March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Finding Needles in Haystacks (the size of Countries)

michael@packetloop.com
@cloudjunky

david@packetloop.com
@dsturnbull

gerald@packetloop.com
@gakman

2011


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

We all know the story

The CEO thinks the network is...


VAULT DOOR
WEIGHT: 22 1/2 Tons
THICKNESS: 22 Inches
STEEL: 11 Layers of Special Cutting and Drill Resistant
LOCKS: 4 Hamilton Watch Movements for Time Locks

The Blackhats are...


www.rabittooth.com
black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Or is it?


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

This is you


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

I burnt the roof of my mouth

Some Consultants are..

And guaranteed you are going to be asked to...

Enhance!

Why is this funny?

Prevention Fails.

Detection is the key.

NSM - “Analysis and escalation of indications and warnings to detect and respond to intrusions”

- Richard Bejtlich

NSM - “focused on providing an intrusion analyst with the best possible information in the shortest amount of time” - NSMWiki

Network Security Monitoring

- Advocates focus on detection and that prevention will fail.
- Believes in inventoried and defensible networks.
- Build entropy from alert (attack) information.
- Provide analysts with the accurate information and context as fast as possible.
- Products provide collection, People the analysis

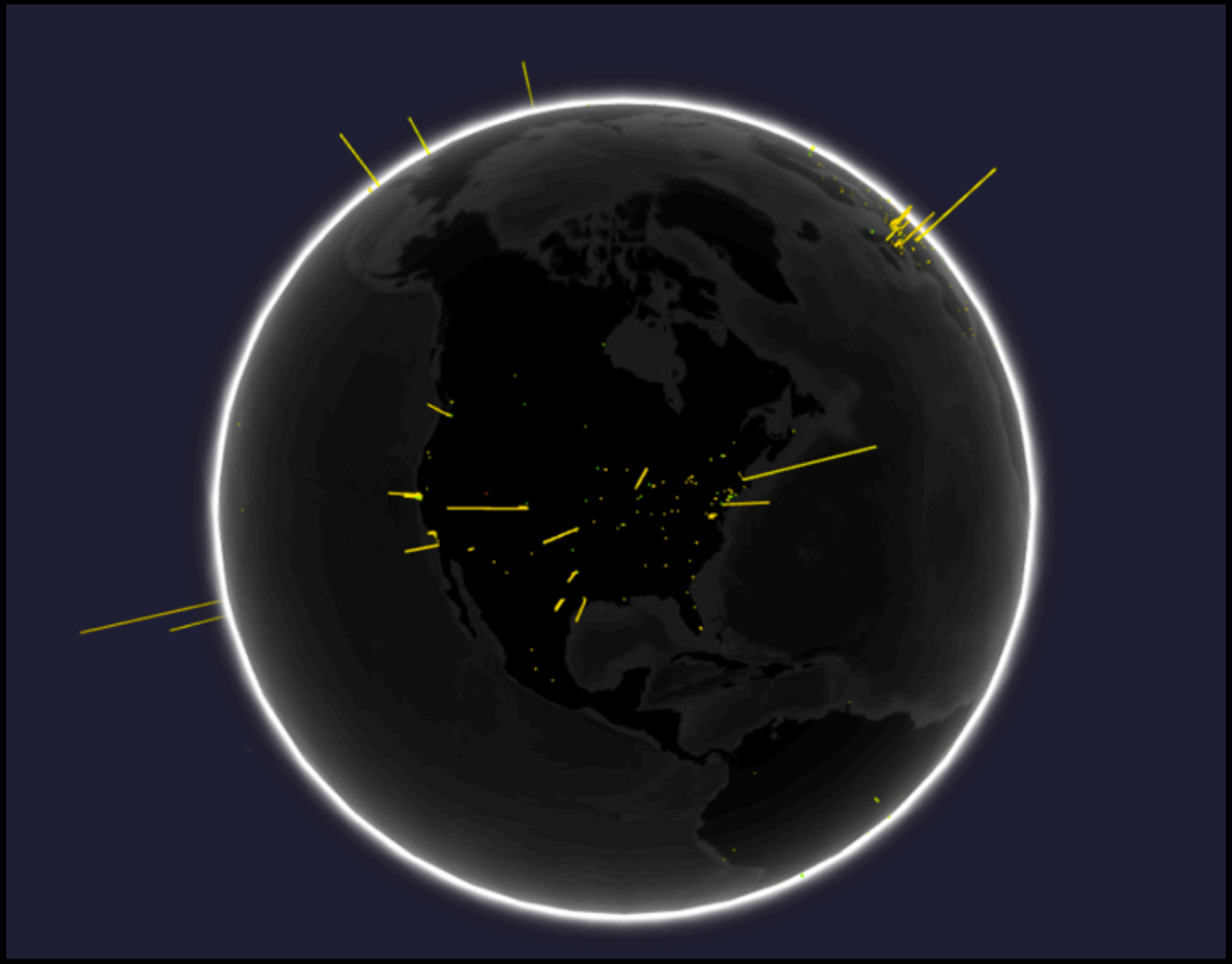
Network Security Monitoring

- Examples of NSM Tools
  - Sguil
  - Argus
  - Flowgrep
  - Snort
  - Bro
  - Network Miner
- Tools -> Collection, Humans -> Analysis

It's all about context.

Context

- Going back to the well.
- Providing as much context as possible in relation to attacks and attackers.
- Security analysis is detective work.
- Able to ask What if? Branch our analysis. React to new information.
- Providing full fidelity and full context quickly.



That's no moon.

- Pretty WebGL globe by Google.
- Each line represents a source IP address of an attacker.
- Height is frequency and Colour is Severity
- The destination (victim) is located in Sydney Australia.
- Approximately 60K Snort alerts in a 10 day period.

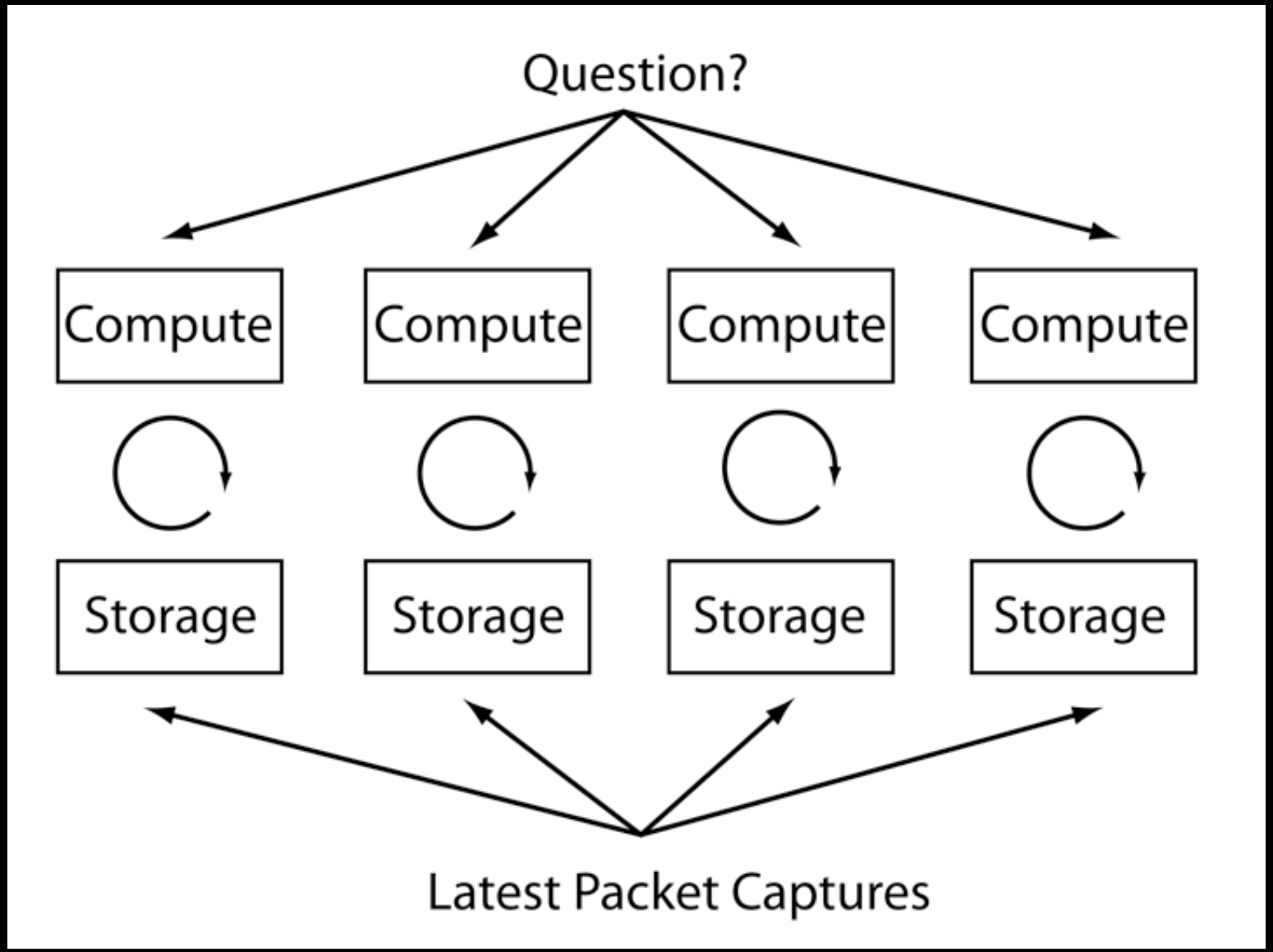
Full Packet Capture

- Complete record of all network transactions.
- If the attack takes place across a network it is in the packet captures.
- Provides the highest fidelity to analysts.
- Only way to really understand subtle and targeted attacks.
- Played, Paused, Stop, Rewind using NSM tools.
- No need to have specific logging setup.

NSM + FPC =
> % OPTIONS

"The difficulty shifts from traffic collection to traffic analysis. If you can store hundreds of gigabytes of traffic per day, how do you make sense of it?"

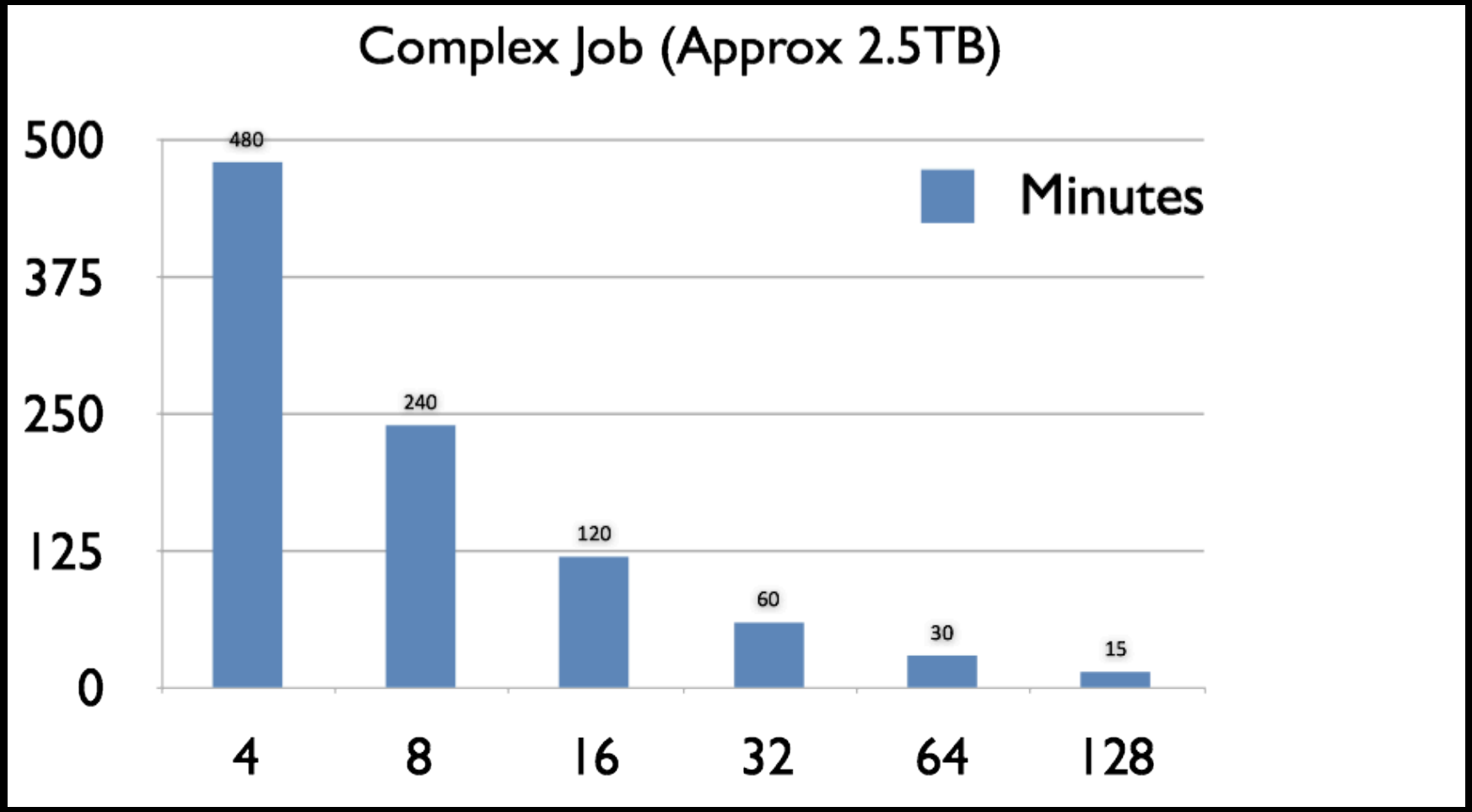
- Richard Bejtlich


Question?
Compute
Compute
Compute
Compute
Storage
Storage
Storage
Storage
Latest Packet Captures

