RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg
Security and Networks Research Group

High level Internet level traffic visualization using Hilbert curve mapping

Barry Irwin & Nick Pilkington

Security and Networks Research Group
Department of Computer Science
Rhodes University

VizSEC '07 Presentation - October 29th, 2007

Sponsored by

Telkom COMVERSE Business Connexion THRIP STORTECH tellabs VERSO TECHNOLOGIES amatole

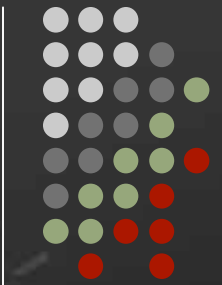
RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

Overview



- The Hilbert Curve
- Mapping IP address space to Curve space
- Using the Curve
- Conclusion and questions

RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

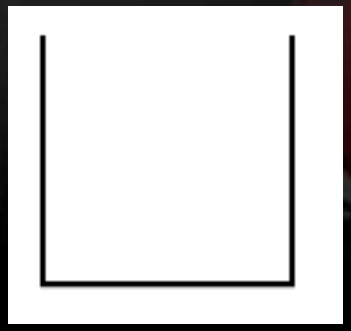
snrg

Security and Networks Research Group

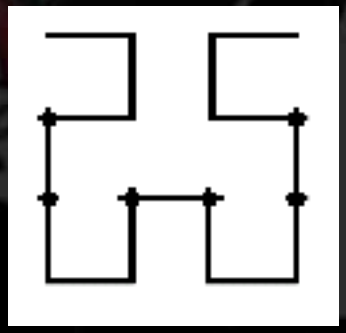
The Hilbert Curve

- Documented by David Hilbert in 1891
- Part of the larger family of Peano curves
- Used to extrapolate data from one dimension into two dimensions
- Maintains properties of the original one dimensional data
- Particularly the notion of ordering and closeness to sequential nodes within the sequence

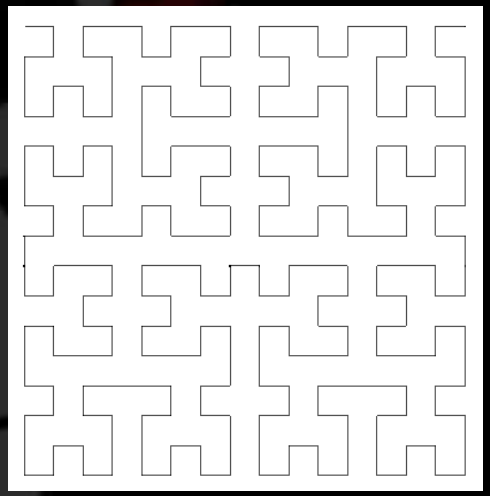
$$
\begin{aligned}
&Alphabet: L, R\\
&Constants: F, +, -\\
&Axiom: L\\
&Production\ rules:\\
&L \rightarrow +RF - LFL - FR +\\
&R \rightarrow -LF + RFR + FL -
\end{aligned}
$$



1st Order



2nd Order



4th Order

RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

Curve Mapping

- Hilbert curves of order 4, 8, 12, and 16 are especially interesting
- Curves have 256 (2^8) , 65536 (2^{16}), 16,777,216 (2^{24}) and 4,294,967,296 (2^{32}) points respectively.
- These values correspond to the natural grouping of Internet networks blocks by Class A (/8), class B (/16), and class C (/24)
- A 16^{th} order curve provides the same number of points as 2^{32} which is the same as the total potential number of addressable nodes on the IP protocol version 4 (IPv4) Internet.
- Curves of orders 8 and 12 have shown to be the most useful, and provide a balance between detail and computational effort

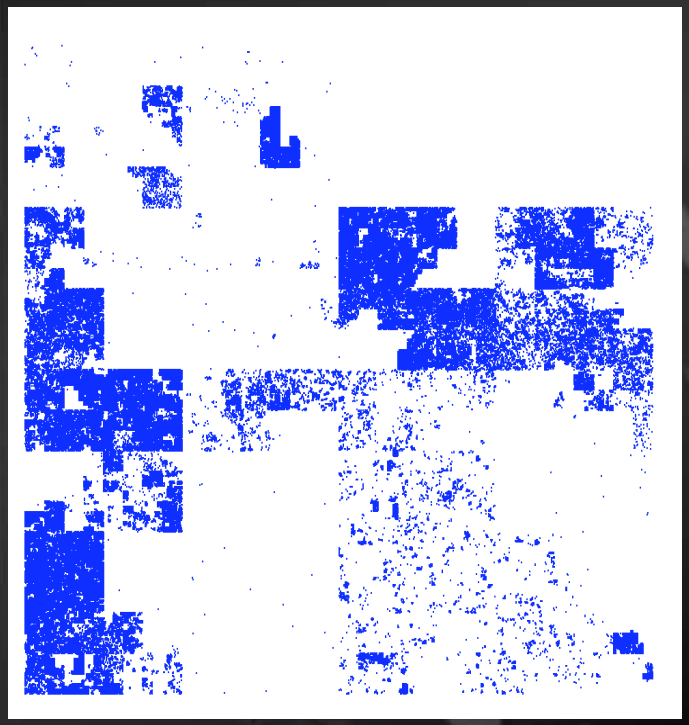
RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

