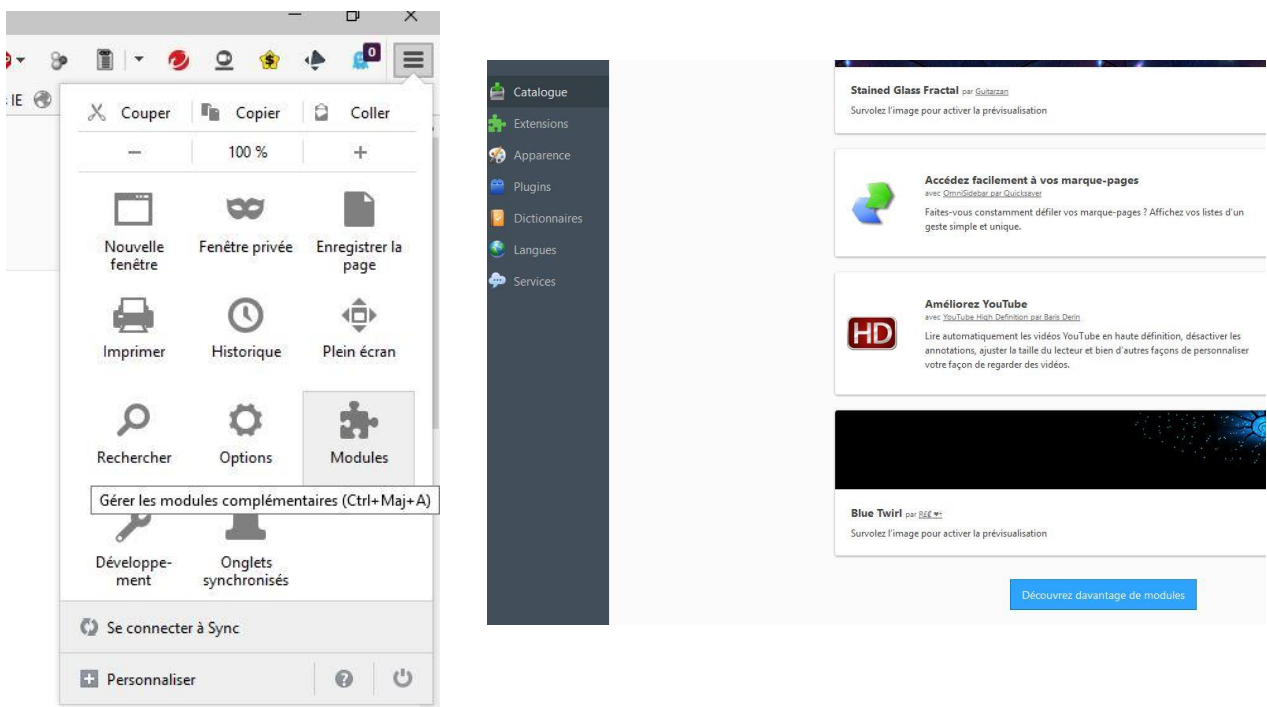
Through this labwork, you are going to find out how many third party sites are connected without your knowing. Where do they from, and their goals.

At the end of this job you will have to explain this Add-on module at your classmate.

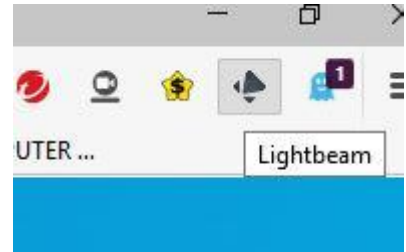
## 2. Labwork

### a) Set lightbeam Add on module

Go to Firefox web browser and choose “Modules” or go to Firefox browser and write lighthouse

