



How do we do SIGDEV on private networks?

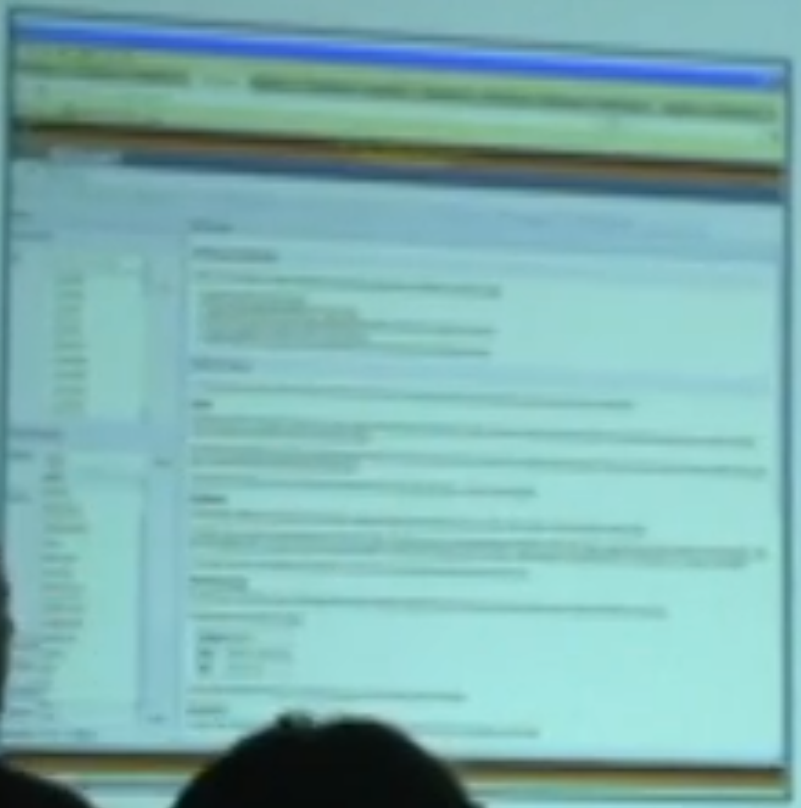
Private Networks are Important

- Many targets use private networks.

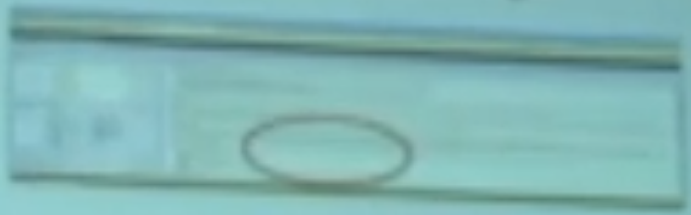
Google infrastructure	SWIFT Network
French MFA	
	Petrobras

- Evidence in Survey: 30%-40% of traffic in BLACKPEARL has at least one endpoint private.

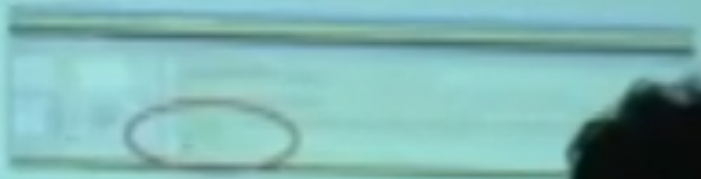
New Analytics for ROYALNET



- Find network features related to your target's netstrings:



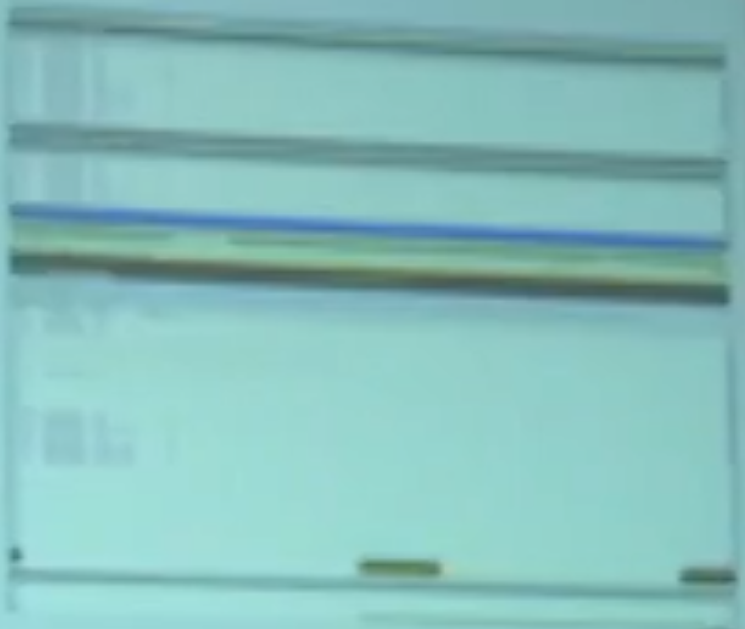
- Find links likely to carry your target's traffic:



SECRET//SI//REL TO USA, FVEY

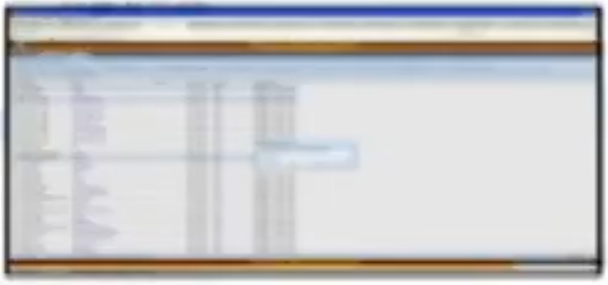
Find Related Links

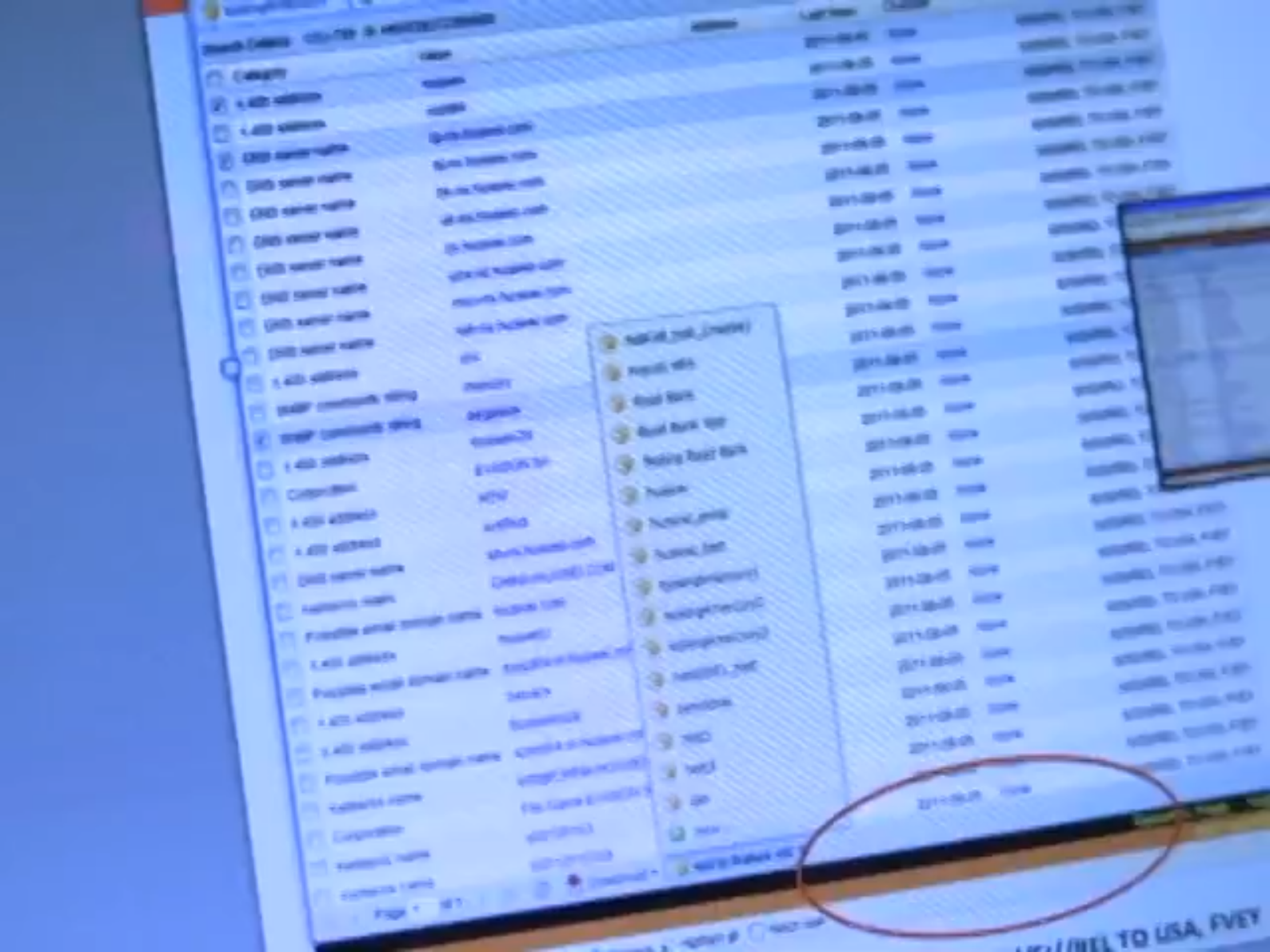


