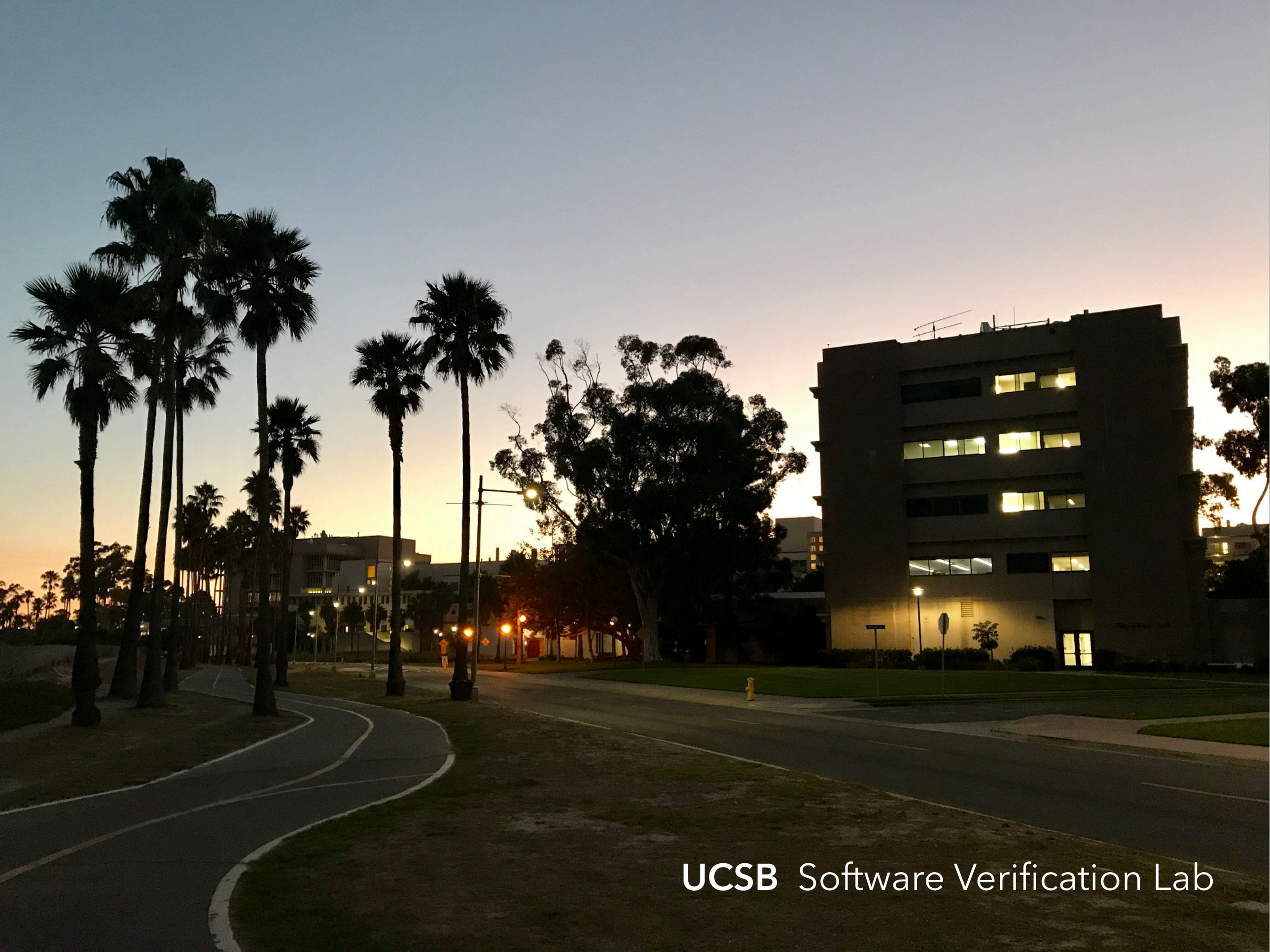
Profit

Detecting and quantifying side channels in networked applications

Nico Rosner Burak Kadron Lucas Bang Tevfik Bultan

University of California Santa Barbara Harvey Mudd College


UCSB Software Verification Lab

STAC

Space-Time Analysis for Cybersecurity

STAC

Goal: Improve degree of automation in detection of…

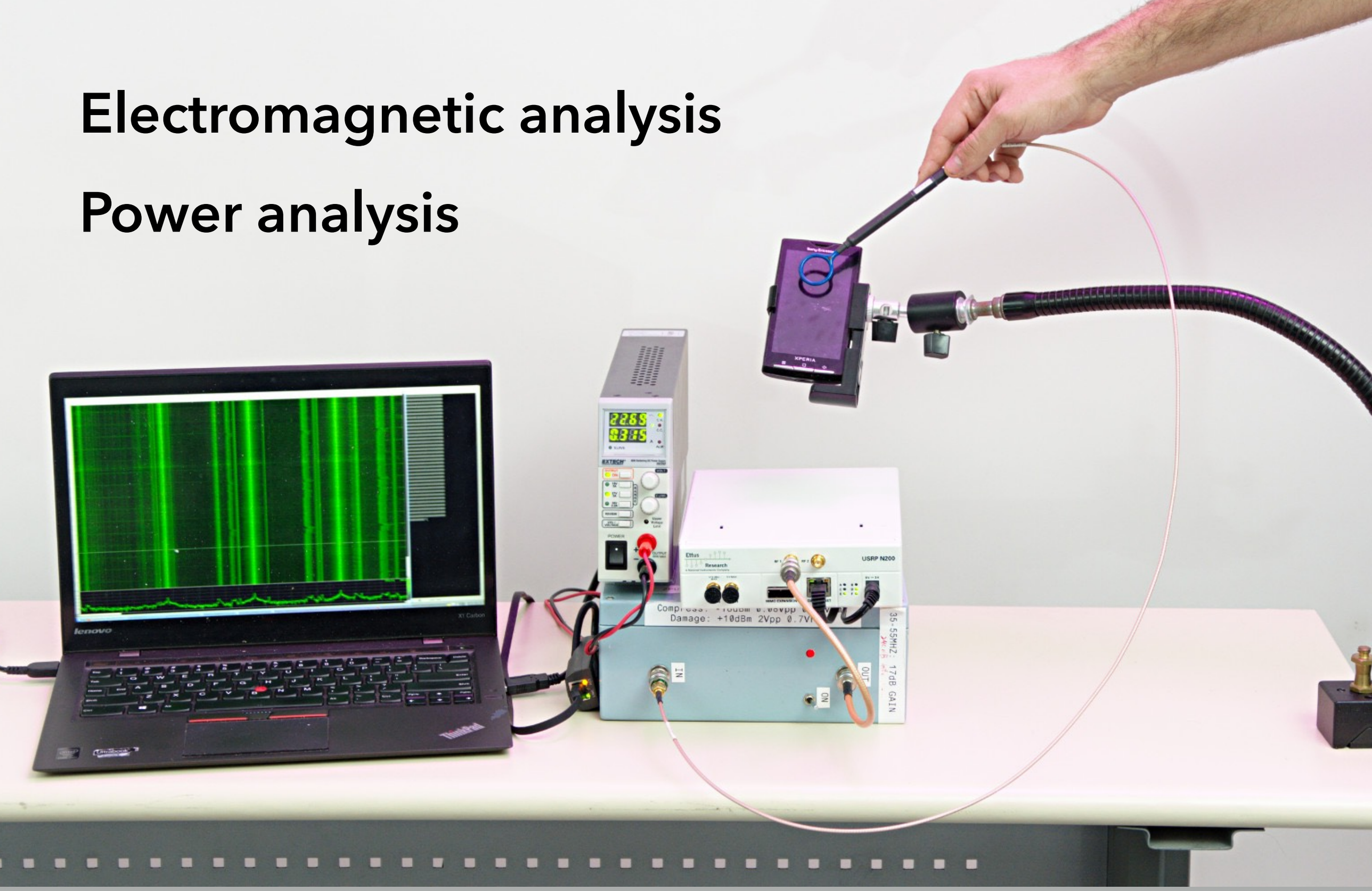
DARPA STAC

Side-channel vulnerabilities

Algorithmic complexity vulnerabilities

Electromagnetic analysis

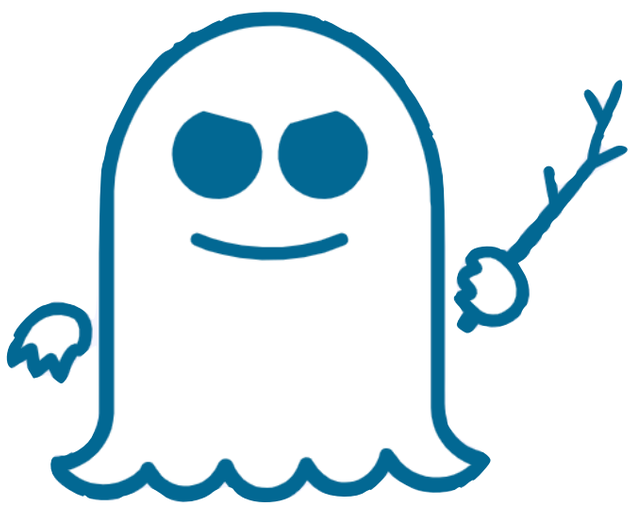
Power analysis



CPU-level **Race conditions**

Cache exploits

Branch prediction



Spectre

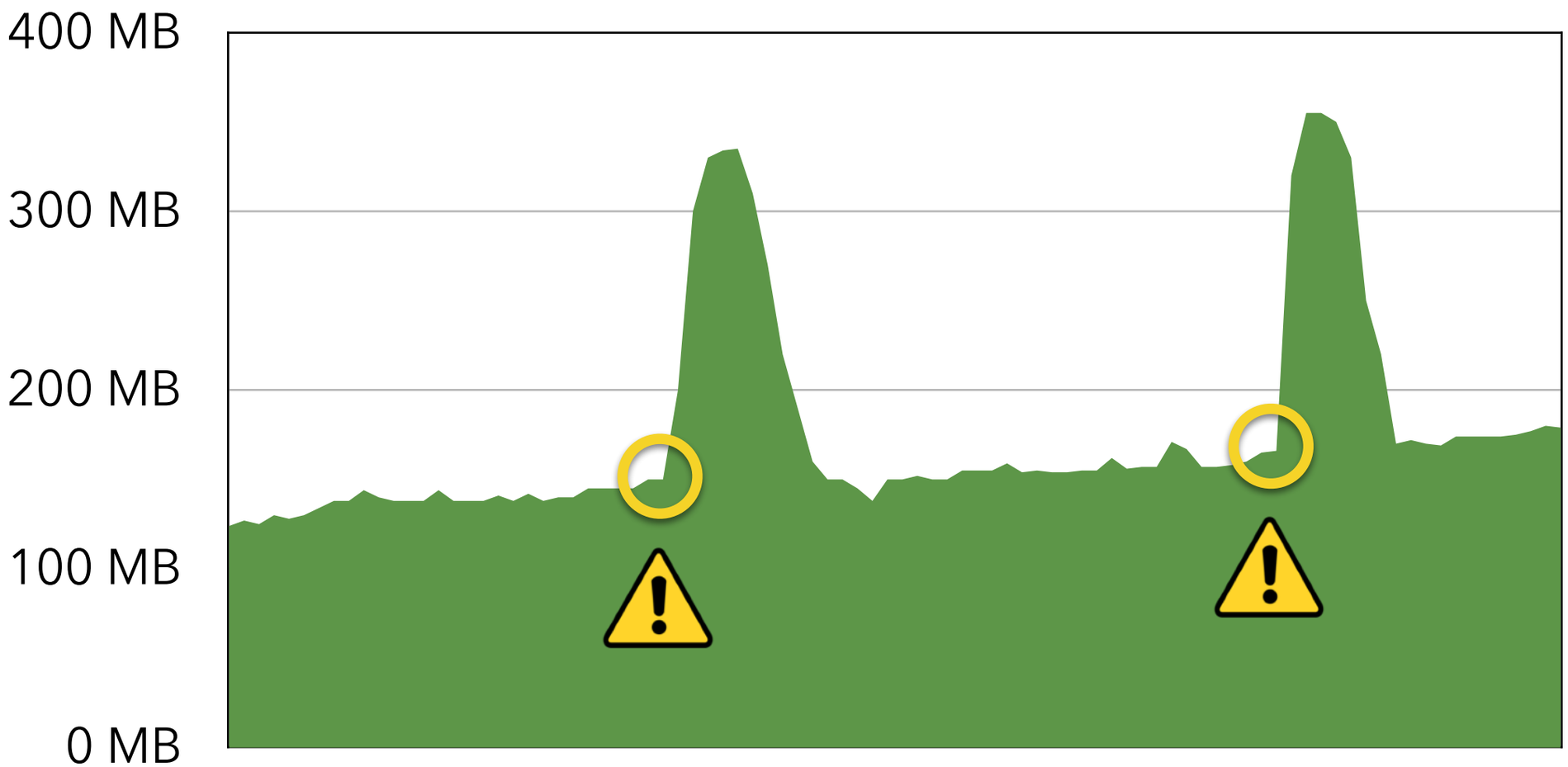
Meltdown

These are side channels

in hardware

Side channels
in software

Memory usage over time



Precise timing of execution

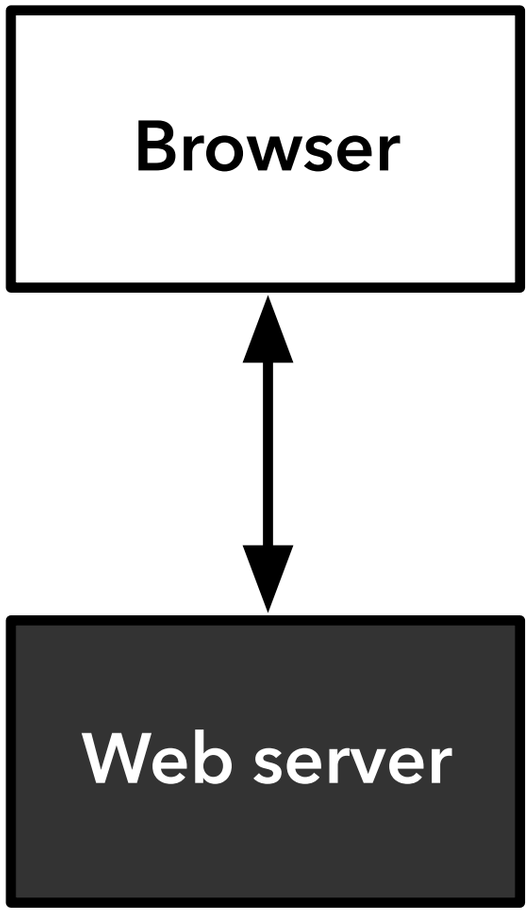
```
public class BiddersStatus {

    public boolean verifyHighest(int claimedOffer) {
        int highest = 0;
        Iterator cwinners = this.claimedWinners.keySet().iterator();
        Iterator everyone = this.everyParticipant.keySet().iterator();

        while(everyone.hasNext()) {
            ProtocolsPublicIdentity peer = (ProtocolsPublicIdentity)everyone.next();
            if(! peer.contactedSoFar) {
                peer.notify(Protocol.END_OF_ROUND);
            }
        }

        while(cwinners.hasNext()) {
            ProtocolsPublicIdentity customer = (ProtocolsPublicIdentity)cwinners.next();
            int offer = ((Integer)this.claimedWinners.get(customer)).intValue();
            if(offer > highest) {
                highest = offer;
            }
        }

        return claimedOffer == highest;
    }

}
```

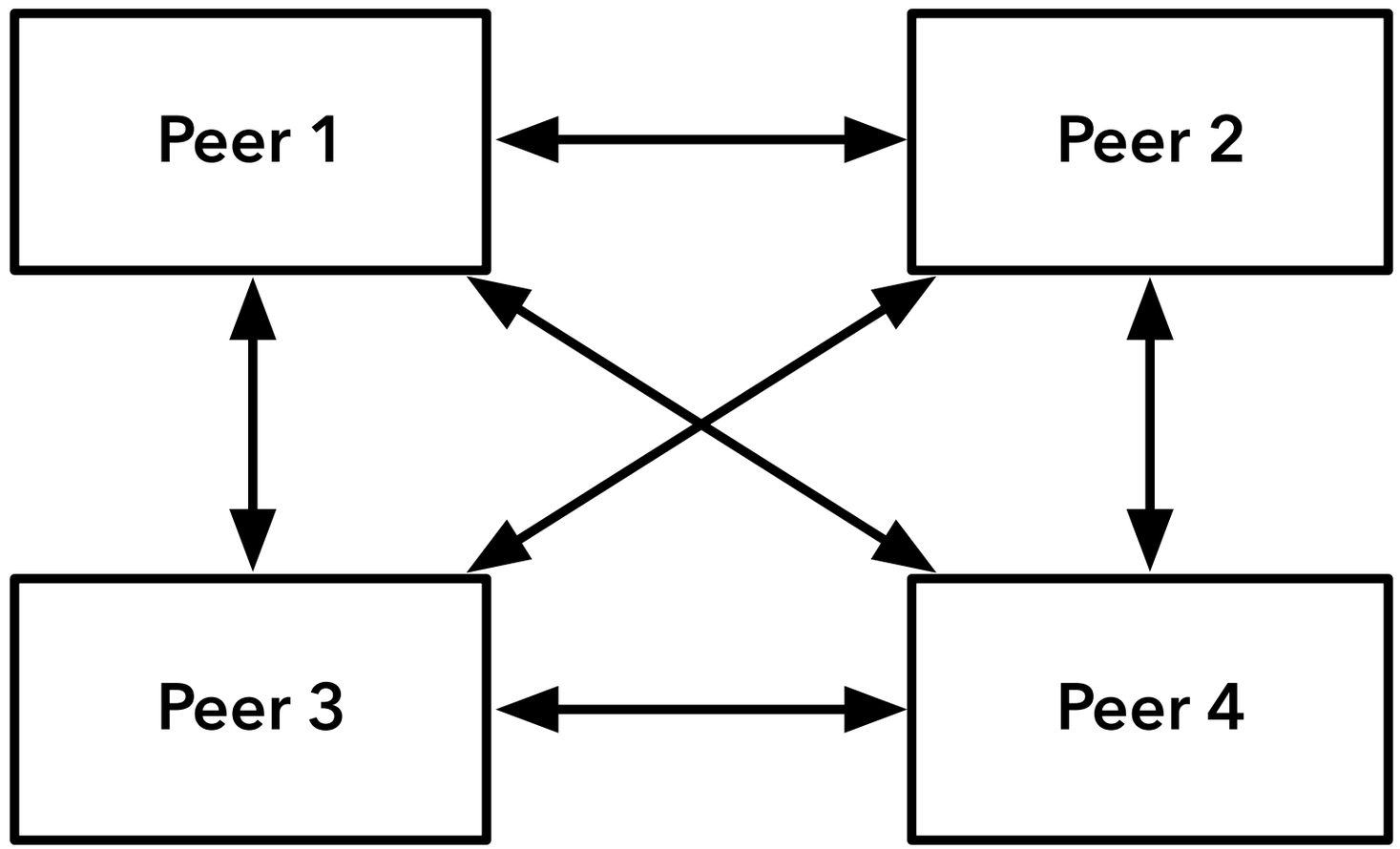
In our attack model:

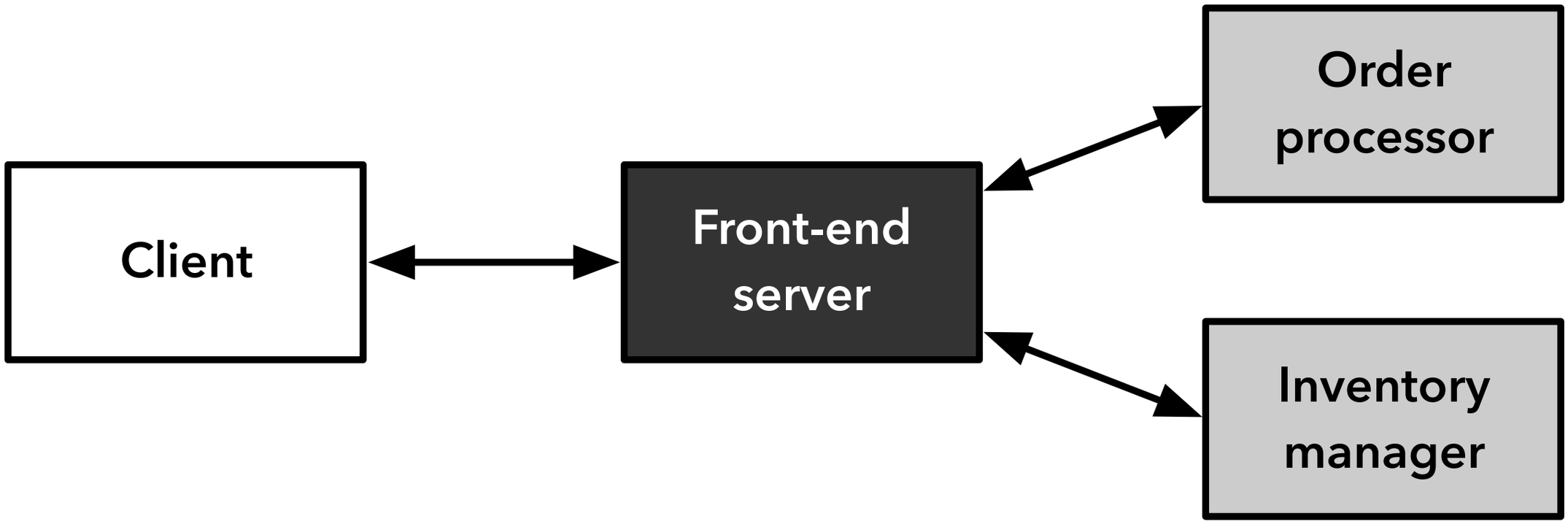
No local measurements

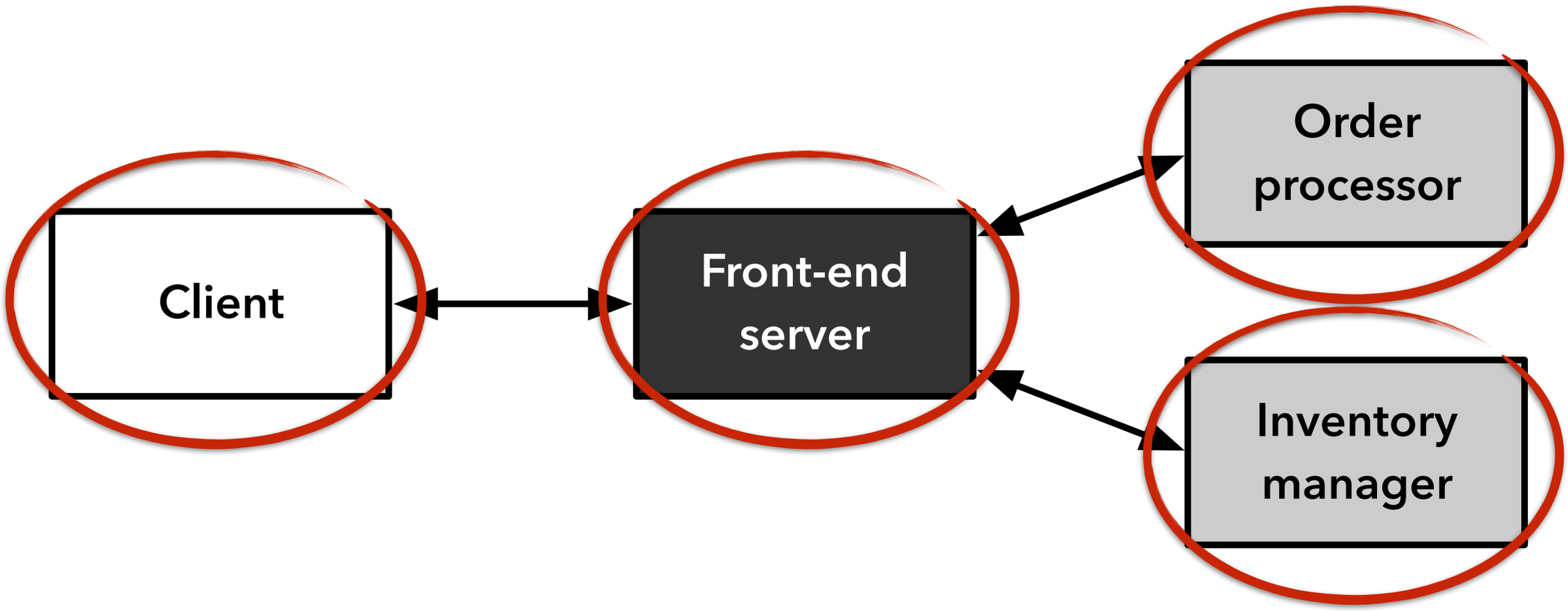
We target

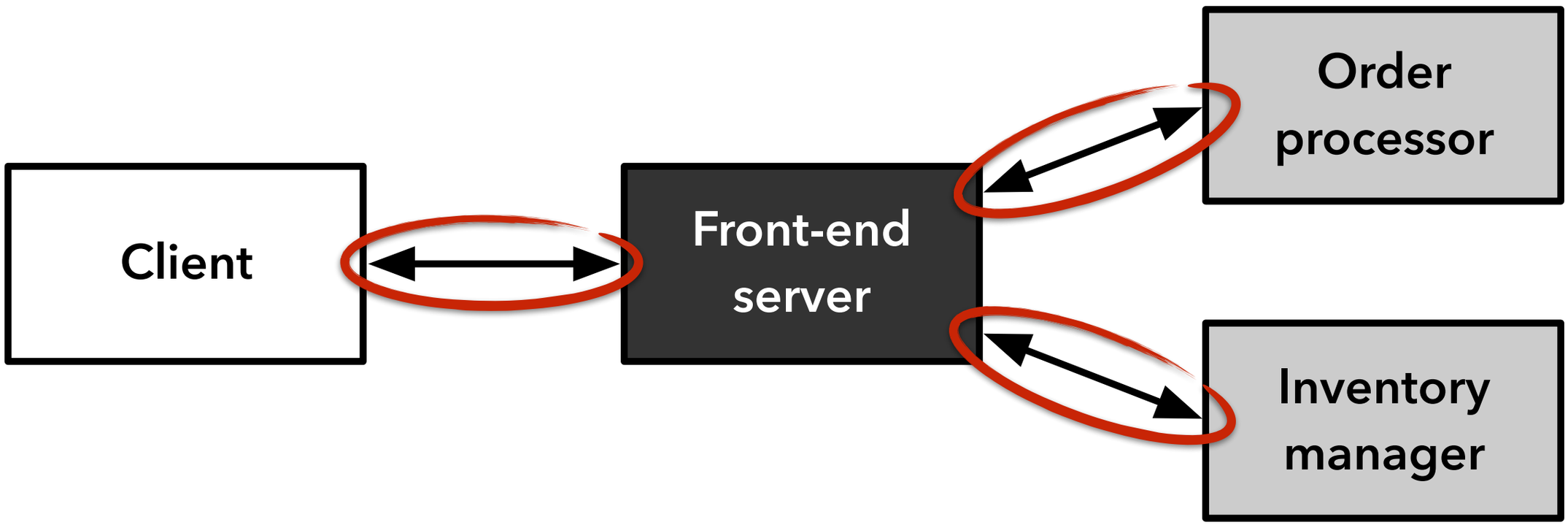
multi-component systems


Browser
Web server

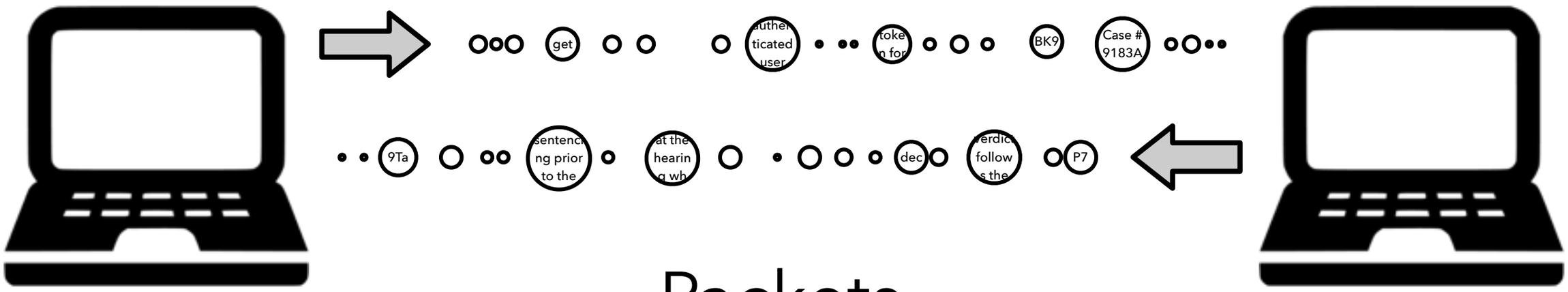

Peer 1
Peer 2
Peer 3
Peer 4


Order processor
Client
Front-end server
Inventory manager


Order processor
Client
Front-end server
Inventory manager

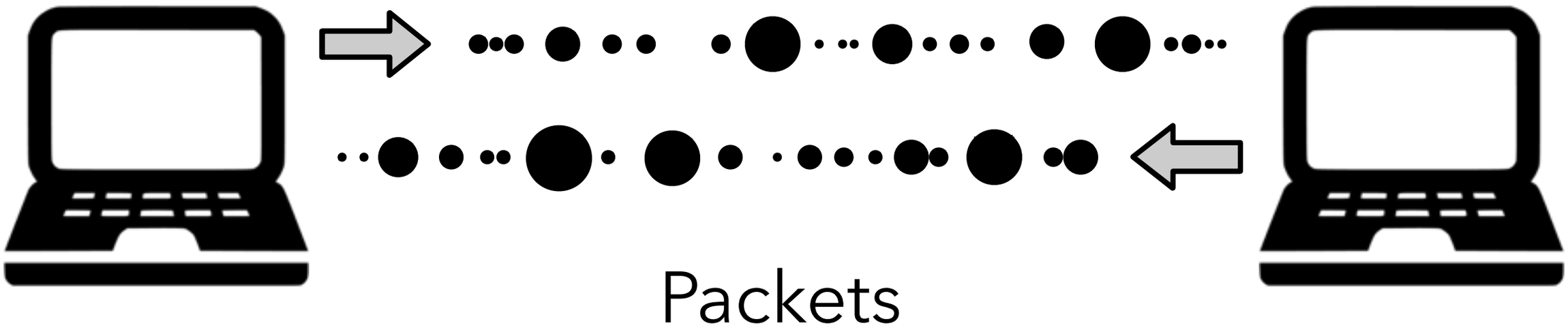

Client
Front-end server
Order processor
Inventory manager

Side-channel measurements on the network


get
authen
ticated
user
toke
n for
BK9
Case #
9183A
9Ta
sentenc
ng prior
to the
at the
hearin
g wh
dec
verdic
follow
s the
P7

Packets

Encryption (TLS/SSL)



~~Payload~~

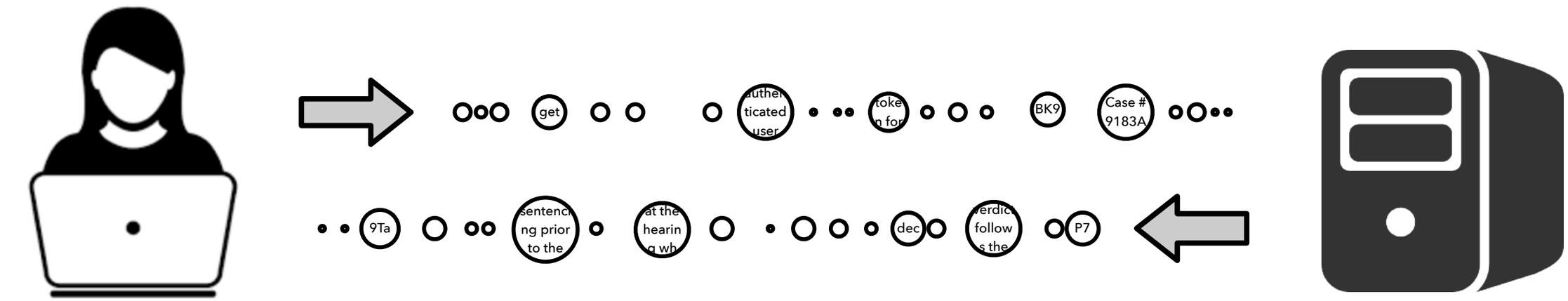
Size

Timing

Direction

In our attack model…

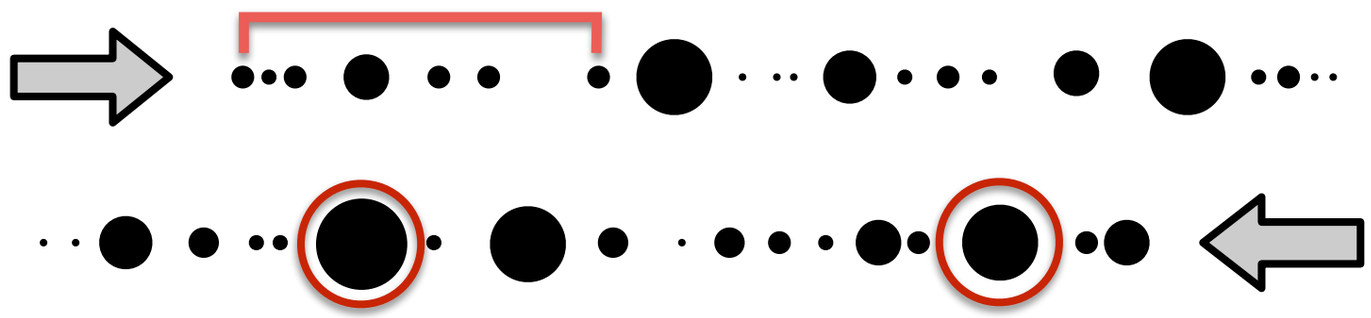
Main channel:



The payloads

(Cryptanalysis is out of scope!)

Side channel:



Size **Source IP:port**

Time **Dest IP:port**

of each packet

Profit

[NDSS 2019]

Black-box profiling
for side-channel detection
and leakage quantification

- Choose an **interaction of interest**.

Login(U,P) ; Upload(X) ; Do(Y) ; Get(Z) ; Logout

- Choose an **interaction of interest**.
- Provide a set of **valid inputs**.

- Choose an **interaction of interest**.
- Provide a set of **valid inputs**.
- Choose a **secret of interest**.

Payroll system	**Salary of employee**
Medical system	**Age of patient**

- Choose an **interaction of interest**.
- Provide a set of **valid inputs**.
- Choose a **secret of interest**.

> Profit runs interaction repeatedly.

- Choose an **interaction of interest**.
- Provide a set of **valid inputs**.
- Choose a **secret of interest**.

> Profit runs interaction repeatedly.

> **Ranking** of top N most-leaky features.

Example

System:

Court records

Interaction:

Clerk logs in, uploads a case file

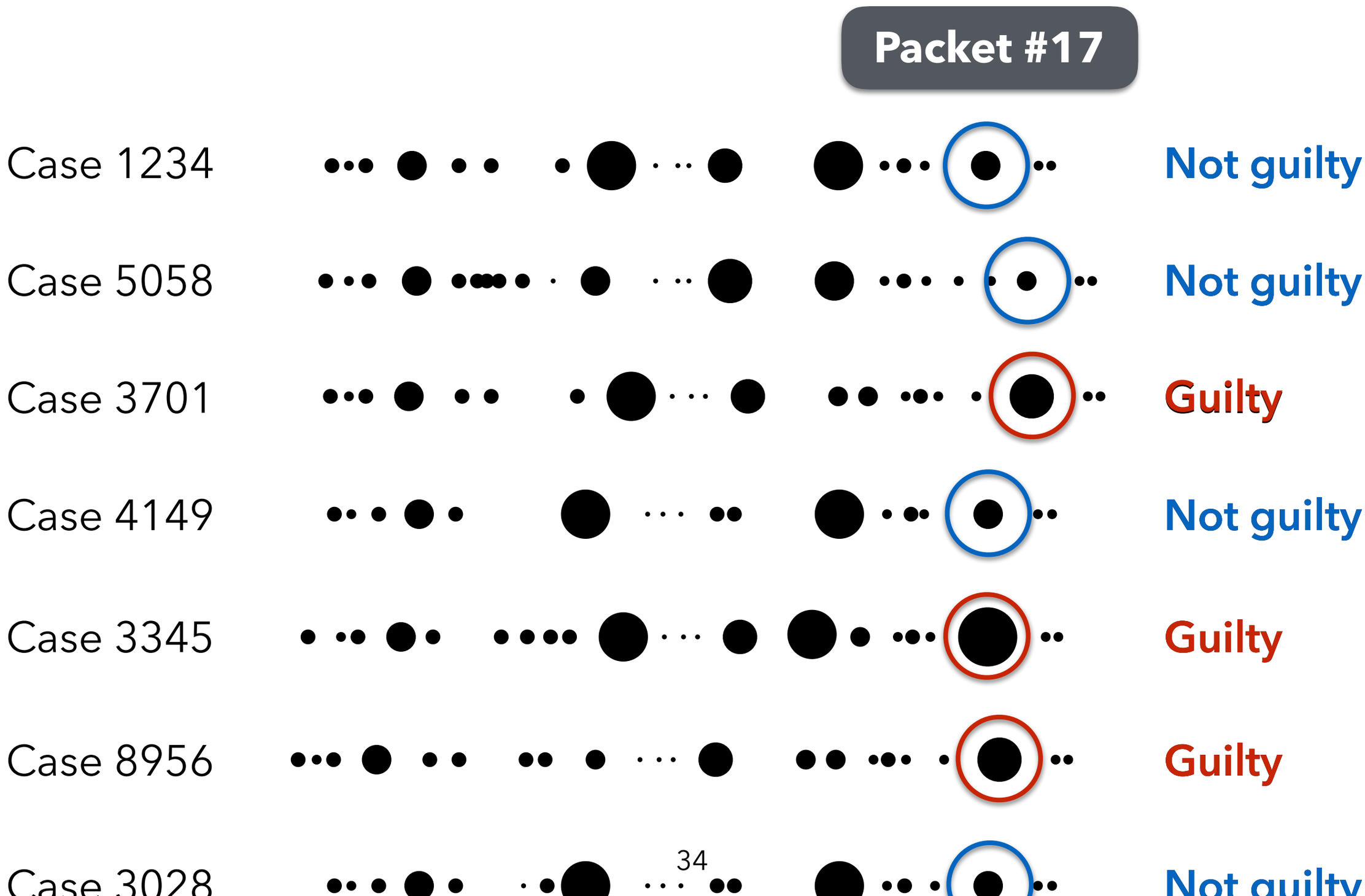
Secret:

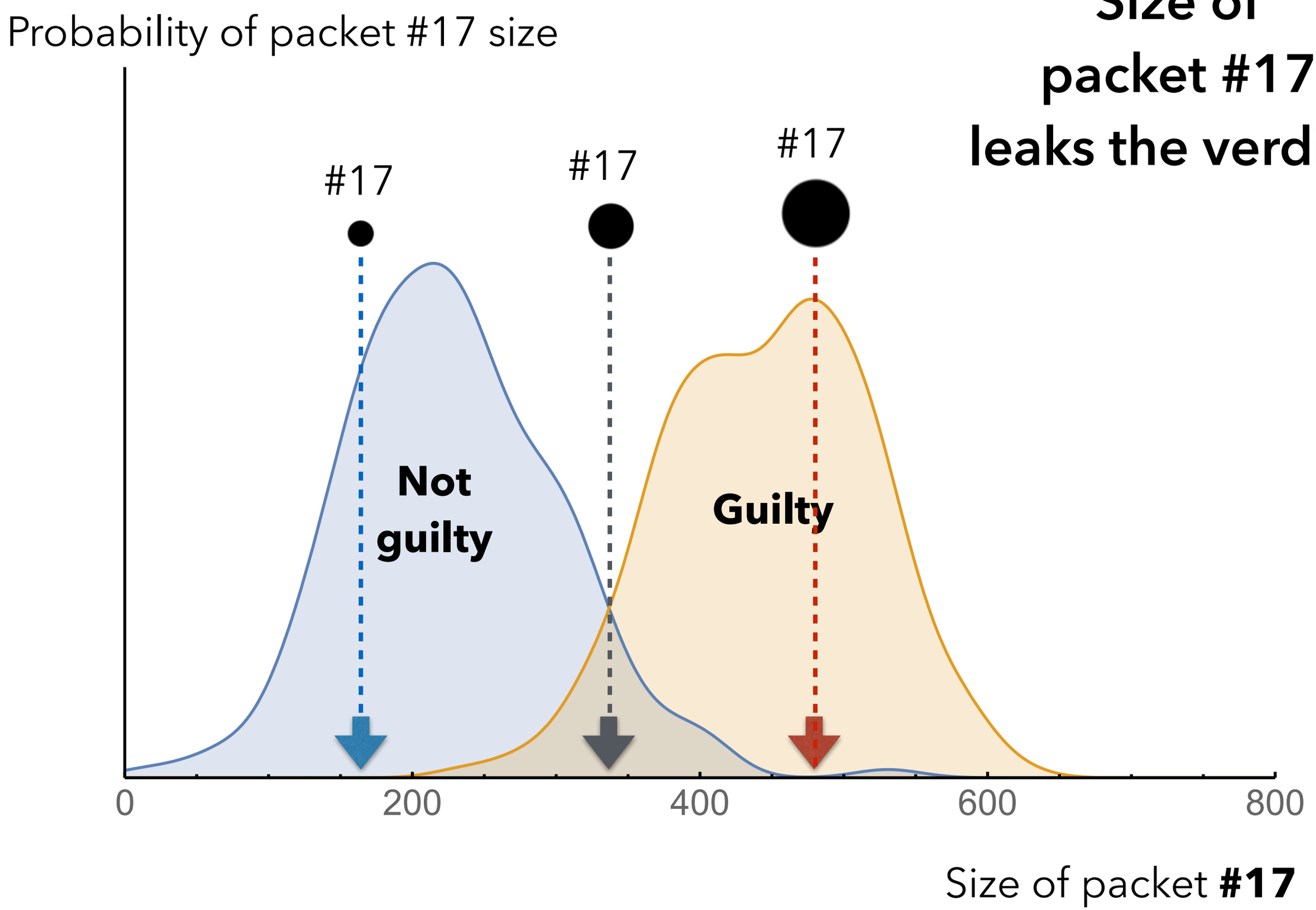
The verdict

Login and transmit case file

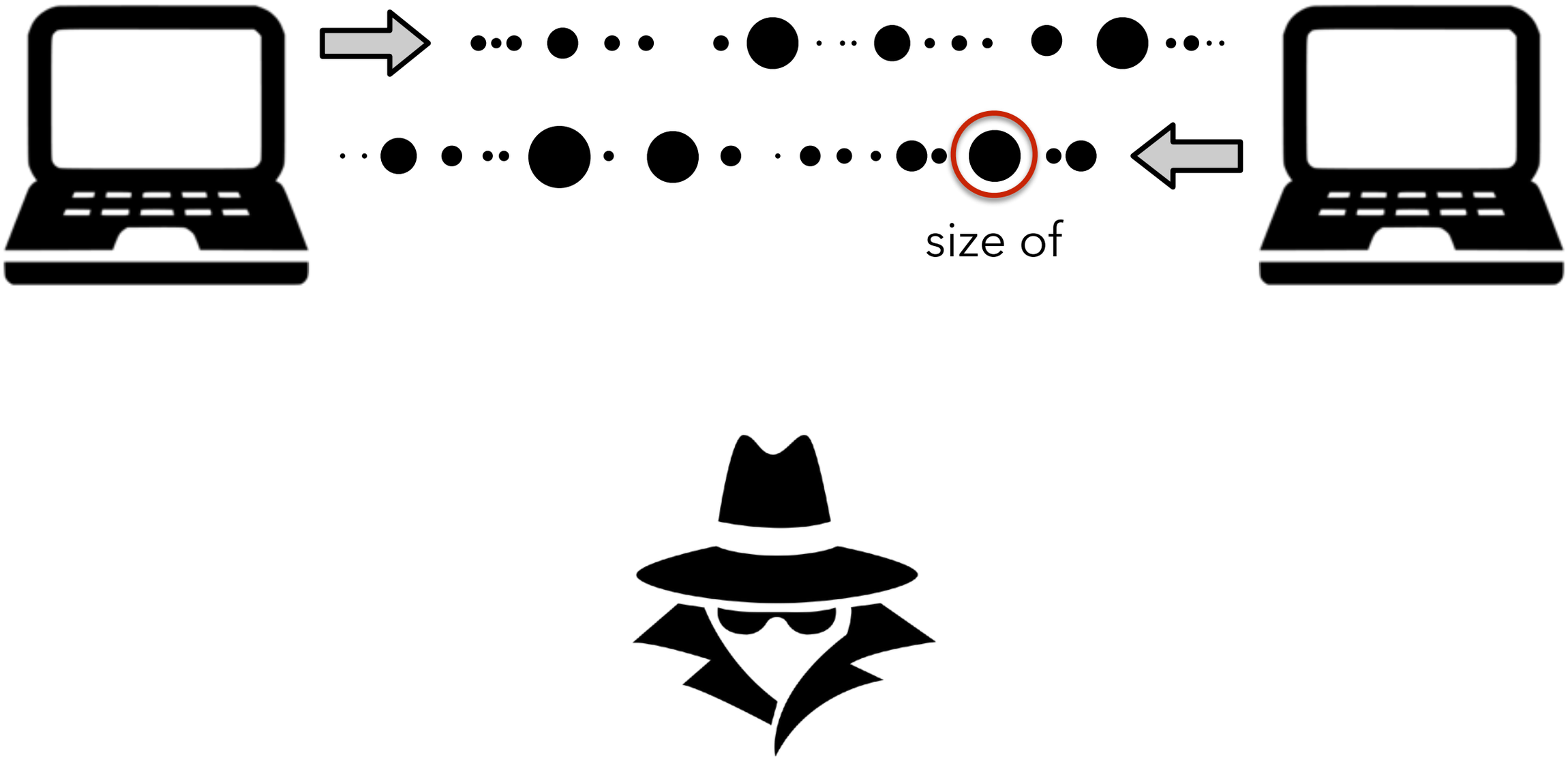
Case 1234		**Not guilty**
Case 5058		**Not guilty**
Case 3701		**Guilty**
Case 4149		**Not guilty**
Case 3345		**Guilty**
Case 8956		**Guilty**
Case 3028		**Not guilty**