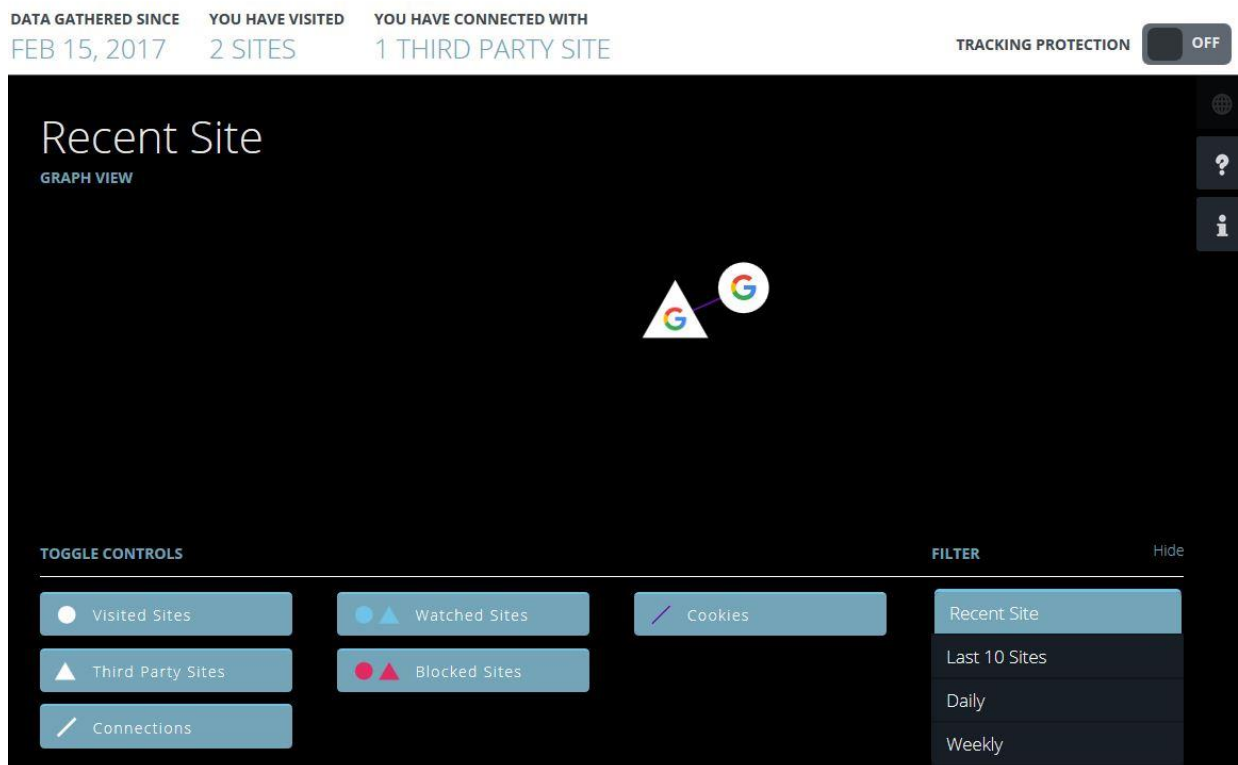


**Research** the “lightbeam” add-on module and set it.



## b) Discovery Lightbeam add-on module

So you can launch lightbeam add-on module by this icon



You would obtain this kind of graph because you use only Firefox web browser

**Find** what the circular node and triangular node signify.

**Click** on the circular node and find which country hosts this web site.

**Browse on these sites :**      **Example French site but you can choose Spanish or Italian sites.**

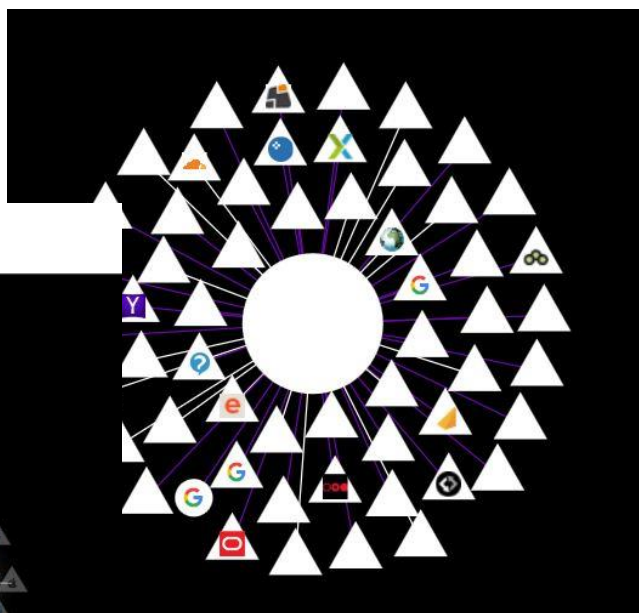
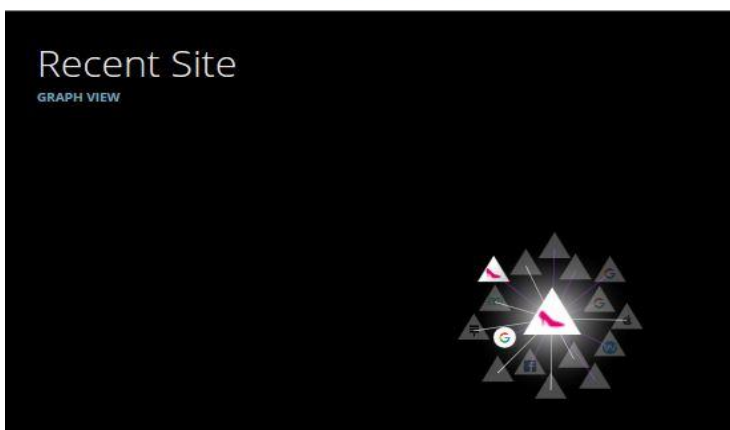
- ✓ <https://www.lequipe.fr/>
- ✓ <http://www.lemonde.fr/>
- ✓ <http://www.lepoint.fr>
- ✓ <https://www.tf1.fr/>
- ✓ <https://www.6play.fr/m6>
- ✓ <http://www.sarenza.com/>
- ✓ <https://www.zalando.fr>
- ✓ <http://www.lefigaro.fr/>
- ✓ <https://www.nouvelobs.com/>
- ✓ <https://www.ouest-france.fr/>

Brows on each site.

Come back to lightbeam Add-on Module.

Try to obtain 200 third sites

DATA GATHERED SINCE FEB 15, 2017    YOU HAVE VISITED 3 SITES    YOU HAVE CONNECTED WITH 33 THIRD PARTY SITES



