Network Security
(6CCS3NSE - 7CCSMNSE)

Diego Sempreboni
Department of Informatics
King's College London, UK

Second term 2019/20
Lecture 2

Objectives and learning outcomes

- At the end of this lecture you should be able to:
  - Understand what sniffing is
  - Understand different types of passive and active sniffing
  - Analyse wired and wireless traffic

The OSI model: a recap

Networking example

- Browsing to google.com

- STEPS:
  - Browser established a TCP connection with google.com server
  - Browser asks using HTTP (command GET) for the index web page (the one you put the text to search for)
  - Browser displays the page in the screen

Encapsulation

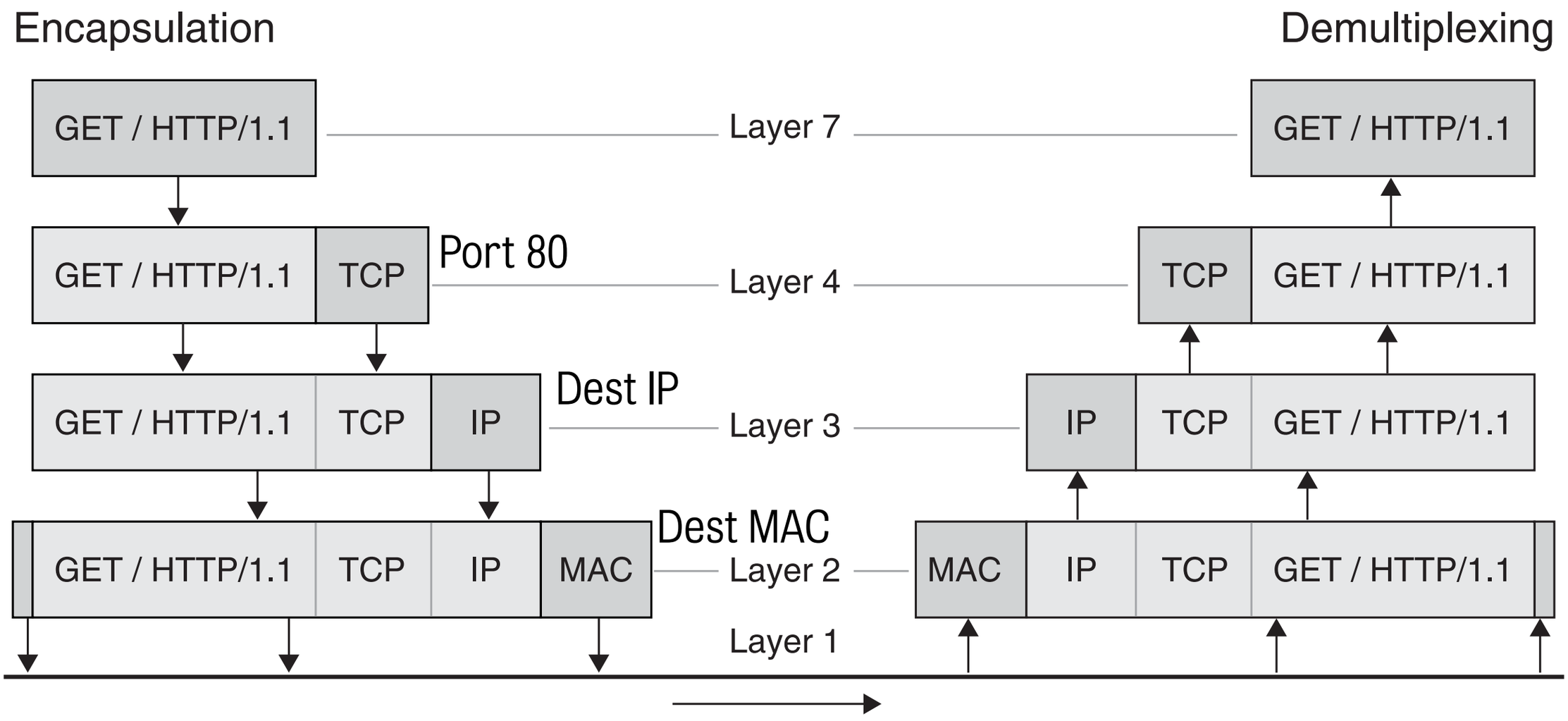
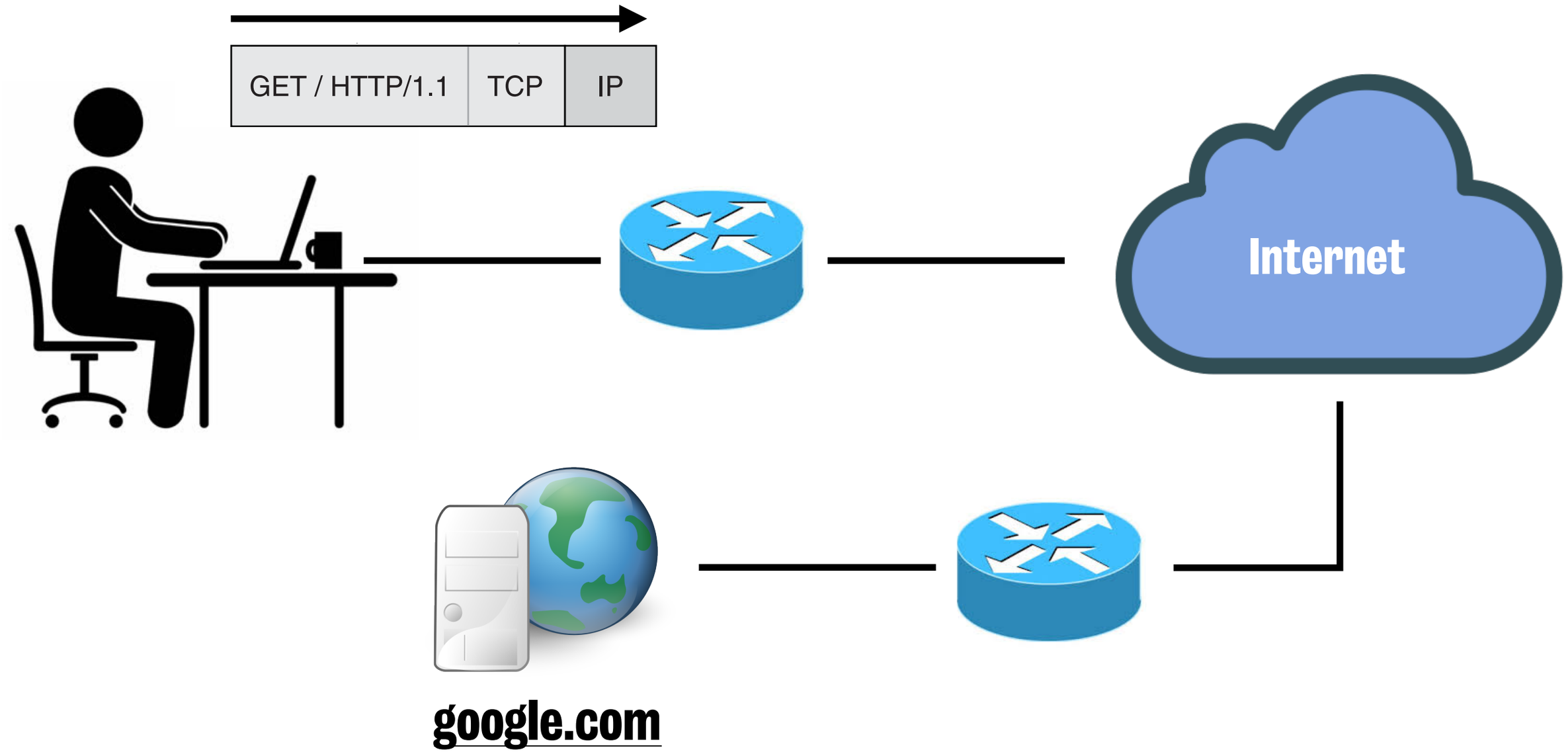
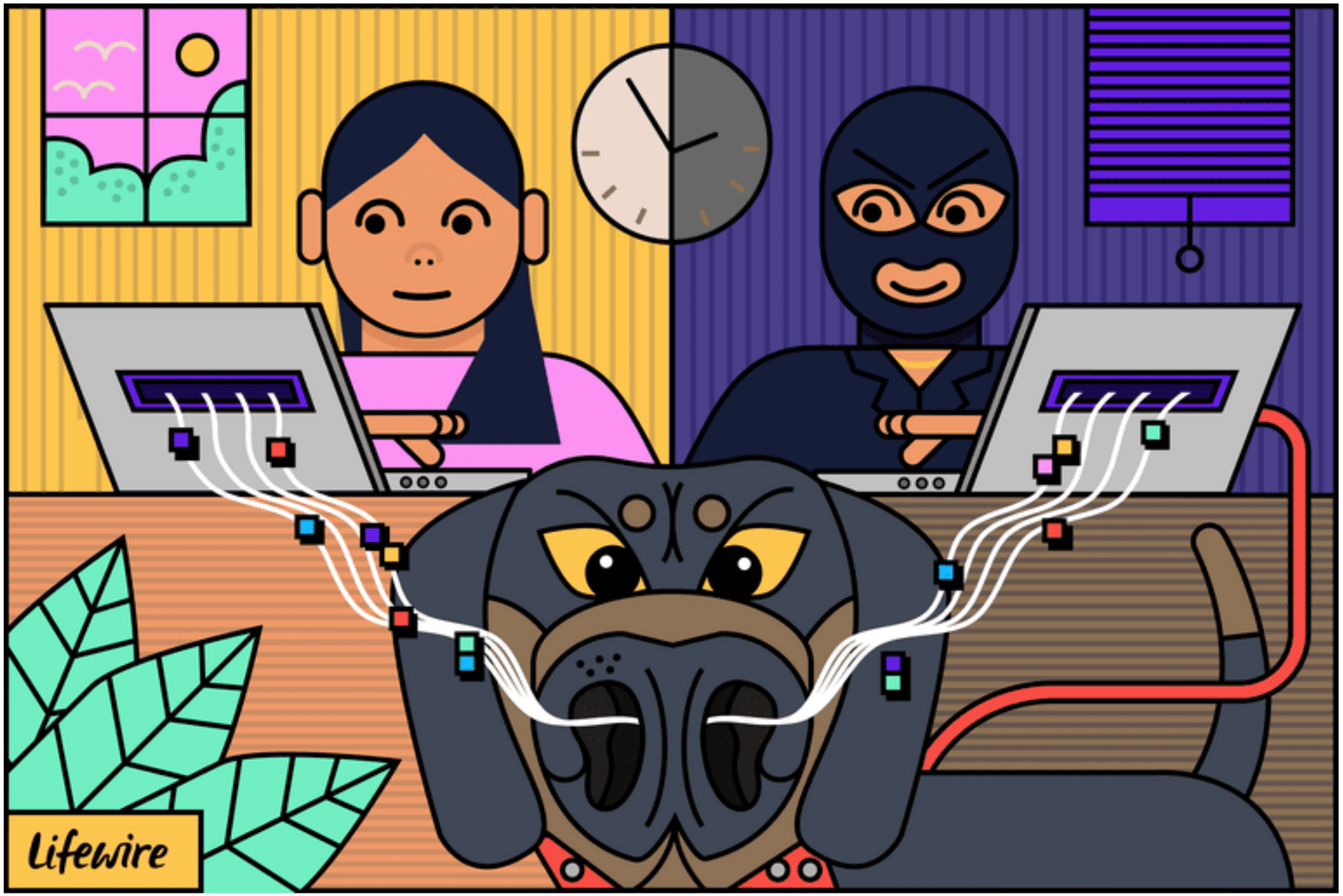


