Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

XMAS Lecture (NetSec)

IN2101 – WS 16/17

Cornelius Diekmann

Version: December 20, 2016

Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Chapter 43: Network Security vs. Network Privacy?

Network Security – Security

- So far, when we discussed security, we considered

  What were the 6 security goals again?

Network Security – Security

- So far, when we discussed security, we considered
  - Data Integrity
  - Confidentiality
  - Availability
  - Authenticity
  - Accountability
  - Controlled Access

Network Security – Security

- We learned about several technical security measures.
- For example
  - IPsec ESP (Secure Channel)
    - Confidentiality
    - Integrity
    - Authenticity
  - Certificates and Signatures
    - Authenticity
    - Accountability
  - Firewalls
    - Controlled Access
  - TCP SYN Cookies
    - Availability
  - ...

Network Security – Security

- So far, we are
  - encrypting
  - integrity protecting
  - authenticating
  - ensuring availability
  - controlling access
- Is this enough?

Network Security – Security

- So far, we are
  - encrypting
  - integrity protecting
  - authenticating
  - ensuring availability
  - controlling access
- Is this enough?
- What about privacy?

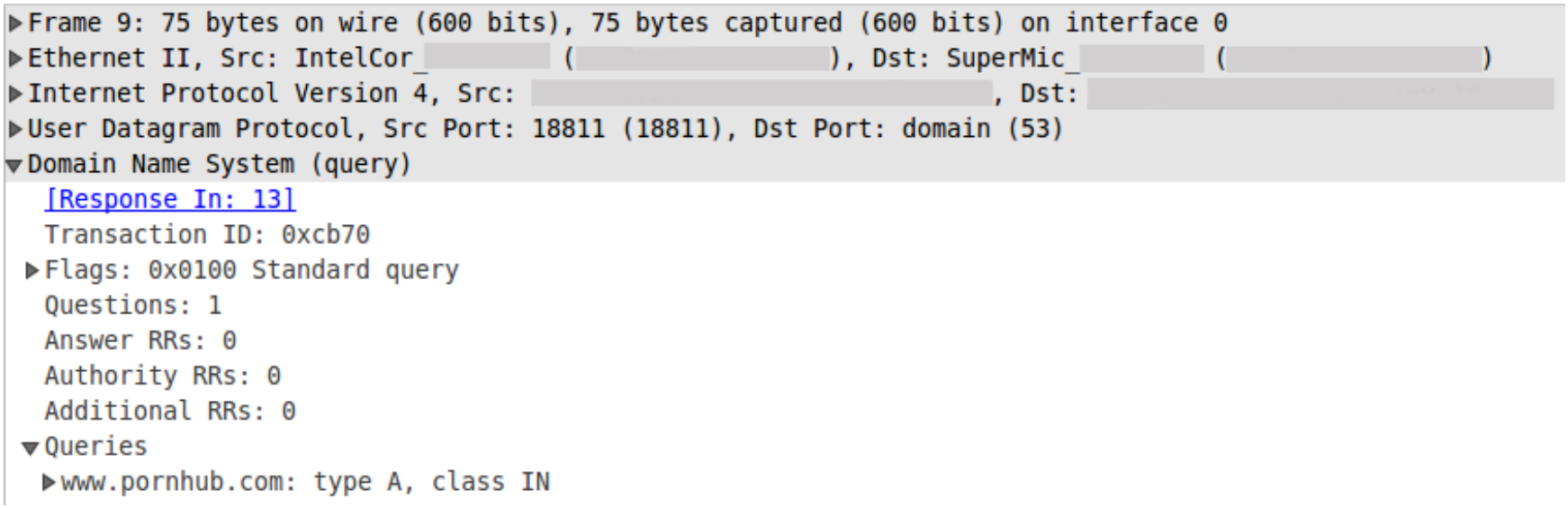
Privacy

- What about the following packet?

```
▶ Frame 9: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
▶ Ethernet II, Src: IntelCor_        (                  ), Dst: SuperMic_        (                  )
▶ Internet Protocol Version 4, Src:                                  , Dst:
▶ User Datagram Protocol, Src Port: 18811 (18811), Dst Port: domain (53)
▼ Domain Name System (query)
    [Response In: 13]
    Transaction ID: 0xcb70
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.pornhub.com: type A, class IN
```

Privacy

- What about the following packet?