Answer at these questions :

✓ How many third party sites are spying you?

✓ What does the triangle icon mean?

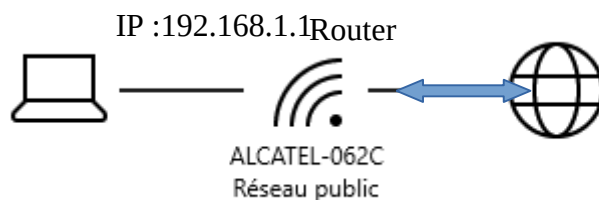
### c) Understanding the impact of the third-part site into the capacity of your computer

#### A What is my logical Address

When you are connected to internet by the means of your smartphone, computer, laptop, the local network identify your device by the mean of a logical address. This address is given automatically by your box or by a server, generally. When you make a request to browse on the net, your data have to past by a router. It has also a IP address. At home, it has often this following address 192.168.0.1. The router allows data to change network. When you are connected to the site you want, the site send data. Thus, some pictures appear on your screen for example. In this case, in the local aera network, the data go from the router to your device.

To resume

Wide  
Area  
Network



So go to the site <http://www.mon-ip.com/>

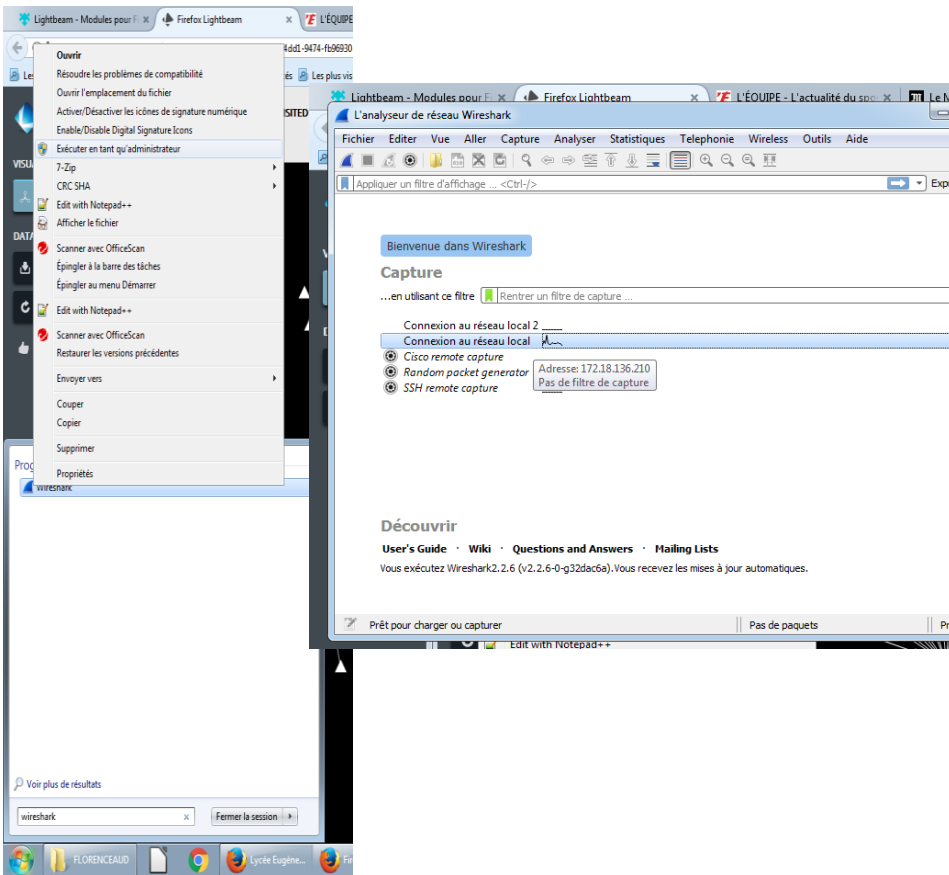
It will give you your local IP Address.

