Symposium on Visualization for Cyber Security (VizSec 2012)
15th October 2012, Seattle, WA, USA

Universität Konstanz

BGP Event Visualizer

VisTracer: A Visual Analytics Tool to Investigate Routing Anomalies in Traceroutes

Fabian Fischer[1], J. Fuchs[1], P.-A. Vervier[2], F. Mansmann[1], O. Thonnard[3]

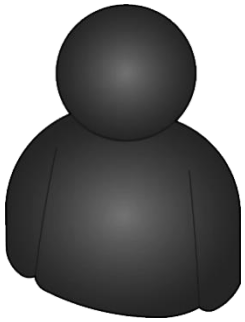
[1] University of Konstanz, Germany
[2] Institut Eurecom, France
[3] Symantec Research Labs, France

VIS-SENSE
www.vis-sense.eu

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257495.

Imagine YOU were a spammer…

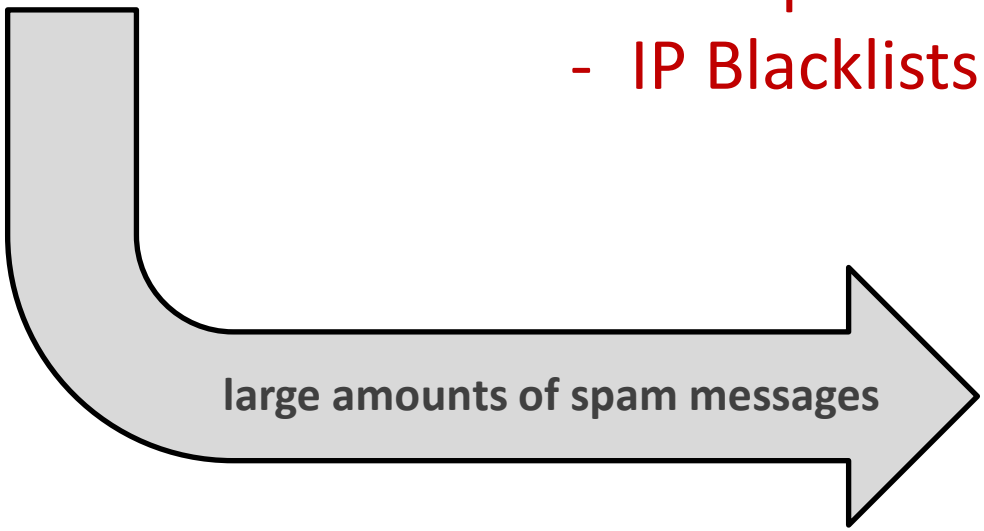
and you want to send large amounts of spam.



YOU

Problem:

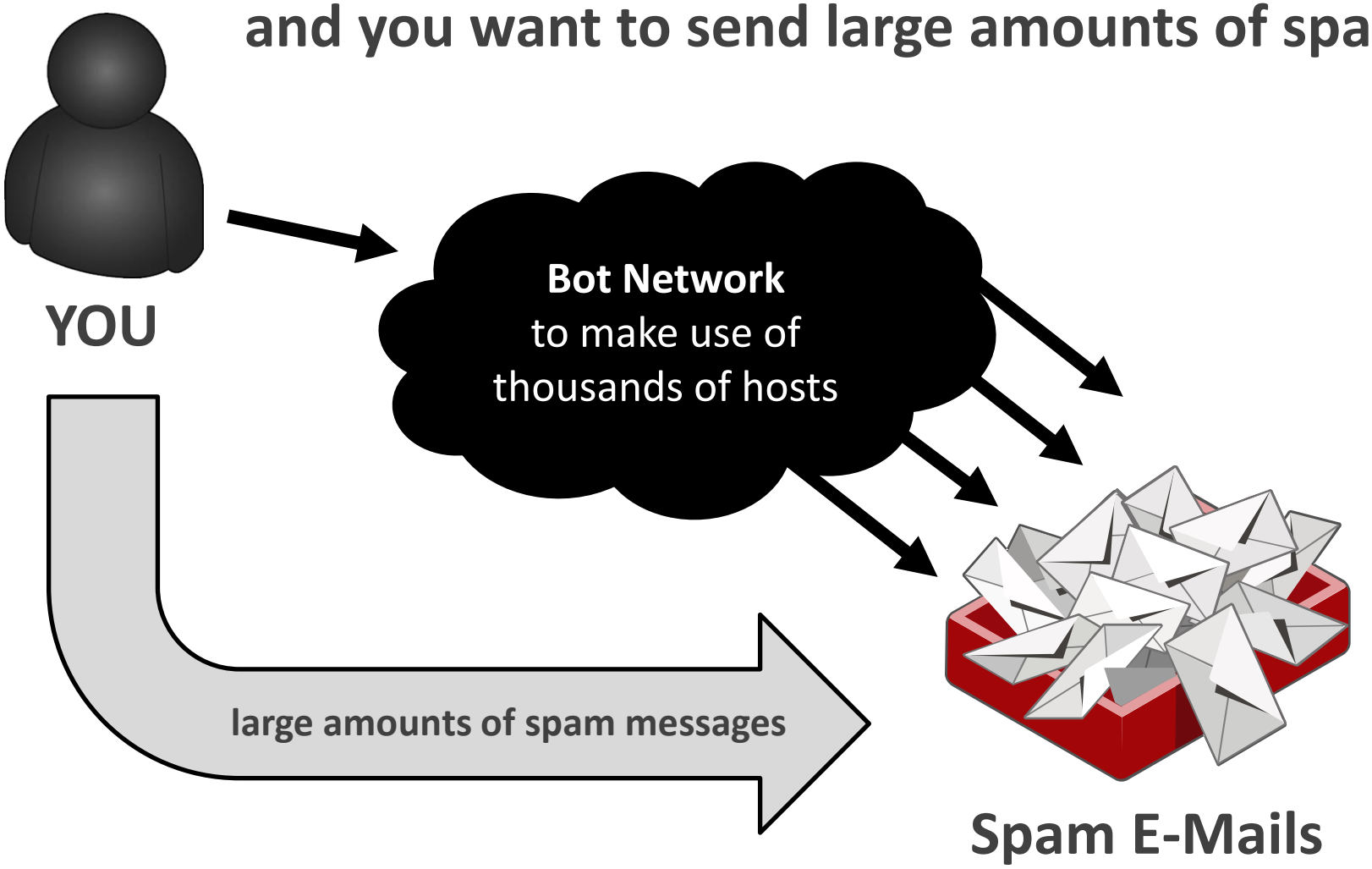
- Spam Filtering
- IP Reputation
- IP Blacklists



Spam E-Mails

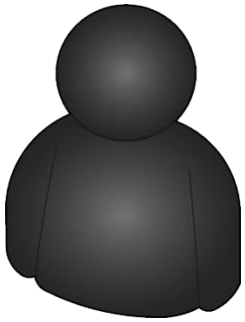
Imagine YOU were a spammer…

and you want to send large amounts of spam.