Big Data Scale

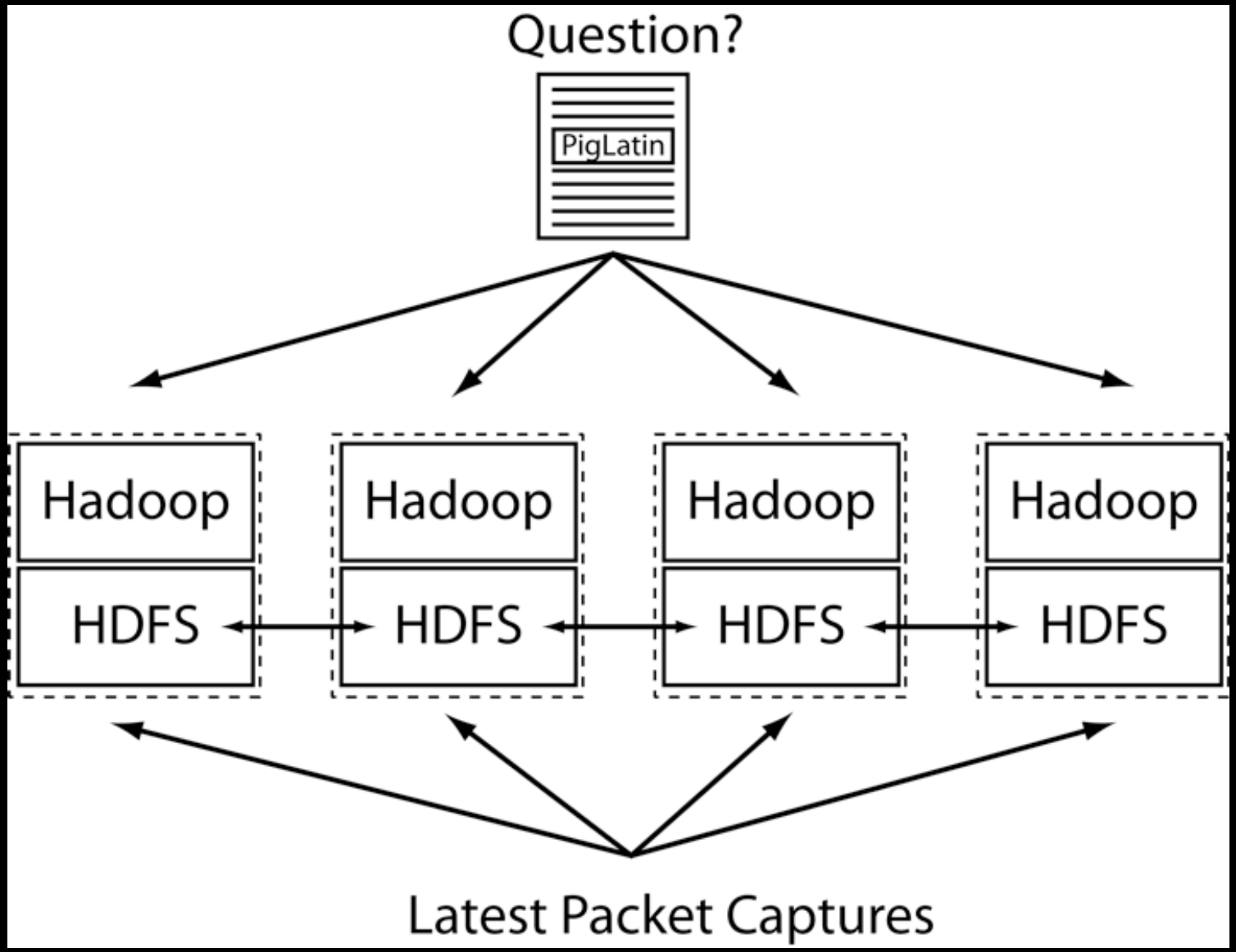
- I want to ask a 2.5TB question
  - Process 2.5TB, 8 hours, 4 Compute units.
  - Process 2.5TB, 4 hours , 8 Compute units.
  - Process 2.5TB, 2 hours, 16 Compute units.
  - Process 2.5TB, 1 hour, 32 Compute units.
  - Process 2.5 TB, 30 minutes, 64 Compute units.
  - Process 2.5 TB , 15 minutes, 128 Compute units.
- Scale my compute to answer my question.

Big Data Scale



Distributed Processing

- Google Map Reduce Whitepaper (2004)
- Google File System Whitepaper (2003)
- Hadoop is an Apache Project for M/R (2007)
- Hadoop File System is a distributed file system for Hadoop nodes (2007)
- Pig is a data analysis language to ease the creation of Map / Reduce jobs that run on Hadoop Clusters (2008)


Question?
PigLatin
Hadoop
Hadoop
Hadoop
Hadoop
HDFS
HDFS
HDFS
HDFS
Latest Packet Captures

Pig

- A acyclic data flow language.
- Transforms data rather than queries data.
- Builds map reduce jobs that are distributed across a Hadoop Cluster.
- Write and debug on your laptop and run on the cluster.
- Relatively easy to learn and brute force.

Pig

- Loaders
- Types
- UDFs
- Java
- Scripts (Python) and
- Binaries (p0f and Snort)

Piglatin

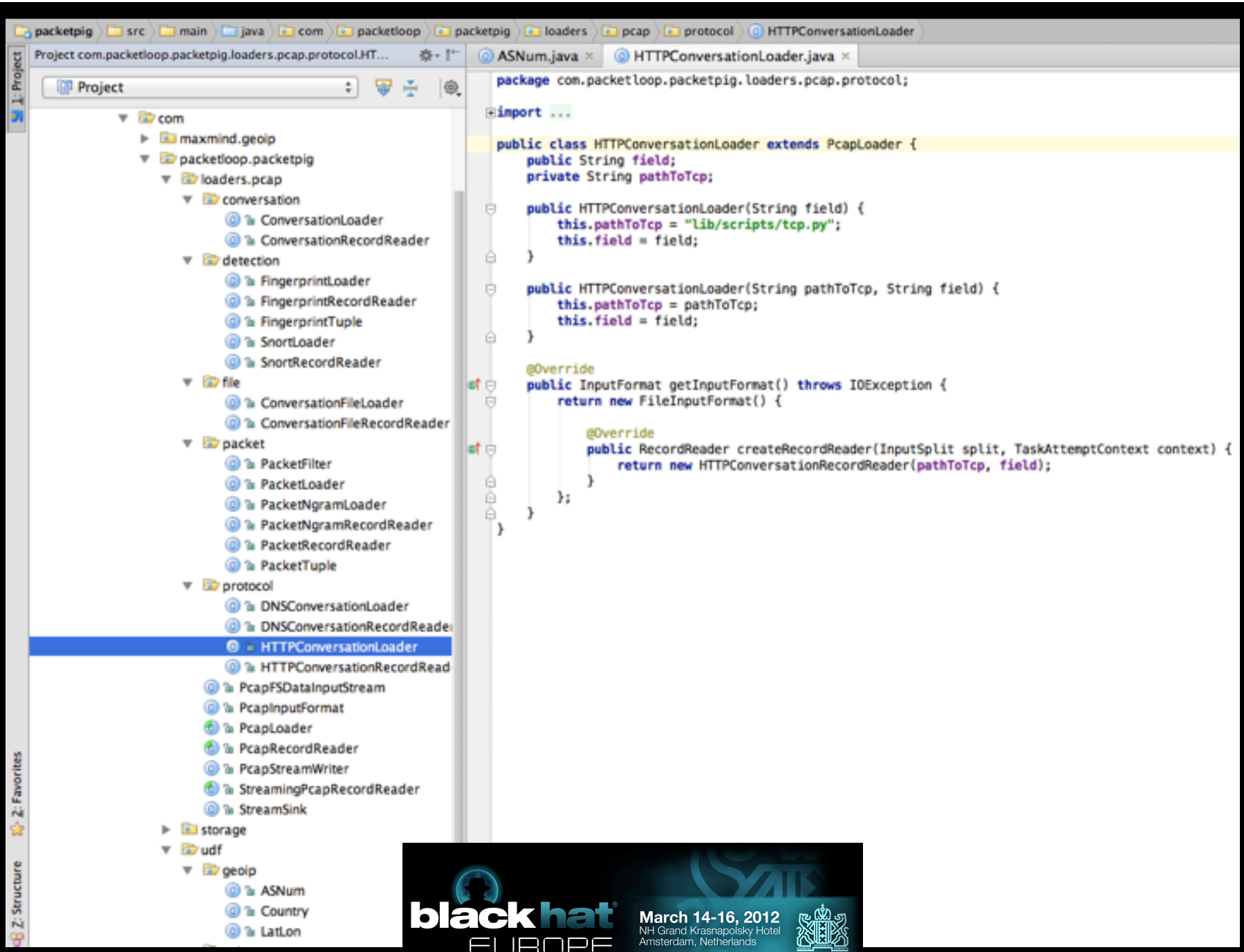
- The data analysis language for Pig scripts
- Group on keys and iterate values
- Iterate using FOREACH
- Filter, Distinct, Sort, Count, Avg, Sum
- Join (LEFT, OUTER)
- Piggybank community tools.
- Illustrate, Explain, Dump or Store.

@packetpig

- Packetloop + Pig = Packetpig
- https://github.com/packetloop/packetpig
- Open Source, Big Data, Security Analytics
- One stop shop for Network Security Monitoring for large data sets.
- Capable of integrating other NSM tools and LOGS!
- Visualisations

@packetpig - Features

- Wireshark the Internet!!
- Bin Time
- Threat Analysis
- Traffic Analysis
- Conversations and Flows
- Geo-Location
- Operating System Fingerprinting
- File Dissection



Wireshark the Internet!

- Access to raw packet captures
- Query, filter, group, sort, count or average anything in the IP, TCP and UDP Headers.
- PacketLoader() acts as a base class for most Loaders.
- Used for bandwidth, packets per second, breakdown by protocol and global queries.
- Search for strange combination of TCP flags

Demo


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Binning Time

- Packetpig can process billions and billions of data points.
- Most other software can't handle loading datasets that big.
- Bin on 5m, 30m, 1h, 4h, 8h, 12h, 24h etc.
- Convert your bin time to seconds and pass as parameter to Packetpig scripts.
- Anything with a timestamp can be binned.

Demo


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Threat Analysis

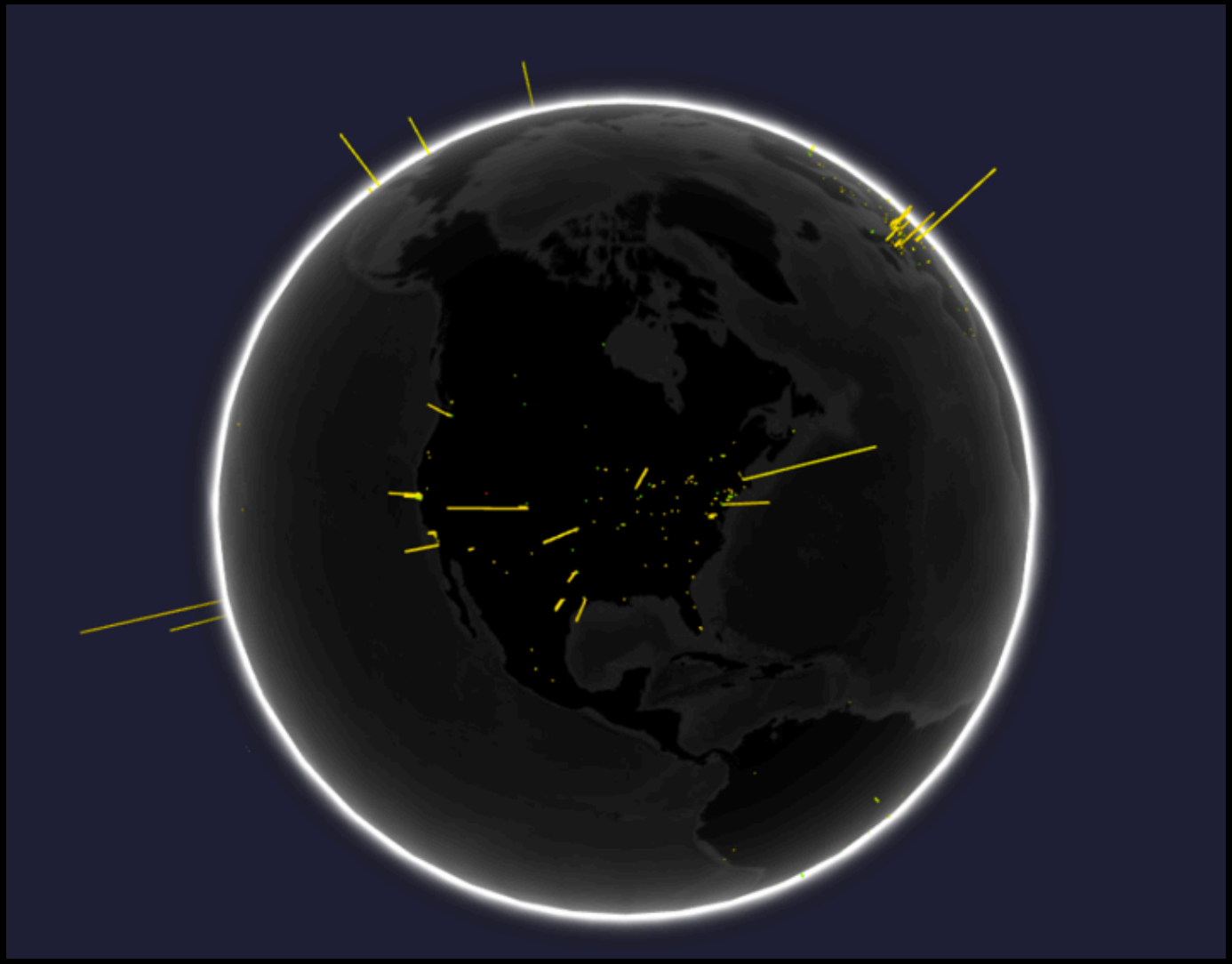
- SnortLoader() is a wrapper for Snort.
- Runs Snort distributed across Hadoop nodes.
- Pass different snort.conf at run time.
- Snort output is returned to the script.
- Loader returns the following schema.
  - Timestamp, Sig ID, Priority, Message, Protocol,
  - Source IP, SPort, Destination IP, DPort

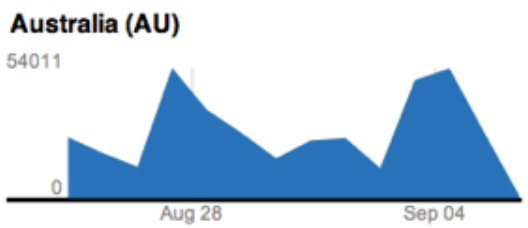
Geo Location

- GeoIP User Defined Function (UDF)
- Wraps the Maxmind Geoip Java library.
- Returns
  - Country
  - ASNum
  - Lat/Long
- Can be used in any script with any loader.

