





# 1. <u>Goal:</u>

Throught 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 ligthbeam



Digital identity : Lightbeam Add-on Module



4







### **Resarch** 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

data gathered since FEB 15, 2017	2 SITES	1 THIRD PARTY SITE		TRACKING PROTECTIO	N OFF
Docont	Cito				
GRAPH VIEW	Sile				?
					i
			GGG		
TOGGLE CONTROLS				FILTER	Hide
O Visited Sites		• 🔺 Watched Sites	/ Cookies	Recent Site	
🔺 Third Party S	lites	Blocked Sites		Last 10 Sites	
/ Connections				Daily	
				Weekly	

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

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

**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.

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



Brows on each site.

**Come back** to lightbeam Add-on Module.

#### Try to obtain 200 third sites



✓ How many third party sites are spying you?

#### 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

34

IP:192.168.1.1Router Wide Area ALCATEL-062C Network Réseau public

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

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

computer to the site I visit. The data transmitted are composed of 1301 packets. The second line indicates the answer of the site to	Normally you will obtain this ki	The first line indicates the data go from my	be afraid!
are composed of 1301 packets. The second line indicates the answer of the site to		computer to the site I visit. The data transmitted	
The second line indicates the answer of the site to		are composed of 1301 packets.	
man computer 54 poplets are cond		The second line indicates the answer of the site to	
my computer. 54 backets are send.		mv computer. 54 packets are send.	



	*Micros	oft: Wi-Fi											
Eil	e <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> a	apture <u>A</u> nalyze <u>S</u> tatistics	s Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> e	elp							
		🛞 📙 🚠 🗙	। 😋 । ९ 👄 🔿 🕾 👔	୍ 🖟 📃 🔳 🔍 ପ୍ ସ୍									
	R Kpply a display filter <ctrl-></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						
	1300	3400.672539	102.160.1.175	35.150.224.70	TCP	54	52000 -> 443 [ACK] Seq-510 Ack-6540 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						
	1200	2404 046045	400 400 4 475	25 450 004 70	700								
>	Frame	1: 1167 bytes	on wire (9336 bits),	1167 bytes captured (	9336 bit	s) on	interface 0						
>	Ethern	et II, Src: Li	iteonTe_f2:41:2e (74:e	e5:43:f2:41:2e), Dst:	de:82:43	:fe:45	i:c9 (de:82:43:fe:45:c9)						
>	Intern	et Protocol Ve	ersion 4, Src: 192.168	8.1.175, Dst: 173.194.	190.168								
>	Transm	ission Control	l Protocol, Src Port:	52270, Dst Port: 443,	Seq: 1,	Ack:	1, Len: 1113						
>	Secure	Sockets Laver	•										

0000	de	82	43	fe	45	<b>c</b> 9	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	с2	···C·@····
0020	be	a8	сс	2e	01	bb	45	9d	<b>c6</b>	d2	с3	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:

35.158.224.78 Go »

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 adress, go to IP Geo Location Lookup

CIDR/Netmask	Enter an IPv4 Address:	
What's your IP	35.158.224.78	Go »
IP Geo-location Lookup		
IPWHOIS Lookup	Related Tools: RFC Lookup Your Connection Speed	

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



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

DD (degré	s décima	*(xL			Udstein Latitude : 50.1109   Longitude : 8.6821	457 Gelphau
Latitude	50.1109				Obtenir l'altitude	genselbold Linsen
					275 Niedernhausen	
Longitude	8.6821				tein NAUROD Eschborn Maintal 65	Freigericht
					417 54 Francfort	
	Obtenir	'adre	sse		Wiesbaden am Taunus go Main Gase Main	Alzenau Kroi
DMS (deg	rés, minut	es,	secor	ndes)*	EUGIAREN Neu-Isenburg Seligenstadt	
Latitude	●NOS	50	° 6	' 39.24	455 Hochheim 43 am Main 50 Dietzenbach 90 April 10 April	Kleinostheim
					Mayence Rüsselsheim 486 Langen 486	Aschaf ' ur
Longitude	● E ○ 0	8	° 40	' 55.56	 Babenhausen	+
	-		-		9 Nauheim 3	
	Obtenir	adre	sse		Gross-Gerau	1-7 I - P

#### e) <u>Track the tracker !</u>

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.

					Lone	1.00	· <u> </u>		conc	<u>A</u> nonyze	<u>o</u> cocia		receptiony
Wait few	seconds to	capture so	ome thi	ird part	- 6	) 💿	010	$\mathbf{X}$	G	₹ 🗢	⇒ 😤	Ŷ	<u>&amp;</u> <u>=</u>   ≡
sites.			pply a display filter <ctrl-></ctrl->										
			Time		0	ource			Destination				
a									ource		_		
Go to wire	eshark and i	restart cur	rent cap	oture	93	2.84	4623	1	92.16	8.1.1/	5		40.67.254.9.
					94	3.07	5322	1	8.195	.27.2			192.168.1.17
	.1 . 1	,				3.12	3171	1	92.16	8.1.17	5		18.195.27.2
Choose on	ie third par	t site		tr.cloud-media.tr									454 404 400
Go to whi	reshark and	d find it				by	writing	g jus	st the	begir	ning (	of 1	the
						2	C			U	U		
string.													
( 🔳 🧟 💿 📄 🗅	रे 🖸 🔍 🗢 🗢 🖽 🕇	🔁 🔄 🖬 🔍 Q	€, Ⅲ										
Apply a display filter <ct< th=""><th>rl-/&gt;</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>• Expr</th></ct<>	rl-/>												• Expr
Packet list 🔹	Narrow & Wide 🔻	Case sensitive	String	tr.clou							→ [	Find	
o. Time	Source	Destination	col Len	gt. Info									
53451 746.992115	192.168.1.1	192.168.1.175	DNS	97 Standard quer	y response	0x1bcf A e	ngage.commander	r1.com A	95.131.143.	. 205			
53452 746.992117	35 227 210 77	192.100.1.175		219 Standard quer	VCK1 Seg=49	0X4801 A C	ag.analytics-co	32 Len-0	COM CNAME 6	events.mediar	ithmics.com t	INAME I	D.medi
53454 746,992305	192.168.1.175	35,227,210,77	TCP	54 54208 + 443	ACK] Seg=96	18 Ack=490	4909 Win=417280	0   en=0					
53455 746.994076	192.168.1.175	192.168.1.1	DNS	80 Standard quer	v 0x42e8 A	lb.mediari	thmics.com						
53456 746.994076	192.168.1.175	192.168.1.1	DNS	81 Standard quer	y 0x52b8 A	engage.com	mander1.com						
53457 747.001946	192.168.1.175	63.140.40.110	TCP	54 54292 → 443 [	ACK] Seq=32	33 Ack=407	2 Win=65536 Len	n=0					
53458 747.002486	192.168.1.1	192.168.1.175	DNS 1	160 Standard quer	y response	0x42e8	h_mediarithmics	s.com A 3	7,187.175.4	46 A 149.202.	194.227 A 145	5.239.1	45.132
53459 747.002487	192.168.1.1	192.168.1.175	DNS 1	183 Standard quer	y response	0x63d8 A t	r.cloud-media.f	fr CNAME	er.cloud-me	edia.fr CNAME	front-383813	3087.eu	-west-
53460 747.011692	104.75.225.129	192.168.1.175	HTTP	500 HTTP/1.1 200	OK (text/h	tml) 🖵							
Frame 53459: 183 by	tes on wire (1464 bit	s), 183 bytes captu	red (1464 bits	) on interface 0									

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** Gosthery 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





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



**Page 9 sur 10** 



## g) Your Job :

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