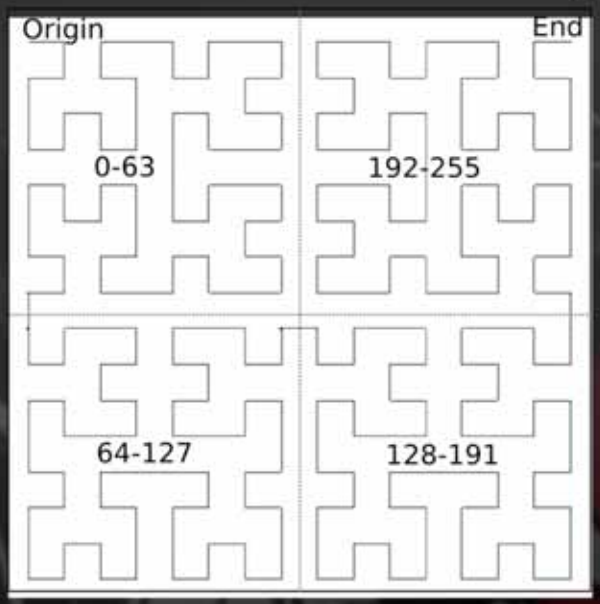
snrg

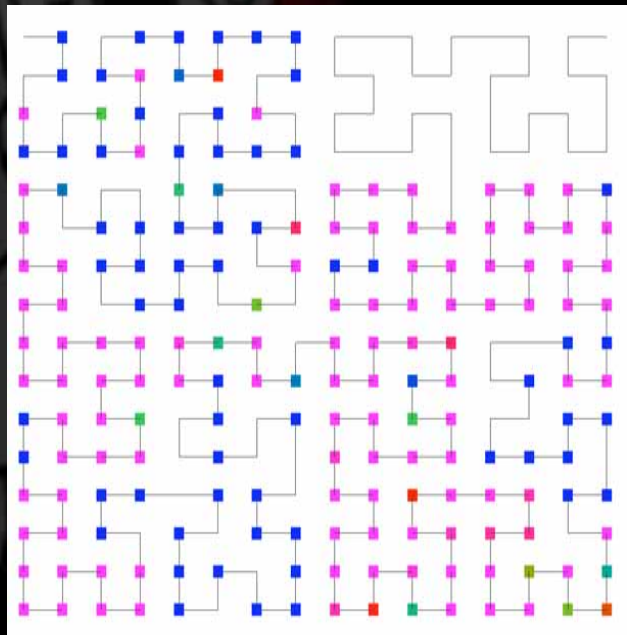
Security and Networks Research Group

Hilbert Curve Packing



12th order curve showing IP clustering by /24 network