- Okay, it's DNS

Privacy

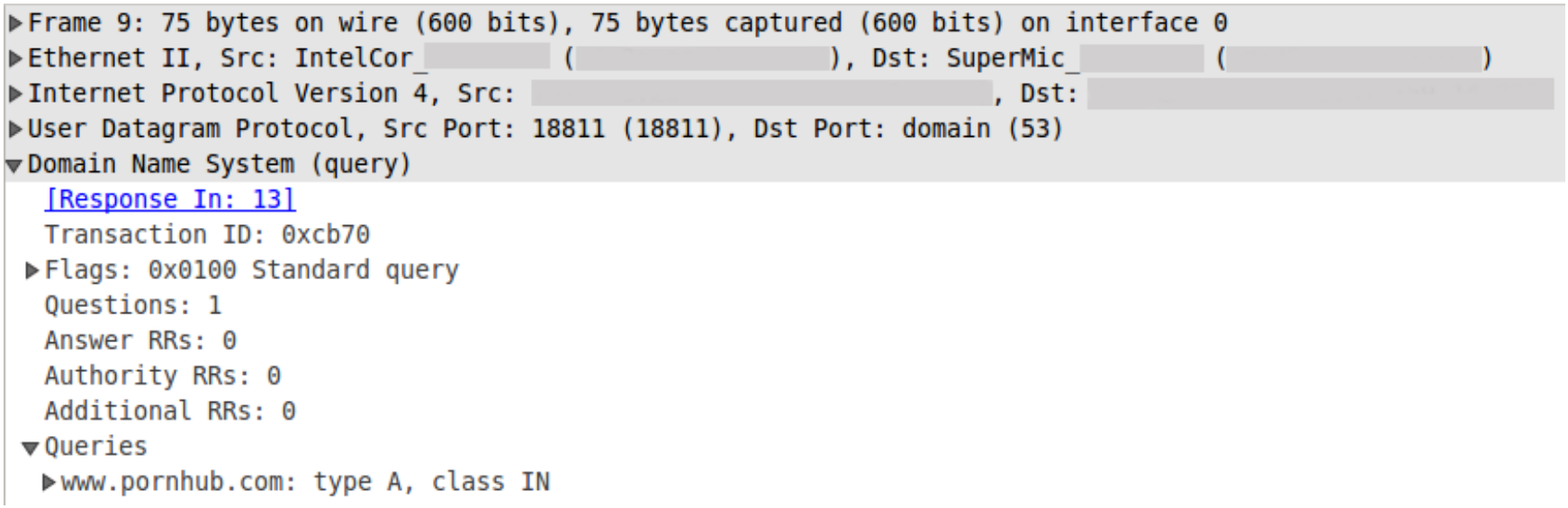
- What about the following packet?

```
▶ Frame 9: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 0
▶ Ethernet II, Src: IntelCor_        (                  ), Dst: SuperMic_        (                  )
▶ Internet Protocol Version 4, Src:                                  , Dst:
▶ User Datagram Protocol, Src Port: 18811 (18811), Dst Port: domain (53)
▼ Domain Name System (query)
    [Response In: 13]
    Transaction ID: 0xcb70
  ▶ Flags: 0x0100 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 0
  ▼ Queries
    ▶ www.pornhub.com: type A, class IN
```

- Okay, it's DNS
- DNS is not secure, but we can use DNSSEC

Privacy

- What about the following packet?



- Okay, it's DNS
- DNS is not secure, but we can use DNSSEC
- Now the answer can be integrity protected

Privacy

- Wait, you want confidentiality?