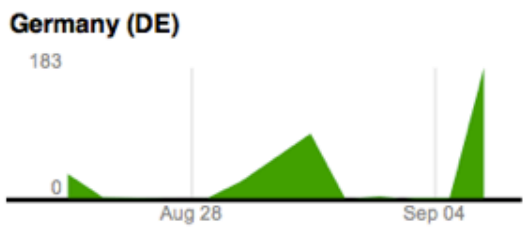
Demo

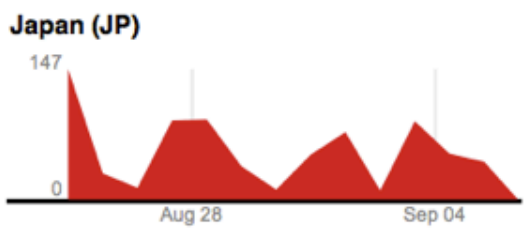

black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

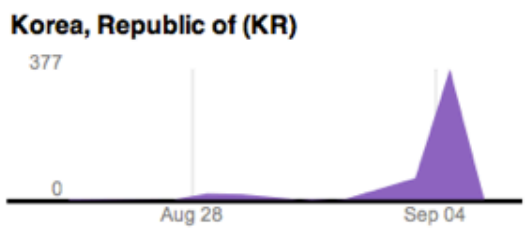


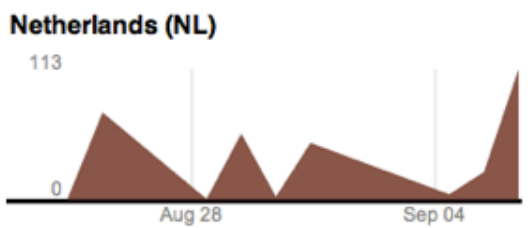

Australia (AU)
54011
0
Aug 28
Sep 04

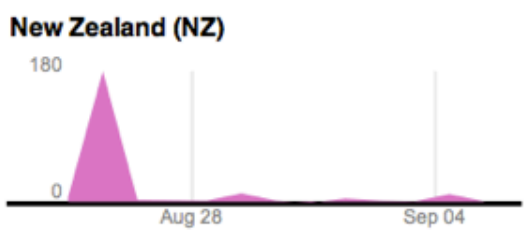

China (CN)
110
0
Aug 28
Sep 04

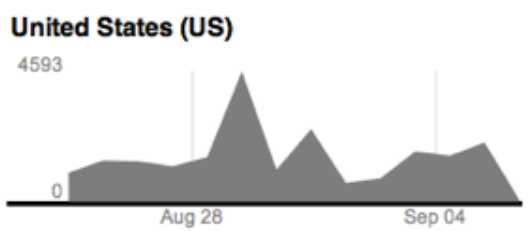

Germany (DE)
183
0
Aug 28
Sep 04

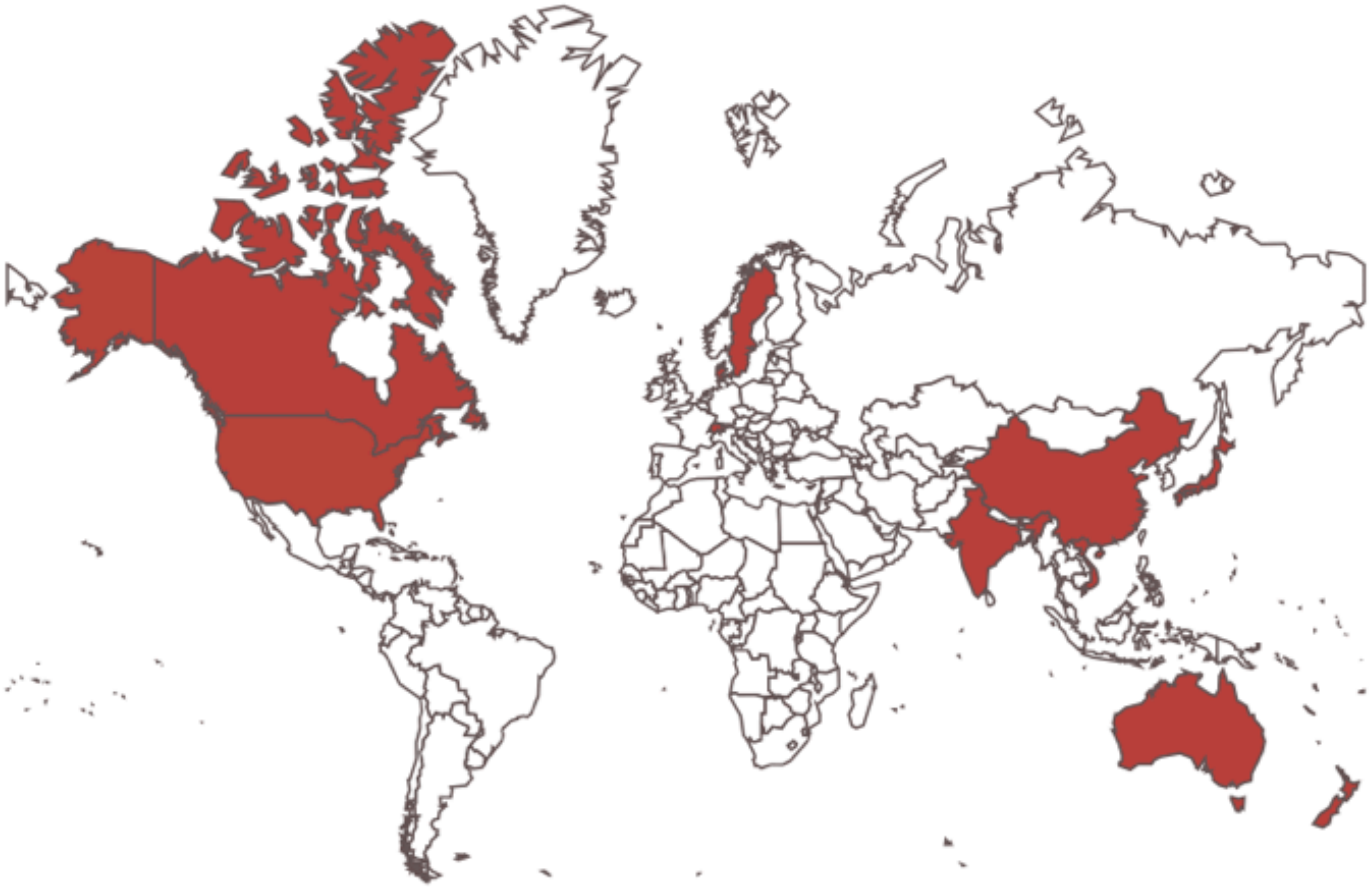

Japan (JP)
147
0
Aug 28
Sep 04


Korea, Republic of (KR)
377
0
Aug 28
Sep 04


Netherlands (NL)
113
0
Aug 28
Sep 04


New Zealand (NZ)
180
0
Aug 28
Sep 04


United States (US)
4593
0
Aug 28
Sep 04

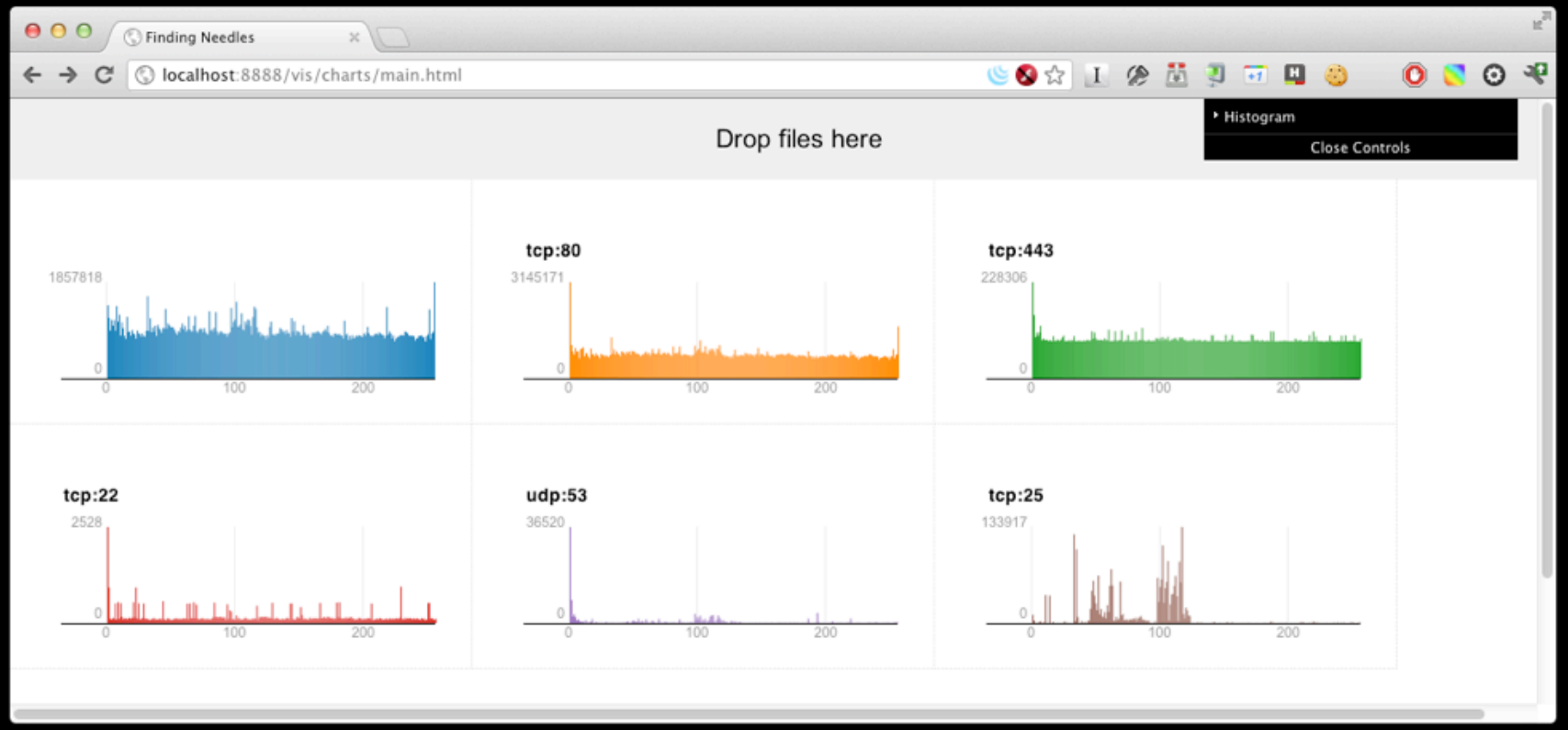


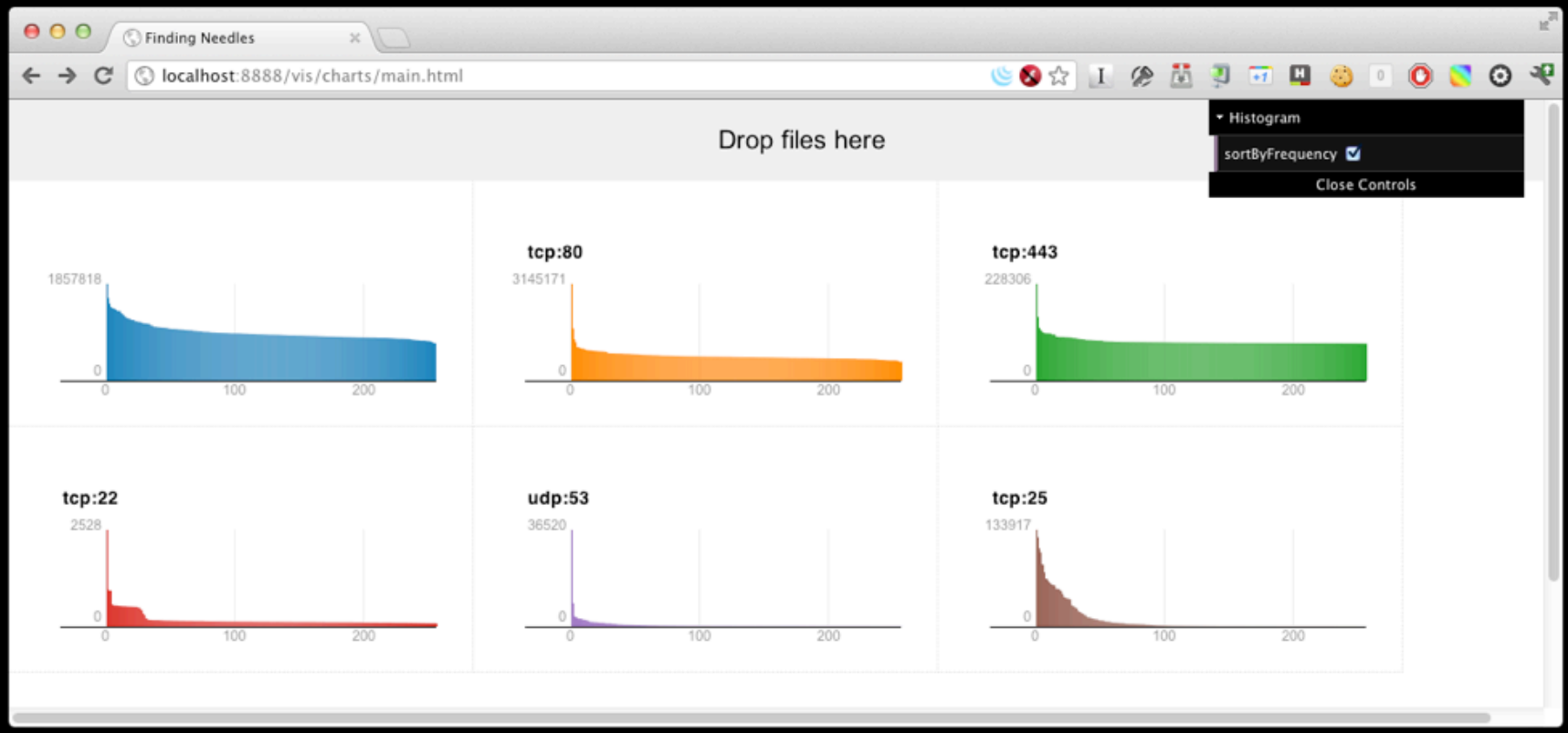
Traffic Analysis

- Detecting covert and encrypted channels
- Packet Size
  - "Traffic analysis of SSL Encrypted Web Browsing" - Heyning Cheng and Ron Avnur
- Packet Size / Inter-packet delay
  - "Datamining for Hackers" - Stefan Burschka at the Chaos Communications Conference.
- Packet Size and Ngram analysis
  - "Anomalous Payload-based Network Intrusion Detection" - Ke Wang and Salvatore J Stolfo.

Ngram Analysis

- Analyse packet payloads for what ASCII codes are used between 0-255.
- Perform unigram, bigram and trigram analysis.
- Analyse the number of characters uses in a frequency of byte ordered plot.
- Packetpig supports N number of grams.