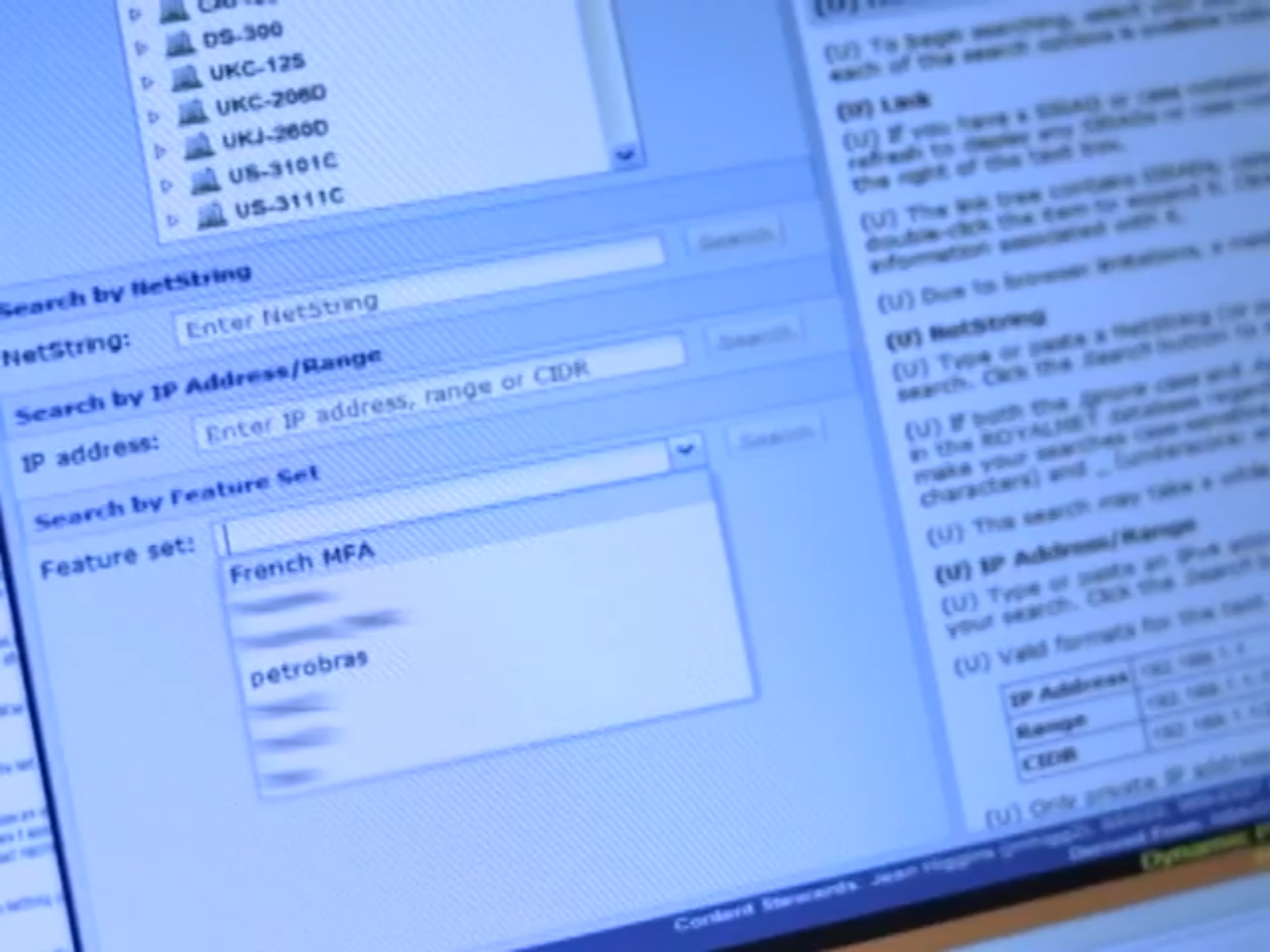


These [illegible]ely to carry Huawei traffic.