4th order curve showing IP clustering by /8 network with colour mapping

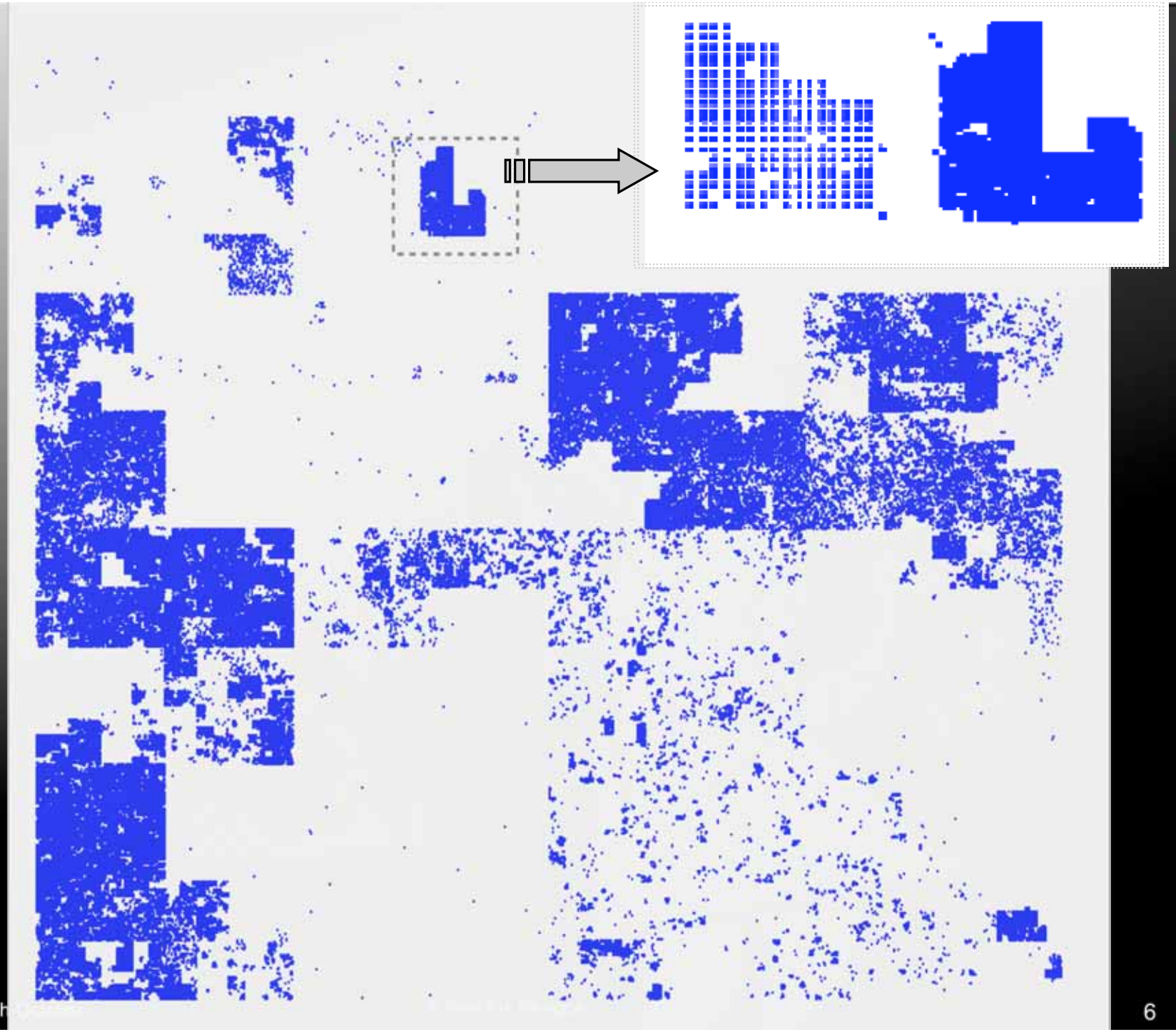
B. Irwin & N. Pilkington

RHODES UNIVERSITY

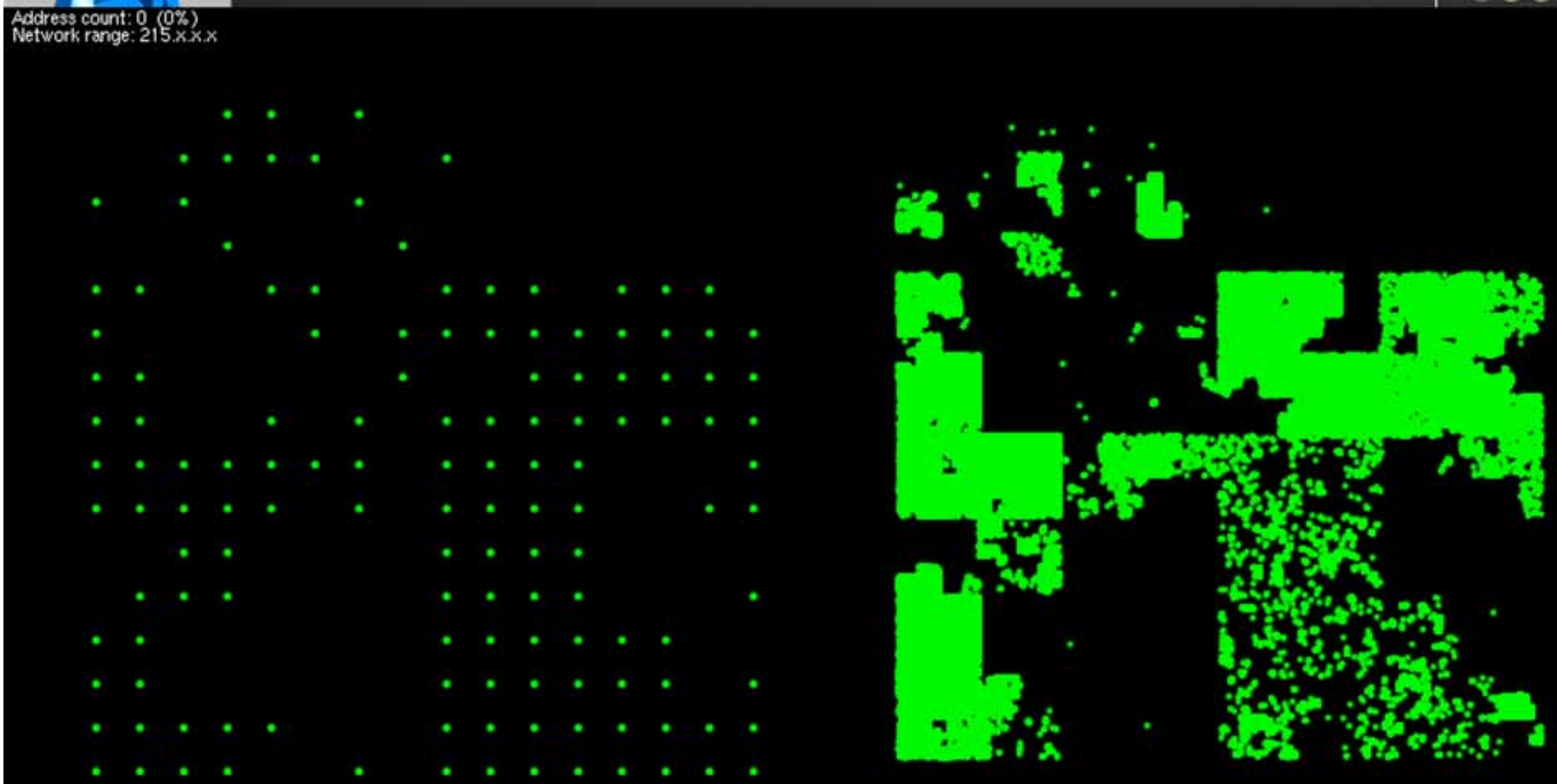
Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group