Finding Needles
localhost:8888/vis/charts/main.html
Drop files here
Histogram
Close Controls
tcp:80
1857818
3145171
tcp:443
228306
tcp:22
2528
udp:53
36520
tcp:25
133917
0
100
200


Finding Needles
localhost:8888/vis/charts/main.html
Drop files here
Histogram
sortByFrequency
Close Controls
tcp:80
1857818
3145171
tcp:443
228306
tcp:22
2528
udp:53
36520
tcp:25
133917
0
100
200

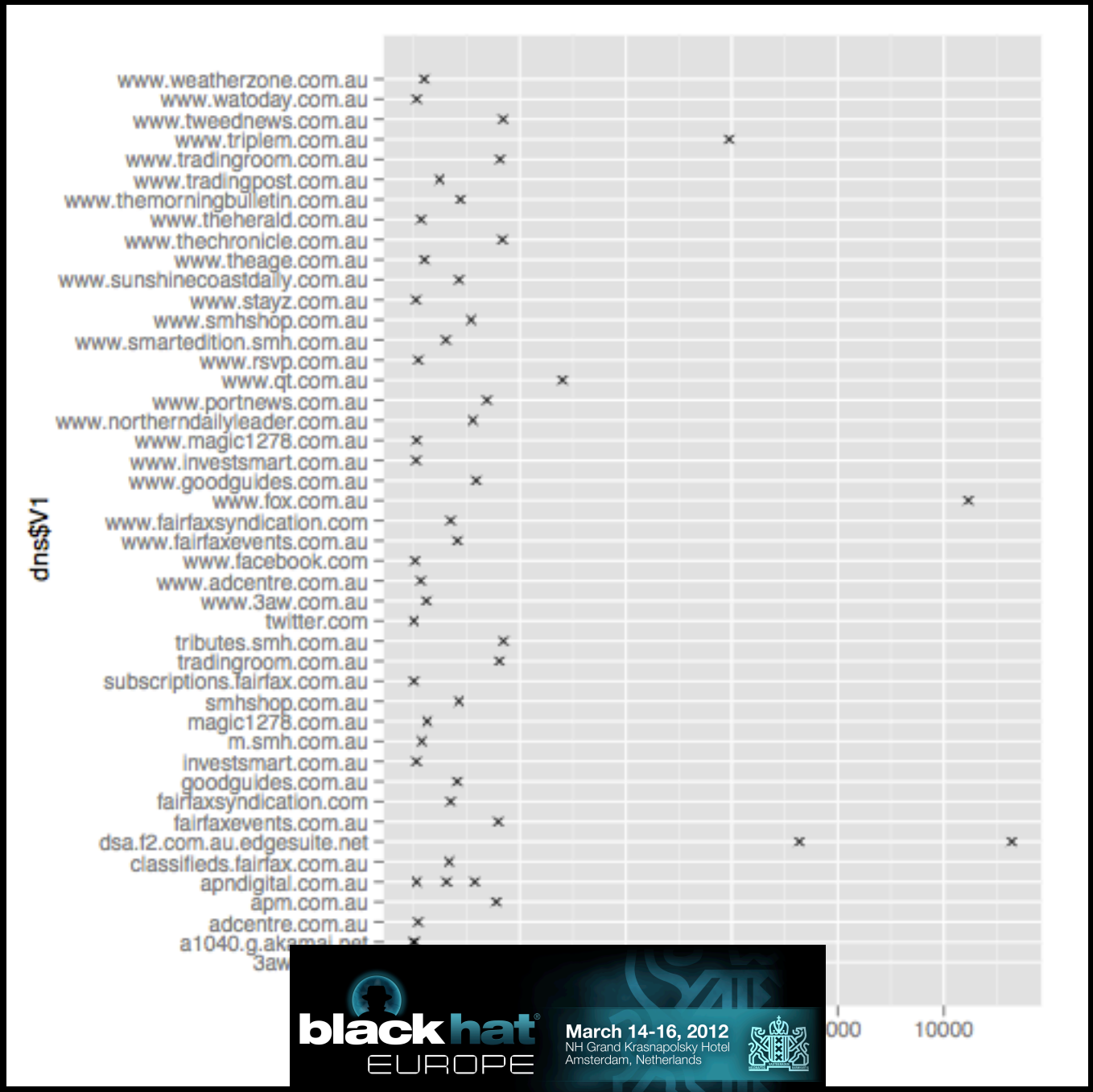
Deep Packet Inspection

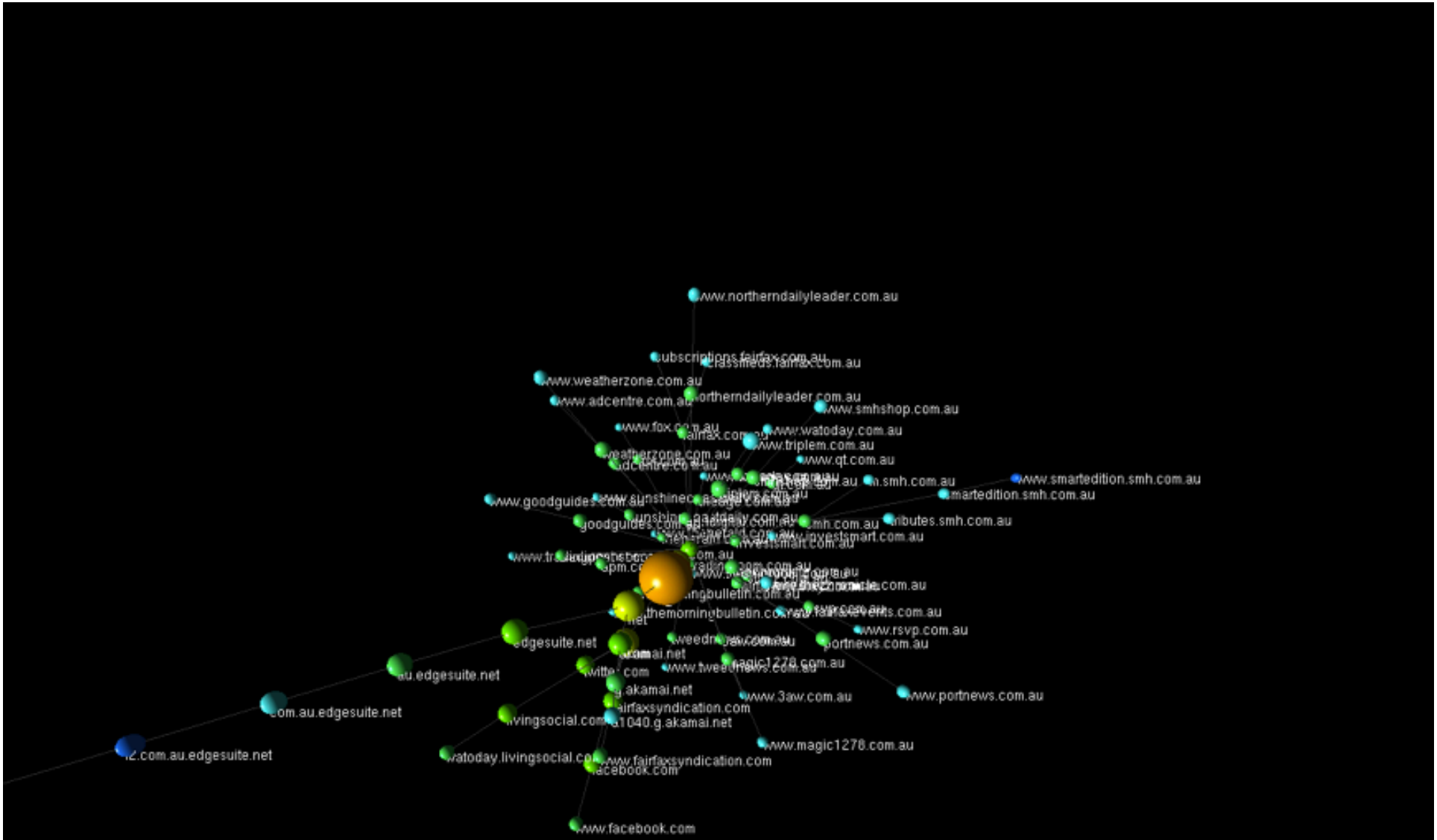
- DNSConversationLoader()
  - Access DNS queries and responses
  - Timestamp, Query ID, Mode, Name, IP Address and TTL
- HTTPConversationLoader()
  - Access to HTTP fields (e.g. user-agent, set-cookie, etag)
  - Access to requests and responses.

Demo
Basic DNS, HTTP

Malware Domain Analysis

- Track increases and decreases in the number of queries per domain.
- Track the TTL for domains and see how they change over time.
- Track the number of IP's returned for each domain and how many distinct countries those IP's reside in.




www.northerndailyleader.com.au
www.weatherzone.com.au
www.adcentre.com.au
www.smhshop.com.au
www.watoday.com.au
www.triplem.com.au
www.qt.com.au
www.smartedition.com.au
www.goodguides.com.au
www.rsvp.com.au
www.portnews.com.au
www.3aw.com.au
www.magic1278.com.au
www.facebook.com

Conversations / Flows

- Track conversation establishment and termination
- Return all packets related to a conversation
- Return inter-packet delay
- Return the size of packets in the conversation.
- Return the end state of the conversation

OS Fingerprinting

- FingerprintLoader() is a wrapper for @lcamtuf's p0f
- FingerprintLoader() returns the information from p0f to the Pig script.
- Perform passive operating system detection across terabytes of data.

Demo

File Extraction

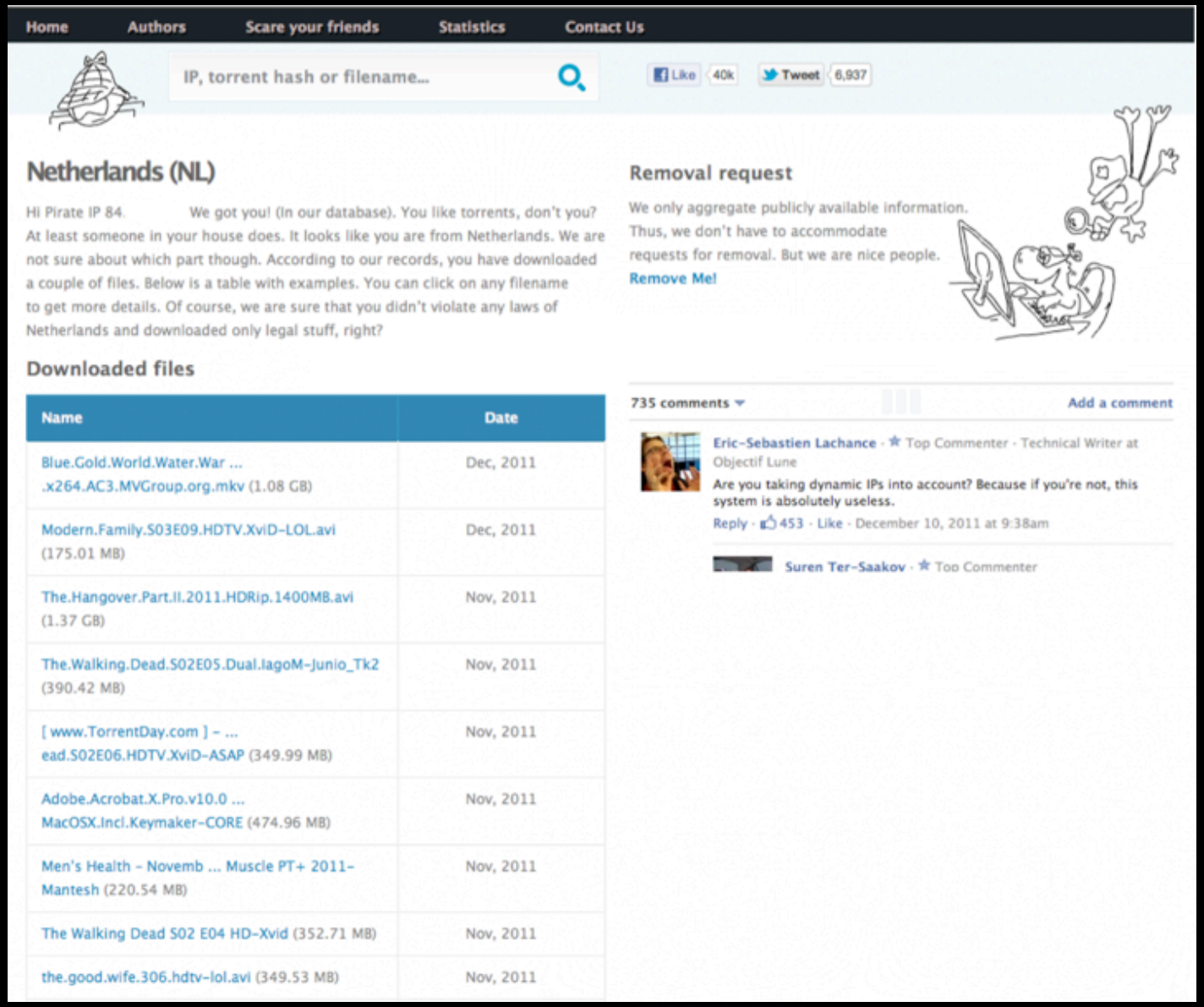
- Analyse every conversation on the network.
- Extraction or just output information
  - Choose whether to extract files or not.
  - Extract based on mime type or file extension.
  - Extract or search for particular hashes.
- Additional file information through libmagic.
- Output file name, file type, name, extension, MD5, SHA1, SHA256 hashes.

Demo

Is Big Data - Big Surveillance?

- Packet capture is analogous to wire tapping.
- Distributed processing of full network data starts to worry you.
- Potential for mis-use, surveillance, data warehouses.
- Reputation services that sell dossiers on hashed IP addresses.
- Data mining ‘networks’ for long periods.

A Simple Experiment


Home
Authors
Scare your friends
Statistics
Contact Us
IP, torrent hash or filename...
Like 40k
Tweet 6,937
Netherlands (NL)
Hi Pirate IP 84. We got you! (In our database). You like torrents, don't you? At least someone in your house does. It looks like you are from Netherlands. We are not sure about which part though. According to our records, you have downloaded a couple of files. Below is a table with examples. You can click on any filename to get more details. Of course, we are sure that you didn't violate any laws of Netherlands and downloaded only legal stuff, right?
Removal request
We only aggregate publicly available information. Thus, we don't have to accommodate requests for removal. But we are nice people.
Remove Me!
Downloaded files
Name
Date
Blue.Gold.World.Water.War ... .x264.AC3.MVGroup.org.mkv (1.08 GB)
Dec, 2011
Modern.Family.S03E09.HDTV.XviD-LOL.avi (175.01 MB)
Dec, 2011
The.Hangover.Part.II.2011.HDRip.1400MB.avi (1.37 GB)
Nov, 2011
The.Walking.Dead.S02E05.Dual.IagoM-Junio_Tk2 (390.42 MB)
Nov, 2011
[www.TorrentDay.com] - ... ead.S02E06.HDTV.XviD-ASAP (349.99 MB)
Nov, 2011
Adobe.Acrobat.X.Pro.v10.0 ... MacOSX.Incl.Keymaker-CORE (474.96 MB)
Nov, 2011
Men's Health - Novemb ... Muscle PT+ 2011-Mantesh (220.54 MB)
Nov, 2011
The Walking Dead S02 E04 HD-Xvid (352.71 MB)
Nov, 2011
the.good.wife.306.hdtv-lol.avi (349.53 MB)
Nov, 2011
735 comments
Add a comment
Eric-Sebastien Lachance · Top Commenter · Technical Writer at Objectif Lune
Are you taking dynamic IPs into account? Because if you're not, this system is absolutely useless.
Reply · 453 · Like · December 10, 2011 at 9:38am
Suren Ter-Saakov · Top Commenter

Torrents

- Connect to the top torrent trackers like the PirateBay 100, dump Seeders and Leechers.
- Record the BitTorrent Client type (entropy).
- Look at all attacks on a particular dataset
- Join Torrent Data and Snort data on Source IP
- What files are downloaded by the people that trigger IDS alerts?
- Does Torrent data allow me to triangulate?

