Davide Ceneda
Marco Di Bartolomeo
Valentino Di Donato
Maurizio Patrignani
Maurizio Pizzonia
Massimo Rimondini

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

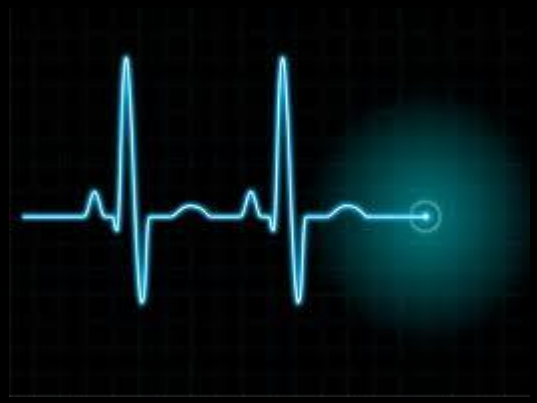
Visual Exploration and Analysis of Routing Events

Davide Ceneda
Marco Di Bartolomeo
Valentino Di Donato
Maurizio Patrignani
Maurizio Pizzonia
Massimo Rimondini

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events



ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI
Department of Engineering

RoutingWatch

Visual Exploration and Analysis of Routing Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

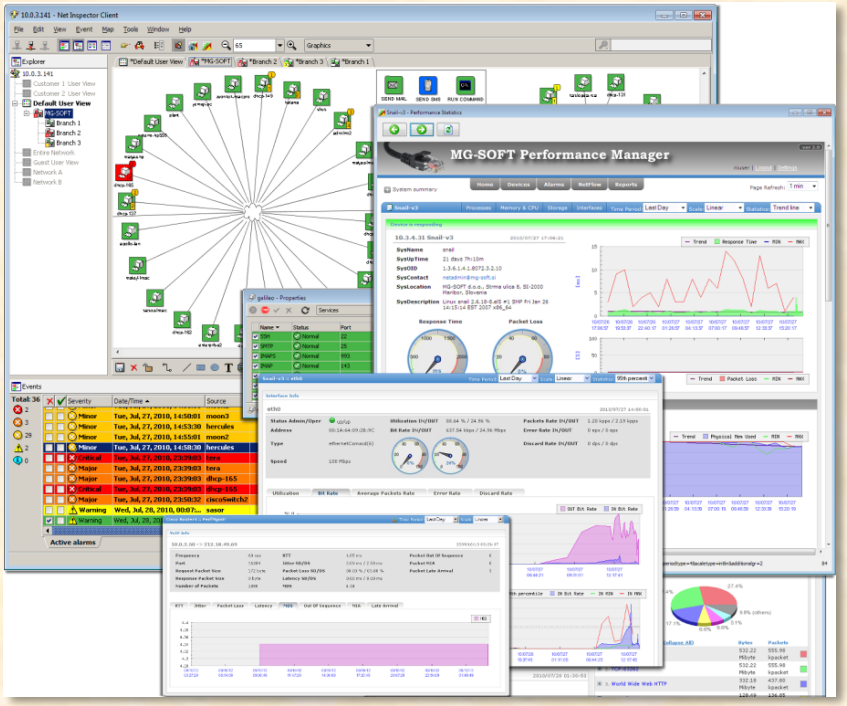
Management & Monitoring Tools	Inference Algorithms	Visualization Systems

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

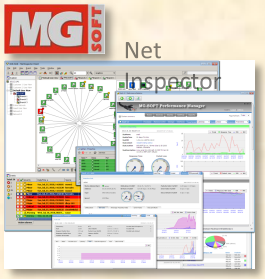
Management & Monitoring Tools | Inference Algorithms | Visualization Systems

Net Inspector



State of the Art

Management & Monitoring Tools | Inference Algorithms | Visualization Systems



CISCO™ Embedded Event Manager

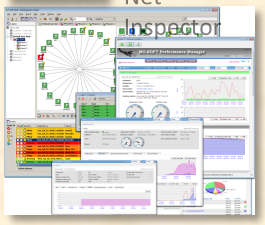
```
event manager applet interface_Shutdown
event syslog pattern "Interface FastEthernet1/0, changed
      state to administratively down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface fa1/0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"
action 3.5 cli command "who"
action 4.0 mail server "192.168.1.1" to
      ".engineer@cisco.com." from ".EEM@cisco.com."
      subject ".ISP1_Interface_fa1/0_SHUT." body "Current
      users $_cli_result"
```

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | Inference Algorithms | Visualization Systems

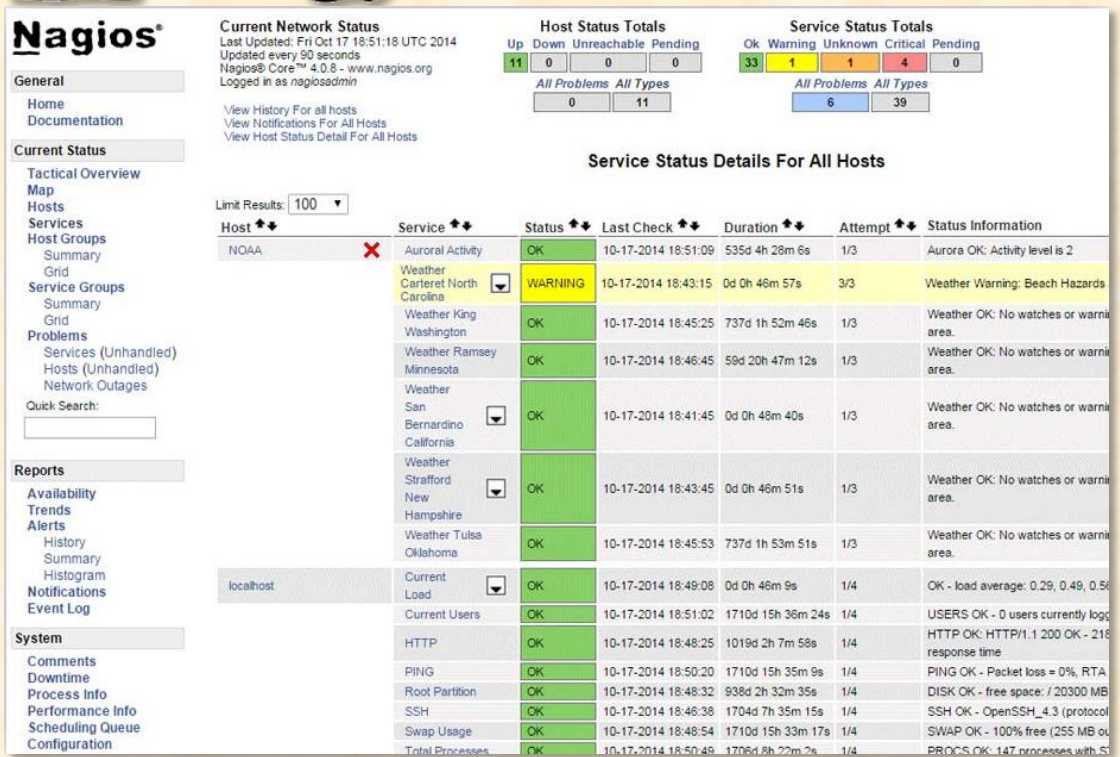
MG SOFT Net Inspector



CISCO Embedded Event Manager

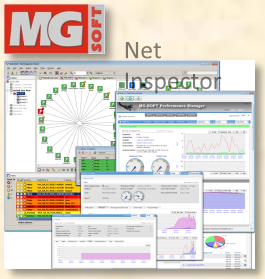
```
event manager applet ISP1_Interface_Shutdown
event syslog pattern "Interface FastEthernet1/0,
                      changed state to administratively
                      down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface fa1/0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"
action 3.5 cli command "who"
action 4.0 mail server "192.168.1.1" to
                      ".engineer@cisco.com." from
                      ".EEM@cisco.com." subject
                      ".ISP1_Interface_fa1/0_SHUT." body
                      "Current users $_cli_result"
```

Nagios® Monitoring System



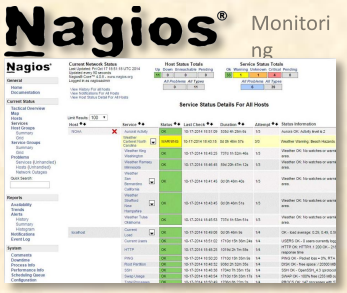
State of the Art

Management & Monitoring Tools | Inference Algorithms | Visualization Systems



Embedded Event Manager

```
event manager applet Interface_Shutdown
event syslog pattern "Interface FastEthernet1/0,
                      changed state to administratively
                      down"
action 1.0 cli command "enable"
action 1.5 cli command "config t"
action 2.0 cli command "interface fa1/0"
action 2.5 cli command "no shutdown"
action 3.0 cli command "end"
action 3.5 cli command "who"
action 4.0 mail server "192.168.1.1" to
                      ".engineer@cisco.com." from
                      ".EEM@cisco.com." subject
                      ".ISP1_Interface_fa1/0_SHUT." body
                      "Current users $_cli_result"
```

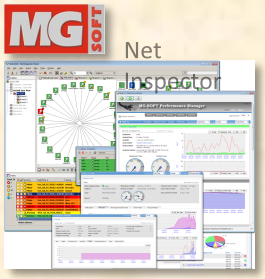


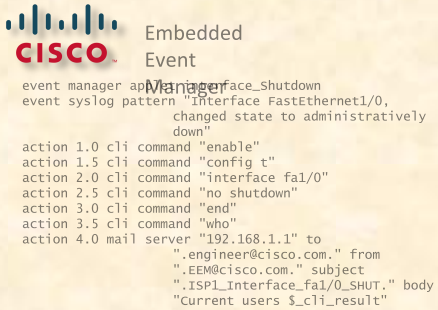
Monitoring

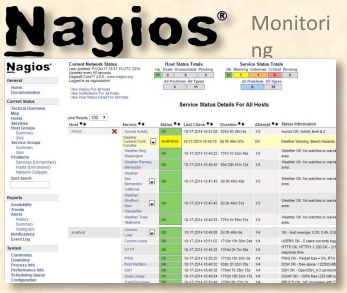
- Raise alarms based on unexpected changes in:
  - performance levels (bandwidth)
  - health flags (interface status)
  - configurations

State of the Art

Management & Monitoring Tools | Inference Algorithms | Visualization Systems







- Raise alarms based on unexpected changes in:
  - performance levels (bandwidth)
  - health flags (interface status)
  - configurations
- Require polling and/or agents
- Must support many technologies

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, “Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network”. Proc. NSDI, 2005
  - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, “Studying Interdomain Routing over Long Timescales”. Proc. IMC, 2013
  - Evolution of the Routing State Distance
- G. Comarela and M. Crovella, “Identifying and Analyzing High Impact Routing Events with PathMiner”. Proc. IMC, 2014
  - Next-hop tensor factorization

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network". Proc. NSDI, 2005
  - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, "Studying Interdomain Routing over Long Timescales". Proc. IMC, 2013
  - Evolution of the Routing State Distance
- G. Comarela and M. Crovella, "Identifying and Analyzing High Impact Routing Events with PathMiner". Proc. IMC, 2014
  - Next-hop tensor factorization

- Focus on BGP
- Long-term Internet evolution studies
- Limited information about each event (typically, cause AS)

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- J. Wu, Z. M. Mao, J. Rexford, and J. Wang, "Finding a Needle in a Haystack: Pinpointing Significant BGP Routing Changes in an IP Network". Proc. NSDI, 2005
  - Online BGP route analysis to find and correlate events
- G. Comarela, G. Gürsun, and M. Crovella, "Studying Interdomain Routing over Long Timescales". Proc. IMC, 2013
  - Evolution of the Routing State Distance
  - Future work envisions combined investigation of **space and time**, assessment of the **type of routing change**, **event inference**
- G. Comarela and M. Crovella, "Identifying and Analyzing High Impact Routing Events with PathMiner". Proc. IMC, 2014
  - Next-hop tensor factorization

- Focus on BGP
- Long-term Internet evolution studies
- Limited information about each event (typically, cause AS)

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Discovering High-impact Routing Events using Traceroutes”. Proc. ISCC, 2015
- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Mining Network Events using Traceroute Empathy”. Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
  - Event inference

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Discovering High-impact Routing Events using Traceroutes”. Proc. ISCC, 2015
- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Mining Network Events using Traceroute Empathy”. Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
  - Event inference

- Lots of inferred events

ROMA TRE
UNIVERSITÀ DEGLI STUDI

State of the Art

Management & Monitoring Tools | **Inference Algorithms** | Visualization Systems

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Discovering High-impact Routing Events using Traceroutes”. Proc. ISCC, 2015

- M. Di Bartolomeo, V. Di Donato, M. Pizzonia, C. Squarcella, and M. Rimondini, “Mining Network Events using Traceroute Empathy”. Tech. Rep., 2015 http://arxiv.org/abs/1412.4074v2.pdf
  - Event inference

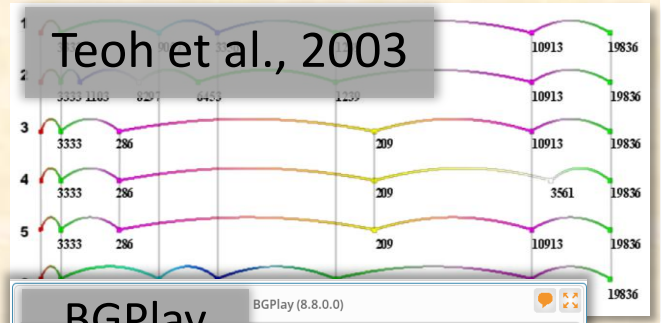
- Lots of inferred events

ROMA TRE
UNIVERSITÀ DEGLI STUDI

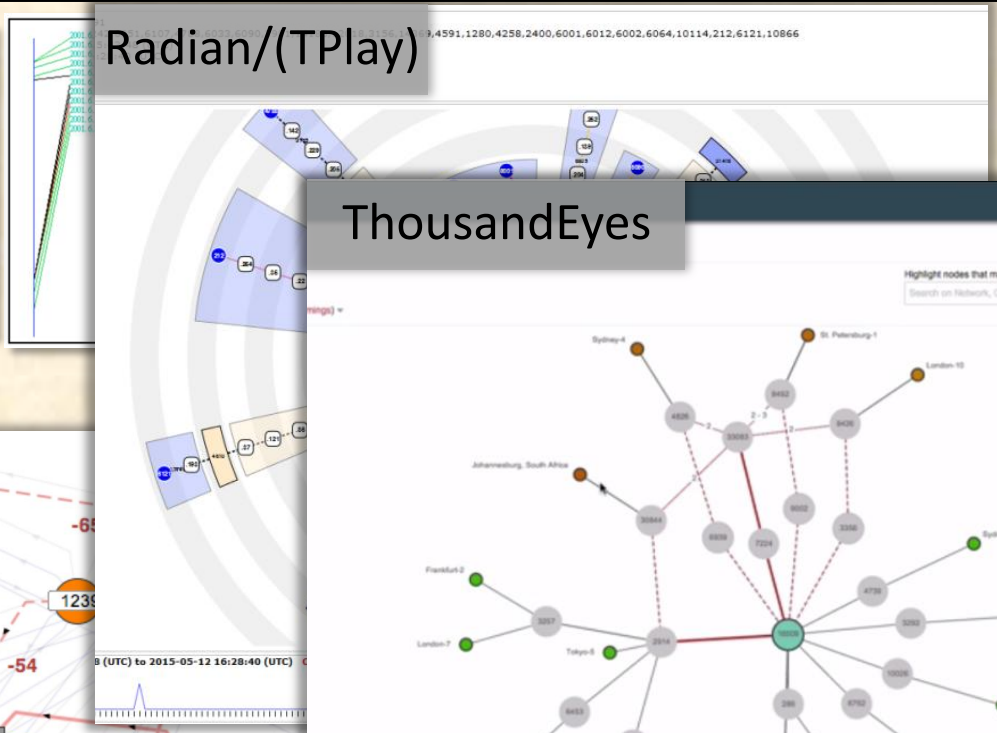
State of the Art

Management & Monitoring Tools | Inference Algorithms | **Visualization Systems**

Teoh et al., 2003

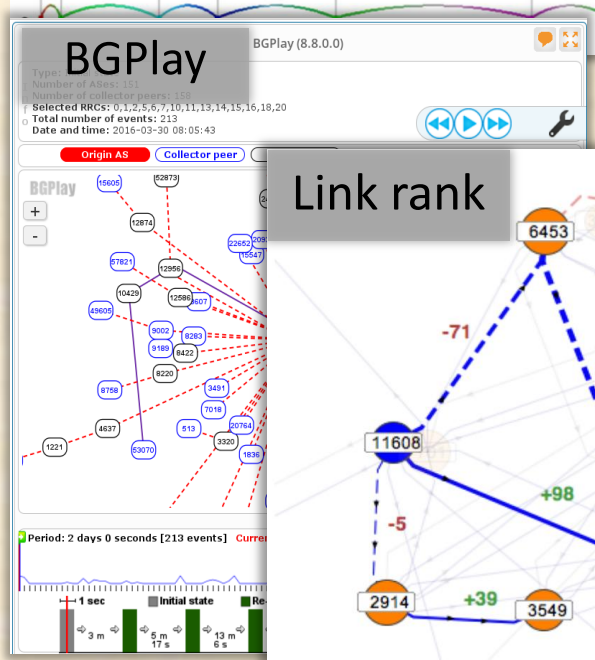


Radian/(TPlay)

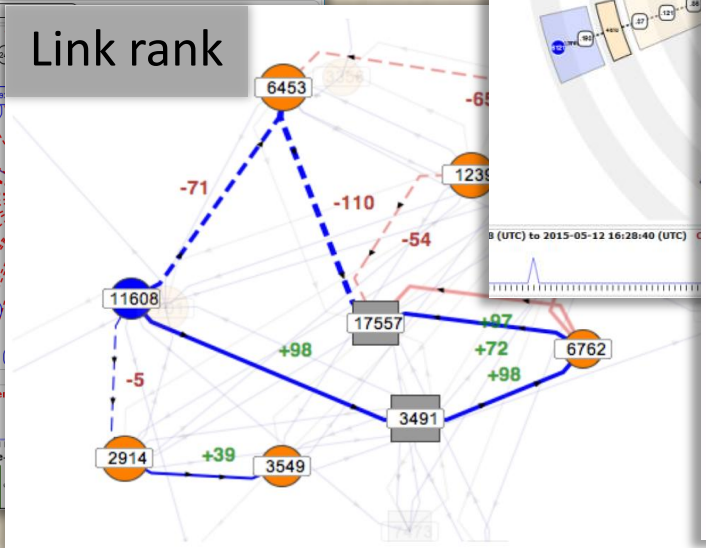


ThousandEyes

BGPlay



Link rank



ROMA TRE
UNIVERSITÀ DEGLI STUDI

RoutingWatch

- Visual exploration tool for a large number of routing events

RoutingWatch

- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports

ROMA TRE
UNIVERSITÀ DEGLI STUDI

RoutingWatch

- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require agents running on devices

ROMA TRE
UNIVERSITÀ DEGLI STUDI

RoutingWatch

- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports

- Does not require agents running on devices

- (Partial) visibility of events in external networks

ROMA TRE
UNIVERSITÀ DEGLI STUDI

RoutingWatch

- Visual exploration tool for a large number of routing events
- Target users: high-level administrators in a NOC, interested in highly informative aggregate reports
- Does not require agents running on devices
- (Partial) visibility of events in external networks

Traceroutes → Events

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Traceroutes → Events

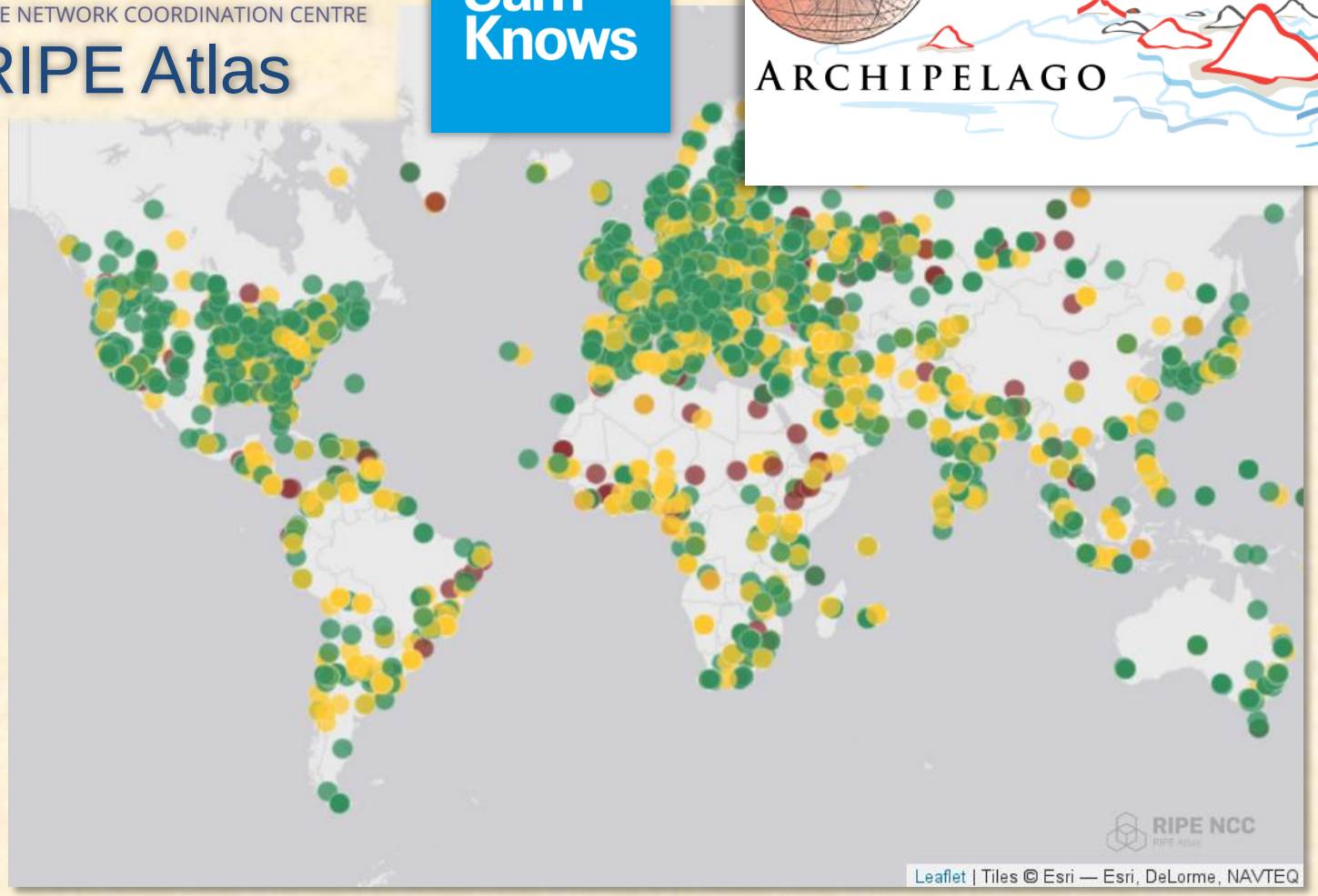
ROMA TRE
UNIVERSITÀ DEGLI STUDI

Traceroutes → Events

RIPE NCC
RIPE NETWORK COORDINATION CENTRE
RIPE Atlas

Sam Knows

caida
ARCHIPELAGO

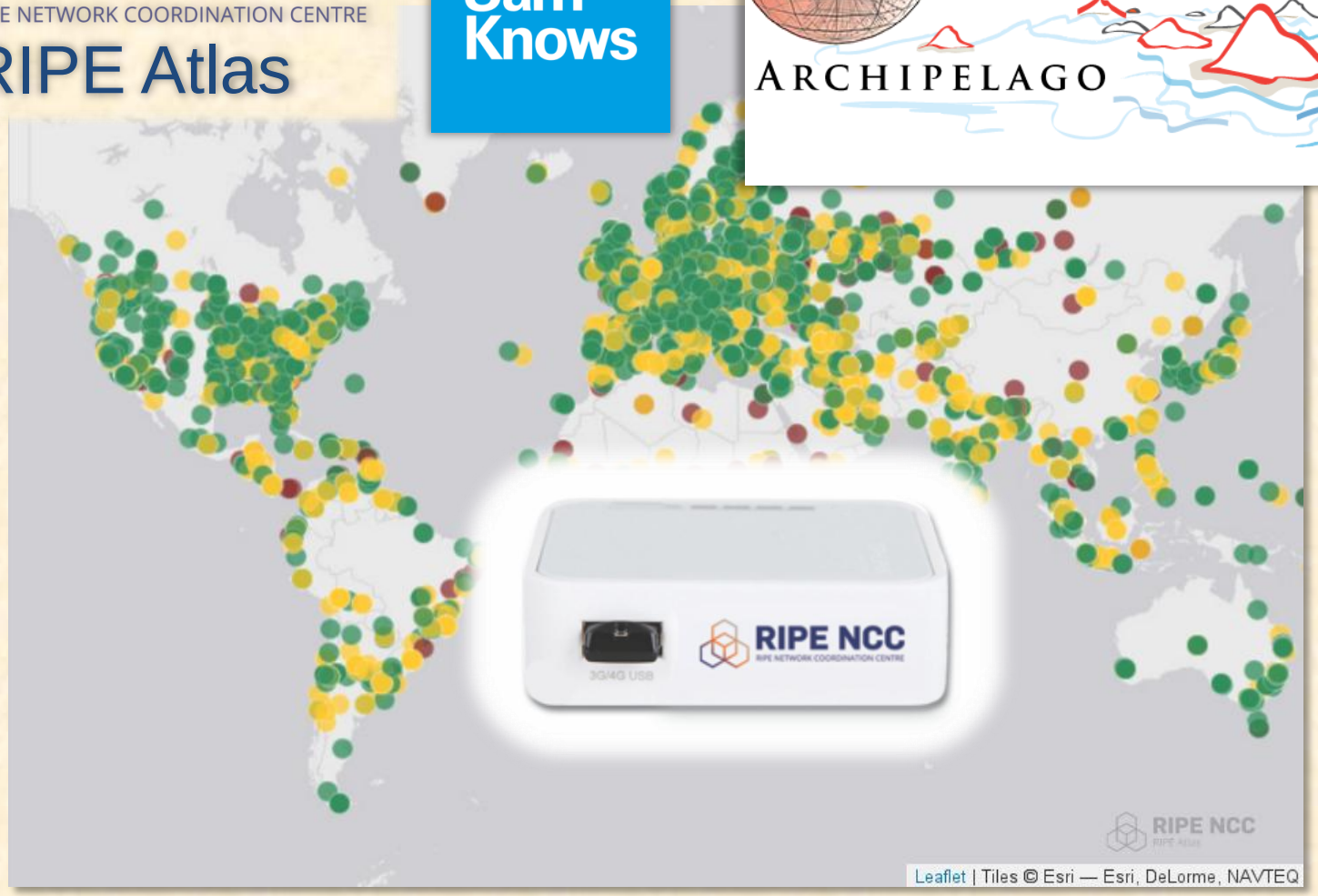


Traceroutes → Events

RIPE NCC
RIPE NETWORK COORDINATION CENTRE
RIPE Atlas

Sam Knows

caida
ARCHIPELAGO



Traceroutes → Events

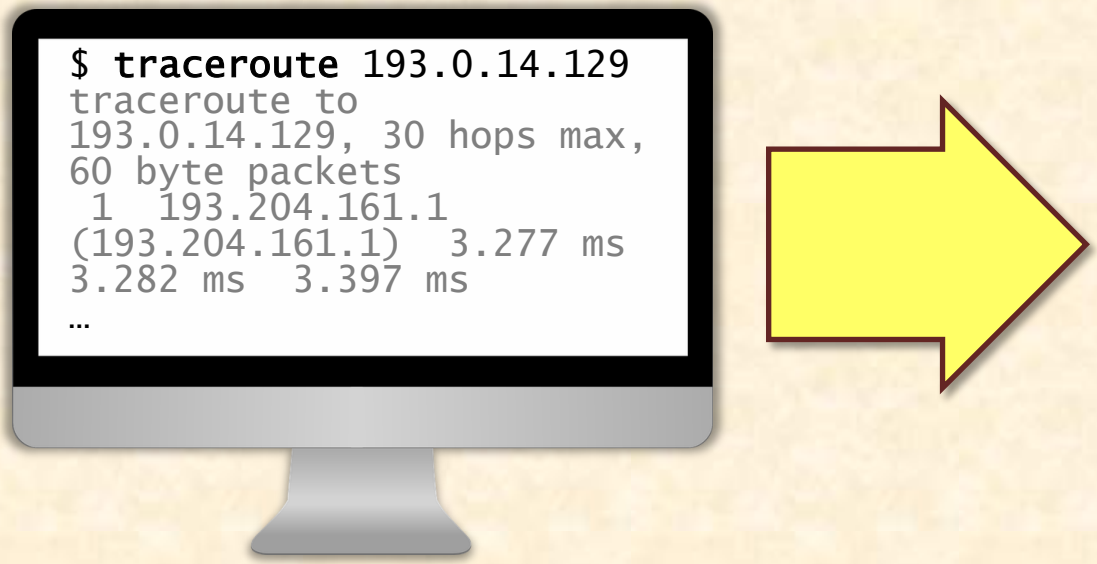
RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Sam Knows

