Radboud University

Computer Security

Network Security

Joan Daemen, Simona Samardjiska, and Katharina Kohls

November 25, 2020

Institute for Computing and Information Sciences
Radboud University Nijmegen

Outline

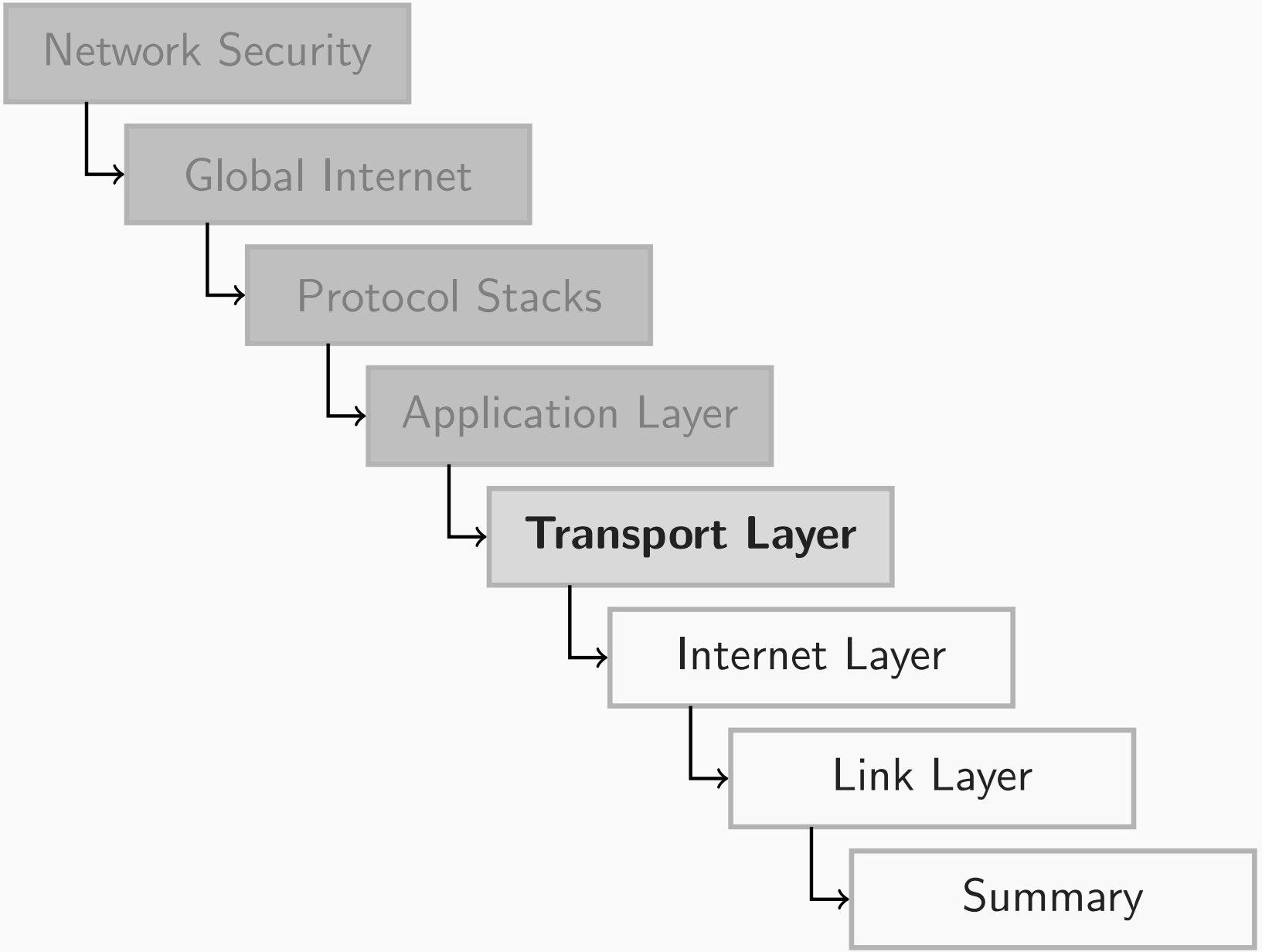
Network Security: Transport $\rightarrow$ Link

Anonymity Trilemma

Privacy Properties

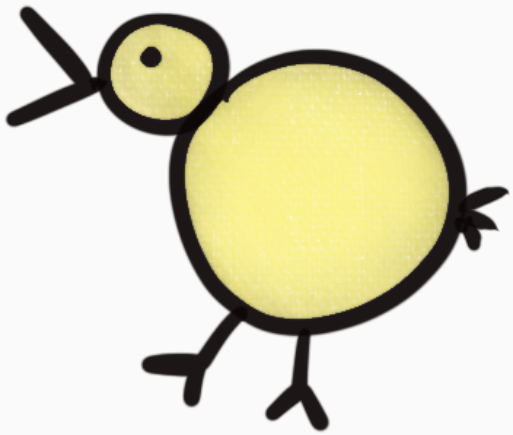
Tor - The Onion Router

Network Security: Transport $\rightarrow$ Link


Network Security
Global Internet
Protocol Stacks
Application Layer
Transport Layer
Internet Layer
Link Layer
Summary

What happens in this section?

- Quick definition of the Transport Layer
- End-to-end connections
- TCP and UDP
- Capturing traffic

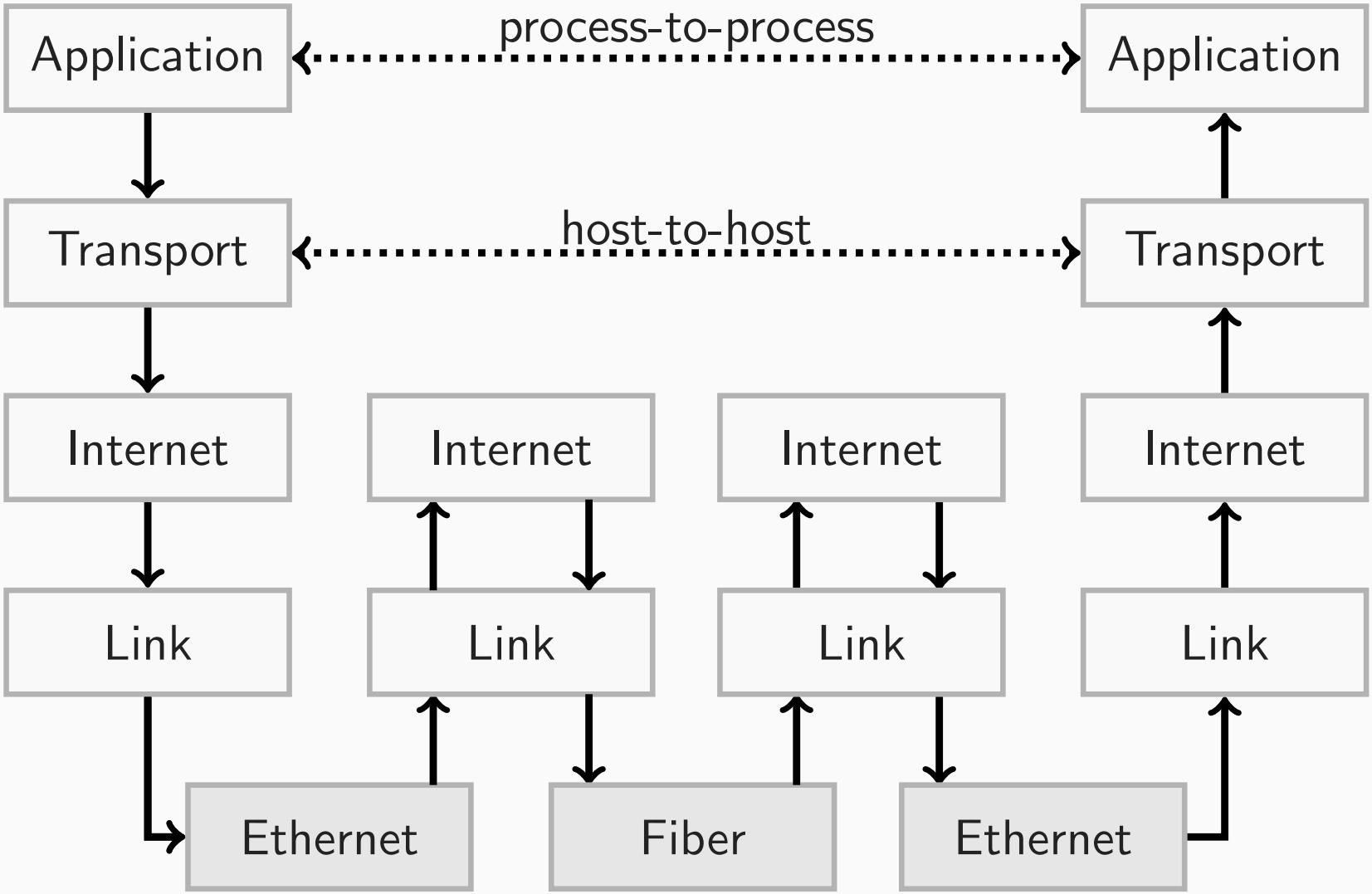


What is the Transport Layer?

End-to-End Message Transfer

- Establish data channels between two hosts of a connection
- Connection-oriented: `TCP`
- Connectionless: `UDP`
- Different features like
  error control, flow control, congestion control, ...
- Application addressing via port numbers

End-to-End Connections



End-to-End Connections

Transport Layer

- Connection established between hosts
- Example: Client and Server
  - Direct *logical* connection
  - Error correction etc. on this connection

Important: Connections have multiple *hops*. These hops are on the Internet Layer.

TCP

provides *reliable*, *ordered*, and *error-checked* data transmission between two applications on separate hosts.

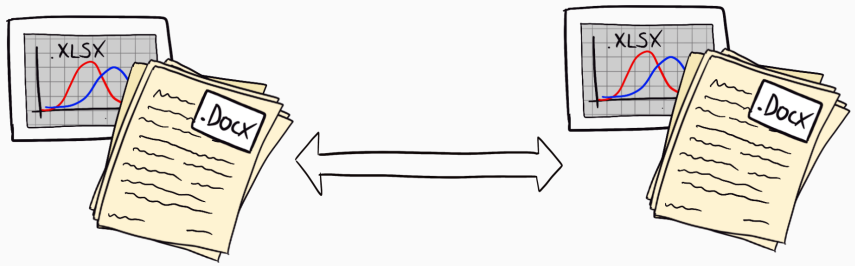
Features

- Reliable: The receive acknowledges received data, the sender can retransmit missing data.
- Ordered: Packets have sequence numbers that help to keep the original order.
- Error-Checked: Simple error detection and correction

When do we need TCP?

When you really want to be sure that everything arrived.

Example: Sending experimental results where every number must be correct.



Pro: Reliable!

Con: Slower...

UDP

UDP

is a connectionless protocol that delivers data with best effort and without any guarantees.

Features

- Connectionless: No static connection opened and closed
- Best Effort: If it gets there fine. If not, who cares?
- Low overhead: No expensive checksums, no responses, no heavy connection establishment.

When do we need UDP?

When some errors are acceptable.

Example: Having a Zoom lecture.

Pro: Fast!

Con: Information loss...

Live Example

Recorded traffic contains sensitive information,

don't share it 😐

Don't just record people in your home network 🏠

Capturing Traffic

Requirements:

- Run as root
- Install `tcpdump` (pre-installed standard tool)
- Install Wireshark

What happens next?

- Select interface
- Record traffic
- Analyze in Wireshark

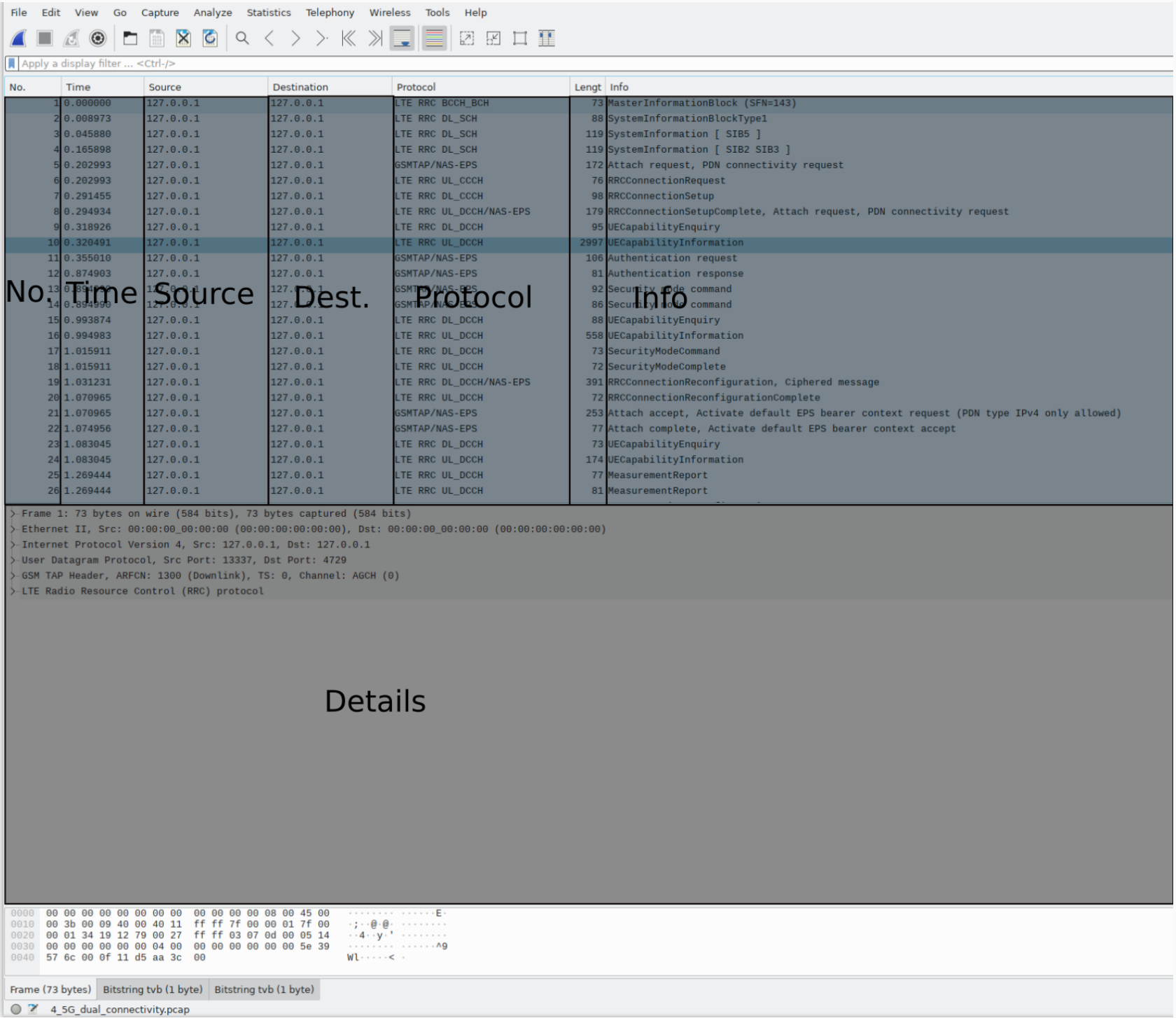
Capture Steps

List interfaces:

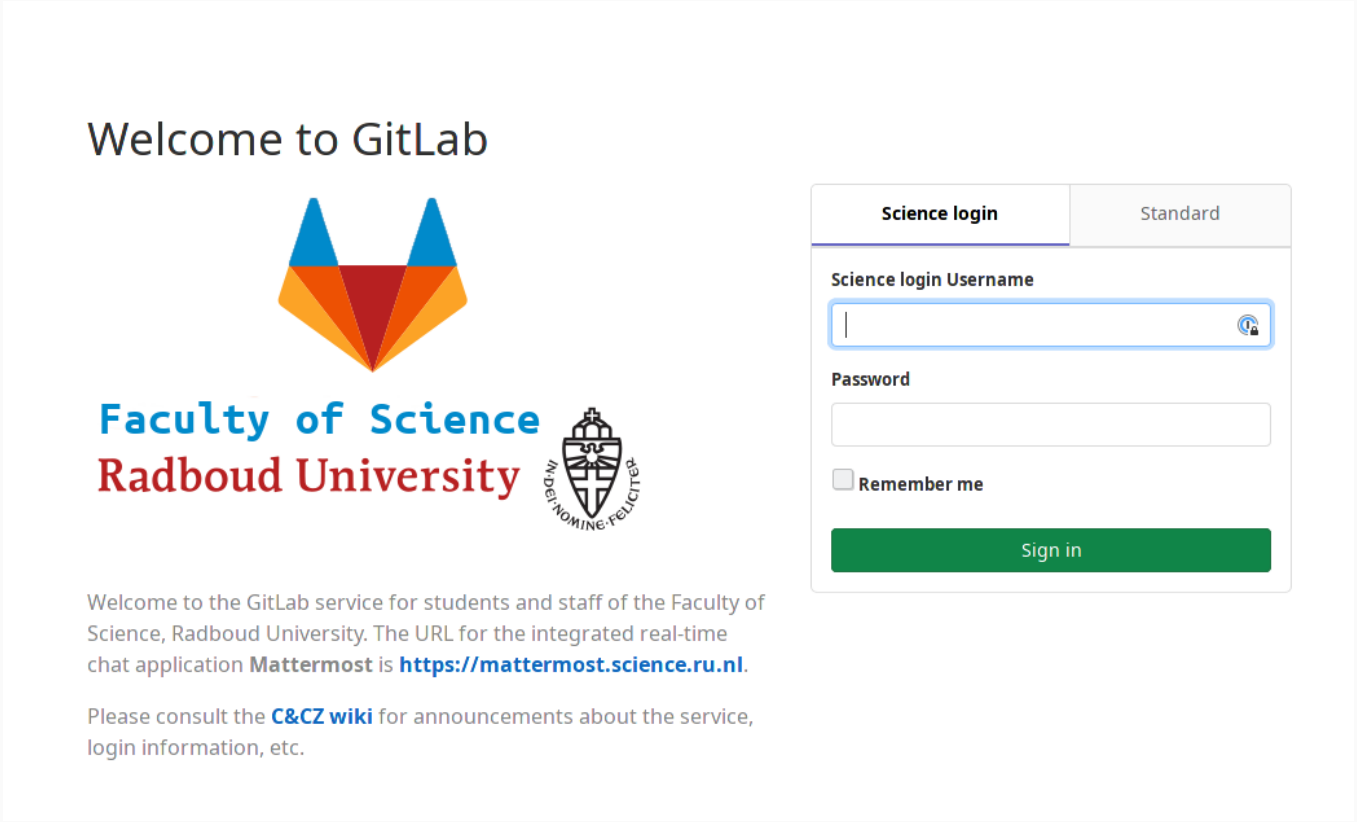
```
$ tcpdump -D
1.wlp0s20f3 [Up, Running]
2.enp0s31f6 [Up, Running]
3.lo [Up, Running, Loopback]
...
```

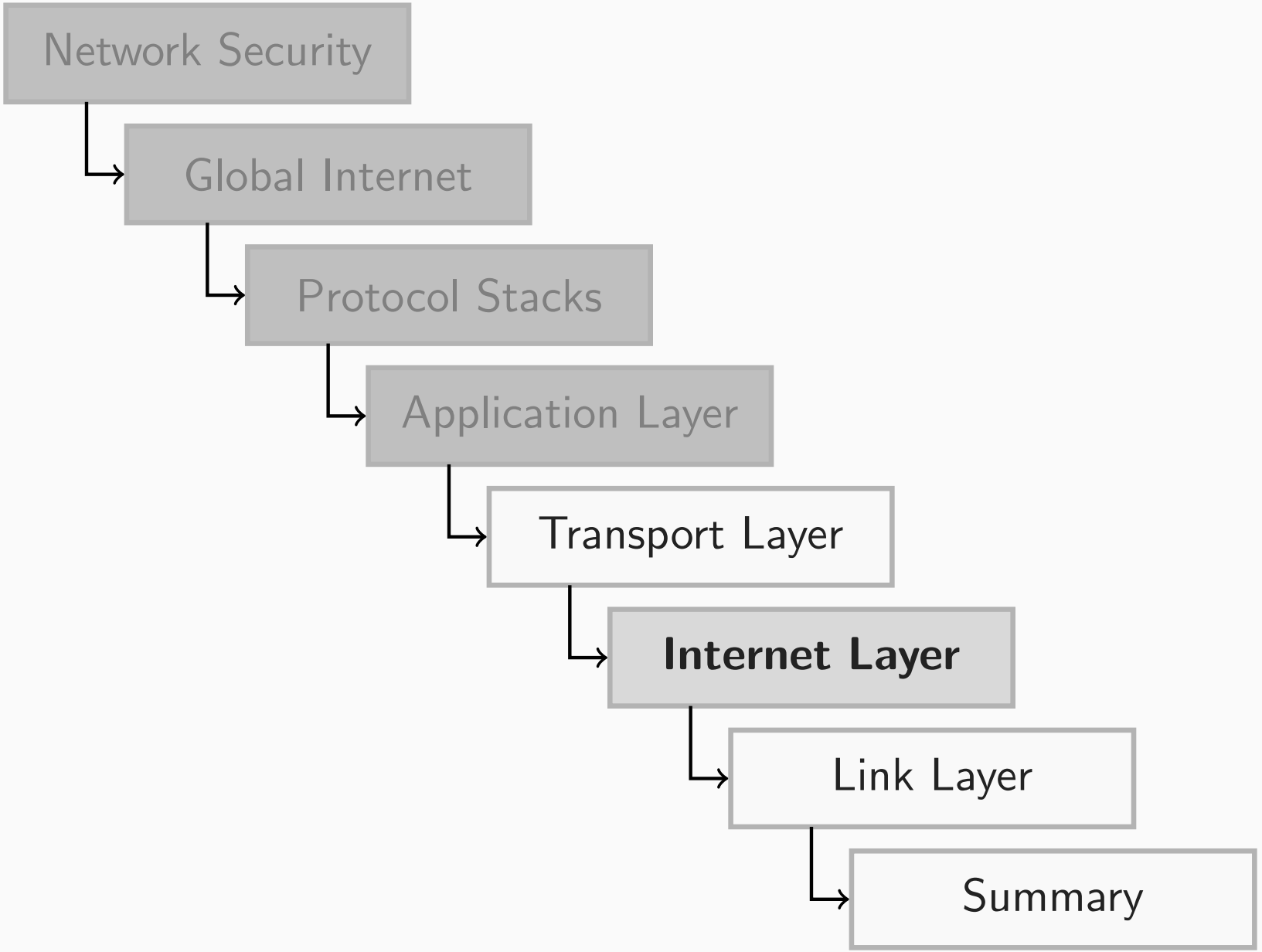
Capture Traffic:

```
sudo tcpdump -i enp0s31f6 -w test.pcap
```


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Lengt Info
1 0.000000 127.0.0.1 127.0.0.1 LTE RRC BCCH_BCH 73 MasterInformationBlock (SFN=143)
2 0.008973 127.0.0.1 127.0.0.1 LTE RRC DL_SCH 88 SystemInformationBlockType1
3 0.045880 127.0.0.1 127.0.0.1 LTE RRC DL_SCH 119 SystemInformation [SIB5]
4 0.165898 127.0.0.1 127.0.0.1 LTE RRC DL_SCH 119 SystemInformation [SIB2 SIB3]
5 0.202993 127.0.0.1 127.0.0.1 GSMTAP/NAS-EPS 172 Attach request, PDN connectivity request
6 0.202993 127.0.0.1 127.0.0.1 LTE RRC UL_CCCH 76 RRCConnectionRequest
7 0.291455 127.0.0.1 127.0.0.1 LTE RRC DL_CCCH 98 RRCConnectionSetup
8 0.294934 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH/NAS-EPS 179 RRCConnectionSetupComplete, Attach request, PDN connectivity request
9 0.318926 127.0.0.1 127.0.0.1 LTE RRC DL_DCCH 95 UECapabilityEnquiry
10 0.320491 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 2997 UECapabilityInformation
11 0.355010 127.0.0.1 127.0.0.1 GSMTAP/NAS-EPS 106 Authentication request
12 0.874903 127.0.0.1 127.0.0.1 GSMTAP/NAS-EPS 81 Authentication response
15 0.993874 127.0.0.1 127.0.0.1 LTE RRC DL_DCCH 88 UECapabilityEnquiry
16 0.994983 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 558 UECapabilityInformation
17 1.015911 127.0.0.1 127.0.0.1 LTE RRC DL_DCCH 73 SecurityModeCommand
18 1.015911 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 72 SecurityModeComplete
19 1.031231 127.0.0.1 127.0.0.1 LTE RRC DL_DCCH/NAS-EPS 391 RRCConnectionReconfiguration, Ciphered message
20 1.070965 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 72 RRCConnectionReconfigurationComplete
21 1.070965 127.0.0.1 127.0.0.1 GSMTAP/NAS-EPS 253 Attach accept, Activate default EPS bearer context request (PDN type IPv4 only allowed)
22 1.074956 127.0.0.1 127.0.0.1 GSMTAP/NAS-EPS 77 Attach complete, Activate default EPS bearer context accept
23 1.083045 127.0.0.1 127.0.0.1 LTE RRC DL_DCCH 73 UECapabilityEnquiry
24 1.083045 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 174 UECapabilityInformation
25 1.269444 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 77 MeasurementReport
26 1.269444 127.0.0.1 127.0.0.1 LTE RRC UL_DCCH 81 MeasurementReport
Frame 1: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 13337, Dst Port: 4729
GSM TAP Header, ARFCN: 1300 (Downlink), TS: 0, Channel: AGCH (0)
LTE Radio Resource Control (RRC) protocol
Details
0000 00 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00
0010 00 3b 00 09 40 00 40 11 ff ff 7f 00 00 01 7f 00
0020 00 01 34 19 12 79 00 27 ff ff 03 07 0d 00 05 14
0030 00 00 00 00 00 00 04 00 00 00 00 00 00 5e 39
0040 57 6c 00 0f 11 d5 aa 3c 00
Frame (73 bytes)
Bitstring tvb (1 byte)
Bitstring tvb (1 byte)
4_5G_dual_connectivity.pcap

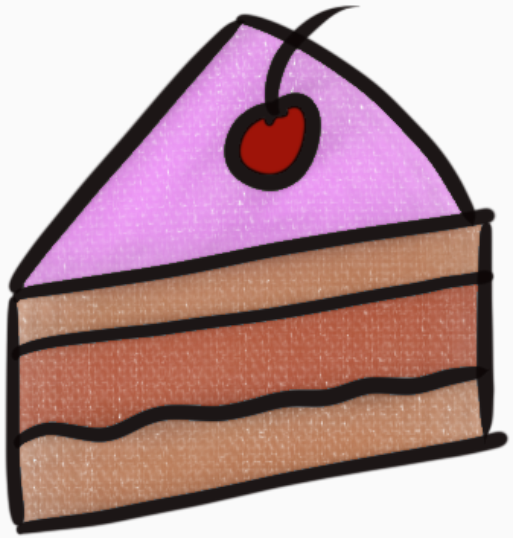
```
whois 131.174.16.187
```




Network Security
Global Internet
Protocol Stacks
Application Layer
Transport Layer
Internet Layer
Link Layer
Summary

What happens in this section?

- Quick definition of the Internet Layer
- Hop-to-hop connections
- Traceroute
- Timing



What is the Internet Layer?

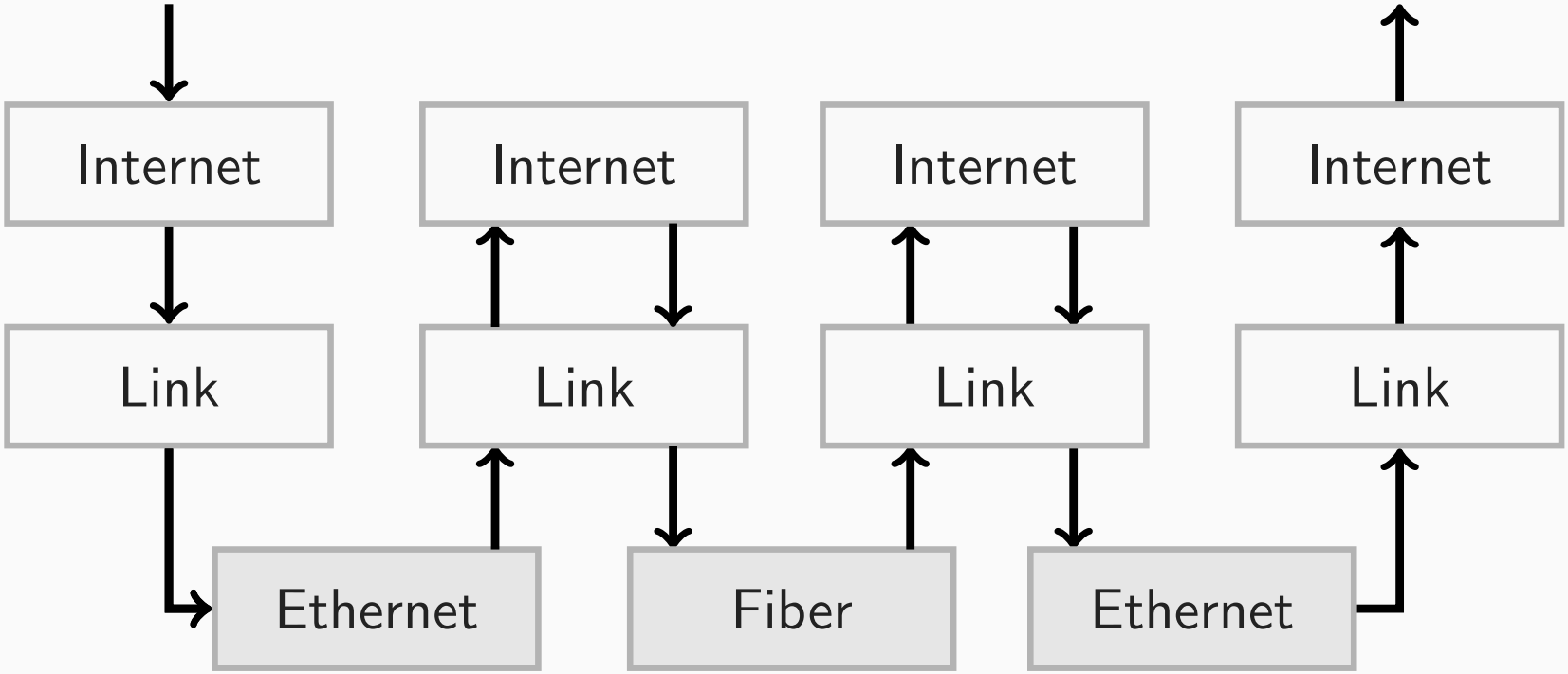
The Internet Layer

transports network packets across network boundaries.

Protocols

- Internet Protocol (`IPv4`, `IPv6`)
- Internet Control Message Protocol (`ICMP`)
- ...