Torrent Results

Attackers and Torrents

- 17 IP addresses matched attacks and torrents.
- 5 Countries - Australia, China, South Africa, Phillipines, Singapore.
- Mainly protocol anomalies and Spyware upload detection.
- Two cases are worth looking into further.
- Use Packetpig to gather Snort, Torrent, p0f and User-Agent data.

Torrent Files

- Justice.League.Doom.2012.BRRip.XviD.Ac3.Feel-Free
- Tower Heist (2011) DVDRip XviD-MAXSPEED
- Friends with Benefits 2011 R5 LiNE READNFO XViD-IMAGiNE
- The.Adventures.of.Tintin.2011.1080p.BluRay.x264-MaxHD
- 7 Weeks to 100 Push-Ups: Strengthen and Sculpt Your Arms, Abs, C
- The Walking Dead S02E04 HDTV XviD-ASAP[ettv]
- Footloose.2011.DVDRip.XviD- PADDO
- Thor (2011) DVDRip XviD-MAX
- Daredevil - Soundtrack:-:Thar
- Rise of the Planet of the Apes (2011) DVDRip XviD-MAX
- Revenge S01E15 HDTV XviD-LOL [VTV]
- 1000 Photoshop Tips and Tricks (Dec 2010)-Mantesh
- CSI.S12E14.HDTV.XviD-LOL.avi

The Suspects

- Two attackers analysed due to Snort Alert severity.
- The South African.
  - Snort triggering on Spyware 'PUT' to a web site.
- The Australian.
  - Protocol anomalies that are worth investigating.

The South African

- 9 IP addresses from AS5713 SAIX-NET
- Reverse DNS links them to SAIX Proxies.
  - e.g. wblv-ip-pcache-4-vif0.telkom-ipnet.co.za.
- Attacks
  - (http_inspect) LONG HEADER
  - SPYWARE-PUT Trackware funwebproducts mywebsearchtoolbar-funtools runtime detection

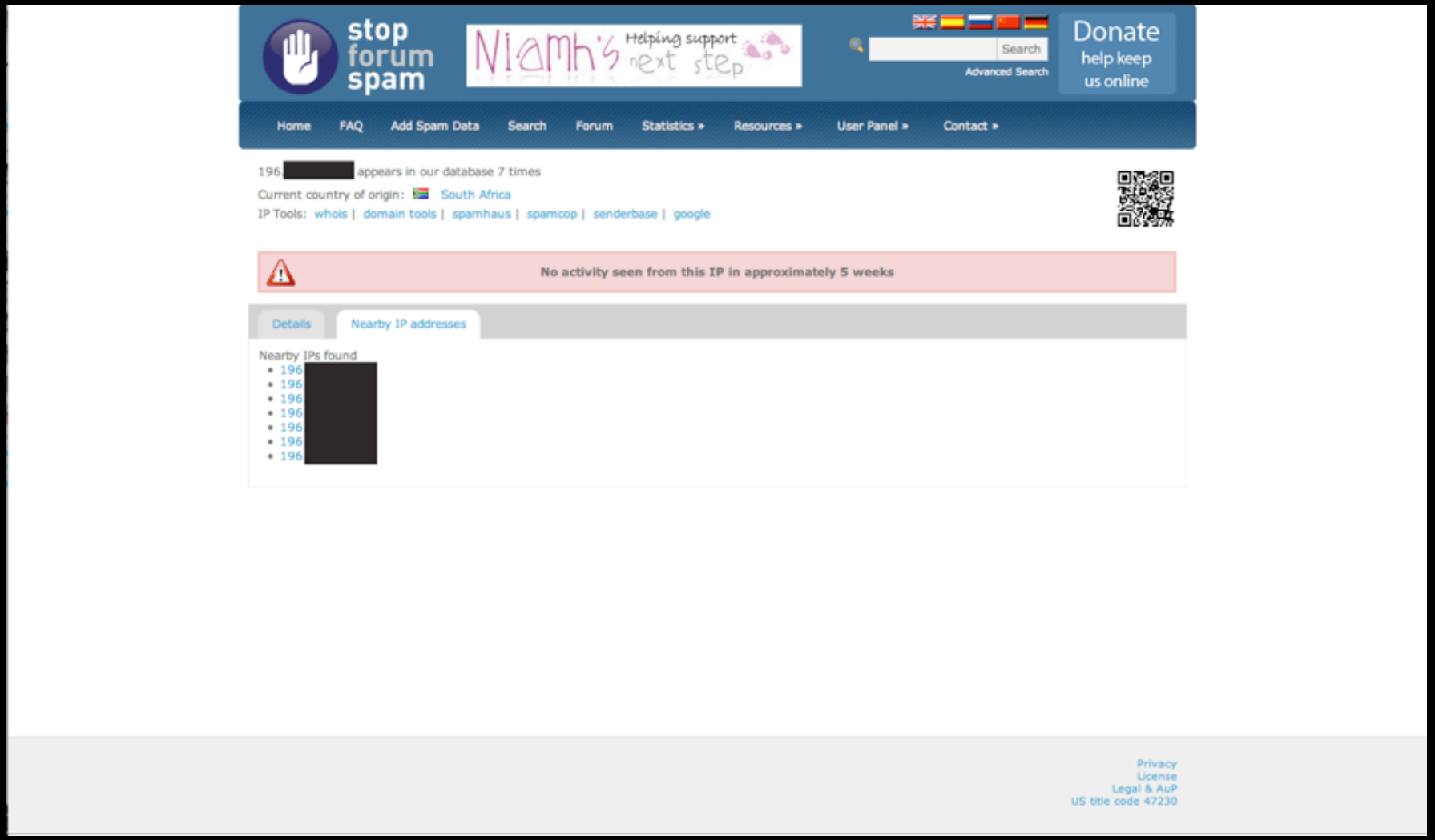
Let's Enhance!

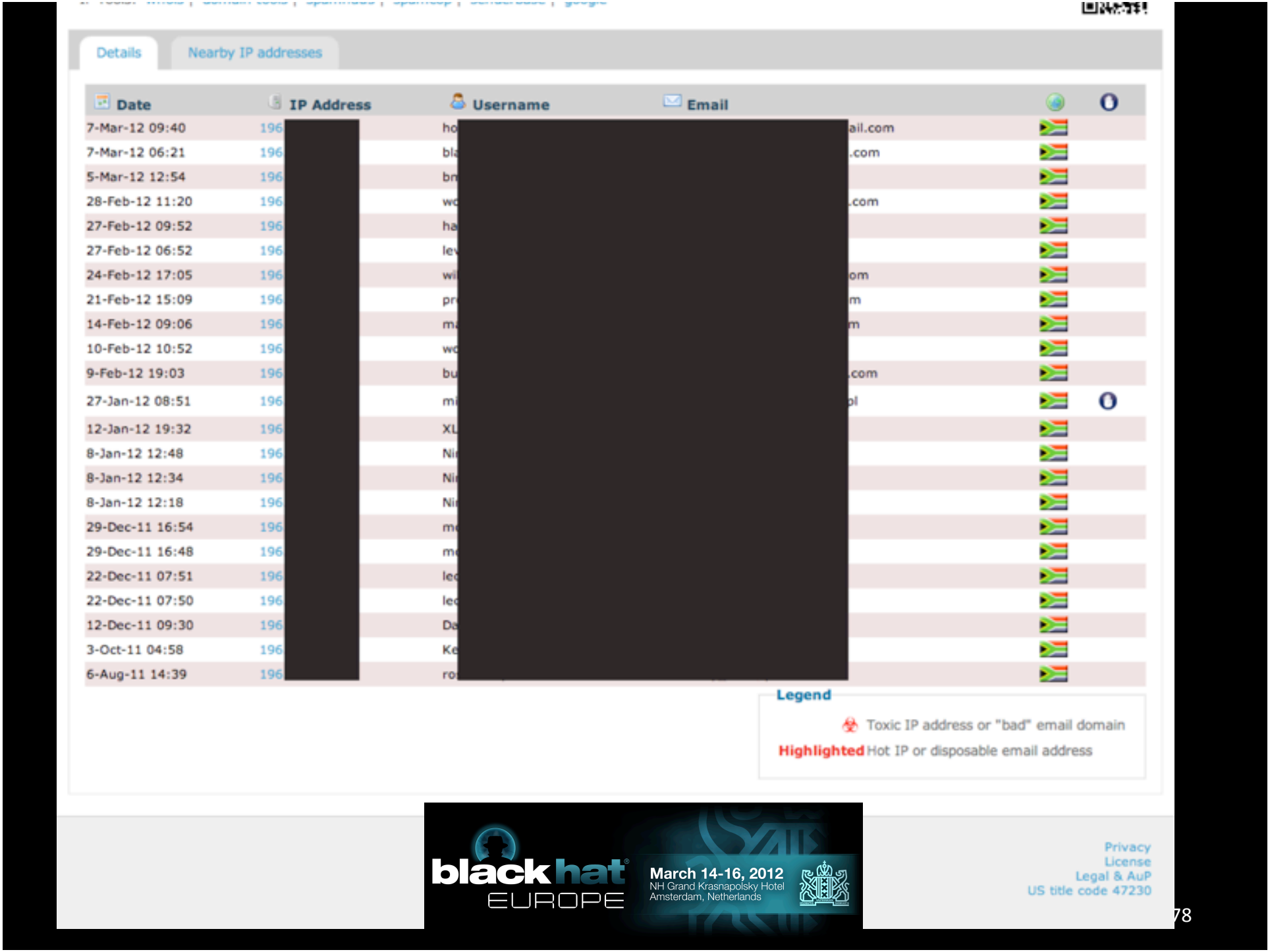
The South African

- Packetpig UDF provided two lat/longs but they were worthless.
- Linked to 7 Torrent files.
  - "7 Weeks to 100 Push-Ups: Strengthen and Sculpt Your Arms, Abs, C" linked two IP addresses to the one user.
  - "The.Adventures.of.Tintin.2011.DVDRip.XviD-TARGET" linked another two IP addresses to another user.
  - User-agents for these individual users confirmed this.
- Using torrents as a way to triangulate works.
  - Spreading malware and forum post abuse

The South African

- Google the IP addresses.
- Linked to a botnet traffic
  - Spreading malware and forum spam.
- Likely some home machine that's torrents and is also infected with Malware.


stop forum spam
Niamh's Helping support next step
Search
Advanced Search
Donate help keep us online
Home
FAQ
Add Spam Data
Search
Forum
Statistics »
Resources »
User Panel »
Contact »
196[redacted] appears in our database 7 times
Current country of origin: South Africa
IP Tools: whois | domain tools | spamhaus | spamcop | senderbase | google
No activity seen from this IP in approximately 5 weeks
Details
Nearby IP addresses
Nearby IPs found
196
196
196
196
196
196
196
Privacy
License
Legal & AuP
US title code 47230


Details
Nearby IP addresses
Date
IP Address
Username
Email
7-Mar-12 09:40
7-Mar-12 06:21
5-Mar-12 12:54
28-Feb-12 11:20
27-Feb-12 09:52
27-Feb-12 06:52
24-Feb-12 17:05
21-Feb-12 15:09
14-Feb-12 09:06
10-Feb-12 10:52
9-Feb-12 19:03
27-Jan-12 08:51
12-Jan-12 19:32
8-Jan-12 12:48
8-Jan-12 12:34
8-Jan-12 12:18
29-Dec-11 16:54
29-Dec-11 16:48
22-Dec-11 07:51
22-Dec-11 07:50
12-Dec-11 09:30
3-Oct-11 04:58
6-Aug-11 14:39
Legend
Toxic IP address or "bad" email domain
Highlighted Hot IP or disposable email address
black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands
Privacy
License
Legal & AuP
US title code 47230


Board index » ZB Block » General ZB Block Help » ZB Block Help
All times are UTC - 7 hours [DST]
How to whitelist a single IP that is listed in SFS?
Moderators: diabolic.bg, Spudzz, macmathan, tobias, trparky, Katana
New Topic
Post Reply
Page 1 of 1 [6 posts]
Print view
Previous topic | Next topic
Download Google Chrome Snel & Eenvoudig Zoeken met De Webbrowser van Google! www.google.com/Chrome
Anti Spam Software Eenvoudig in gebruik en installatie Voor Microsoft Outlook en Live Mail www.spamfighter.com
Free Network Monitoring Remote Management Software Tool Try N-central® Free for 30 days! N-able.com/?Network-Management
AdChoices
How to whitelist a single IP that is listed in SFS?
Author
Message
How to whitelist a single IP that is listed in SFS?
Joined: Fri Mar 05, 2010 5:43 pm
Posts: 7
I have a legit user with an IP: 196.
Indeed this IP is in the SFS database (what's more. there are records from last month, too):
http://www.stopforumspam.com/ipcheck/196.
yet I would still like to know how I can get around this. I tried to whitelist the IP in the customsig file this way:
Code:
$ax = $ax - (lmatch($address,"196 ,"In SFS database. ")); //Andrew McK...
but it does not seem to have any effect.
Is there a way to whi it was recorded in SFS, it may now
belong to a legit use I seem to have several issues with
ISP's. His host is (not
http://wblv-ip-pcac
but shown as proxy server here (which does not necessarily mean bad though admittedly suspicious
black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Packetpig Query

- Packetpig
  - SnortLoader()
  - FingerPrintLoader()
  - HTTPConversationLoader()
  - GeoIP UDF to determine Country, ASNum, Lat/Long
  - Torrent output as a CSV text file.

Packetpig Query

- All 9 IP addresses are OpenBSD 3.X
- A number of distinct user-agents making requests of different web sites.
- User-agents triggering alerts include the Trident/4.0 or Trident/5.0 and FunWebProducts user-agent strings.
- Host,Connection=[keep-alive],Accept=[*/*],?Referer,Accept-Language=[en-ZA],User-Agent,Accept-Encoding=[gzip, deflate],?X-Forwarded-For,?Via:Accept-Charset,Keep-Alive:Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; FunWebProducts; GTB7.1; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; HPNTDF; InfoPath.)

Conclusion

- Just some infected Windows machines sitting behind OpenBSD proxies that were browsing a website.
- When analysing the HTTP queries there were no PUTs.
- Snort signature is matching on the user-agent.
- No reason to run more detailed jobs to dump all conversations, protocols or files.