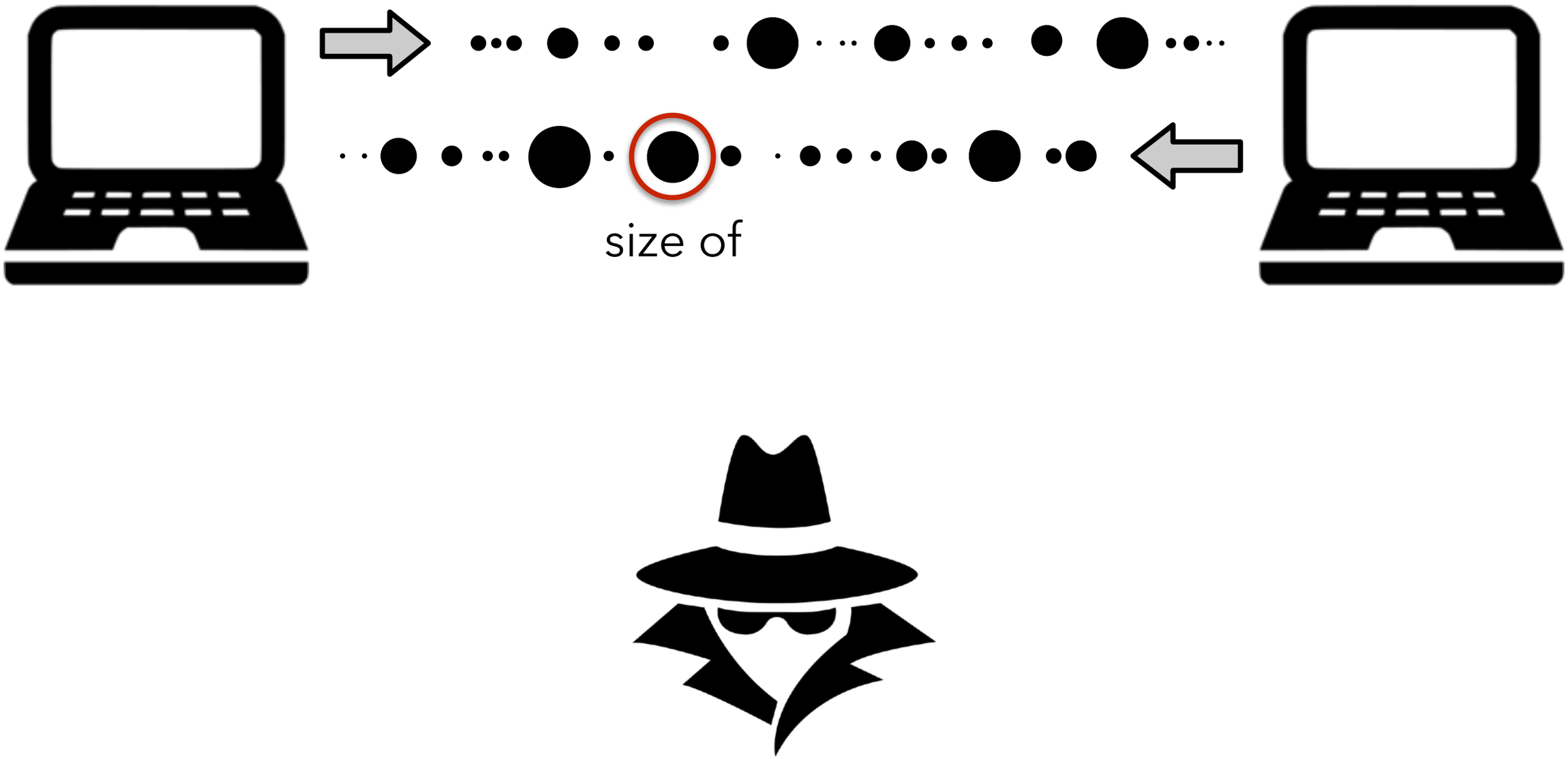
Login and transmit case file

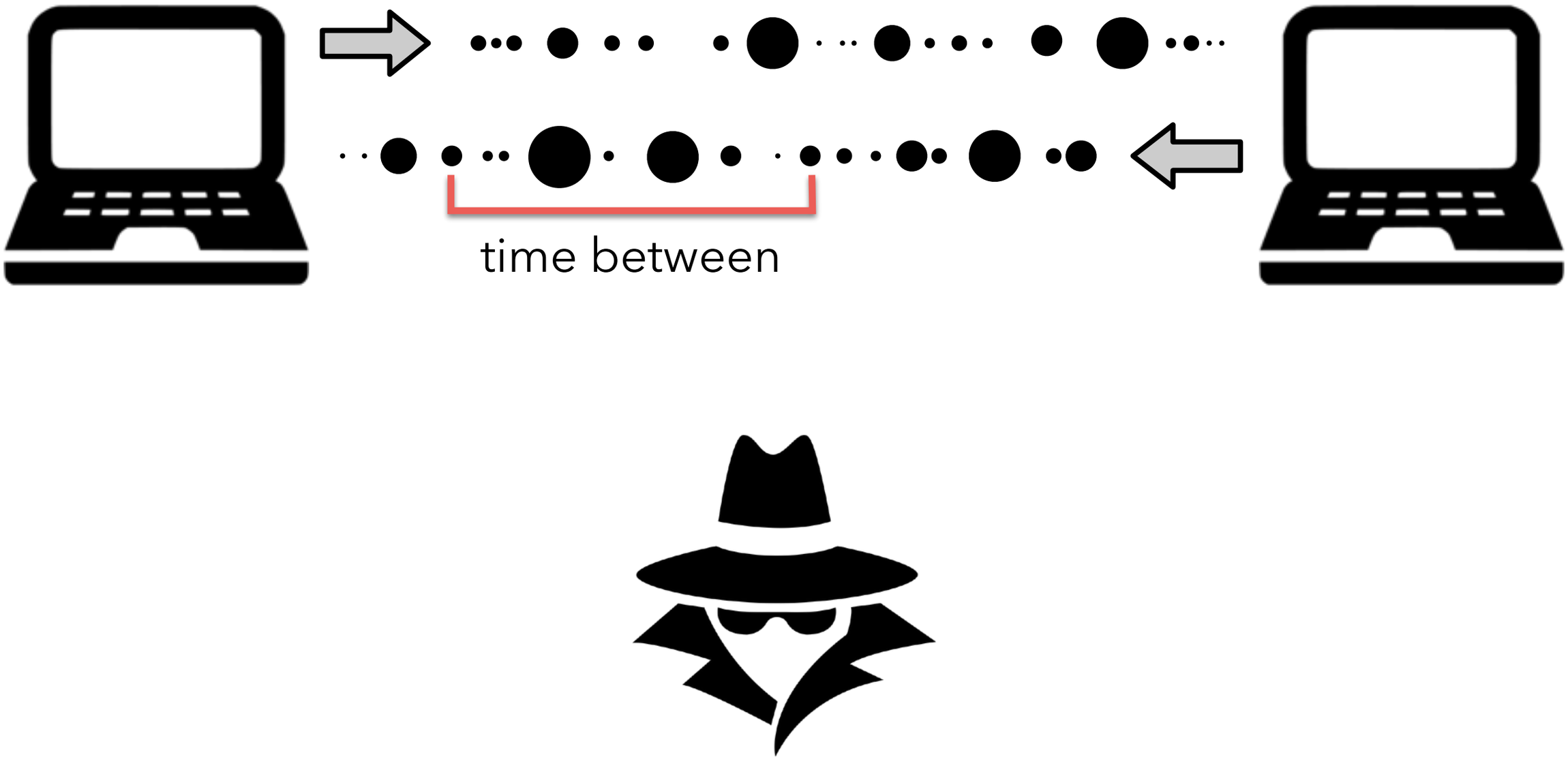


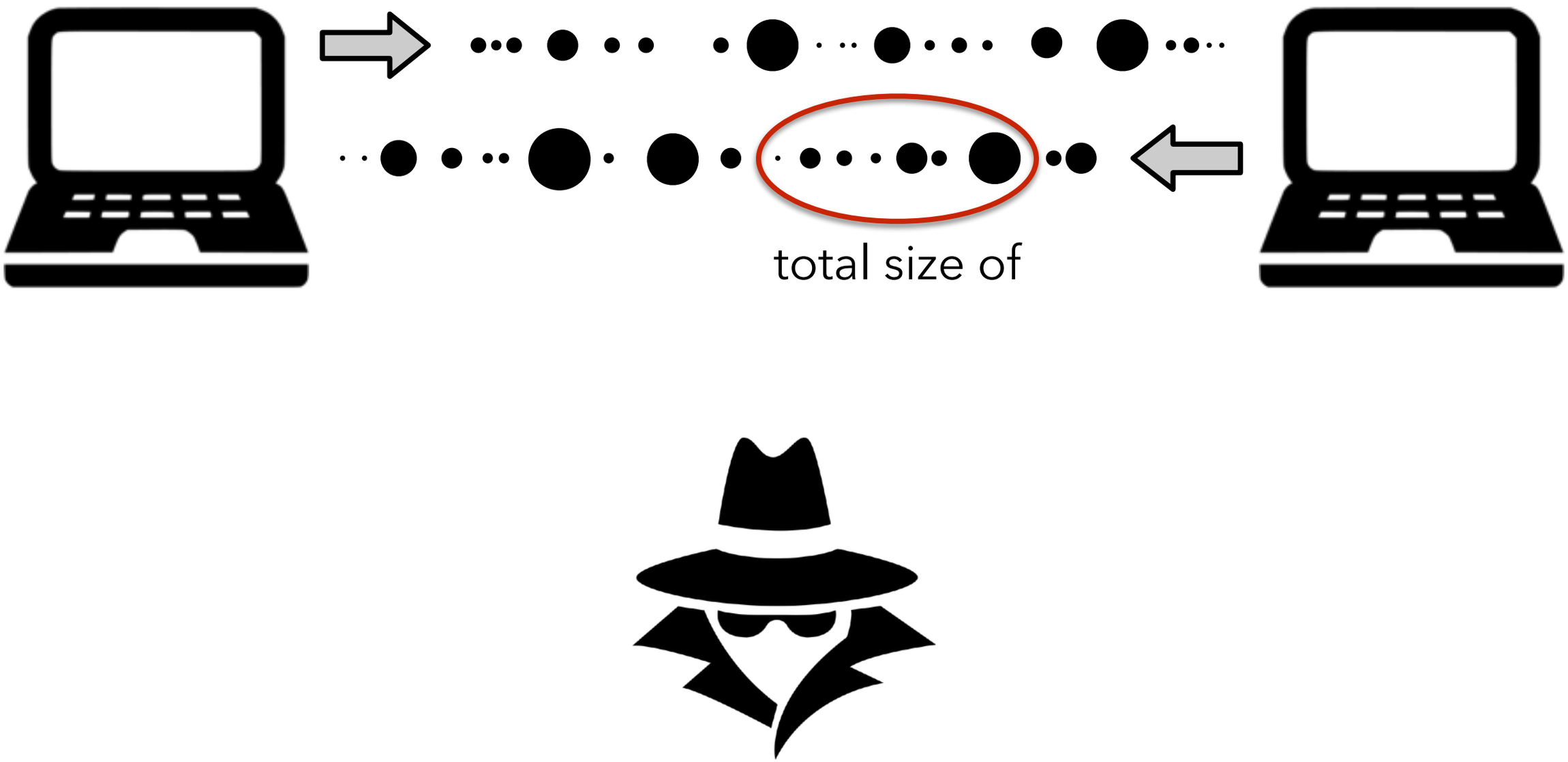


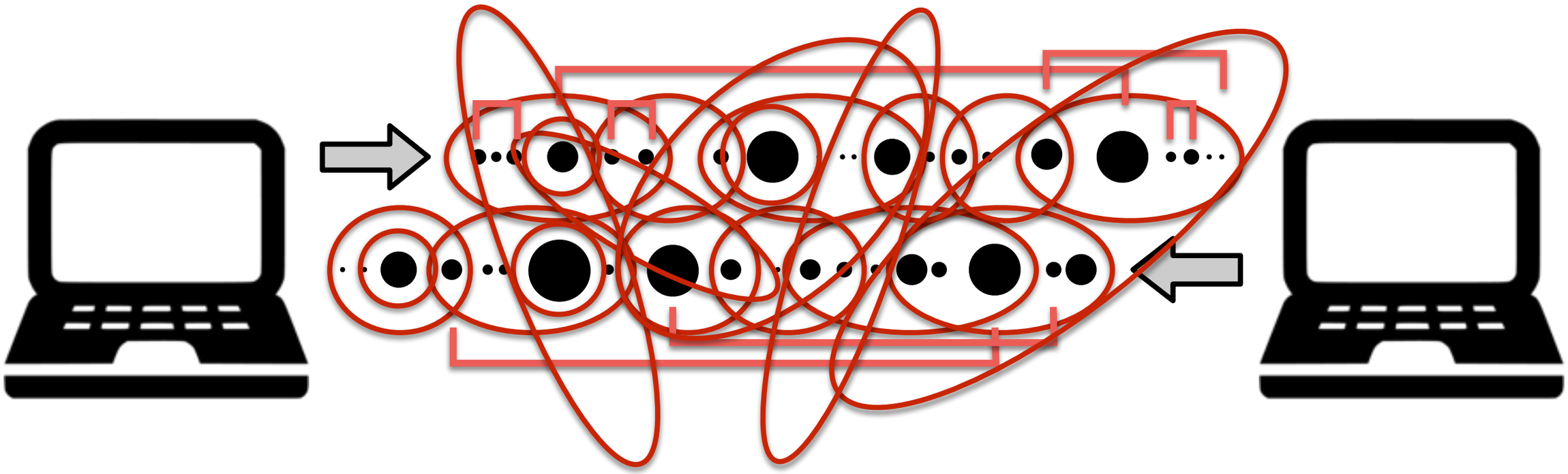
Size of packet #17 leaks the verdict!


size of


size of


time between

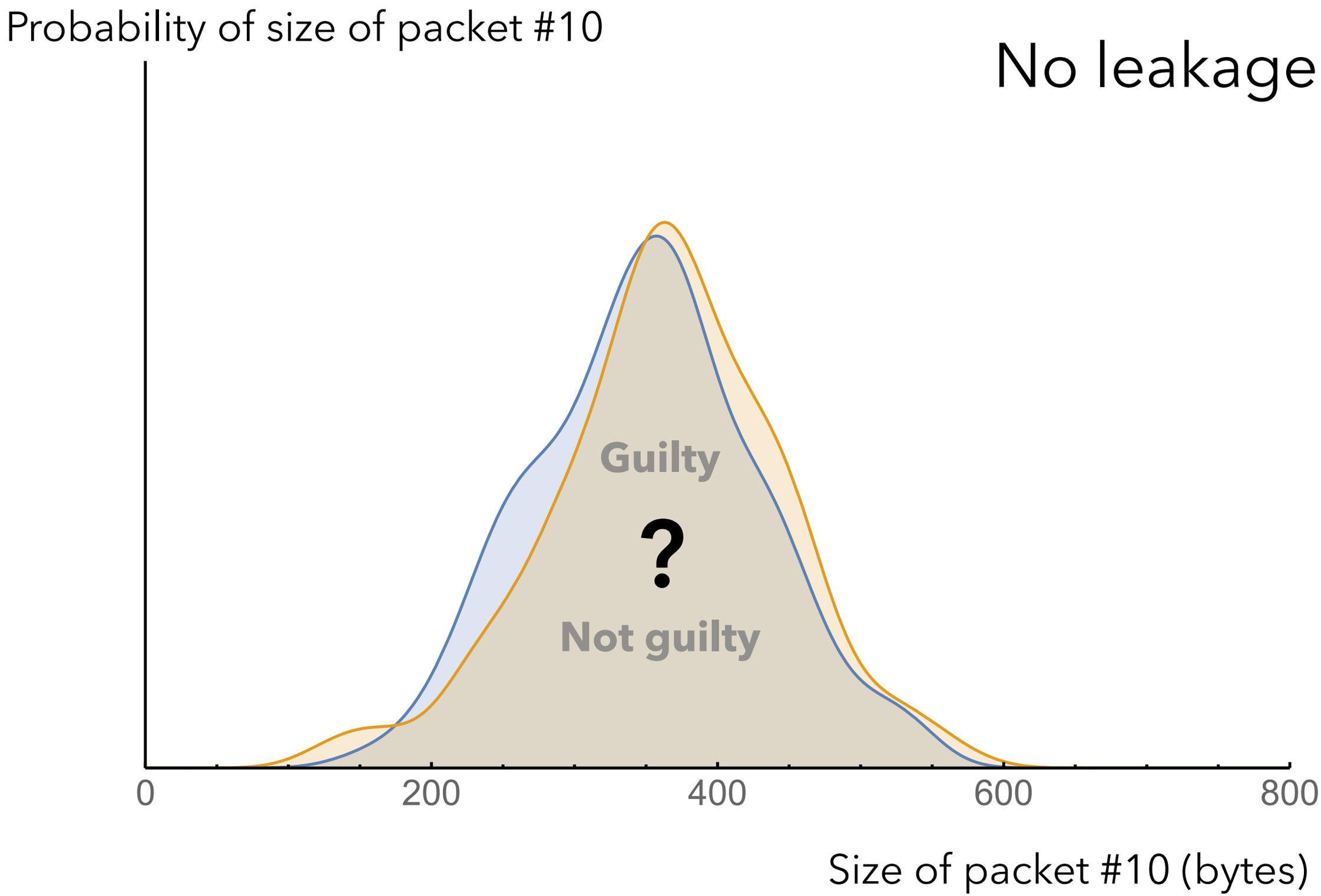

total size of



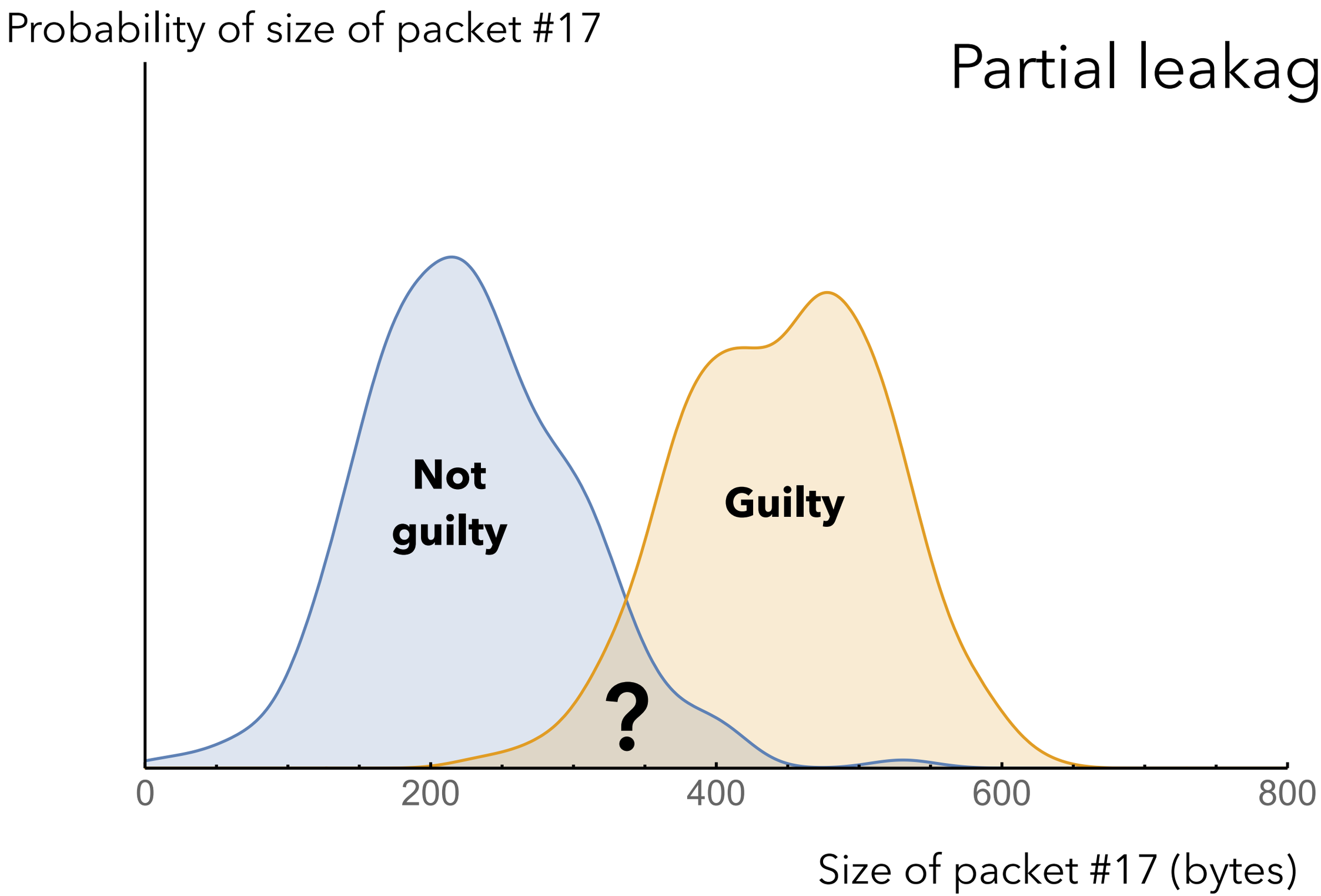
Too many features

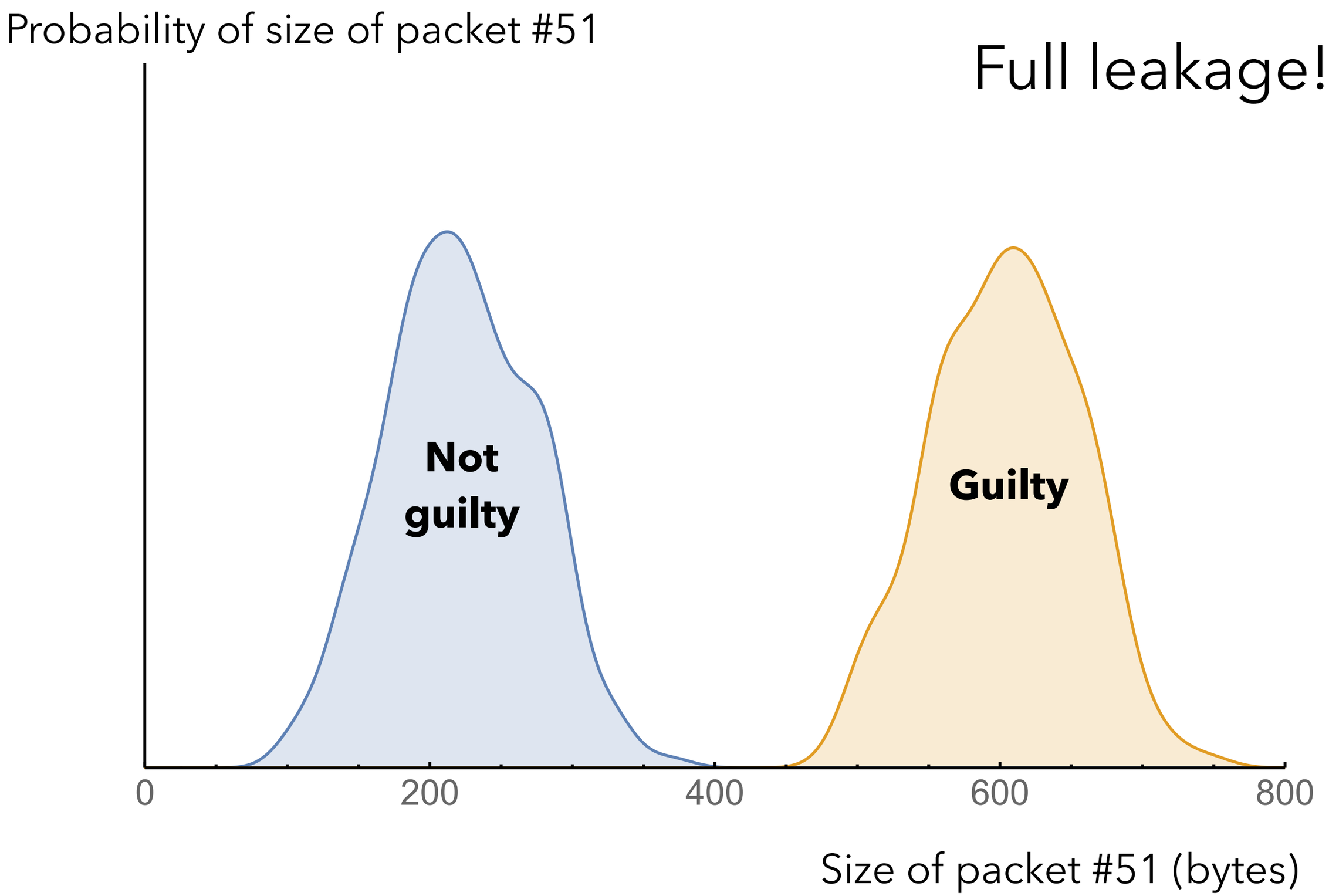
Impossible to analyze all of them

And depending on the feature …


Probability of size of packet #10
No leakage
Guilty
?
Not guilty
0
200
400
600
800
Size of packet #10 (bytes)