Imagine YOU were a spammer…

and you want to send large amounts of spam.



YOU

But why not:

Steal someone's else IP space using BGP Hijacking?

A. Ramachandran and N. Feamster (2006).
Understanding the network-level behavior of spammers.
In SIGCOMM '06: Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications, pages 291– 302, New York, NY, USA, 2006. ACM.

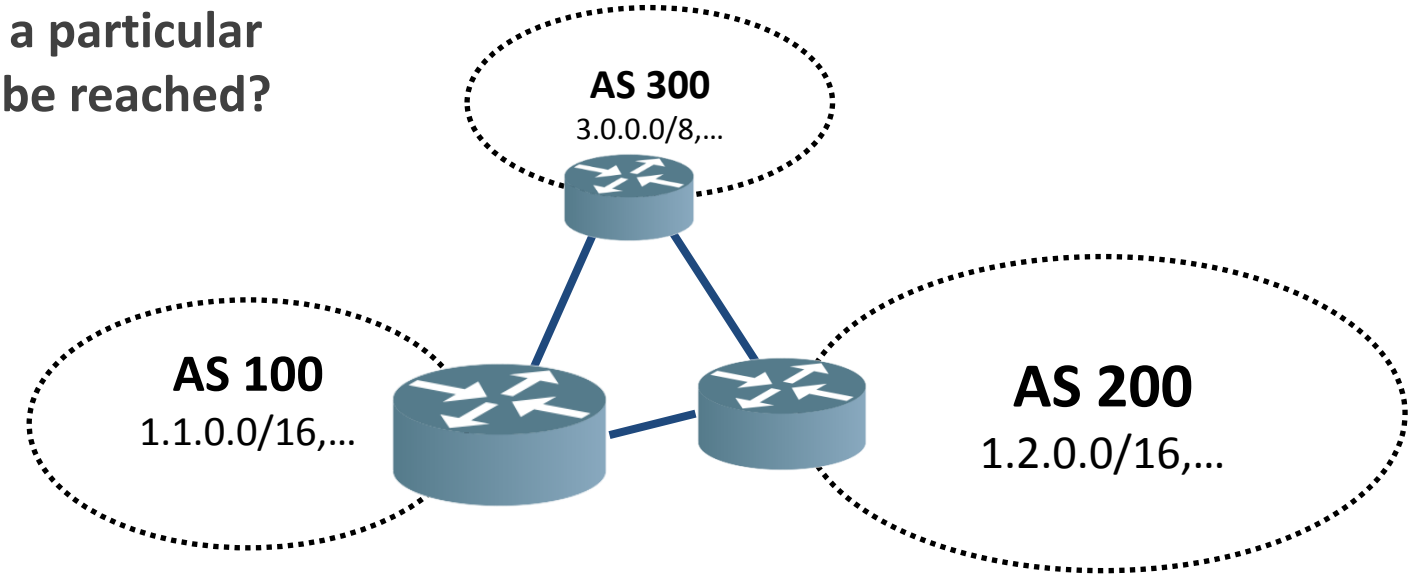
large amounts of spam messages

Spam E-Mails

Border Gateway Protocol – BGP is insecure…

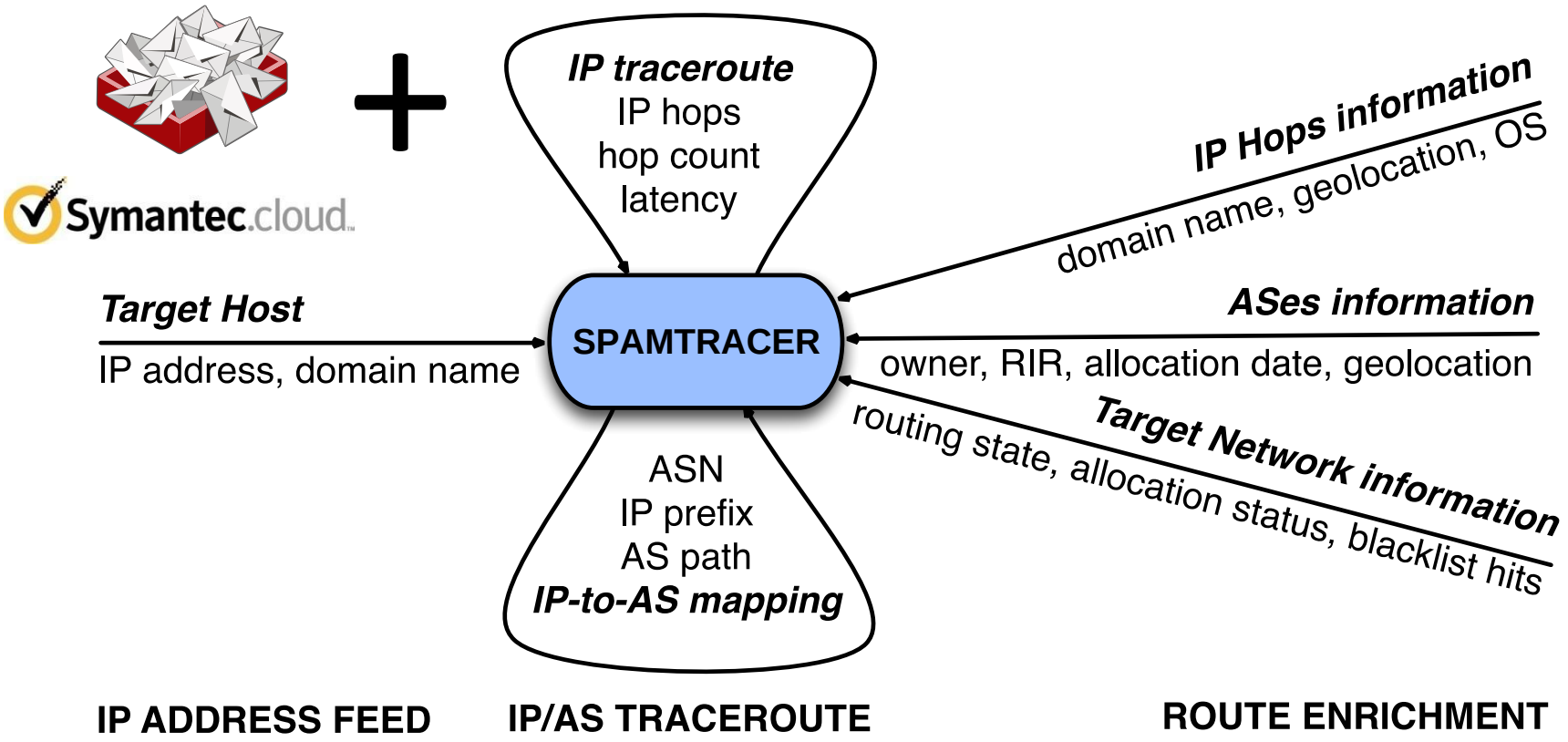
BGP is responsible for routing in the Internet.