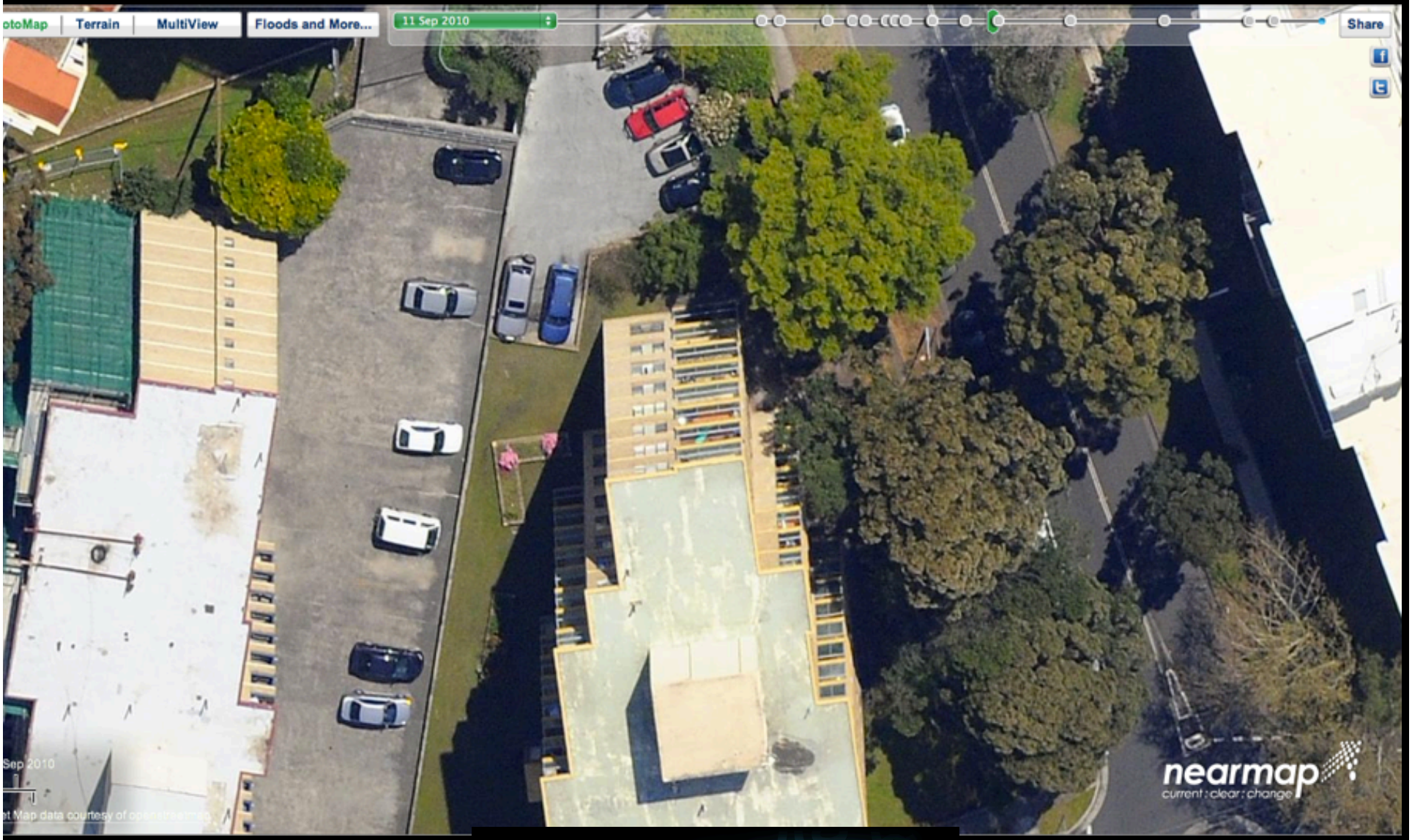
The Australian

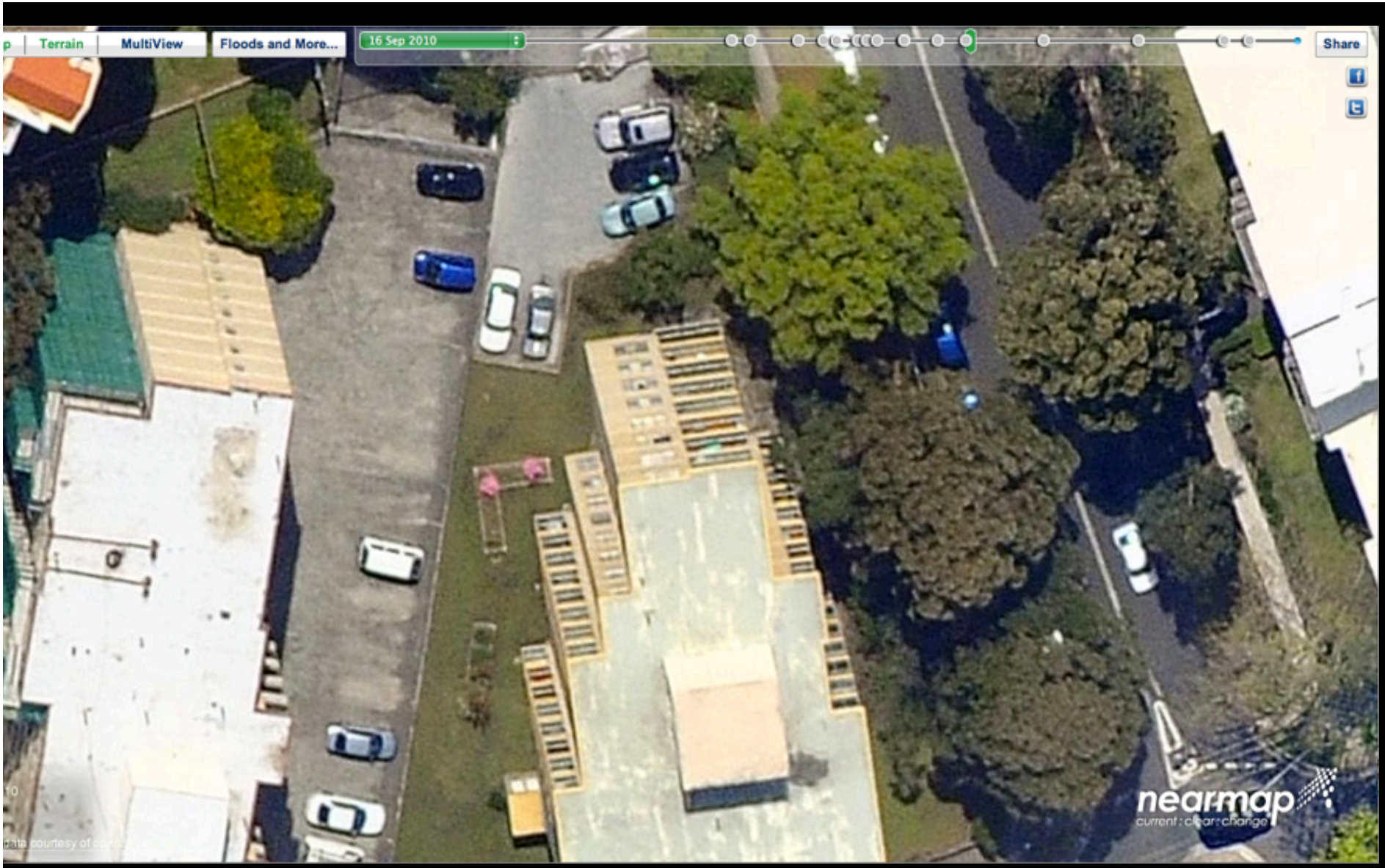
- Single IP address from AS18291 Vodafone Australia.
- Attacks (read: Crimes!)
  - TCP Timestamp is outside of PAWS window
  - Bad segment, adjusted size <= 0
- Packetpig geoip provides a Lat/Long.

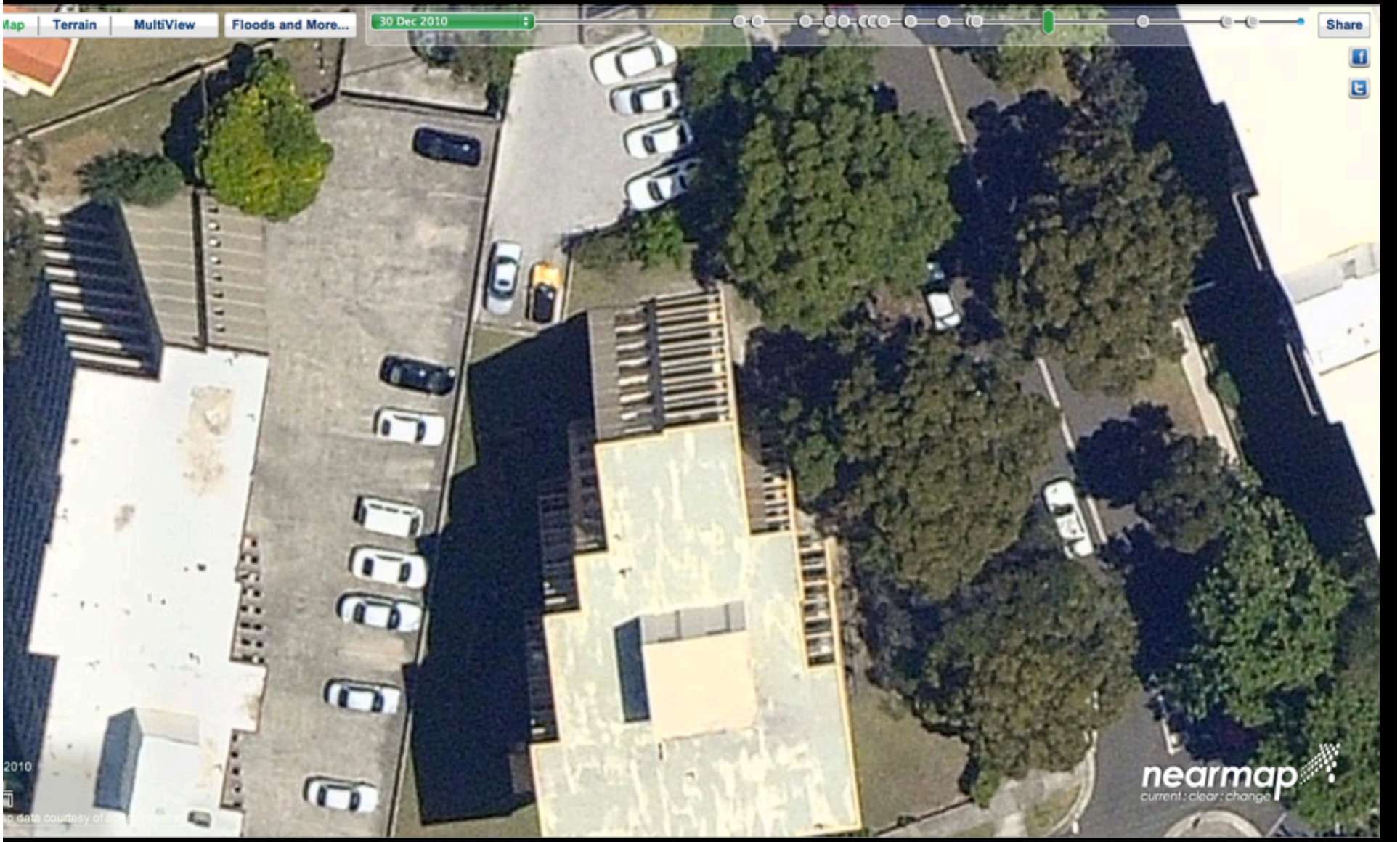
Packetpig Query

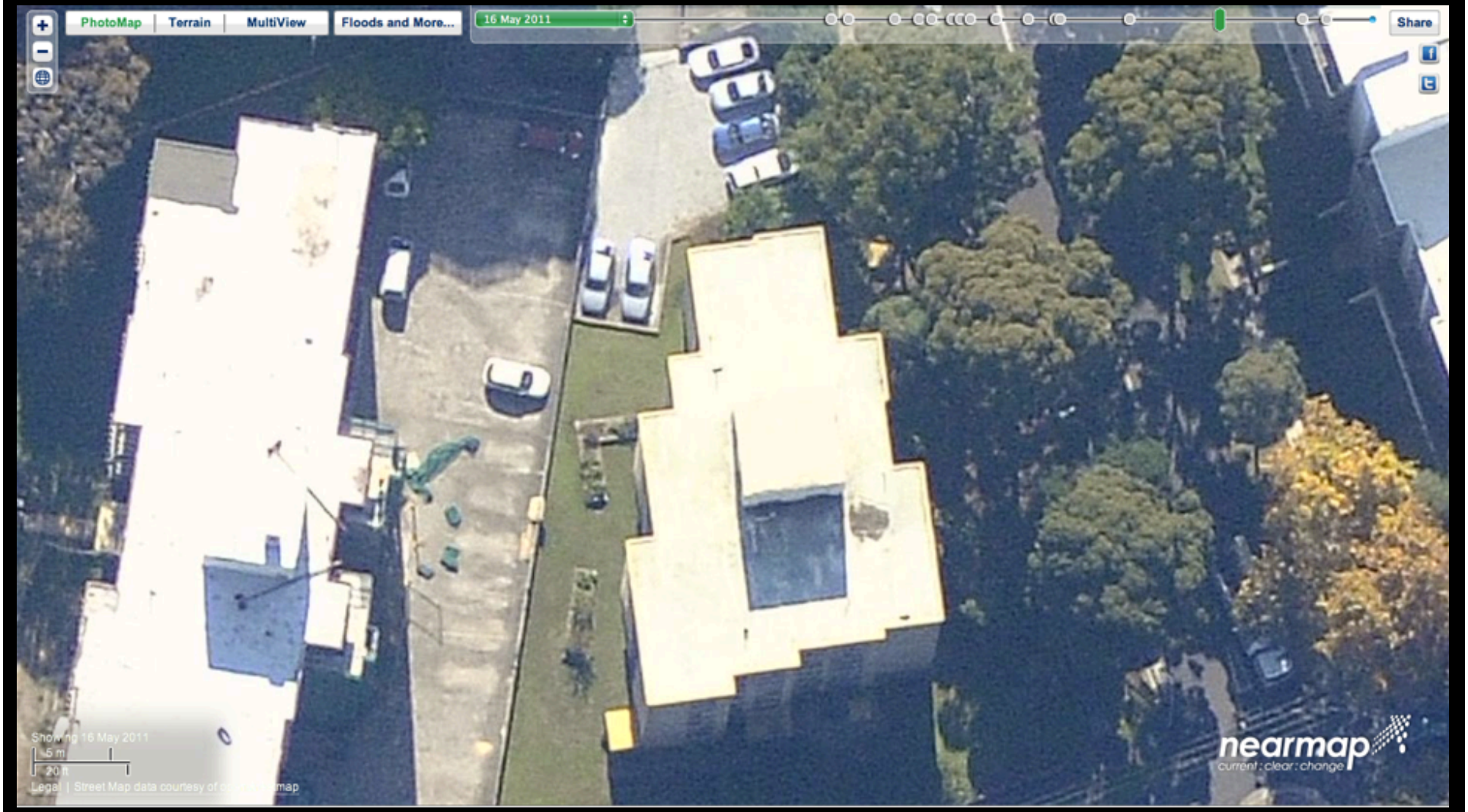
- Packetpig
  - SnortLoader()
  - FingerPrintLoader()
  - HTTPConversationLoader()
  - GeoIP UDF to determine Country, ASNum, Lat/Long
  - Torrent output as a CSV text file.