Network Telescope Traffic



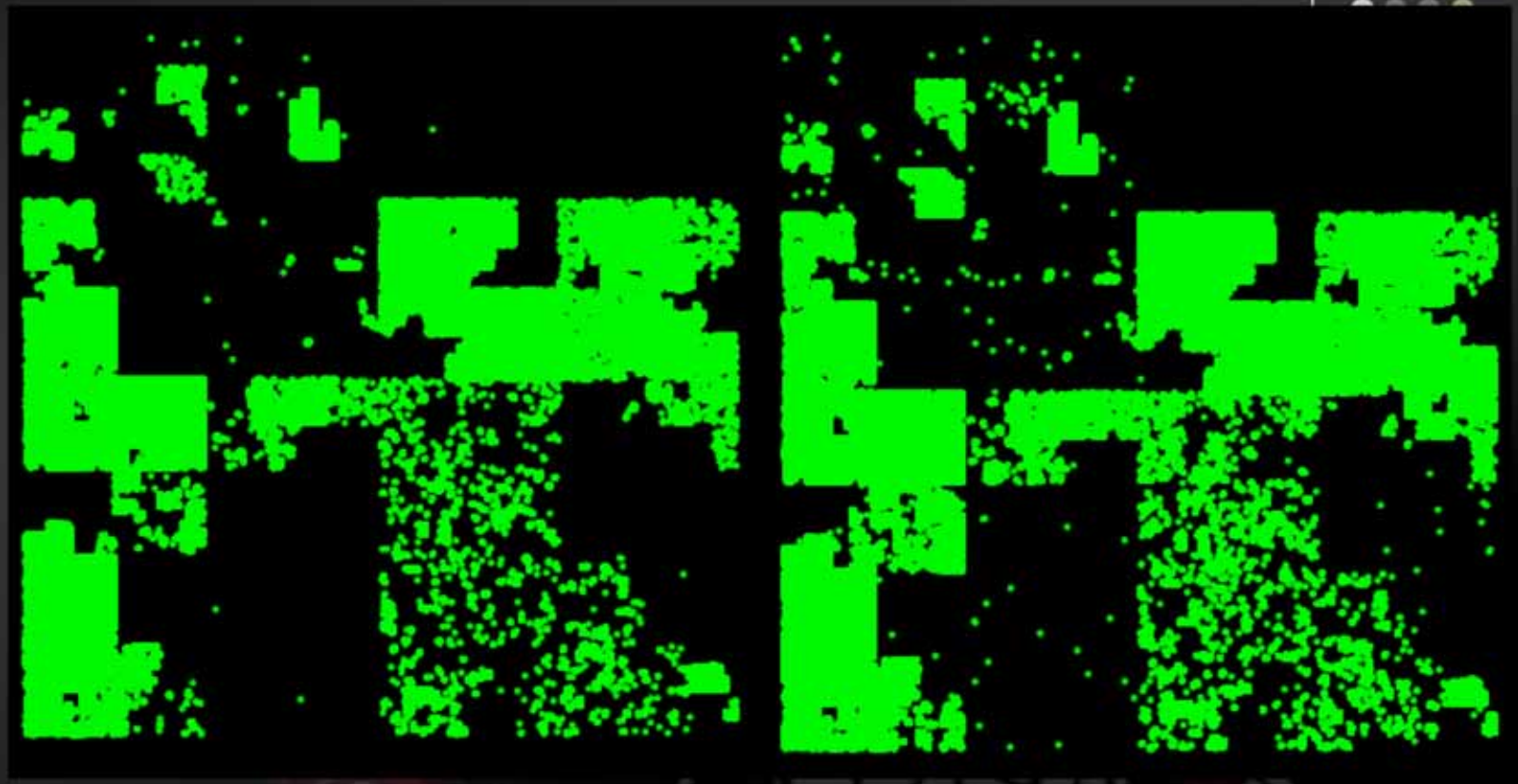
- /8 and /24 bins mapping to 4th and 12th order curves

RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

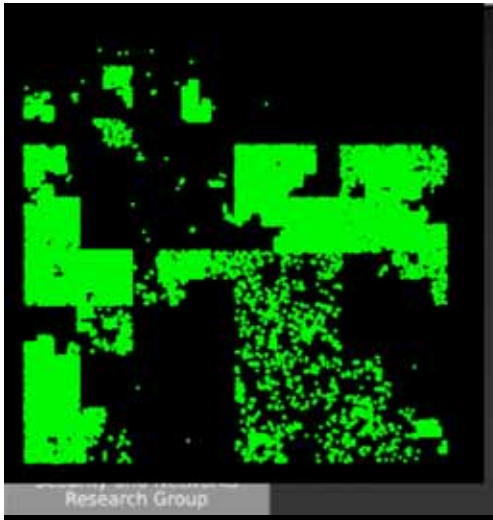
Security and Networks Research Group



- Rhodes /24 Telescope
- Aug 2005-June2007
- 13 Million events

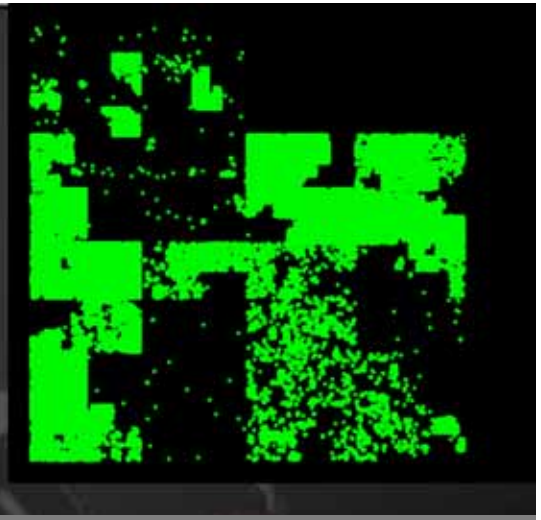
- CAIDA /8 Telescope 12h00-16h00 22 Feb 2007
- 59Million events