Figure 2–2. An HTTP "GET" request, shown in the framework of the OSI model.

Networking example



Sniffing



What is network packet sniffing

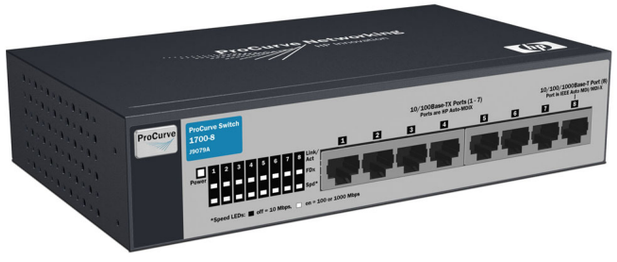
- Sniffing attacks involve listening to network conversations that are **not intended for you**

- Sniffing can have a benign purpose: it is very useful for network debugging & diagnostics

Physical (Layer 1 OSI)

On the wire

In the air



Switches

Routers

Mr. Robot: Sniffing

Physical interception (Layer 1 OSI)

- How to get information in transit?
- Different depending on:
  - We are in a network or not
  - The attack is passive or active

Passive interception

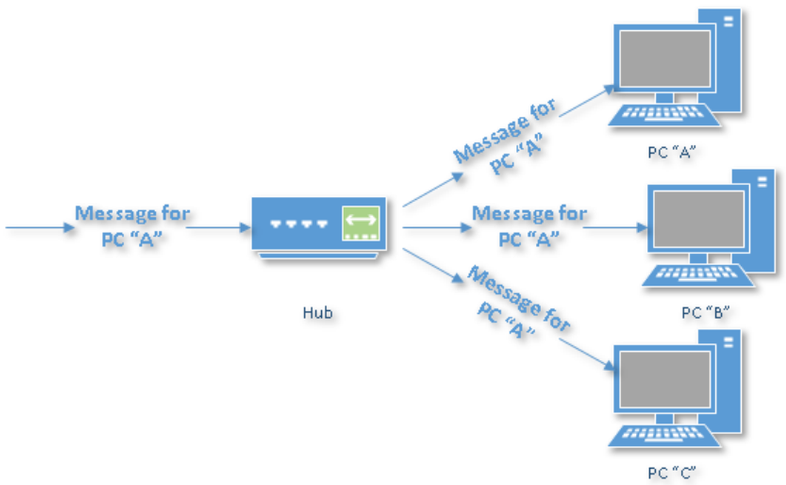
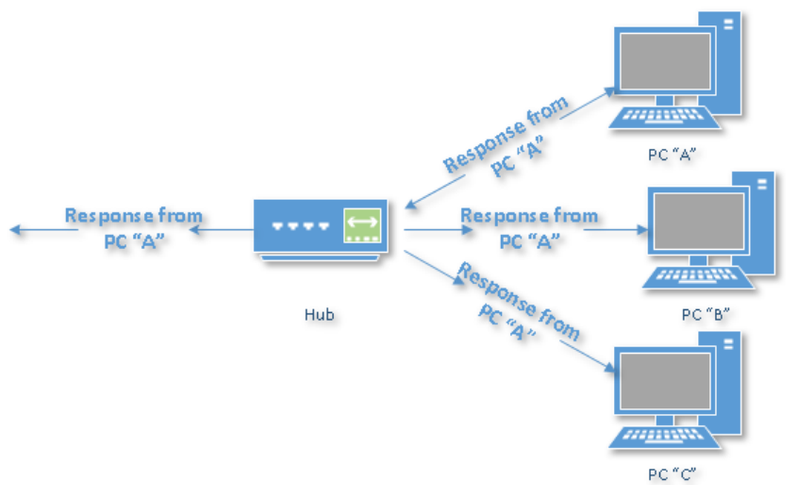
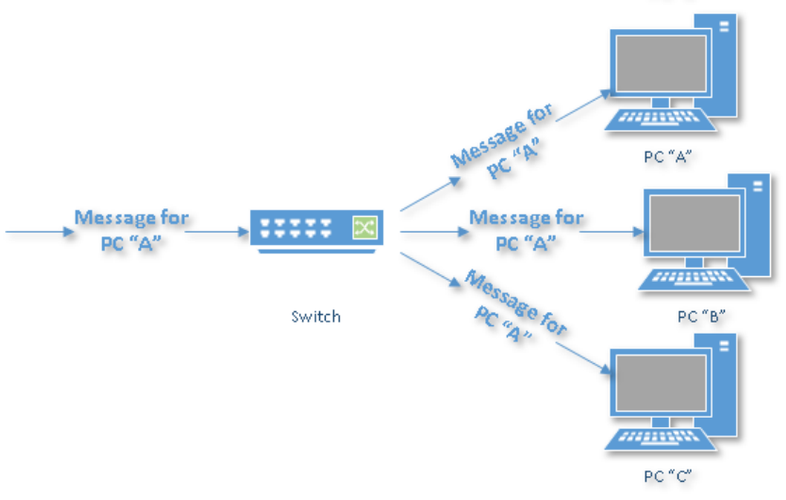
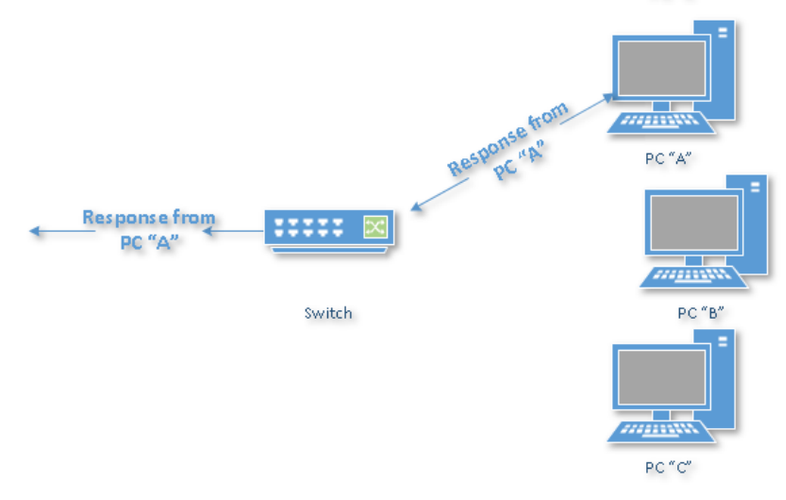
- Network card returns packets destined for you. But card may be put in a **promiscuous mode** to get all packets from network.

- Works for networks using HUBS and WIFI networks

- It does not work for networks using switches

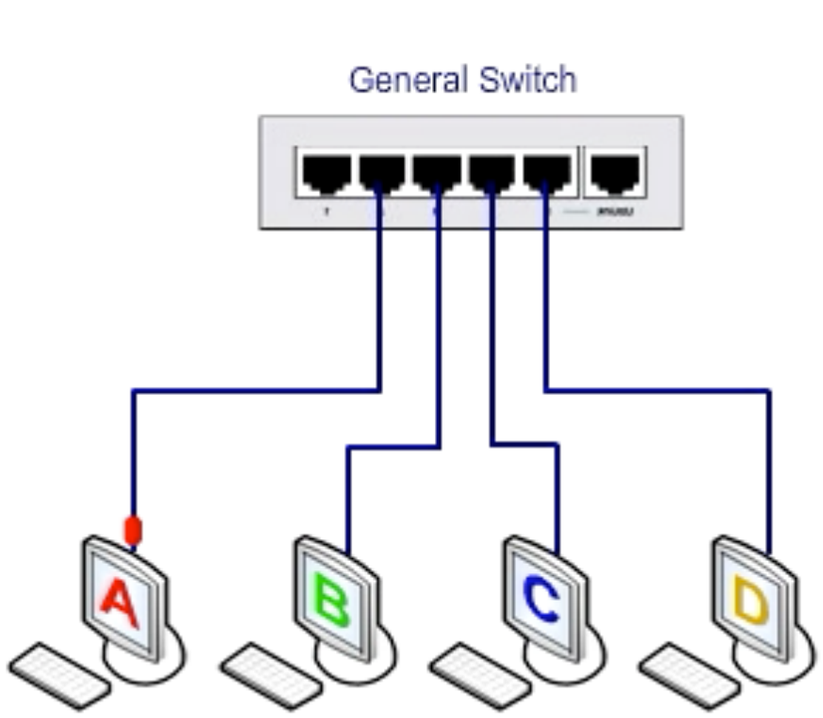
HUBS ??? SWITCHES ???

