TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

PROFILING SSL AND ATTRIBUTING PRIVATE NETWORKS

An introduction to FLYING PIG and HUSH PUPPY

ICTR - Network Exploitation
GCHQ

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Motivations for FLYING P

NETWORK
EXPLOITATION

More and more services used by GCHQ targets
TLS/SSL to increase user confidence, e.g. Hotm

Terrorists and cyber criminals are common use
their comms (not necessarily using the big pro

SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

ations for FLYING PIG

NETWORK EXPLOITATION

re services used by GCHQ targets are moving to
ncrease user confidence, e.g. Hotmail, Yahoo, Gmai

nd cyber criminals are common users of TLS/SSL to
s (not necessarily using the big providers).

Query by certificate metadata

FLYING PIG

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Query by certificate metadata



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

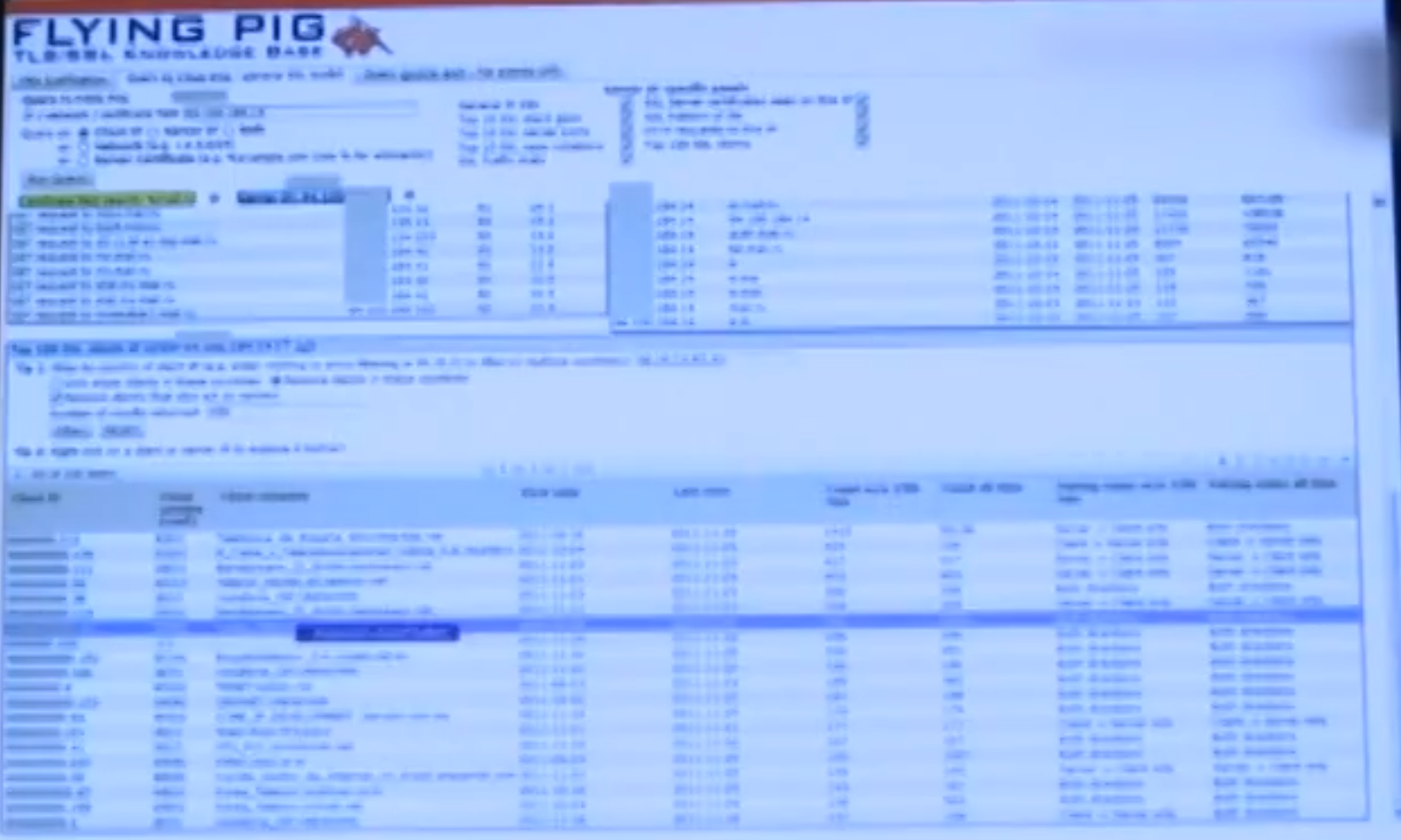
Query by server IP

Query by server IP



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

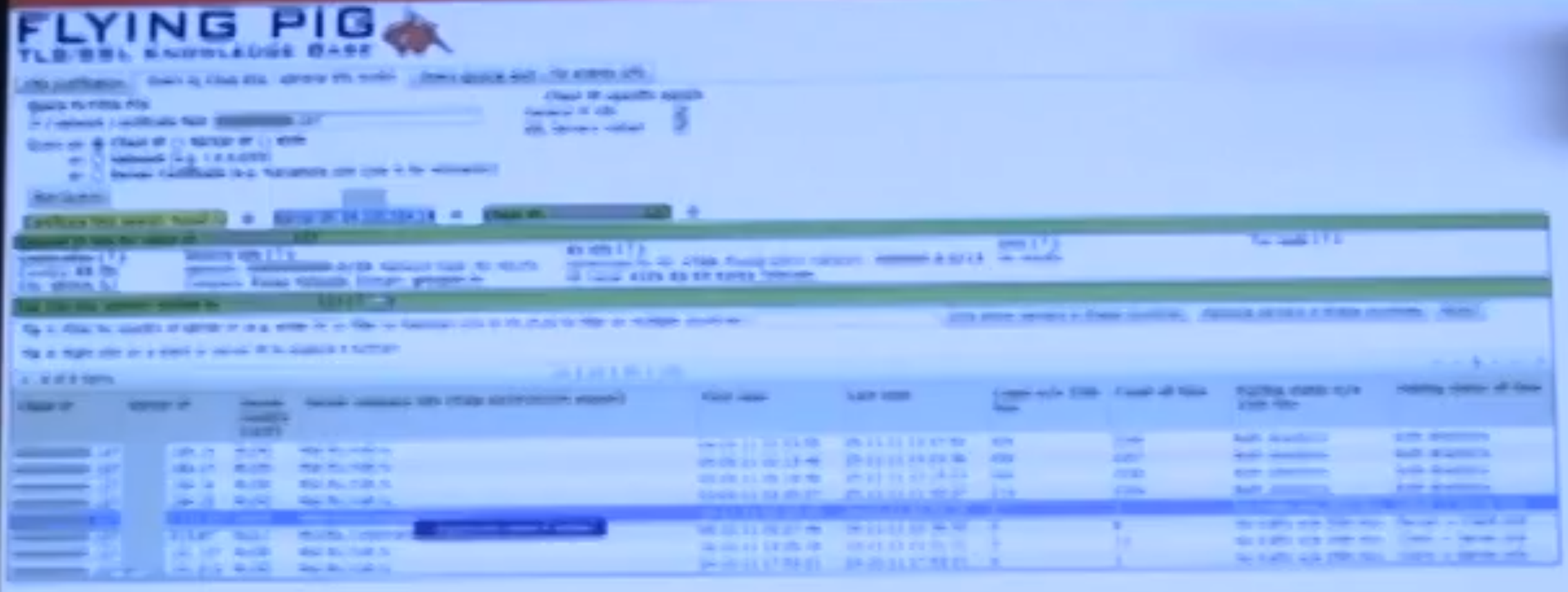
Query by server IP



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Query by client IP



TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

Query by ne

YING PIG

SSL KNOWLEDGE BASE

Query FLYING PIG - general SSL toolkit | Query QUICK ANT - Tor events QFD