Partial leakage




Probability of size of packet #51
Full leakage!
Not guilty
Guilty
0
200
400
600
800
Size of packet #51 (bytes)

Profit automatically produces a ranking
sorted by amount of information leaked

Rank	Leaks	Feature	Direction
1	**99%**	**Size of packet #51**	banjo:13207 –> tuba:8080
2	**85%**	**Size of packet #17**	banjo:13207 –> tuba:8080
3	**14%**	**Total size of all packets**	banjo:13207 –> tuba:8080
4	**4%**	**Time between #12 and #13**	tuba:8080 –> banjo:13207
5	**3%**	**Size of packet #10**	banjo:13207 –> tuba:8080

Profit automatically produces a ranking
sorted by amount of information leaked

Rank	Leaks	Feature	Direction
1	**99%**	**Size of packet #51**	banjo:13207 –> tuba:8080
2	**85%**	**Size of packet #17**	banjo:13207 –> tuba:8080
3	**14%**	**Total size of all packets**	banjo:13207 –> tuba:8080
4	**4%**	**Time between #12 and #13**	tuba:8080 –> banjo:13207
5	**3%**	**Size of packet #10**	banjo:13207 –> tuba:8080

Profit automatically produces a ranking
sorted by amount of information leaked

Rank	Leaks	Feature	Direction
1	**99%**	**Size of packet #51**	banjo:13207 –> tuba:8080
2	**85%**	**Size of packet #17**	banjo:13207 –> tuba:8080
3	**14%**	**Total size of all packets**	banjo:13207 –> tuba:8080
4	**4%**	**Time between #12 and #13**	tuba:8080 –> banjo:13207
5	**3%**	**Size of packet #10**	banjo:13207 –> tuba:8080

Quantifying leakage

Quantifying leakage

Shannon entropy

$$\mathcal{H}(X) = -\sum_{x \in X} p(x) \log_2 p(x)$$

Information content
of a random variable

Quantifying leakage

Shannon entropy

$$\mathcal{H}(X) = -\sum_{x \in X} p(x) \log_2 p(x)$$

Information ~= Uncertainty

Entropy as a measure of
the *initial* uncertainty

$$\mathcal{H}(S) = -\sum_{s \in \mathbb{S}} p(s) \log_2 p(s) \text{ bits}$$

Each value of the secret

Conditional entropy as a measure of
the *remaining* uncertainty

$$\mathcal{H}(S|V) = -\sum_{v \in \mathbb{V}} p(v) \sum_{s \in \mathbb{S}} p(s|v) \log_2 p(s|v)$$

Each value of the
observable feature

Each value of the
secret

Conditional entropy as a measure of
the *remaining* uncertainty

$$\mathcal{H}(S|V) = -\sum_{v \in \mathbb{V}} p(v) \sum_{s \in \mathbb{S}} p(s|v) \log_2 p(s|v)$$

We estimate this distribution using profiling results for ***p(v|s)*** and Bayes' theorem

Mutual information

$$\mathcal{I}(S;V) = \mathcal{H}(S) - \mathcal{H}(S|V)$$

Initial
uncertainty

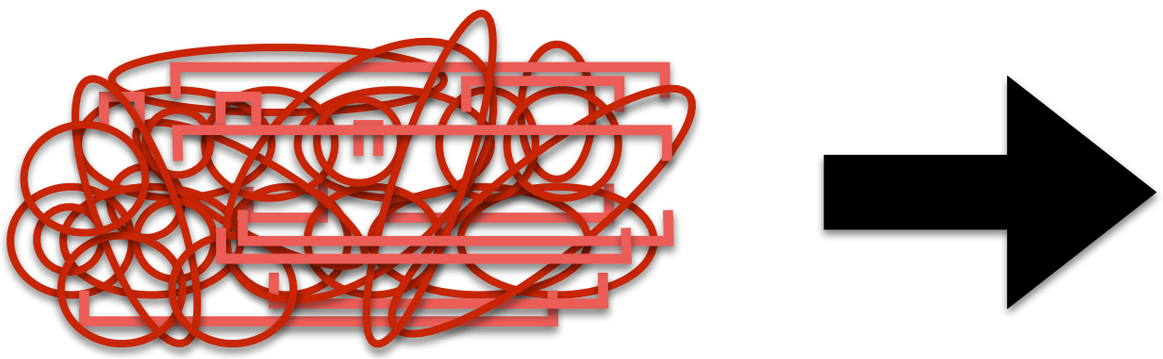
Remaining
uncertainty

How much information about the secret did we **gain** by observing this feature?

$$\mathcal{I}(S;V) = \mathcal{H}(S) - \mathcal{H}(S|V)$$

Initial uncertainty

Remaining uncertainty



Entropy

Classifiers

AI / ML

Which features do we consider?

Which correlations can we learn about?

Library of simple features

Size of *n*-th packet

Time between adjacent packets

Total size (whole interaction)

Total time (whole interaction)