IP Connections



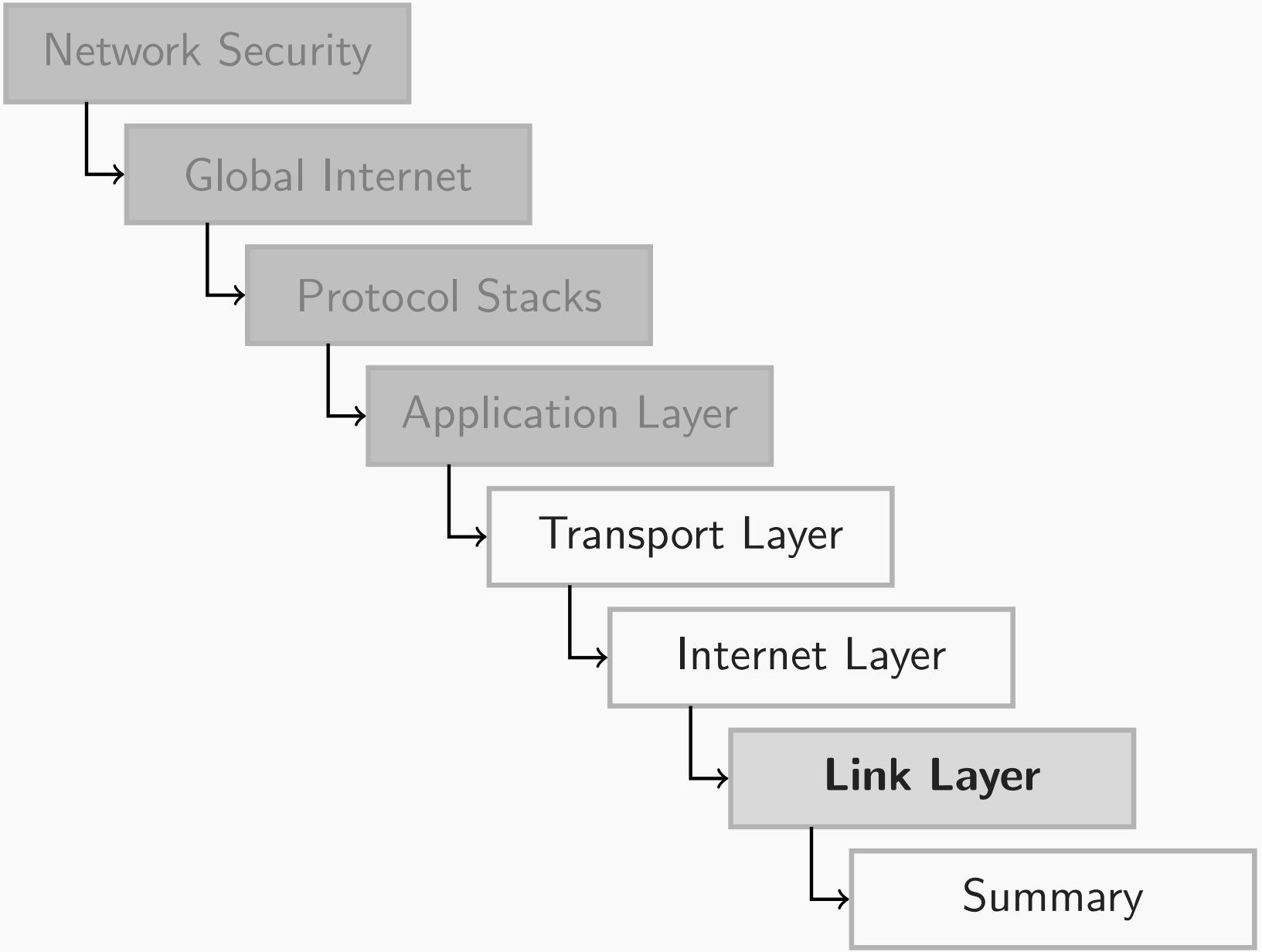
Reaching a WhatsApp Server

```
$ traceroute 157.240.11.53
 1..3 # my network
 4  217.161.69.141 # Vodafone
 5  ae33-xcr1.hex.cw.net (195.2.3.246)
 6  ae28-ucr1.pra.cw.net (195.2.10.82)
 7  ae29-xcr2.ash.cw.net (195.2.24.245)
 8  ae5-xcr2.lax.cw.net  (195.2.2.153)
 9  ae12.pr08.lax1.tfbnw.net (157.240.67.46) # Facebook
10  po108.psw03.lax3.tfbnw.net
11  157.240.39.25
12  whatsapp-cdn-shv-02-lax3.fbcdn.net (157.240.11.53)
```

Measuring Times

Measure the round trip time (RTT):

```
$ ping 157.240.11.53
PING 157.240.11.53 (157.240.11.53) 56(84) bytes of data.
64 bytes from 157.240.11.53: icmp_seq=1 time=140 ms
64 bytes from 157.240.11.53: icmp_seq=2 time=140 ms
64 bytes from 157.240.11.53: icmp_seq=3 time=140 ms
64 bytes from 157.240.11.53: icmp_seq=4 time=140 ms
64 bytes from 157.240.11.53: icmp_seq=5 time=139 ms
```


Network Security
Global Internet
Protocol Stacks
Application Layer
Transport Layer
Internet Layer
Link Layer
Summary

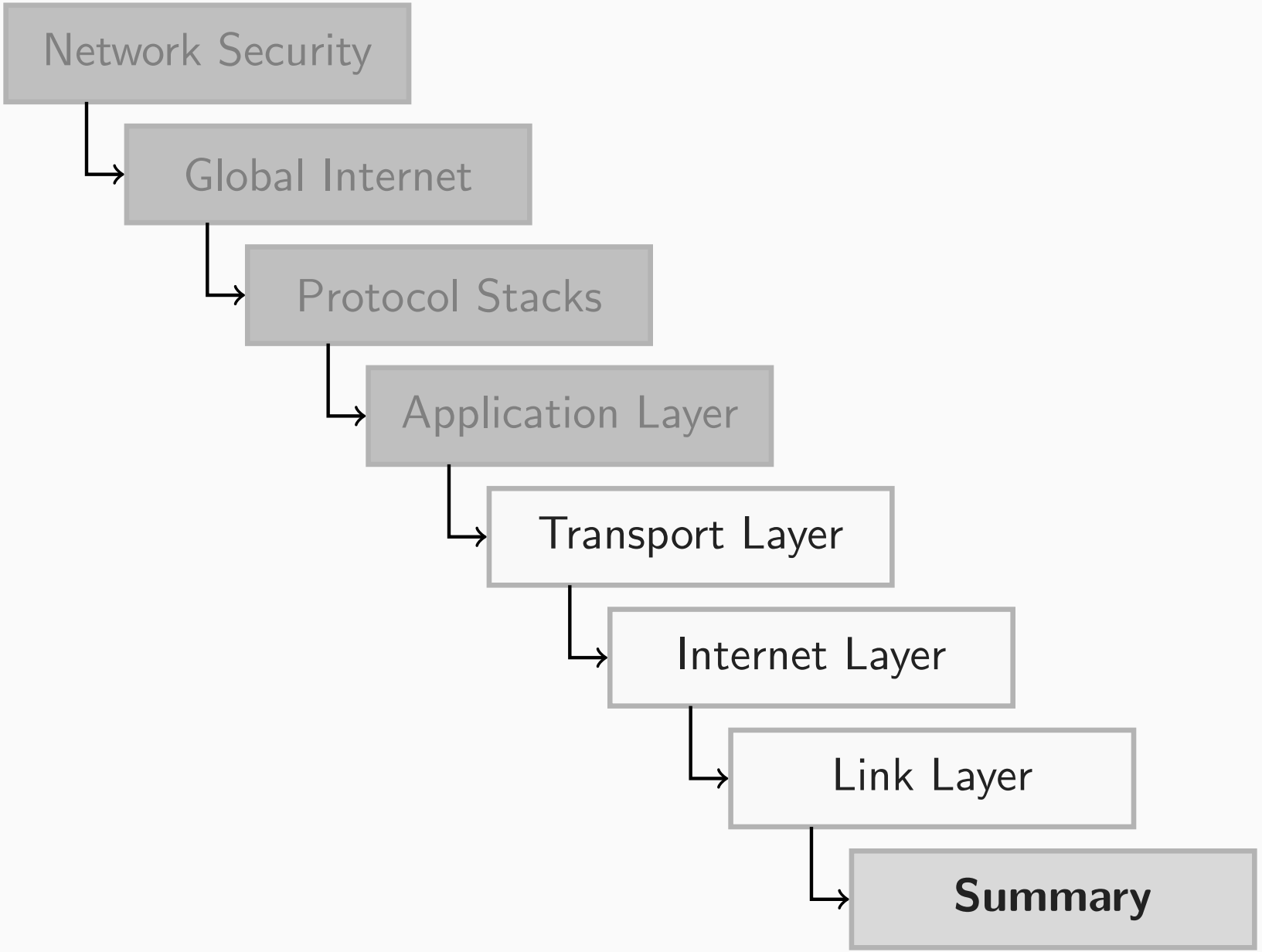
What is the Link Layer?

The Link Layer

provides the protocols to connect physical connections to the network.

Protocols

- Address Resolution Protocol (`ARP`)
- Medium Access Control (`MAC`)
- Point-to-Point Protocol (`PPP`)
- ...


Network Security
Global Internet
Protocol Stacks
Application Layer
Transport Layer
Internet Layer
Link Layer
Summary

Summary

We looked at:

- The Internet, the WWW, and what languages they speak
- The protocol stack to organize it all
- Application layer: Helping the user
- Transport layer: Establishing end-to-end connections
- Internet layer: Transport packets
- Link Layer: Connect to physical medium

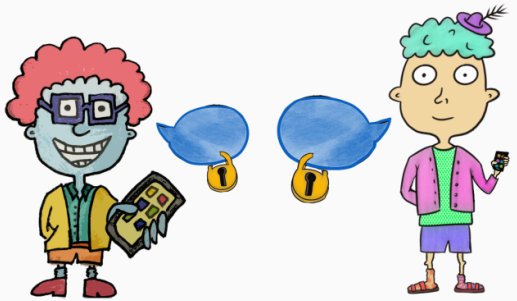
Privacy and Anonymity

What is the difference between privacy and anonymity?

Protection of Data

Internet *privacy* is the *privacy* and security level of personal data published via the Internet.

Private Communication: Alice and Bob communicate and don't want to share the conversation with the provider.

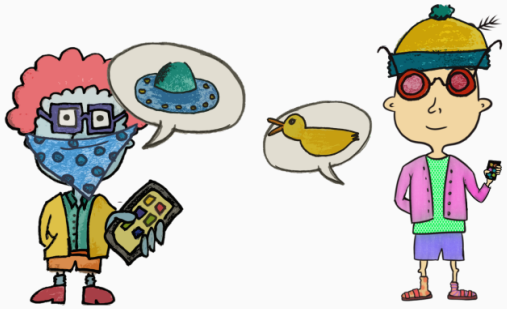


Anonymity

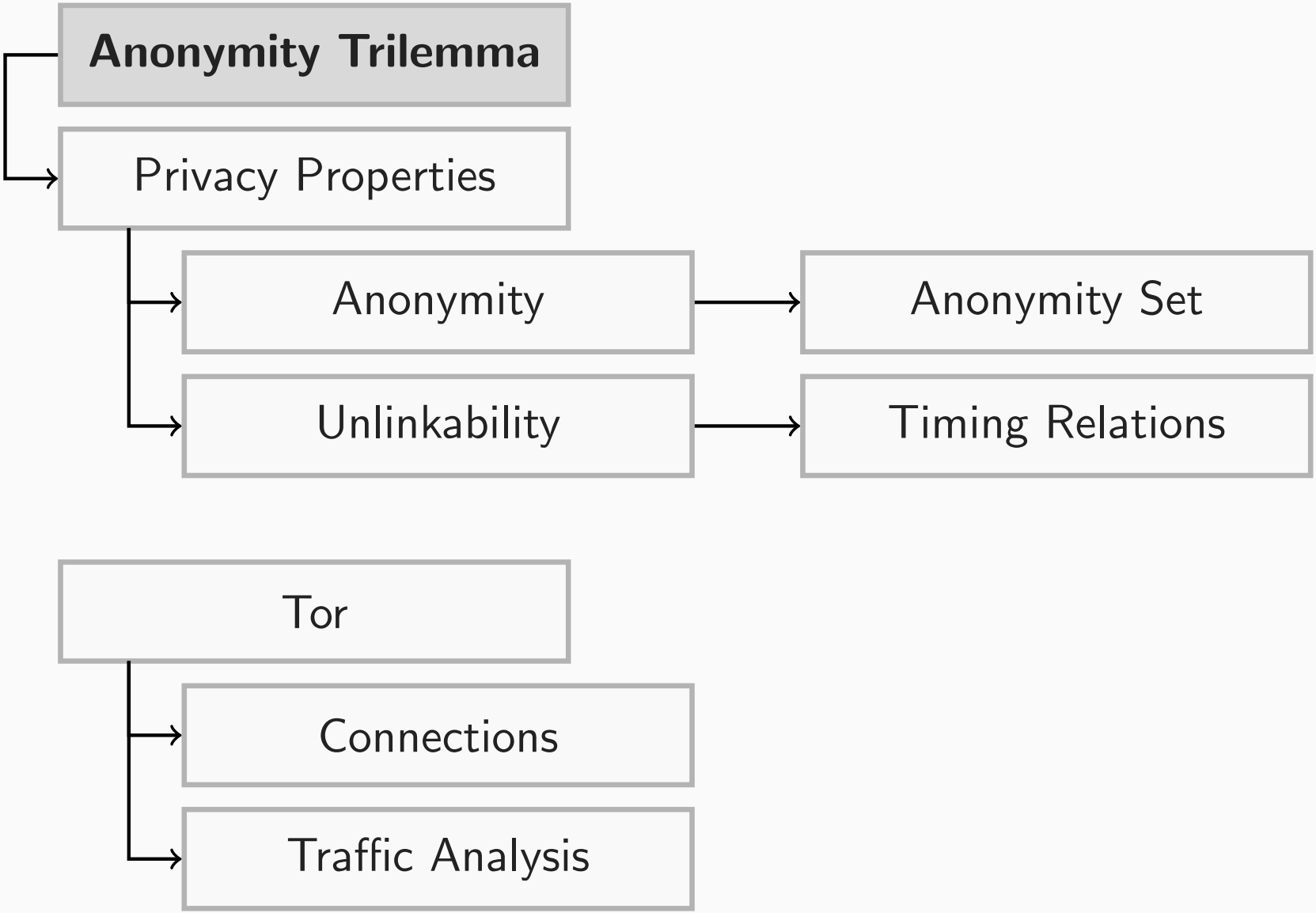
Protection of Identities

Anonymity is the state of being not identifiable within a set of subjects, the *anonymity set*.

Anonymous Communication: Alice and Bob communicate and don't want the provider to know it's them.



Anonymity Trilemma


Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

The Good, the Bad and the Ugly

Intentions:

- I want tickets to the [very bad artist] concert.
  Google shouldn't know it's me.
- I want to tell the teacher that the slides are too colorful.
  The teacher shouldn't know me.
- I want to share secret documents about [very bad corp.].
  The company shouldn't know it was me.

Even More Requirements

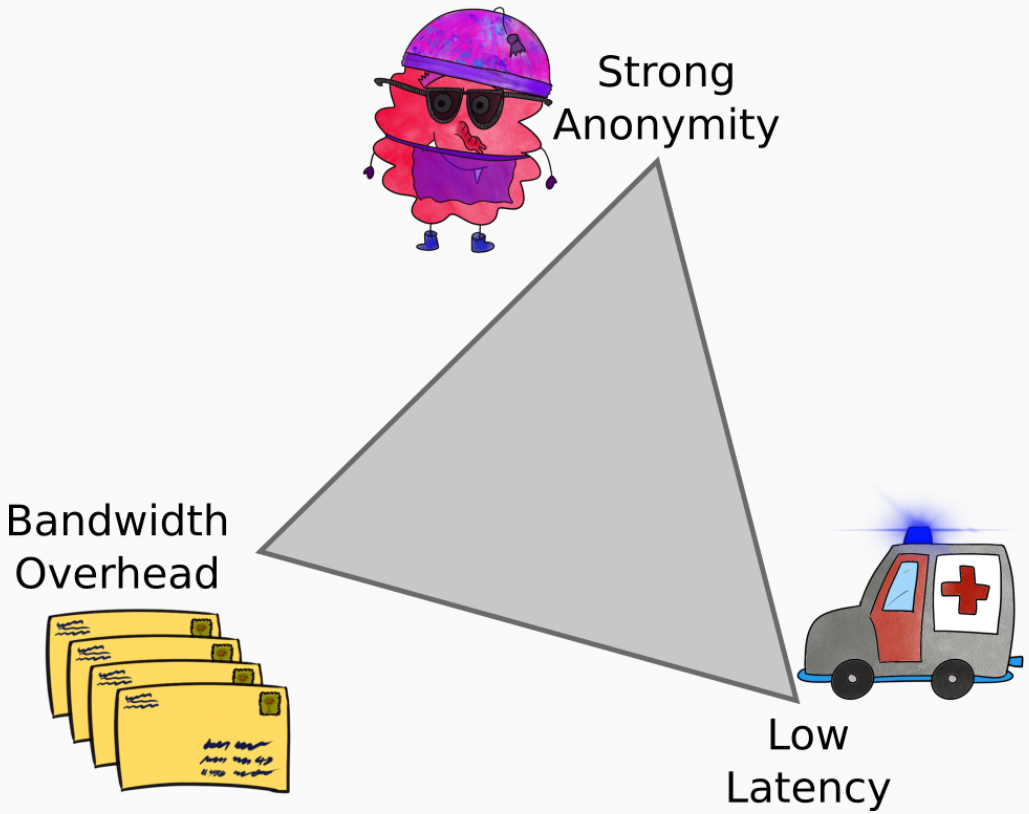
Different Intentions

Different performance requirements

- Browse the web without a 90s experience.
- A little more privacy can take some extra time, I can wait.
- I don't care if it takes two more days to share these documents.