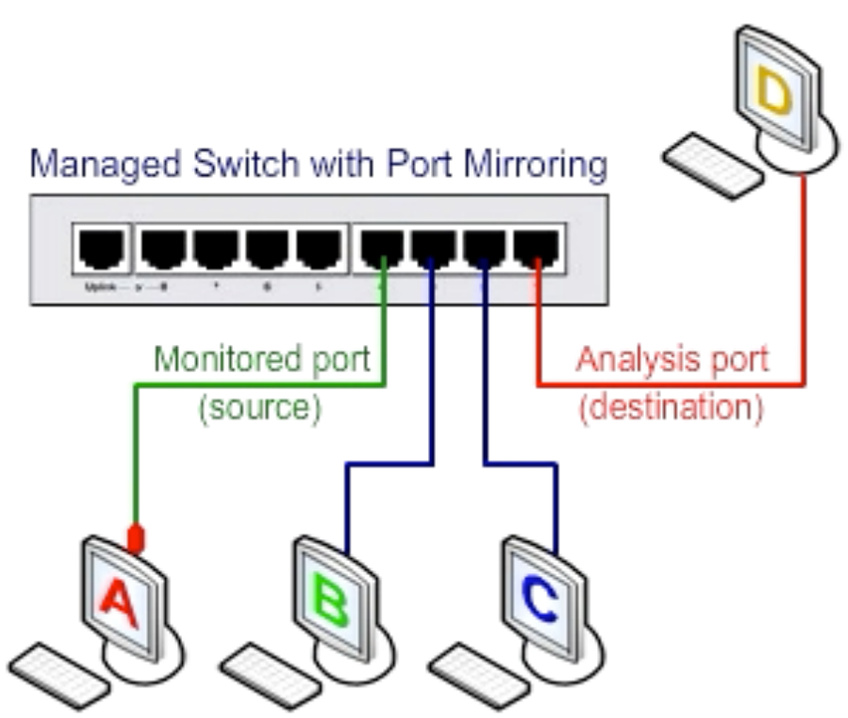
- Unlike less advanced repeater hubs, which broadcast the same data out of each of its port and let the devices decide what data they need, a network switch forwards data only to the devices that need to receive it.

Device	Layer	Incoming data	Returned response
HUB	Layer 1 OSI		
SWITCH	Layer 2 OSI		

Active interception

- Switch SPAN port mirrors all traffic through the switch
- Good purpose:
  - Network diagnostics
  - Intrusion detection

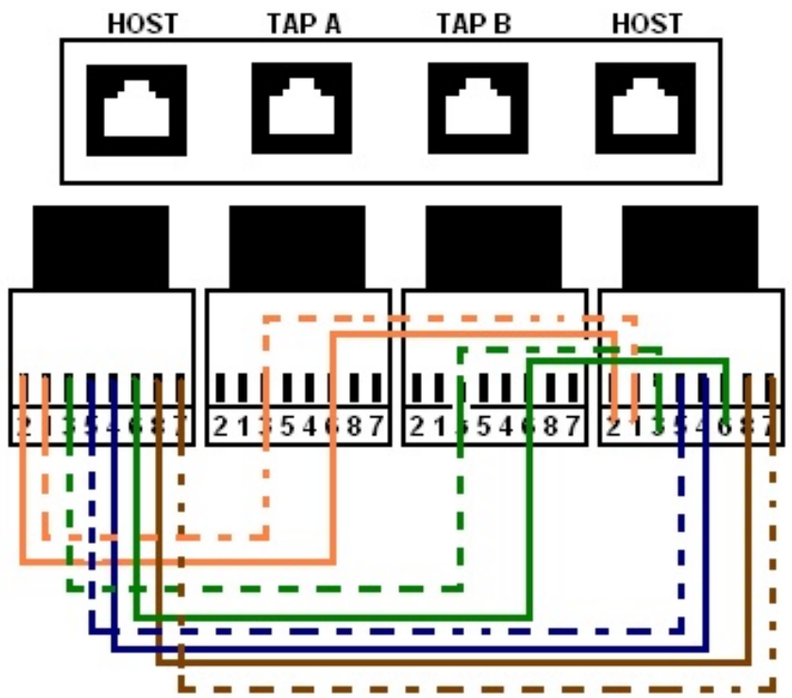


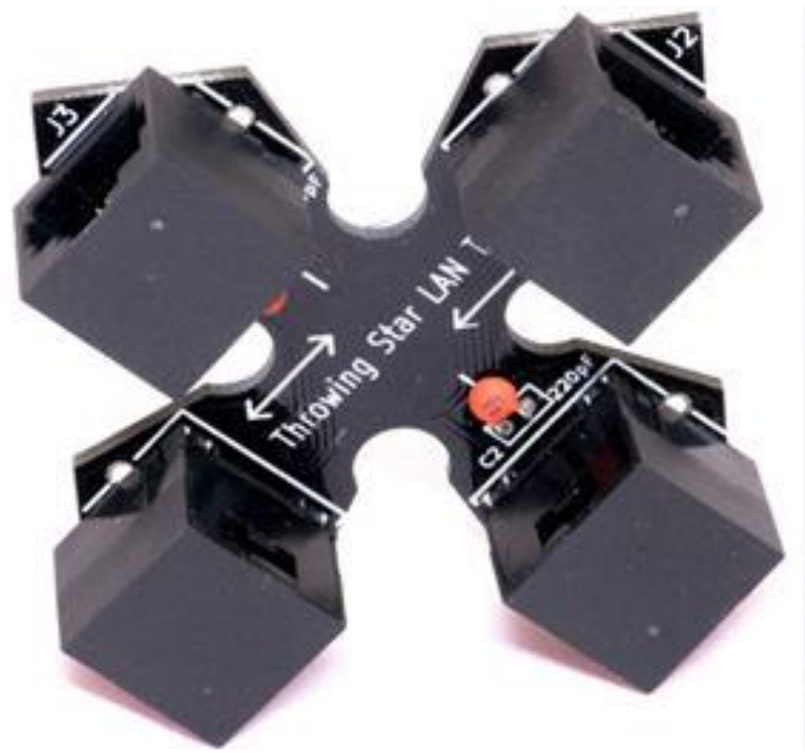


- **Malicious behaviour:** if an attacker plugs into the port, they could see all traffic (but it requires physical access to the switch)

Active interception: Tap into a network

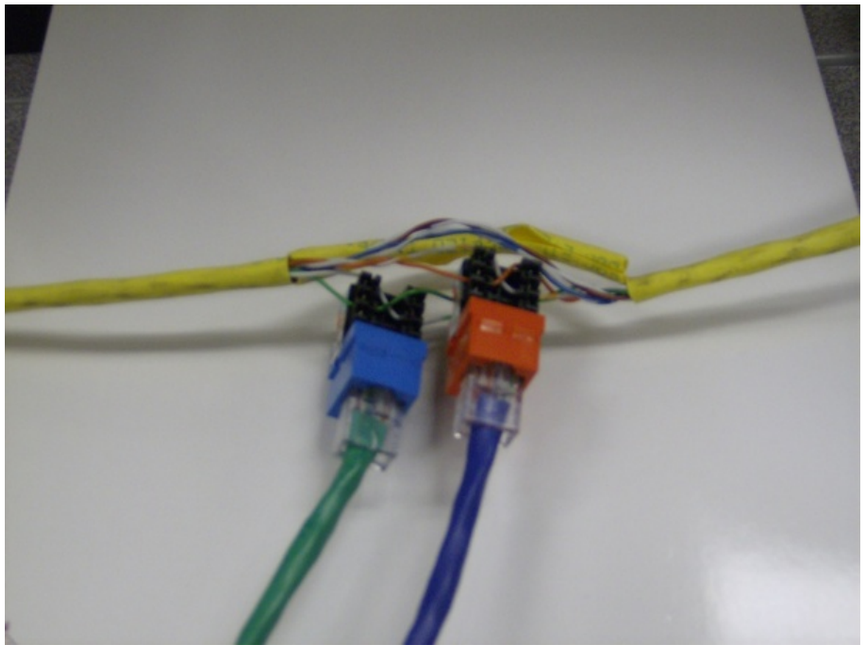
- Layer 1 device: In line network taps
- Causes brief disruption as cable needs to be separated