How can a particular IP prefix be reached?



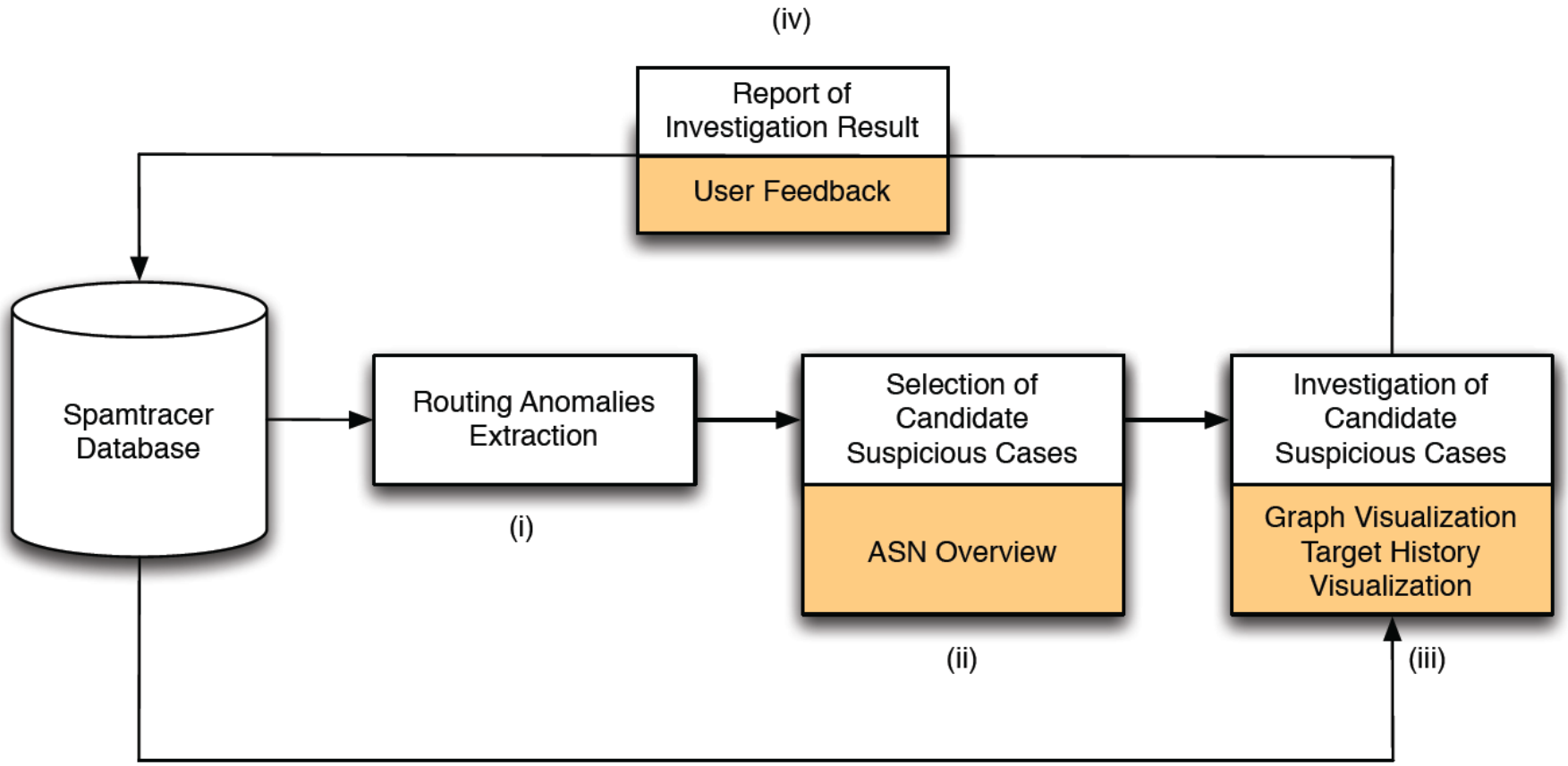
VisTracer: Helps the analyst to explore malicious activities (e.g., Spam) with respect to routing changes based on traceroutes.

Data Collection of Spamtracer



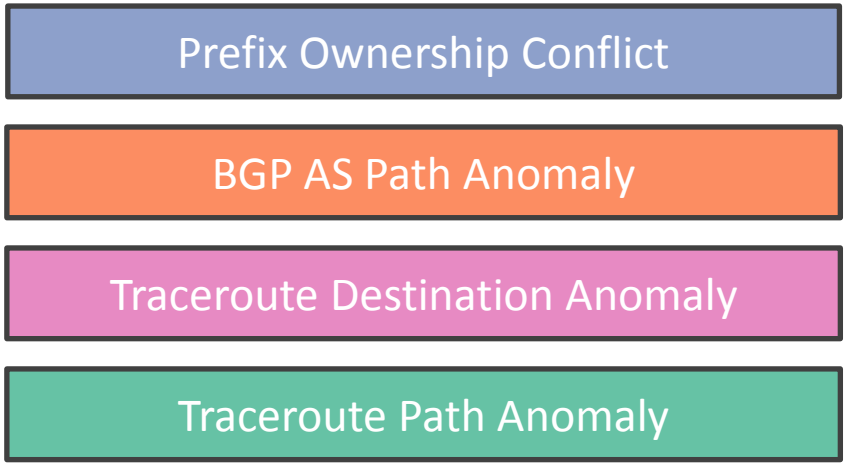
P.-A. Vervier and O. Thonnard (2012).
Spamtracer: Using Traceroute To Track Fly-By Spammers.
Submitted to the 8th International Conference on emerging Networking EXperiments and Technologies Student Workshop, December 2012.

