

Network Game 2.0

Server edition

Hack4Kids@Deloitte





Outline/Plan/Agenda

- Basic
 - Network
 - IP address
 - IP packet
 - DNS
 - Ping Command
 - http/https
- Advanced
 - SERVER GAME

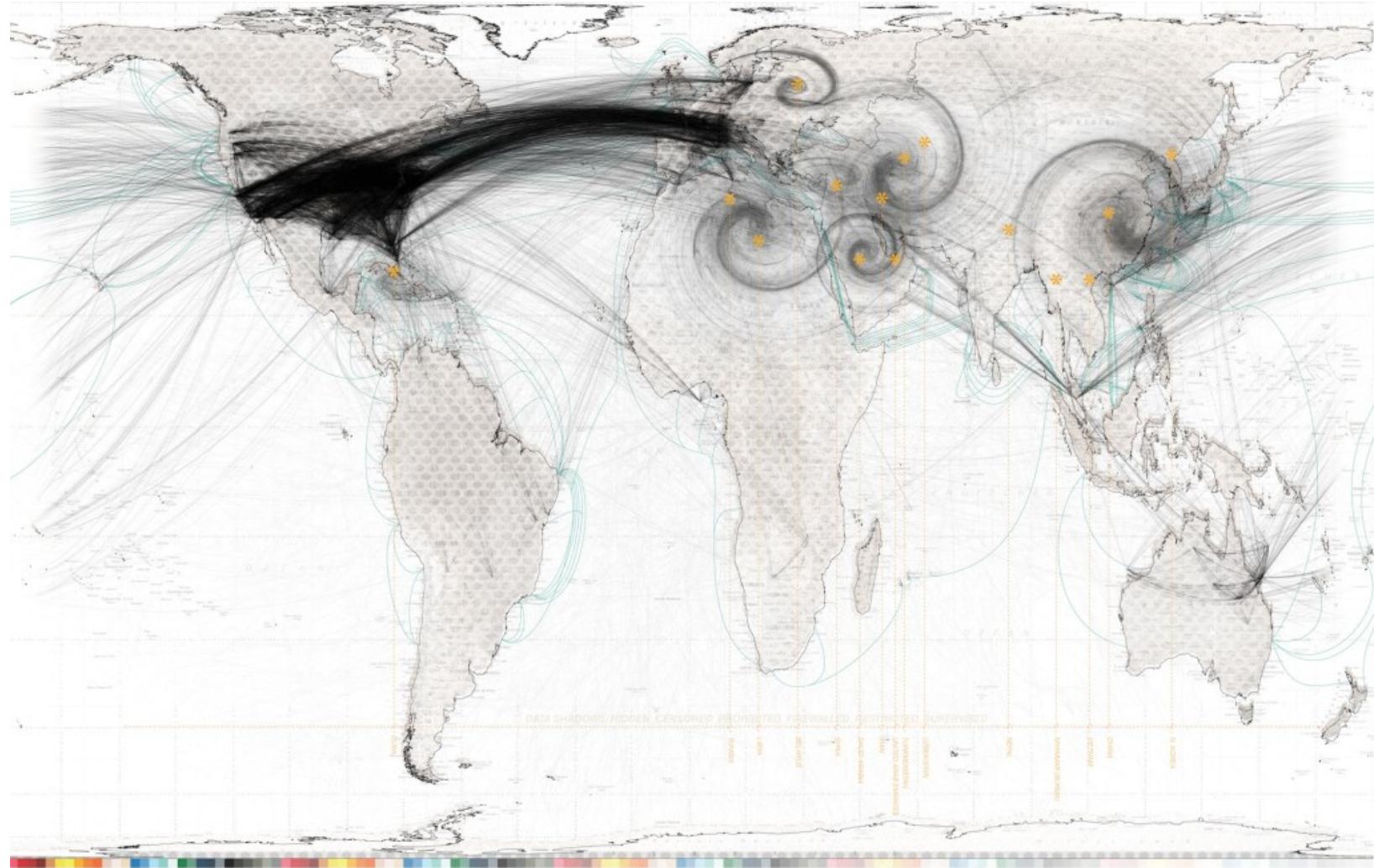


Network/ Réseau/ Netzwerk



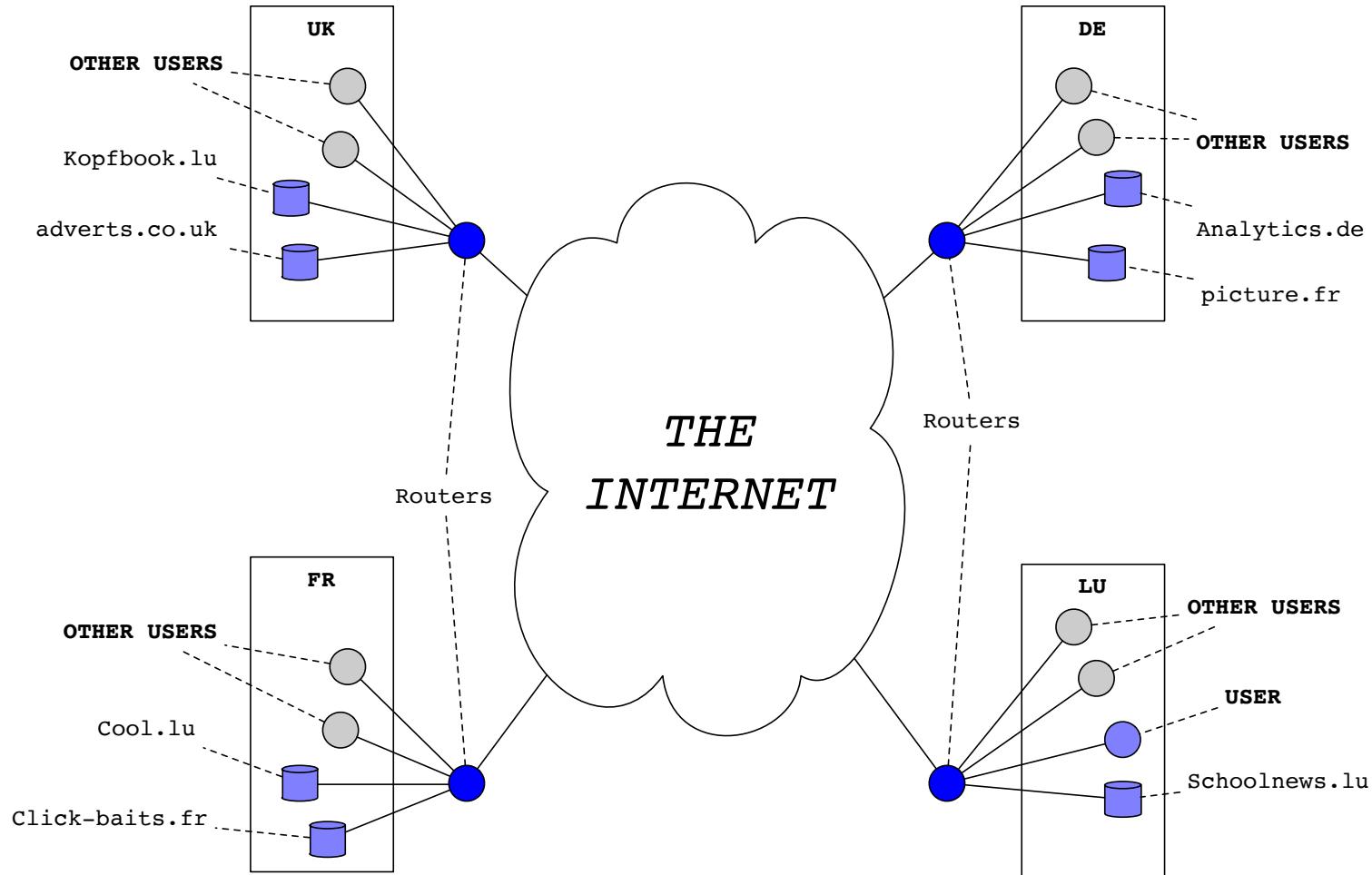


Network/Réseau/Netzwerk



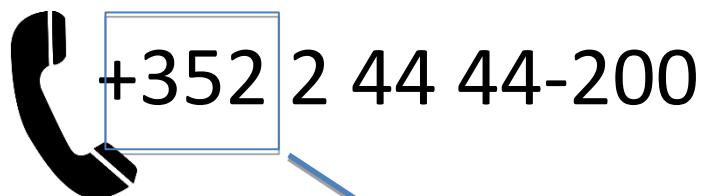


Network/Réseau/Netzwerk

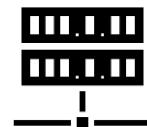




IP address/ Adresse IP/ IP-Adresse



Luxembourg



XXX.XXX.XXX.XXX



IP packet/ Paquet IP/ IP-Paket

Source (From)

Destination (To)



*Time
Protocol
Length*

*Meta Data
Metadonnées
Metadaten*
+ Content



IP packet/ Paquet IP/ IP-Paket

Advanced Network Game – © Securitymadein.lu – M. Farcot – Licensed Under CC BY SA 4.0

Capturing from en0 [Wireshark 1.8.5 (SVN Rev 47350 from /trunk-1.8)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