Misaligned packet traces

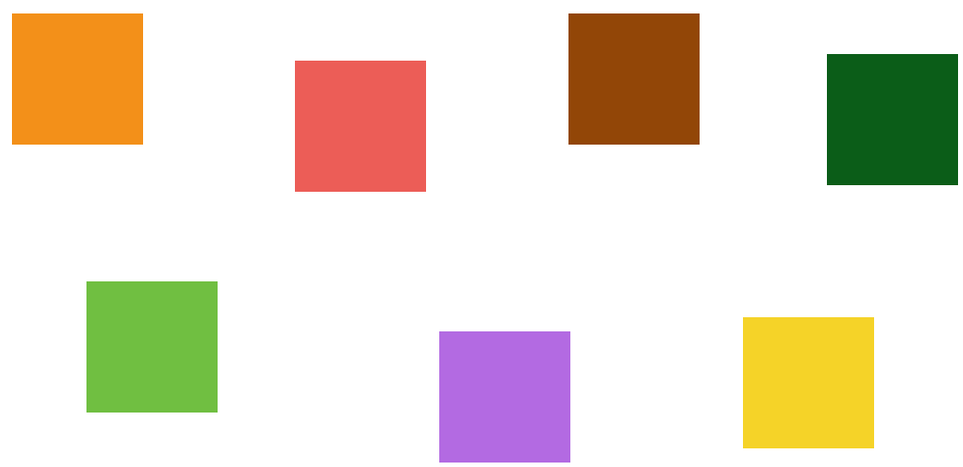
hinder feature extraction,

especially with variable-length actions

Smart alignment

can extract meaningful features

Each square is one packet



Colors represent **size** and **direction**

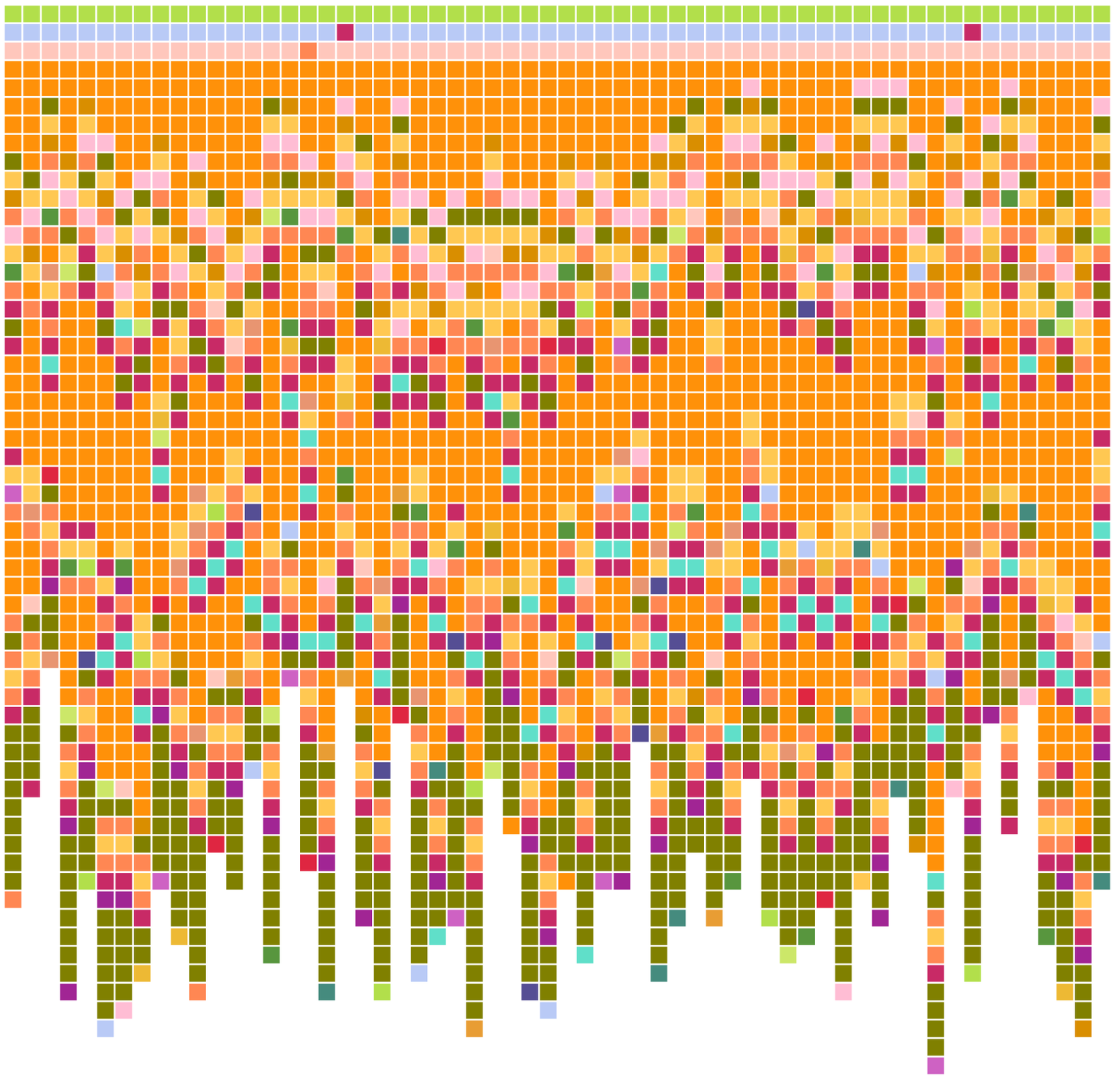
Each time we run an interaction…

…we record a **packet trace**

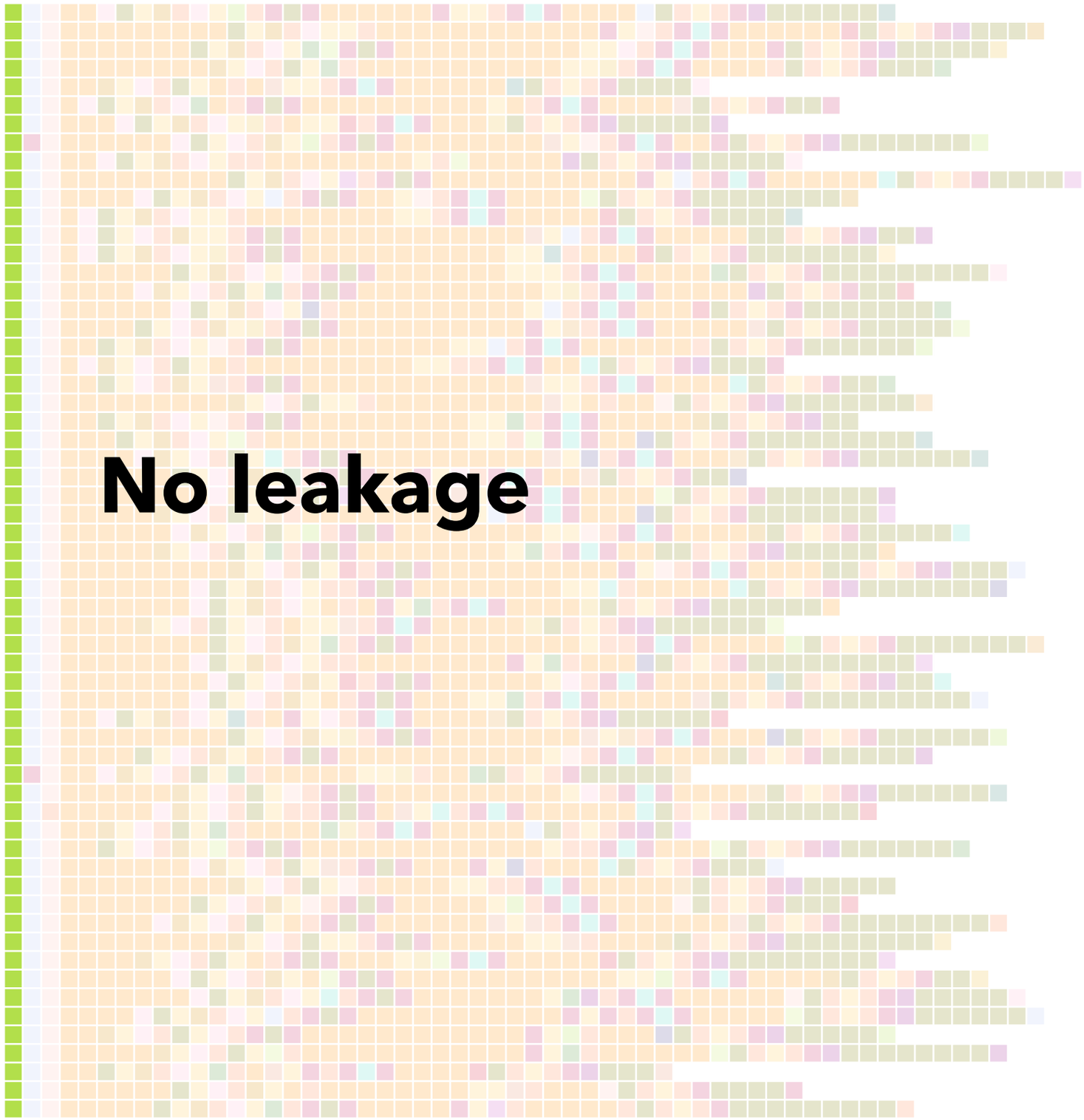
Multiuser chat system

Interaction: Login, then send a message

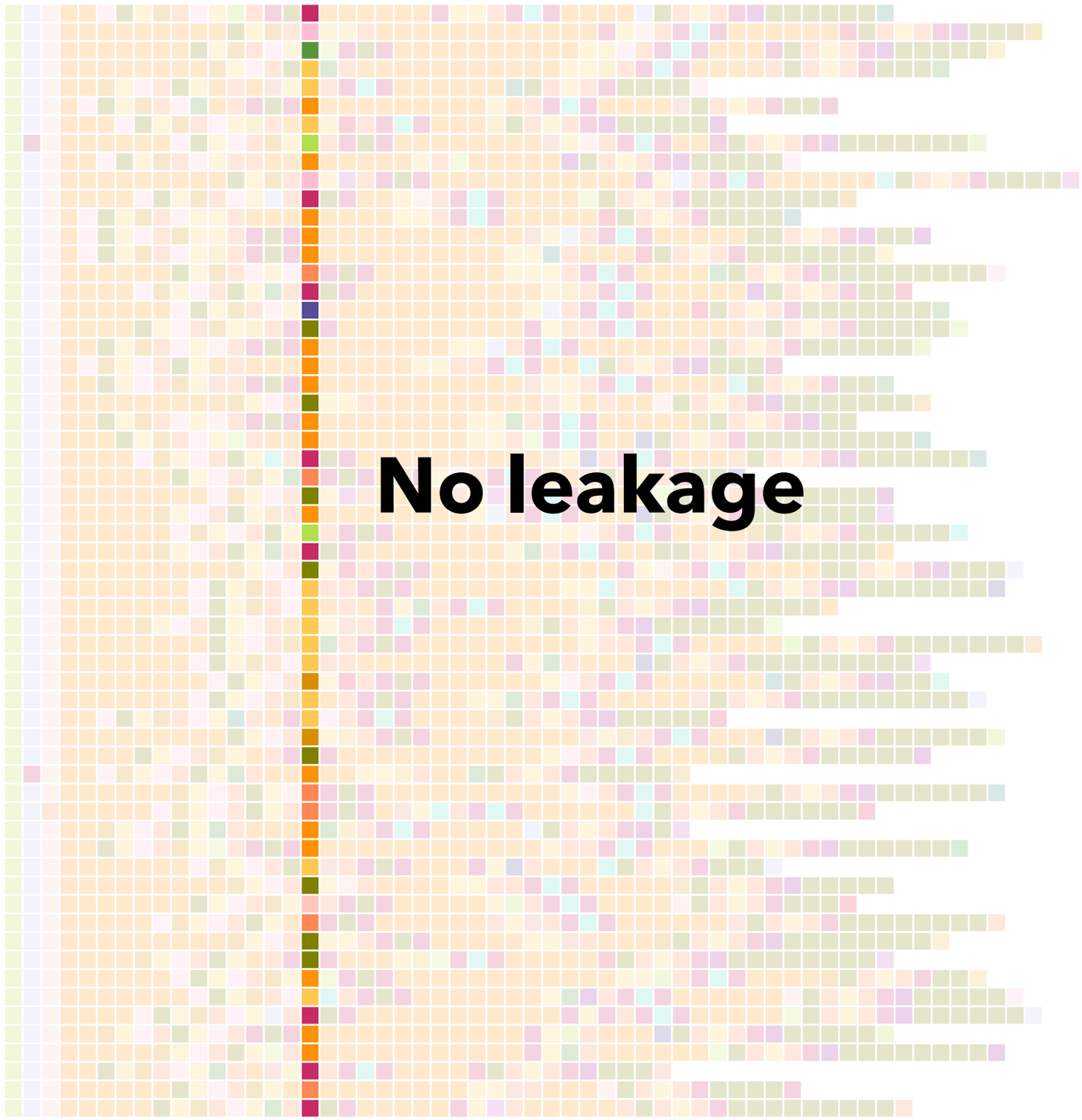
Secret: Location of user during login



Packet #1 of each trace

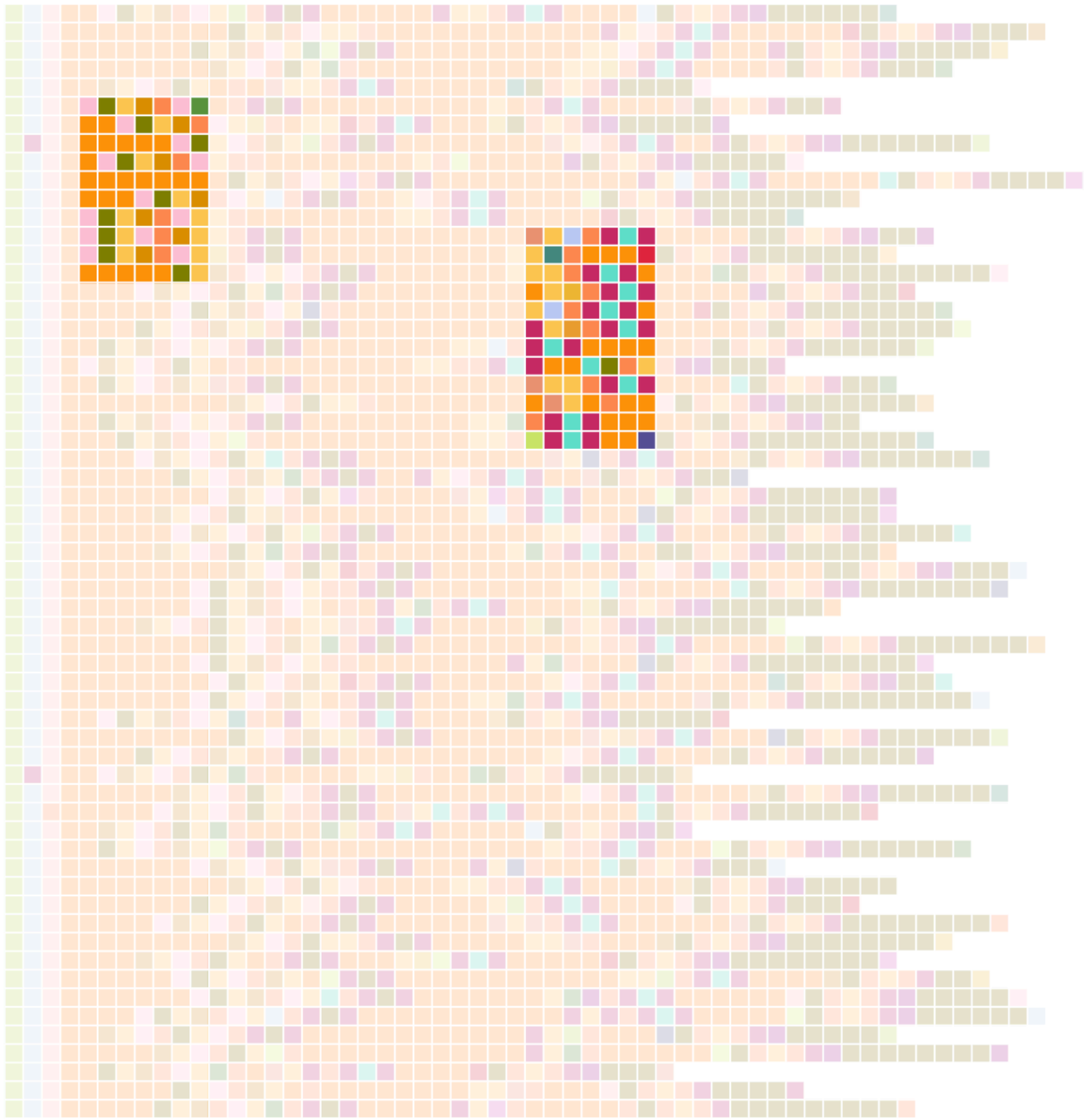


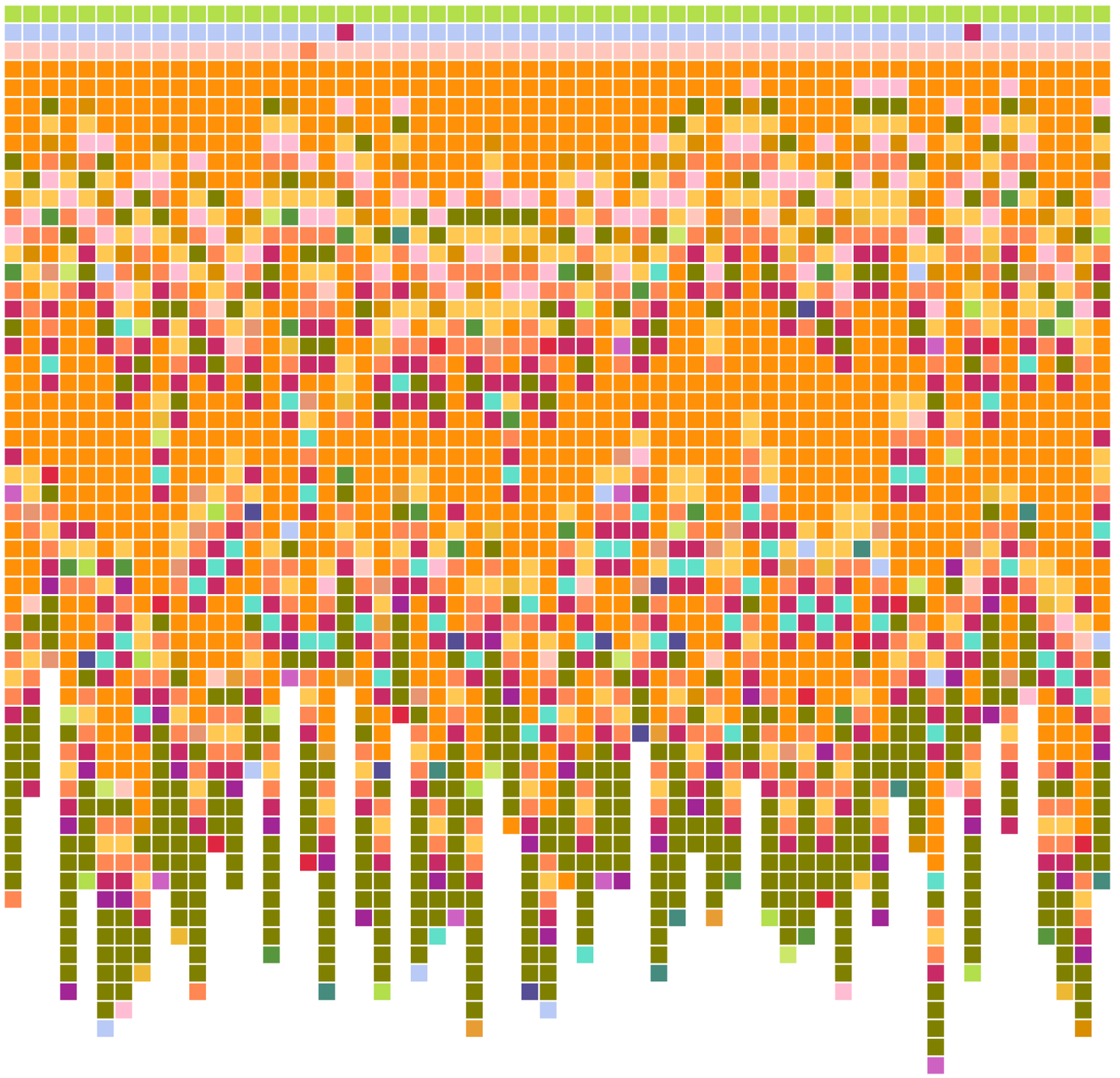
Packet #17 of each trace



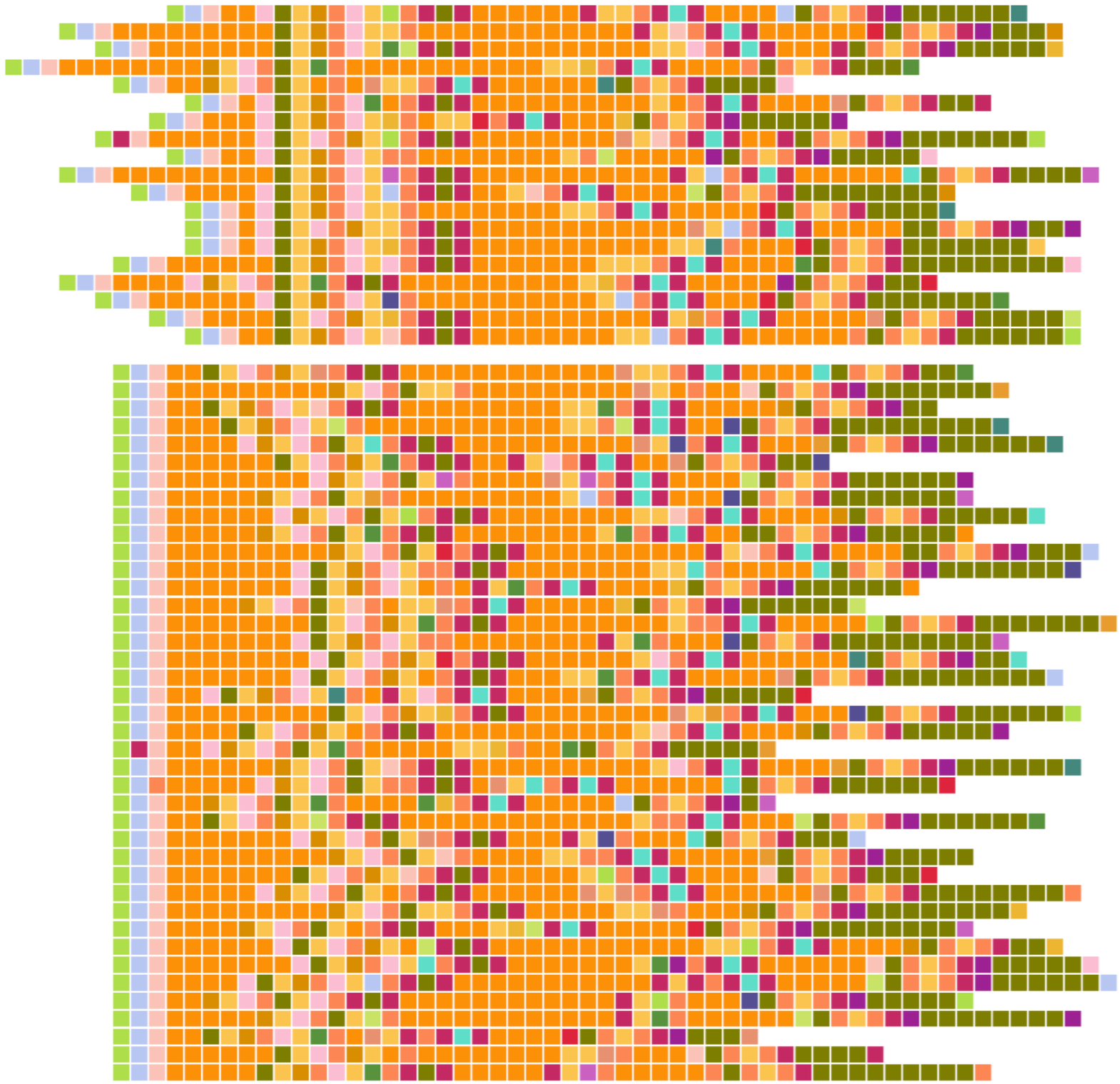
Packet #n of each trace for every possible n