Privacy

- Wait, you want confidentiality?
- Okay, send the DNSSEC via an ESP tunnel

Privacy

- Wait, you want confidentiality?
- Okay, send the DNSSEC via an ESP tunnel
- BTW: Who is your DNS provider?

```
▶ Frame 1: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 0
▶ Ethernet II, Src: IntelCor_        (                  ), Dst: Sphairon_        (                  )
▶ Internet Protocol Version 4, Src: 192.168.1.170 (192.168.1.170), Dst: 8.8.8.8 (8.8.8.8)
▶ User Datagram Protocol, Src Port: 36471 (36471), Dst Port: domain (53)
▼ Domain Name System (query)
    Transaction ID: 0x0bf5
  ▶ Flags: 0x0120 Standard query
    Questions: 1
    Answer RRs: 0
    Authority RRs: 0
    Additional RRs: 1
  ▼ Queries
    ▶ pornhub.com: type A, class IN
  ▶ Additional records
```

Privacy – Lessons Learned

Your DNS provider knowns what you are doing!

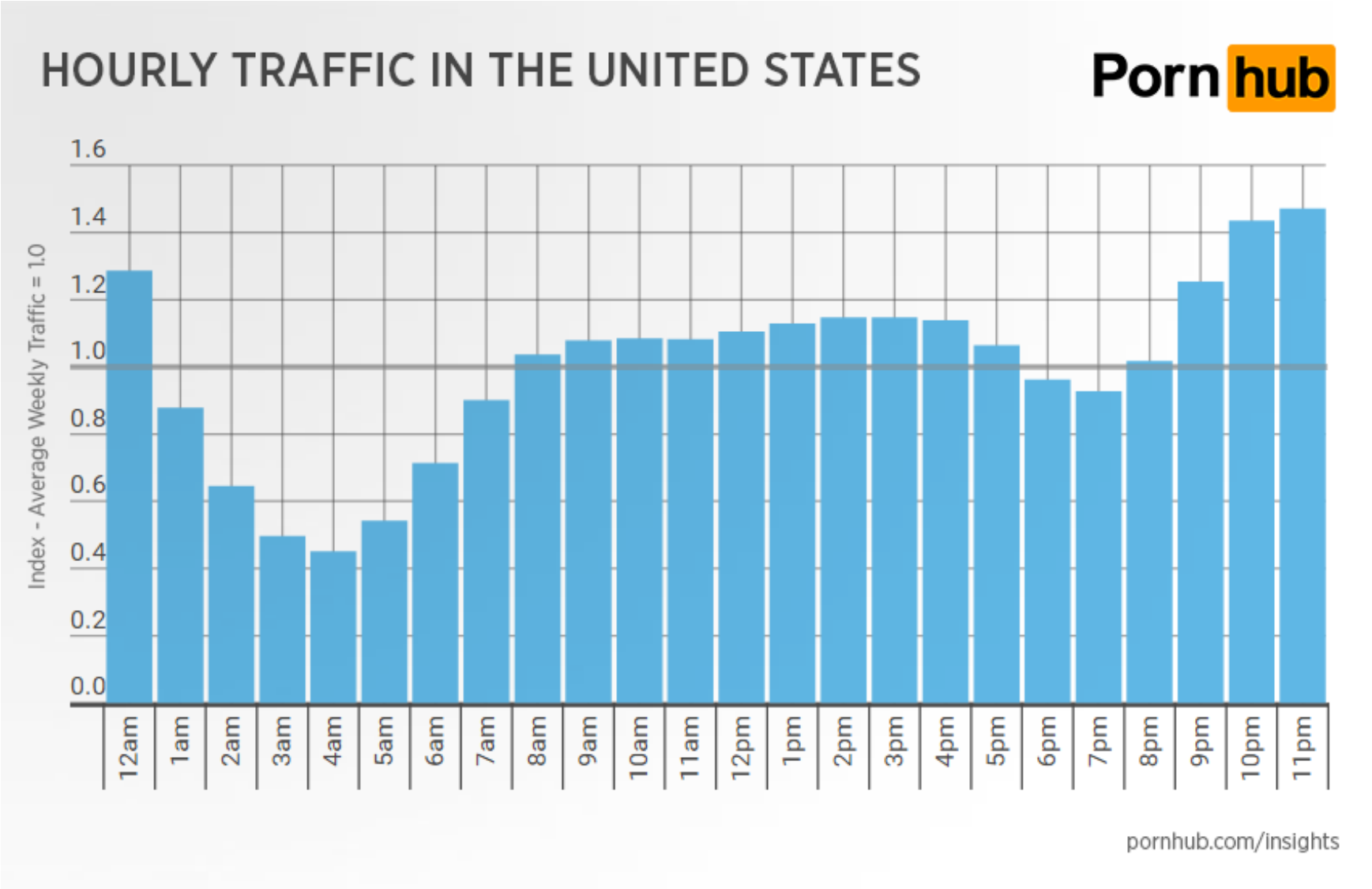
About this Example

- It is widely acknowledged that there are many pages in the web with dubious content
- Among the top 500 sites on the web[1], many serve adult content
- PornHub is among the 100 most popular web sites globally[2]
- We used PornHub as example for this lecture

[1] http://www.alexa.com/topsites

[2] Rank 72 on Dec 17 2014, http://www.alexa.com/siteinfo/pornhub.com

Meta Data


HOURLY TRAFFIC IN THE UNITED STATES
Pornhub
Index - Average Weekly Traffic = 1.0
1.6
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
12am
1am
2am
3am
4am
5am
6am
7am
8am
9am
10am
11am
12pm
1pm
2pm
3pm
4pm
5pm
6pm
7pm
8pm
9pm
10pm
11pm
pornhub.com/insights

Meta Data

- We can protect your traffic

Meta Data

- We can protect your traffic
  - But some information needs to be accessible in plaintext

Meta Data

- We can protect your traffic
  - But some information needs to be accessible in plaintext
  - IP source and destination