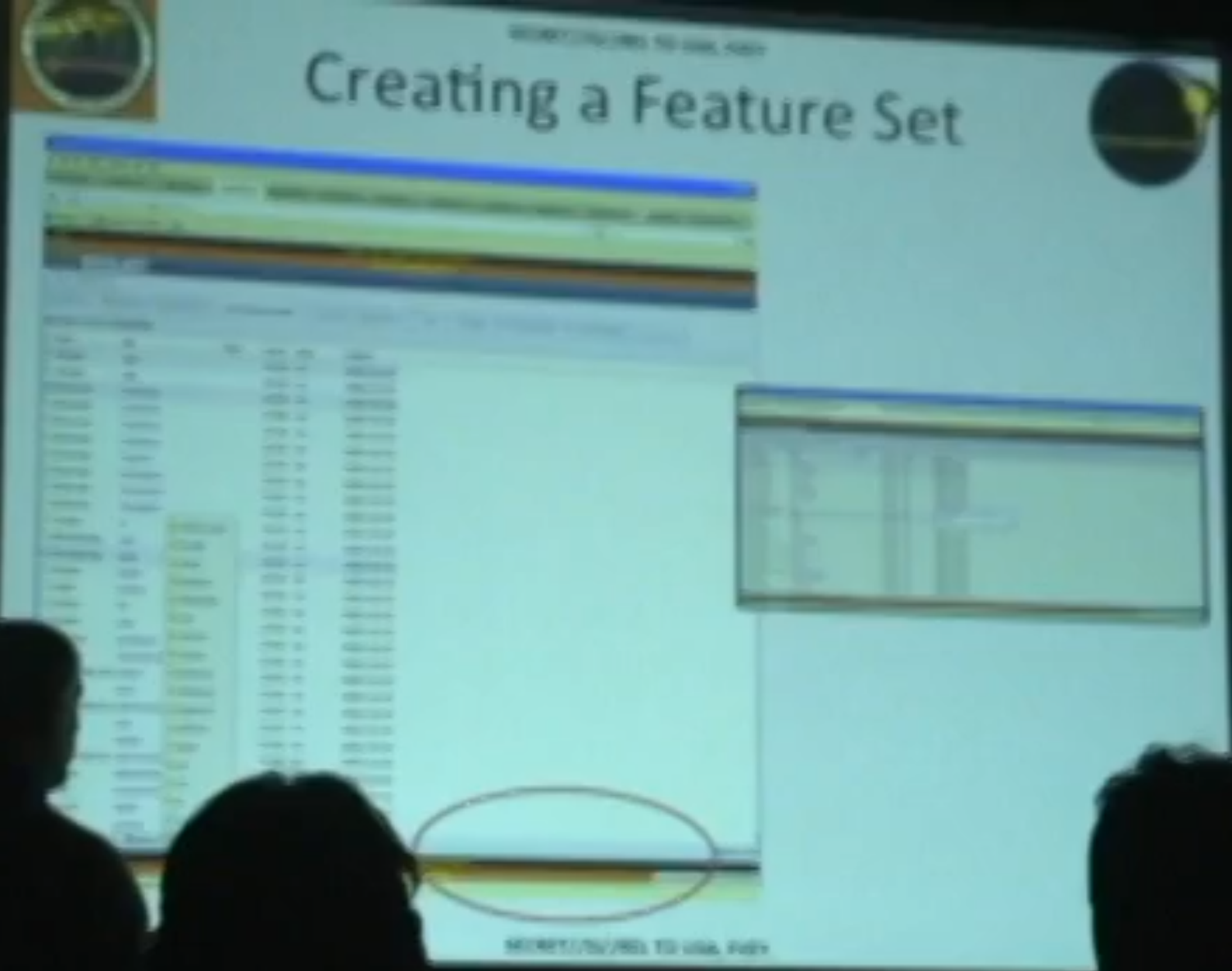
Creating a Feature Set



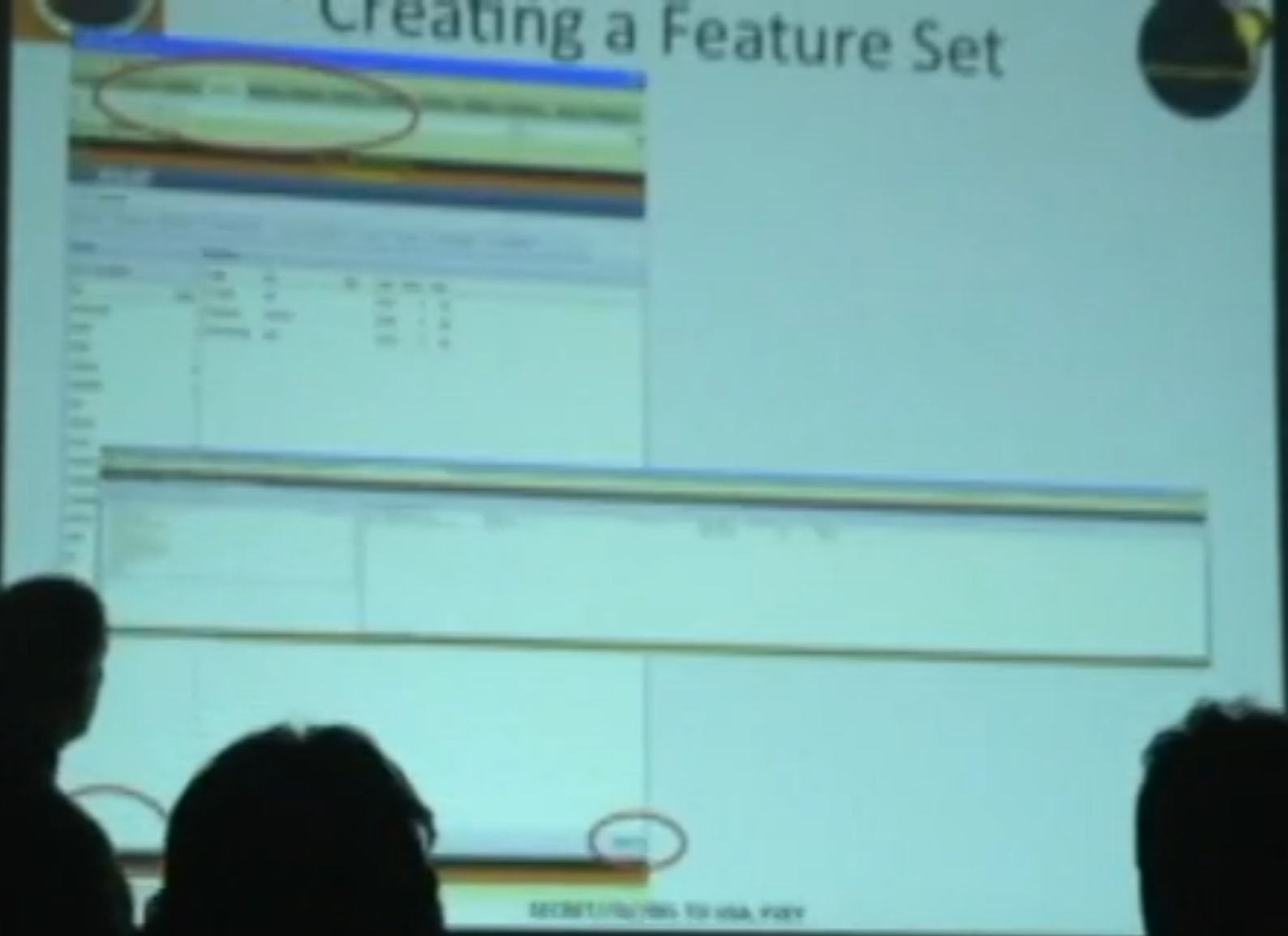


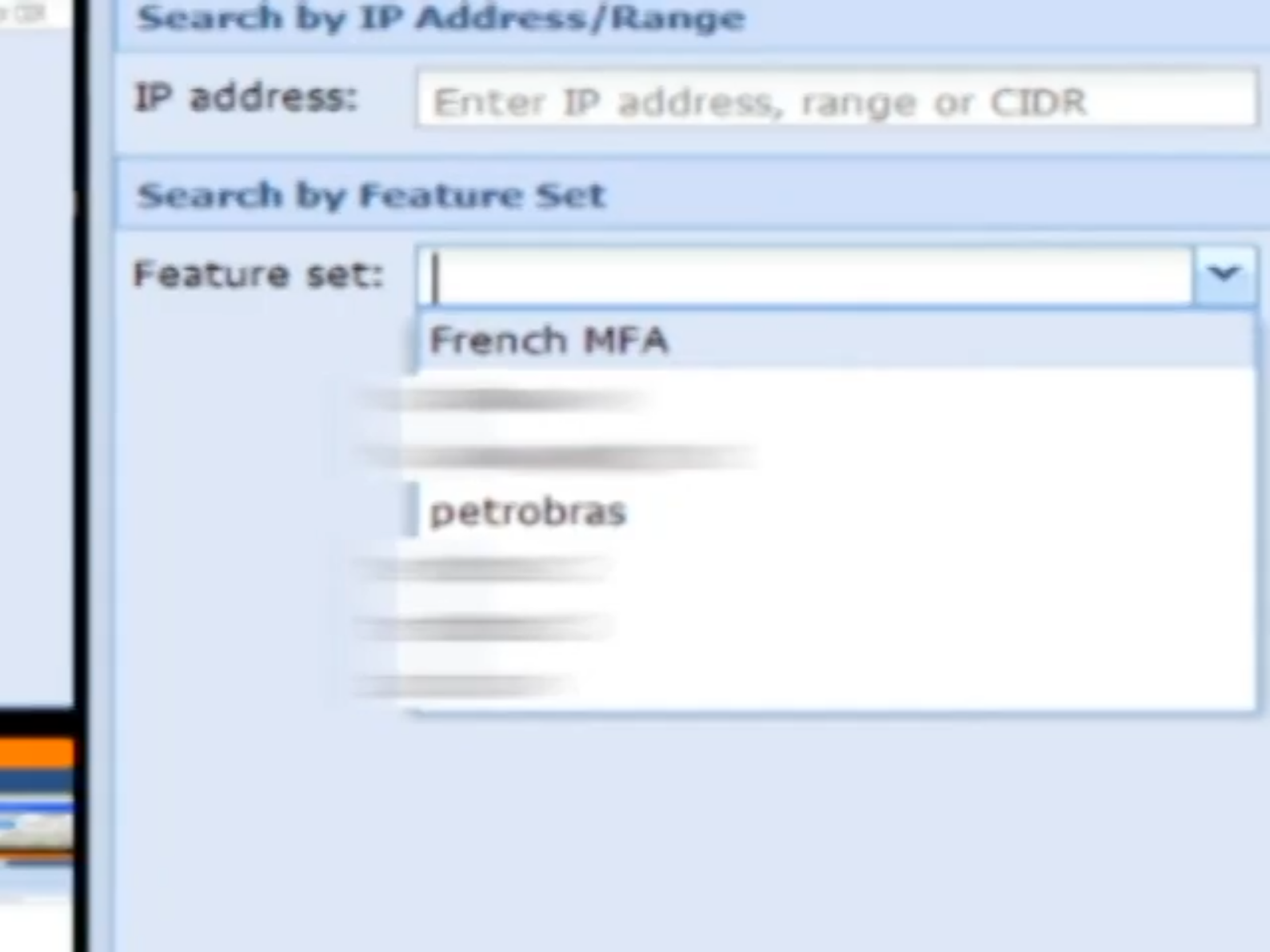

DS-300
UKC-125
UKC-206D
UKJ-260D
US-3101C
US-3111C
Search by NetString
NetString:
Enter NetString
Search by IP Address/Range
IP address:
Enter IP address, range or CIDR
Search by Feature Set
Feature set:
French MFA
petrobras
(U) Link
(U) NetString
(U) IP Address/Range
IP Address
Range
CIDR