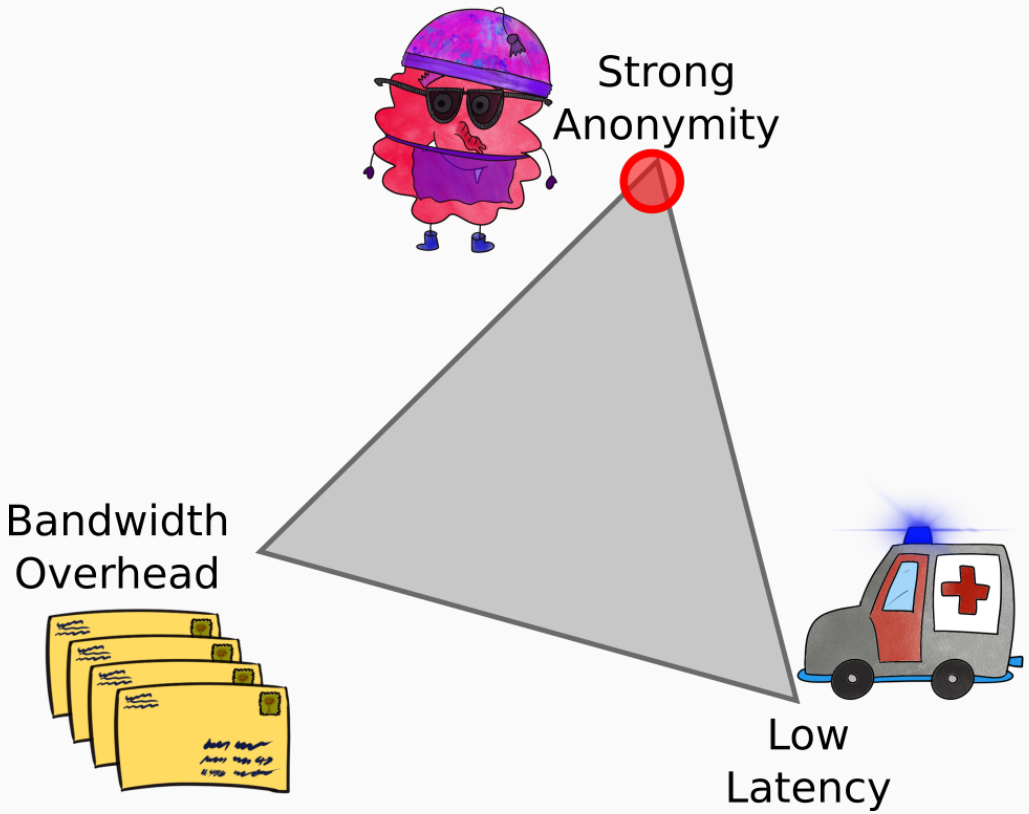
Anonymity Trilemma

Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two

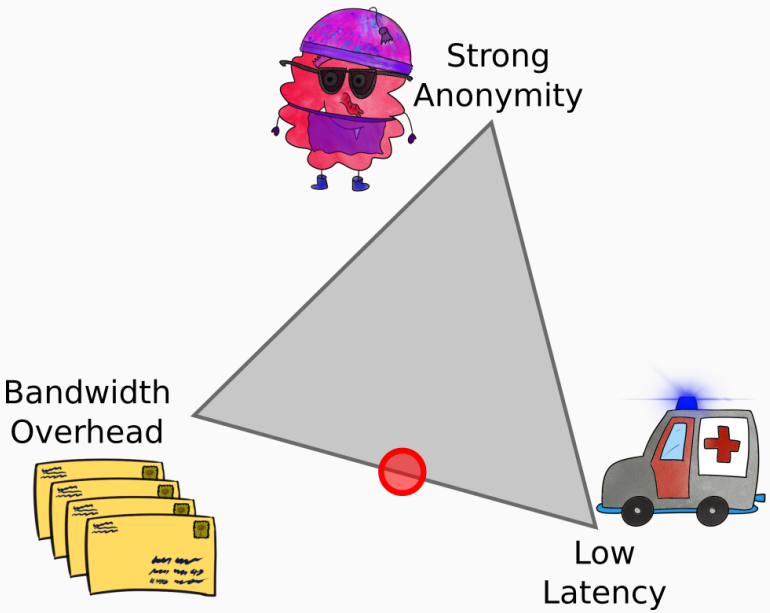


Anonymity Trilemma

Strong Anonymity, Low Bandwidth Overhead, Low Latency—Choose Two



Security versus Performance



- Real-world systems need performance
- Can only be achieved at the expense of security

→ **Security is limited by the performance we can achieve.**

→ **Practical systems cannot reach perfect security.**

Two Fundamental Problems

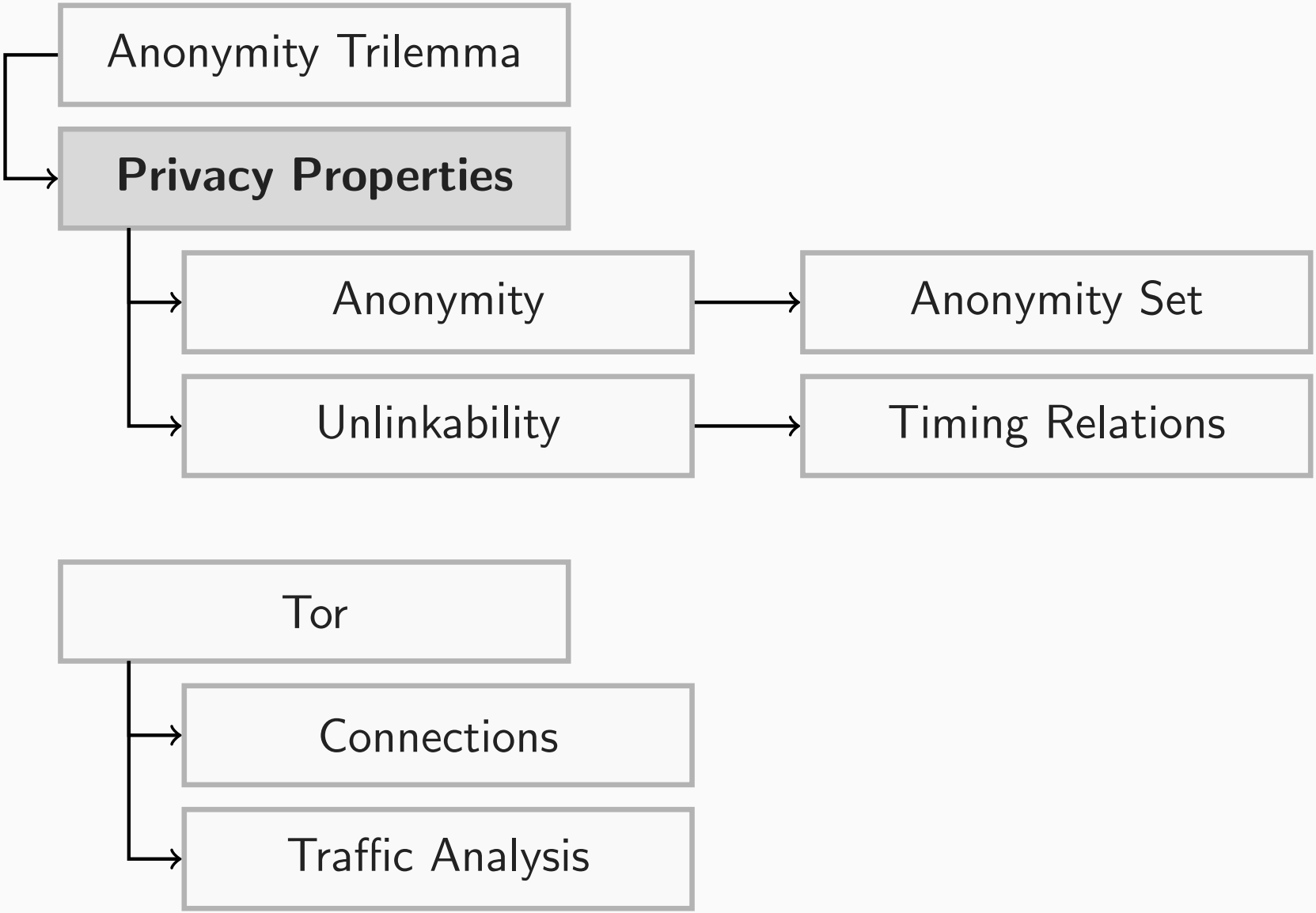
Drawing a straight line

- Users and authorities follow their interests
- Legal versus illegal is not always obvious

Security versus Performance

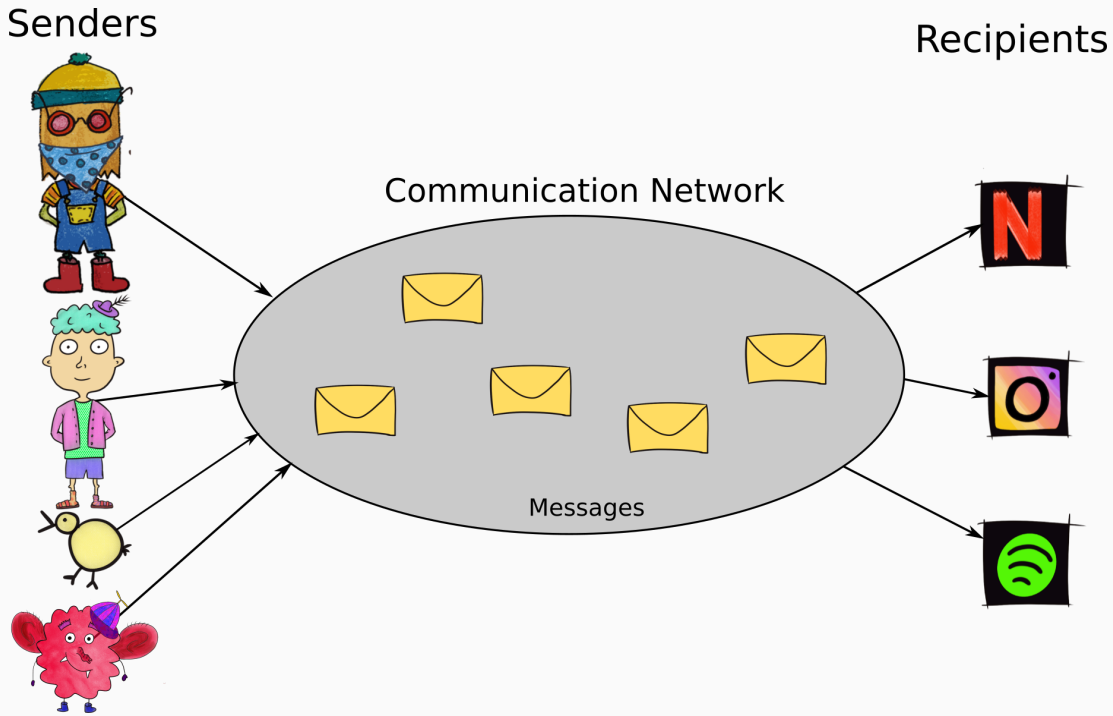
- Security is limited by the performance we need
- Leads to *persisting* attack vectors

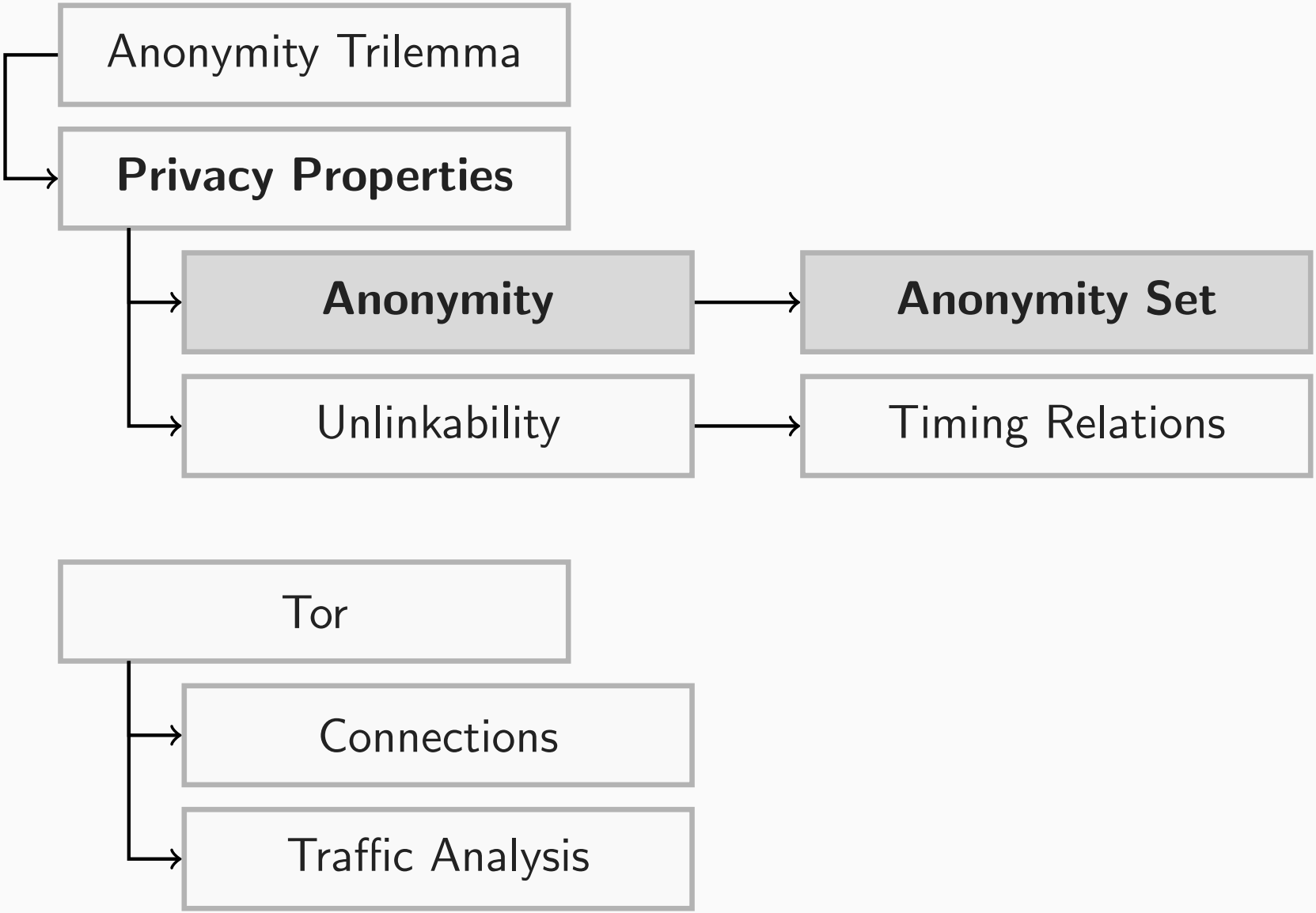
Privacy Properties


Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

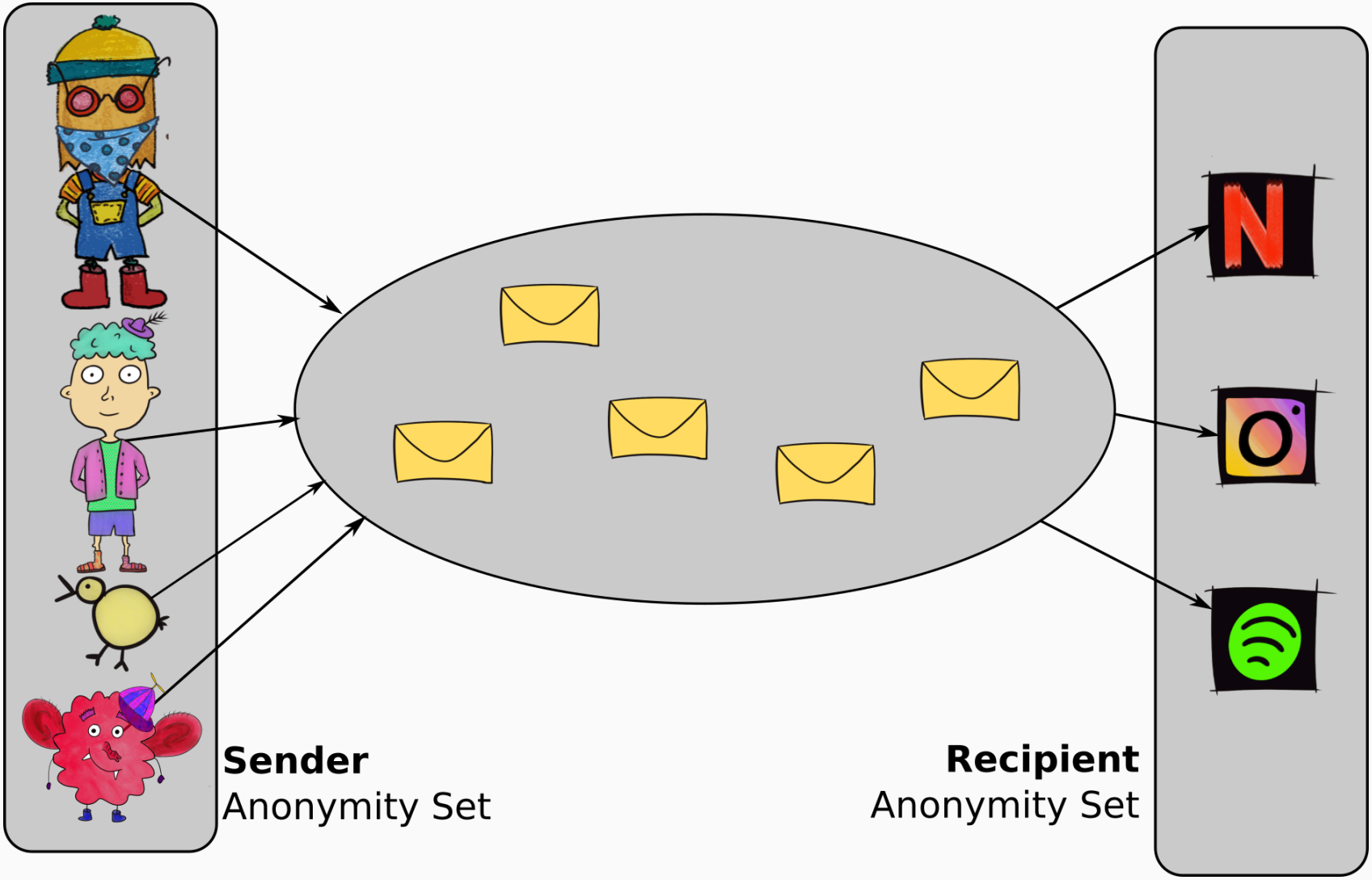
Technical Privacy Properties

- **Anonymity**
- Unlinkability
- Unobservability
- Undetectability
- Indistinguishability
- Pseudonymity
- Plausible deniability
- Location privacy