153	25.002462000	10.9.0.201	10.9.0.255	DB-LSP-DI	175	Dropbox LAN sync Discovery Protocol
154	25.279451000	10.9.0.23	10.9.0.255	NBNS	92	Name query NB SOFTPEDIA-KE<lc>
155	25.453558000	AsustekC_95:34:b5	Broadcast	ARP	64	Who has 10.9.0.1? Tell 10.9.0.2 [ETHERNET FRAME CHECK S
156	25.491924000	10.9.0.41	239.255.255.250	SSDP	165	M-SEARCH * HTTP/1.1
157	26.026587000	10.9.0.23	10.9.0.255	NBNS	92	Name query NB SOFTPEDIA-KE<lc>
158	26.048341000	10.9.0.48	10.9.0.255	NBNS	110	Registration NB SOFTPEDIA-PC<00>
159	26.048602000	Dell_Oc:74:ad	Broadcast	ARP	60	Who has 10.9.0.48? Tell 10.9.0.92
160	26.280066000	Dell_Oc:ff:83	Broadcast	ARP	60	Who has 10.9.0.1? Tell 10.9.0.31
161	26.471554000	10.9.0.26	10.9.0.255	SMB Mails	321	Write Mail Slot
162	26.472024000	10.9.0.26	10.9.0.255	SMB Mails	390	Write Mail Slot
163	26.535934000	10.9.0.31	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1
164	26.778531000	10.9.0.23	10.9.0.255	NBNS	92	Name query NB SOFTPEDIA-KE<lc>
165	26.811758000	10.9.0.31	10.9.0.255	UDP	82	Source port: 64695 Destination port: sentinelrsm

Frame 157: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface 0

Ethernet II, Src: Dell_81:87:48 (00:18:8b:81:87:48), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)
Address: Broadcast (ff:ff:ff:ff:ff:ff)
.... .1 = LG bit: Locally administered address (this is NOT the factory default)
.... .1 = IG bit: Group address (multicast/broadcast)

Source: Dell_81:87:48 (00:18:8b:81:87:48)
Address: Dell_81:87:48 (00:18:8b:81:87:48)
.... ..0 = LG bit: Globally unique address (factory default)
.... ..0 = IG bit: Individual address (unicast)

Type: IP (0x0800)

Internet Protocol Version 4, Src: 10.9.0.23 (10.9.0.23), Dst: 10.9.0.255 (10.9.0.255)

User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (137)

Source port: netbios-ns (137)
Destination port: netbios-ns (137)
Length: 58

Checksum: 0xbce [validation disabled]