network-specific panels

VING PIG

ork / certificate field 0/24

Client IP Server IP Both

Network (e.g. 1.2.3.0/24)

Server Certificate (e.g. %.example.com (use % for wildcards))

General network info

SSL Clients present in network

SSL Servers present in network

HTTP requests to IPs in network

ery!

Server IP: 94.100.184.14

Client IP:

0/24

WHOIS info (?):

Network: No results. Network type: No results.

Company: No results. Domain: No results.

AS info (

Advertise

AS name

0/24: (?):

ght click on a client IP to explore it further!

10 | 25 | 50 | 100

57 items

Client company info (from GEOFUSION export)

First se

2011-0

Cyber app

iginotar certificate
uthority compromise :

Private keys of legitimate certificate
authority, Diginotar, stolen by hacker.

FLYING PIG was used to identify a Fl

How the attack was done:



ation using SSL have been fou

LEGION JADE, LEGION RUBY,

n FLYING PIG using known sig

Results - what do we find?

- Foreign government networks
- Airlines
- Energy companies
- Financial organisations

- In cases of good collection, 50-80% of collected private network traffic has been attributed

- Some false positives can arise if few events correlated, due to factors such as TDIs not being completely unique and public internet proxies giving misleading public IP results

- Results can frequently be verified using Kerberos etc data