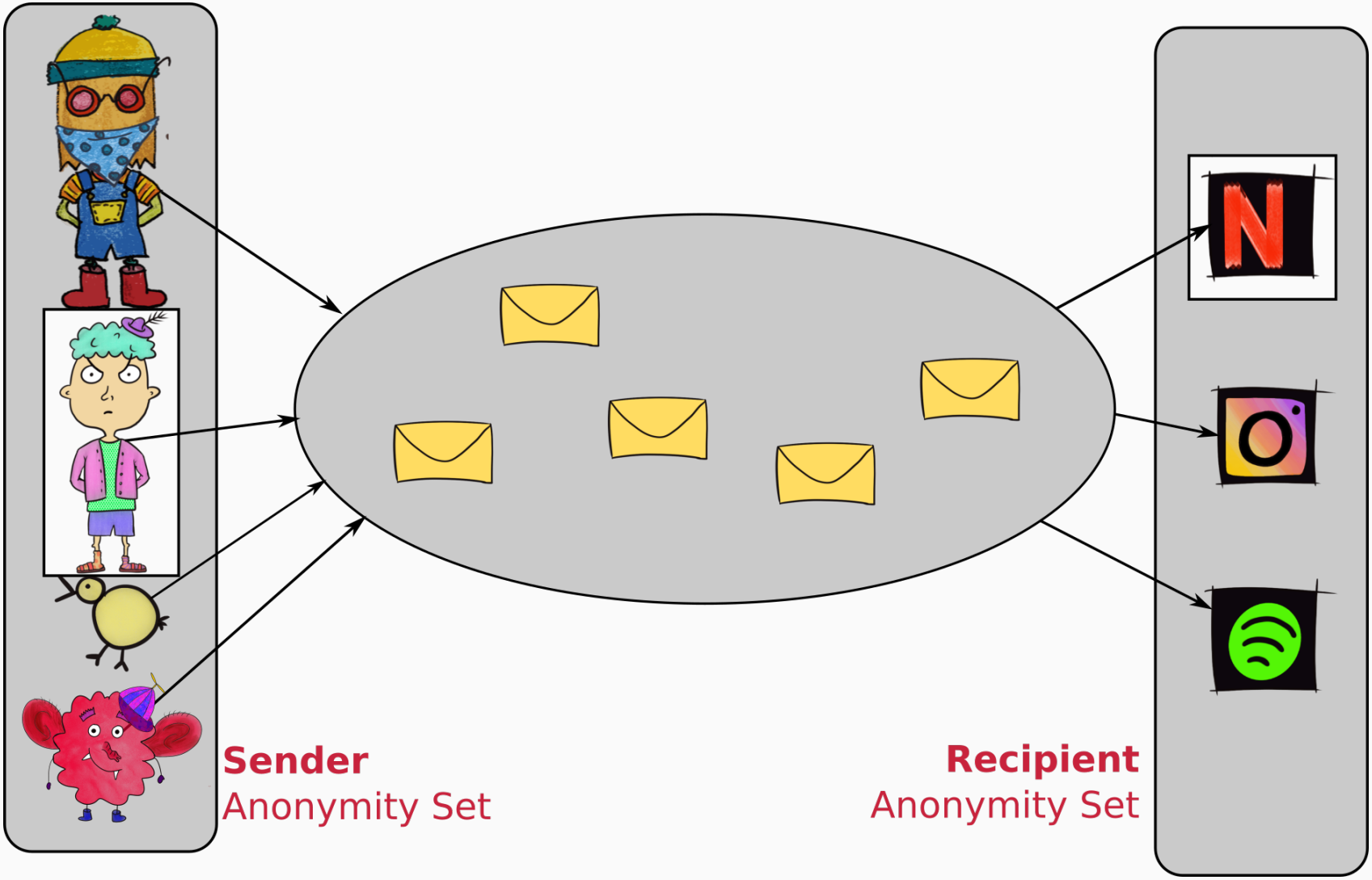



Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

Anonymity Set



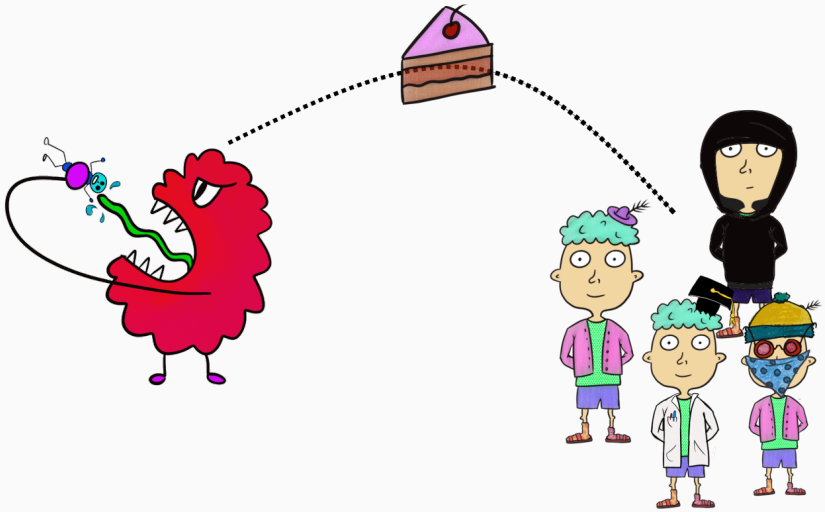
Infiltrated Anonymity Set



Hiding in the Anonymity Set

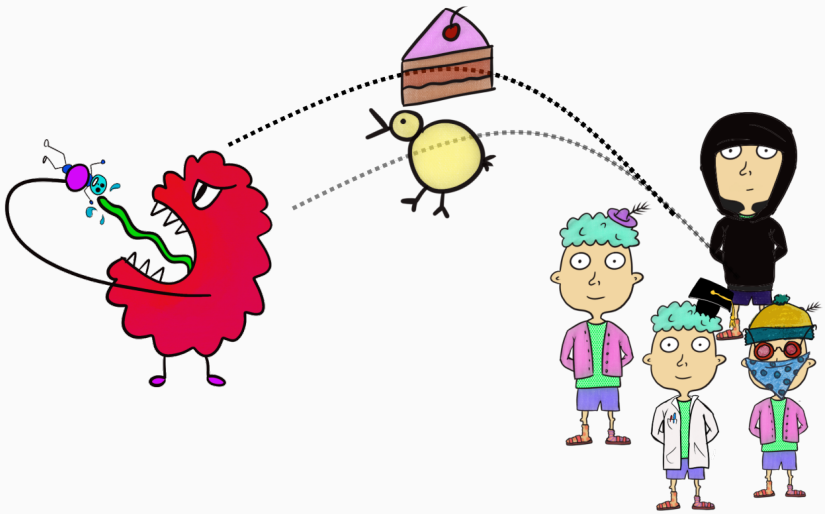
Hiding in Groups

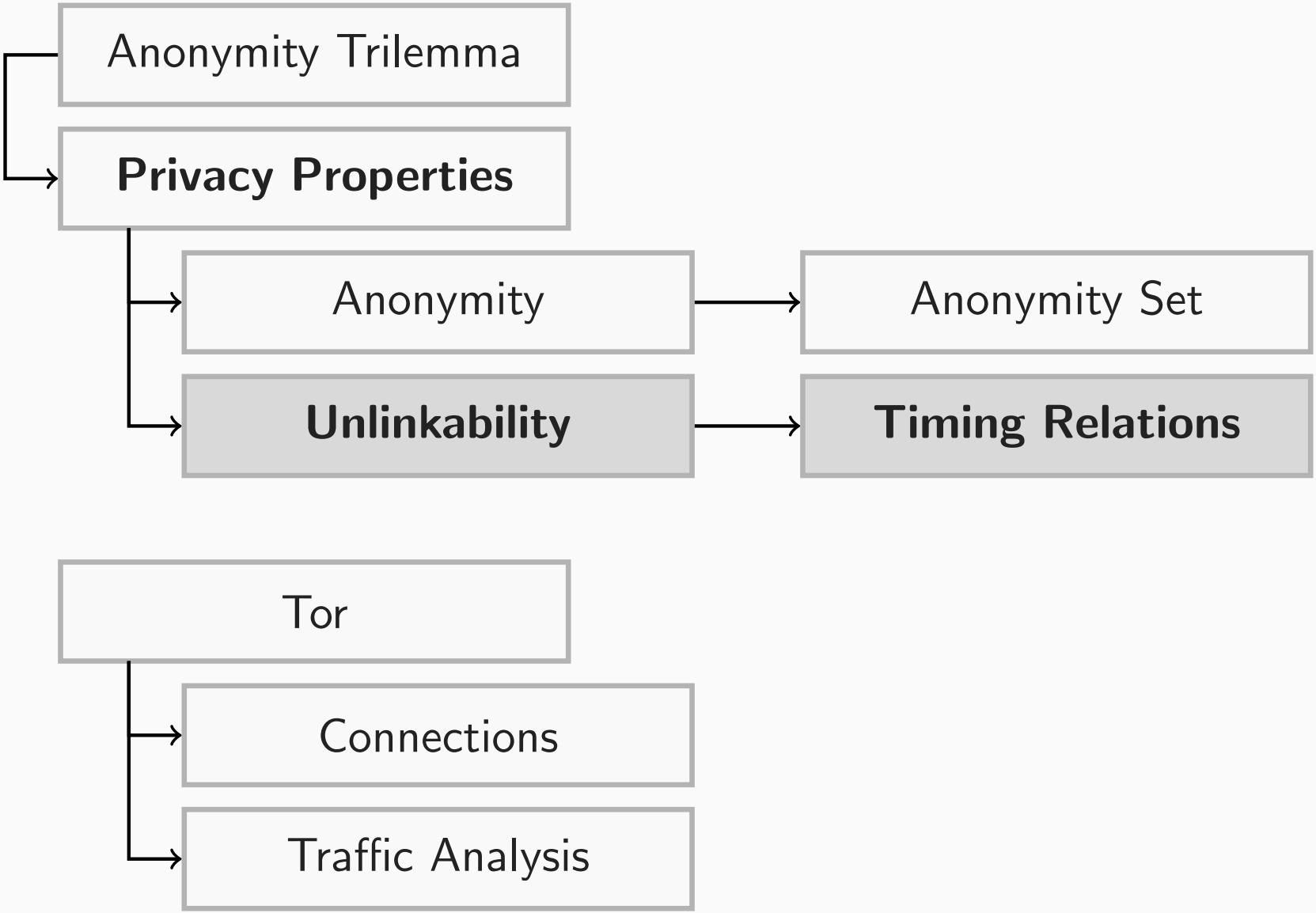
- Hide in the anonymity set:
- More items, more search



Being Uniform

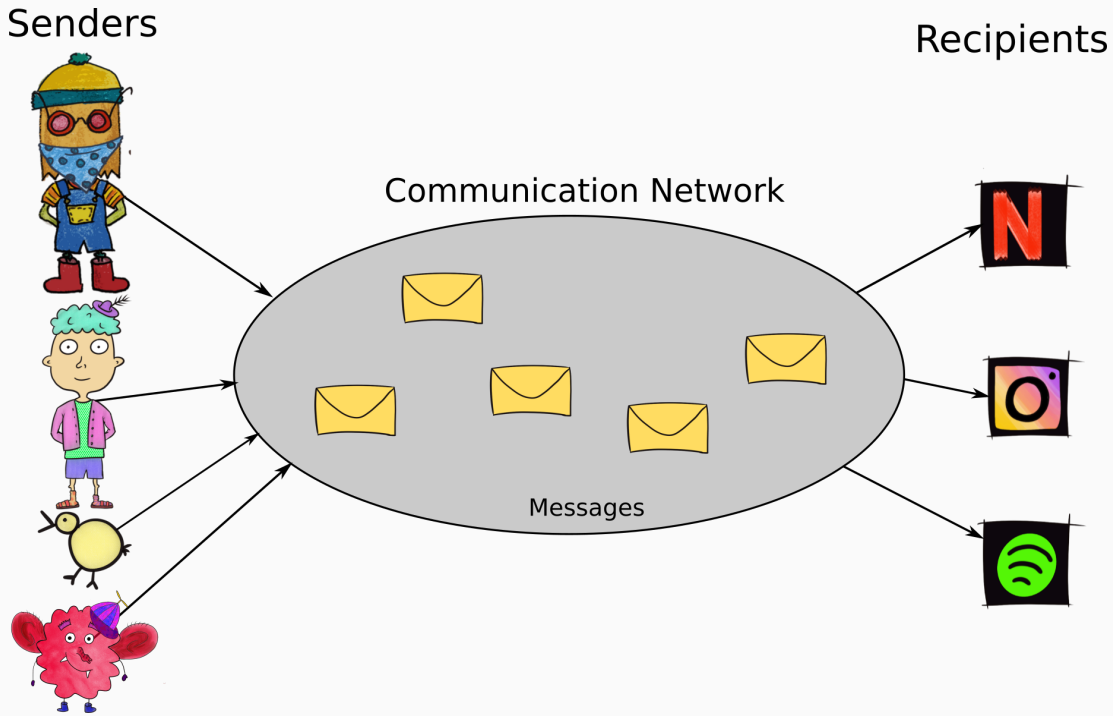
- Everyone must act the same
- Unique actions split the set