Patterns

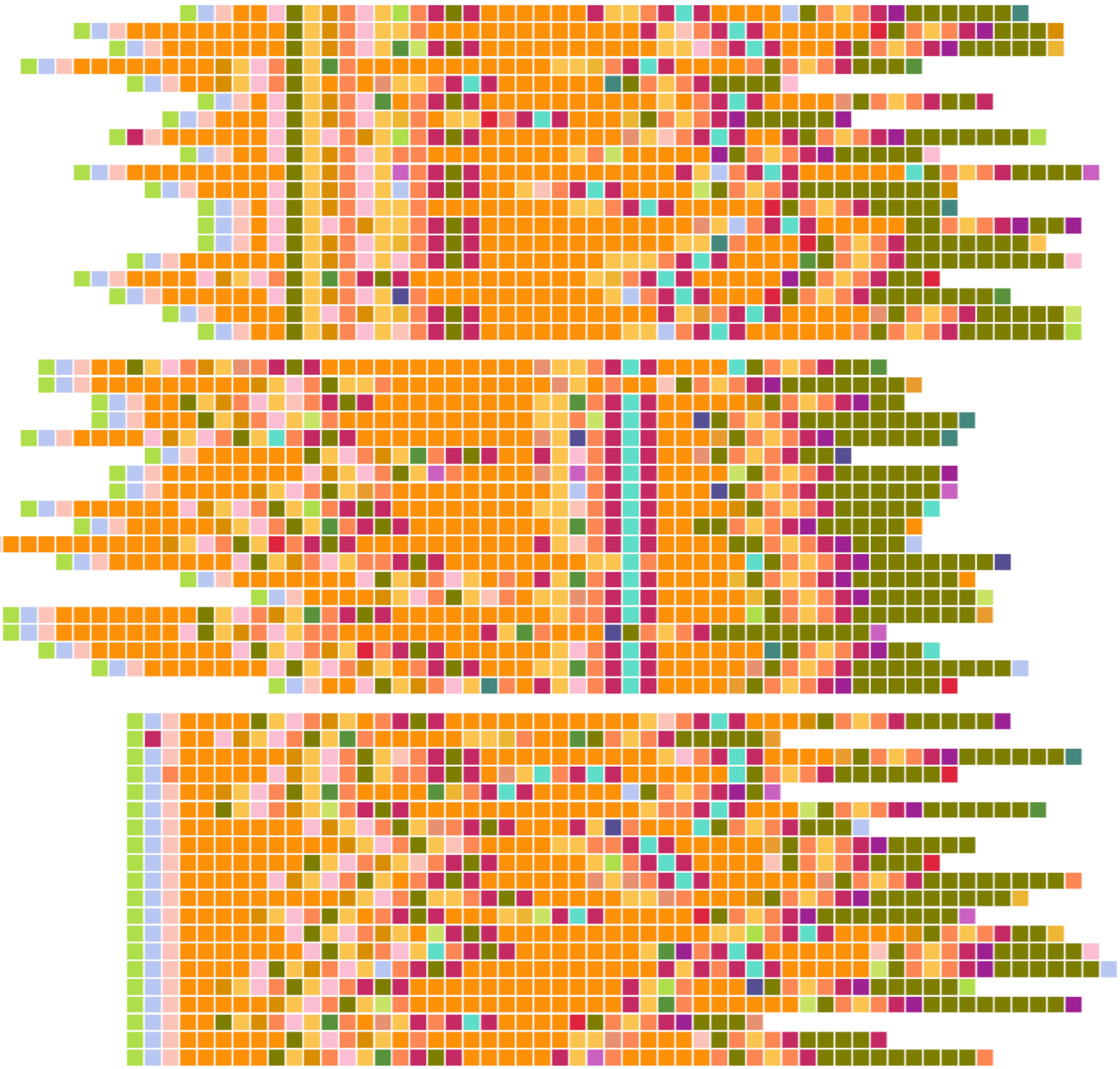




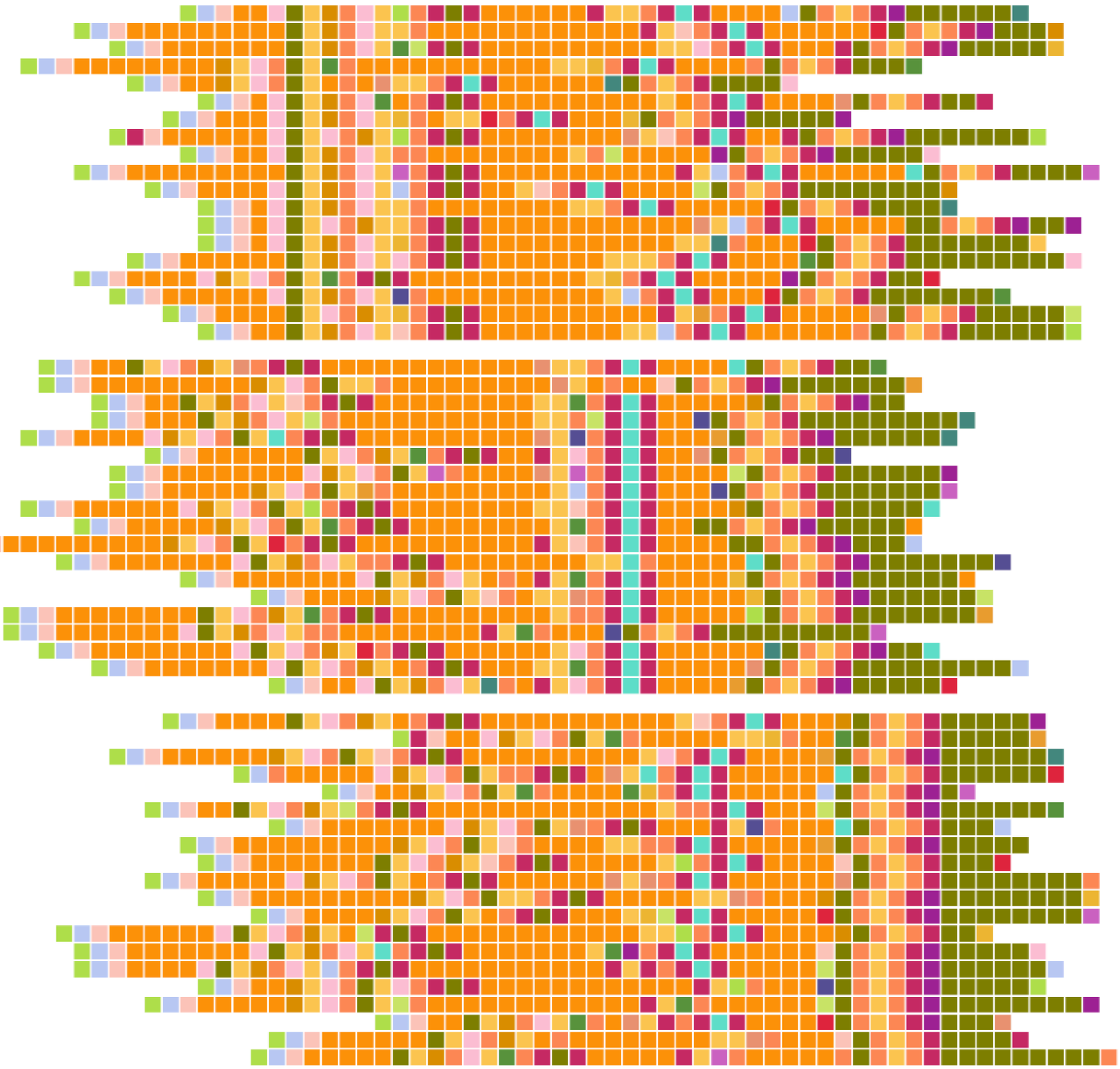
Alignment



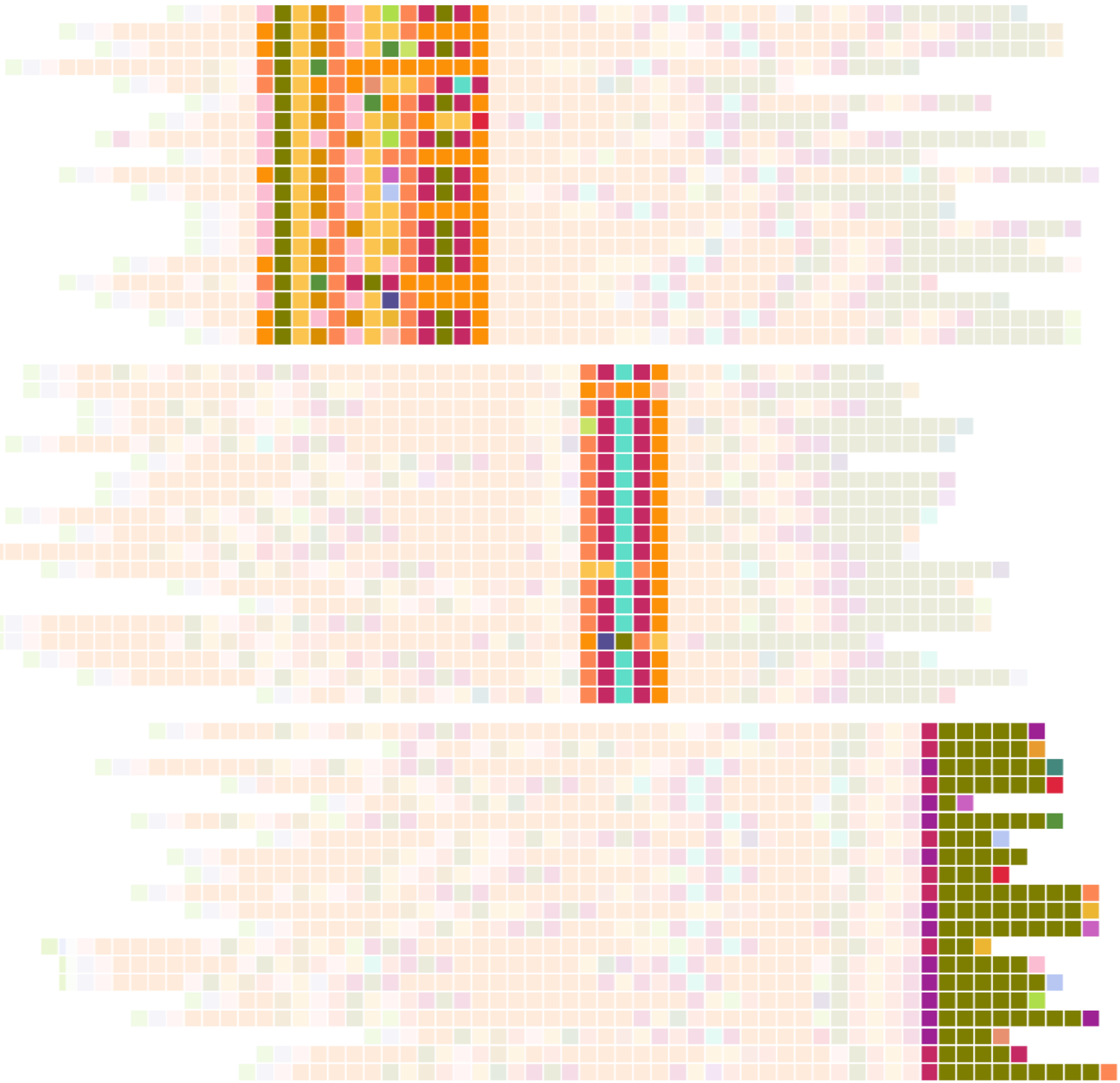
Alignment



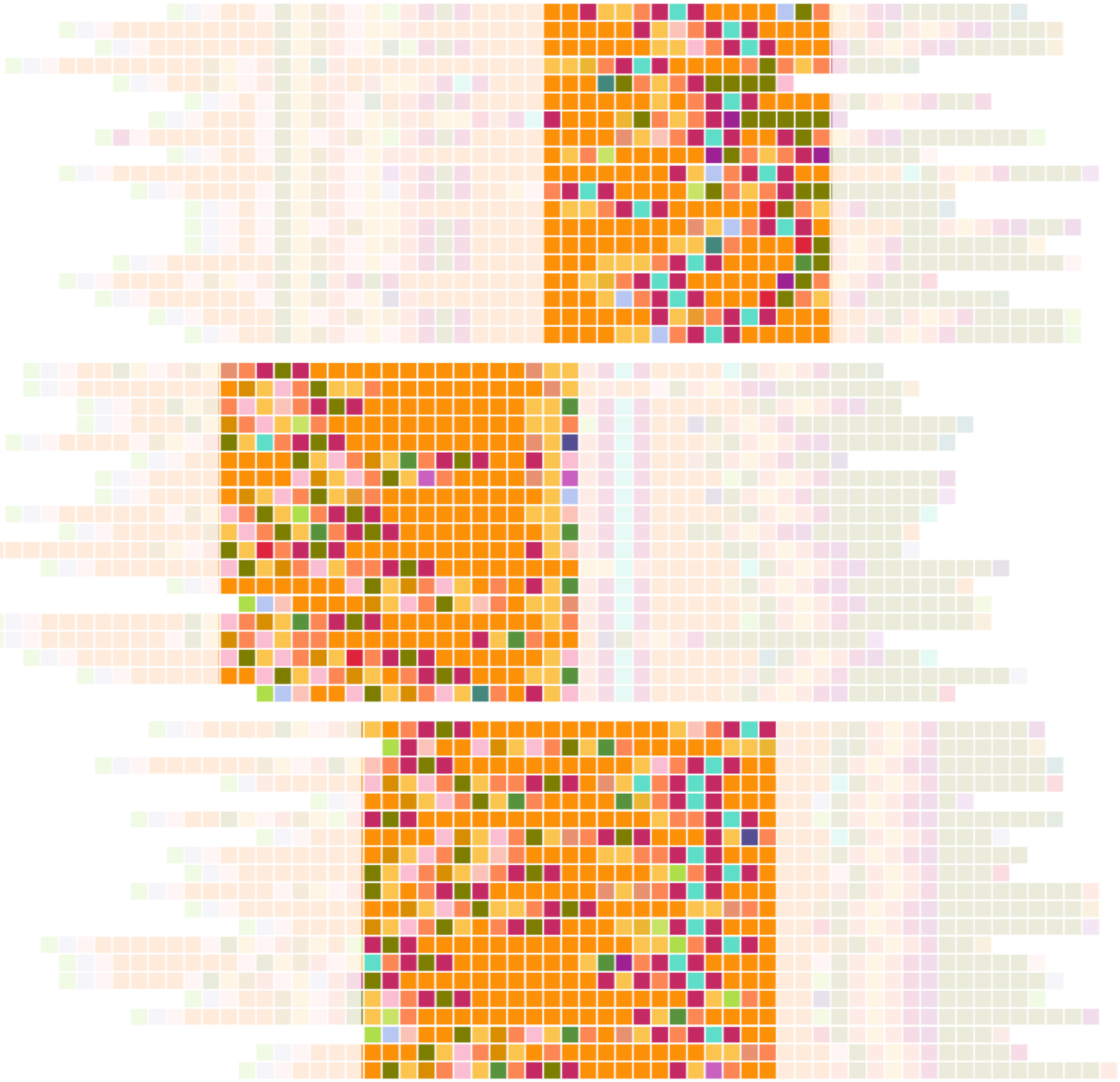
Alignment



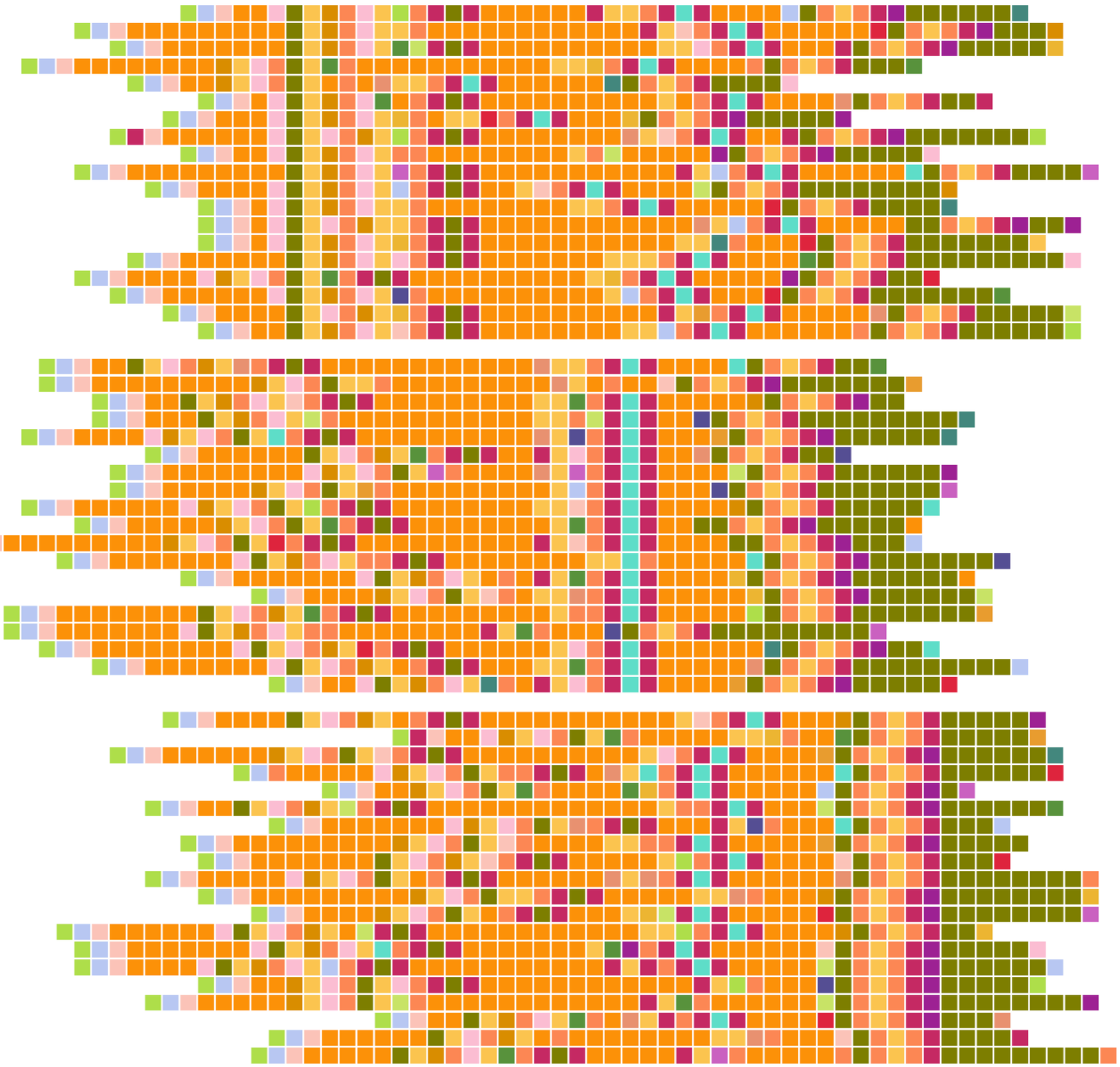
Alignment



Alignment



Alignment



Finding the best alignment for all patterns and all traces

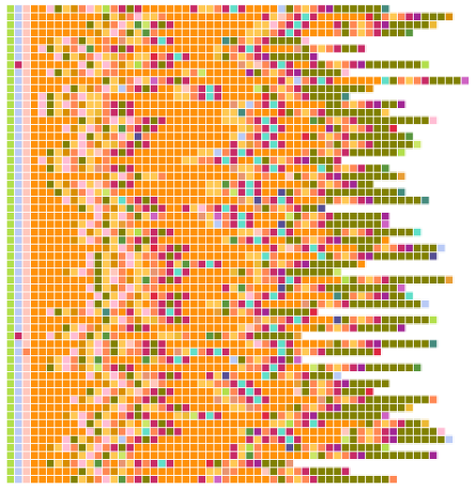
Hard problem!

Computational biology

Multiple sequence alignment

```
GGATGCAACTGGTAGTCCCGCGGACGGCTATGCTAGTCTAATCTCTGGCG
AGATGCAACTAGTTGTCTCGCGGACGGC--TGCTAGTCCATCT------A
AGAGGCAGCTGGTTGTCCCACAGACGGCCATGCTAGACCGGTTTCTACAA
AGAGGCACCTGGTTGTCCCGCAGACGGCCATGCTAGACCAGTTTCTACAA
-------------TAACATGCGGCACGCGCATGCTAGTCCAATCGAAATCG
-------------TAACATGCGGCACGCGCATGCTAGTCCAATTGAAATCG
------TAATATAAGGCACTAGCATGCTTGACGGAGTCCAATGGAGTTCC
------TAATATAAGGCACGCGCCTGCT------AGTCTAATGGAATTCG
```

DNA and protein sequencing

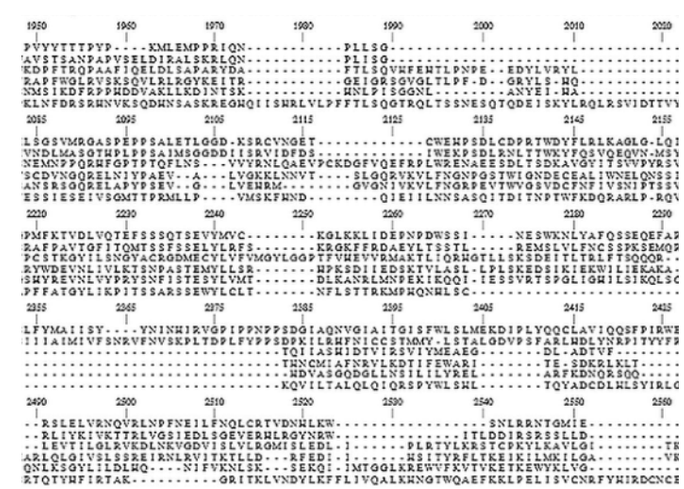


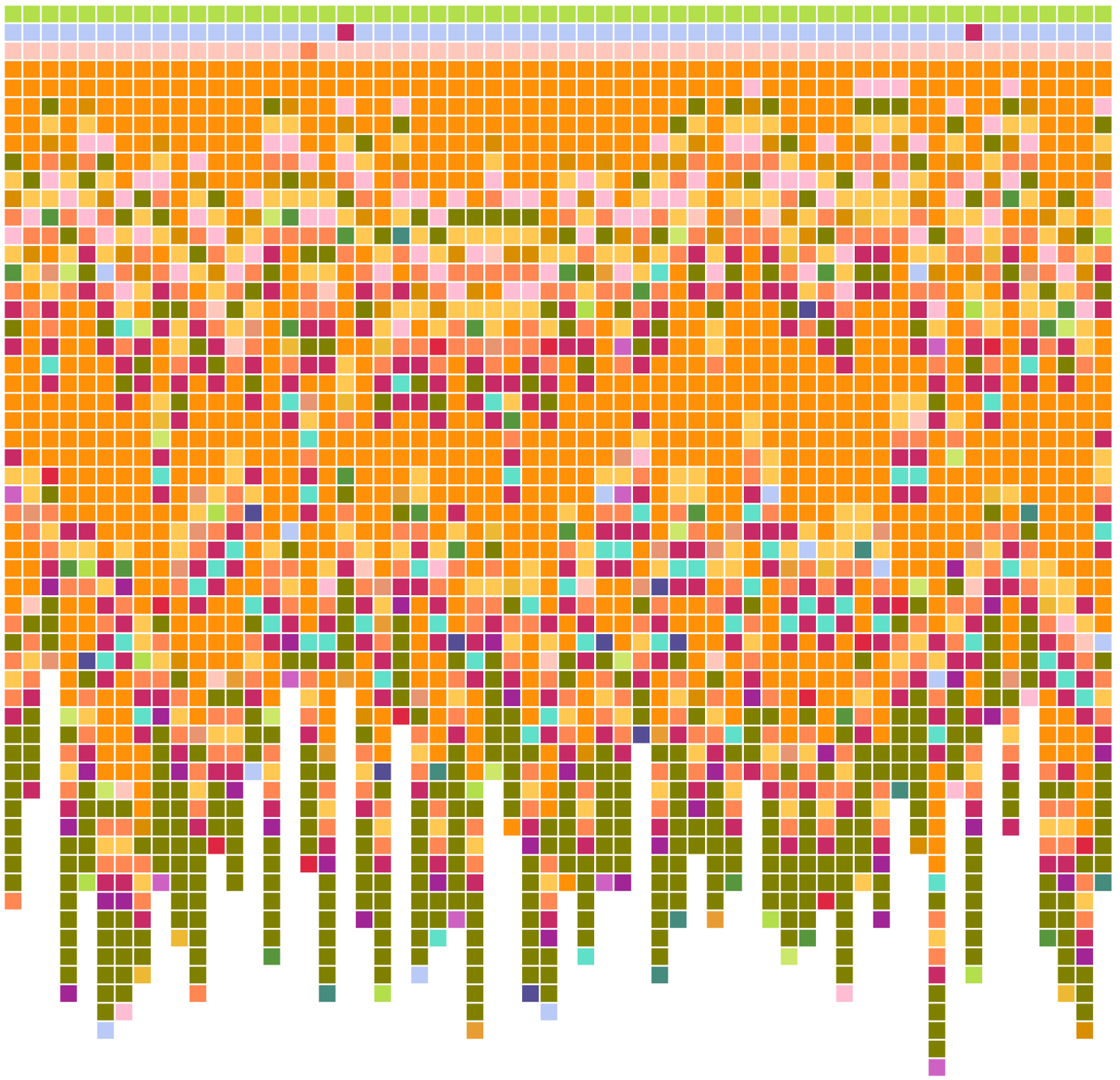
Encode

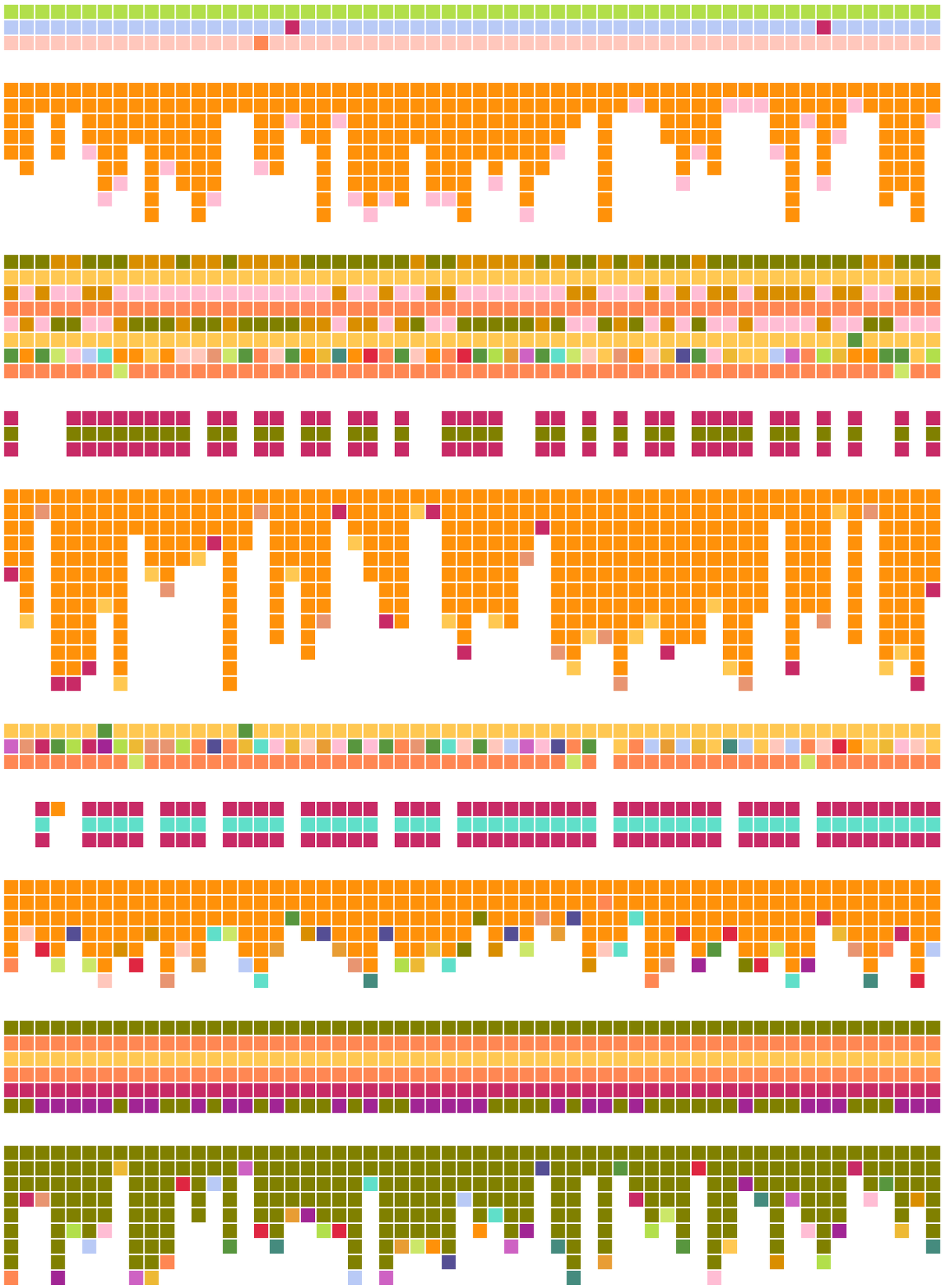
Decode

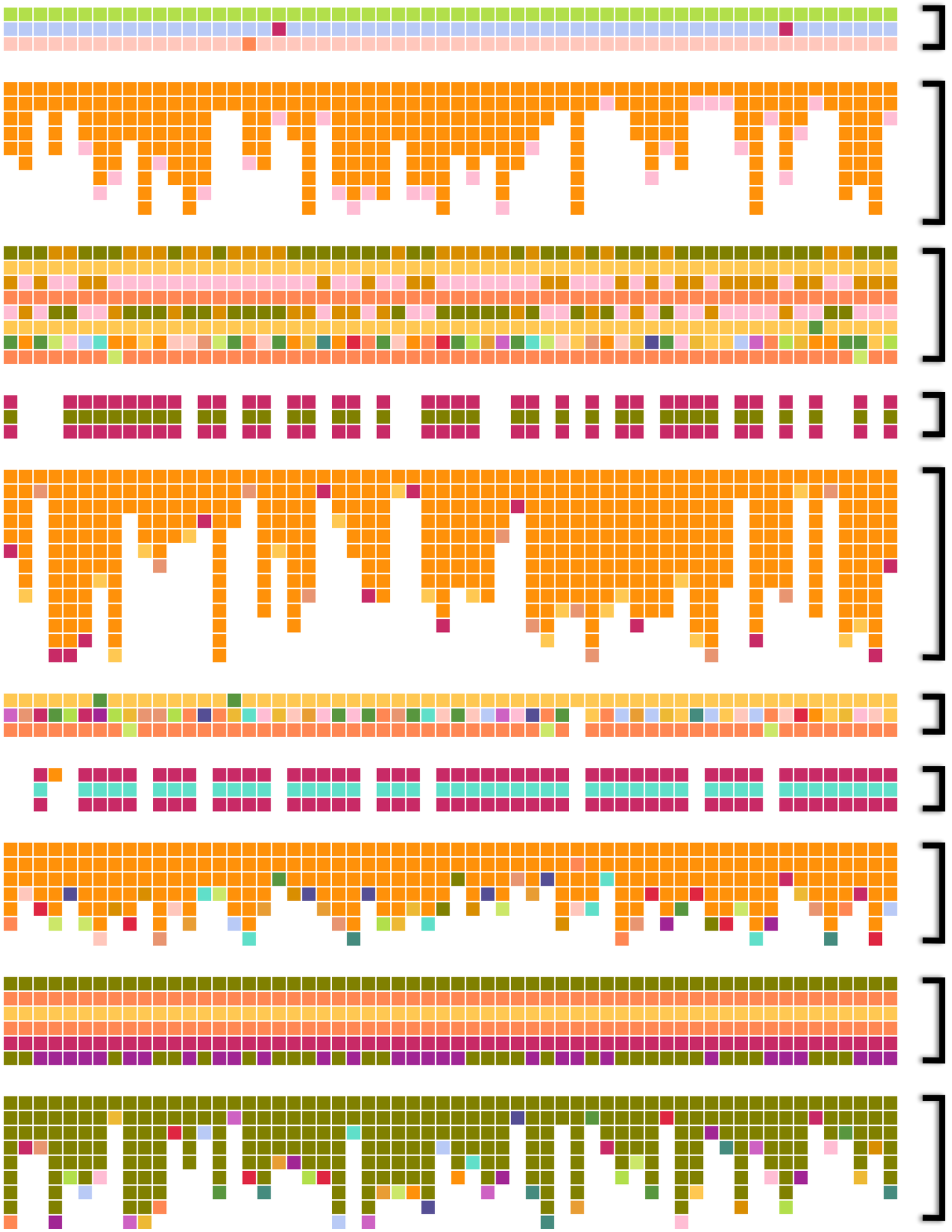
ATTACGTGACGACGAATCGTAGCTACGATCAGCATCGA
GGATTACGTGACGACGAATCGTAGCTACGATCAGCATC
CAGACGTTGAGACGAATCGTAGCTACGATCAGCATCGA
CCATAATTACGTGACGACGAATCGTAGCTACGATCAGC
ATGACTACGTGACGACGAATCGTAGCTACGATCAGCAT
TAGTATGGACGACGAATCGTAGCTACGATCAGCATCGA
GAGACACCACGTGACGACGAATCGTAGCTACGATCAGC
CGTCCGCGTGACGACGAATCGTAGCTACGATCAGCATC
TCCAAATTACGTGACGACGAATCGTAGCTACGATCAGC
GAGACACCACGTGACGACGAATCGTAGCTACGATCAGC
CATGATACGTTGAGACGAATCGTAGCTACGATCATCGA
TAGTATGGACGACGAATCGTAGCTACGATCAGCATCGA
CACCAGGCACGTGACGACGAATCGTAGCTACGATCAGC
CGTCCGCGTGACGACGAATCGTAGCTACGATCAGCATC
ATGACTACGTGACGACGAATCGTAGCTACGATCAGCAT