Meta Data

- We can protect your traffic
  - But some information needs to be accessible in plaintext
  - IP source and destination
- Btw: what is this 31.192.117.132 IP address on TCP port 80 you are visiting?
- ```
  curl -v http://31.192.117.132/
  Connected to 31.192.117.132 (31.192.117.132) port 80
  > GET / HTTP/1.1
  > User-Agent: curl/7.35.0
  > Host: 31.192.117.132
  > Accept: */*
  >
  < HTTP/1.1 301 Moved Permanently
  < Date: Tue, 09 Dec 2014 17:27:59 GMT
  < Location: http://www.pornhub.com/
  ```
  ```

Meta Data

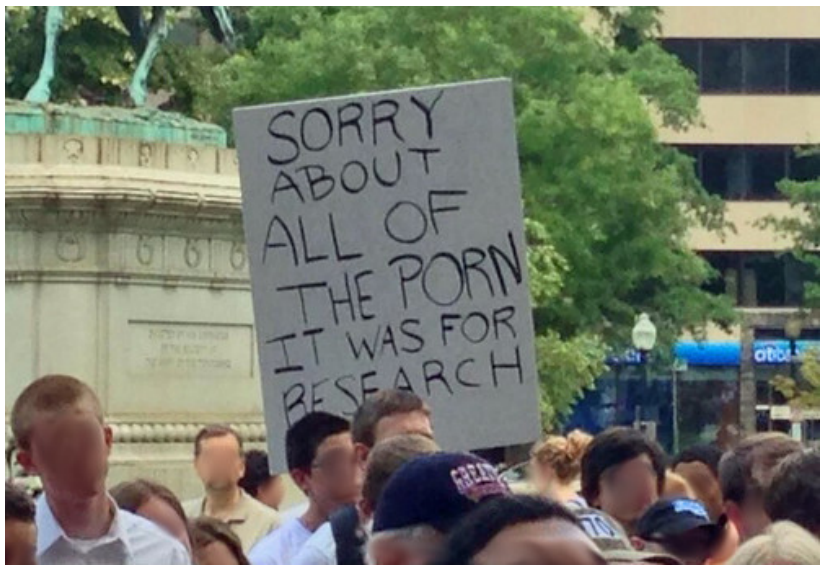
- Okay, Okay, I set up an IPsec tunnel to a secure server
- The secure server forwards my packets to the Internet