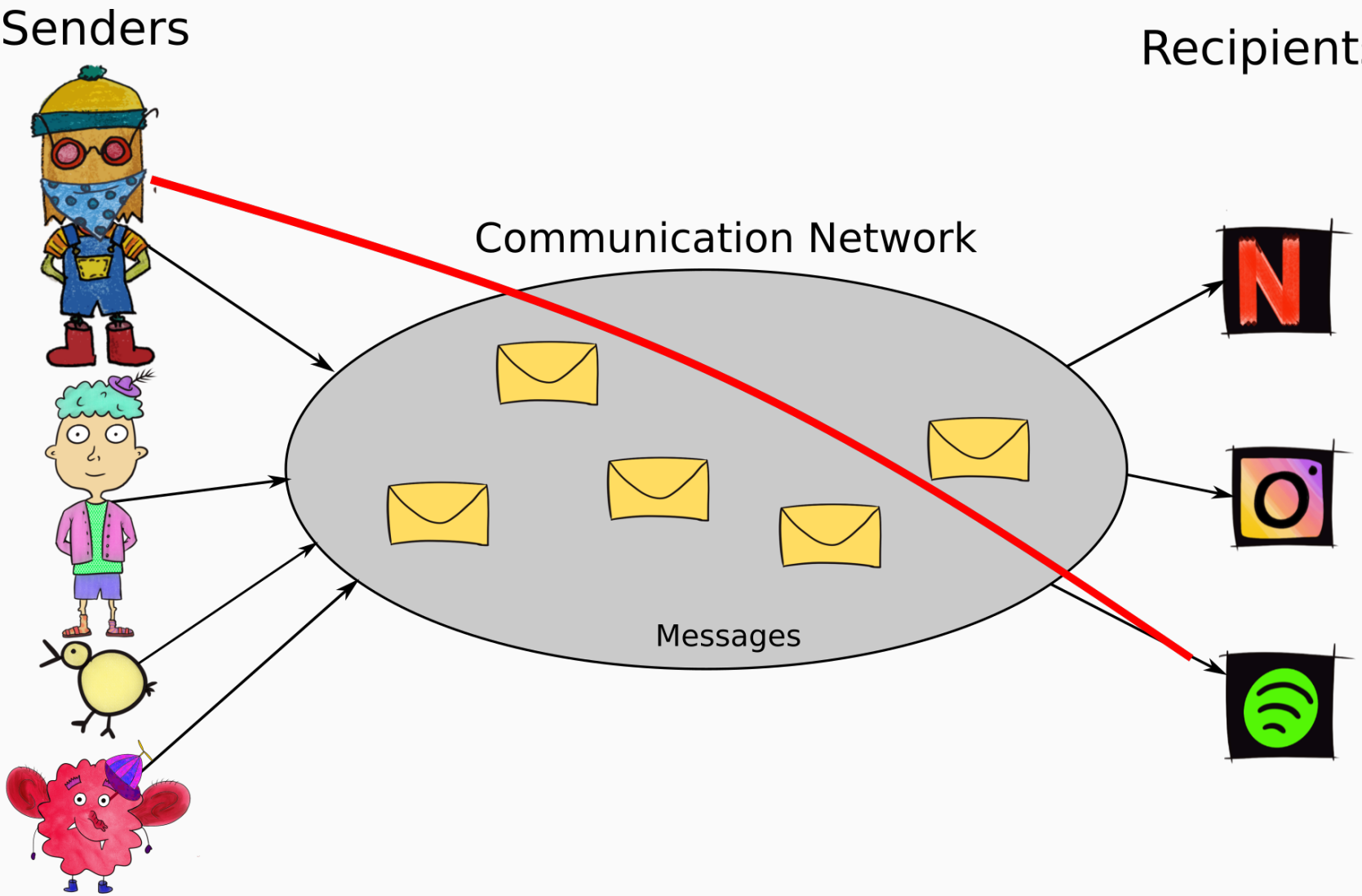

Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

Technical Privacy Properties

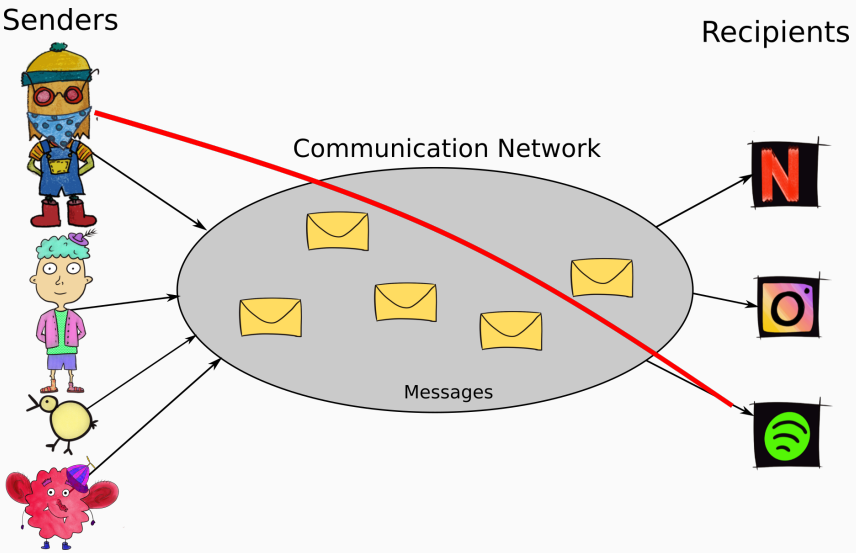
- Anonymity
- **Unlinkability**
- Unobservability
- Undetectability
- Indistinguishability
- Pseudonymity
- Plausible deniability
- Location privacy



Unlinkability



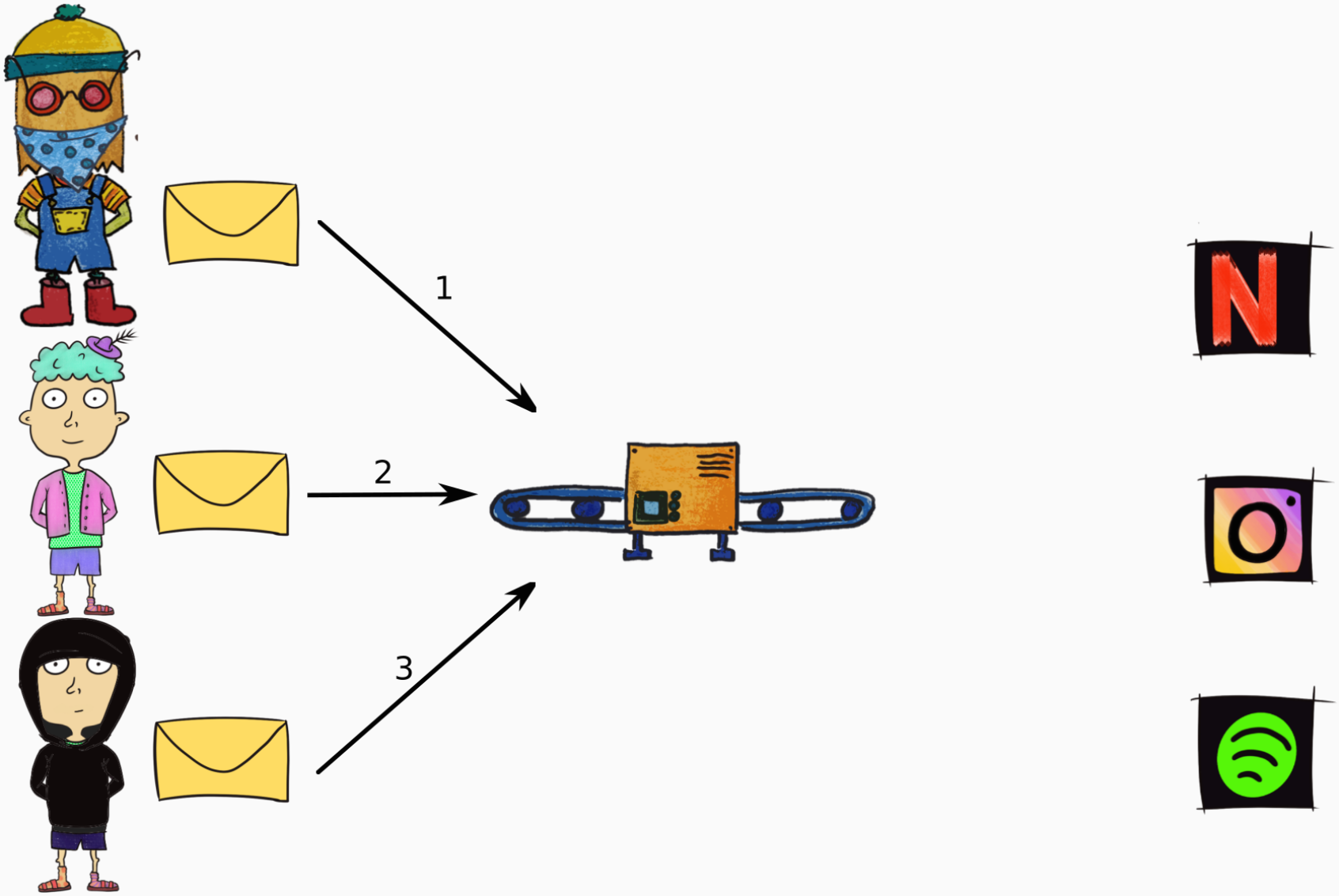
Types of Unlinkability



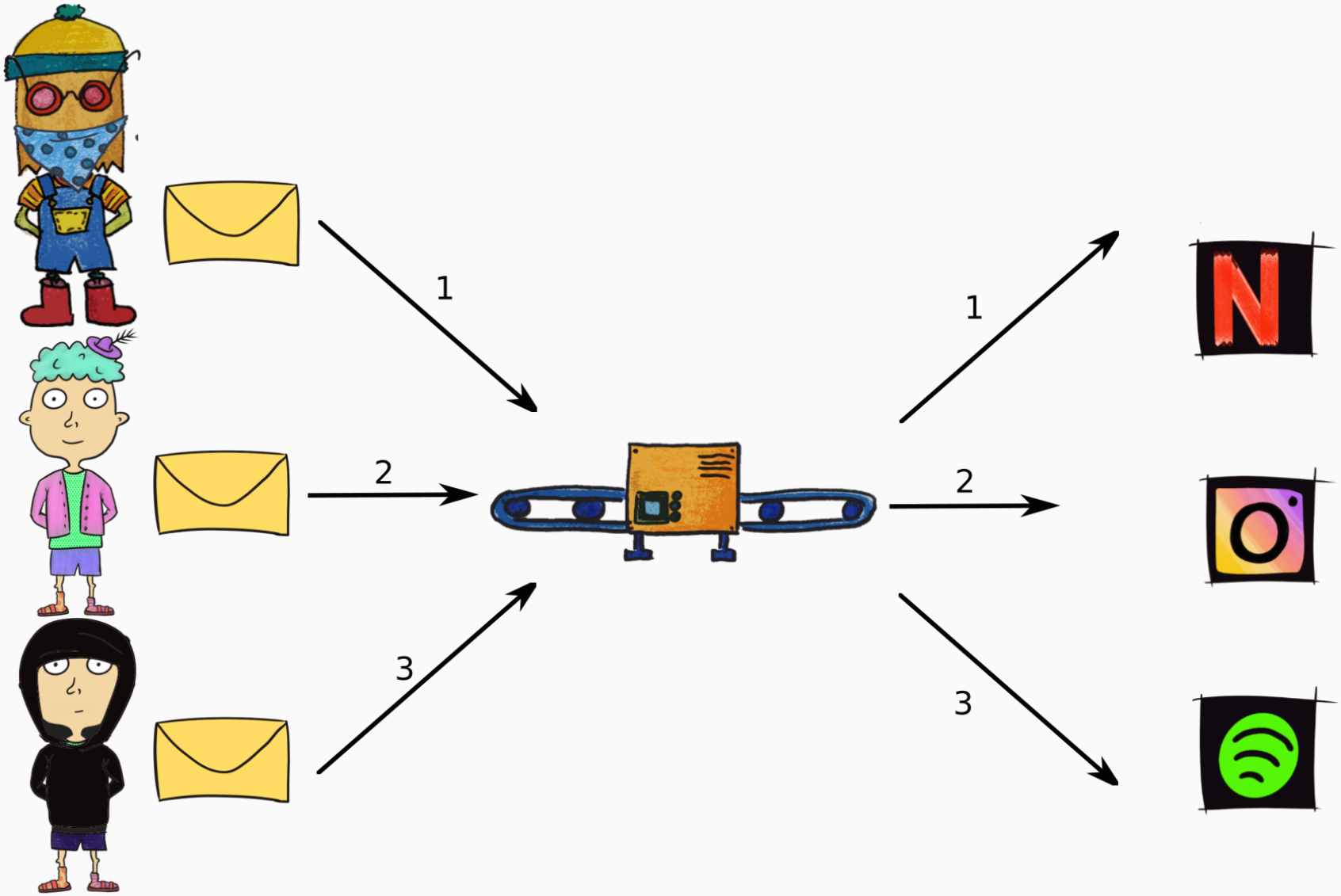
- **Sender Anonymity:** Message is unlinkable to the sender
- **Recipient Anonymity:** Message is unlinkable to the recipient
- **Relationship Anonymity:** Message is unlinkable to sender *and* recipient

Timing Relations

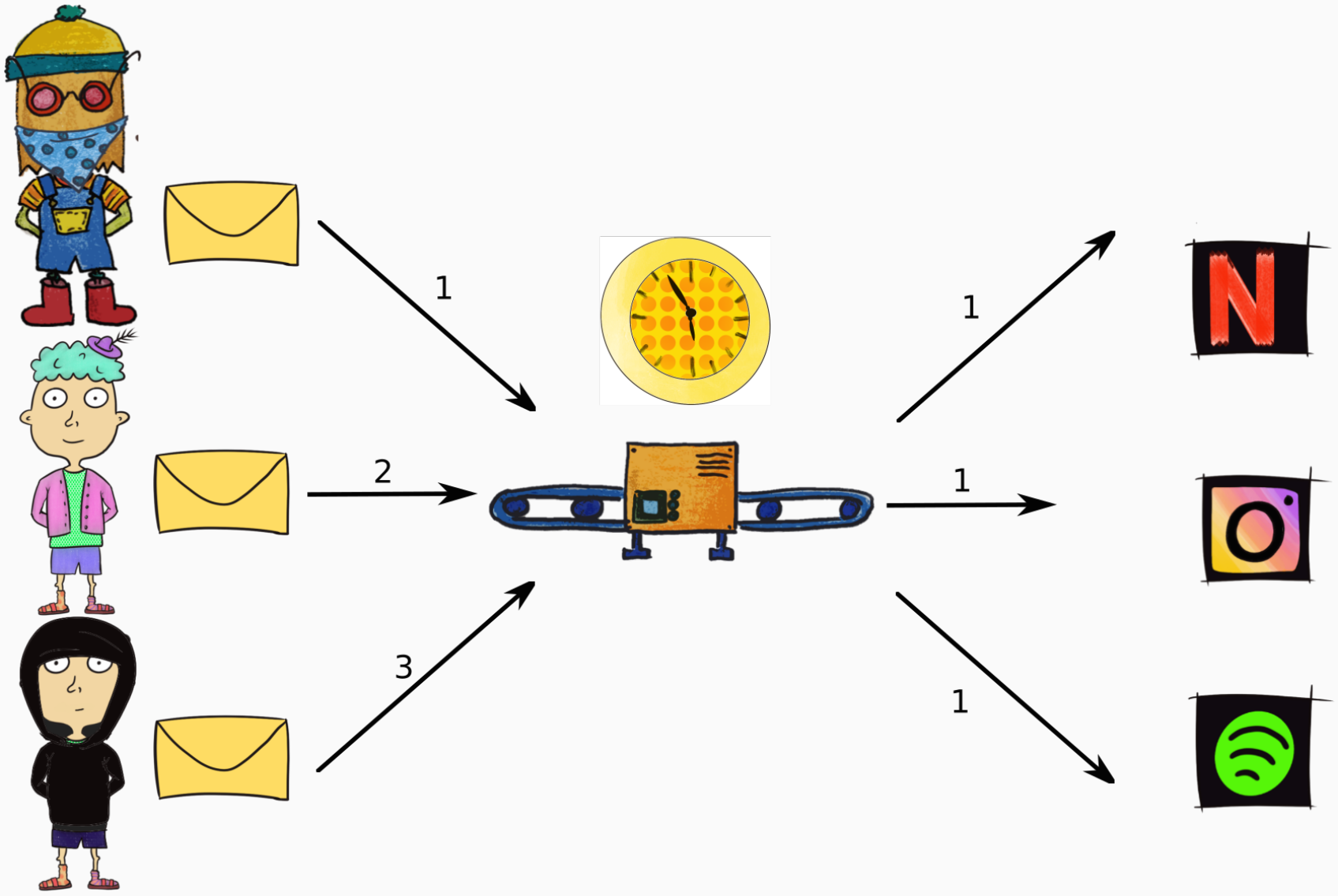
Timing Relations



Timing Relations



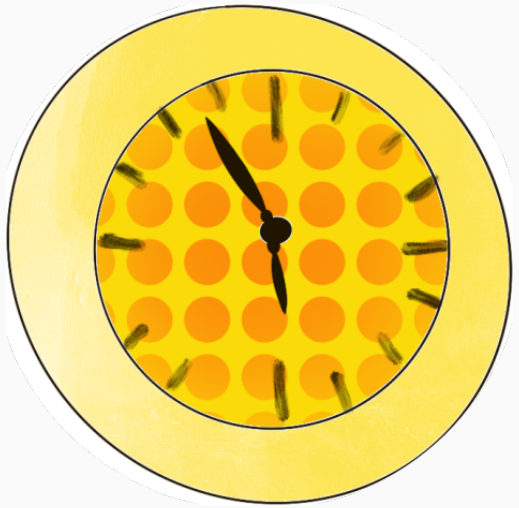
Timing Relations



Timing Relations

Timing versus Unlinkability:

- Timing relations can link sender and recipient
- Example: Ordering of transmissions
- Counter: Gather messages and send out all at once
- Pro: Destroys timing relations
- Con: Introduces delays



Mix Types

Pool and Batch Mixes

- Gather incoming messages
- Flush out when threshold is reached
- **Problem:** Attacker can flush mix with own messages!