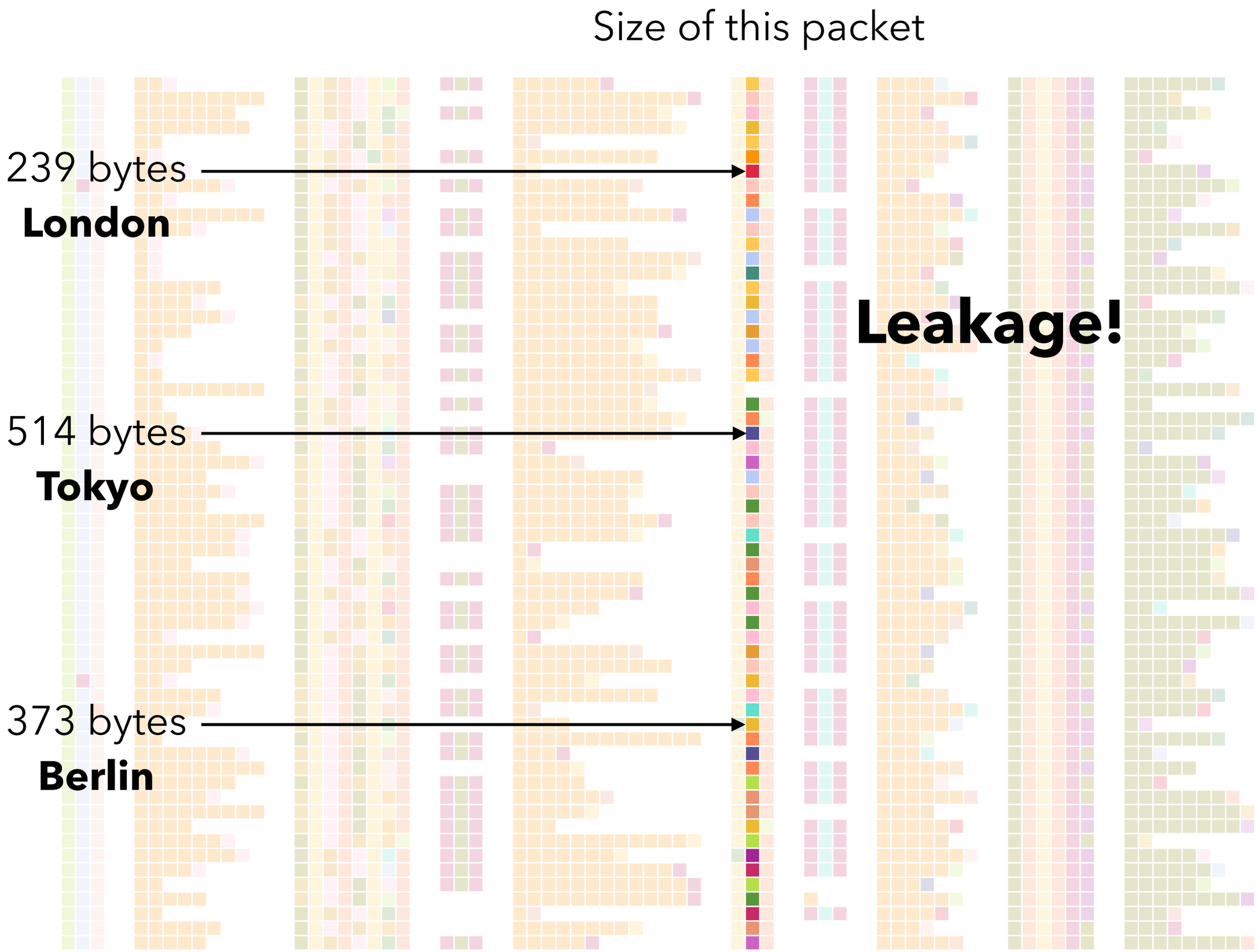
MSA

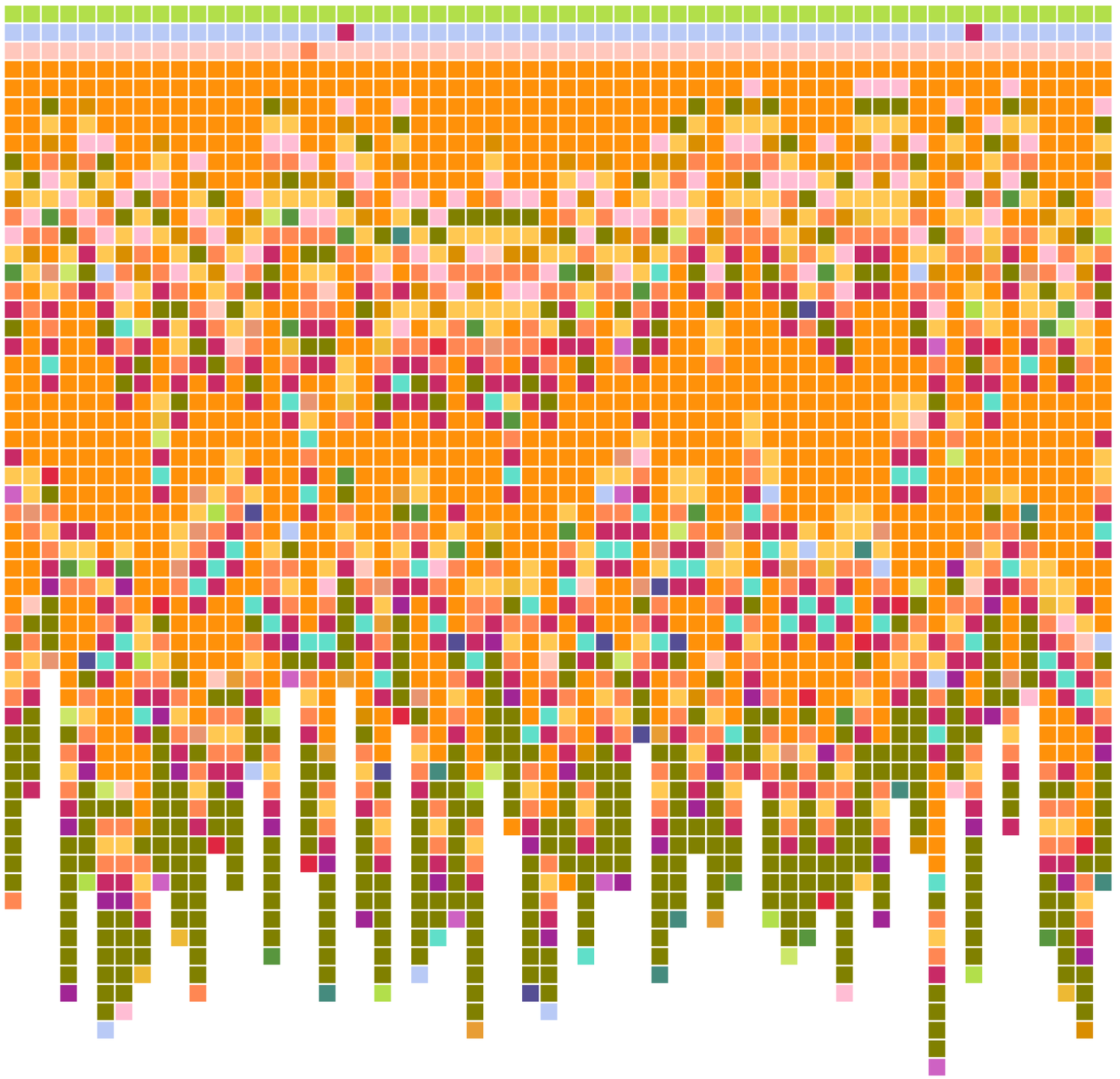




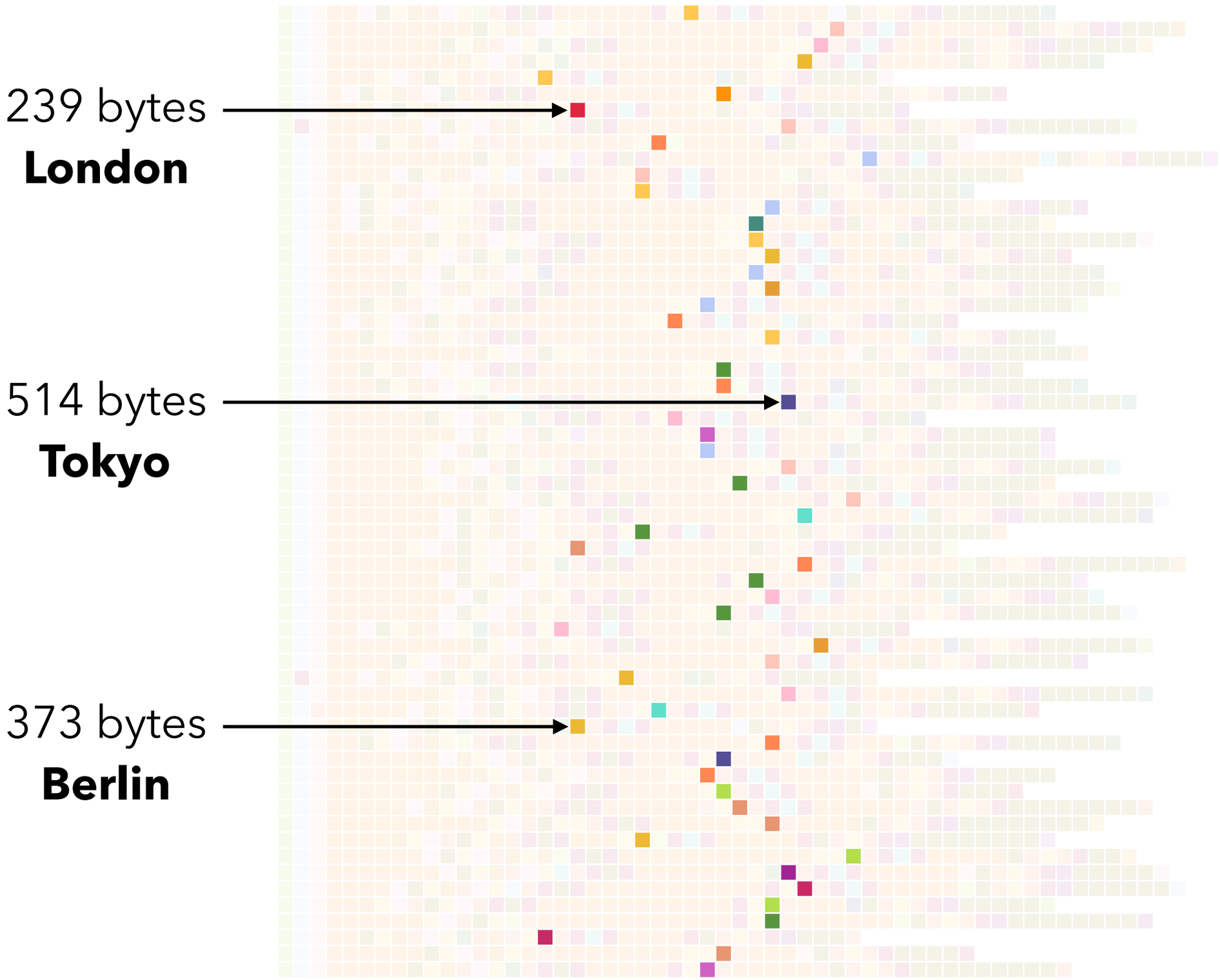




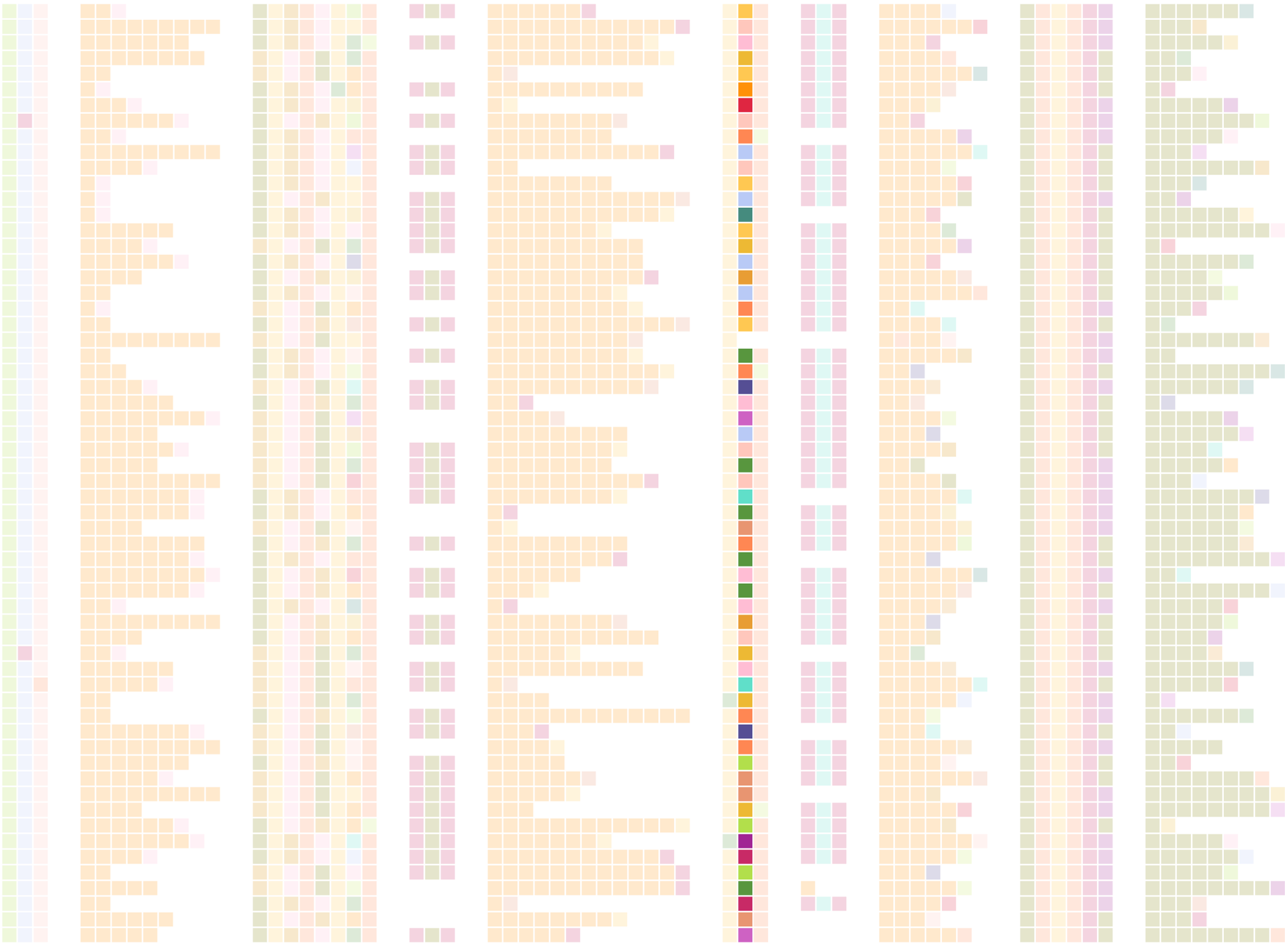

Size of this packet
239 bytes
London
514 bytes
Tokyo
373 bytes
Berlin
Leakage!



How do we call this feature?



Packet #2 of phase #6



Profit's ranking now includes phases

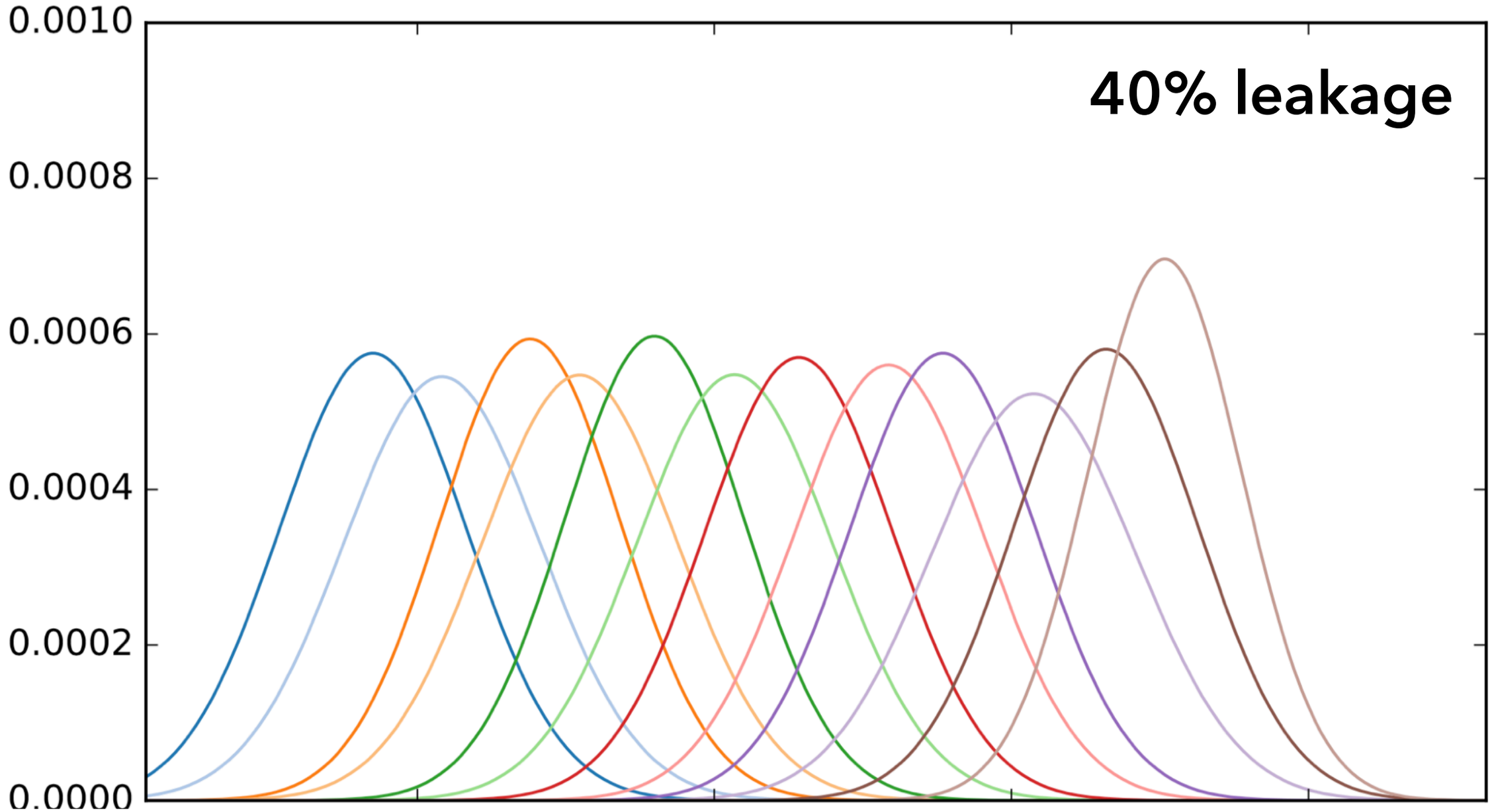
Rank	Leaks	Feature	Direction
1	**97%**	**Size of packet #2 of phase #6**	banjo:22509 –> sax:8443
2	**81%**	**Total size of phase #6**	banjo:22509 –> sax:8443
3	**3%**	**Total time of phase #4**	banjo:22509 <–> sax:8443
4	**2%**	**Total time of full trace**	banjo:22509 <–> sax:8443
5	**2%**	**Size of packet #14 of full trace**	sax:8443 –> banjo:22509

Profit's ranking now includes phases

Rank	Leaks	Feature	Direction
1	**97%**	**Size of packet #2 of phase #6**	banjo:22509 –> sax:8443
2	**81%**	**Total size of phase #6**	banjo:22509 –> sax:8443
3	**3%**	**Total time of phase #4**	banjo:22509 <–> sax:8443
4	**2%**	**Total time of full trace**	banjo:22509 <–> sax:8443
5	**2%**	**Size of packet #14 of full trace**	sax:8443 –> banjo:22509

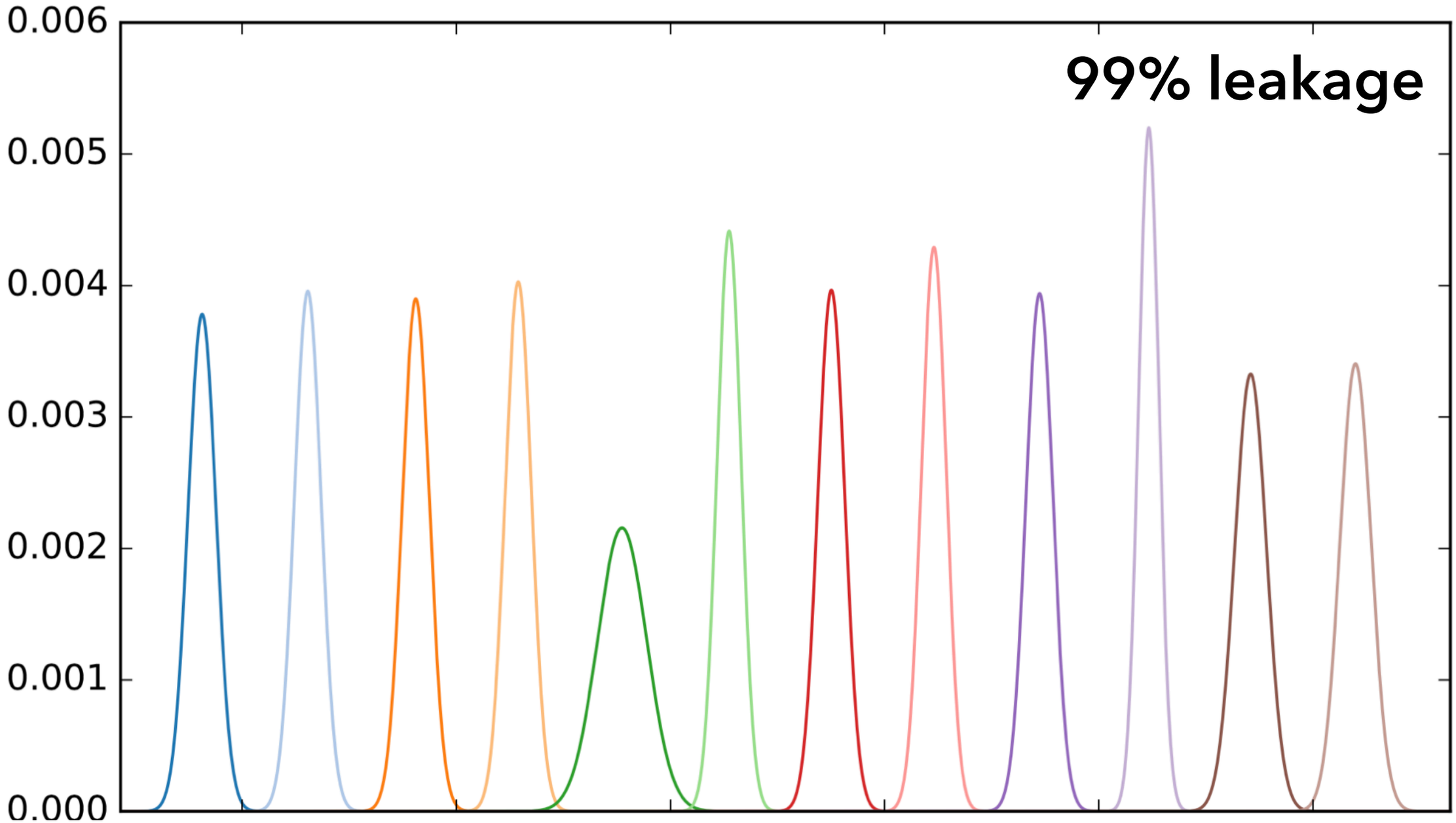
Profit's ranking now includes phases

Rank	Leaks	Feature	Direction
1	**97%**	**Size of packet #2 of phase #6**	banjo:22509 –> sax:8443
2	**81%**	**Total size of phase #6**	banjo:22509 –> sax:8443
3	**3%**	**Total time of phase #4**	banjo:22509 <–> sax:8443
4	**2%**	**Total time of full trace**	banjo:22509 <–> sax:8443
5	**2%**	**Size of packet #14 of full trace**	sax:8443 –> banjo:22509



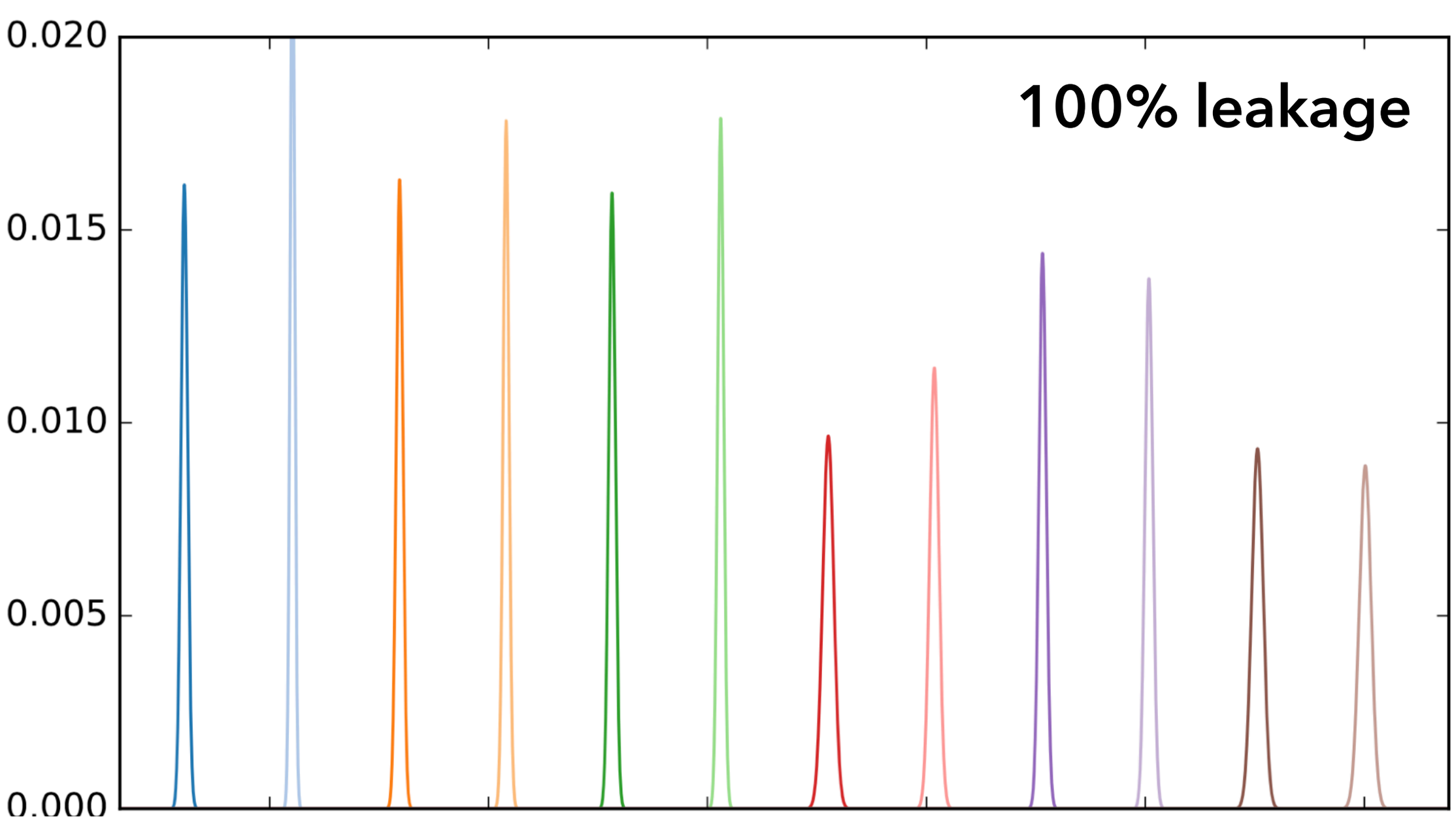
Without phase detection

Top feature: **Duration of whole trace**



With phase detection

Better feature: **Duration of phase #5**



With phase detection

Top feature: **Time between two packets of phase #5**

Excellent results in DARPA challenge

Engagements 4, 5, 6

For side-channel analysis problems
(depending on the metric used)

Often #1 team
Always within top 3

Vulnerable or not?