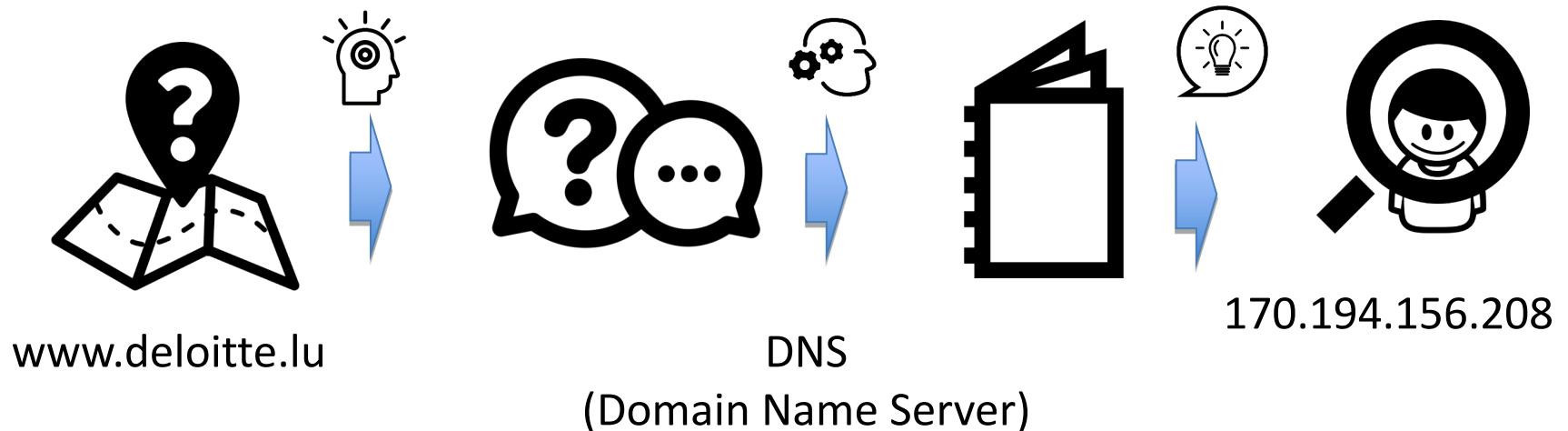
NetBIOS Name Service

0000 ff ff ff ff ff 00 18 8b 81 87 48 08 00 45 00H..E.
0010 00 4e 05 47 00 00 80 11 20 31 0a 09 00 17 0a 09 .N.G.... 1.....
0020 00 ff 00 89 00 89 00 3a bc 8e 9f 33 01 10 00 01: ...3....
0030 00 00 00 00 00 20 46 44 45 50 45 47 46 45 46 F DEPEGFEF
0040 41 45 46 45 45 44 42 43 4e 45 4c 45 46 43 AEFEJE BCNLEFC
0050 41 43 41 43 41 42 4d 00 00 20 00 01 ACACABM. . .

en0: <live capture in progress...> | Packets: 201 Displayed: 201 Marked: 0 | Profile: Default