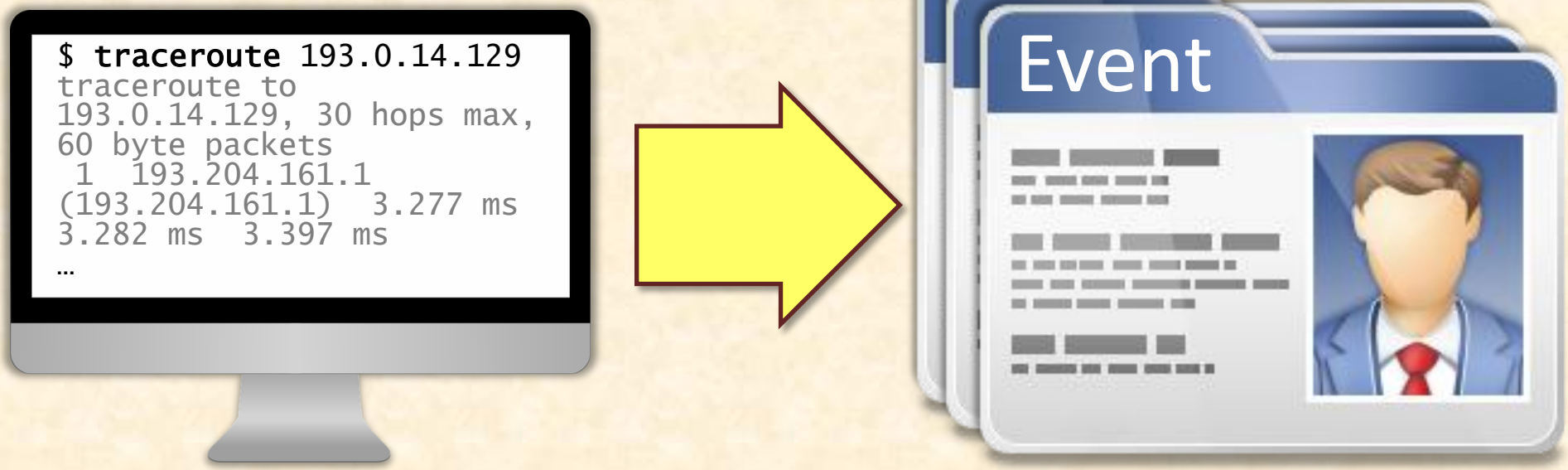
caida
ARCHIPELAGO

```
$ traceroute 193.0.14.129
traceroute to
193.0.14.129, 30 hops max,
60 byte packets
 1  193.204.161.1
(193.204.161.1)  3.277 ms
3.282 ms  3.397 ms
…
```