Consistent with ground truth

Application	Secret	Type	Vulnerability	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Number of cities	Space	Strong	Sum ↓ phase 4	100%
AIRPLAN 5	Number of cities	Space	Medium	Sum ↓ phase 4	79%
AIRPLAN 3	Number of cities	Space	Absent	Packet 20 ↓ full trace	36%
AIRPLAN 3	Strong connectivity	Space	Present	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Strong connectivity	Space	Absent	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Location of user	Space	Present	Sum ↑ phase 2	95%
BIDPAL 2	Secret bid value	Time	Present	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Secret bid value	Time	Absent	Δ 16-17 ↑ full trace	19%
GABFEED 1	Server key Hamming wt.	Time	Present	Δ 6-7 ↓ full trace	100%
GABFEED 5	Server key Hamming wt.	Time	Absent	Δ 6-7 ↓ full trace	24%
GABFEED 2	Server key Hamming wt.	Time	Absent	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Price offered	Time	Present	Total time ↕ full trace	60%
POWERBROKER 2	Price offered	Time	Absent	Total time ↕ full trace	13%
POWERBROKER 4	Price offered	Time	Absent	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Places to visit	Time	Present	Total time ↓ phase 3	30%

Vulnerable or not?

Consistent with ground truth

Application	Secret	Type	Vulnerability	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Number of cities	Space	Strong	Sum ↓ phase 4	100%
AIRPLAN 5	Number of cities	Space	Medium	Sum ↓ phase 4	79%
AIRPLAN 3	Number of cities	Space	Absent	Packet 20 ↓ full trace	36%
AIRPLAN 3	Strong connectivity	Space	Present	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Strong connectivity	Space	Absent	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Location of user	Space	Present	Sum ↑ phase 2	95%
BIDPAL 2	Secret bid value	Time	Present	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Secret bid value	Time	Absent	Δ 16-17 ↑ full trace	19%
GABFEED 1	Server key Hamming wt.	Time	Present	Δ 6-7 ↓ full trace	100%
GABFEED 5	Server key Hamming wt.	Time	Absent	Δ 6-7 ↓ full trace	24%
GABFEED 2	Server key Hamming wt.	Time	Absent	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Price offered	Time	Present	Total time ↕ full trace	60%
POWERBROKER 2	Price offered	Time	Absent	Total time ↕ full trace	13%
POWERBROKER 4	Price offered	Time	Absent	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Places to visit	Time	Present	Total time ↓ phase 3	30%

Vulnerable or not?

Consistent with ground truth

Application	Secret	Type	Vulnerability	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Number of cities	Space	Strong	Sum ↓ phase 4	100%
AIRPLAN 5	Number of cities	Space	Medium	Sum ↓ phase 4	79%
AIRPLAN 3	Number of cities	Space	Absent	Packet 20 ↓ full trace	36%
AIRPLAN 3	Strong connectivity	Space	Present	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Strong connectivity	Space	Absent	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Location of user	Space	Present	Sum ↑ phase 2	95%
BIDPAL 2	Secret bid value	Time	Present	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Secret bid value	Time	Absent	Δ 16-17 ↑ full trace	19%
GABFEED 1	Server key Hamming wt.	Time	Present	Δ 6-7 ↓ full trace	100%
GABFEED 5	Server key Hamming wt.	Time	Absent	Δ 6-7 ↓ full trace	24%
GABFEED 2	Server key Hamming wt.	Time	Absent	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Price offered	Time	Present	Total time ↕ full trace	60%
POWERBROKER 2	Price offered	Time	Absent	Total time ↕ full trace	13%
POWERBROKER 4	Price offered	Time	Absent	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Places to visit	Time	Present	Total time ↓ phase 3	30%

Top-leaking feature

Consistent with ground truth and manual analysis

Application	Vulnerability	Best feature for vulnerability (manually found)	Leak_G	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Strong	Sum ↓ phase 4	100%	Sum ↓ phase 4	100%
AIRPLAN 5	Medium	Sum ↓ phase 4	79%	Sum ↓ phase 4	79%
AIRPLAN 3	Absent	Sum ↓ phase 4	25%	Packet 20 ↓ full trace	36%
AIRPLAN 3	Present	Packet 10 ↓ phase 3	100%	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Absent	Packet 10 ↓ phase 3	0%	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Present	Sum ↑ phase 2	95%	Sum ↑ phase 2	95%
BIDPAL 2	Present	Δ 19-20 ↓ full trace	59%	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Absent	Δ 19-20 ↓ full trace	9%	Δ 16-17 ↑ full trace	19%
GABFEED 1	Present	Δ 6-7 ↓ full trace	100%	Δ 6-7 ↓ full trace	100%
GABFEED 5	Absent	Δ 6-7 ↓ full trace	24%	Δ 6-7 ↓ full trace	24%
GABFEED 2	Absent	Δ 6-7 ↓ full trace	19%	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Present	Δ 9-10 ↑ full trace	60%	Total time ↕ full trace	60%
POWERBROKER 2	Absent	Δ 9-10 ↑ full trace	13%	Total time ↕ full trace	13%
POWERBROKER 4	Absent	Δ 9-10 ↑ full trace	9%	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Present	Total time ↓ phase 3	30%	Total time ↓ phase 3	30%

Top-leaking feature

Consistent with ground truth and manual analysis

Application	Vulnerability	Best feature for vulnerability (manually found)	Leak_G	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Strong	Sum ↓ phase 4	100%	Sum ↓ phase 4	100%
AIRPLAN 5	Medium	Sum ↓ phase 4	79%	Sum ↓ phase 4	79%
AIRPLAN 3	Absent	Sum ↓ phase 4	25%	Packet 20 ↓ full trace	36%
AIRPLAN 3	Present	Packet 10 ↓ phase 3	100%	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Absent	Packet 10 ↓ phase 3	0%	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Present	Sum ↑ phase 2	95%	Sum ↑ phase 2	95%
BIDPAL 2	Present	Δ 19-20 ↓ full trace	59%	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Absent	Δ 19-20 ↓ full trace	9%	Δ 16-17 ↑ full trace	19%
GABFEED 1	Present	Δ 6-7 ↓ full trace	100%	Δ 6-7 ↓ full trace	100%
GABFEED 5	Absent	Δ 6-7 ↓ full trace	24%	Δ 6-7 ↓ full trace	24%
GABFEED 2	Absent	Δ 6-7 ↓ full trace	19%	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Present	Δ 9-10 ↑ full trace	60%	Total time ↕ full trace	60%
POWERBROKER 2	Absent	Δ 9-10 ↑ full trace	13%	Total time ↕ full trace	13%
POWERBROKER 4	Absent	Δ 9-10 ↑ full trace	9%	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Present	Total time ↓ phase 3	30%	Total time ↓ phase 3	30%

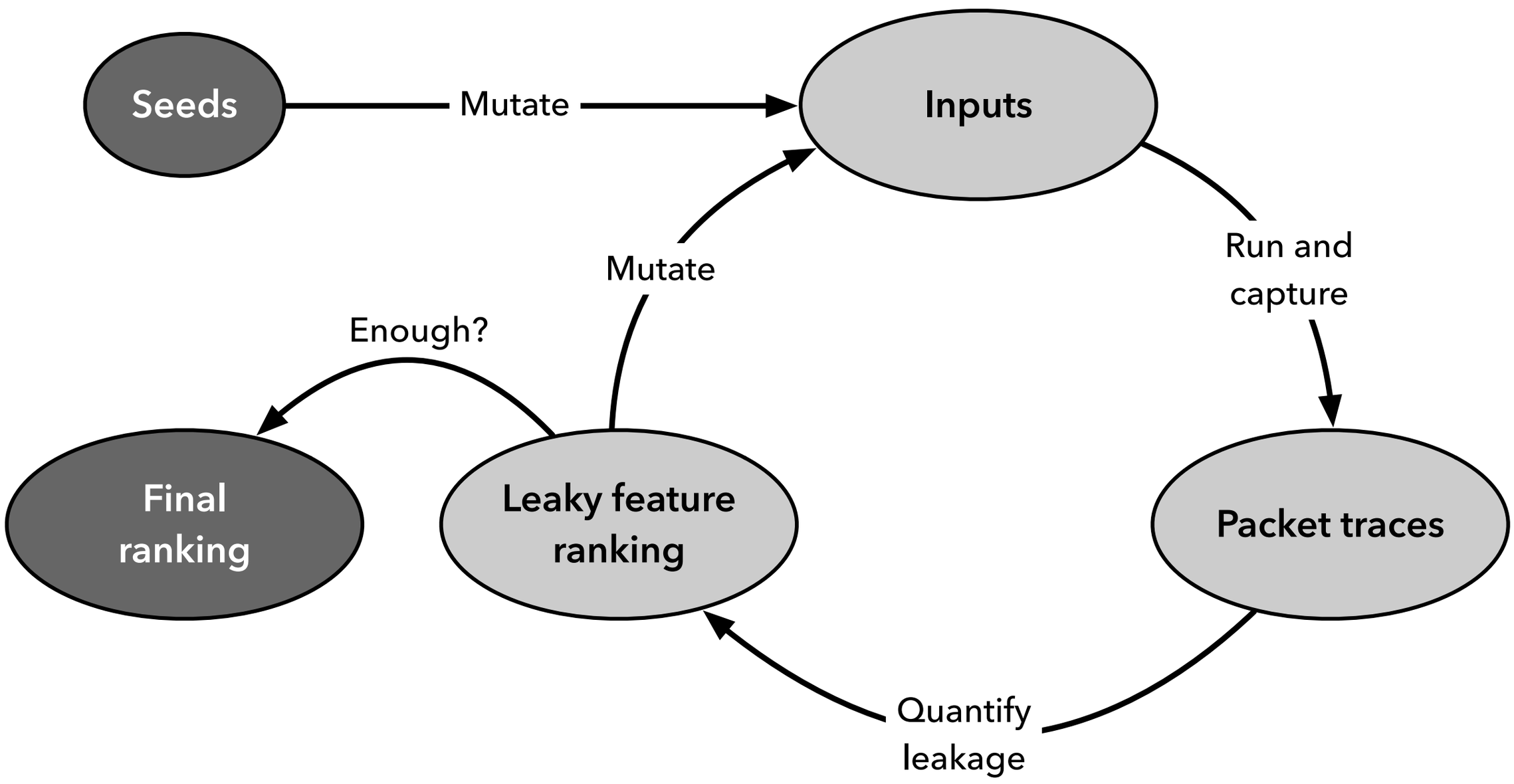
Top-leaking feature

Consistent with ground truth and manual analysis

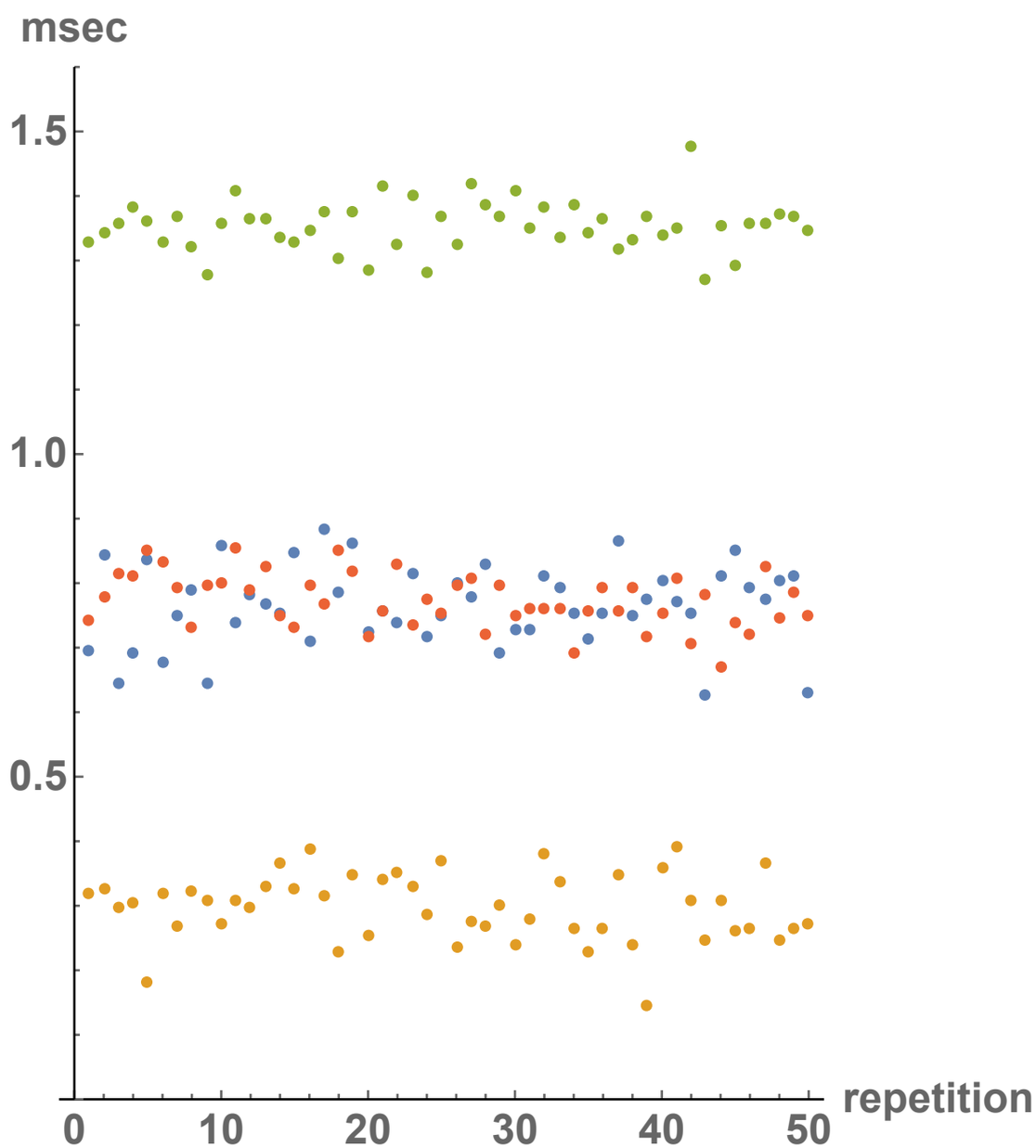
Application	Vulnerability	Best feature for vulnerability (manually found)	Leak_G	Top-ranking feature (reported by Profit)	Leak_G
AIRPLAN 2	Strong	Sum ↓ phase 4	100%	Sum ↓ phase 4	100%
AIRPLAN 5	Medium	Sum ↓ phase 4	79%	Sum ↓ phase 4	79%
AIRPLAN 3	Absent	Sum ↓ phase 4	25%	Packet 20 ↓ full trace	36%
AIRPLAN 3	Present	Packet 10 ↓ phase 3	100%	Packet 10 ↓ phase 3	100%
AIRPLAN 4	Absent	Packet 10 ↓ phase 3	0%	Packet 1 ↑ phase 2	4%
SNAPBUDDY 1	Present	Sum ↑ phase 2	95%	Sum ↑ phase 2	95%
BIDPAL 2	Present	Δ 19-20 ↓ full trace	59%	Δ 19-20 ↓ full trace	59%
BIDPAL 1	Absent	Δ 19-20 ↓ full trace	9%	Δ 16-17 ↑ full trace	19%
GABFEED 1	Present	Δ 6-7 ↓ full trace	100%	Δ 6-7 ↓ full trace	100%
GABFEED 5	Absent	Δ 6-7 ↓ full trace	24%	Δ 6-7 ↓ full trace	24%
GABFEED 2	Absent	Δ 6-7 ↓ full trace	19%	Δ 11-12 ↕ full trace	20%
POWERBROKER 1	Present	Δ 9-10 ↑ full trace	60%	Total time ↕ full trace	60%
POWERBROKER 2	Absent	Δ 9-10 ↑ full trace	13%	Total time ↕ full trace	13%
POWERBROKER 4	Absent	Δ 9-10 ↑ full trace	9%	Δ 16-17 ↑ full trace	18%
TOURPLANNER	Present	Total time ↓ phase 3	30%	Total time ↓ phase 3	30%

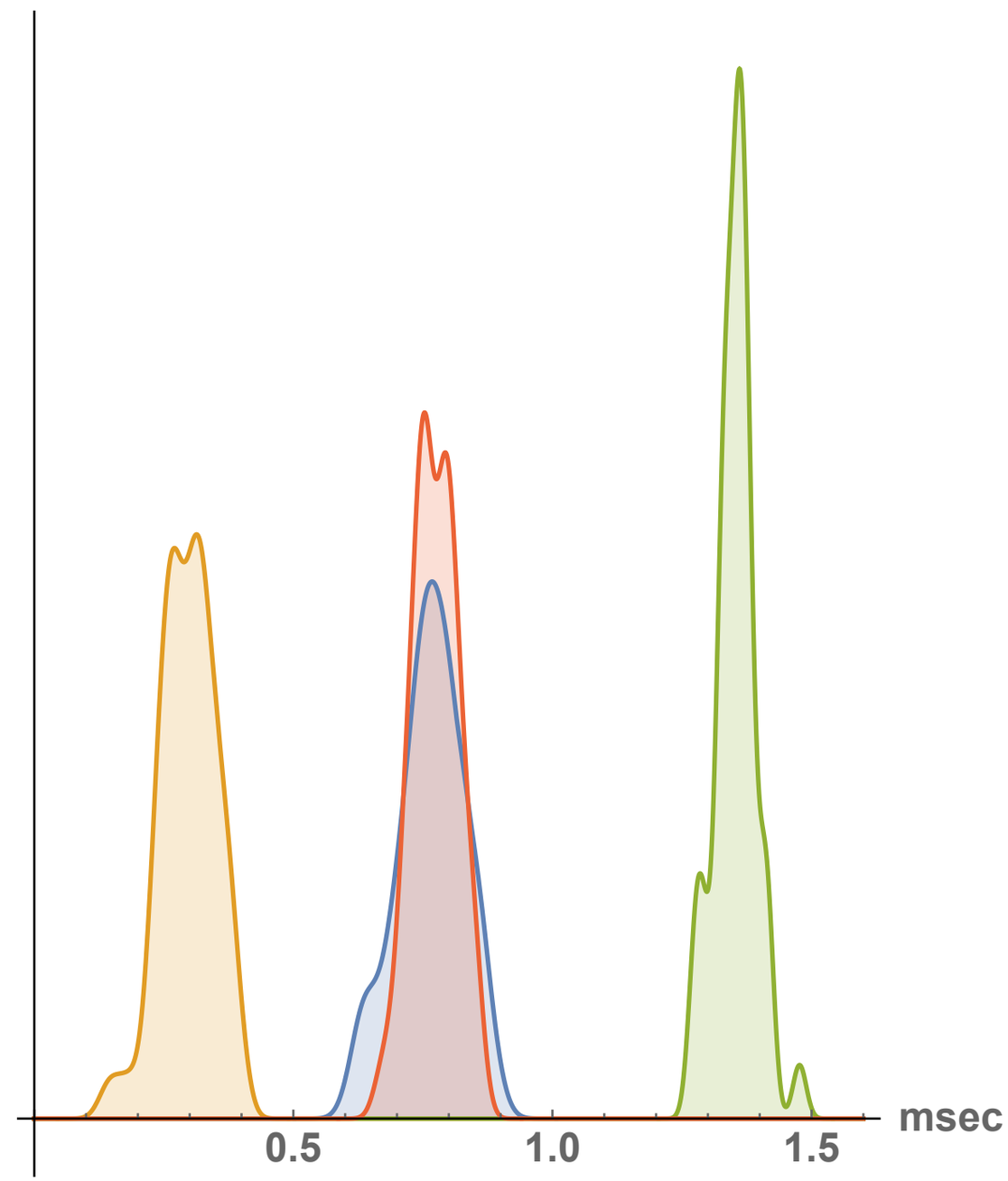
Ongoing work

Feedback-driven mutation



Self-adjusting noise modeling





Thank you!