Visual Analytics Workflow – Overview



Extraction of Routing Anomalies

- Extraction of ***routing anomalies*** based on known BGP hijack scenarios



Defined Routing Anomalies

Prefix Ownership Conflict

Possible Reason:
Advertising someone else's IP space

Possibilities:
Same prefix (→ MOAS)
Slightly different prefix (→ subMOAS)

BGP AS Path Anomaly

Possible Reason:
Changed location in Internet topology

Possibilities:
Different next hop AS
Sequence change in complete AS path

Traceroute Destination Anomaly

Possible Reason:
Suspicious values in trace metadata

Possibilities:
Host/AS reachability changed
Traceroute hop count changed

Traceroute Path Anomaly

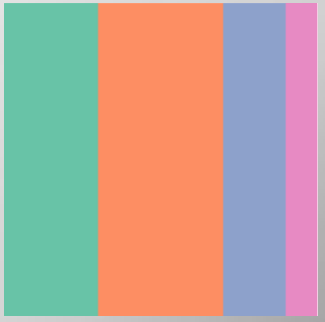
Possible Reason:
Significant change in the traceroute

Possibilities:
AS sequence changed
Country sequence changed

Used Glyph Representations

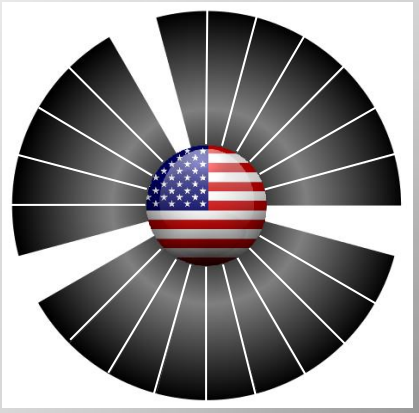
Design Decisions for Glyph Representations