- You will only see the outer IP header

Meta Data

- Okay, Okay, I set up an IPsec tunnel to a secure server
- The secure server forwards my packets to the Internet
- You will only see the outer IP header
- But at some point, the inner packet needs to be given to the Internet

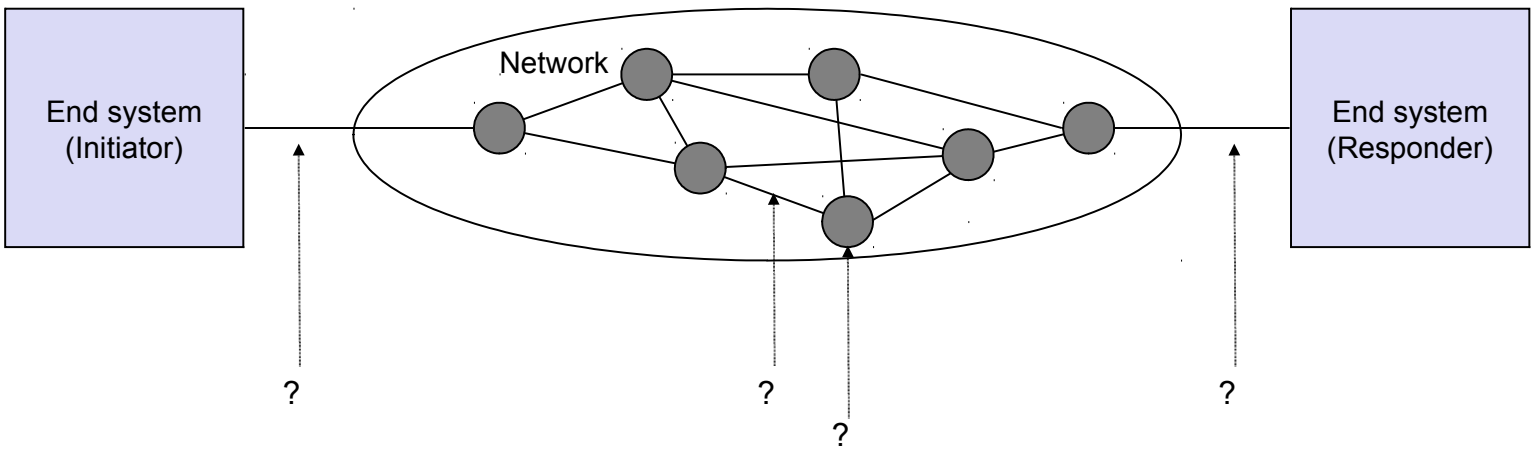
Meta Data

- Okay, Okay, I set up an IPsec tunnel to a secure server
- The secure server forwards my packets to the Internet
- You will only see the outer IP header
- But at some point, the inner packet needs to be given to the Internet
- Global attacker (e. g., state-level attackers) still know what you are doing