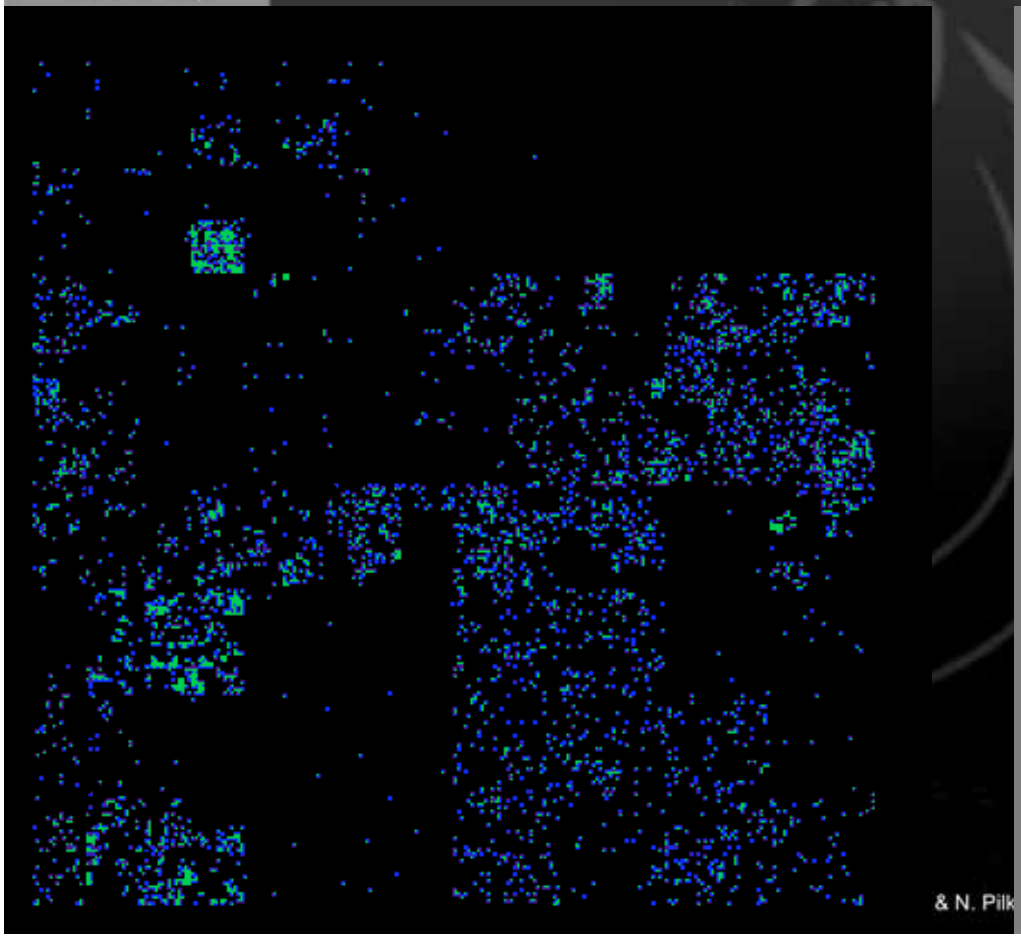
Telescope Comparison

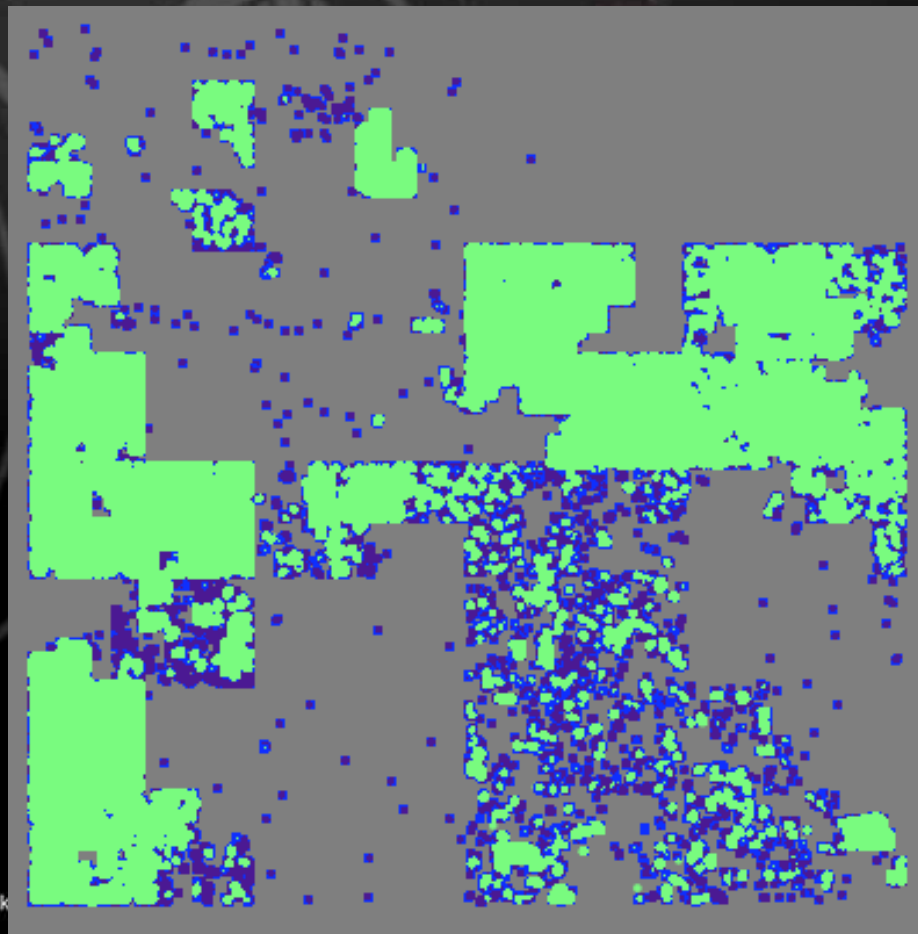


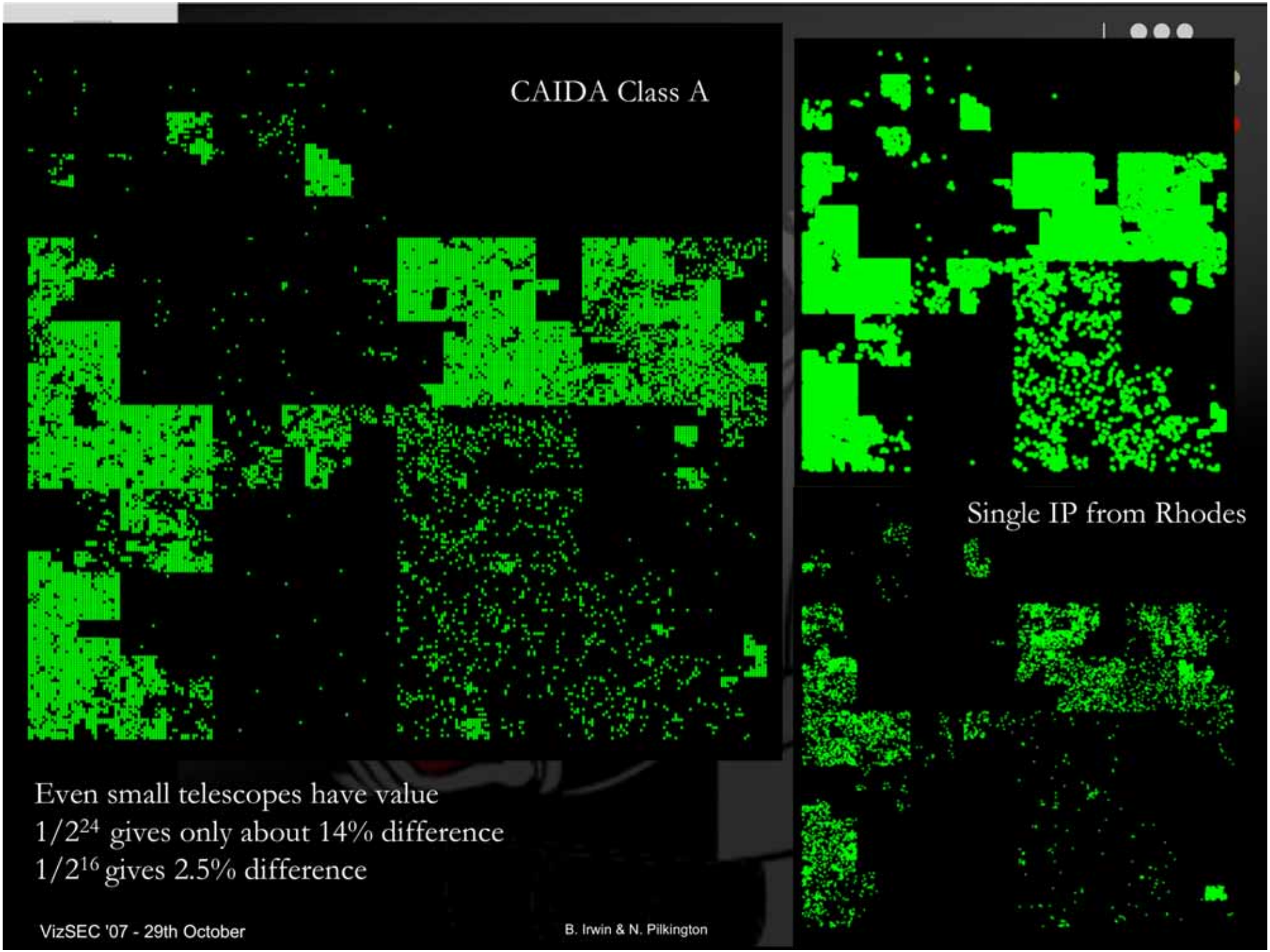
RU Telescope (/24)