Anomaly Glyph



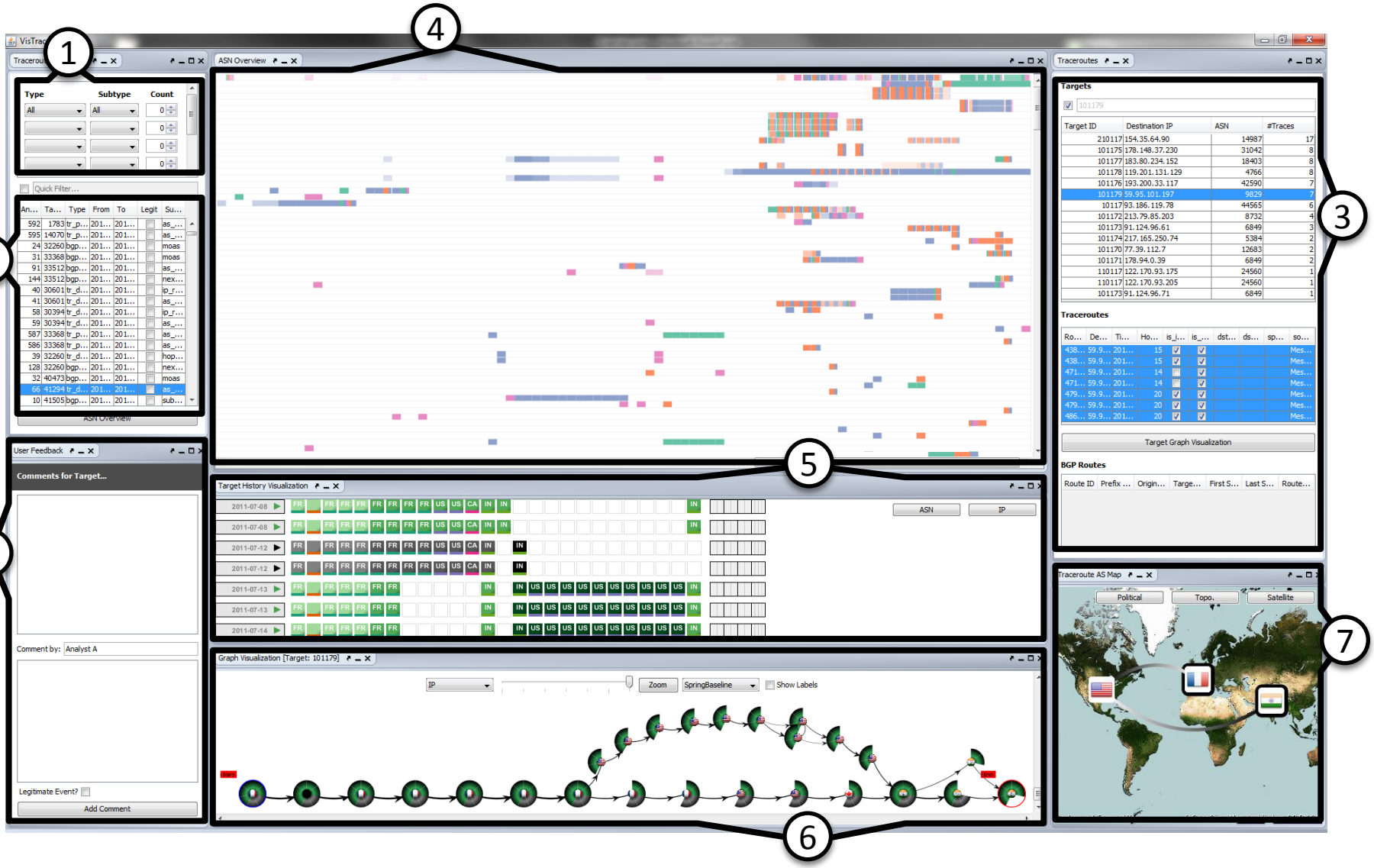
Hop Glyph

Clock Glyph



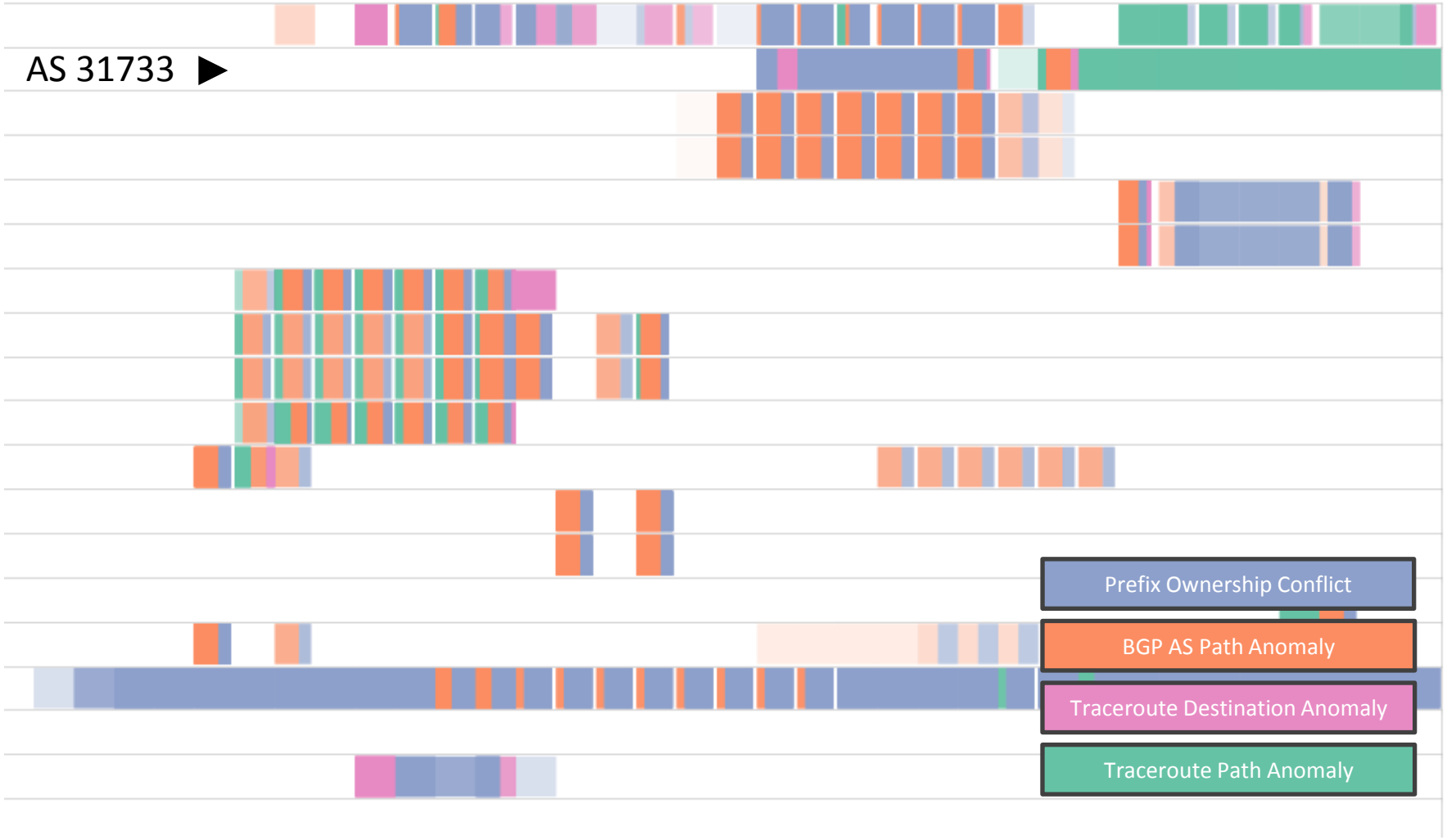
- Using glyphs as compact representations for different visualization types.