Protest sign, Anti-NSA demonstration “Restore The Fourth”, July 2013

Meta Data

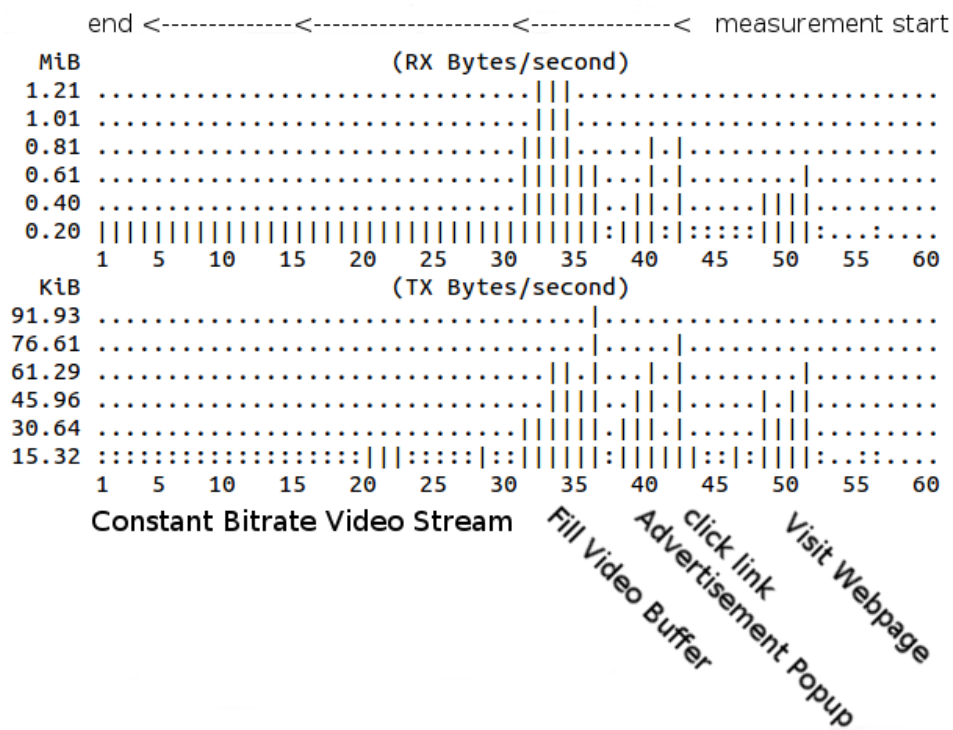


Traffic Analysis

- What about traffic analysis?
- Maybe I'm not the NSA and cannot see your unencrypted traffic
- I can still observe
  - The amount of data you are transmitting
  - Timing information

Traffic Analysis – Network Bandwidth (Example)

1. 7 high spikes in network load
   - As if you were visiting 7 webpages (figure below only shows 3)
2. A high burst of traffic
3. A constant rate of network load
   - As if a web player is filling its buffers
   - And playing a video afterwards at constant rate
4. The constant network load last for about 8 minutes (not shown)