CAIDA (/8)







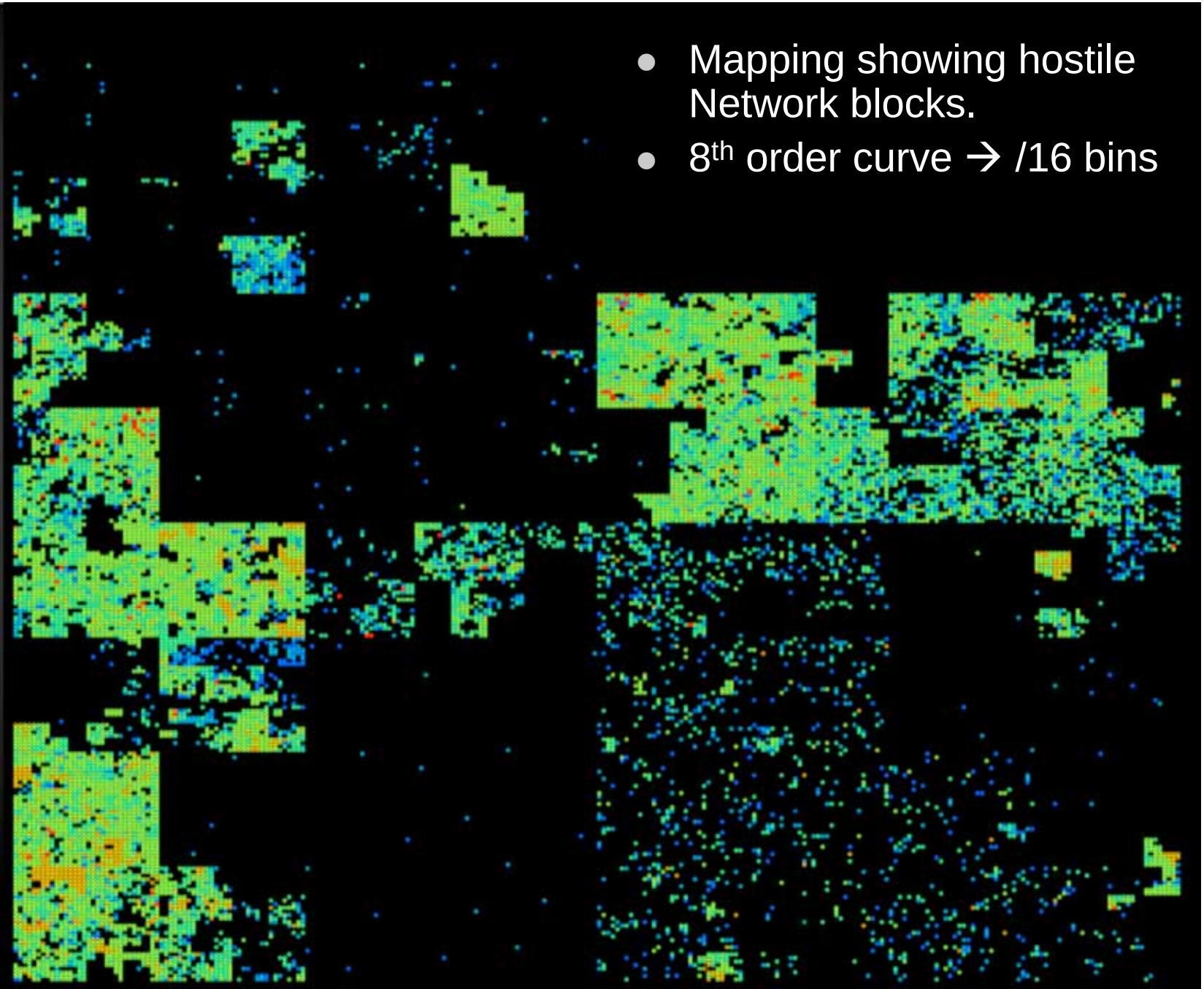

CAIDA Class A
Single IP from Rhodes
Even small telescopes have value
1/2^24 gives only about 14% difference
1/2^16 gives 2.5% difference
VizSEC '07 - 29th October
B. Irwin & N. Pilkington