Graphical User Interface of VisTracer



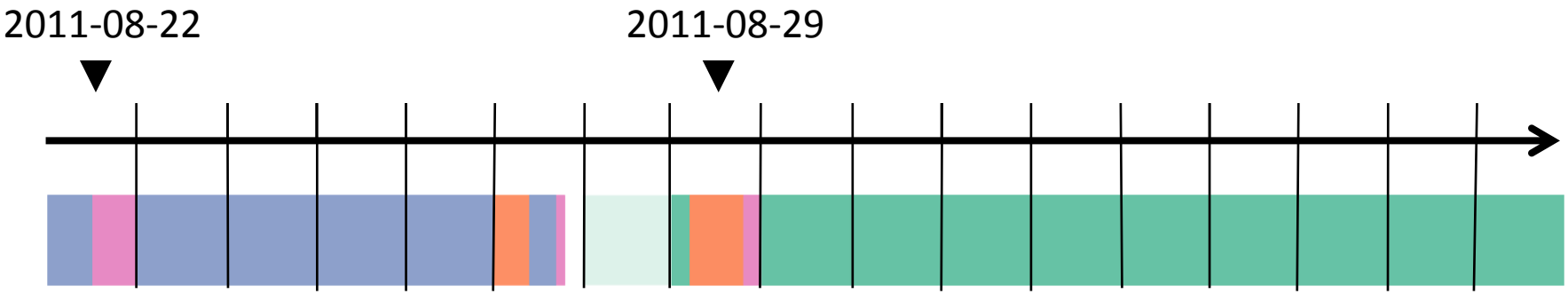
Pixel-Based ASN Overview Matrix

Identifying General Patterns and Combinations

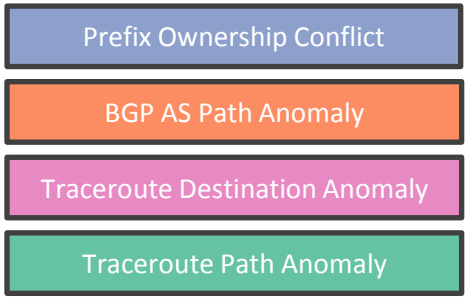


Pixel-Based ASN Overview Matrix

Interesting Anomalies for AS 31733

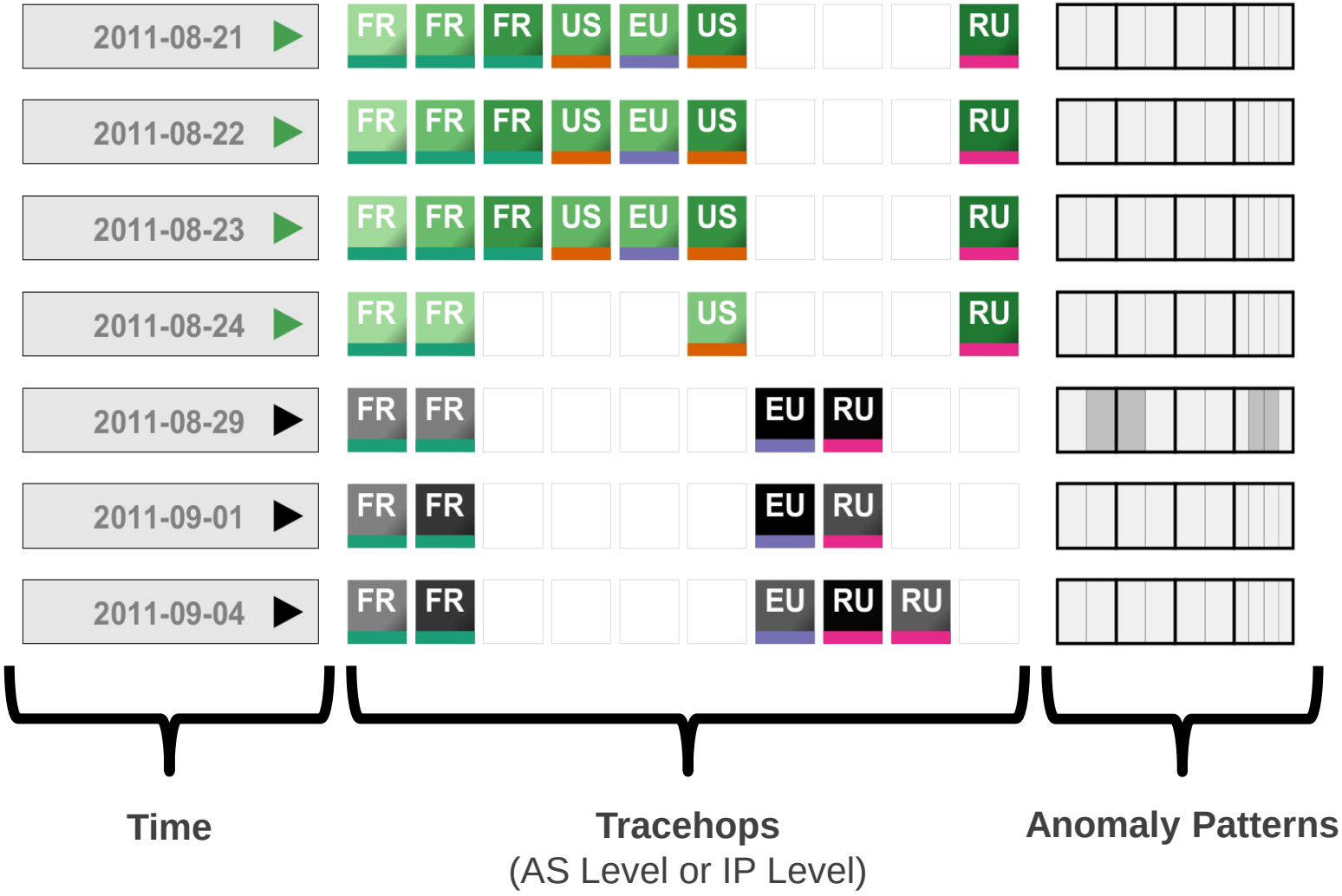


- Many diverse routing anomalies occurred within a limited period of time.
- Several anomalies occurred on same day



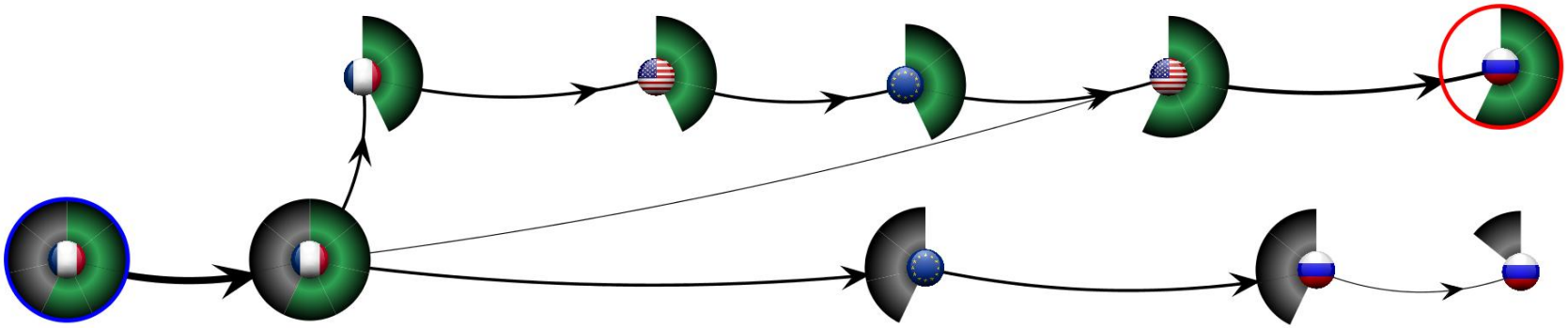
Glyph-Based Target History Visualization

Compact Traceroute History



Graph-Based Visualization

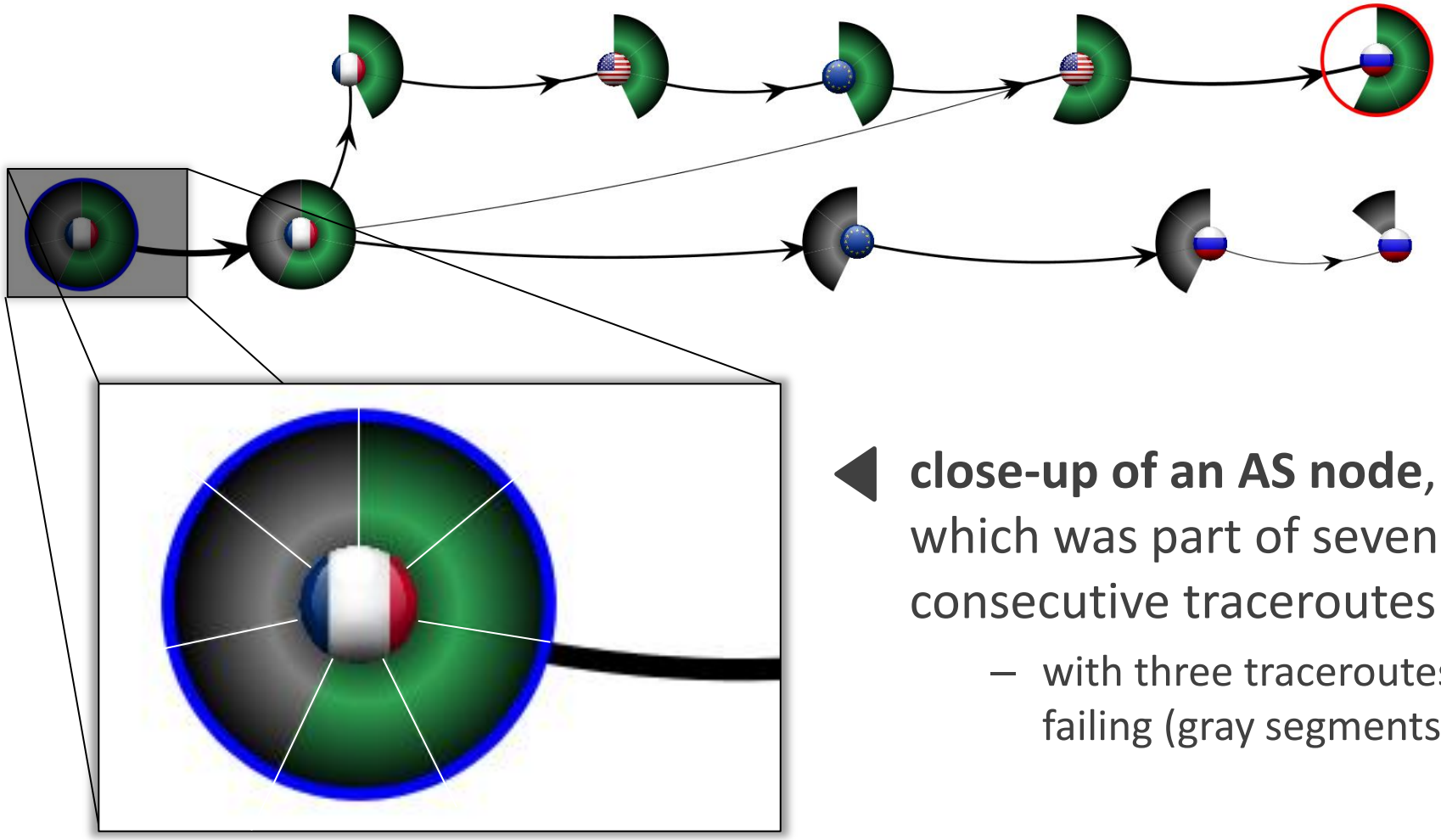
Usage of Clock Glyph to encode temporal information