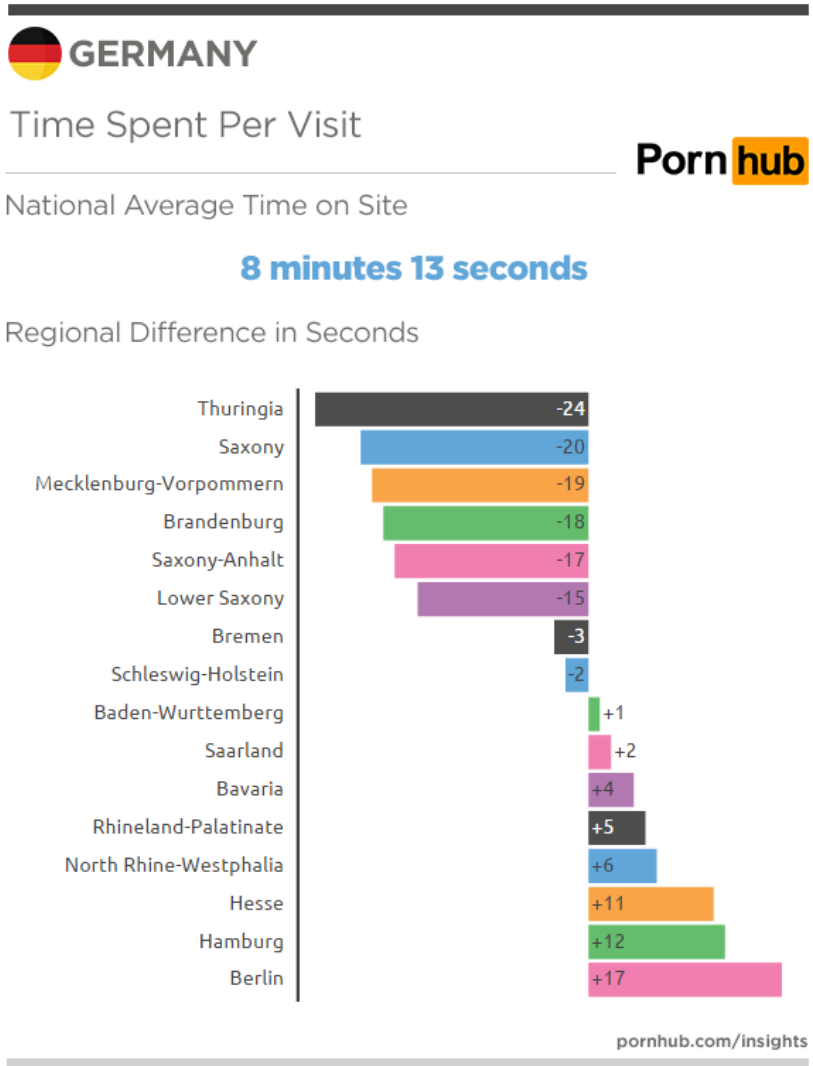


I'll just leave this here

- PornHub statistics for Germany

PornHub Insights, *Pornhub & Germany*, May 2014, `http://www.pornhub.com/insights/` retrieved Dec 2014

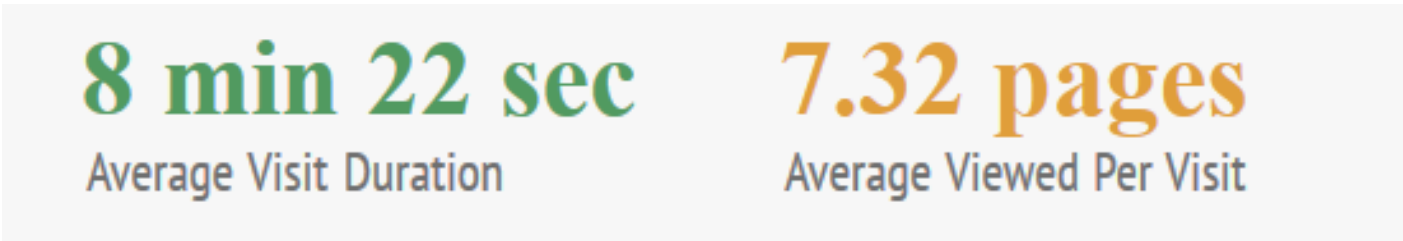
I'll just leave this here



PornHub Insights, *Germany in Review*, Mar 2016, `http://www.pornhub.com/insights/` retrieved Dec 2016

I'll just leave this here

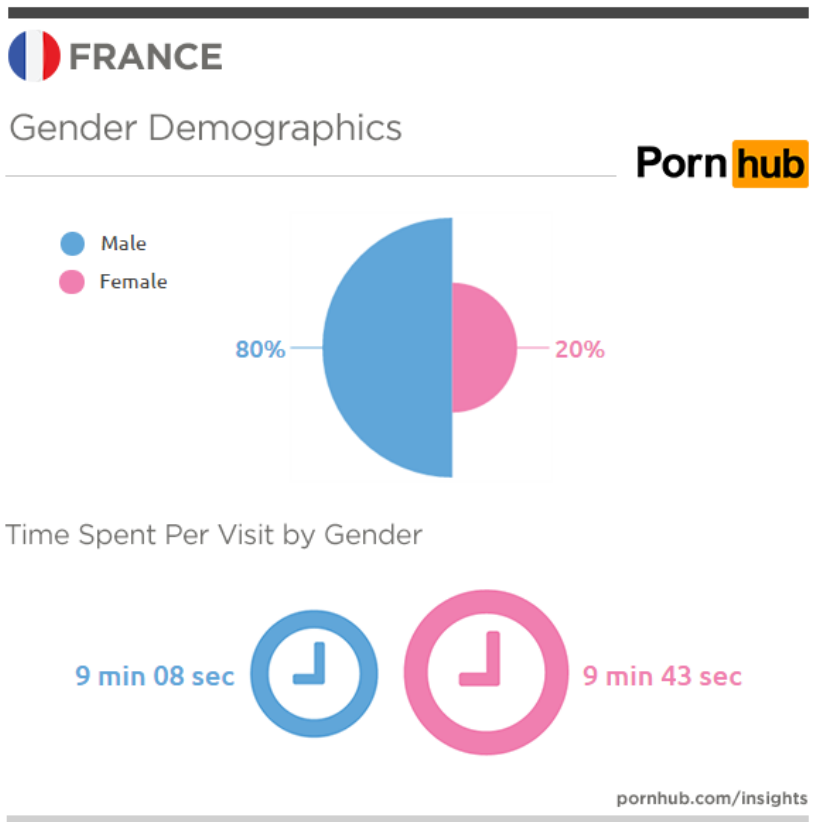
- I's not just Germany...
- Statistics for India



PornHub Insights, *Pornhub & India*, Nov 2014, `http://www.pornhub.com/insights/` retrieved Dec 2014

I'll just leave this here

- I's not just Germany...
- Statistics for France