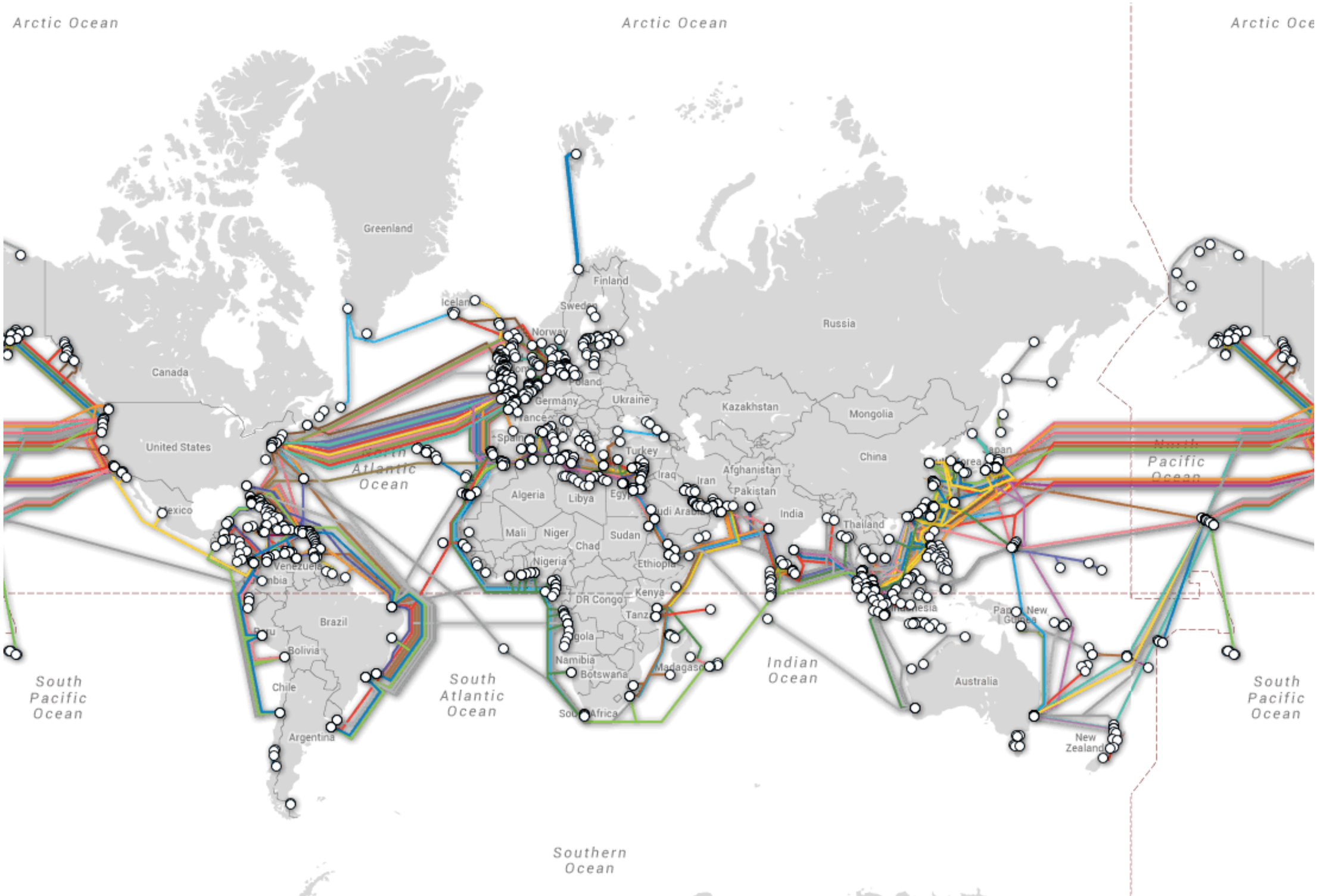


Active interception: Tap into a network

- Layer 1 device: In line network taps
- **Vampire taps:** pierce the shielding of copper wires in order to provide access to the signal within.
- This may bring down the link
- Used a lot by Telco, engineers



Tap into a network EVEN IN UNDERSEA CABLES



Is it happening? (Undersea cable cuts: Truth or Conspiracy Theory?)

- In early 2008, a series of undersea cable disruptions in the Middle East were reported. These caused Internet and voice outages and slowdowns in India, Pakistan, Egypt, Qatar, Saudi Arabia and several other countries.

- After three separate incidents in which five cables were damaged, many people began speculating that the cuts were not a coincidence, but rather deliberately caused to induce economic disruptions, to cause Internet rerouting, or to cover the installation of covert fibre optic network taps.

Is it happening? (Undersea cable cuts: Truth or Conspiracy Theory?)

- Security Prof. Steve Bellovin wrote:

  "Four failures in less than a week. Coincidence? Or enemy action? If so, who's the enemy, and what are the enemy's goal? You can't have the many failures in one place - especially such a politically sensitive place - without people getting suspicious..."

  "Now - the US certainly has the ability to tap undersea cables. After all, they did just that to the Soviets several decades ago... That said, I don't think it's an NSA or Mossad operation... Four failures at once will raise suspicions, and that's the last thing you want when you're eavesdropping on people."

  "If it wasn't a direct attempt at eavesdropping, perhaps it was indirect. Several years ago, a colleague and I wrote about a link-cutting attacks. In these, you cut some cables, to force traffic past a link you're monitoring. Link-cutting for such purposes isn't new; at the start of World War I, the British cut Germany's overseas telegraph cable to force them to use easily-monitored links."

Is it happening? (Undersea cable cuts: Truth or Conspiracy Theory?)

https://youtube.com/watch?v=lgjbib9H8XY

Is it happening? (Undersea cable cuts: Truth or Conspiracy Theory?)

https://youtube.com/watch?v=0vSGCjEV1ng

Warwalking / Wardriving

There are several tools that do this, like **netstumbler**

Is it happening? (Dutch intelligence thwarted a Russian hacking operation)