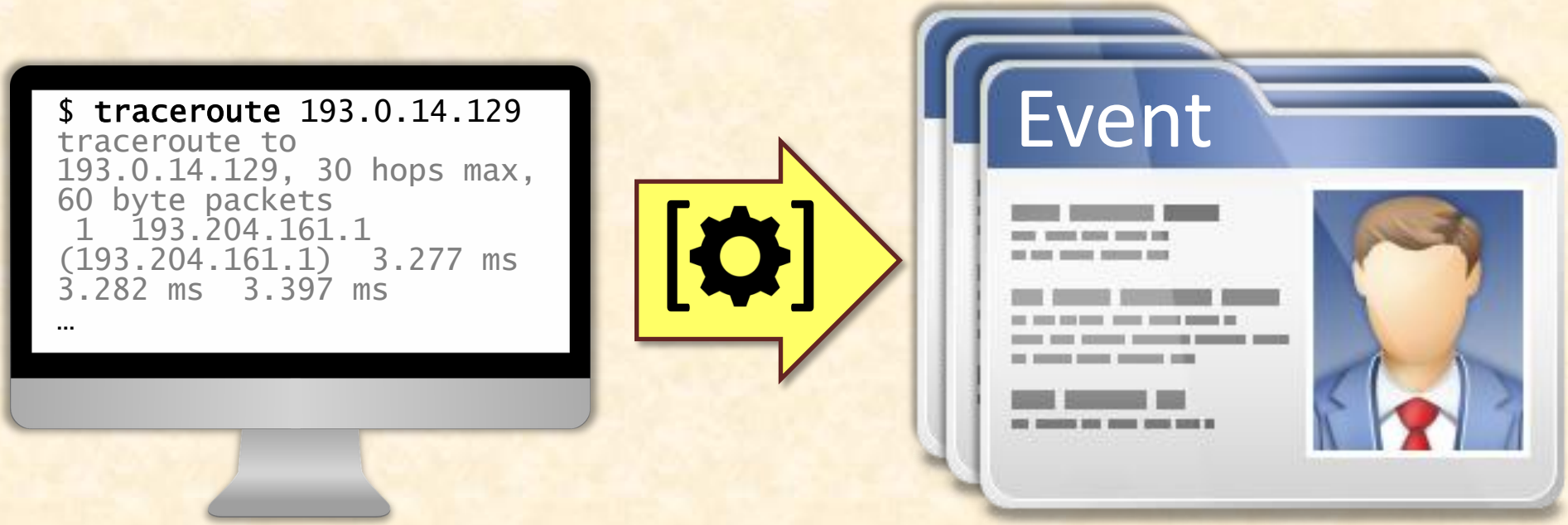
Traceroutes → Events



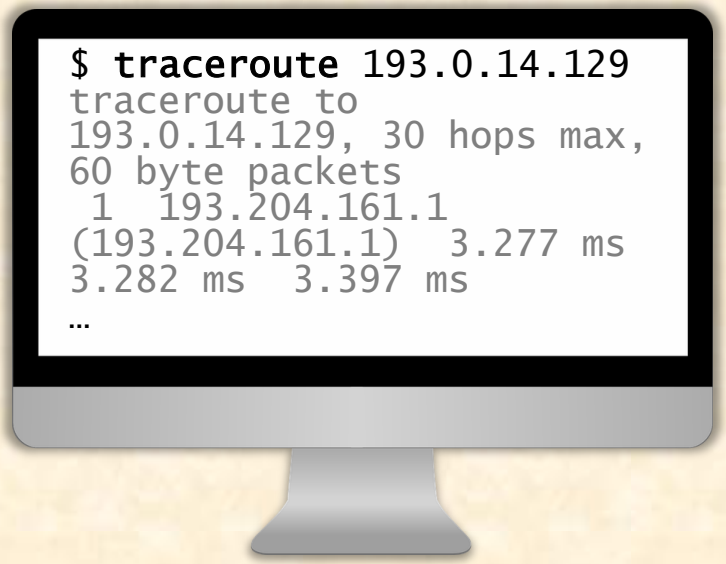
Traceroutes → Events

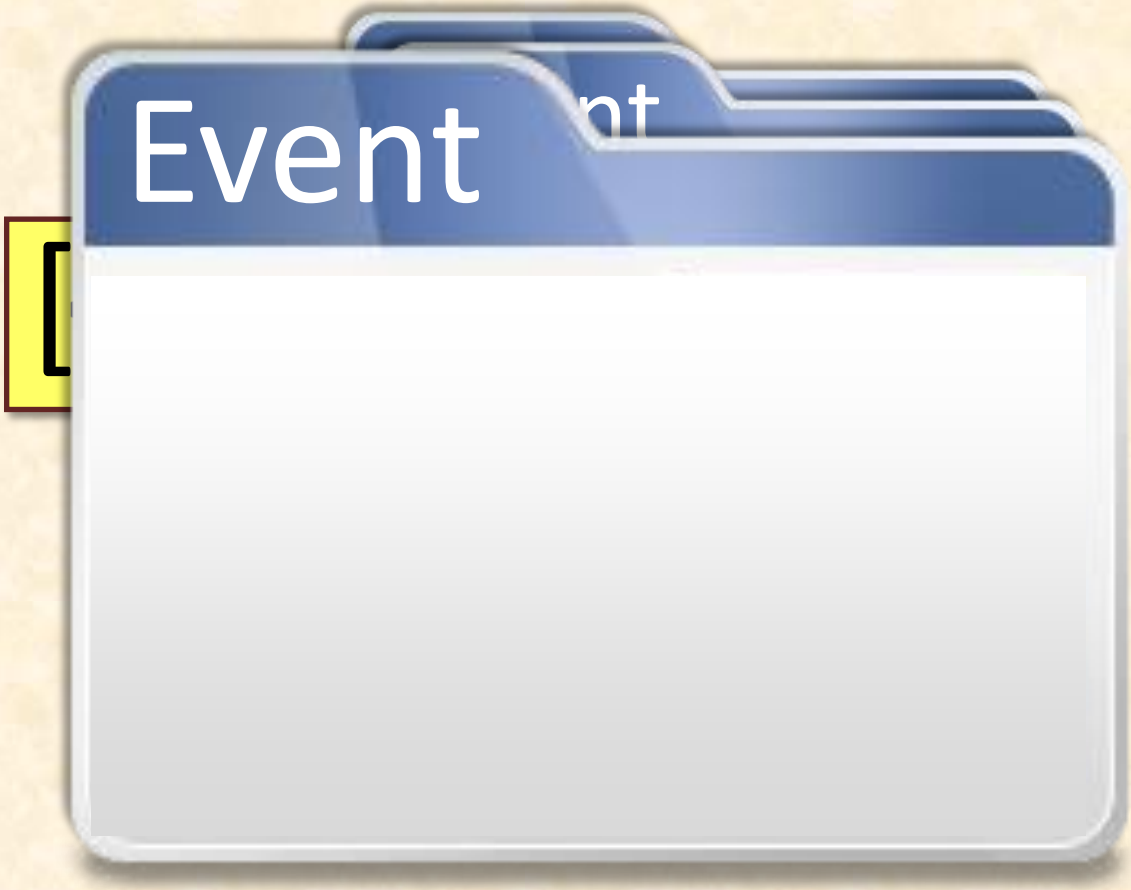


Traceroutes → Events

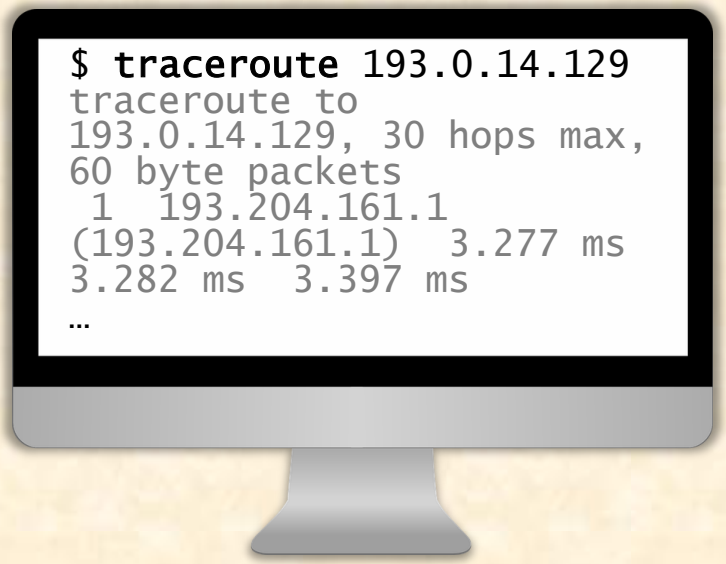


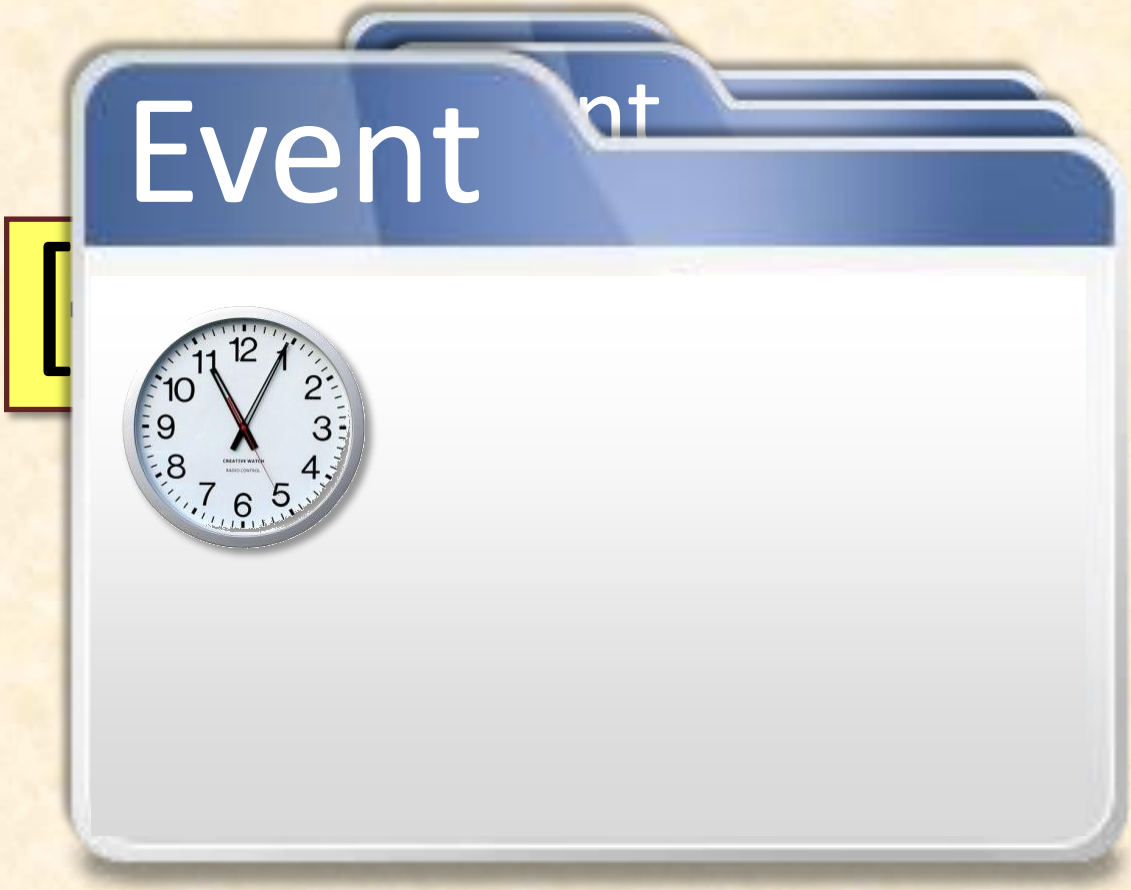
Traceroutes → Events



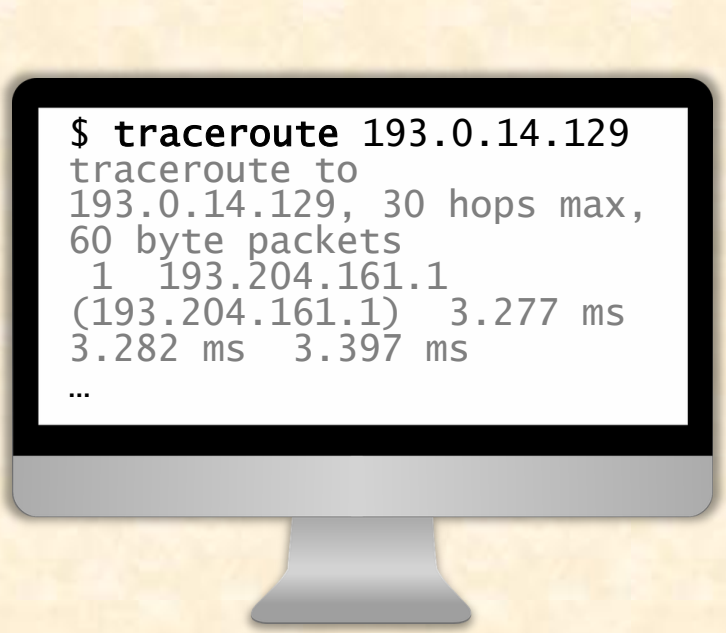


Traceroutes → Events

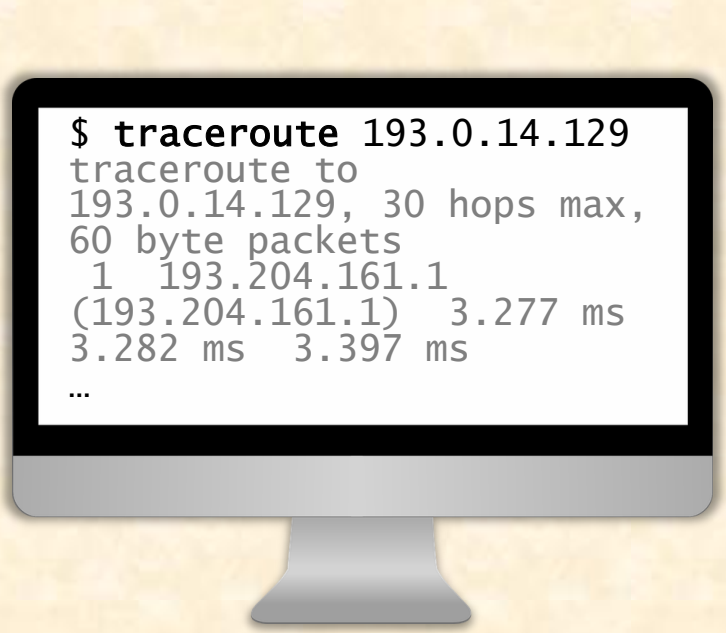




Traceroutes → Events



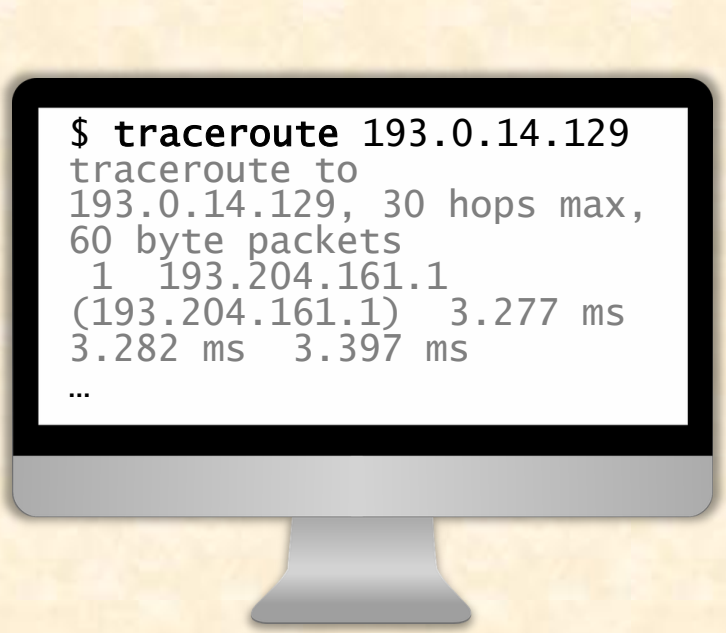
Traceroutes → Events



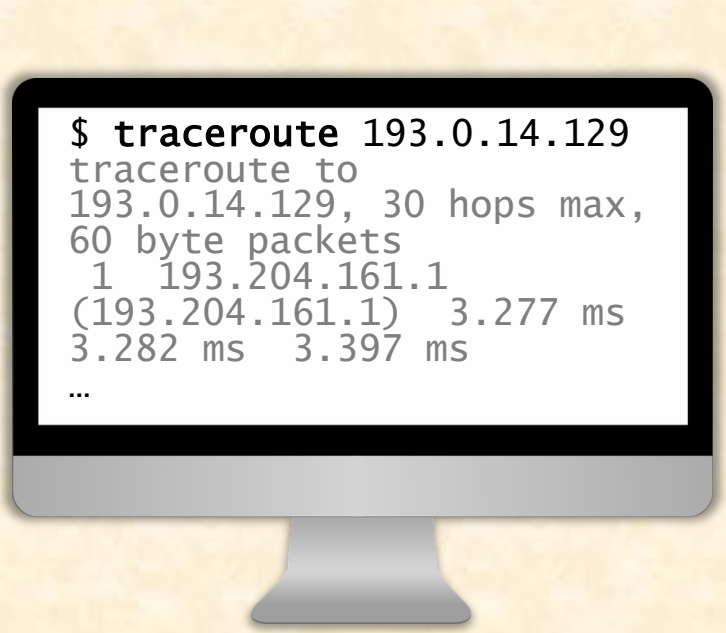
Traceroutes → Events

Traceroutes → Events

Traceroutes → Events



Traceroutes → Events

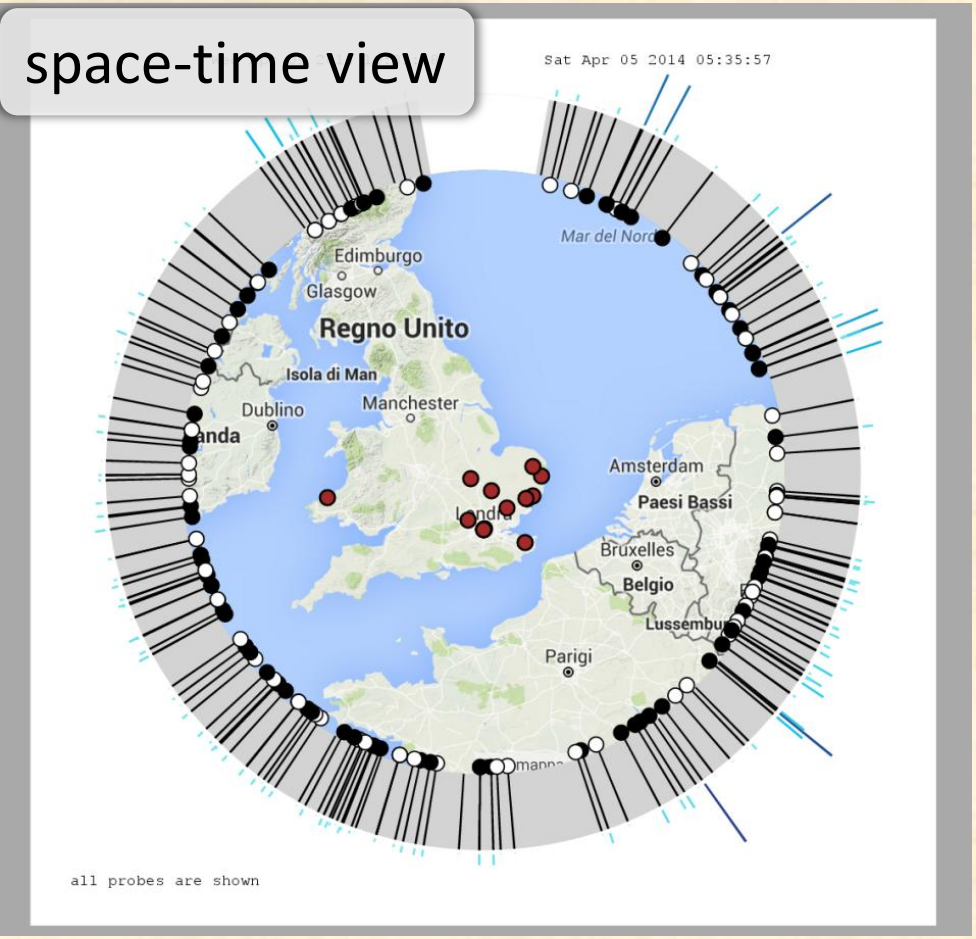


ROMA TRE
UNIVERSITÀ DEGLI STUDI

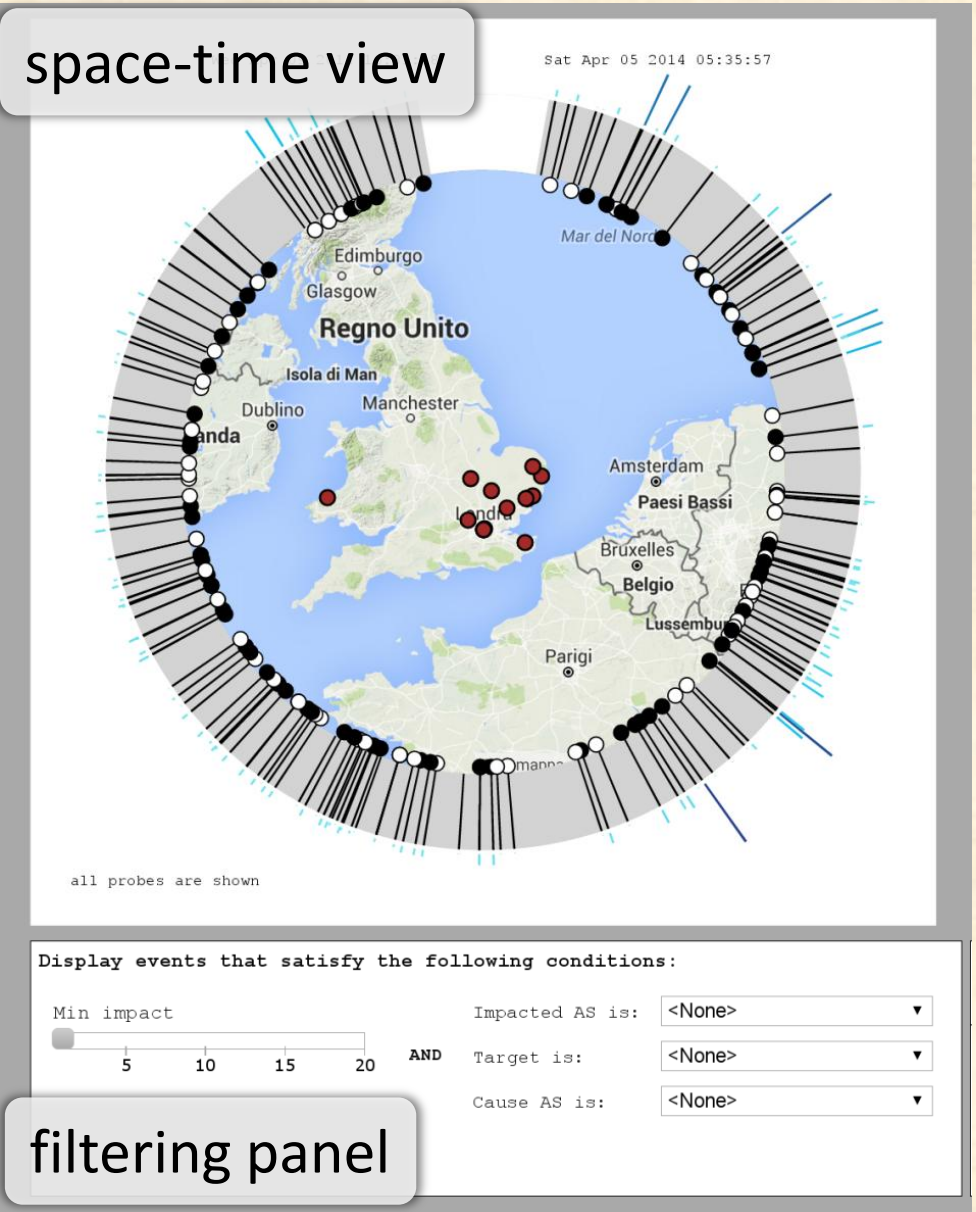
User interface

User interface

space-time view

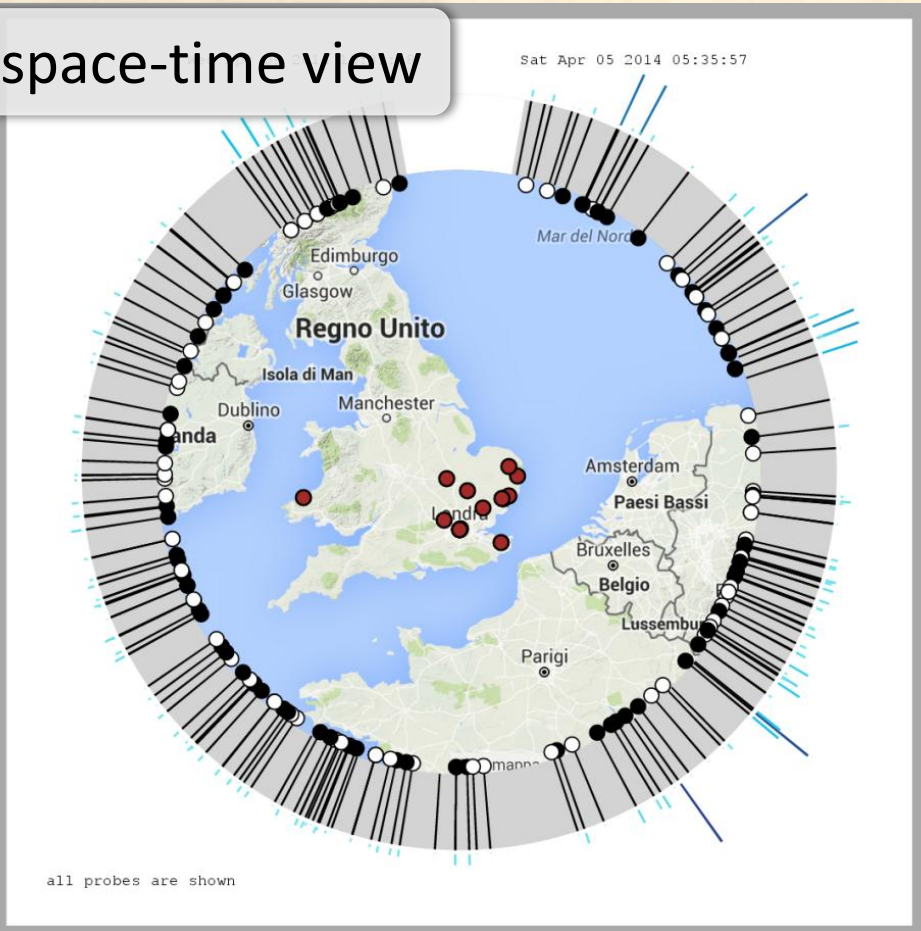


User interface

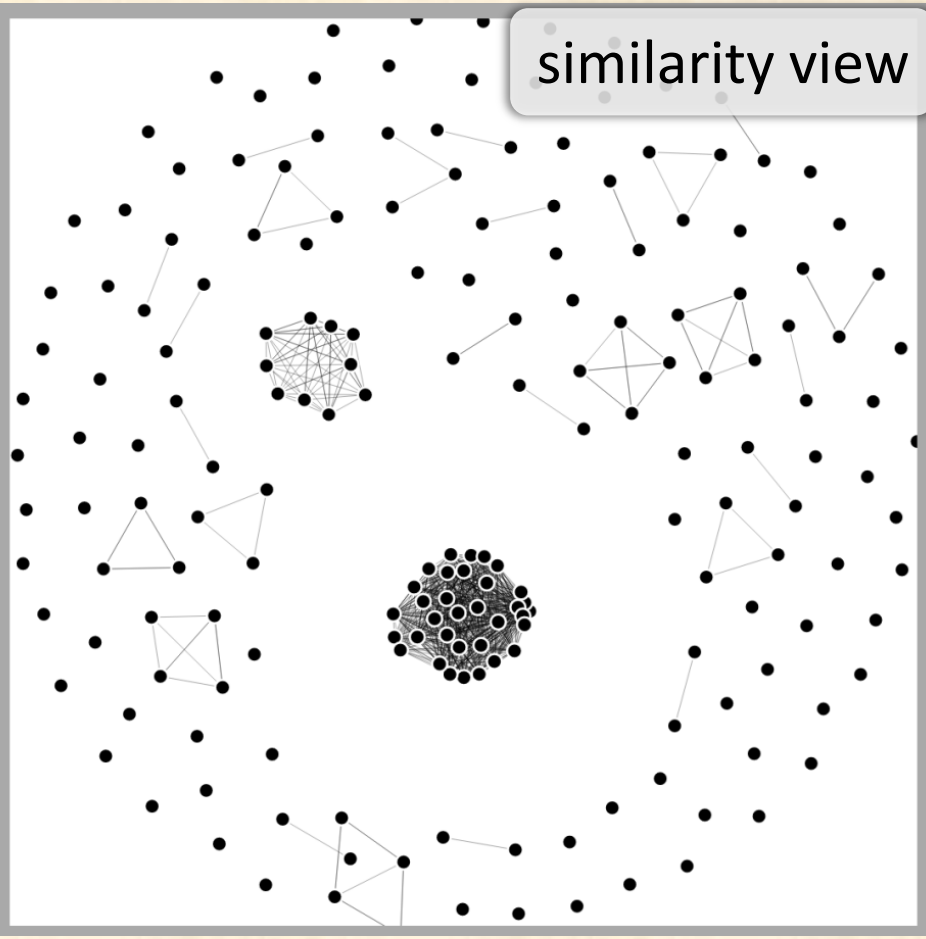


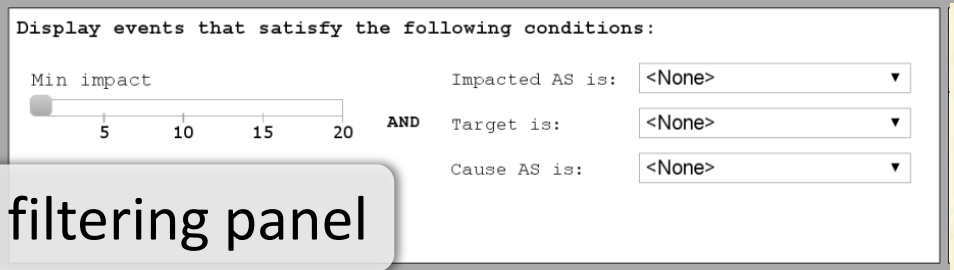
User interface

space-time view



similarity view

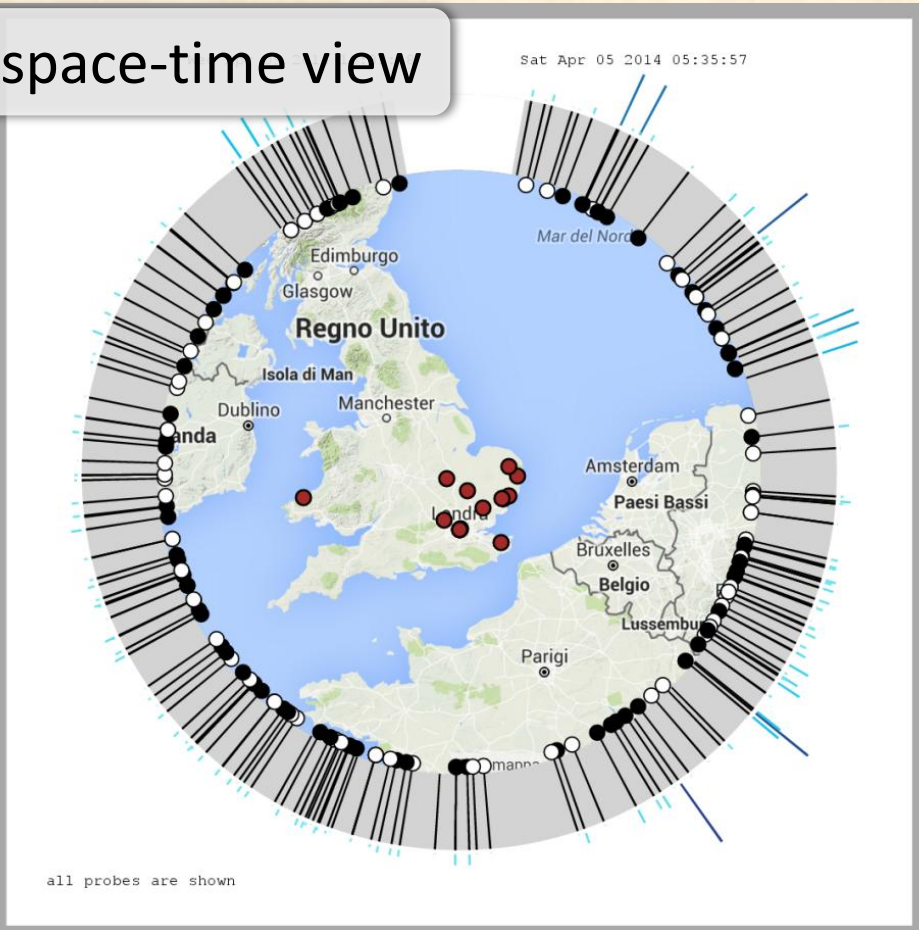




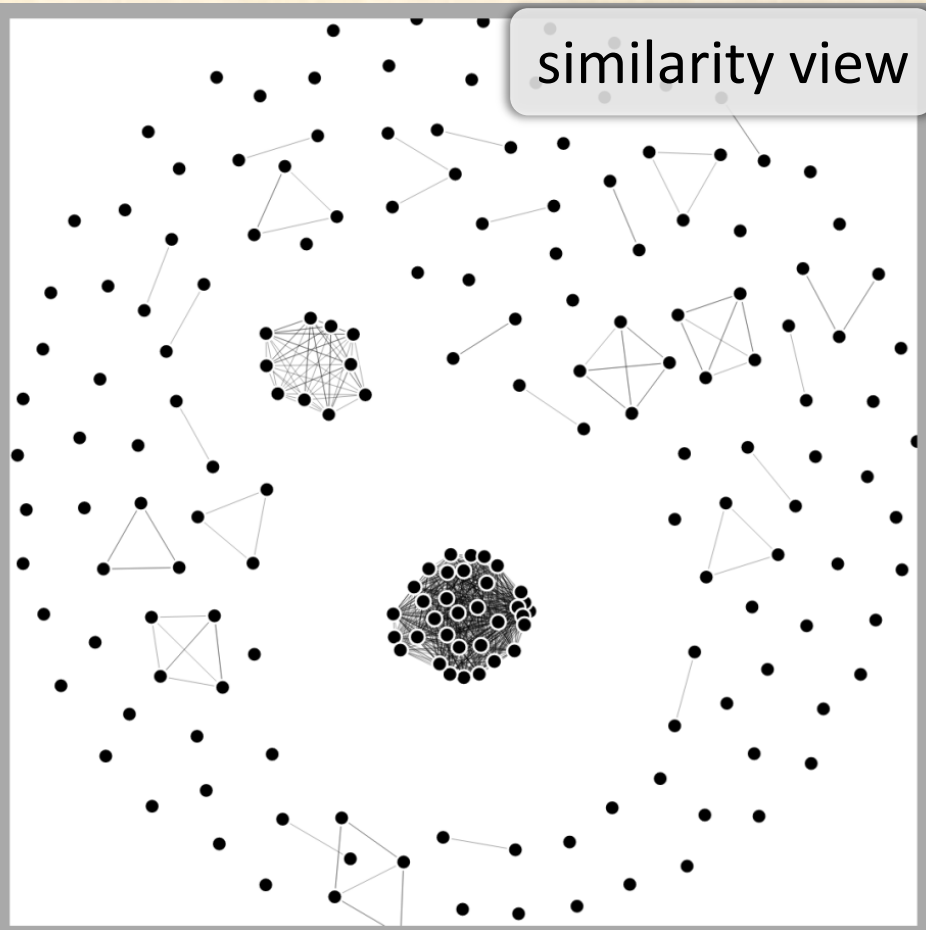
filtering panel

User interface

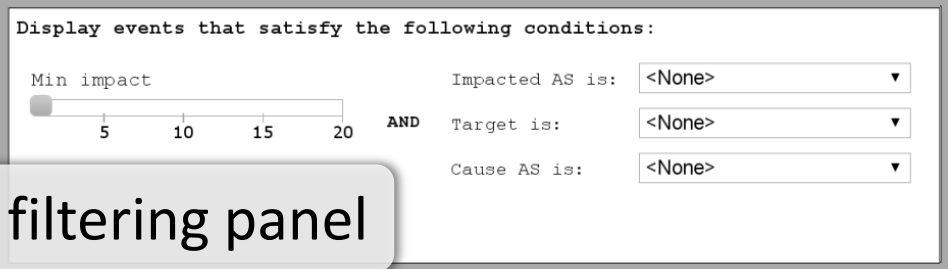
space-time view



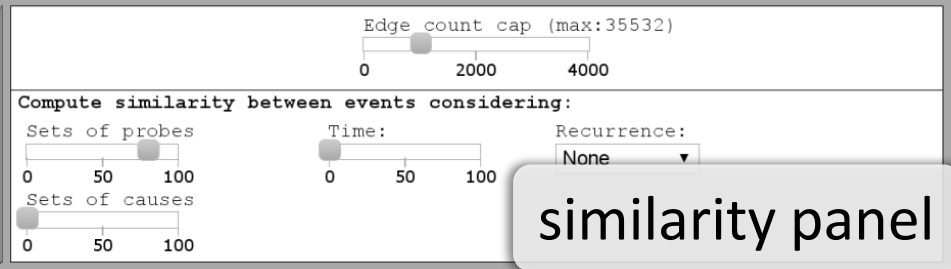
similarity view



filtering panel



similarity panel



User interface

space-time view

similarity view

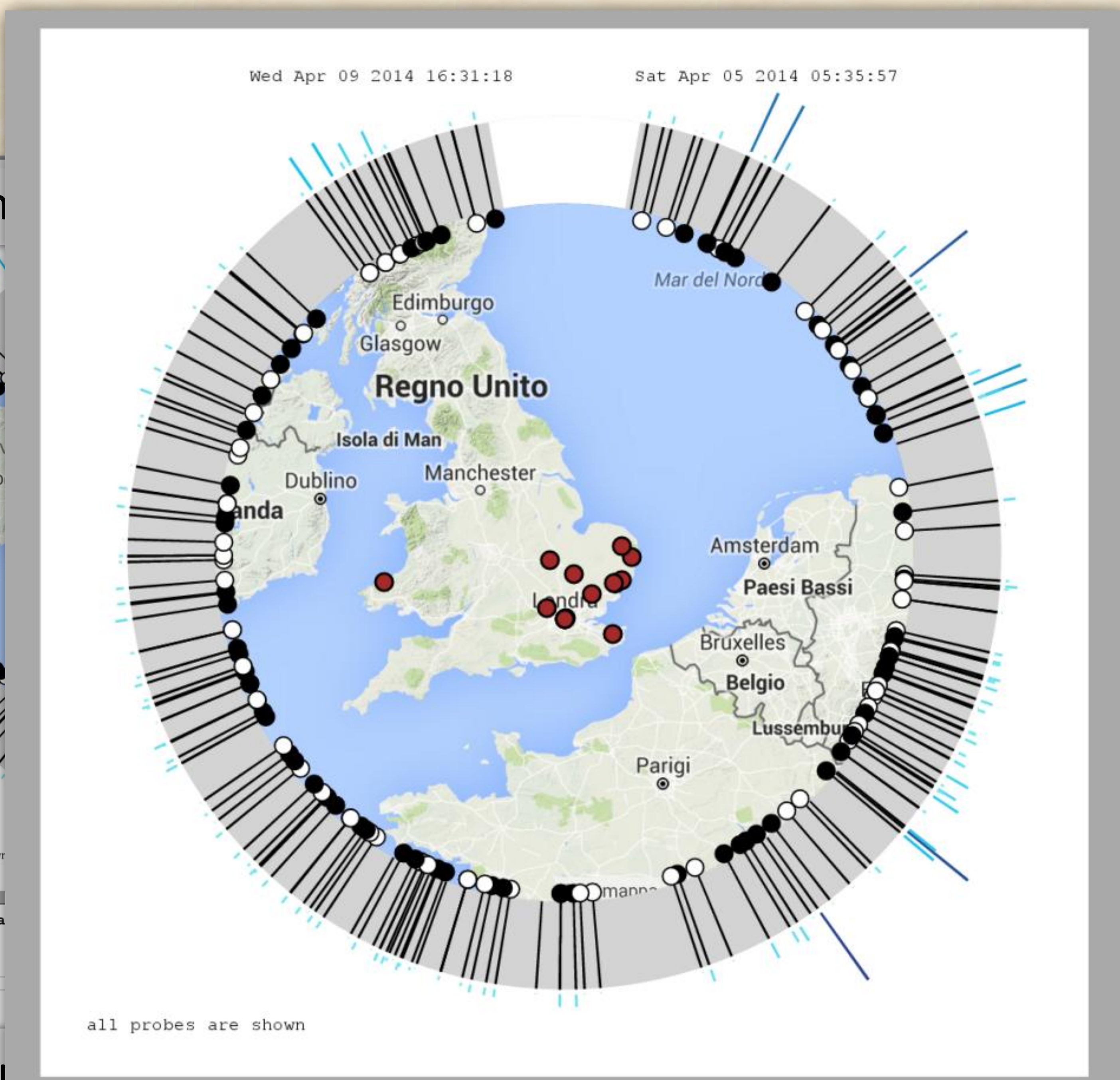
filtering panel

similarity panel