Continuous Mixes

- Add a random delay to packets
- Send out each one after time passed
- **Problem:** Weak anonymity with low num. of messages!

Mixing: Summary

Problem: Timing reveals identities

Solution: Wait a while before sending

- Mixes provide anonymity by destroying time relations
- Different concepts exist:
  - Gather a certain number
  - Add random delays

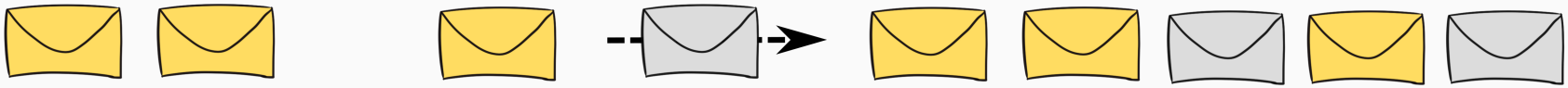
Mixes create high latency, classical use case is email.

Traffic Patterns

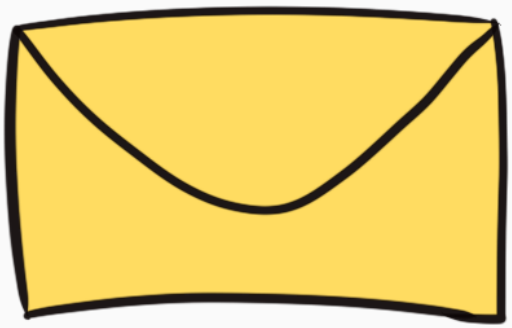
- Timing between packets creates patterns
- Recognize patterns at both ends

Destroy Patterns

- Previously: Hold packets back
- Now: Add dummy packets



Dummy Traffic



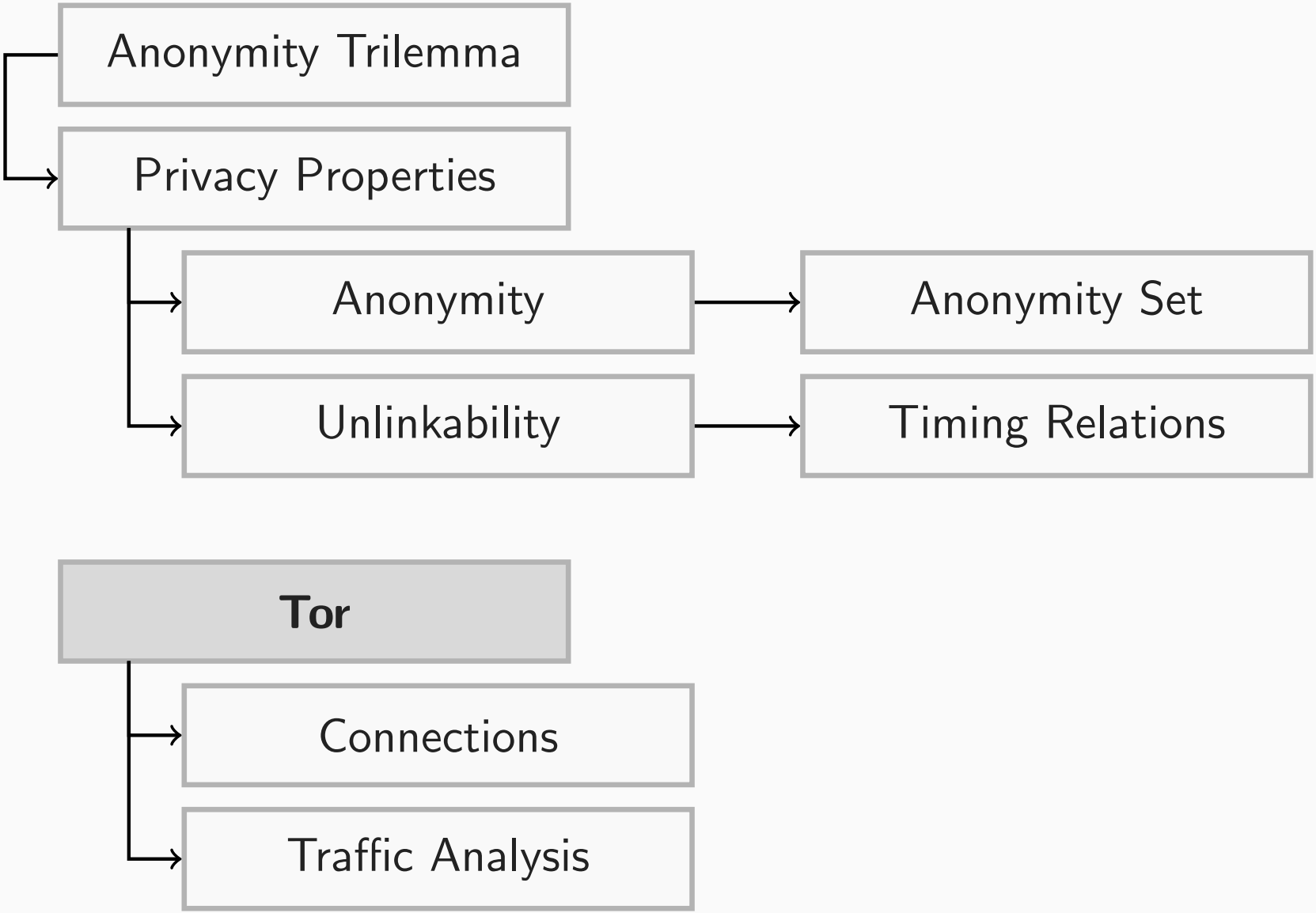
Inject Dummy Traffic

- Dummy packets:
  Messages with no payload
- Create a constant rate of traffic
- Everything has the same pattern
- Pro: Indistinguishable
- Con: Dummy overhead

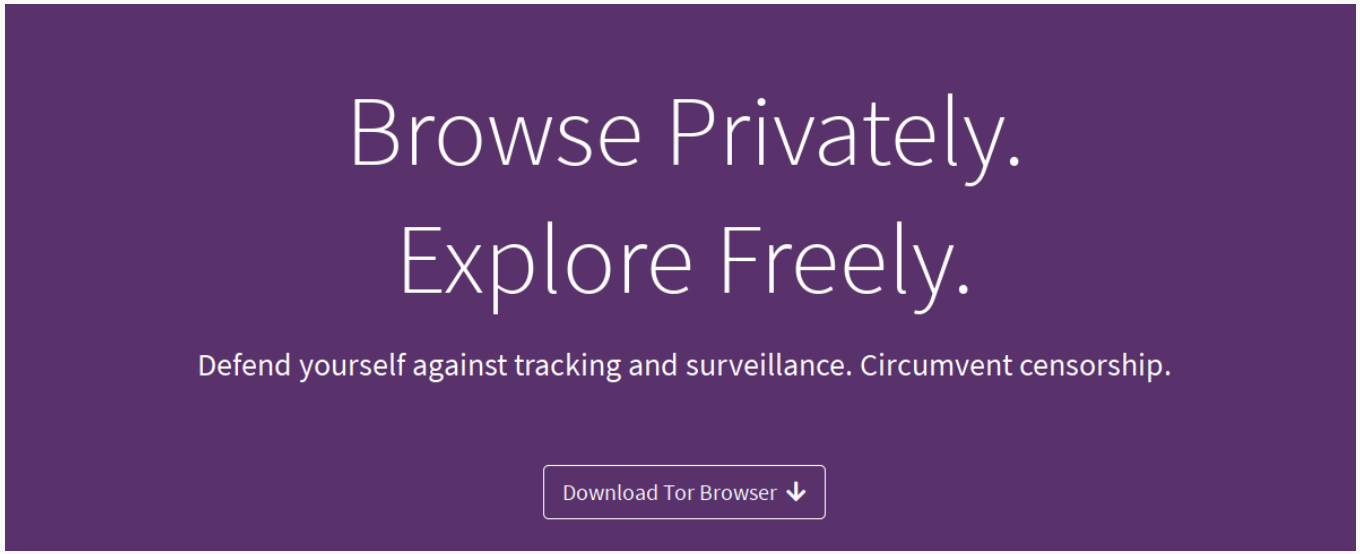
Quick Summary

- We looked at privacy features
- **Anonymity**
  - Hiding in a group
  - Without being distinguishable
- **Unlinkability**
  - Hide relations
  - Sender, recipient, or both
- Methods to achieve this:
  - Mixing: Add delays to packets
  - Batch or continuous time mix
  - Dummy traffic: Inject packets
  - Create constant rate

Tor - The Onion Router


Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

What is Tor?



We believe everyone should be able to explore the internet with privacy. We are the Tor Project, a 501(c)3 US nonprofit. We advance human rights and defend your privacy online through free software and open networks.[1]

[1] https://www.torproject.org/

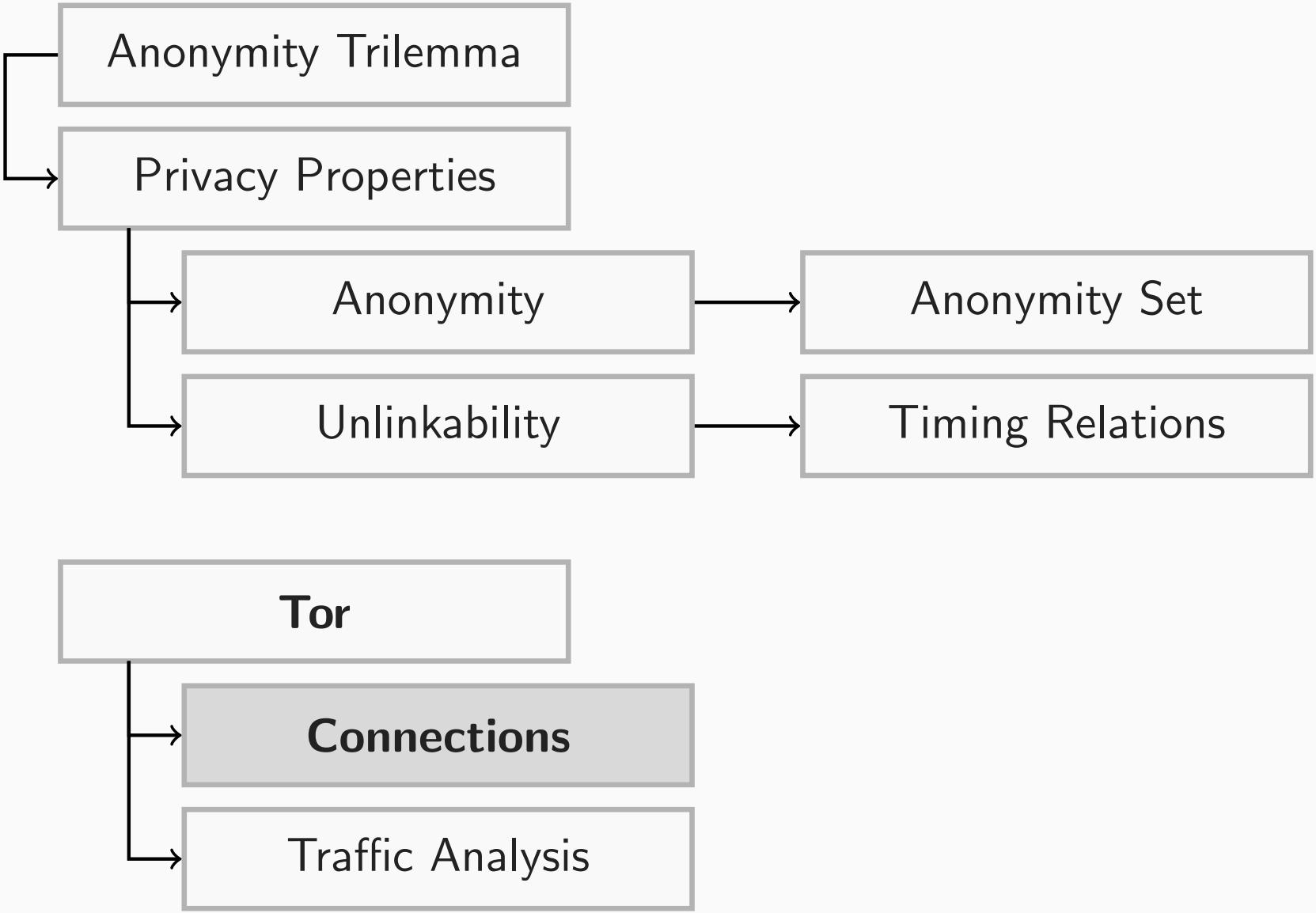
Tor Browser

The Tor Browser

is a Firefox-based browser that allows for normal web browsing. It uses the underlying Tor mechanisms to provide anonymity.

Example:

- *You* type in `www.duckduckgo.com` in the address line.
- *The Tor Browser* picks a circuit and establishes a connection.
- *Tor* creates these circuits.


Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

Tor: Making Connections

Requesting a website:

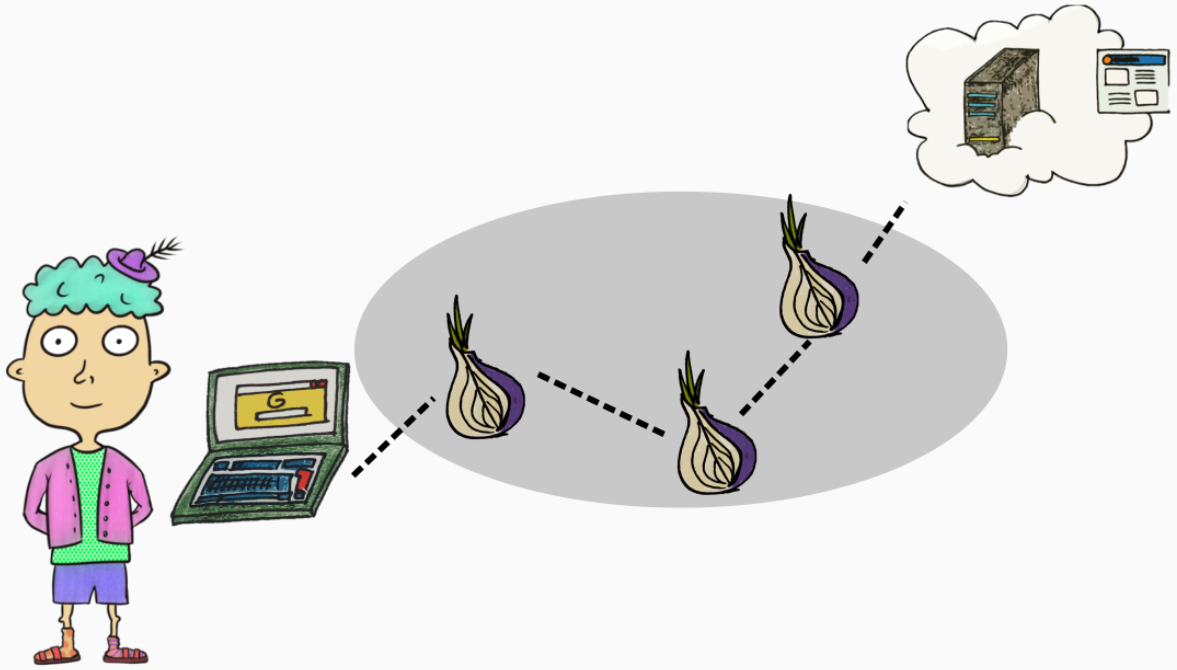
- You connect to the server of a website
- Your IP address is personal information, the website is, too.
- `www.much-secret.com`, `77.654.123.99` match.