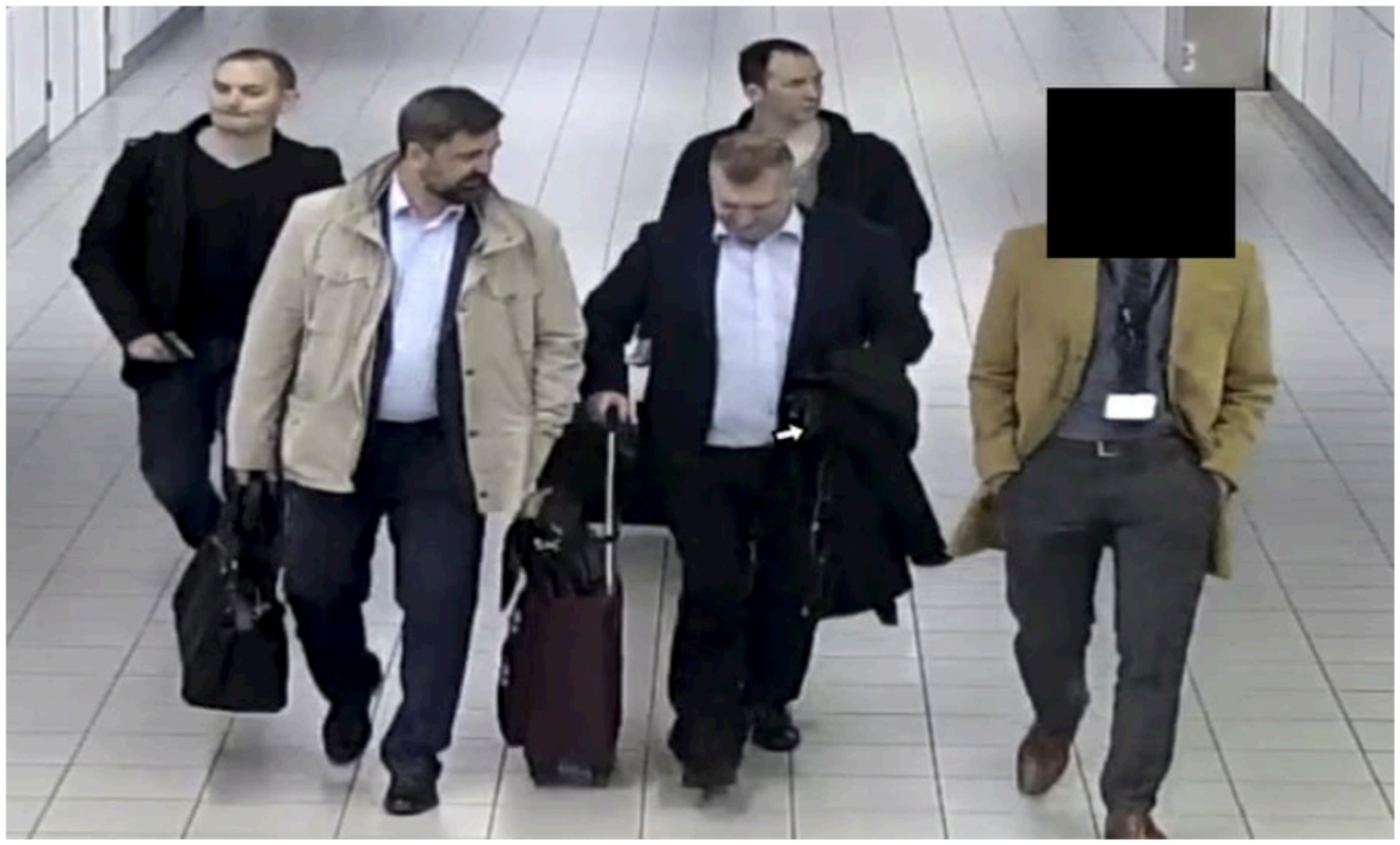
Russia

Visual guide: how Dutch intelligence thwarted a Russian hacking operation

Jon Henley
@jonhenley

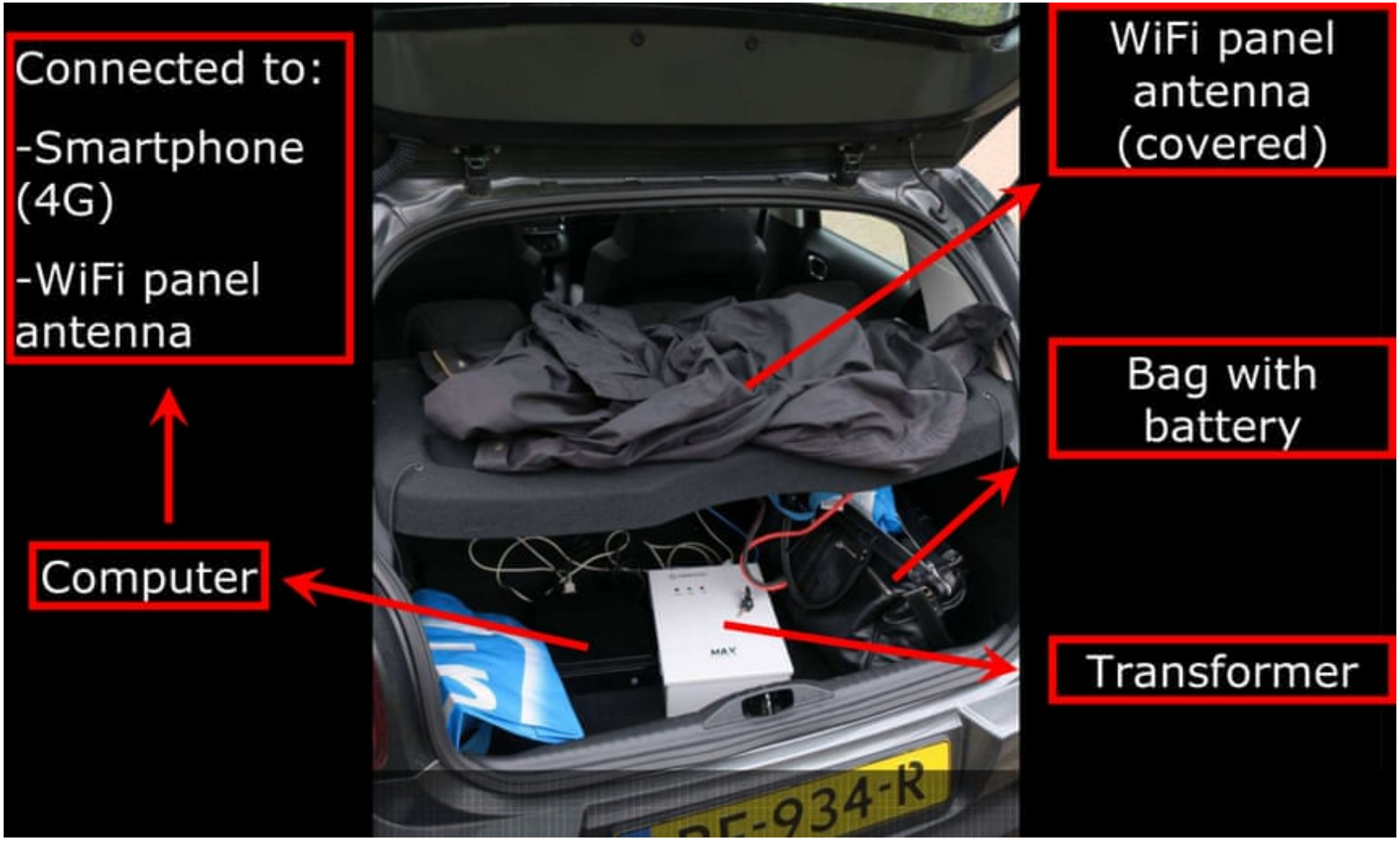
Thu 4 Oct 2018 15.55 BST

303

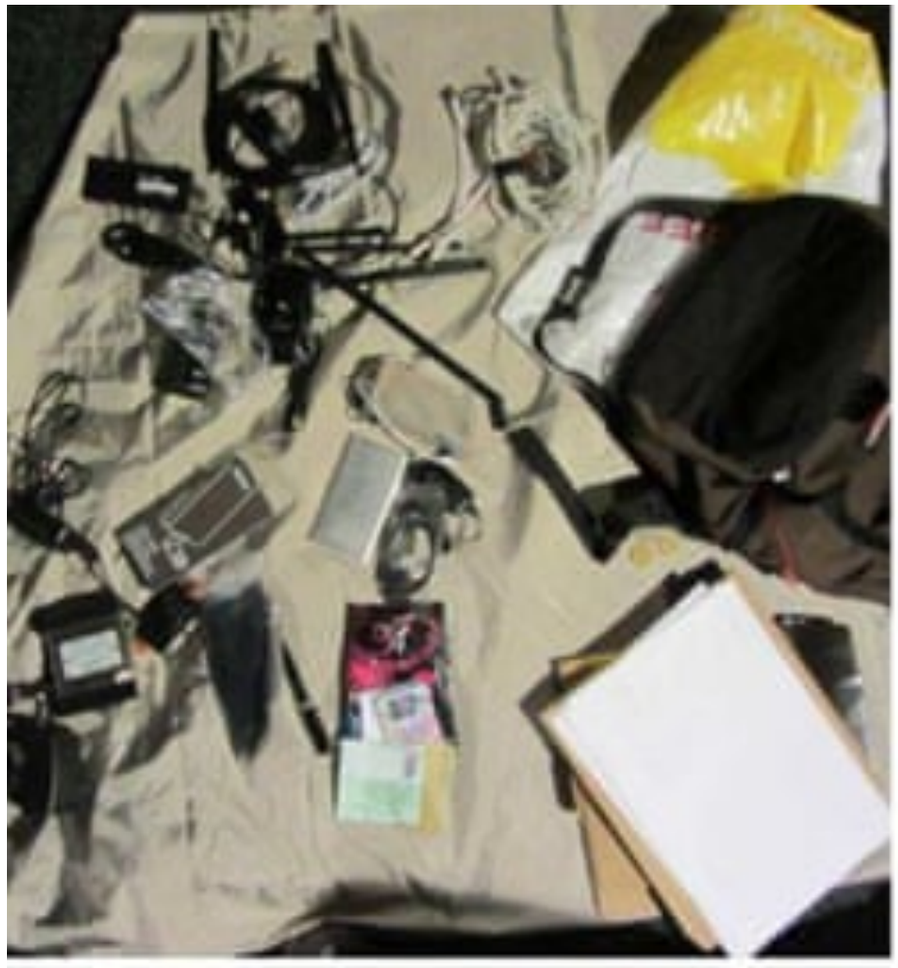


▲ Four Russian GRU arrive in the Netherlands. Photograph: AP

Is it happening? (Dutch intelligence thwarted a Russian hacking operation)



Is it happening? (Dutch intelligence thwarted a Russian hacking operation)



Warflying: has someone said Drones?

https://youtube.com/watch?v=Ed1OjAuRARU

Rogue Access Point

- A rogue access point is a wireless access point that has been installed on a network without explicit authorisation from a local network administrator

- Types:
  - **Hardware**: a wireless router
  - **Software**: a computer/laptop with virtual one

- They are usually open and/or try to mimic a known WIFI network ID - e.g., Eduroam!

Data acquisition (Layer 2 OSI)

- We have chunks of bytes from Layer 1 OSI
- What is the meaning of these?
- Who is talking to whom?

- Layer 2 protocols (usually LAN or WAN)
- Ethernet (wired)
- Wi-Fi

- Both based on MAC addresses and ARP to get IP

pcap: basis of Wireshark & tcpdump

- Both Wireshark and tcpdump built on libcap, a very versatile library for all kinds of capture:

1. Capture only packets of the icmp protocol

tcpdump -i eth0 icmp

2. Capture ssh packets between two hosts

tcpdump src <x> and dst <y> and port 22

More here: thegeekstuff.com/2010/08/tcpdump-command-examples

How to make pcap efficient

- PROBLEM: diversity of requests -> network card has to pass all packets to filtering program (**performance issue**)