**d) Which IP Address communicates with me, what is its name and where is it ?**

**Open** Wire- Software [start Wire-shark software in administrator mode by the mean of right click ].

Choose network board "Connexion à un réseau local".

Go to capture tab if necessary



**Start** network analyse

Normally you will obtain this ki

The first line indicates the data go from my computer to the site I visit. The data transmitted are composed of 1301 packets. The second line indicates the answer of the site to my computer. 54 packets are send.

be afraid!

Microsoft Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1390..	3480.672429	35.158.224.78	192.168.1.175	TCP	1384	443 → 52899 [ACK] Seq=4097 Ack=518 Win=3999488 Len=1330 [TCP segment
1390..	3480.672432	35.158.224.78	192.168.1.175	TLSv1.2	1175	Certificate, Server Key Exchange, Server Hello Done
1390..	3480.672630	192.168.1.175	35.158.224.78	TCP	54	52899 → 443 [ACK] Seq=518 Ack=5548 Win=66304 Len=0
1390..	3480.676117	192.168.1.175	35.158.224.78	TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
1390..	3480.698144	192.168.1.175	35.158.224.78	TLSv1.2	1301	Application Data
1390..	3480.727198	35.158.224.78	192.168.1.175	TCP	54	443 → 52899 [ACK] Seq=6548 Ack=644 Win=3999488 Len=0
1390..	3480.735935	35.158.224.78	192.168.1.175	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
1390..	3480.747116	35.158.224.78	192.168.1.175	TCP	54	443 → 52899 [ACK] Seq=6599 Ack=1891 Win=3998464 Len=0
1390..	3480.796261	192.168.1.175	35.158.224.78	TCP	54	52899 → 443 [ACK] Seq=1891 Ack=6599 Win=66304 Len=0
1390..	3480.961216	35.158.224.78	192.168.1.175	TLSv1.2	353	Application Data

> Frame 1: 1167 bytes on wire (9336 bits), 1167 bytes captured (9336 bits) on interface 0  
 > Ethernet II, Src: LiteonTe\_f2:41:2e (74:e5:43:f2:41:2e), Dst: de:82:43:fe:45:c9 (de:82:43:fe:45:c9)  
 > Internet Protocol Version 4, Src: 192.168.1.175, Dst: 173.194.190.168  
 > Transmission Control Protocol, Src Port: 52270, Dst Port: 443, Seq: 1, Ack: 1, Len: 1113  
 > Secure Sockets Layer

```

0000 de 82 43 fe 45 c9 74 e5 43 f2 41 2e 08 00 45 00  ..C.E.t. C.A...E.
0010 04 81 43 0a 40 00 80 06 84 aa c0 a8 01 af ad c2  ..C@...
0020 be a8 cc 2e 01 bb 45 9d c6 d2 c3 d4 f7 eb 50 18  ....E.....P.
  