Tor: Adversary Eavesdropping

Someone monitors the connection:

- Adversary monitoring between you and the server
- Learns your IP address and the target server
- **Adversary knows you visited site!**

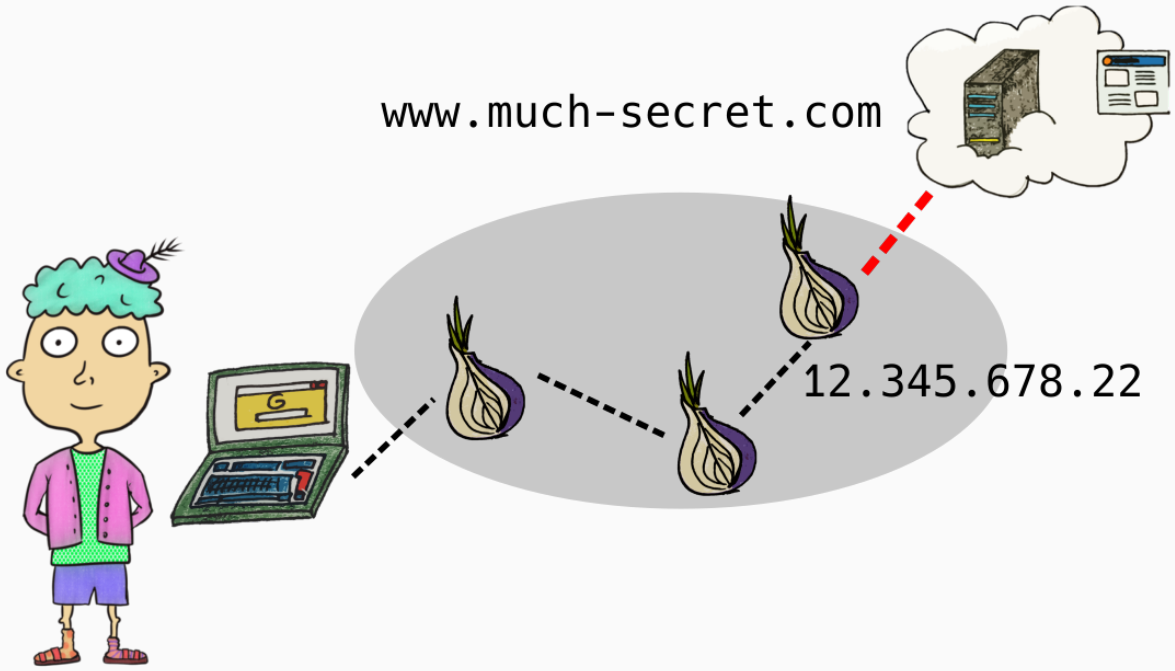
Tor: Intermediate Network



Separate endpoints:

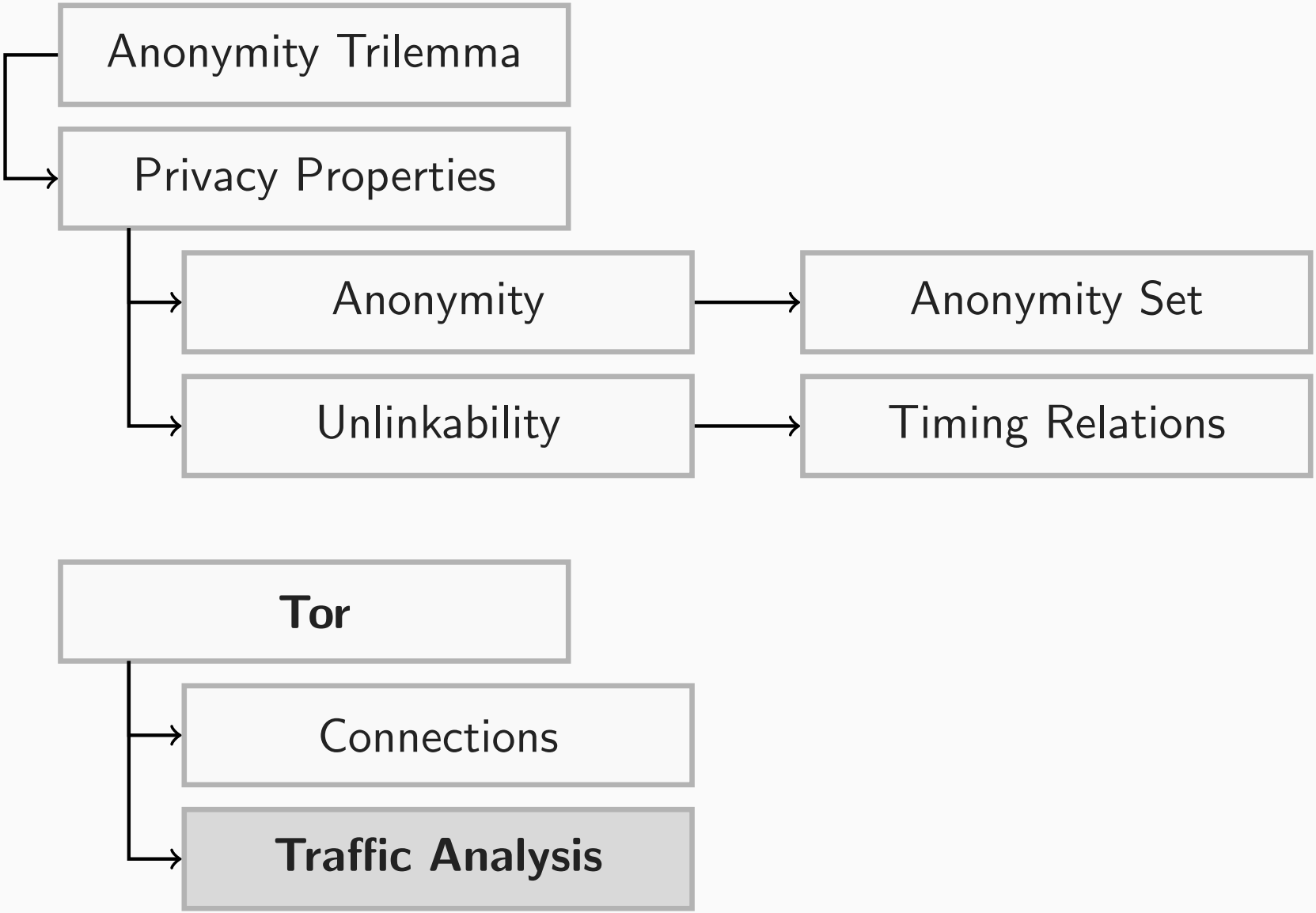
- Instead of *direct* connection, use intermediate Tor network
- Connect to `entry`,`middle`,`exit`, then to server
- Separates you (IP) from the destination (server)!

Tor: Adversary!?



Request made from exit:

- Adversary can still monitor the connection
- Learns the server and the *IP of the exit relay*
- Officially, you never visited `much-secret.com`!


Anonymity Trilemma
Privacy Properties
Anonymity
Anonymity Set
Unlinkability
Timing Relations
Tor
Connections
Traffic Analysis

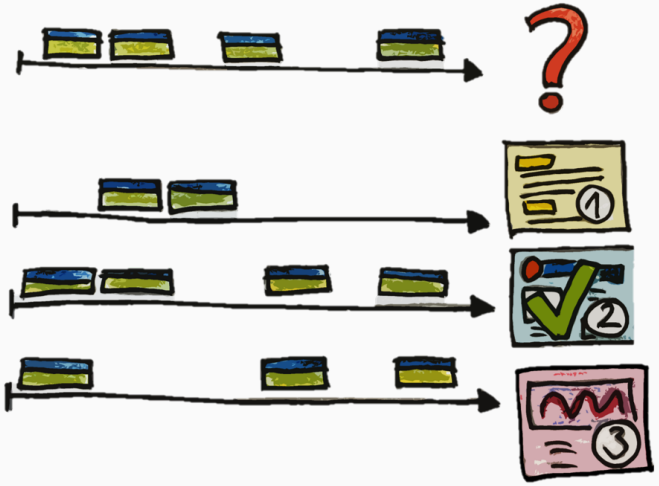
Traffic Analysis Attacks

Before going into detail, what is a traffic analysis *attack*?

- Traffic is *encrypted*
- We still see other information:
  - Packet size
  - Timing between packets
  - ...
- We use this *metadata* to learn something about the connection!

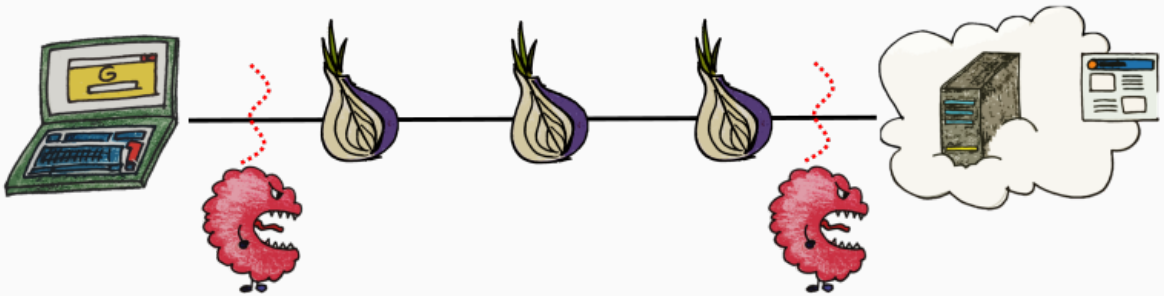
What can we learn from metadata?

- Sizes and timings help us to see *patterns*
- By comparing traces[2], we try to find matches.
- **Example:** To which *website* does the top trace belong?



[2]Packet trace, a timestamped sequence of packets captured on a computer network with a sniffer or similar tools (wikipedia.org)

End-to-End Monitoring



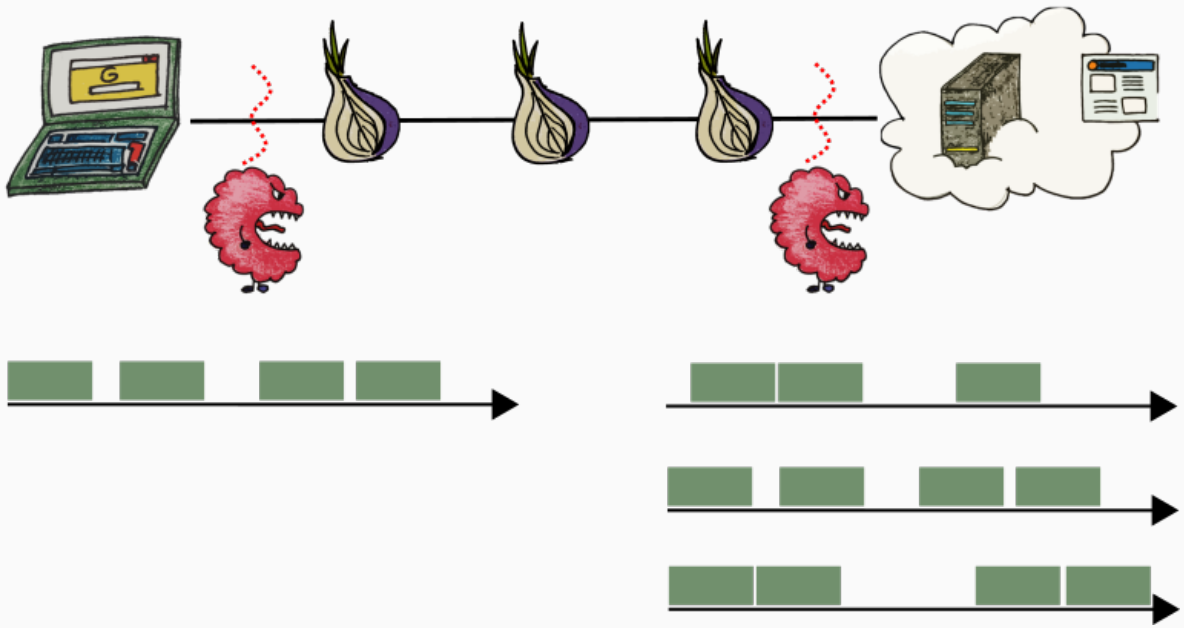
Adversary monitors traffic at both ends

- The *entry* traffic relates to the identity of the user.
- The *exit* traffic relates to the destination of the connection.
- In combination, this information *de-anonymizes* the user.

Tor is an anonymity system.

De-Anonymization is the worst-case.

Capture Traffic

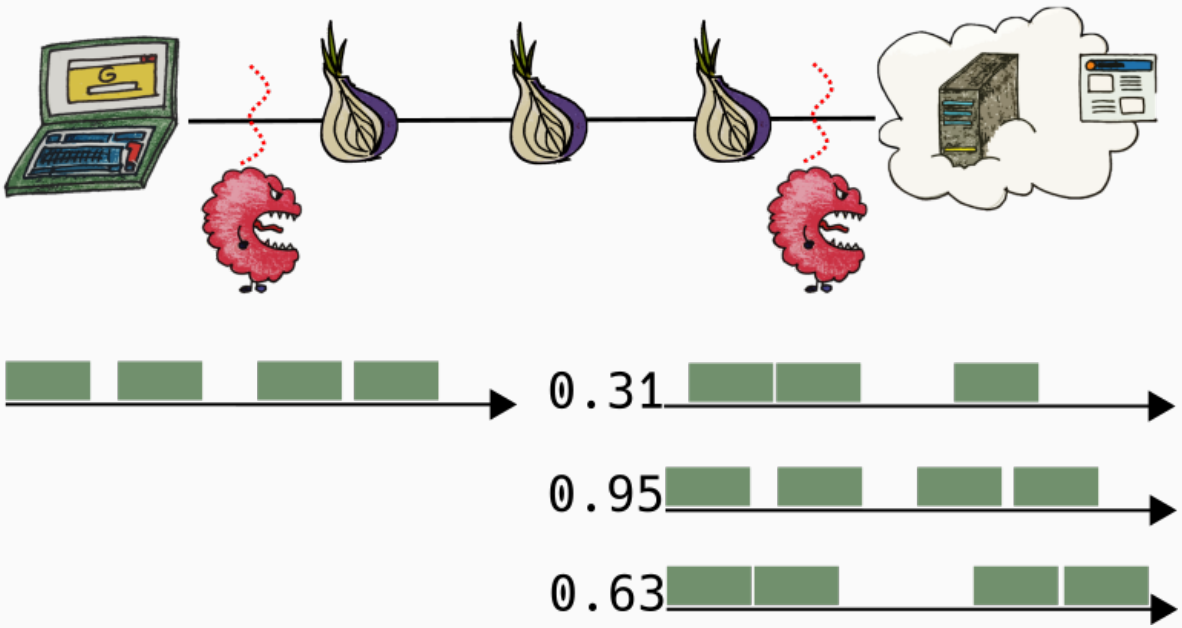


Encrypted traces with metadata information

- We have *one* trace on the entry side.
- We receive *multiple* possible traces at the exit.[3]

[3] Relays in Tor are shared. Multiple users connect to a relay at the same time, especially in exit nodes.

End-to-End Correlation



Compare traces

- We match a user to the server by comparing traces.
- The highest similarity is our guess.[4]

[4] Common similarity measures are Pearson's correlation coefficient, or mutual information.

Real-World Traffic Analysis

Tor | Blog

Tor security advisory: "relay early" traffic confirmation attack
by arma | July 30, 2014

SUMMARY:
On July 4 2014 we found a group of relays that we assume were trying to deanonymize users. They appear to have been targeting people who operate or access Tor hidden services. The attack involved modifying Tor protocol headers to do traffic confirmation attacks.

Tor | Blog

Did the FBI Pay a University to Attack Tor Users?
by arma | November 11, 2015

MOTHERBOARD | November 11 2015

TECH BY VICE

Court Docs Show a University Helped FBI Bust Silk Road 2, Child Porn Suspects
A "university-based research institute" was crucial to the busts of a Silk road 2.0 staffer and suspected child abuser.

Summary

We looked at:

- Definitions of privacy and anonymity
- Why it is so difficult to employ simple rules
- The “Anonymity Trilemma”
- Anonymity and unlinkability in a system
- Timing relations and counters
- Tor and traffic analysis attacks

Reading List

- Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two
  Theoretical analysis of security and performance relations
- Automated Website Fingerprinting through Deep Learning
  Deep Learning traffic analysis attacks
- A Critical Evaluation of Website Fingerprinting Attacks
  Things you should not do when analyzing website fingerprinting attacks
- The Loopix Anonyimity System
  Introducing and explaining Loopix