DNS = Domain Name Server





DNS = Domain Name Server

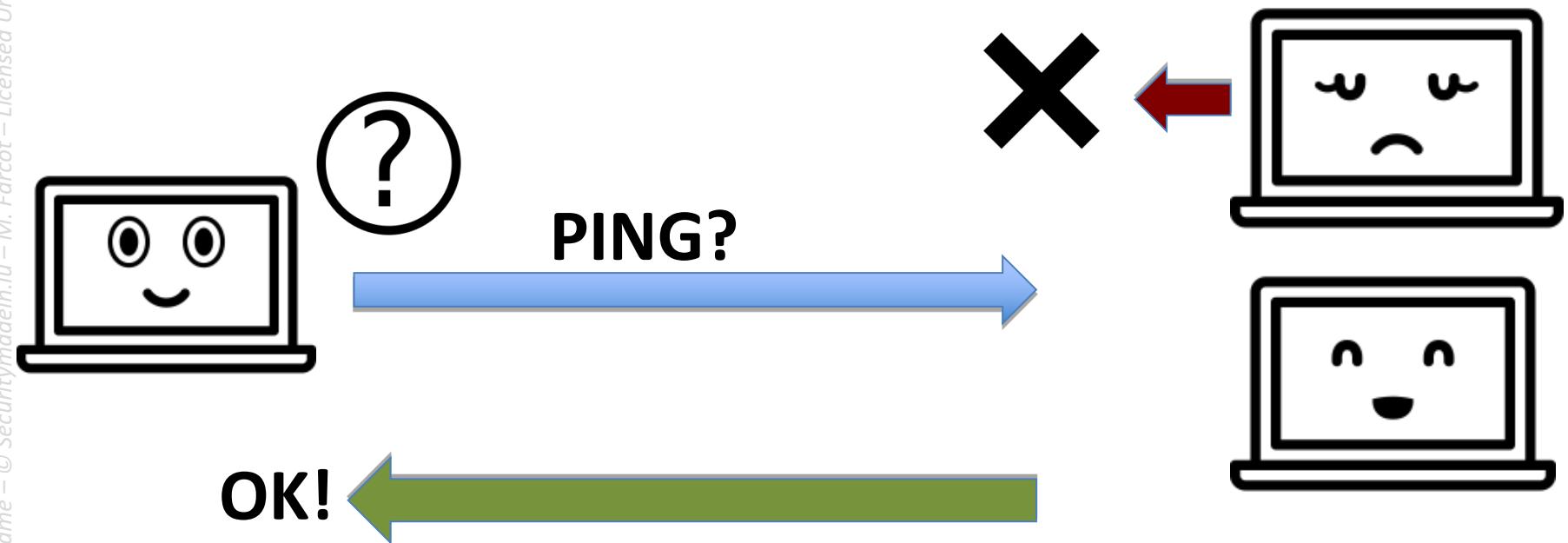
```
matthieu — -bash — 79x24
/Users/matthieu — -bash
[MacBook-Pro-de-Matthieu:~ matthieu$ nslookup www.deloitte.lu
Server:      10.8.0.2
Address:     10.8.0.2#53

Non-authoritative answer:
Name:   www.deloitte.lu
Address: 170.194.156.208

MacBook-Pro-de-Matthieu:~ matthieu$ ]
```



Ping Game/ Jeu du Ping/ Ping-Spiel





Ping Game/ Jeu du Ping/ Ping-Spiel

```
matthieu — -bash — 79x24
? matthieu — -bash
+/Users/matthieu — -bash +]

[MacBook-Pro-de-Matthieu:~ matthieu$ ping www.deloitte.lu
PING www.deloitte.lu (170.194.156.208): 56 data bytes
64 bytes from 170.194.156.208: icmp_seq=0 ttl=240 time=106.167 ms
64 bytes from 170.194.156.208: icmp_seq=1 ttl=240 time=105.828 ms
64 bytes from 170.194.156.208: icmp_seq=2 ttl=240 time=107.041 ms
64 bytes from 170.194.156.208: icmp_seq=3 ttl=240 time=106.274 ms
^C
--- www.deloitte.lu ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 105.828/106.328/107.041/0.444 ms
MacBook-Pro-de-Matthieu:~ matthieu$ ]
```