- Graph showing the sequence of traceroutes
- Nodes represent IPs / ASes / Countries
- Temporal information as Clock Glyph
- Different Layouts

Graph-Based Visualization

Usage of Clock Glyph to encode temporal information



- **close-up of an AS node**, which was part of seven consecutive traceroutes
  - with three traceroutes failing (gray segments)

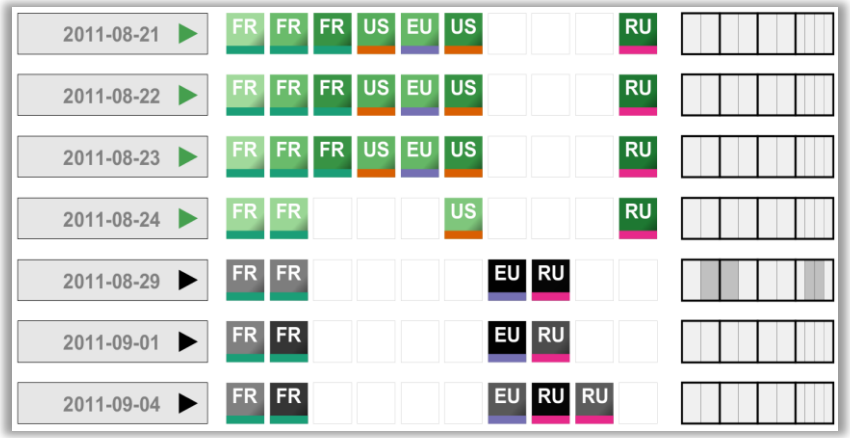
Malicious BGP Hijack

Visual Exploration with VisTracer

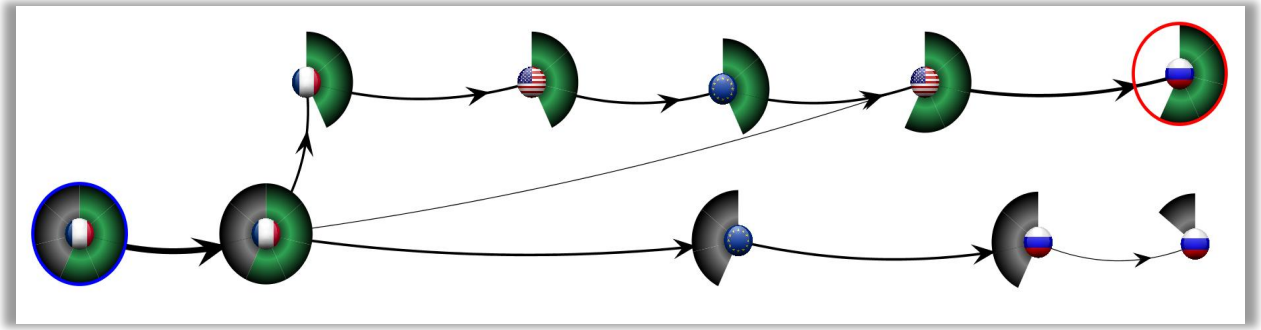
More information about this case:

Symantec Internet Security Threat Report (April 2012).
Future Spam Trends: BGP Hijacking. Case Study - Beware of "Fly-by Spammers".
http://www.symantec.com/threatreport/, April 2012.

- **Link Telecom BGP Hijack**
  - Spammer stole IP address space
- **The network administrator complained on 2011-08-20.**
  - Observed changes were the result of the owner regaining control over his network.



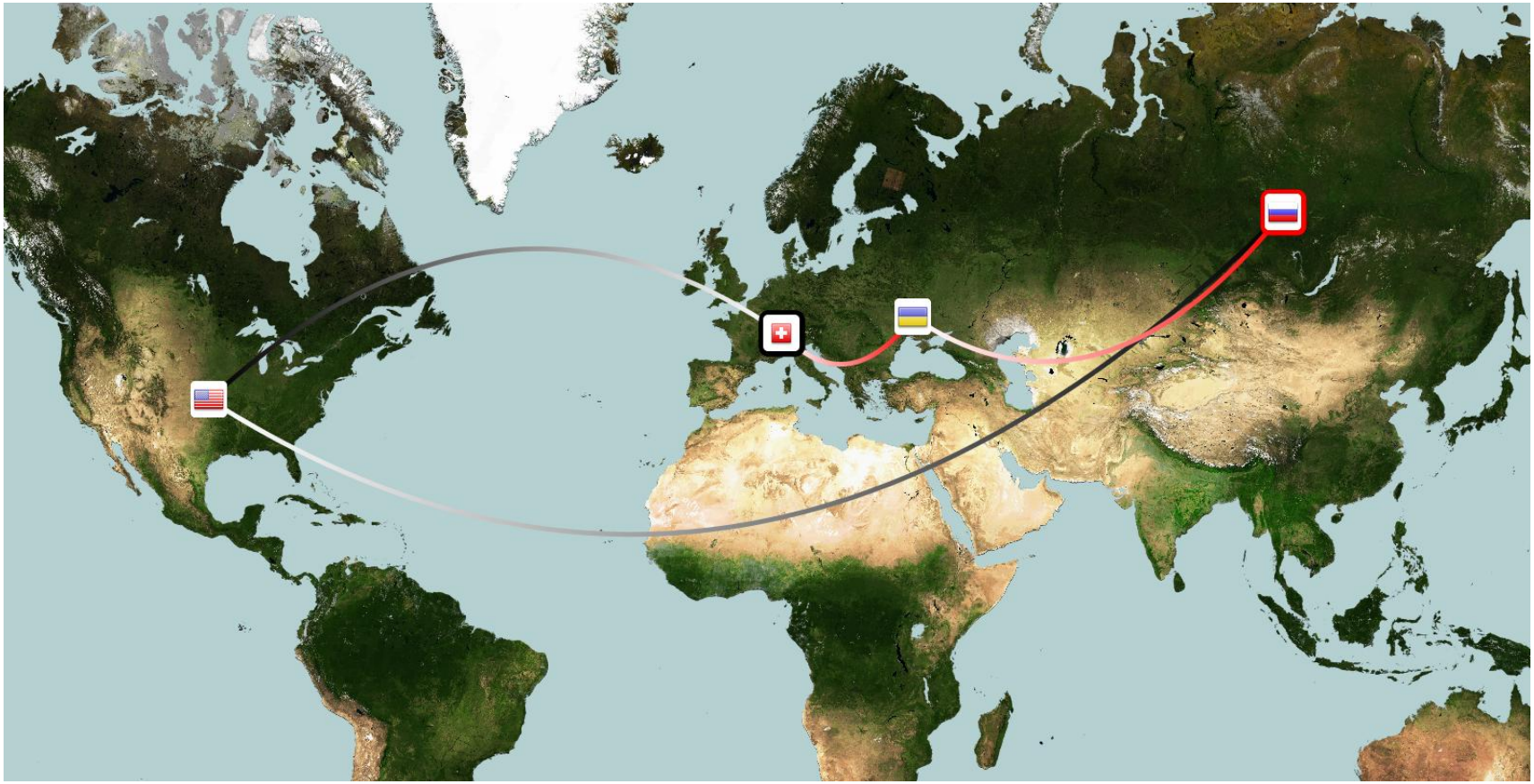
Target History Visualization shows the different traceroutes revealing the anomalies and route changes.