RHODES UNIVERSITY

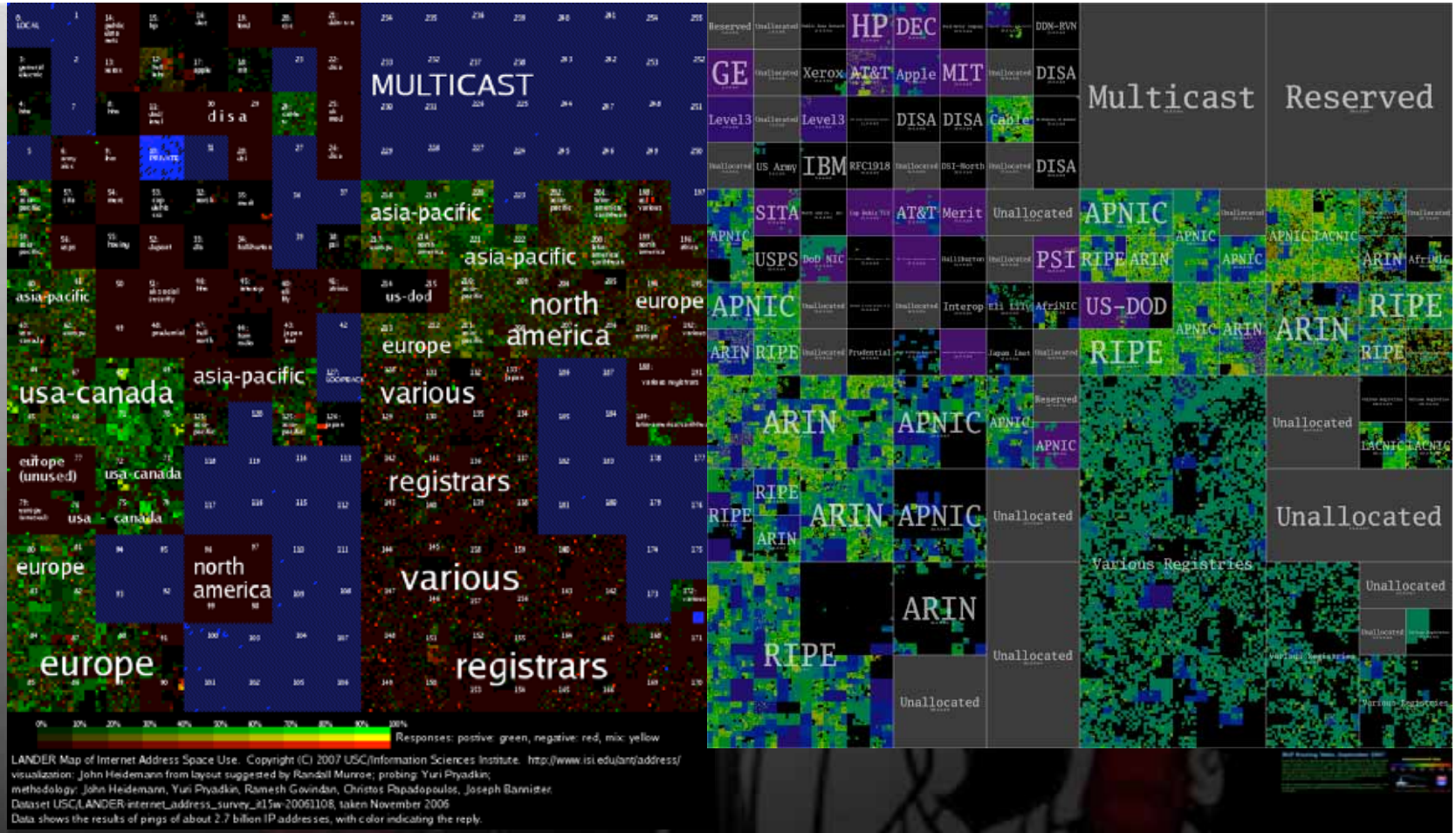
Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group



- Mapping showing hostile Network blocks.
- 8th order curve → /16 bins



http://www.isi.edu/ant/address/

http://maps.measurement-factory.com/gallery/Routeviews

- These other projects have been used for validating our implementation
- Should provide an interesting set of alternate implementations for user tests
- Examples of other types of data being plotted

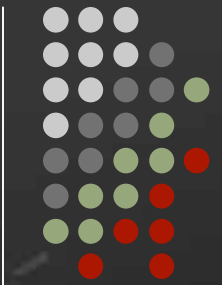
RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

Conclusion (and Future Work)



- Curves have proved very useful for providing rapid high-level overview of very large datasets
- Future work
  - Optimize implementation – possibly with GPUGPU implementation
  - Add more interactivity and shading options
  - Complete User Study

RHODES UNIVERSITY

Centre of Excellence in Distributed Multimedia

snrg

Security and Networks Research Group

Questions?

Barry Irwin

- b.irwin@ru.ac.za
- Project supervisor

Nick Pilkington

- nick@rucus.net
- BSc Hons Student