ROMA TRE UNIVERSITÀ DEGLI STUDI

space-tim

rity view



all probes are shown

Display events tha

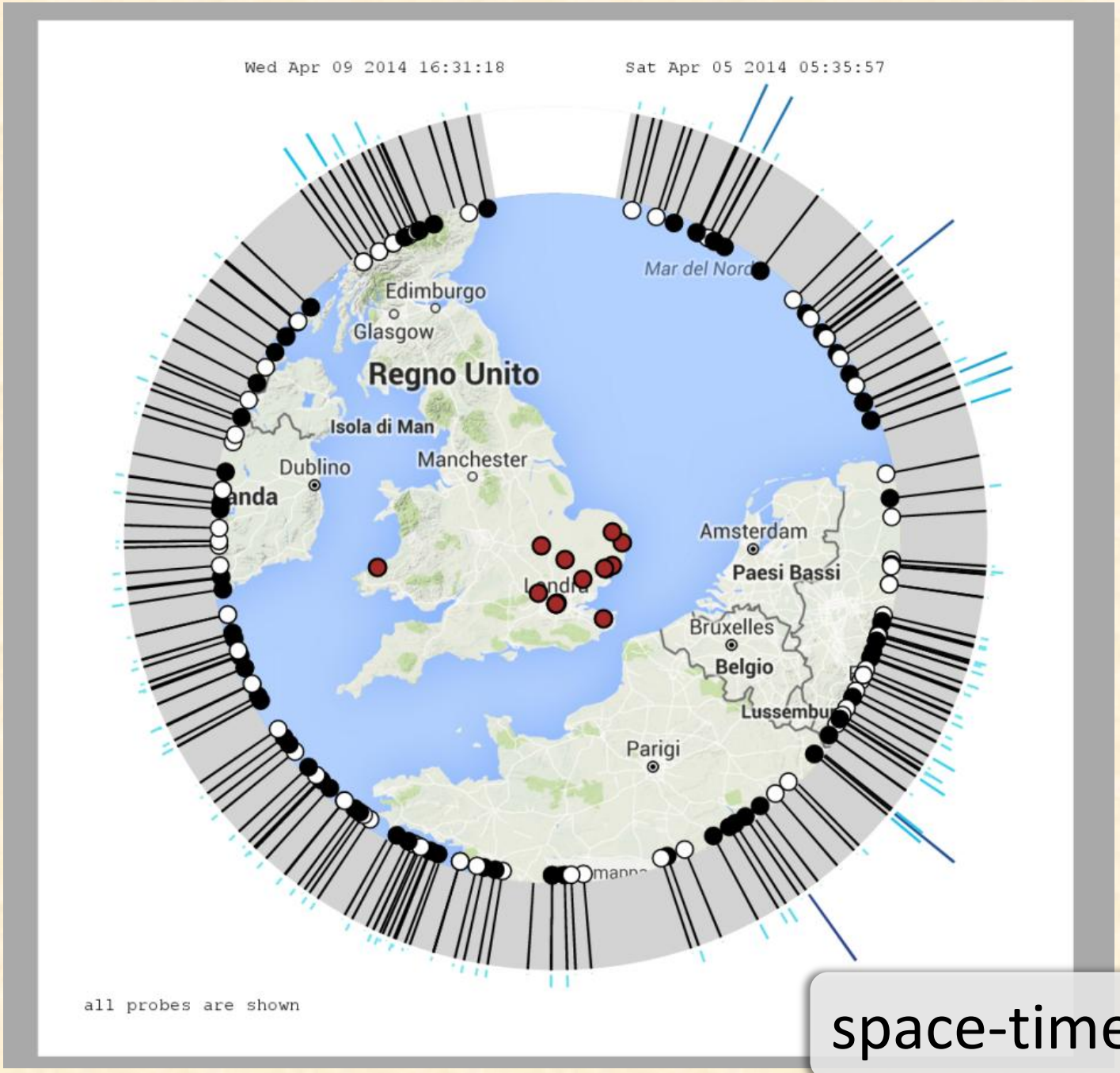
Min impact

5 10

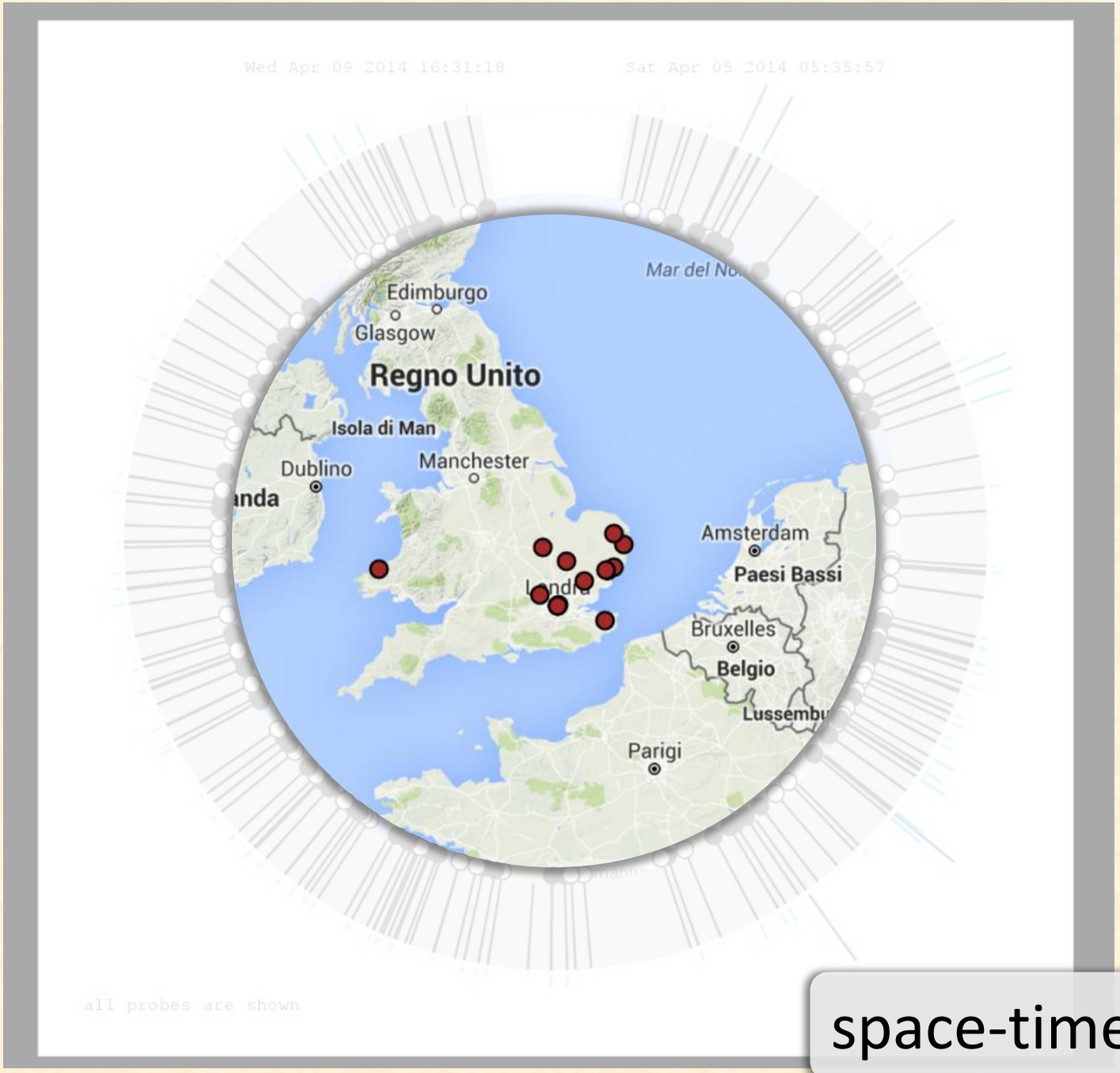
0 50 100

filtering p

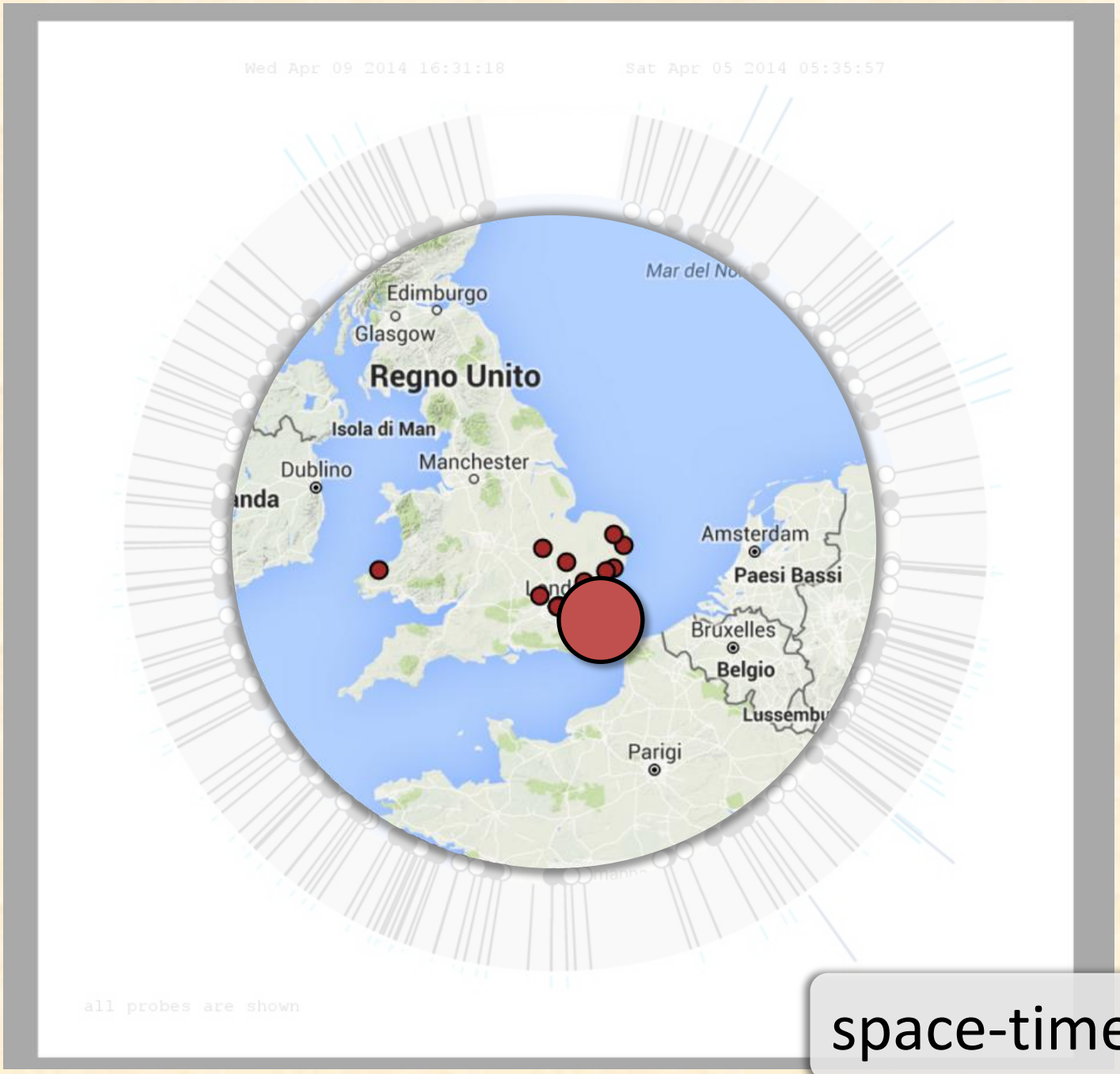
rity panel



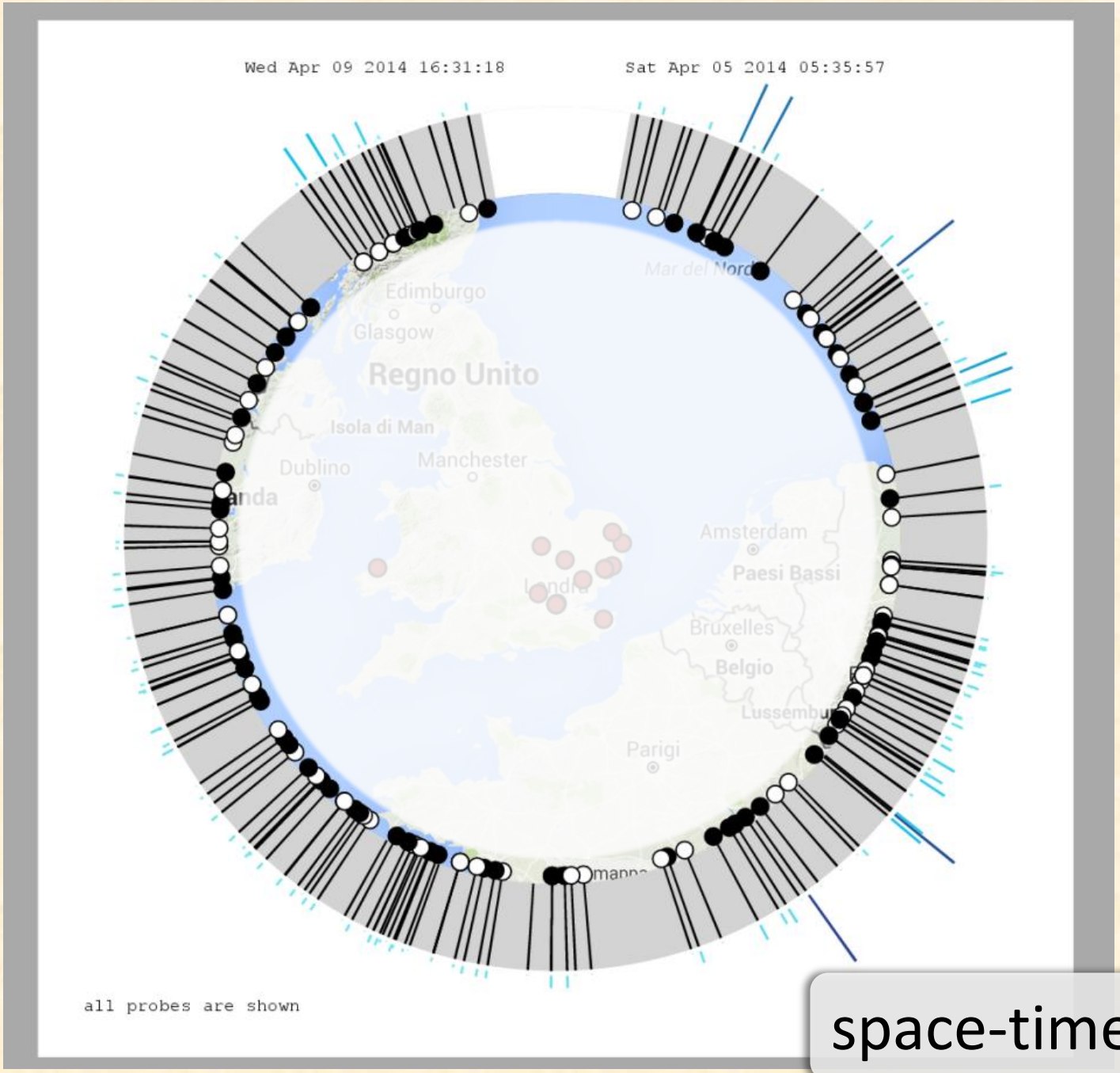
space-time view



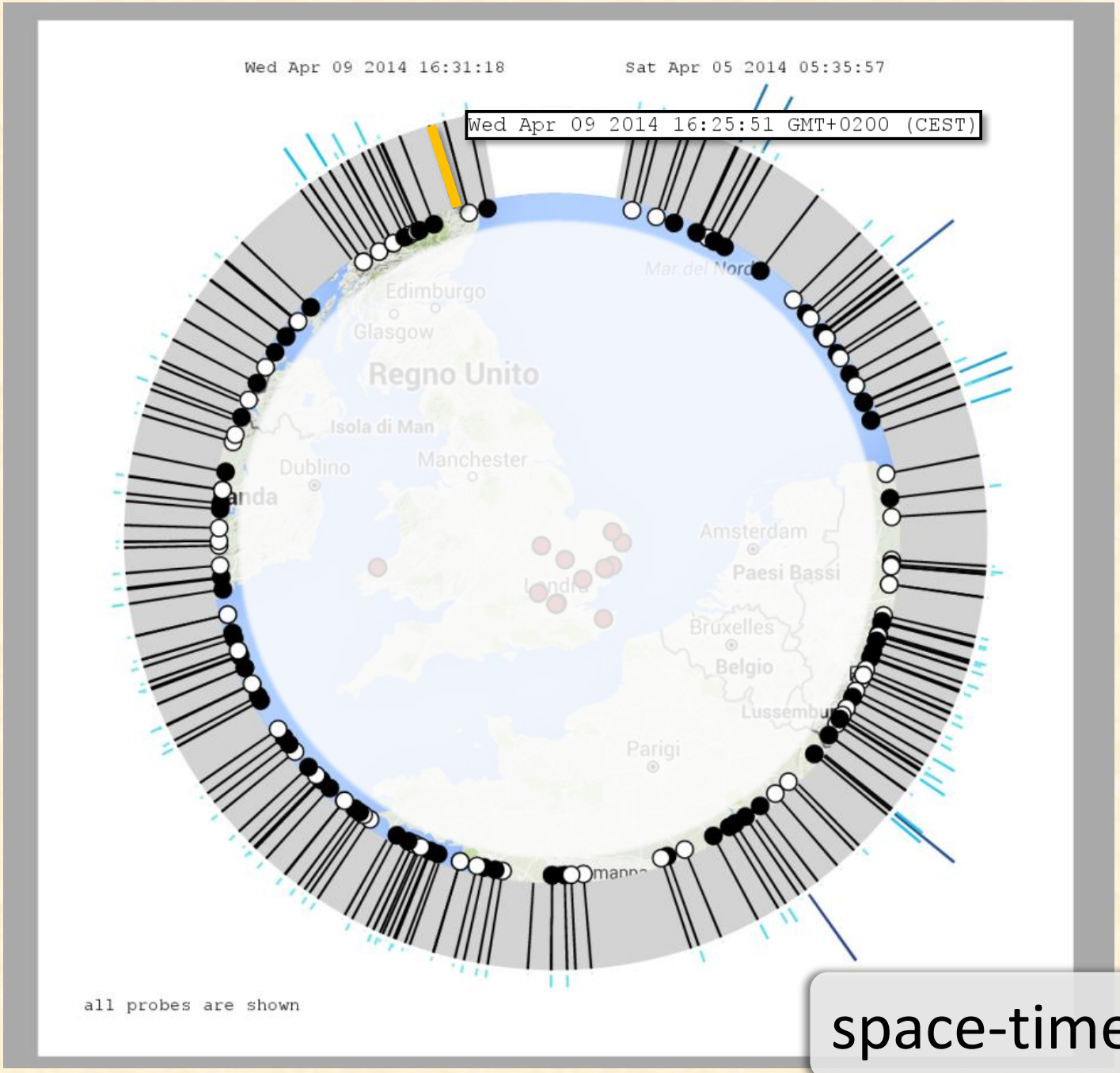
space-time view



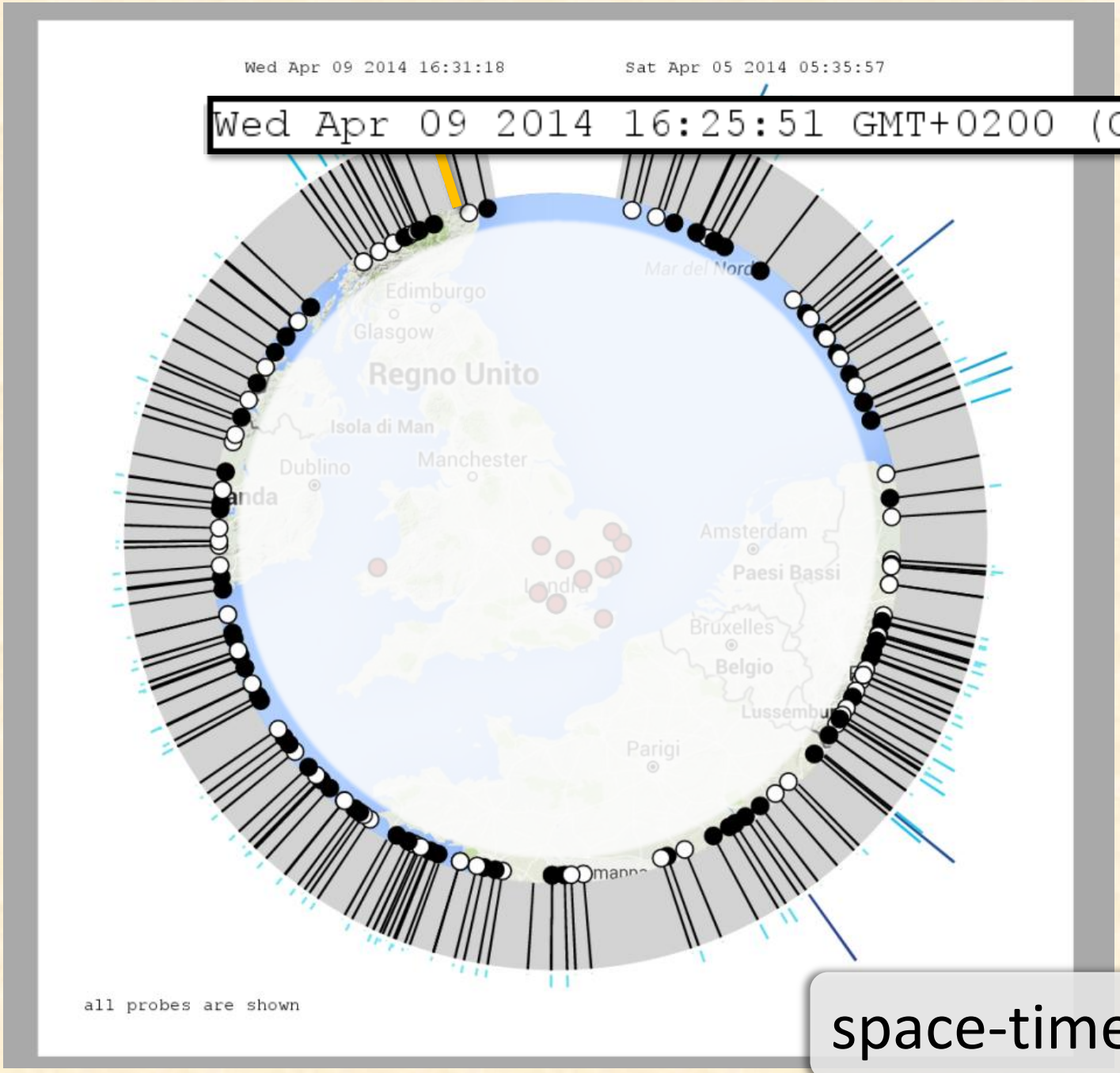
space-time view



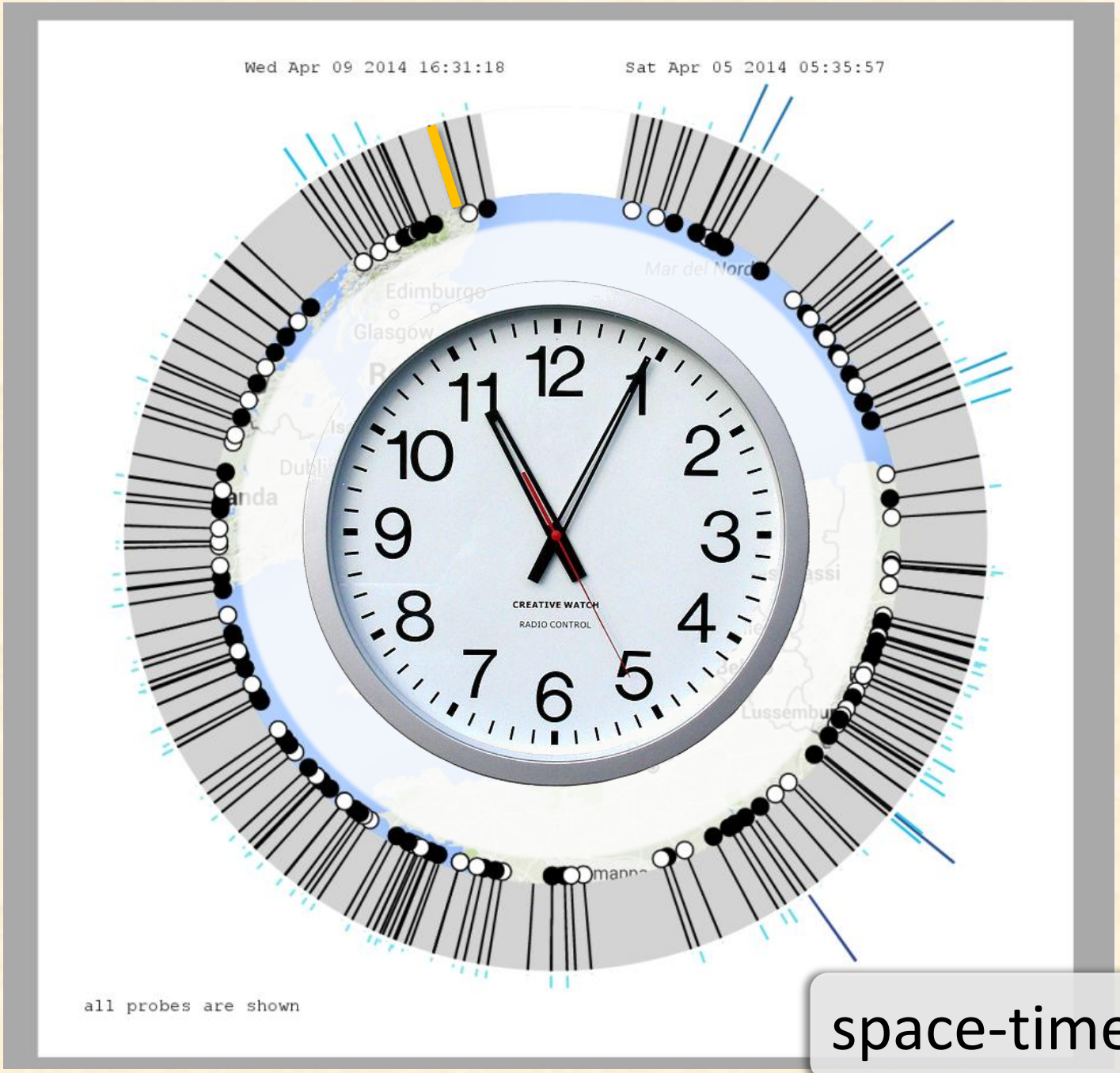
space-time view



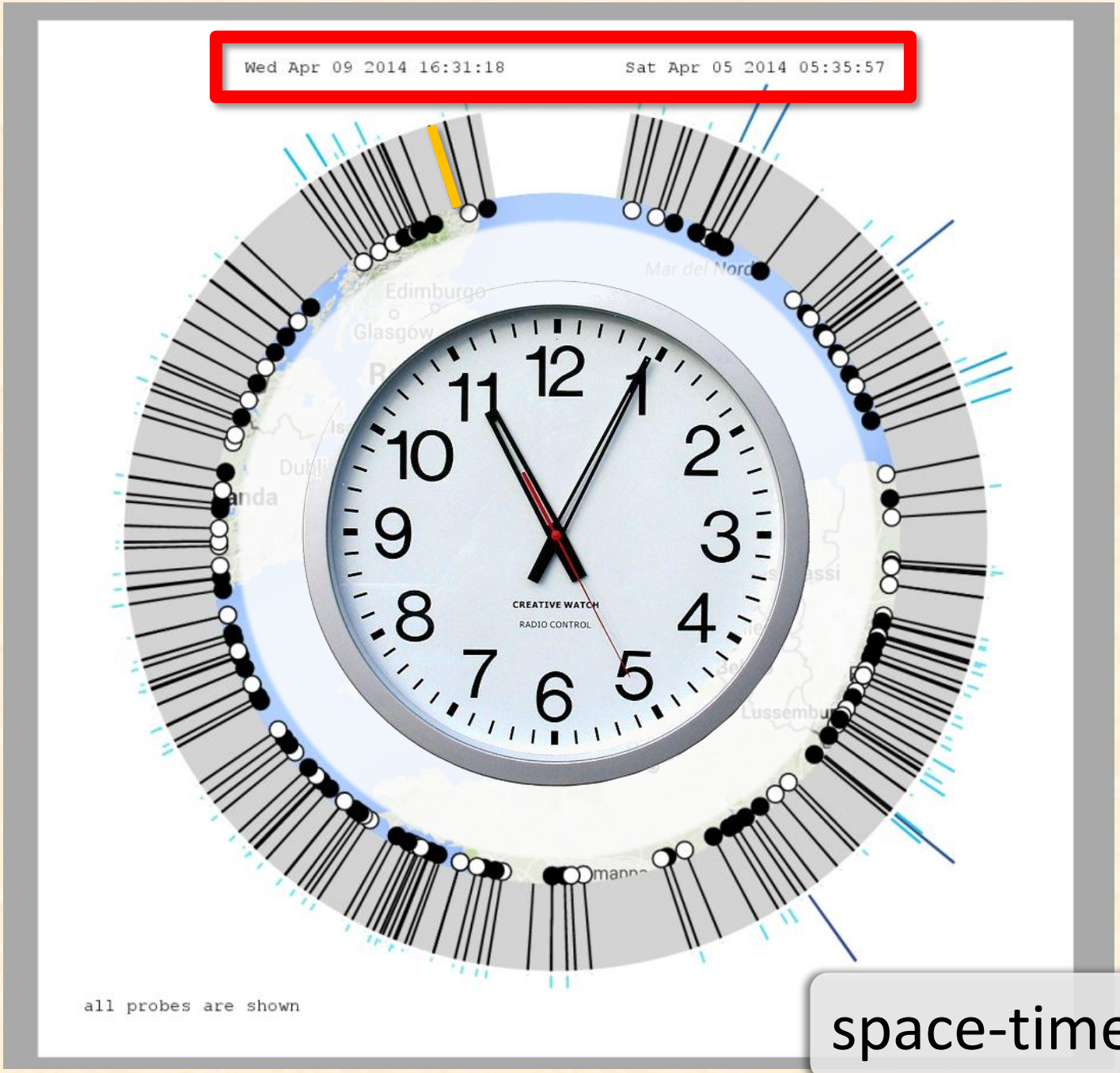
space-time view



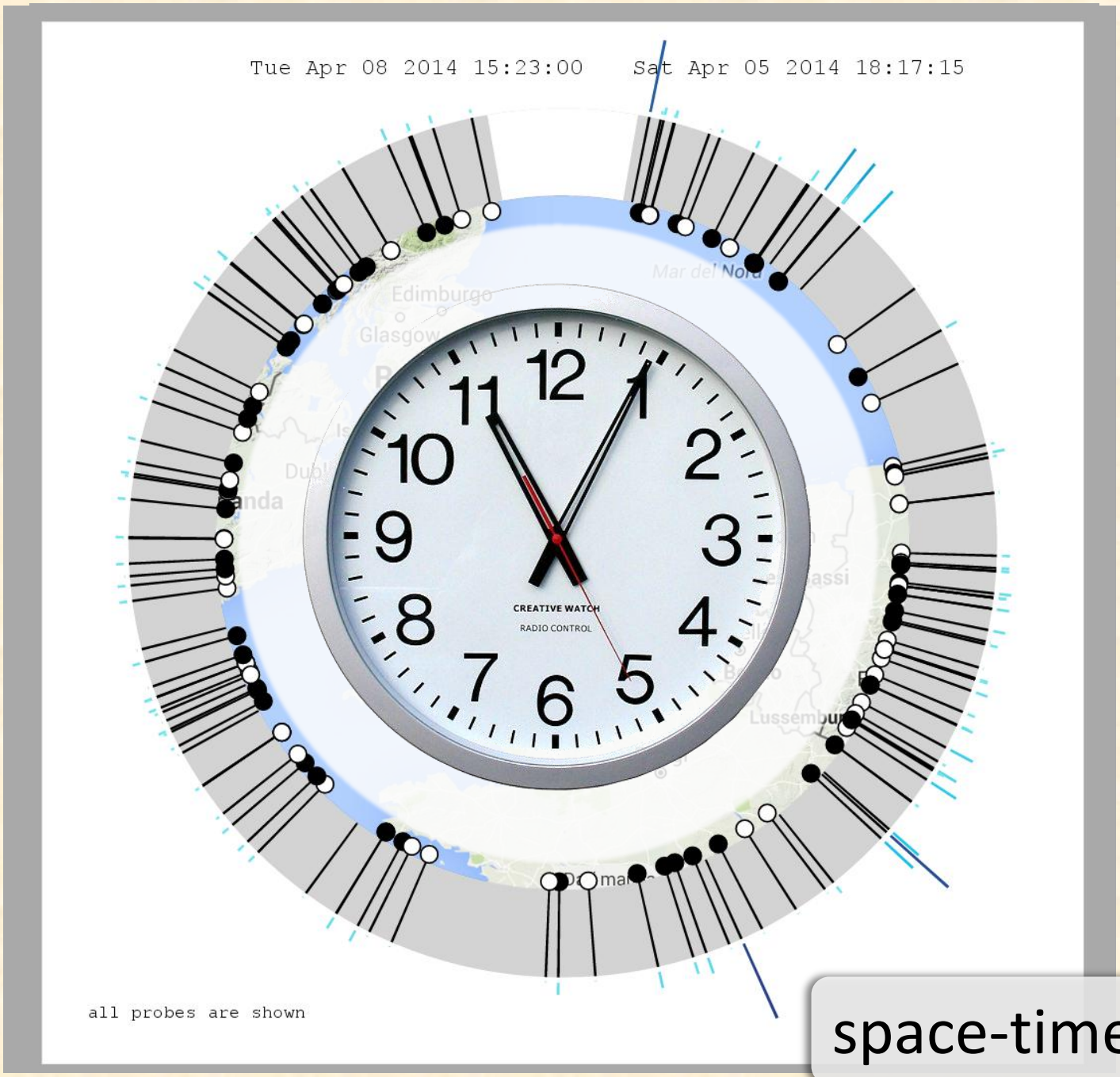
space-time view



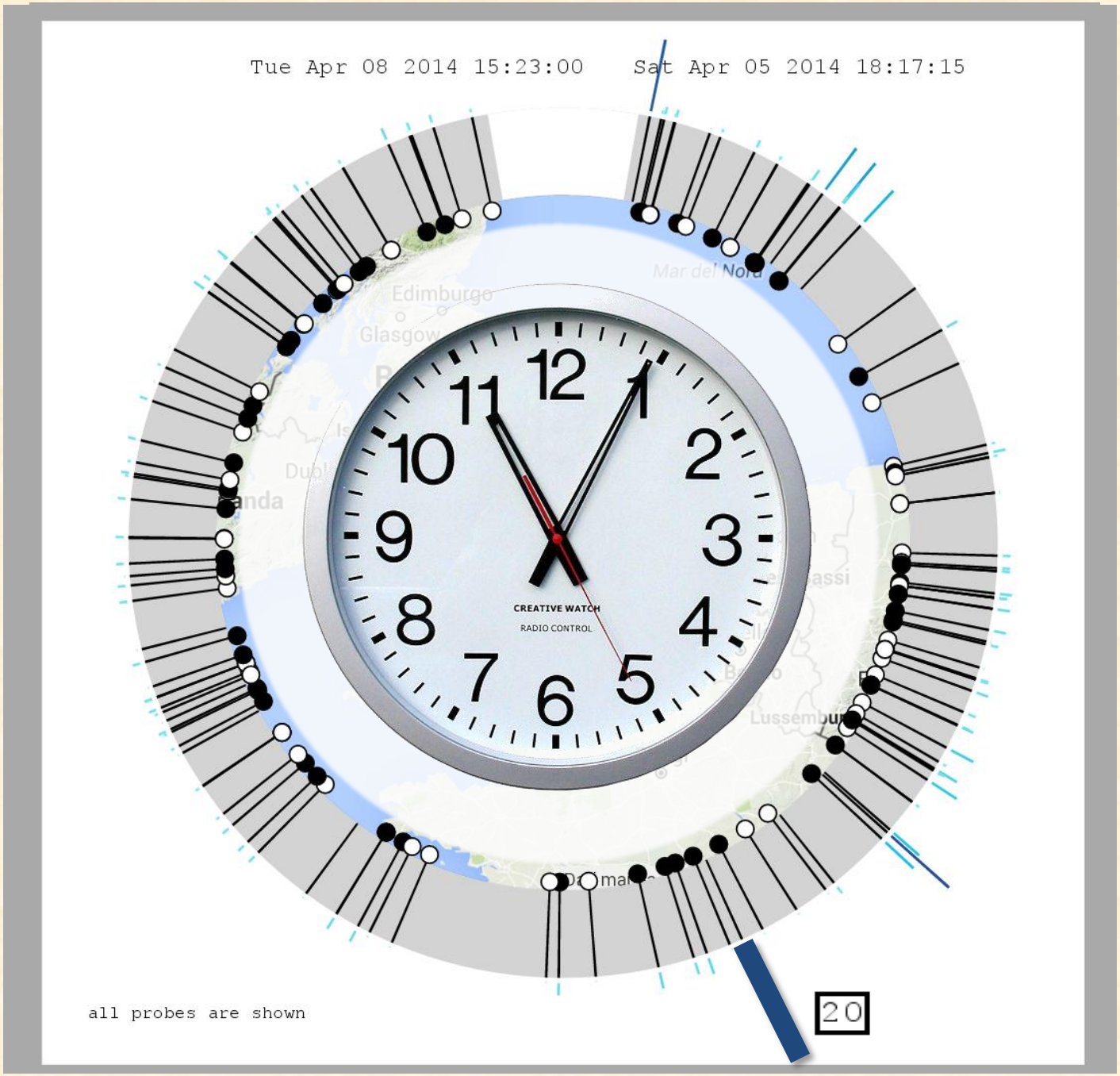
space-time view

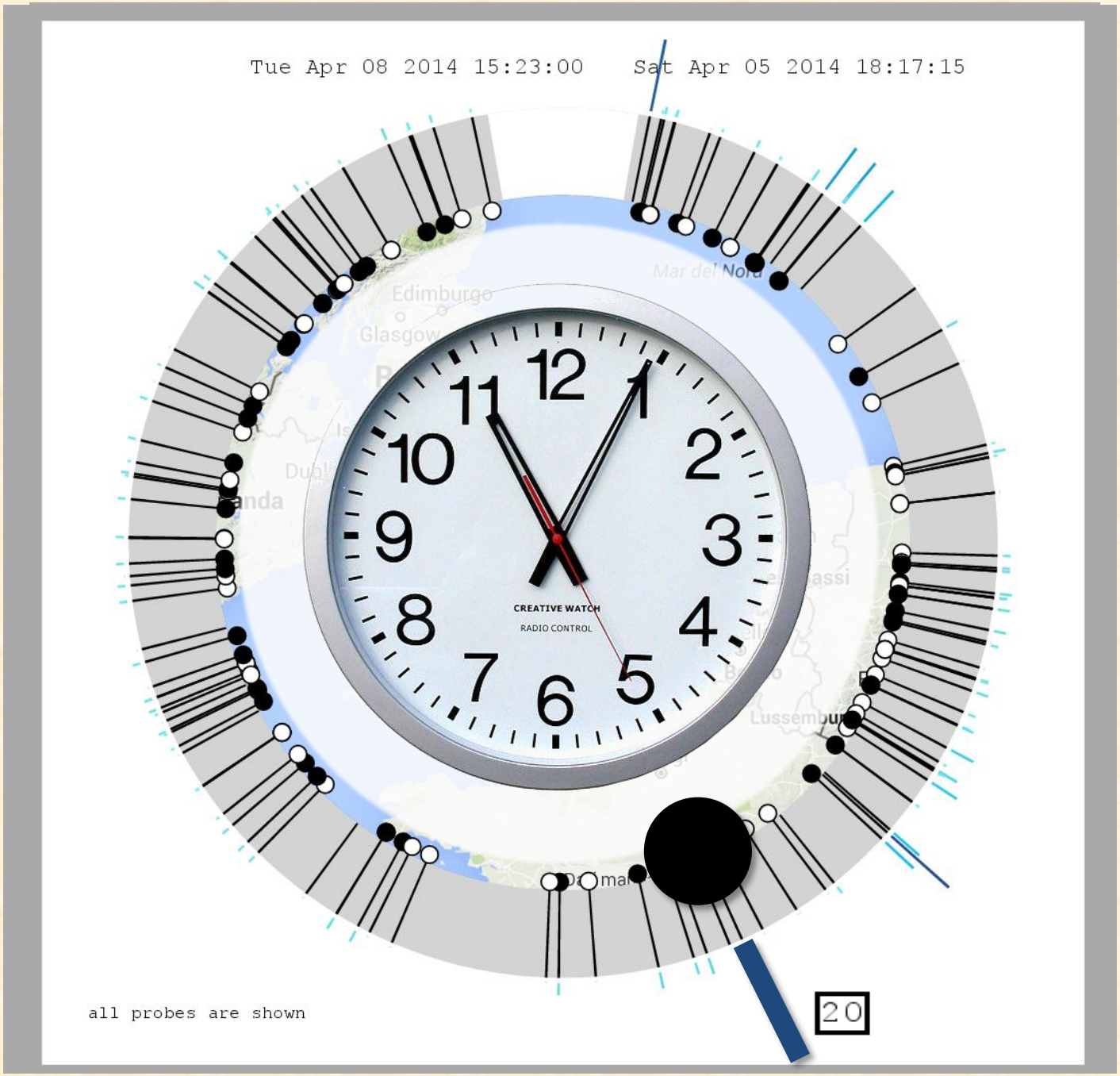


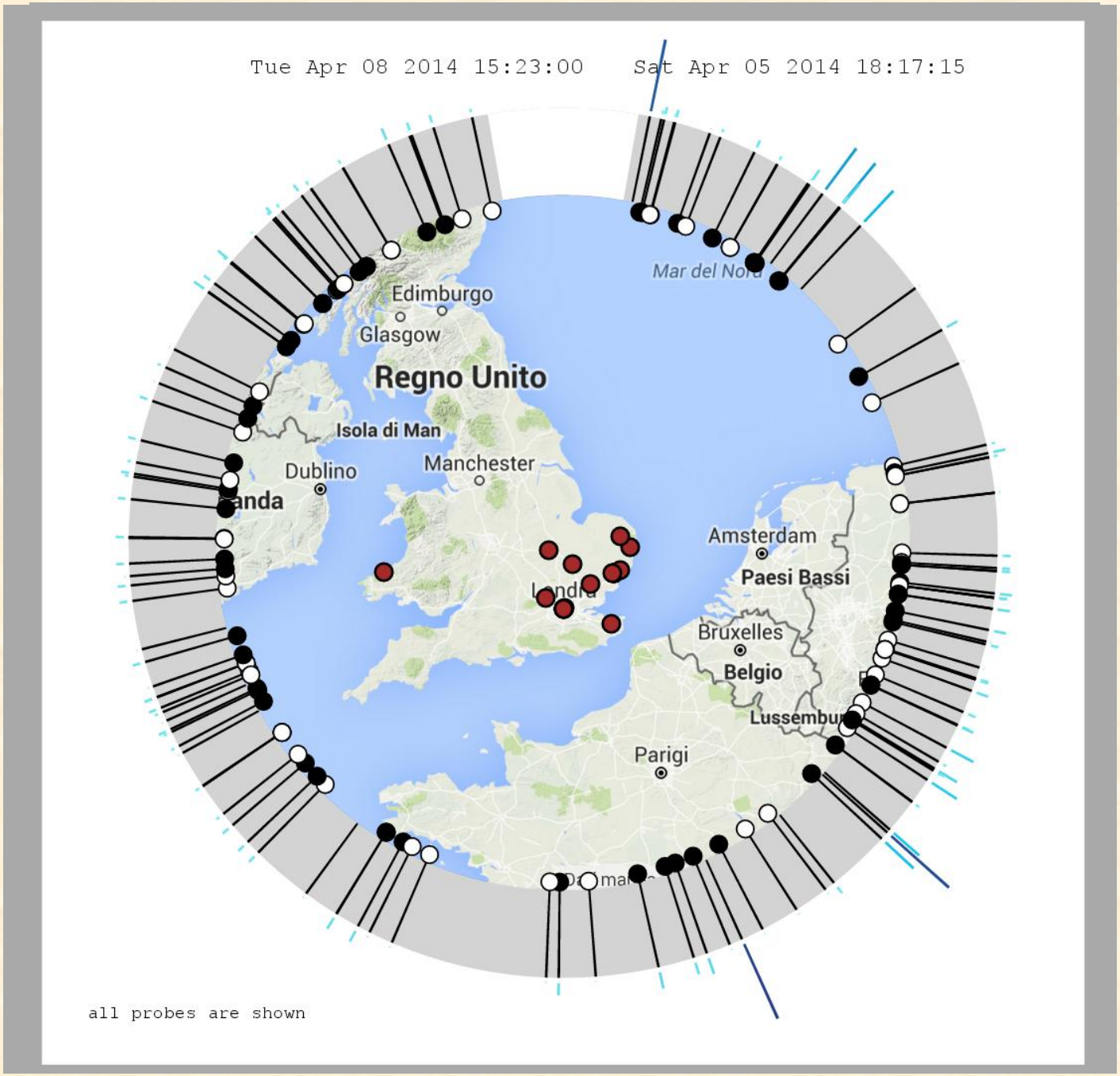
space-time view

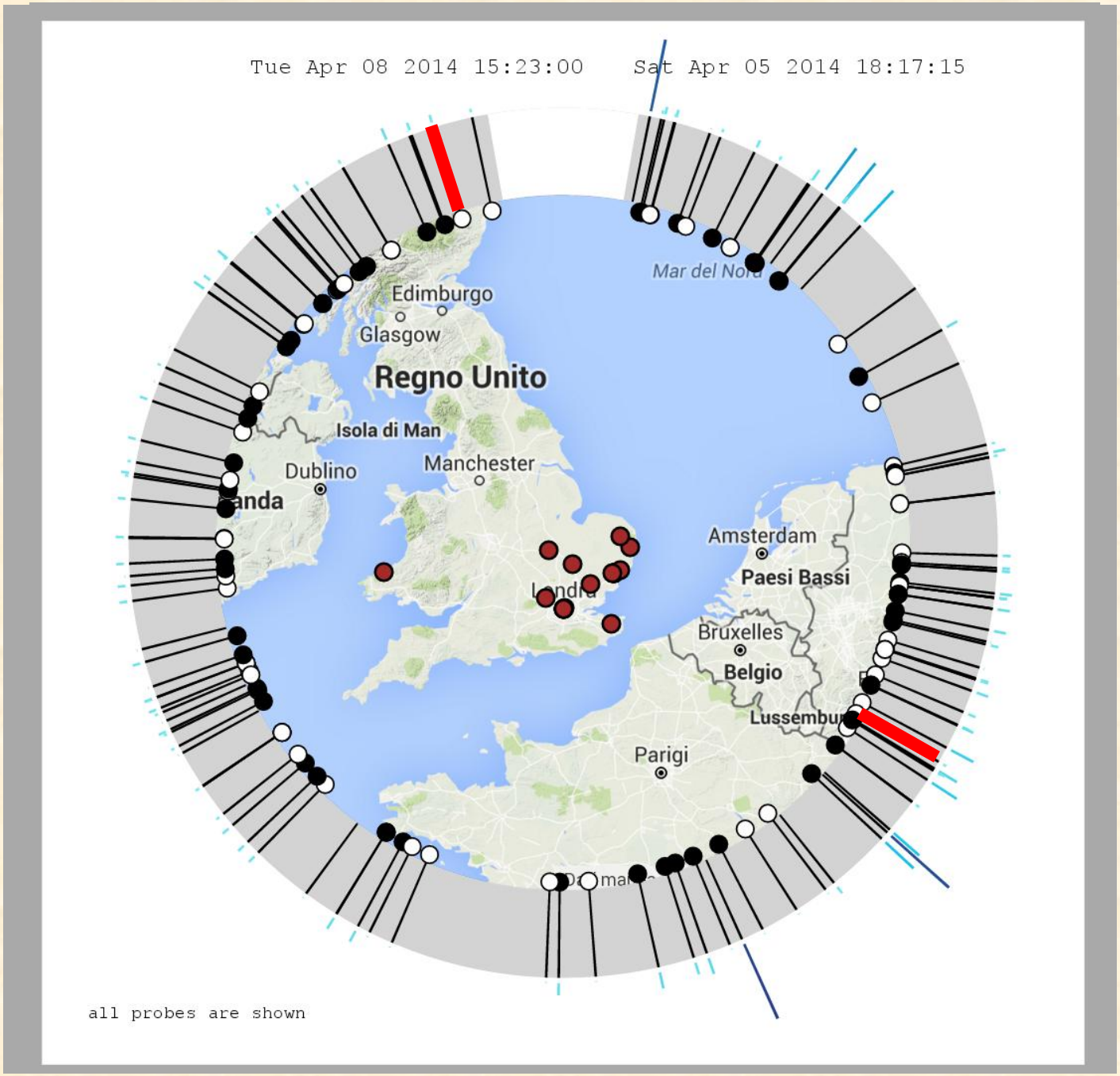


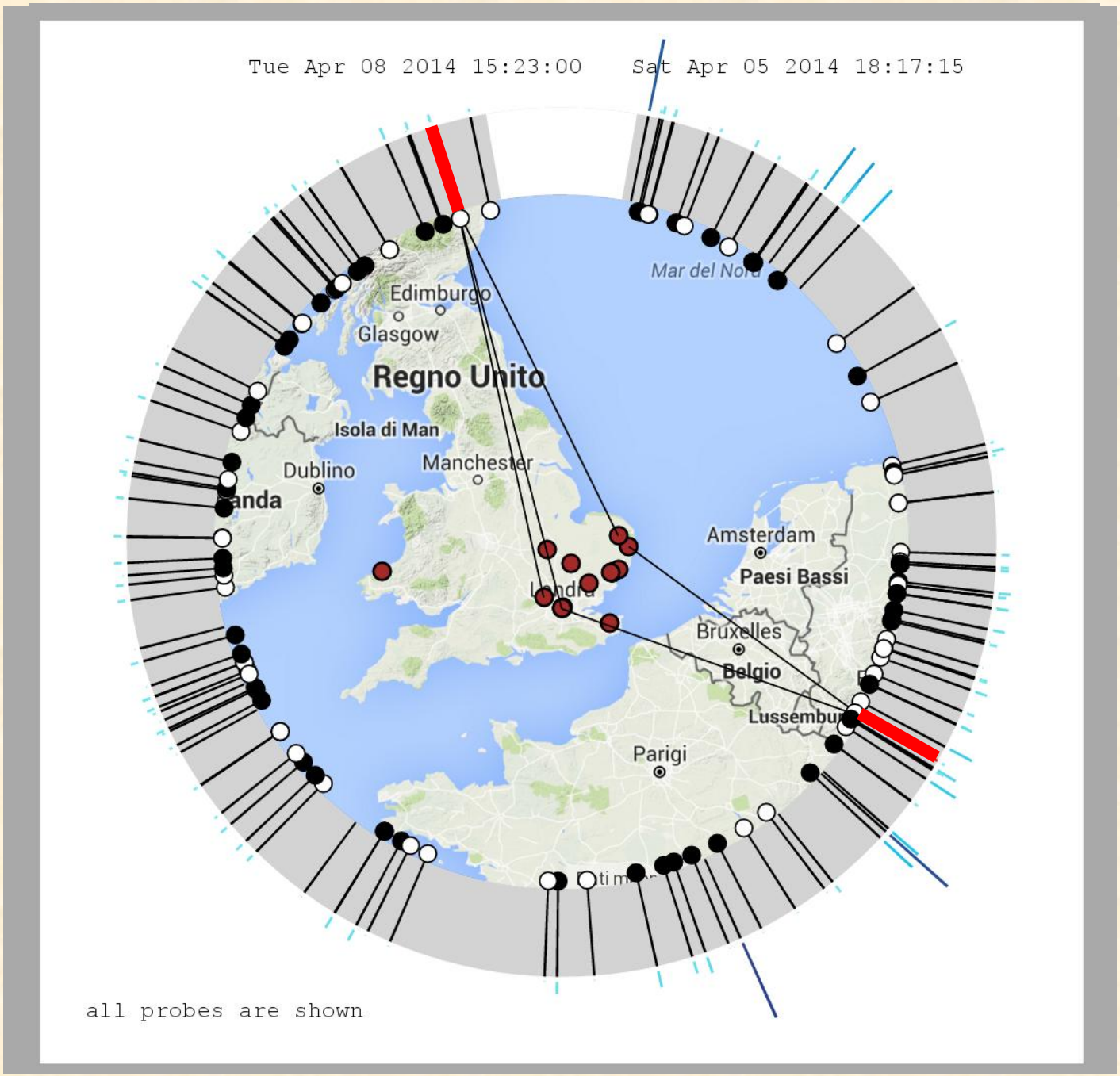
space-time view

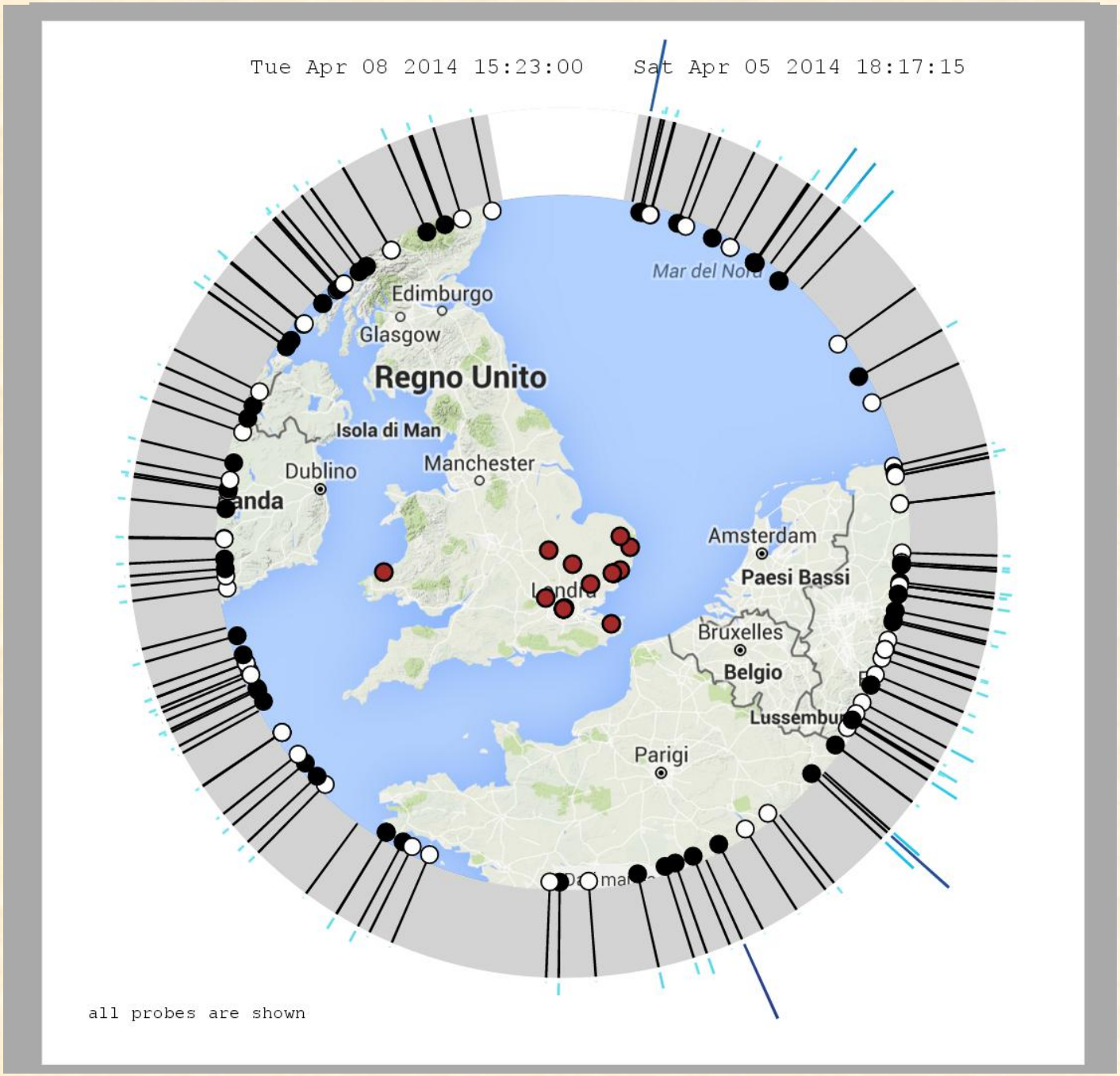

Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
CREATIVE WATCH
RADIO CONTROL
all probes are shown
20

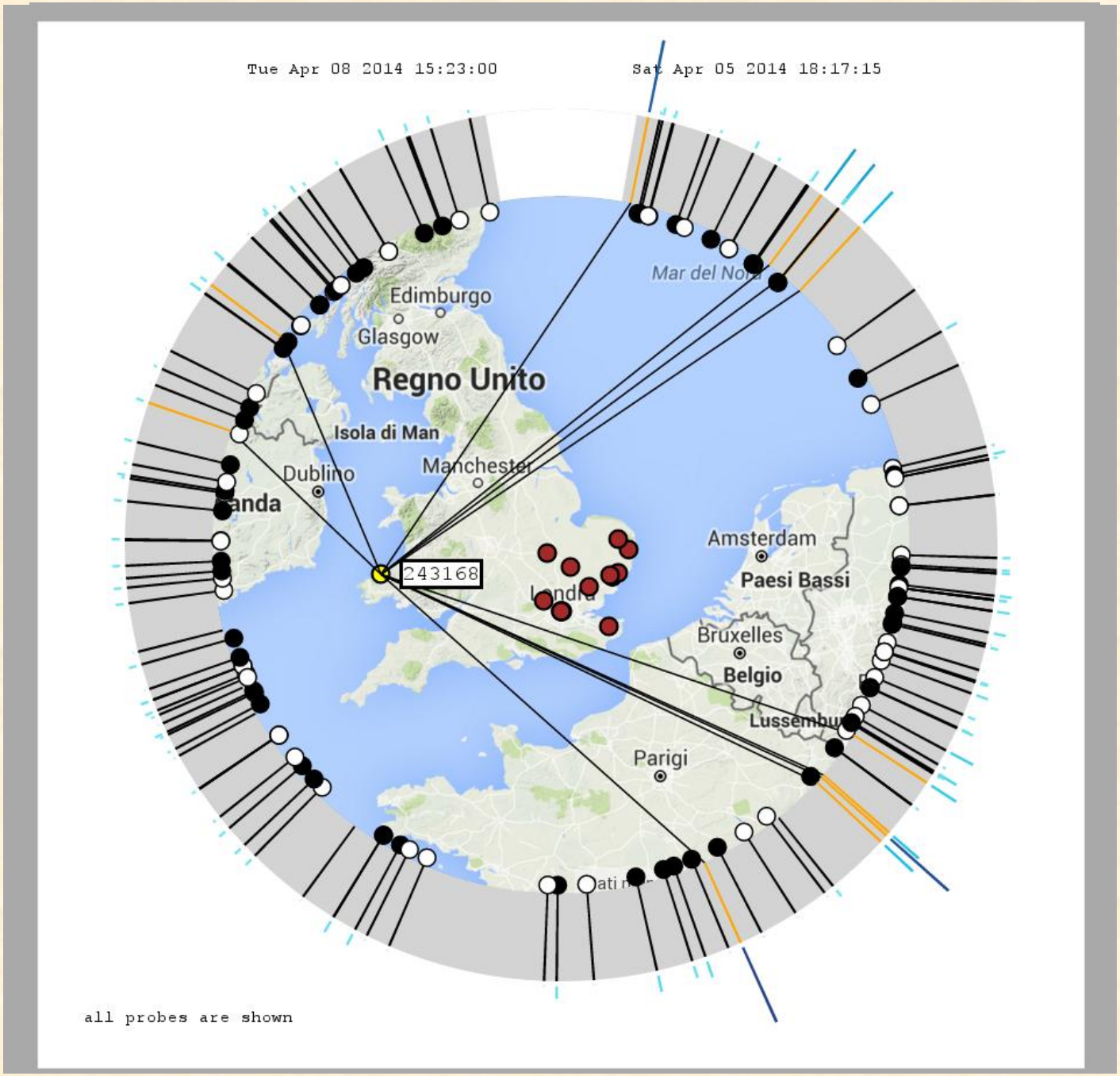

Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
CREATIVE WATCH
RADIO CONTROL
all probes are shown
20

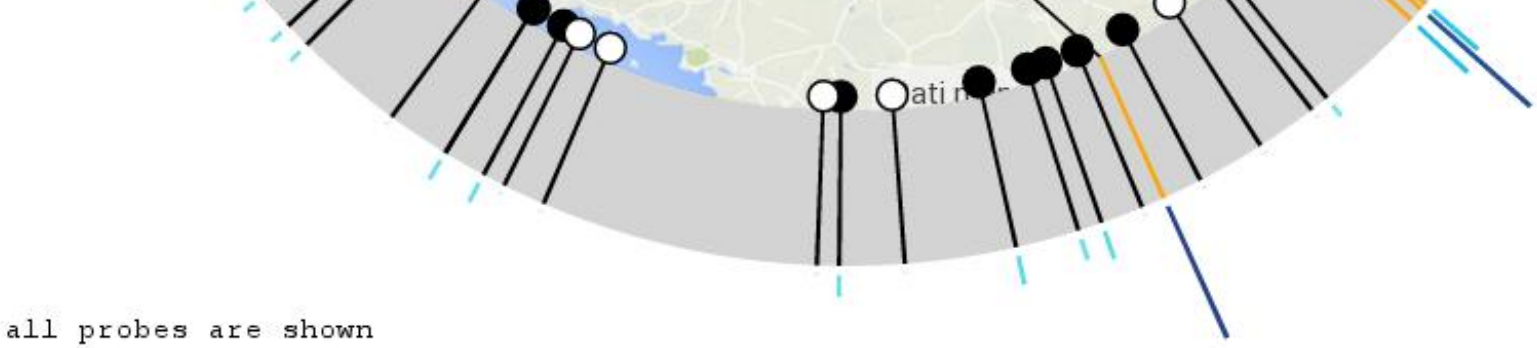

Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Manchester
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Parigi
all probes are shown


Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Manchester
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Parigi
all probes are shown


Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
Mar del Nord
Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Manchester
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Parigi
all probes are shown


Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Manchester
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Parigi
all probes are shown


Tue Apr 08 2014 15:23:00
Sat Apr 05 2014 18:17:15
Edimburgo
Glasgow
Regno Unito
Isola di Man
Dublino
Manchester
243168
Amsterdam
Paesi Bassi
Bruxelles
Belgio
Parigi
all probes are shown



all probes are shown

Display events that satisfy the following conditions:

Min impact

5 10 15 20

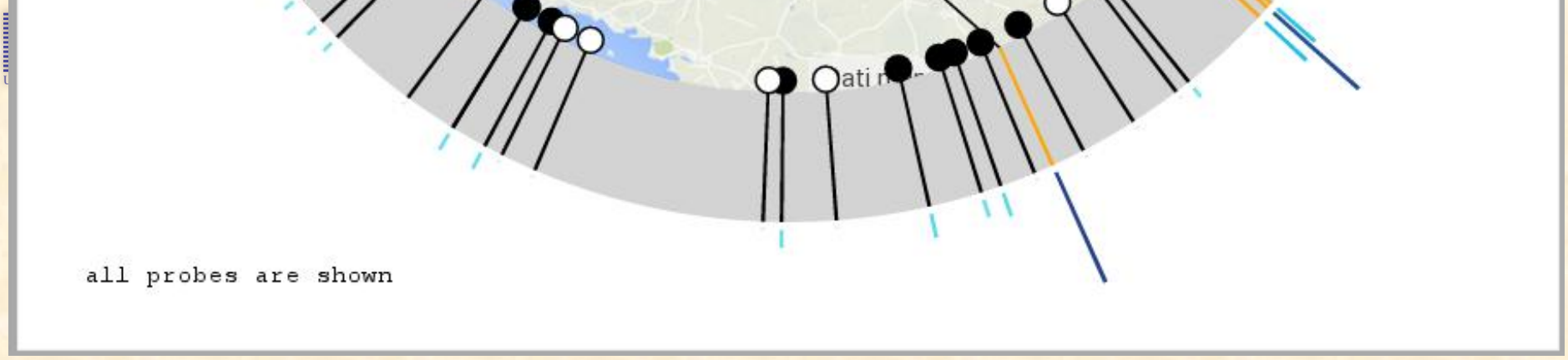
AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

filtering panel



all probes are shown

Display events that satisfy the following conditions:

Min impact

5 10 15 20

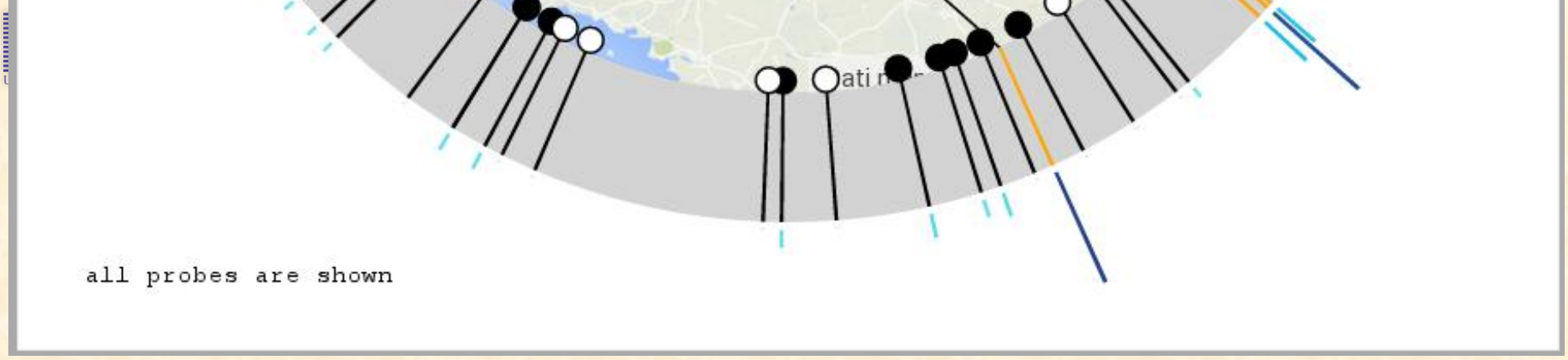
AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

filtering panel



all probes are shown

Display events that satisfy the following conditions:

Min impact

5 10 15 20

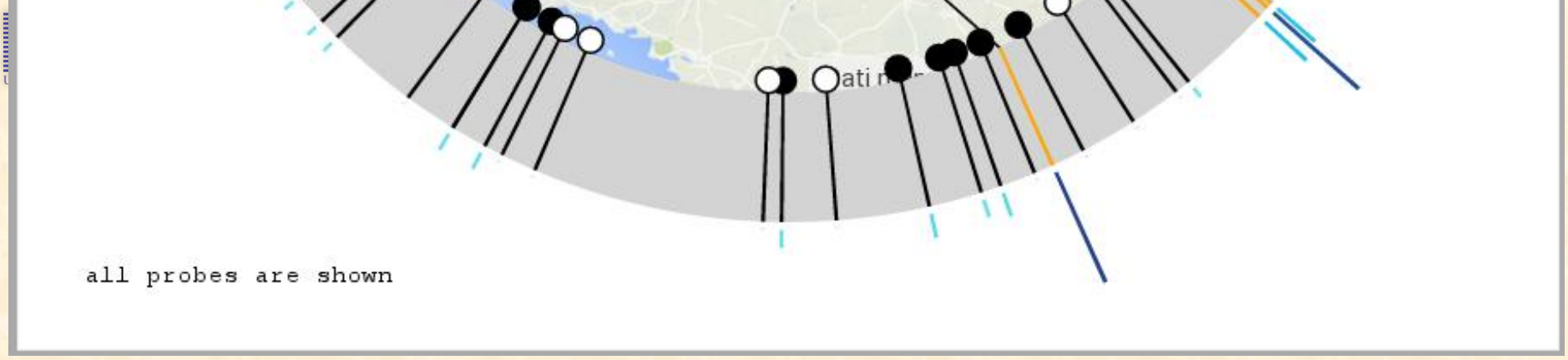
AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

filtering panel



Display events that satisfy the following conditions:

Min impact

5 10 15 20

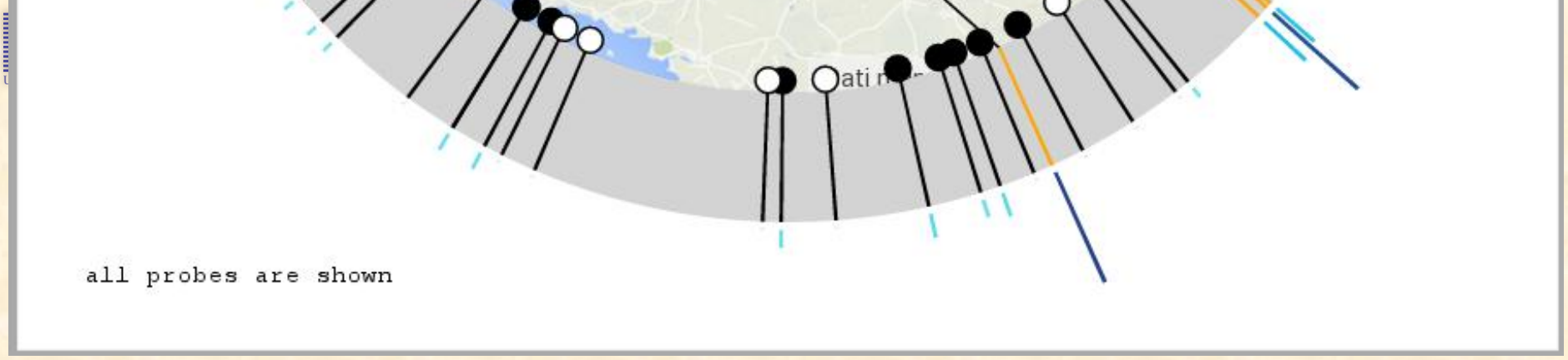
AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

filtering panel



all probes are shown

Display events that satisfy the following conditions:

Min impact

5 10 15 20

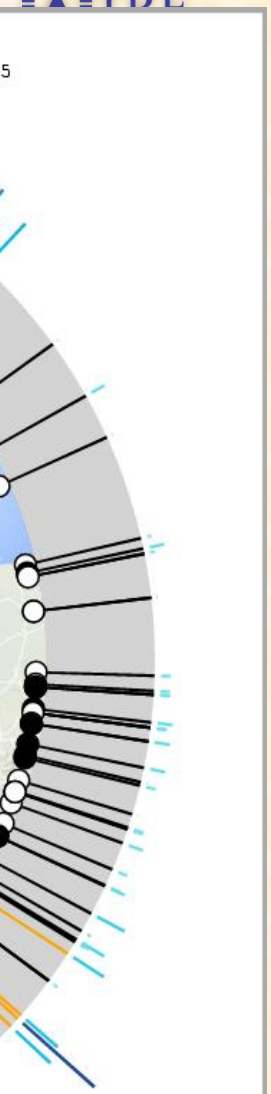
AND

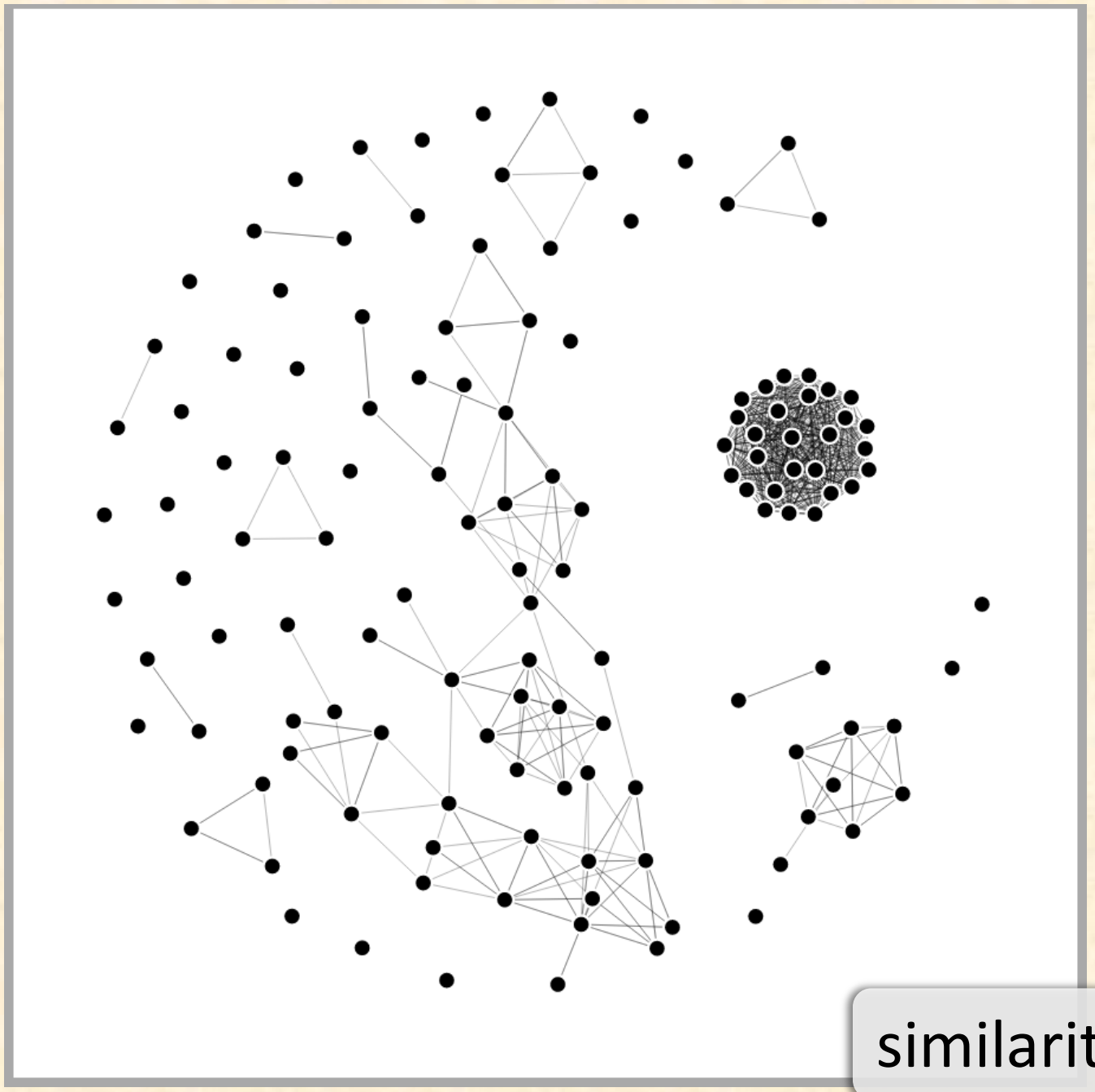
Impacted AS is: <None>

Target is: <None>

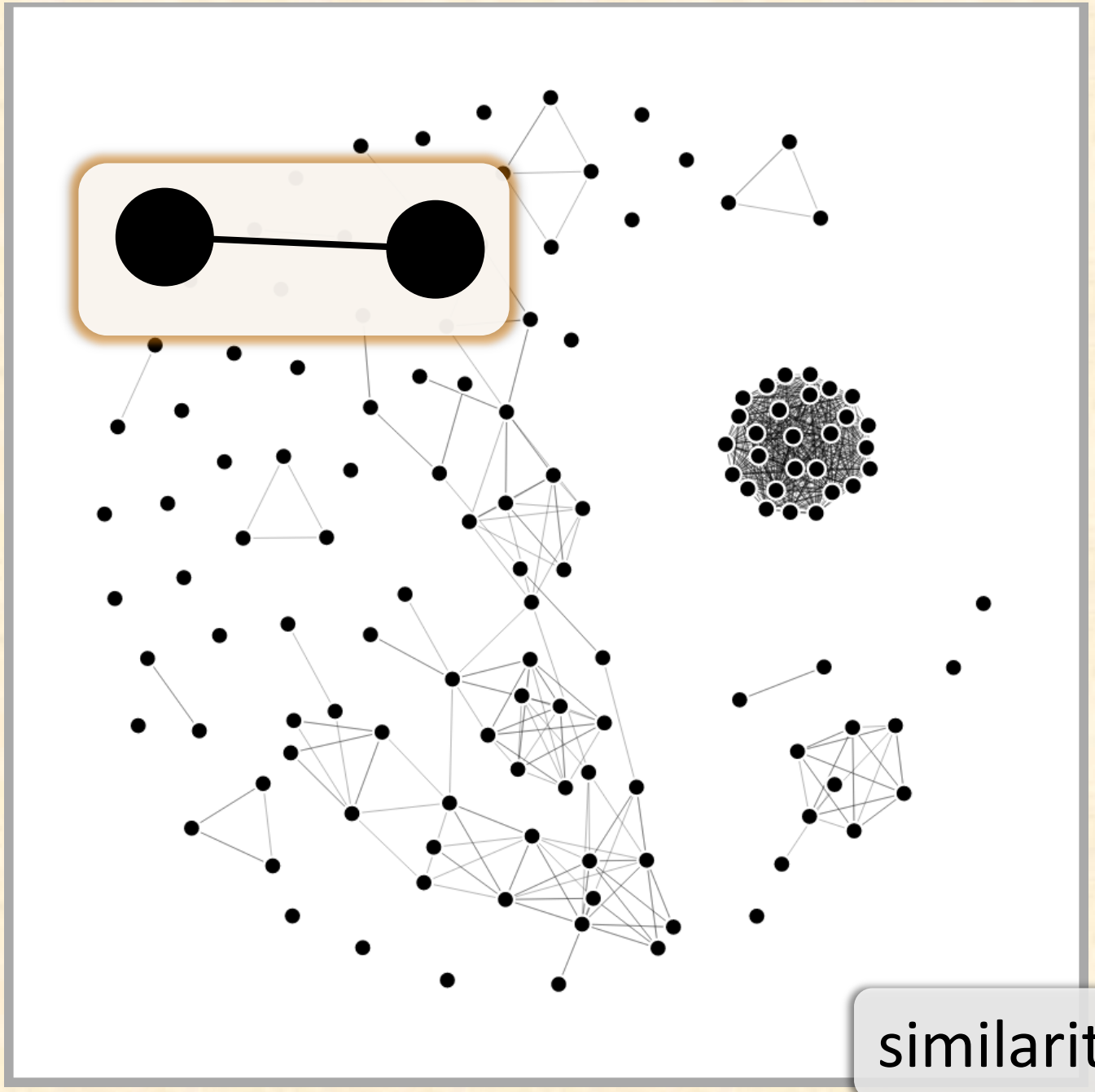
Cause AS is: <None>

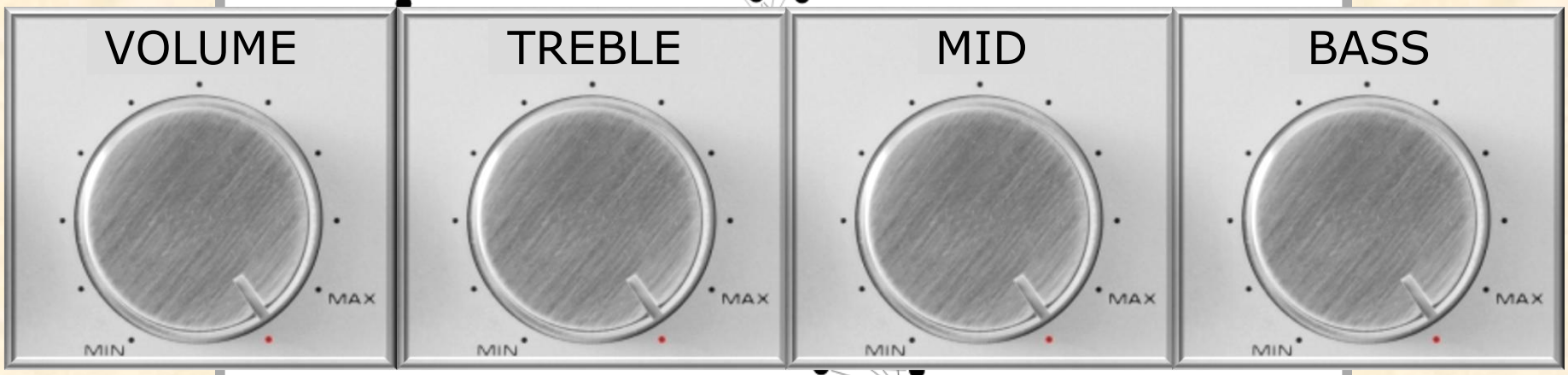
filtering panel





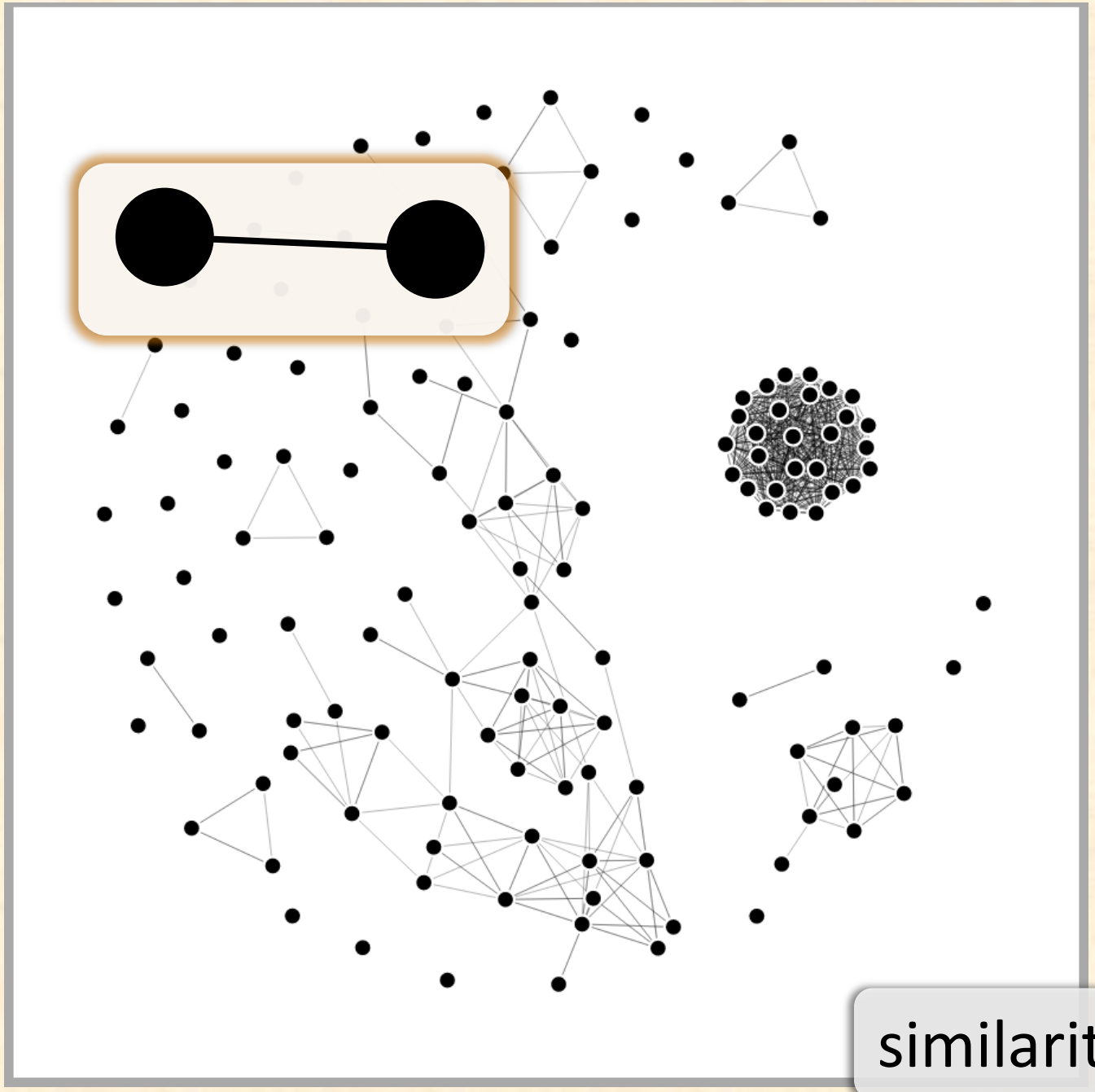
similarity view

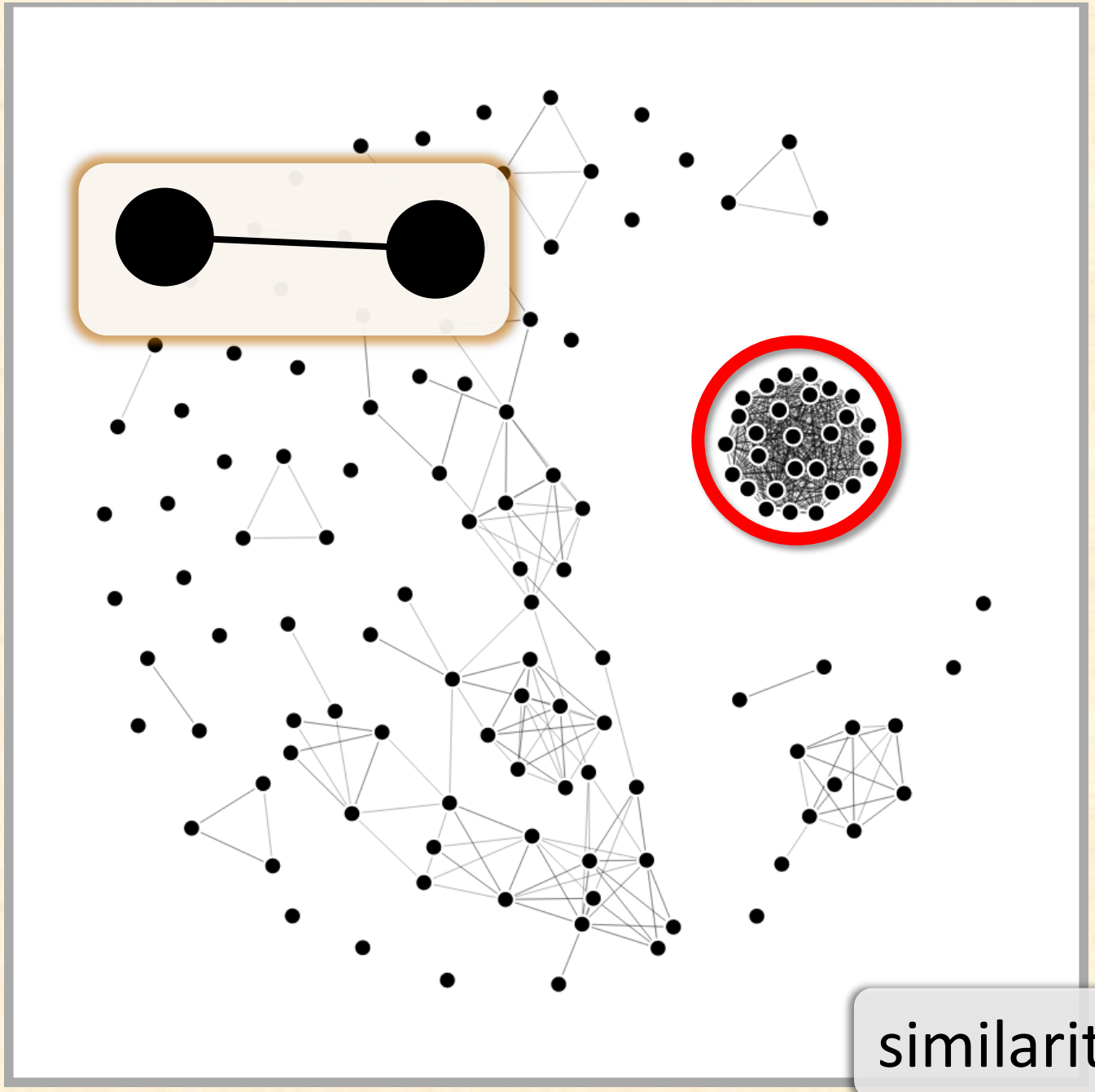

similarity view



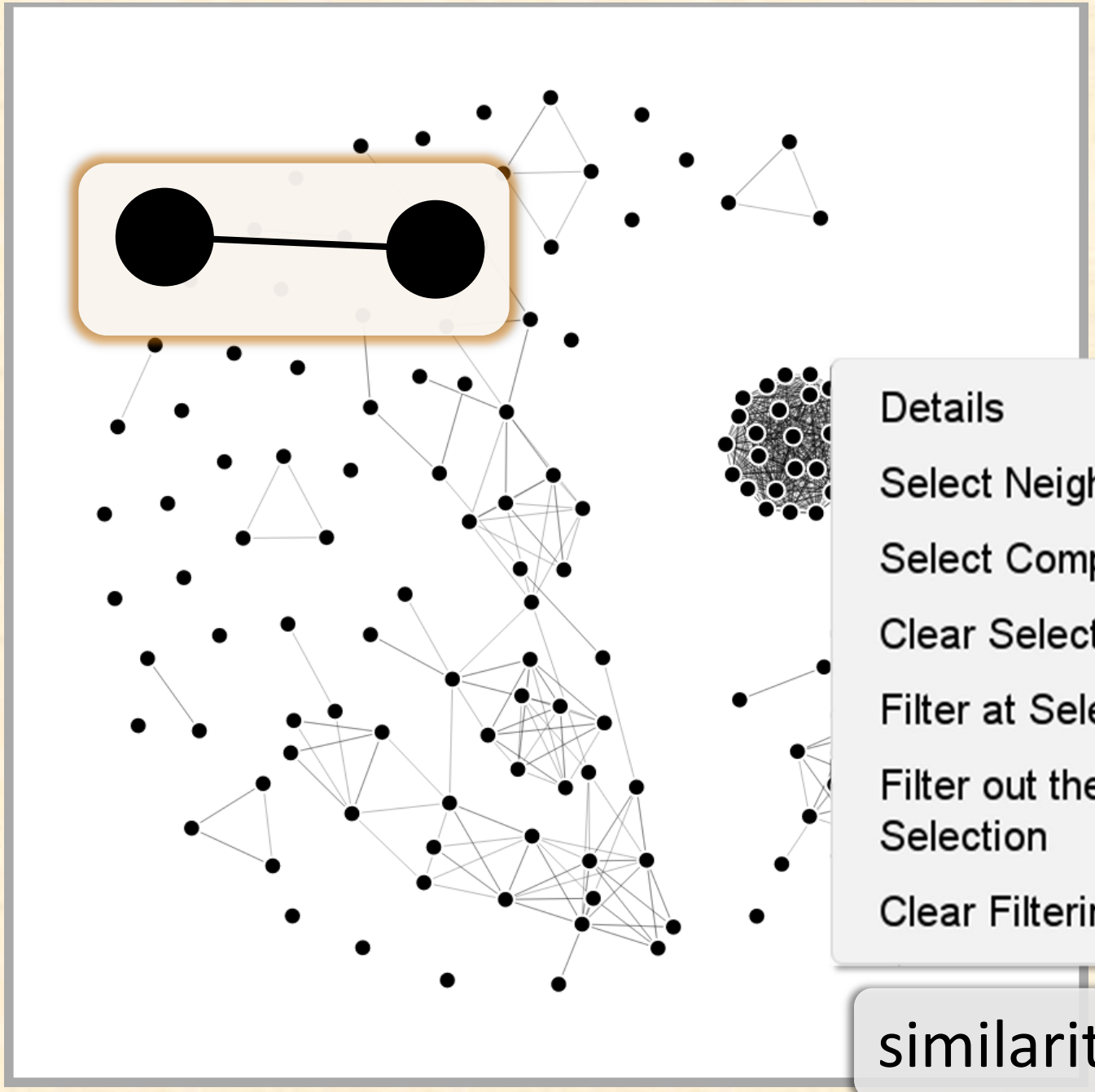
similarity view

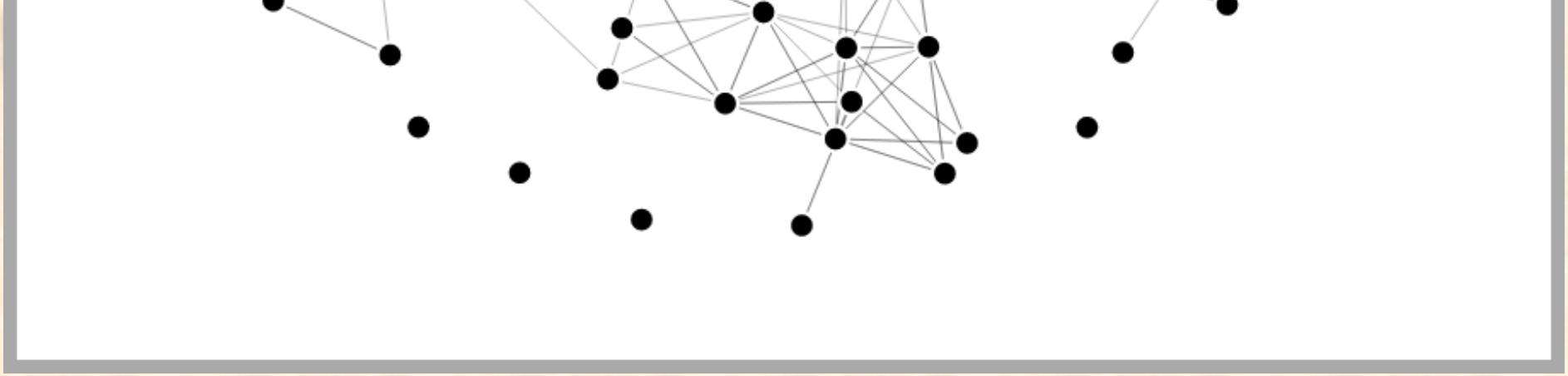
similarity view


similarity view



similarity view


Details
Select Neighbors
Select Component
Clear Selection
Filter at Selection
Filter out the Selection
Clear Filtering
similarity view



Edge count cap (max:35532)

0 2000 4000

Compute similarity between events considering:

Sets of probes

0 50 100

Time:

0 50 100

Recurrence:

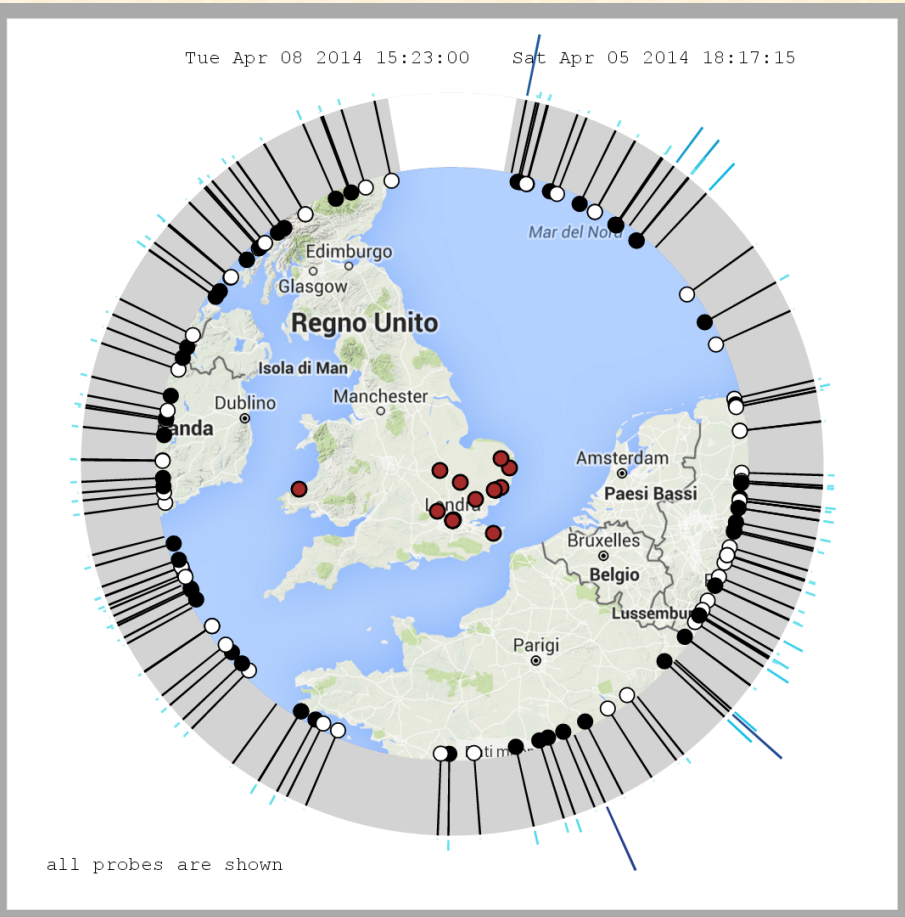
None

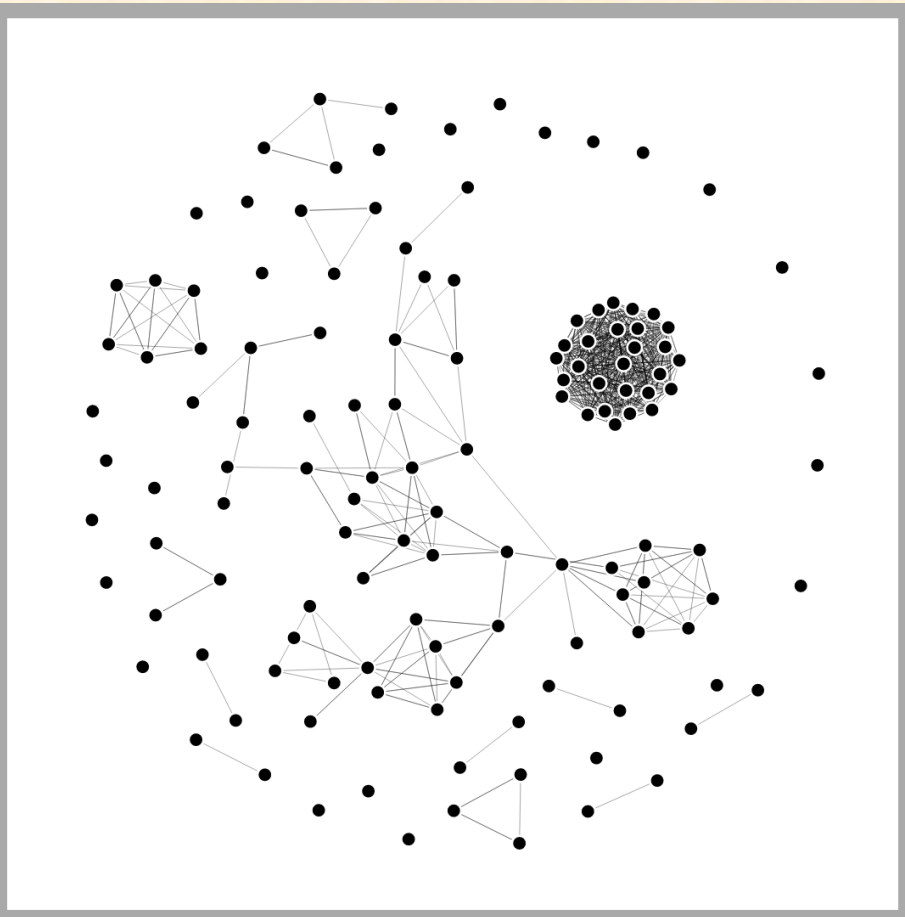
Sets of causes

0 50 100

similarity panel

ROMA TRE
UNIVERSITÀ DEGLI STUDI





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

Compute similarity between events considering:

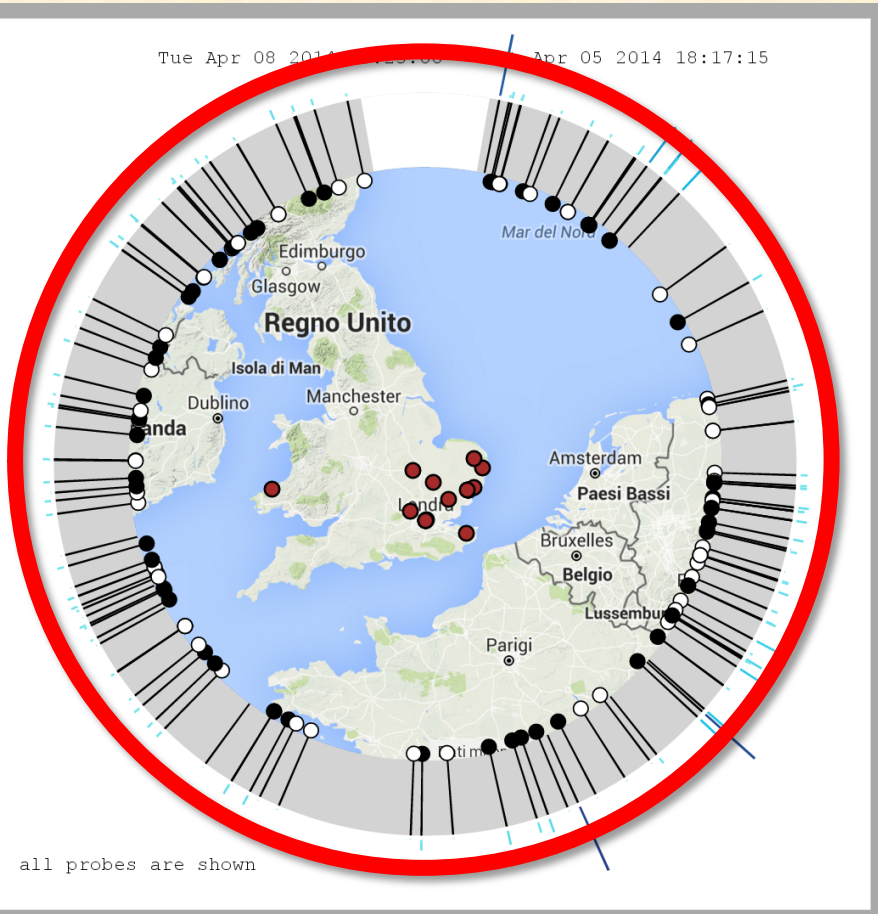
Sets of probes
0 50 100

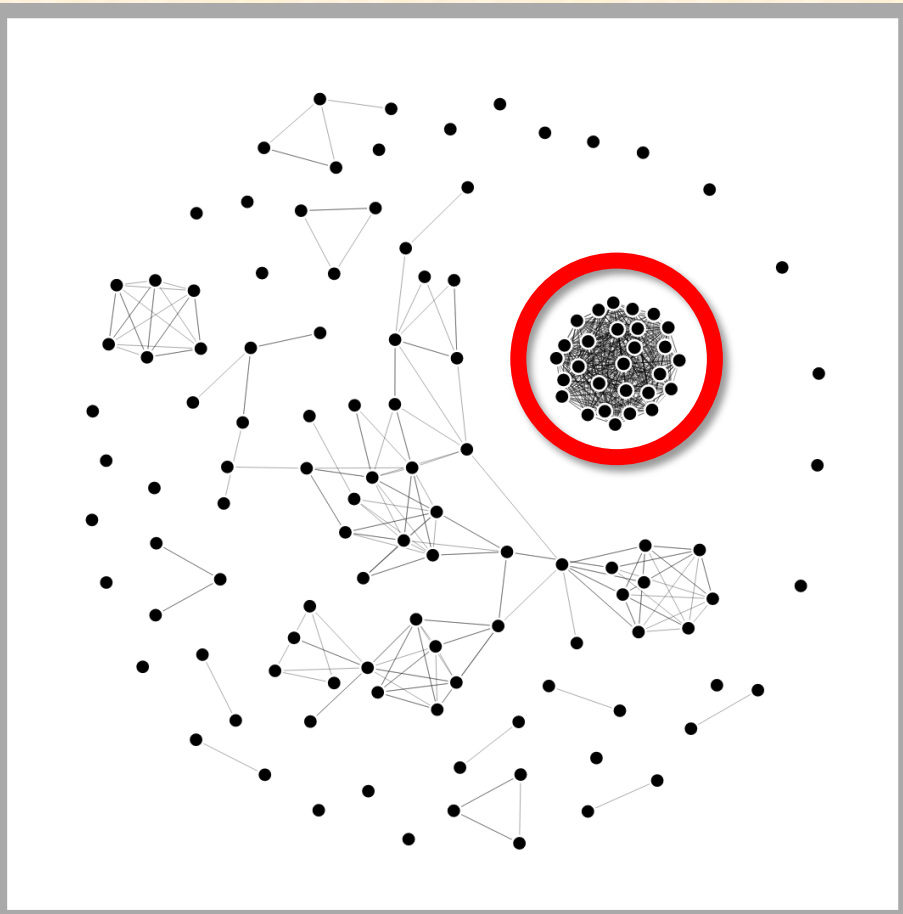
Time:
0 50 100

Recurrence:
None

Sets of causes
0 50 100

ROMA TRE
UNIVERSITÀ DEGLI STUDI





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

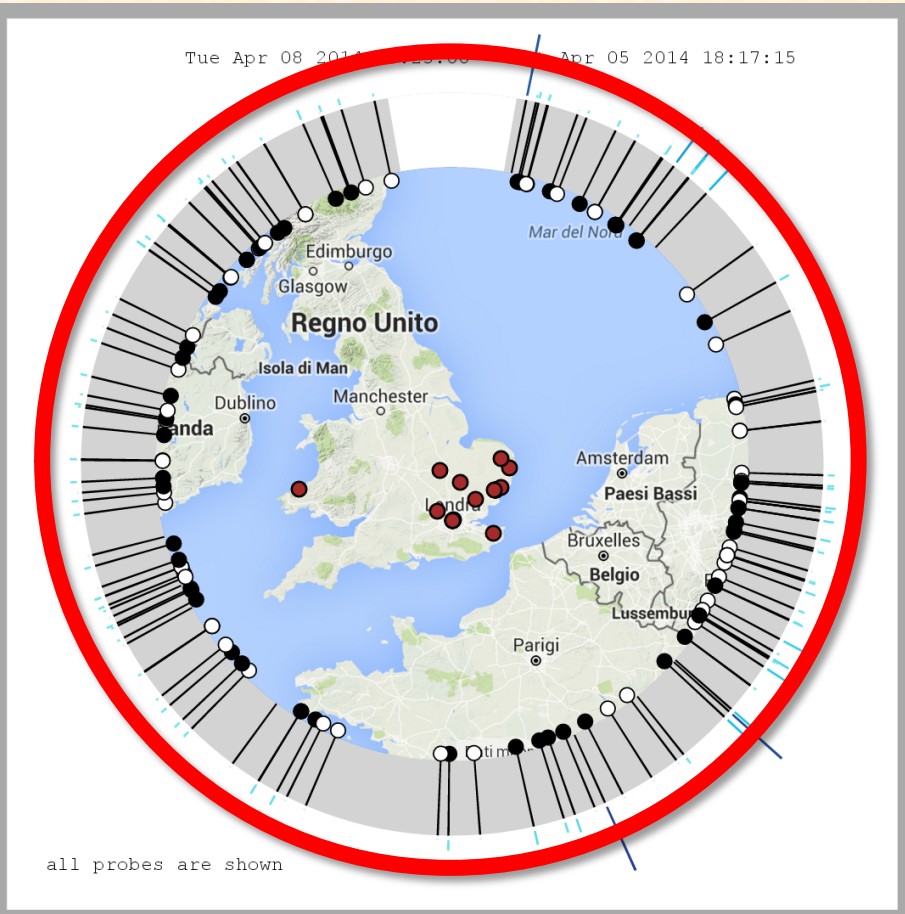
Compute similarity between events considering:

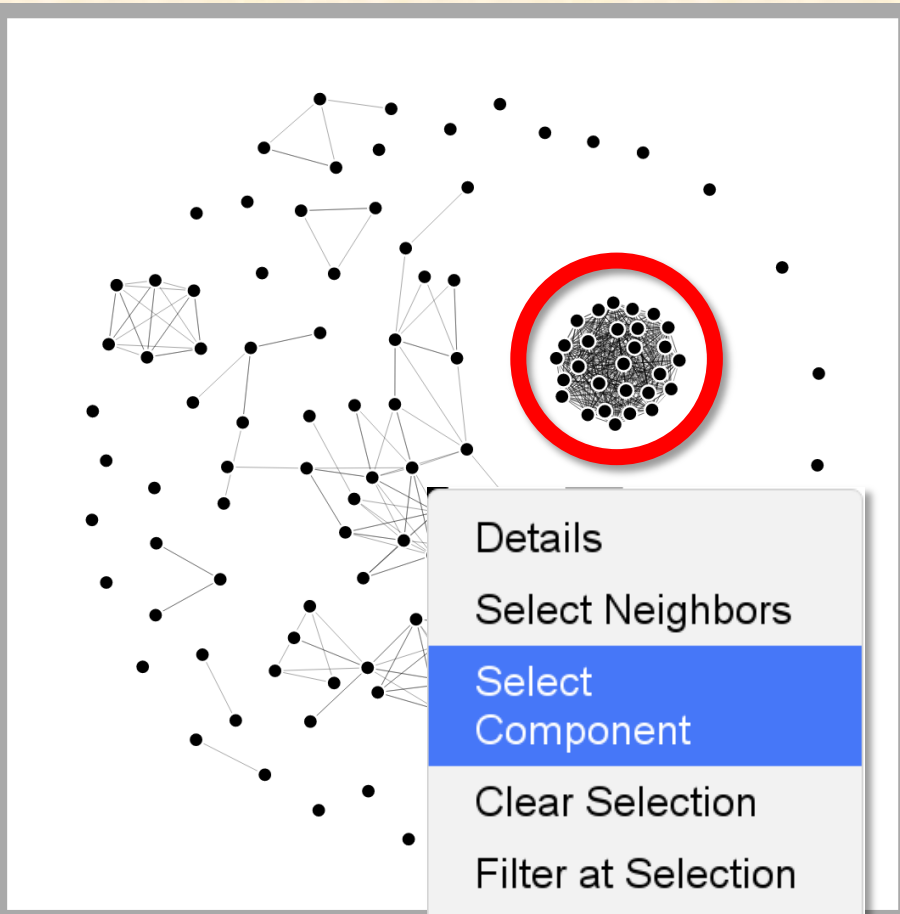
Sets of probes
0 50 100

Time:
0 50 100

Recurrence:
None

Sets of causes
0 50 100





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge cou
0 2

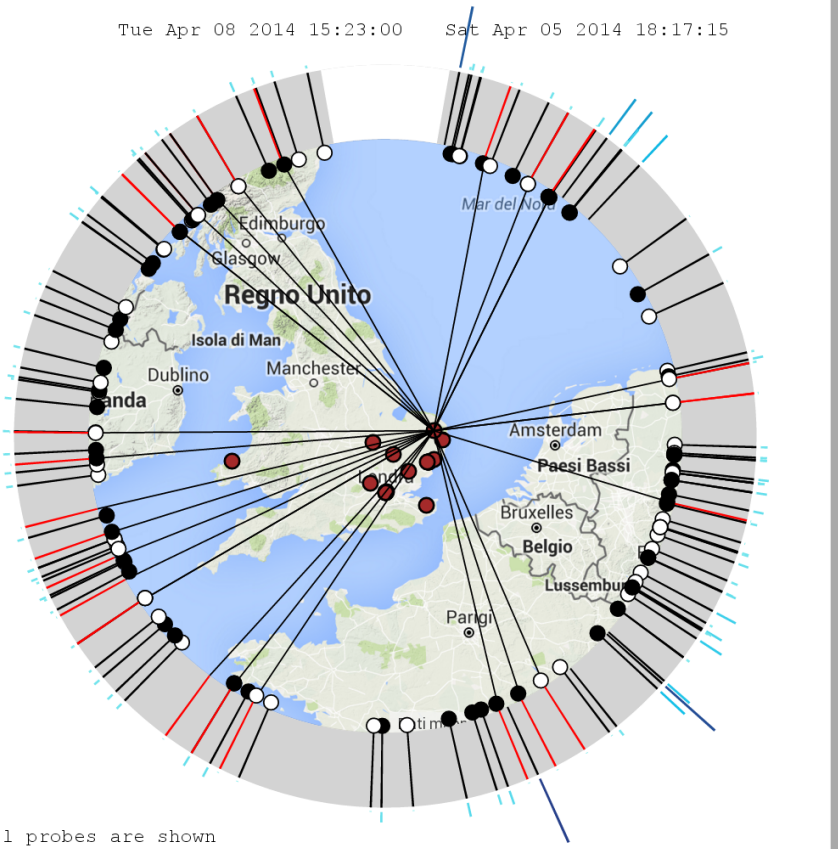
Compute similarity between events con

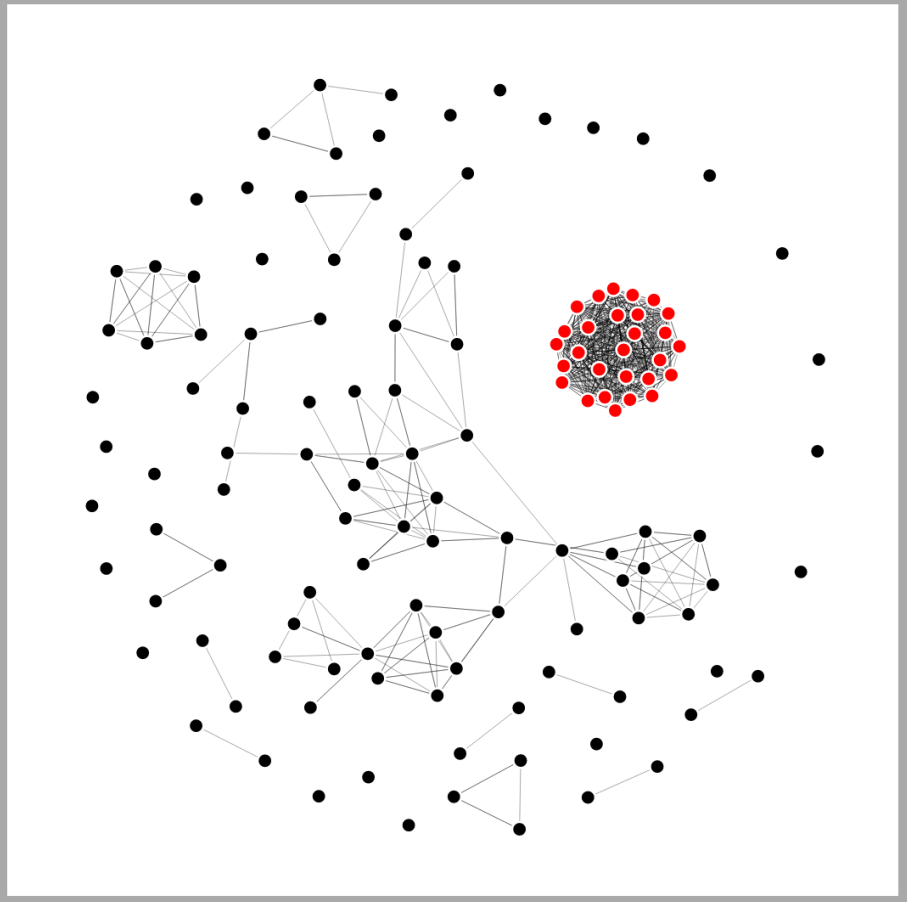
Sets of probes
0 50 100

Time:
0 50

Sets of causes
0 50 100

ROMA TRE
UNIVERSITÀ DEGLI STUDI





Display events that satisfy the following conditions:

Min impact: 5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292): 0 2000 4000

Compute similarity between events considering:

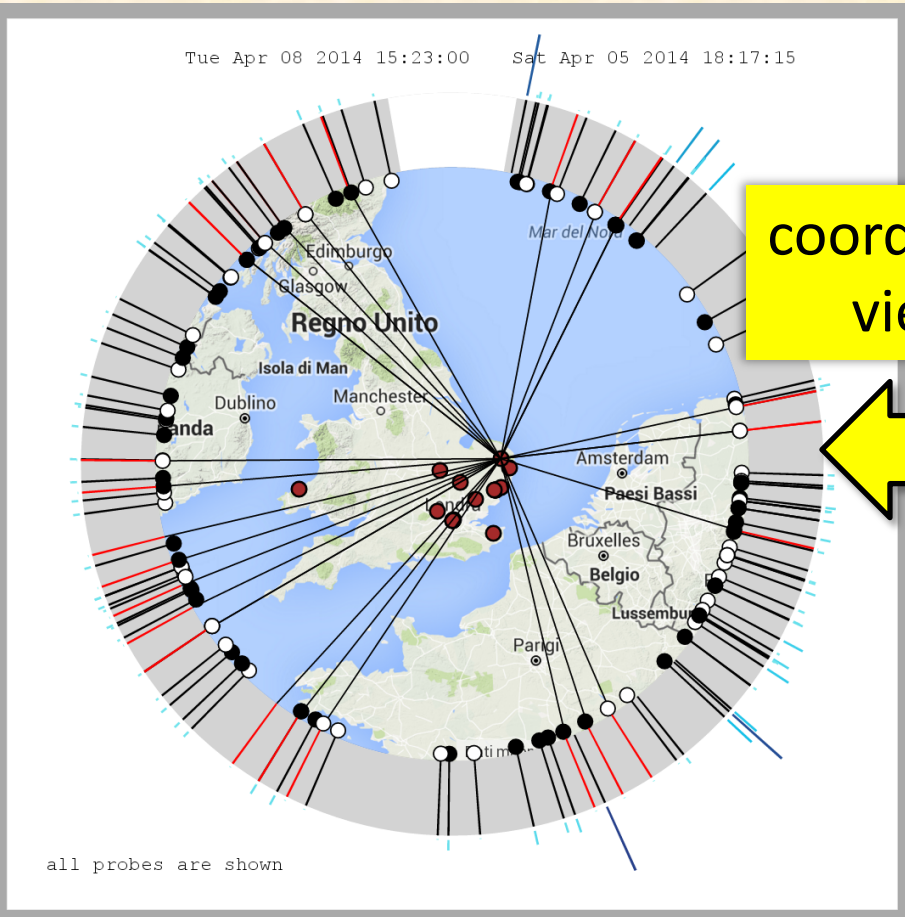
Sets of probes: 0 50 100

Time: 0 50 100

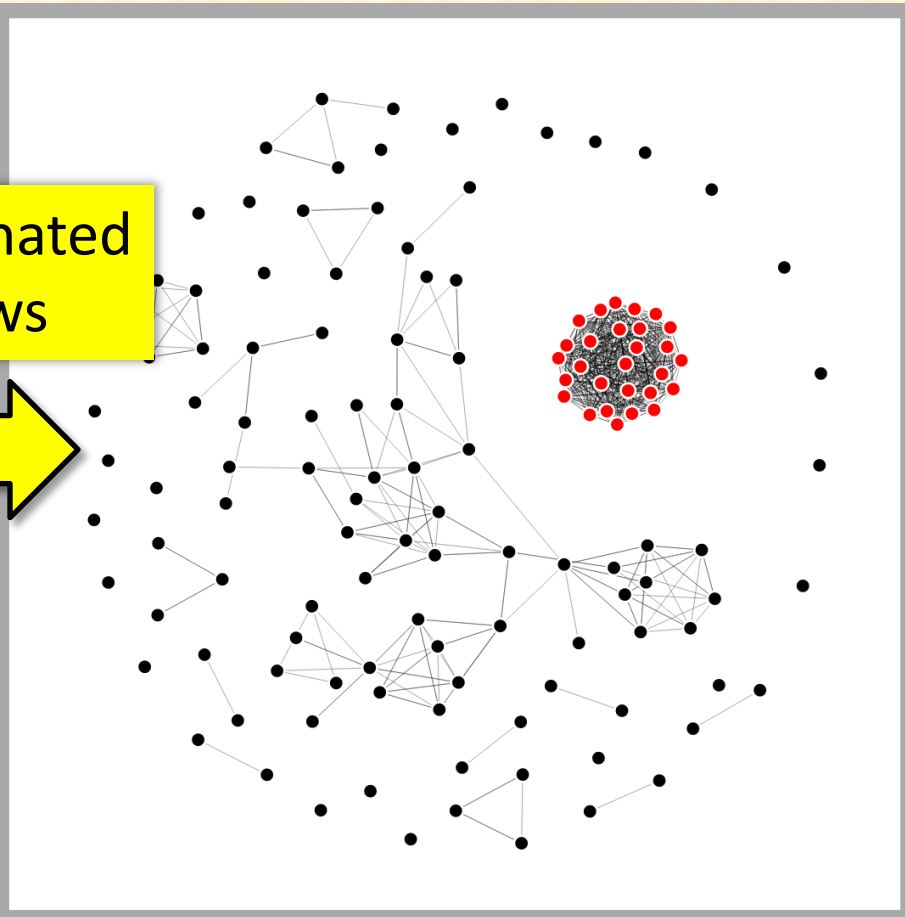
Recurrence: None

Sets of causes: 0 50 100

ROMA TRE
UNIVERSITÀ DEGLI STUDI



coordinated views



Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

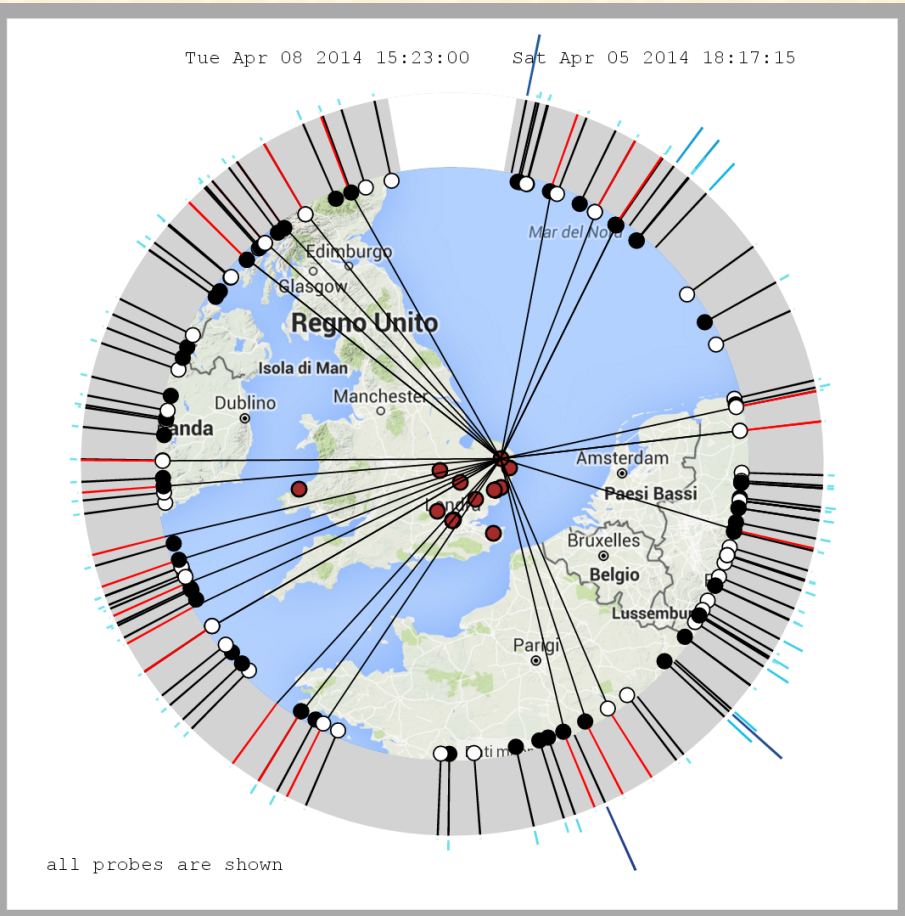
Compute similarity between events considering:

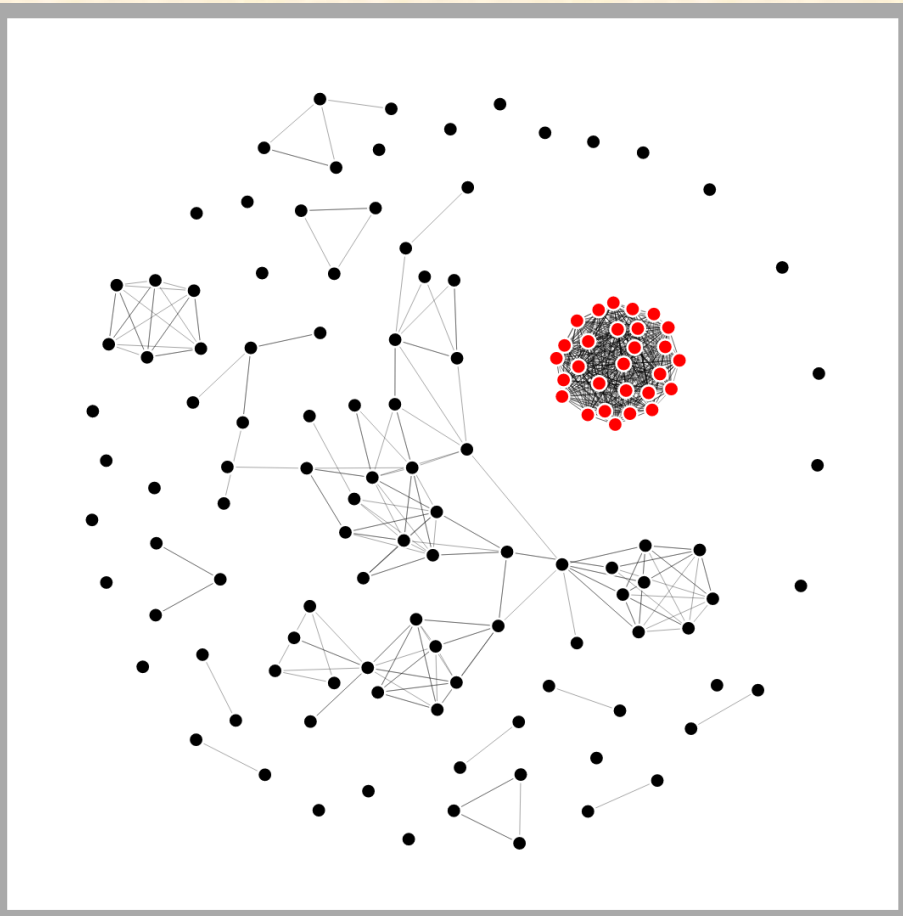
Sets of probes
0 50 100

Time:
0 50 100

Recurrence:
None

Sets of causes
0 50 100





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>
Target is: <None>
Cause AS is: <None>