- It is one thing to process your packet, another to process all packets in the subnetwork (e.g., all KCL pkts)

- Why is this difficult?

  - Each time data has to be fetched, user code has to trap to kernel and have buffer be filled

How to make pcap efficient: SOLUTION

- Steve McCanne and Van Jacobson, LBNL, 1992

- Filtering commands written as commands for a virtual machine interpreter run by the kernel. Just-in-time compilation of filtering regular expressions is used to decrease overheads.

Wireless data acquisition (Layer 2 OSI)

- Trivial if the network is open or Rogue Access Point
- Trivial if the network is encrypted using WEP
  - Tools like Aircrack-ng, Kismet, Cain&Abel, etc…

- A bit more difficult with WPA-PSK WPA2-PSK
  - If in the same network, trivial!
  - If not, may take a while but possible (WPA-PSK easier)

- More difficult with WPA-Enterprise, WPA2-Enterprise, WPA3
  - But not impossible with enough time (see the recent key reinstallation attack https://krackattacks.com)
  - Once unencrypted, **libcap!**

Traffic Analysis

Type of traffic analysis

- Protocol analysis
- Packet analysis
- Flow analysis

Protocol analysis

- Tons of different network protocols
  - IP, TCP, UDP, HTTP, HTTPS, SMTP, ...

- The specification of many of them is public
  - IETF Request for Comment (RFC) documents
  - RFC 793 - TCP v4
  - RFC 2613 - HTTP v1.1

- Other may be proprietary
  - Need to buy specific tools
  - Need to reverse-engineer

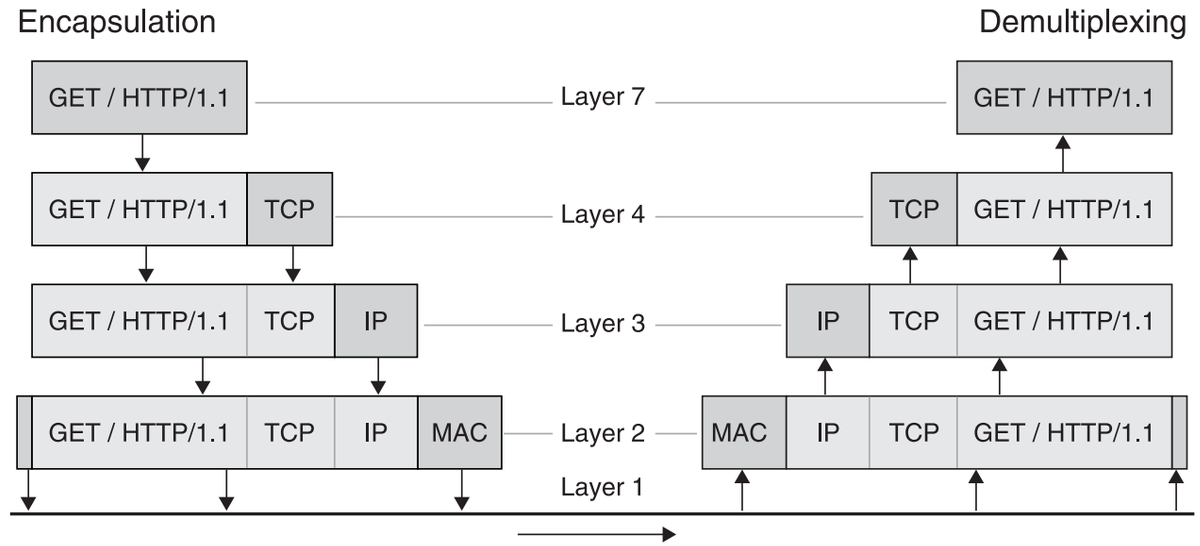


Figure 2–2. An HTTP "GET" request, shown in the framework of the OSI model.