```

Now go to <https://www.ultratools.com/tools/ipWhoisLookupResult>

I enter this and I obtain plenty of informations ! So choose one address you have obtained by wireshark

Enter a host name or an IP address:



Related Tools: [DNS Traversal](#) [Traceroute](#) [Vector Trace](#) [Ping](#) [WHOIS Lookup](#)

```

Source: whois.arin.net
IP Address: 35.158.224.78
Name: AMAZO-ZFRA
Handle: NET-35-156-0-0-1
Registration Date: 26/09/16
Range: 35.156.0.0-35.159.255.255
Org: A100 ROW GmbH
Org Handle: RG-123
Address: Marcel-Breuer-Strasse 10
City: Munchen
State/Province:
Postal Code: 80807
Country: Germany
Name Servers:
  
```

Now after copy this address, go to IP Geo Location Lookup

Related Tools: [RFC Lookup](#) [Your Connection Speed](#)

Then go to this site : <https://www.coordonnees-gps.fr/>

Enter the latitude and the longitude. It is really incredible. Now you have the skills to identify a IP address.

DD (degrés décimaux)\*

Latitude:

Longitude:

DMS (degrés, minutes, secondes)\*

Latitude:  N  O  S 50 ° 6 ' 39.24 "

Longitude:  E  O 8 ° 40 ' 55.56 "

\* Système géodésique WGS 84

**e) Track the tracker !**

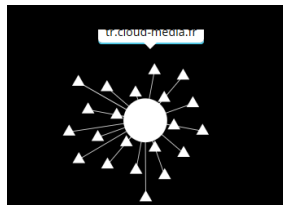
**Go back** to your browser and close all the internet pages or tab.

After **go back** to Lightbeam, **reset** data and **choose** only one site you like to go.

**Wait** few seconds to capture some third part sites.

**Go to** wireshark and restart current capture

**Choose** one third part site



Go to whireshark and find it string.

by writing just the beginning of the

Time	Source	Destination
93 2.844623	192.168.1.175	40.67.254.97
94 3.075322	18.195.27.2	192.168.1.175
95 3.123171	192.168.1.175	18.195.27.2
96 3.273328	192.168.1.175	18.195.27.2

If you want, you can localisable where comes it from

You can see on this example this site uses some data. These data use the media ( the mean to transmit the information) by busying 1464 digits ( 8 digits x 183 bytes : one byte = 8 digits).

So the drawbacks are :

- energy consumption.
- speed decline.
- spying .



f) Who are the snitch and how to do to block third party sites

Now, you are going to discovery the different kinds of snitch and how to do to block them thanks to an another Firefox module. This module is called Goshtery.



So **Set** Goshtery module as you have done with lightbeam module.

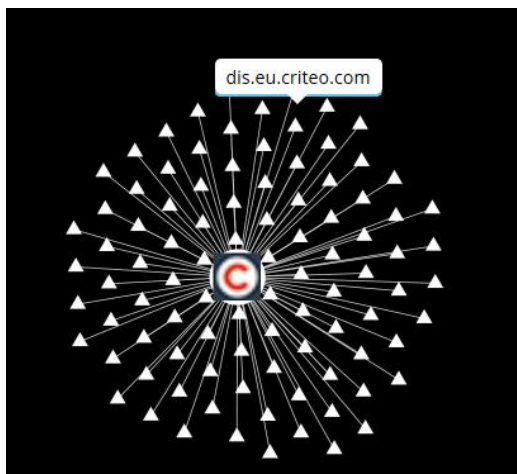
**List** the 8 different types of snitch after you click on “parameter”.

**Go** now to extension management and **disable** this module for the moment

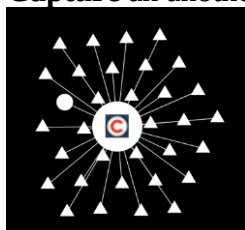
**Go** to Ligtbeam, **reset** and **choose** to browse one site you like to go.

**Capture** thanks to snipping tool for example the graph

DATA GATHERED SINCE	YOU HAVE VISITED	YOU HAVE CONNECTED WITH
JAN 09 2019	1 SITES	96 THIRD PARTY SITES



**Enable** Gohsthery, **reset** Lightbeam **wait** few minutes but **don't forget** to browse on your site. **Capture** an another picture.



JAN 09 2019	2 SITES	32 THIRD PARTY SITES
-------------	---------	----------------------

**g) Your Job :**

Now you have to prepare a presentation to explain what have you got found out thanks to this labworks.