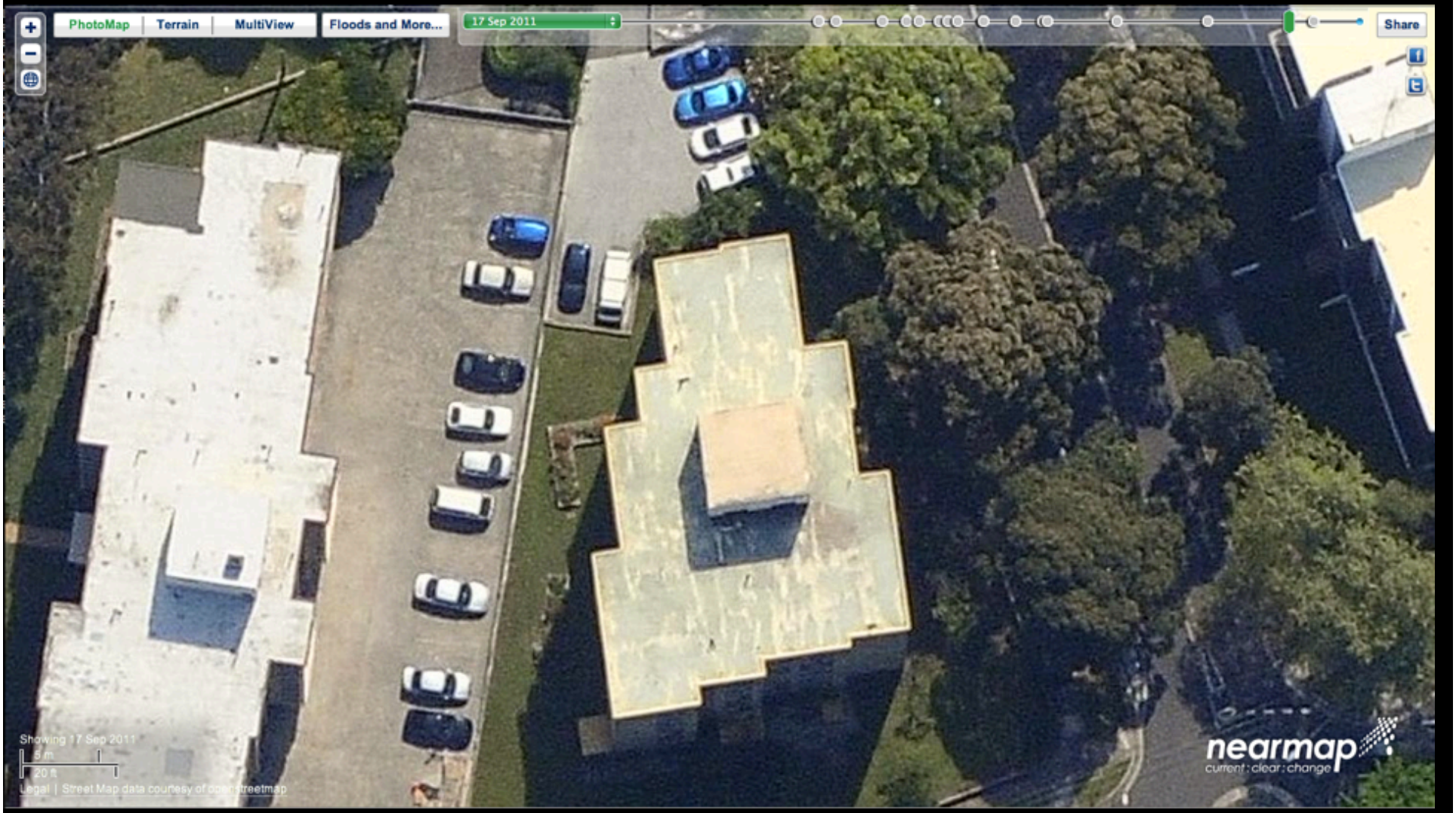
Let's Enhance!

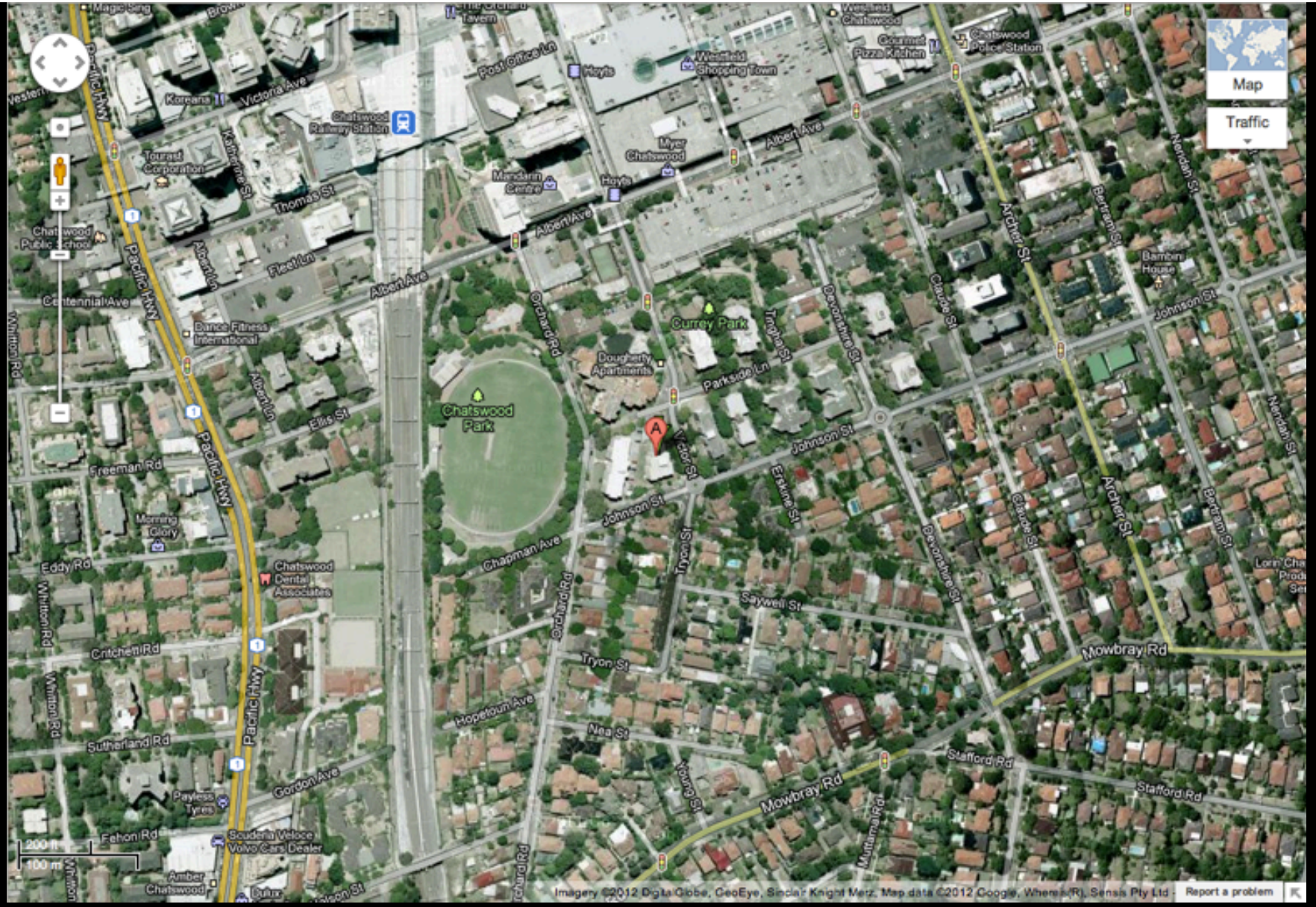

otoMap
Terrain
MultiView
Floods and More...
11 Sep 2010
Share
nearmap
current : clear : change

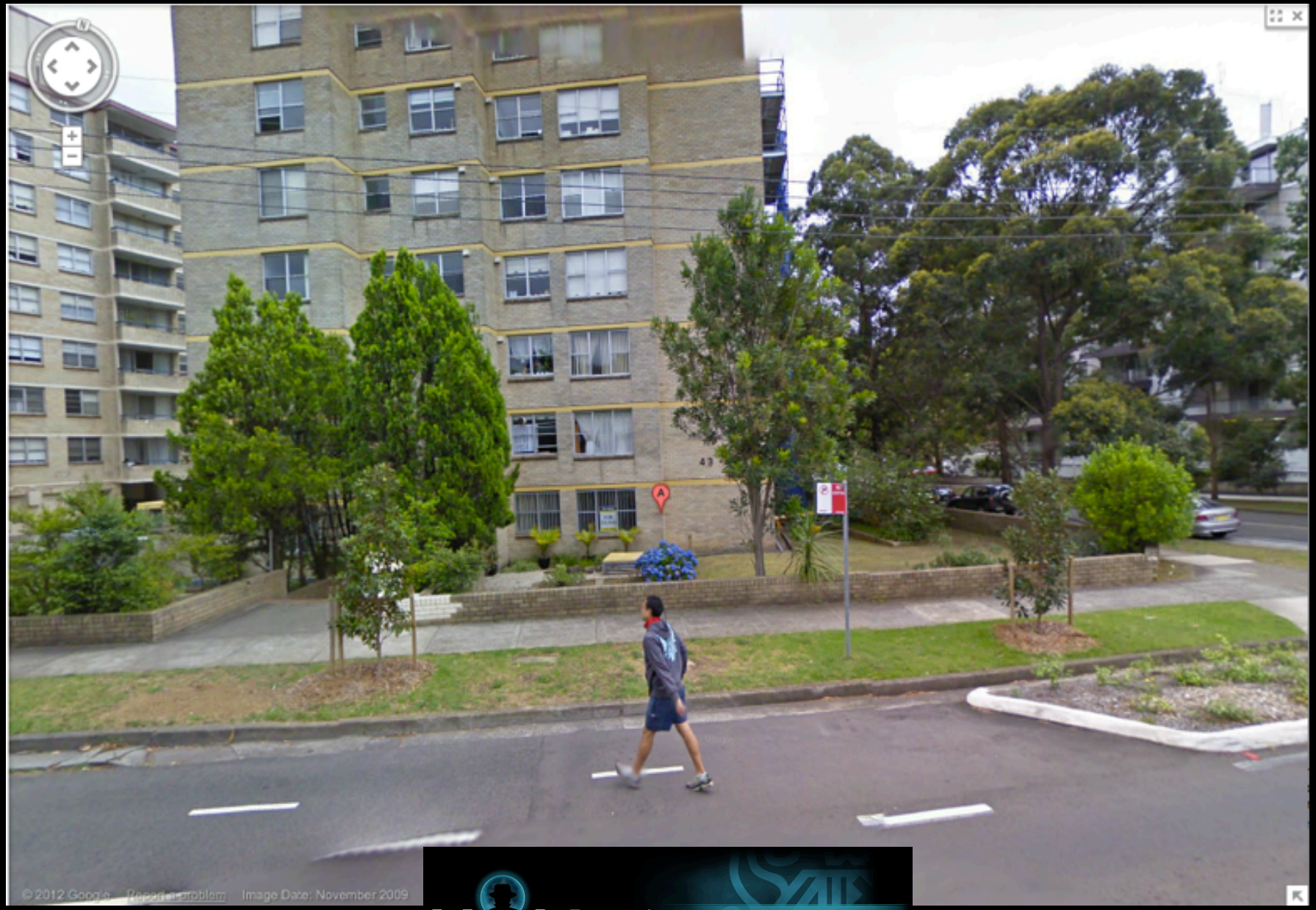

Terrain
MultiView
Floods and More...
16 Sep 2010
Share
nearmap
current : clear : change


Map
Terrain
MultiView
Floods and More...
30 Dec 2010
Share
2010
nearmap
current : clear : change

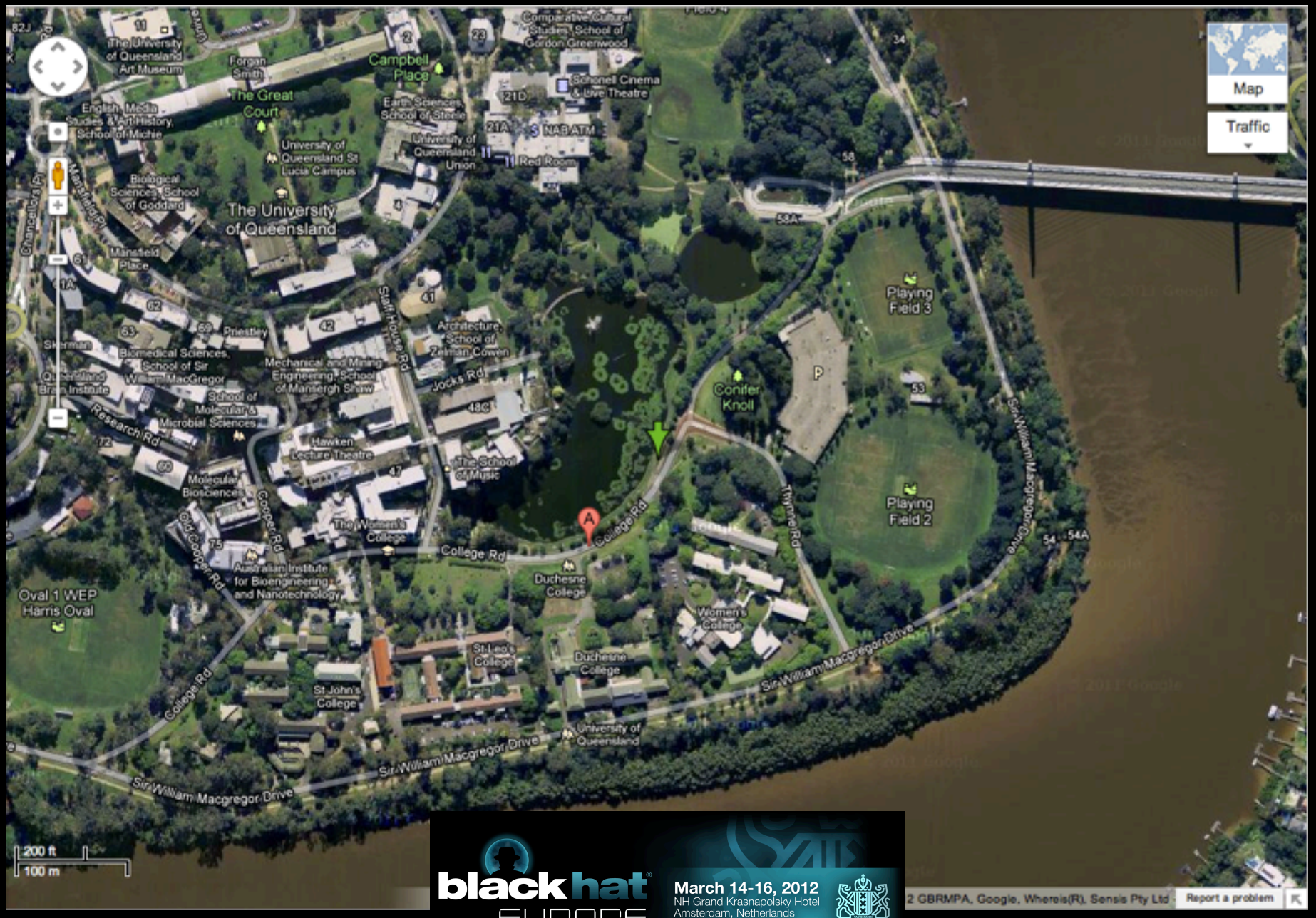

PhotoMap
Terrain
MultiView
Floods and More...
16 May 2011
Share
Showing 16 May 2011
5 m
20 ft
Legal | Street Map data courtesy of
nearmap
current : clear : change