Protocol analysis

- Why?
  - To understand the semantics of the information being transmitted to be able to interpret it
- Support for public protocols is usually implemented in tools like Wireshark
  - Wireshark shows headers, flags, content in a more user-friendly and navigable way

Protocol analysis

tv-netflix-problems-2011-07-06.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
343	65.142415	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
344	65.142715	192.168.0.21	174.129.249.228	HTTP	253	GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
345	65.230738	174.129.249.228	192.168.0.21	TCP	66	80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
346	65.240742	174.129.249.228	192.168.0.21	HTTP	828	HTTP/1.1 302 Moved Temporarily
347	65.241592	192.168.0.21	174.129.249.228	TCP	66	40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
348	65.242532	192.168.0.21	192.168.0.1	DNS	77	Standard query 0x2188 A cdn-0.nflximg.com
349	65.276870	192.168.0.1	192.168.0.21	DNS	489	Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
350	65.277992	192.168.0.21	63.80.242.48	TCP	74	37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
351	65.297757	63.80.242.48	192.168.0.21	TCP	74	80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
352	65.298396	192.168.0.21	63.80.242.48	TCP	66	37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
353	65.298687	192.168.0.21	63.80.242.48	HTTP	153	GET /us/nrd/clients/flash/814540.bun HTTP/1.1
354	65.318730	63.80.242.48	192.168.0.21	TCP	66	80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
355	65.321733	63.80.242.48	192.168.0.21	TCP	1514	[TCP segment of a reassembled PDU]

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Packet analysis

- Inspecting the protocols within a set of packets transmitted, identifying packets of interest using packet analysis techniques

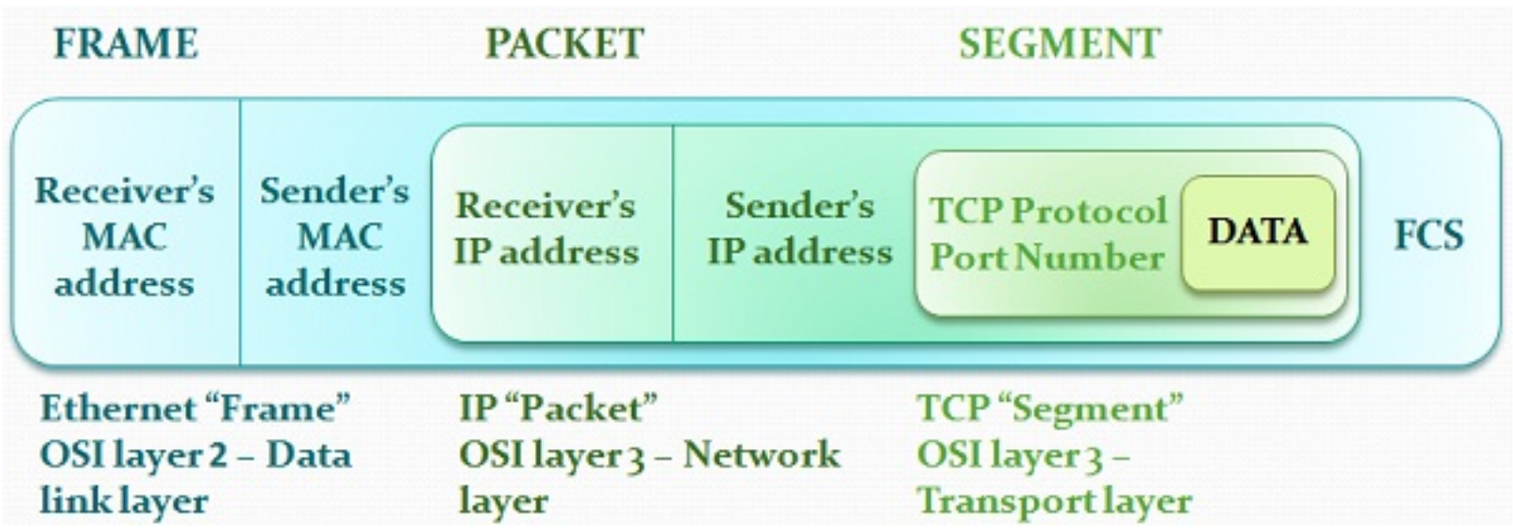
- What does packet analysis do?
  - **Network professionals** -> monitor the health of a network
  - **Security professionals** -> passive network vulnerability assessment
  - **Attackers** -> passive attack tool -> stolen information such as passwords

- Passive means: Inspection without doing anything

Packet analysis: the word packet is misleading

- **Frames** is actually captured and analysed
- **Frames** are what carry packets in a local network
  - When a frame is captured, within the frame, a packet is discovered

- Packet analysis results:
  - Frame are always mentioned
  - Frame details are provided in addition to the packet payload



Packet analysis techniques

- **Pattern matching**
  - Identify packets of interest by matching specific values within the packet capture
- **Parsing protocol fields**
  - Extract the contents of particular protocol fields
- **Packet filtering**
  - Separate packets based on the values of fields in protocol metadata

Flow analysis

- Flow analysis is the practice of examining related groups of packets in order to:

  1. Identify patterns (e.g., repeated communications)

  2. Isolate suspicious activity and discard irrelevant data

  3. Analyse higher-layer protocols (e.g., reconstructing segment TCP packets and get the full picture of the protocol encapsulated in it: HTTP, SSL…)

  4. Extract data (e.g., a binary file to be analysed)

Flow analysis: what I need?

- Wireshark “Follow TCP Stream” feature

- Selecting any packet part of a TCP stream, Wireshark **reconstructs the full duplex contents of that steam from beginning to end**

- Conversations, transactions and file transfers that span multiple packets in a stream can be reconstructed **in their entirety**

- Only info that is contained **within the packet capture!**

Flow analysis techniques

- **List conversations and flows**
  - List all conversations and/or flows within a packet capture or only specific flows based on their characteristics.

- **Export a flow**
  - Isolate a flow or multiple flows, and store the flow(s) of interest to disk for further analysis

- **File and data carving**
  - Extract files or other data of interest from the reassembled flow

KRACK Attacks: Bypassing WPA2 against Android and Linux

Demonstration based on the paper

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

(CSS 2017)

Made by Mathy Vanhoef

www.krackattacks.com

See https://krackattacks.com/ for details

LAB time (EPISODE 1)

- Introduction to Linux and Scripting
- Even if you are familiar with Linux and Scripting, you need to attend the lab
- Specific commands for policy permissions will be explained
- Optional slide deck in KEATS for an intro to Linux