Graph Visualization shows the sequence of ASes traversed.

Map-Based Geographic Representation

Link Telecom BGP Hijack (April to August 2011)



Future Work

- Improve the usability of the expert tool.
- Integrate additional views,
  based on analysts' feedback.
- Layout improvements for the graph layout
  (reduce clutter).
- Alternative sorting algorithms
  for overview visualization.

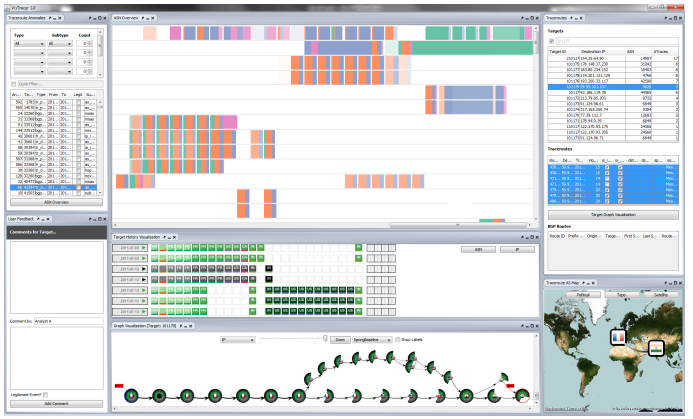
Contributions

i. A visual analytics tool to analyze traceroutes.

ii. Integration into our large-scale automatic analysis system for traceroutes (*Spamtracer*).

iii. Pixel-, glyph- and graph-based visualizations for traceroutes.

Thank you very much for your attention!



Questions?

For more information
about this work please contact

Fabian Fischer
Tel. +49 7531 88-2780
Fabian.Fischer@uni-konstanz.de

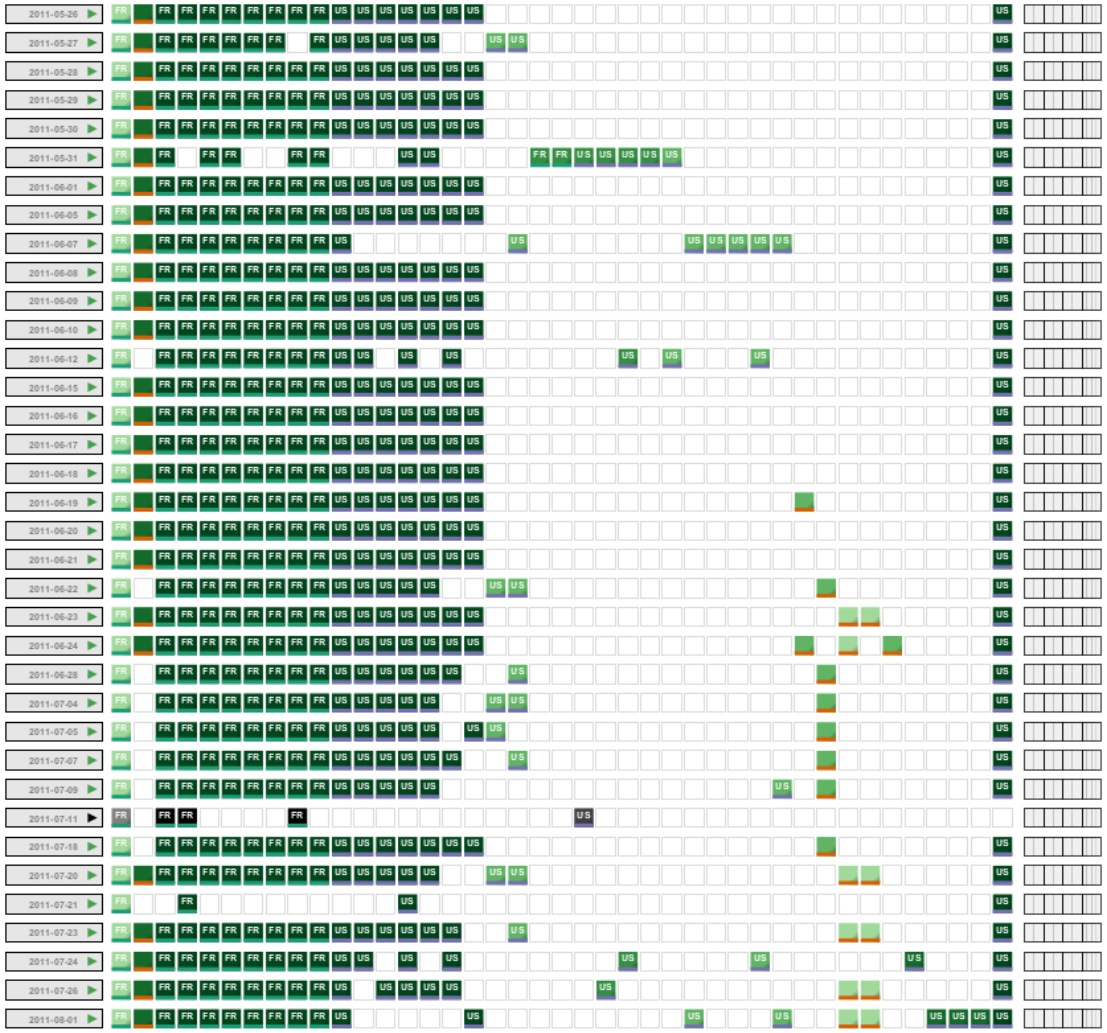
twitter
@f2cx

http://www.vis-sense.eu/

VIS-SENSE
www.vis-sense.eu

The research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 257495.

Glyph-Based Target History Visualization



Dataset 1: April until end of August 2011

- **Collected Data:**
  - **848 916** data plane routes collected
  - towards **239 907** IP addresses and **5 912** ASes

- **After extracting routing anomalies:**
  - **41 430** destination IP addresses
    - with at least one anomaly.