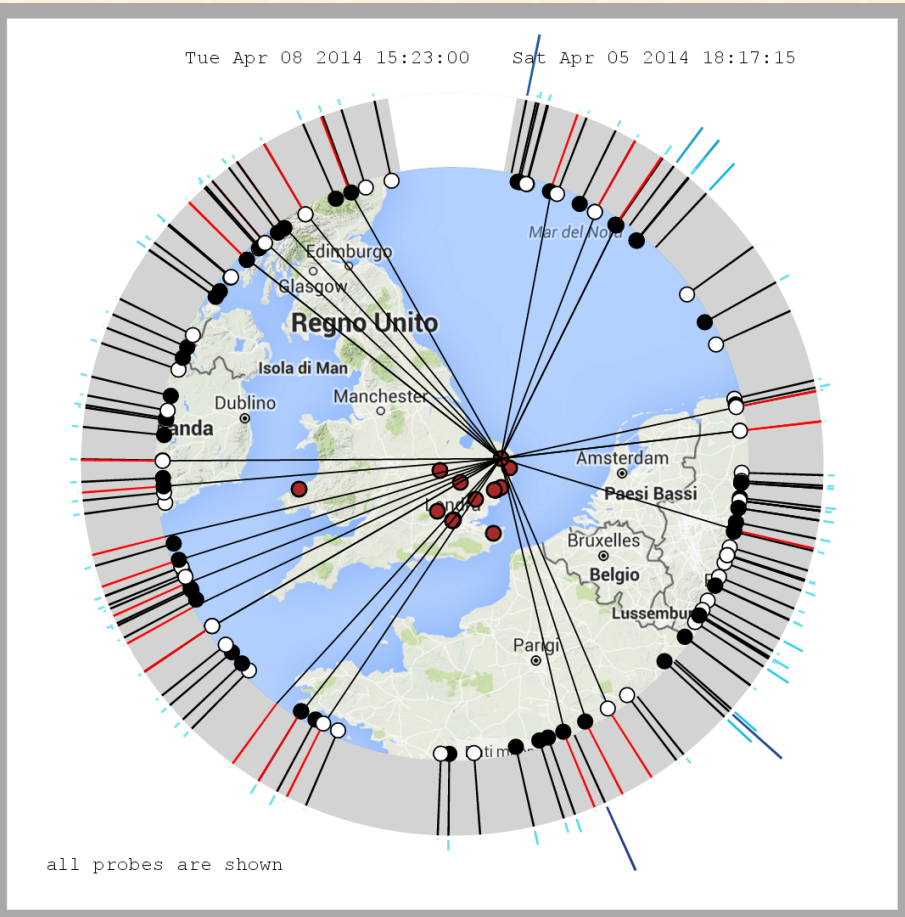
Edge count cap (max:17292)
0 2000 4000

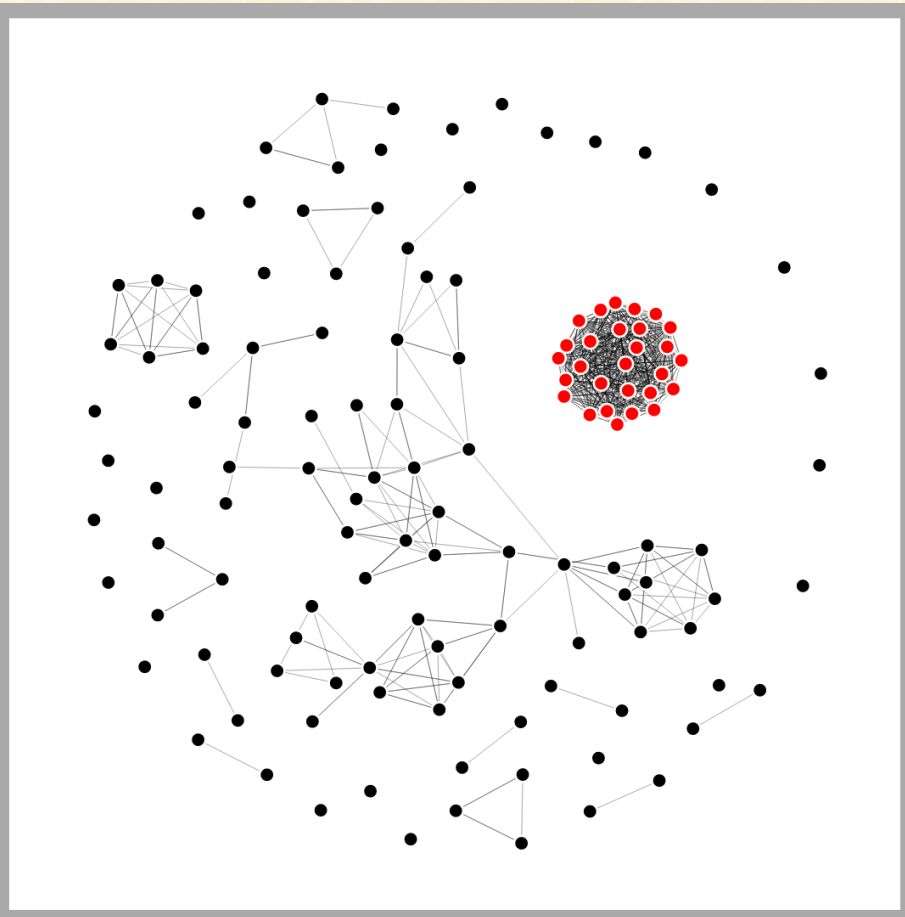
Sets of probes
0 50 100

Time:
0 50 100

Recurrence:
None

0 50 100





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>
Target is: <None>
Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

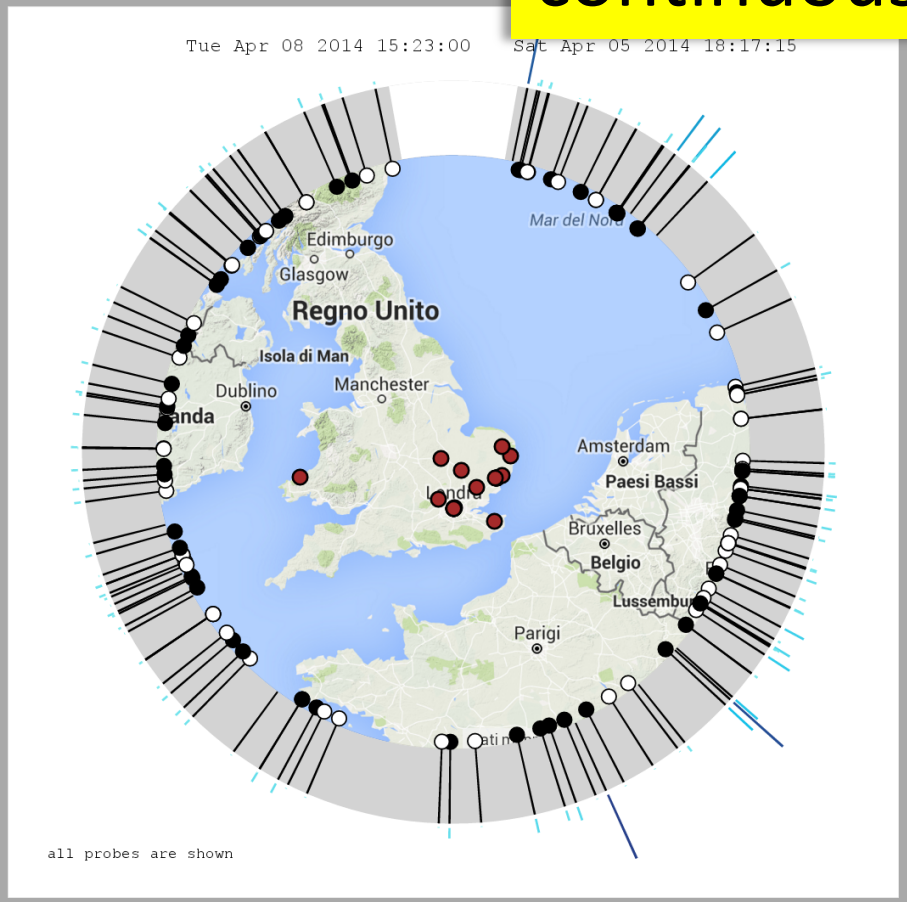
Sets of probes
0 50 100

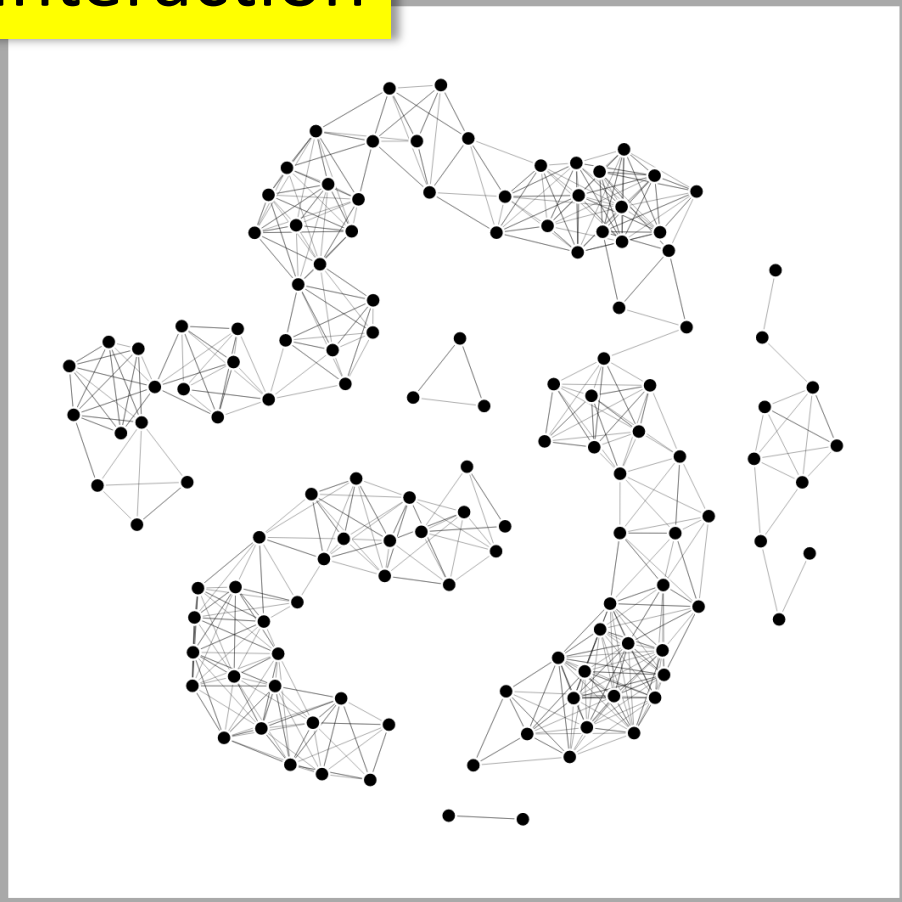
Time:
0 50 100

Recurrence:
Time of day

0 50 100

continuous interaction





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

Compute similarity between events considering:

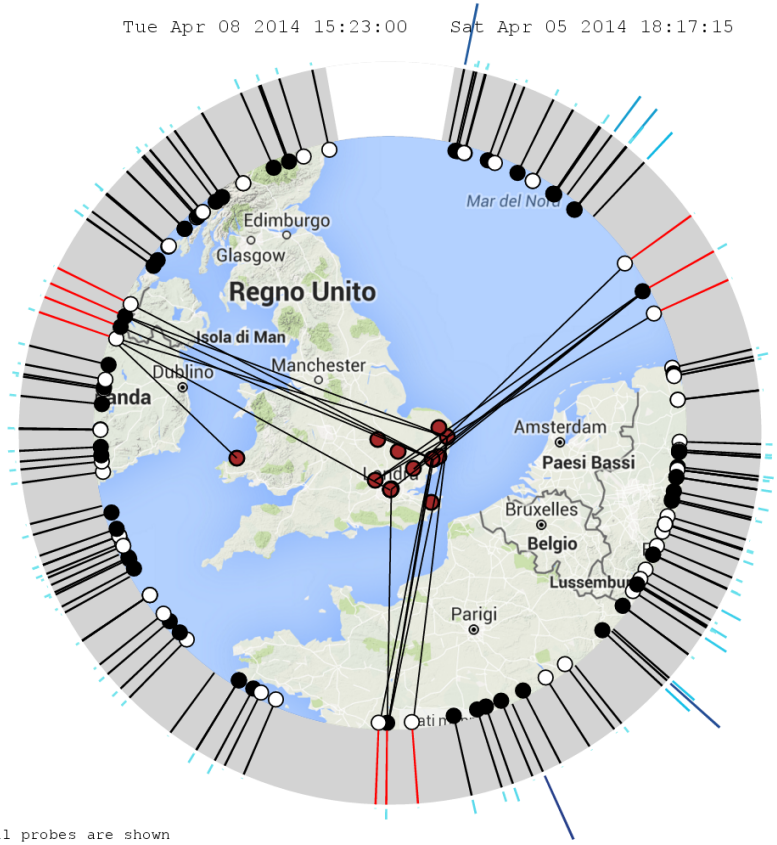
Sets of probes
0 50 100

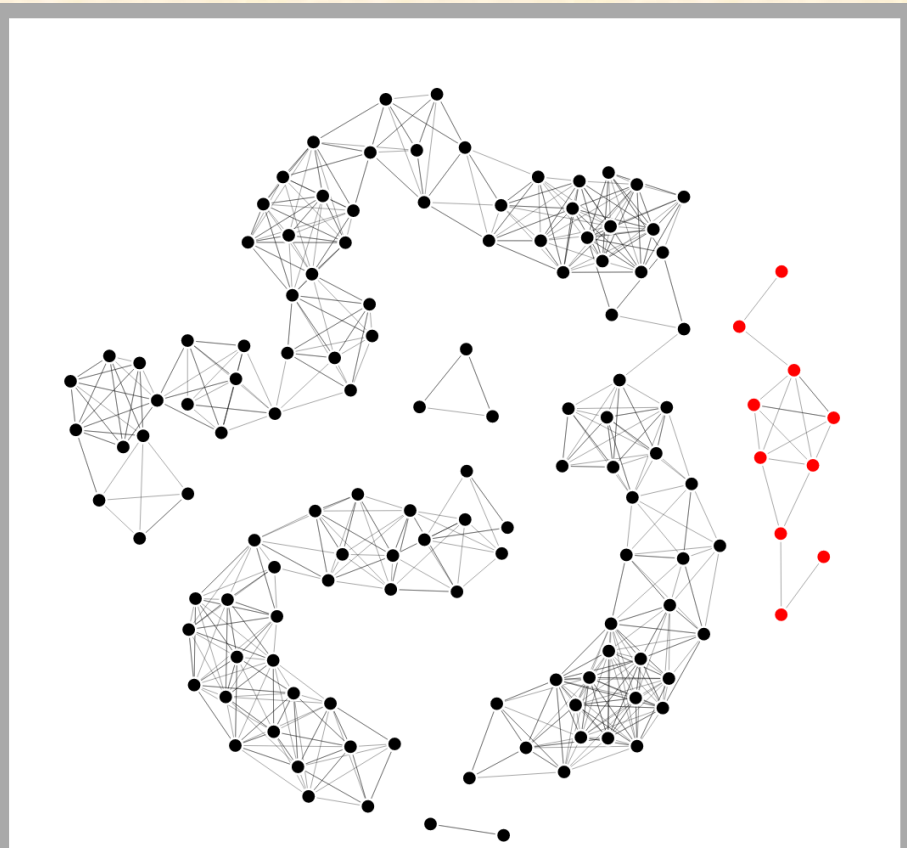
Time:
0 50 100

Recurrence:
Time of day

Sets of causes
0 50 100

ROMA TRE
UNIVERSITÀ DEGLI STUDI





Display events that satisfy the following conditions:

Min impact
5 10 15 20

AND

Impacted AS is: <None>

Target is: <None>

Cause AS is: <None>

Edge count cap (max:17292)
0 2000 4000

Compute similarity between events considering:

Sets of probes
0 50 100

Time:
0 50 100

Recurrence:
Time of day

Sets of causes
0 50 100

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:

1 5

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:

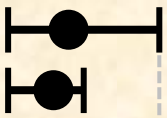
1 5

- events are a useful aggregation of routing dynamics

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:

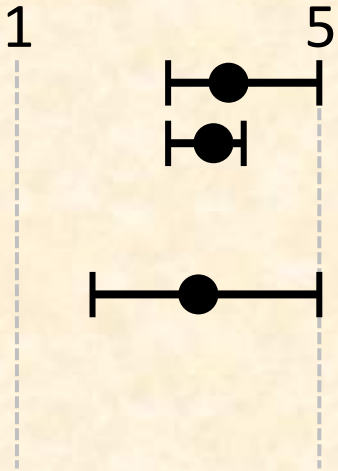
1 5



  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events

User study

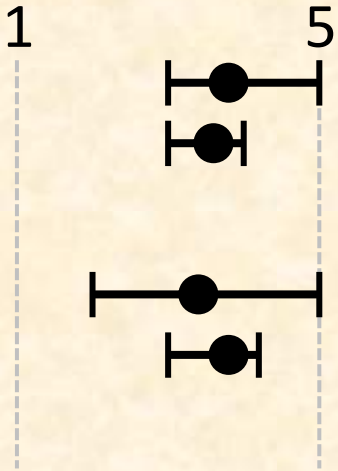
- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:



  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively

User study

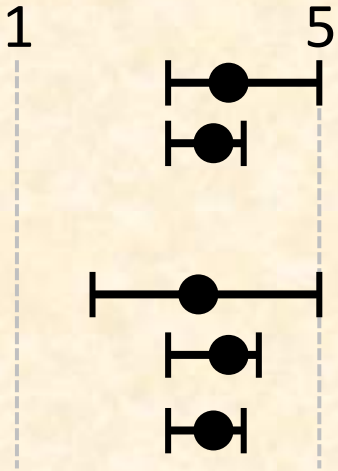
- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:



  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively
  - finding related events is useful

User study

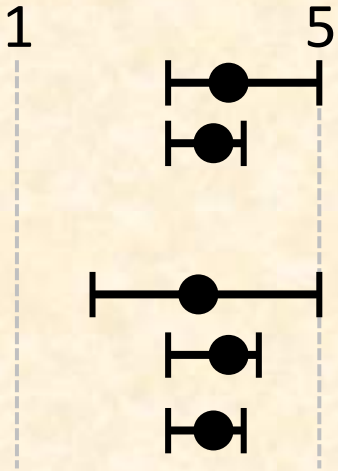
- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:



  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively
  - finding related events is useful
    - the tool supports it effectively

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:

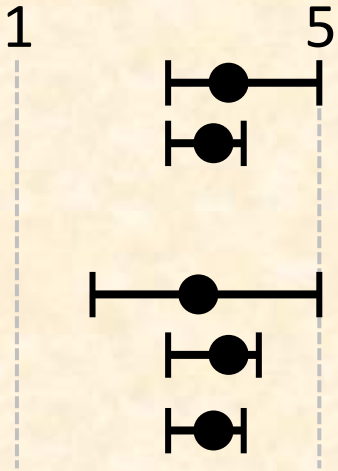


  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively
  - finding related events is useful
    - the tool supports it effectively

Filters

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:



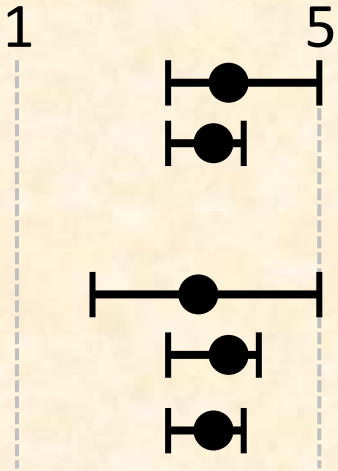
  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively
  - finding related events is useful
    - the tool supports it effectively

Filters

Event patterns

User study

- User sample: employees of the R&D of a prominent italian ISP (experts in IP edge innovation, cyber-security threats, video/multimedia platforms)
- Questionnaire results:



  - events are a useful aggregation of routing dynamics
  - comparing events by probes/geography/time is useful to find related events
    - the tool supports it effectively
  - finding related events is useful
    - the tool supports it effectively

Filters

Event patterns

"A tool for mining traceroutes"

Future Work

Future Work

Future Work

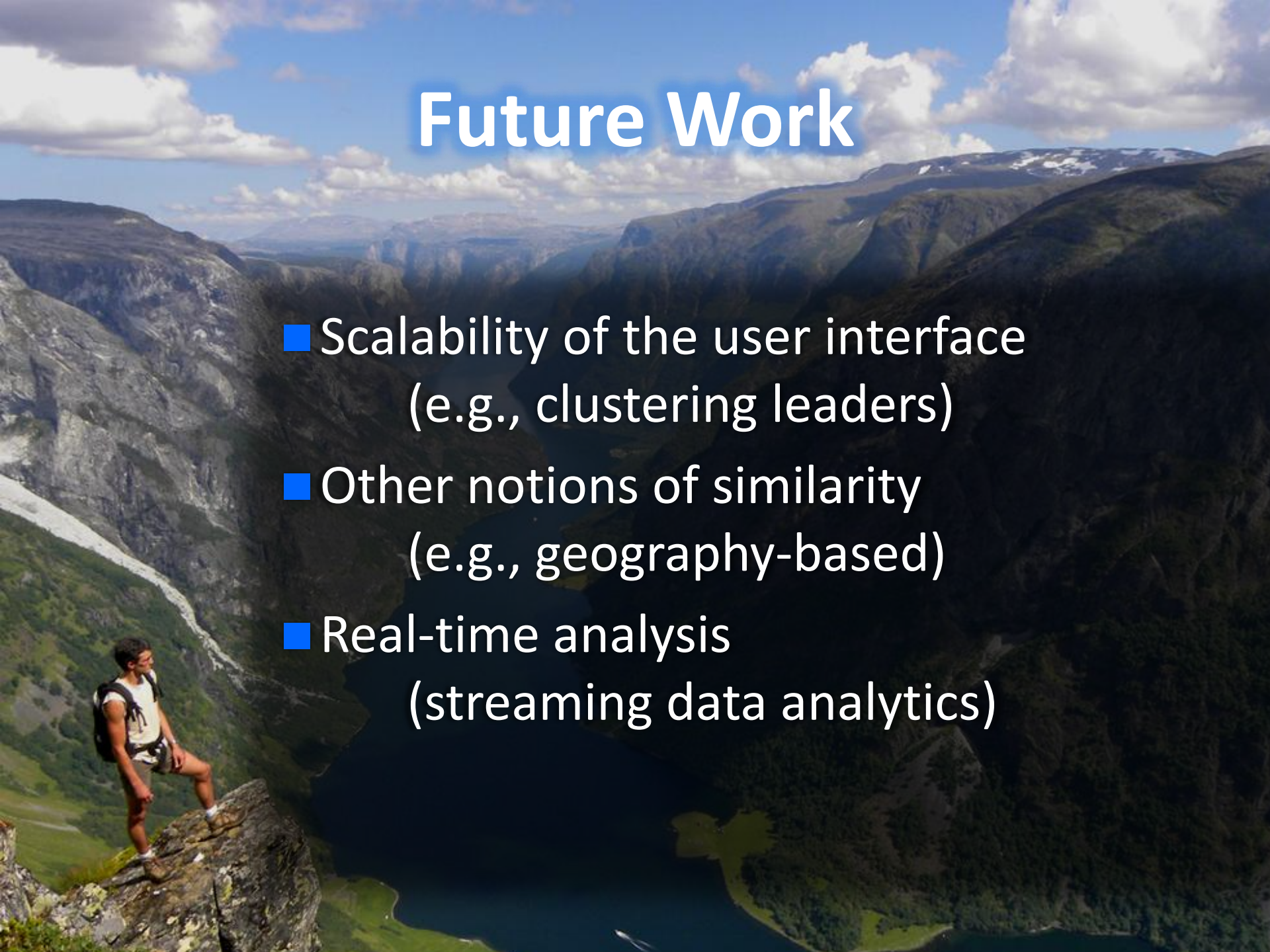
- Scalability of the user interface (e.g., clustering leaders)

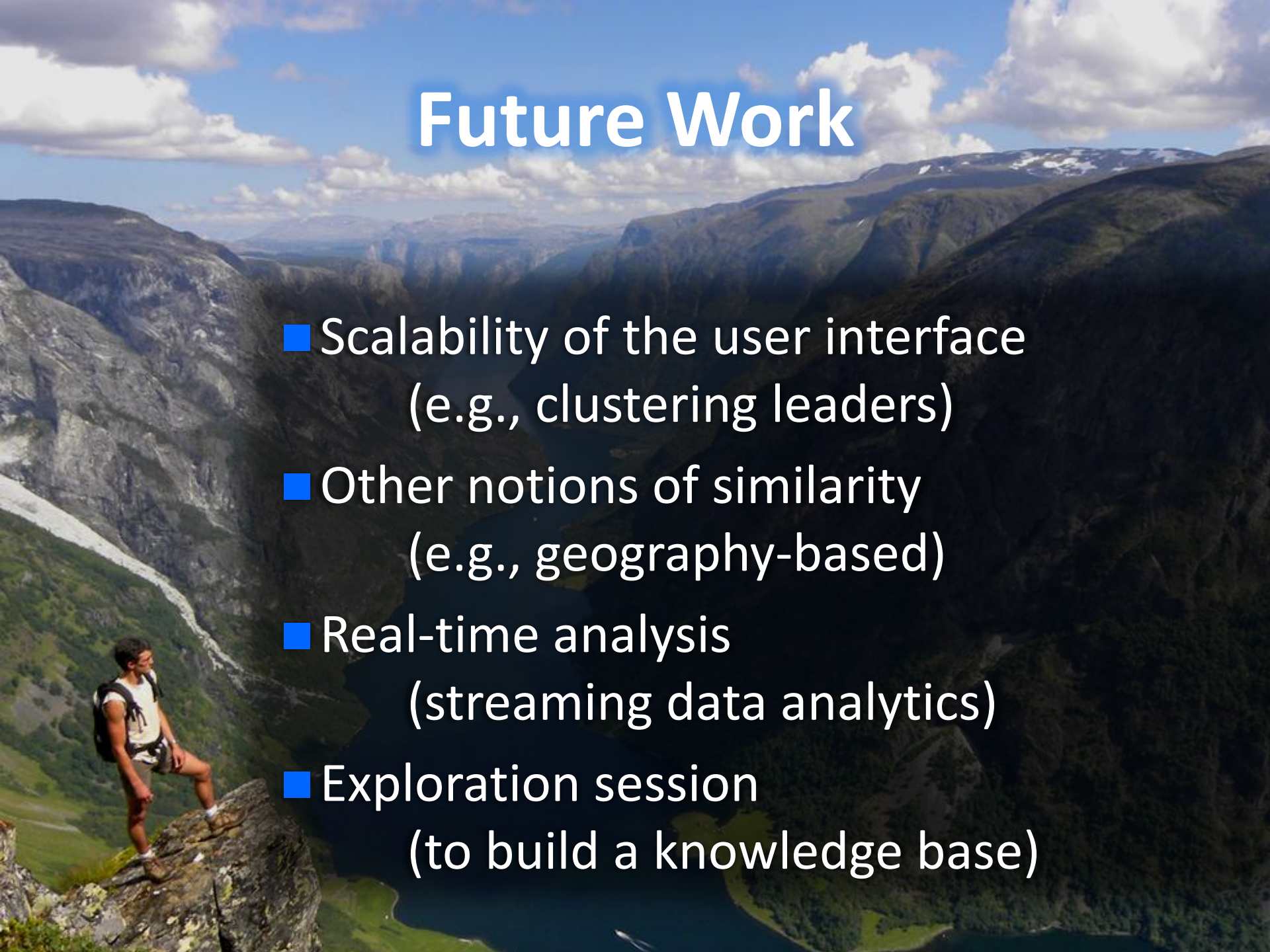
Future Work

- Scalability of the user interface (e.g., clustering leaders)
- Other notions of similarity (e.g., geography-based)

Future Work

- Scalability of the user interface
  (e.g., clustering leaders)
- Other notions of similarity
  (e.g., geography-based)
- Real-time analysis
  (streaming data analytics)





Future Work

- Scalability of the user interface
  (e.g., clustering leaders)
- Other notions of similarity
  (e.g., geography-based)
- Real-time analysis
  (streaming data analytics)
- Exploration session
  (to build a knowledge base)