PhotoMap
Terrain
MultiView
Floods and More...
17 Sep 2011
Share
Showing 17 Sep 2011
5 m
20 ft
Legal | Street Map data courtesy of openstreetmap
nearmap
current : clear : change


Map
Traffic
Chatswood Park
Currey Park
Victor St
Johnson St
Archer St
Pacific Hwy
Albert Ave
Mowbray Rd
Chapman Ave
Tryon St
Orchard Rd
Saywell St
Hopetoun Ave
Nea St
Stafford Rd
Eddy Rd
Crichett Rd
Sutherland Rd
Gordon Ave
Fehon Rd
Freeman Rd
Centennial Ave
Ellis St
Thomas St
Fleet Ln
Parkside Ln
Claude St
Bertram St
Nerdan St
Johnson St
Chatswood Railway Station
Chatswood Police Station
Chatswood Public School
Chatswood Dental Associates
Souderia Veloce Volvo Cars Dealer
Imagery ©2012 DigitalGlobe, GeoEye, Sinclair Knight Merz, Map data ©2012 Google, Whereis(R), Sensis Pty Ltd
Report a problem



Just before calling the police...



Google

AWSTATS [redacted]

Search

About 140 results (0.34 seconds)

Everything
Images
Videos
News
Shopping
More

Show search tools

AWSTATS DATA FILE 6.95 (build 1.943) # If you remove this file, all ...
www.sanctuaryspringbrook.com.au/.../**awstats**/**awstats**092011.info....
AWSTATS DATA FILE 6.95 (build 1.943) # If you remove this file, all statistics for ..... 0 9 271017 196.219.172.179 1 1 4598 20110908141058 **123.**[redacted] 4 25 ...

AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all ...
www.steelrod.com.au/**awstats**/data/**awstats**122011.steelrod.com.au.txt
AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all statistics ..... 8 93 1653201 20111206193345 **123.**[redacted] 3 10 180650 20111212234001 ...

AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all ...
www.steelrod.com.au/**awstats**/data/**awstats**102011.steelrod.com.au.txt
AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all statistics ..... 20111014031149 208.80.194.63 1 1 12978 20111019052515 **123**[redacted] 0 ...

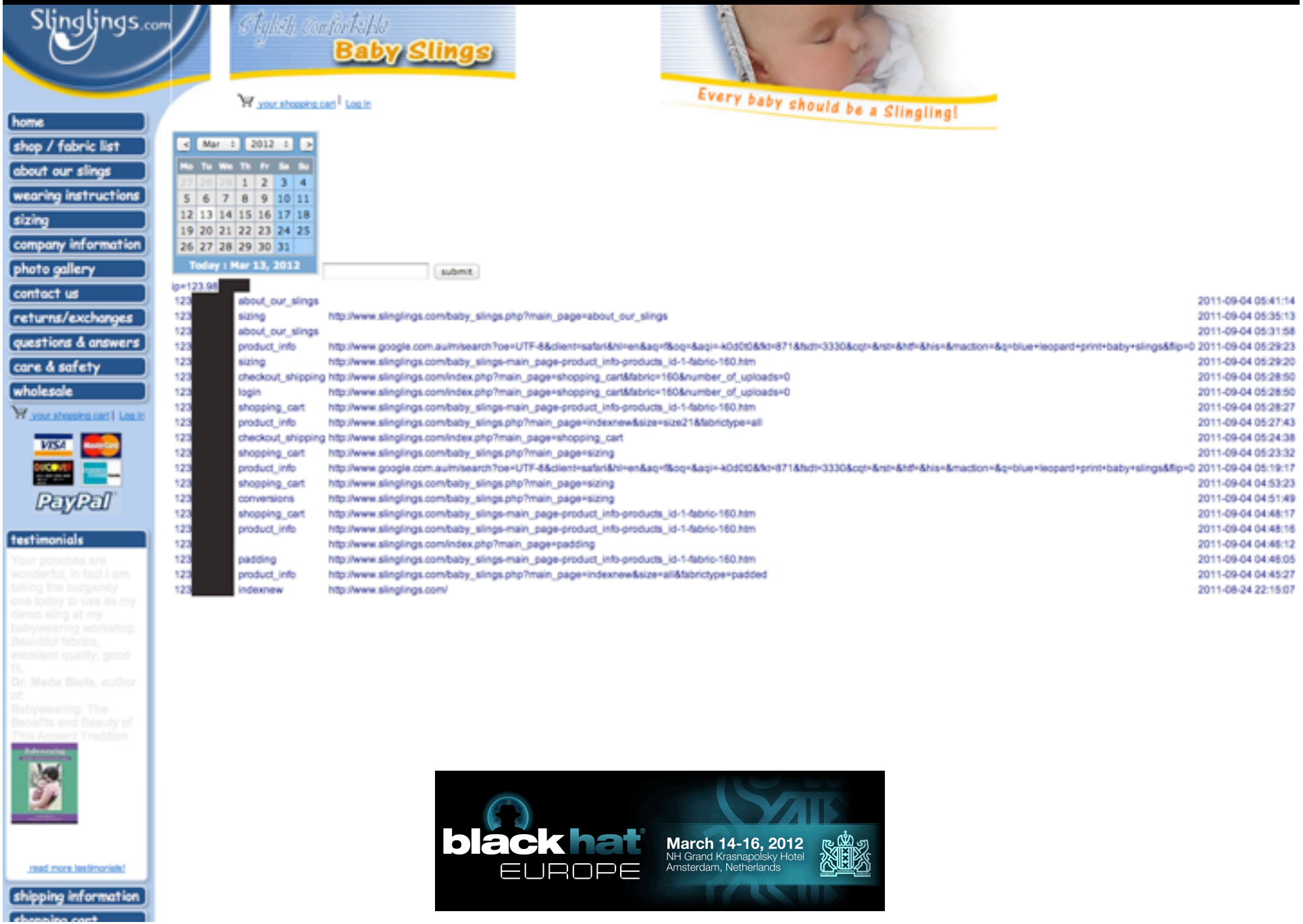
AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all ...
www.steelrod.com.au/**awstats**/data/**awstats**112011.steelrod.com.au.txt
AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all statistics for ..... 1 2 12908 20111110015106 **123**[redacted] 1 6 178243 20111117032811 ...

AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all ...
www.swanplastics.com.au/**awstats**/.../**awstats**102011.swanplastics.com...
AWSTATS DATA FILE 6.8 (build 1.910) # If you remove this file, all statistics for ..... 1 1 13187 20111009165853 **123**[redacted] 2 40 264038 20111026050205 ...

AWSTATS DATA FILE 6.9 (build 1.925) # If you remove this file, all ...
tabten.org/**awstats**/**awstats**022012.dtc.txt
AWSTATS DATA FILE 6.9 (build 1.925) # If you remove this file, all statistics for ..... 8 8 955956 20120220171600 **123.**[redacted] 6 6 1054976 20120220154031 ...

AWSTATS DATA
www.hi.net.au/**awstat**
AWSTATS DATA FIL
94804 201203021813

AWSTATS DATA


Slinglings.com
Stylish Comfortable
Baby Slings
your shopping cart | Log In
Every baby should be a Slingling!
home
shop / fabric list
about our slings
wearing instructions
sizing
company information
photo gallery
contact us
returns/exchanges
questions & answers
care & safety
wholesale
your shopping cart | Log In
VISA
DISCOVER
PayPal
testimonials
Your pouches are wonderful, in fact I am taking the burgandy one today to use as my demo sling at my babywearing workshop. Beautiful fabrics, excellent quality, good fit.
Dr. Maria Blois, author of: Babywearing: The Benefits and Beauty of This Ancient Tradition
read more testimonials!
shipping information
Mar
2012
Mo Tu We Th Fr Sa Su
Today : Mar 13, 2012
submit
ip=123.98
about_our_slings 2011-09-04 05:41:14
sizing http://www.slinglings.com/baby_slings.php?main_page=about_our_slings 2011-09-04 05:35:13
about_our_slings 2011-09-04 05:31:58
product_info http://www.google.com.au/m/search?oe=UTF-8&client=safari&hl=en&aq=f&oq=&aqi=-k0d0t0&kt=871&fsdt=3330&cqt=&nst=&htf=&his=&maction=&q=blue+leopard+print+baby+slings&flip=0 2011-09-04 05:29:23
sizing http://www.slinglings.com/baby_slings-main_page-product_info-products_id-1-fabric-160.htm 2011-09-04 05:29:20
checkout_shipping http://www.slinglings.com/index.php?main_page=shopping_cart&fabric=160&number_of_uploads=0 2011-09-04 05:28:50
login http://www.slinglings.com/index.php?main_page=shopping_cart&fabric=160&number_of_uploads=0 2011-09-04 05:28:50
shopping_cart http://www.slinglings.com/baby_slings-main_page-product_info-products_id-1-fabric-160.htm 2011-09-04 05:28:27
product_info http://www.slinglings.com/baby_slings.php?main_page=indexnew&size=size21&fabrictype=all 2011-09-04 05:27:43
checkout_shipping http://www.slinglings.com/index.php?main_page=shopping_cart 2011-09-04 05:24:38
shopping_cart http://www.slinglings.com/baby_slings.php?main_page=sizing 2011-09-04 05:23:32
product_info http://www.google.com.au/m/search?oe=UTF-8&client=safari&hl=en&aq=f&oq=&aqi=-k0d0t0&kt=871&fsdt=3330&cqt=&nst=&htf=&his=&maction=&q=blue+leopard+print+baby+slings&flip=0 2011-09-04 05:19:17
shopping_cart http://www.slinglings.com/baby_slings.php?main_page=sizing 2011-09-04 04:53:23
conversions http://www.slinglings.com/baby_slings.php?main_page=sizing 2011-09-04 04:51:49
shopping_cart http://www.slinglings.com/baby_slings-main_page-product_info-products_id-1-fabric-160.htm 2011-09-04 04:48:17
product_info http://www.slinglings.com/baby_slings-main_page-product_info-products_id-1-fabric-160.htm 2011-09-04 04:48:16
http://www.slinglings.com/index.php?main_page=padding 2011-09-04 04:46:12
padding http://www.slinglings.com/baby_slings-main_page-product_info-products_id-1-fabric-160.htm 2011-09-04 04:46:05
product_info http://www.slinglings.com/baby_slings.php?main_page=indexnew&size=all&fabrictype=padded 2011-09-04 04:45:27
indexnew http://www.slinglings.com/ 2011-08-24 22:15:07
black hat EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

VPN PROVIDING INTERNET SERVICES SINCE 1995

StrongVPN Accounts Allow You Access To Over
6959 IP's on **283 servers** in **19 countries** around the world

HOME | ABOUT US | SETUP HOWTO | FAQ | WHY VPN? | FORUM | ORDER | CONTACT US | PACKAGES

What country do you want our next VPN server to be in?

Korea
29%

Ireland
14%

Australia
36%

Brazil
21%

Total votes: 16040

What country do you want our next VPN server to be in?

View | Votes

This table lists all the recorded votes for this poll. If anonymous users are allowed to vote, they will be identified by the IP address of the computer they used when they voted.

Visitor	Vote	Timestamp
80	Australia	Wed, 09/14/2011 - 12:15
60	Australia	Wed, 09/14/2011 - 15:48
10	Australia	Wed, 09/14/2011 - 16:14
21	Australia	Wed, 09/14/2011 - 19:58
87	Australia	Wed, 09/14/2011 - 21:06
20	Australia	Wed, 09/14/2011 - 22:40
83	Australia	Wed, 09/14/2011 - 23:02
2.6	Australia	Wed, 09/14/2011 - 23:48
41	Australia	Thu, 09/15/2011 - 01:23
20	Australia	Thu, 09/15/2011 - 03:29
13	Australia	Thu, 09/15/2011 - 03:41
66	Australia	Thu, 09/15/2011 - 06:06
11	Australia	Thu, 09/15/2011 - 11:18
11	Australia	Thu, 09/15/2011 - 11:29
12	Australia	Thu, 09/15/2011 - 12:09
17		
50		
12		
11		
79		

114 | 115 | 116 | 117

Moral of the story...

Moral of the Story

- In both cases IDS alerts can be investigated quickly through a joined query.
- Joining Snort Source IP with p0f, http and torrent data provides additional context.
- Torrent data provides triangulation when matched to user-agent information.
- Didn't justify a query of all connections, sessions, protocols and files for these sources.

What about TOR?

TOR

- Track TOR Exit Gateways every hour.
- Record every IP address with Geo information
- Correlate TOR Gateway addresses with sources of attack on the network.

TOR Results


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Future Features

- Statistical Analysis
- Machine Learning.
- Loaders for more NSM tools.
- Sentiment Analysis
- Build Lucene search indexes.

Questions?


black hat
EUROPE
March 14-16, 2012
NH Grand Krasnapolsky Hotel
Amsterdam, Netherlands

Feedback Forms

Information

- Packetpig
  - https://github.com/packetloop/packetpig
  - @packetpig on twitter.
- Packetloop
  - www.packetloop.com
  - @packetloop on twitter.
  - blog.packetloop.com