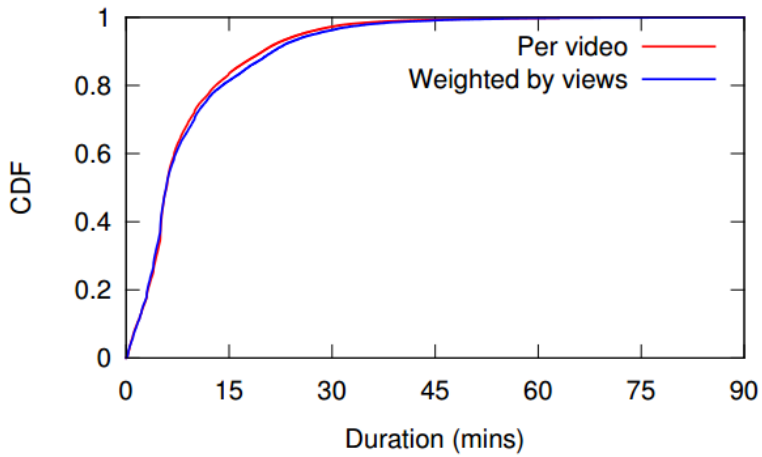


PornHub Insights, *France's Favorite Searches*, May 2016, `http://www.pornhub.com/insights/` retrieved Dec 2016

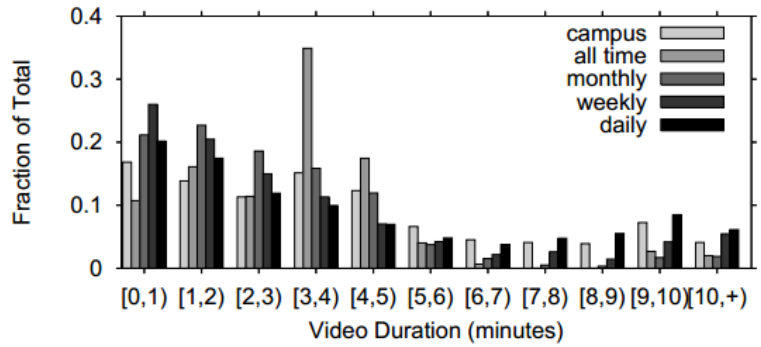
Such Meta Data, Very Traffic Analysis, Wow

PornHub Insights, *United States vs Russia*, May 2014, `http://www.pornhub.com/insights/` retrieved Dec 2014

Content Duration of Available Content



Tyson, Gareth, et al. *Demystifying porn 2.0: a look into a major adult video streaming website.* IMC 2013 – (YouPorn data)



Gill, Phillipa, et al. *Youtube traffic characterization: a view from the edge.* IMC 2007

Happy Holidays

Best wishes for a wonderful Holiday
and a Happy New Year!