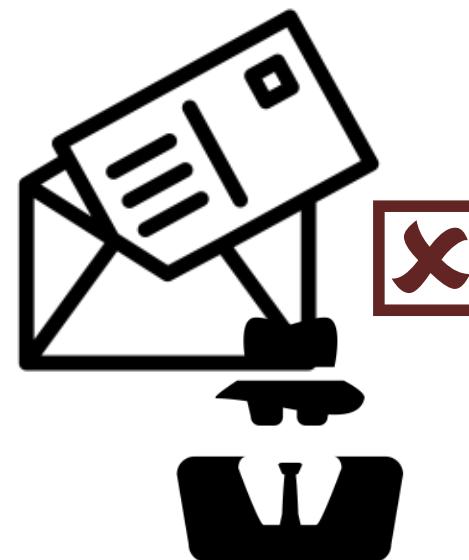
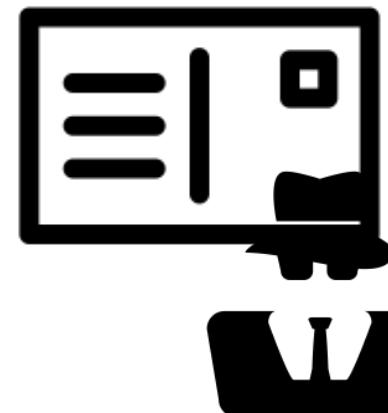
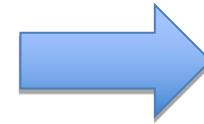
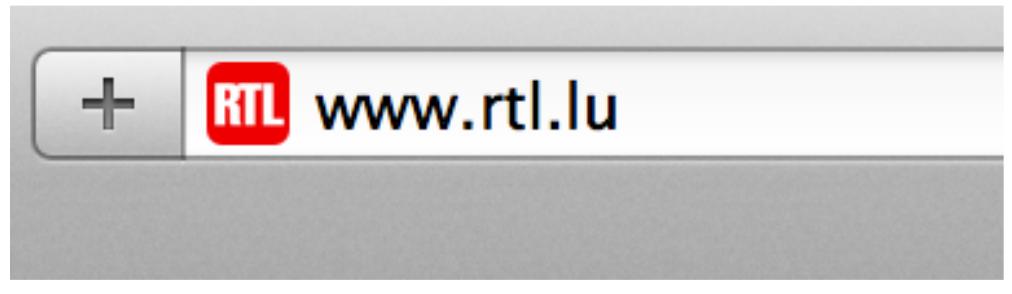


HTTP/HTTPS





HTTP/HTTPS



Server Game / Jeu du serveur/ Server Spiel



TheSchoolNews.lu
A Publication of Hack4kids
For H4K Event

Wow!
A major Headline!

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam.

Nemo enim ipsum voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt.

Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consecetur, adipisci velit, sed quia non numquam eius modi tempora incident ut labore et dolore magnam aliquam quaerat voluptatem.

Ut enim ad minima veniam, quis nostrum exercitationem ullam

Big story headline goes here!
by Hack4Kids!

Nemo enim ipsum voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt.

Quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur.

Adverts.co.uk/Script4
Advertisement for you

Tracking and profiling Scripts

Analytics.de/Script1

Cool Video! Check it out!
Just wow. Click me.

KopfBook.lu/User22

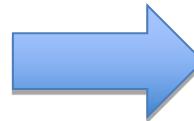
Cool.lu/video.mp4

Picture .fr/School_1.png
Photo of the Big Story!

Click-baits.fr/Script3

Complementary stories

Load the page



TheSchoolNews.lu
A Publication of Hack4kids
For H4K Event

Wow!
A major Headline!

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam.

Nemo enim ipsum voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt.

Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consecetur, adipisci velit, sed quia non numquam eius modi tempora incident ut labore et dolore magnam aliquam quaerat voluptatem.

Ut enim ad minima veniam, quis nostrum exercitationem ullam

Big story headline goes here!
by Hack4Kids!

Nemo enim ipsum voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt.

Quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur.

APPLE KIDS
COMIC BOOKS INC.
www.applekids.com

Advertisement for you

Tracking and profiling Scripts

SCANDAL AT THE SCHOOL... CLICK HERE FOR MORE INFORMATION

Sponsored content

Complementary stories

Log-in and react with KopfBook

Cool Video! Check it out!
Just wow. Click me.

KopfBook

Server Game / Jeu du serveur/ Server Spiel