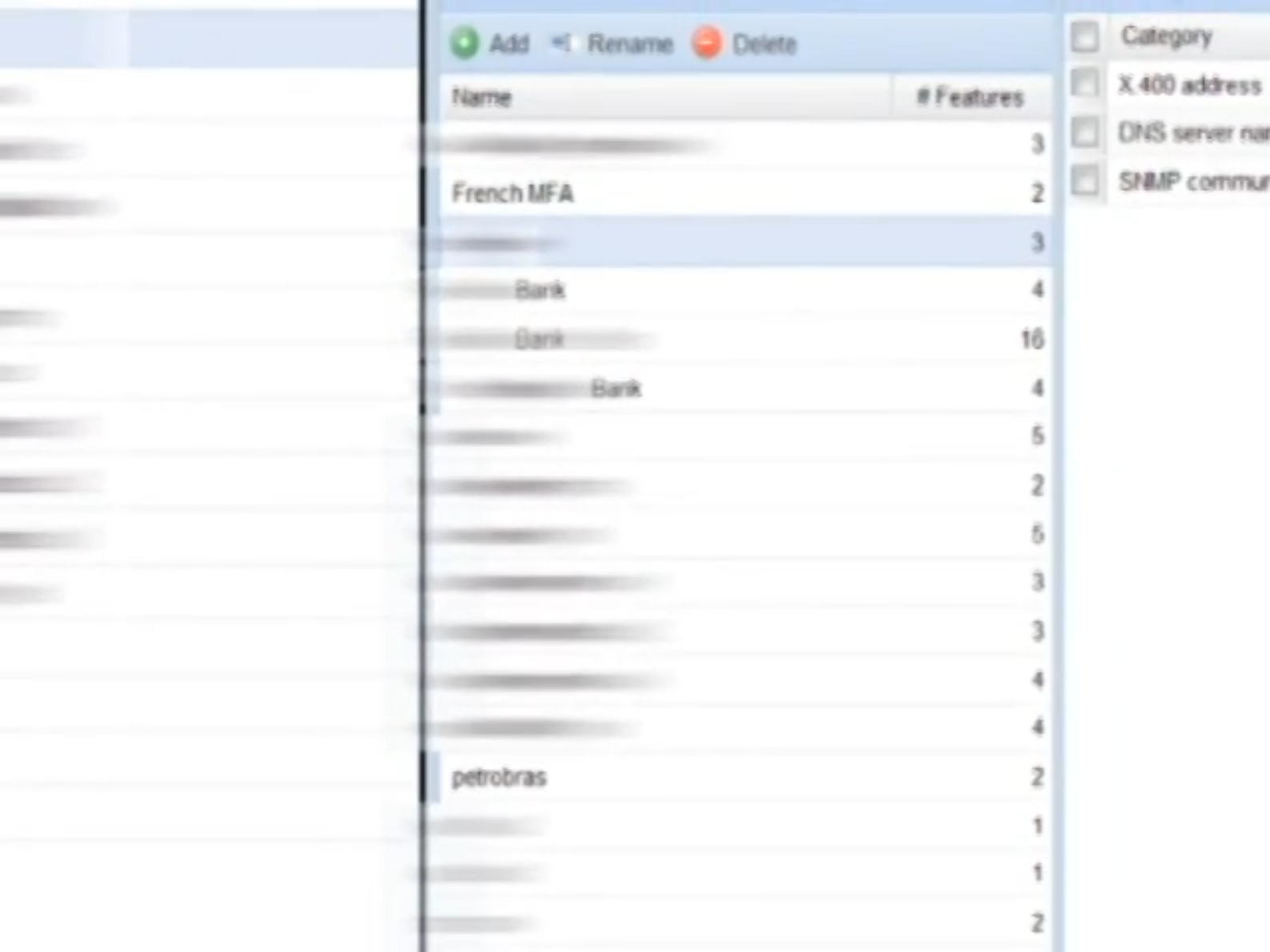
Creating a Feature Set

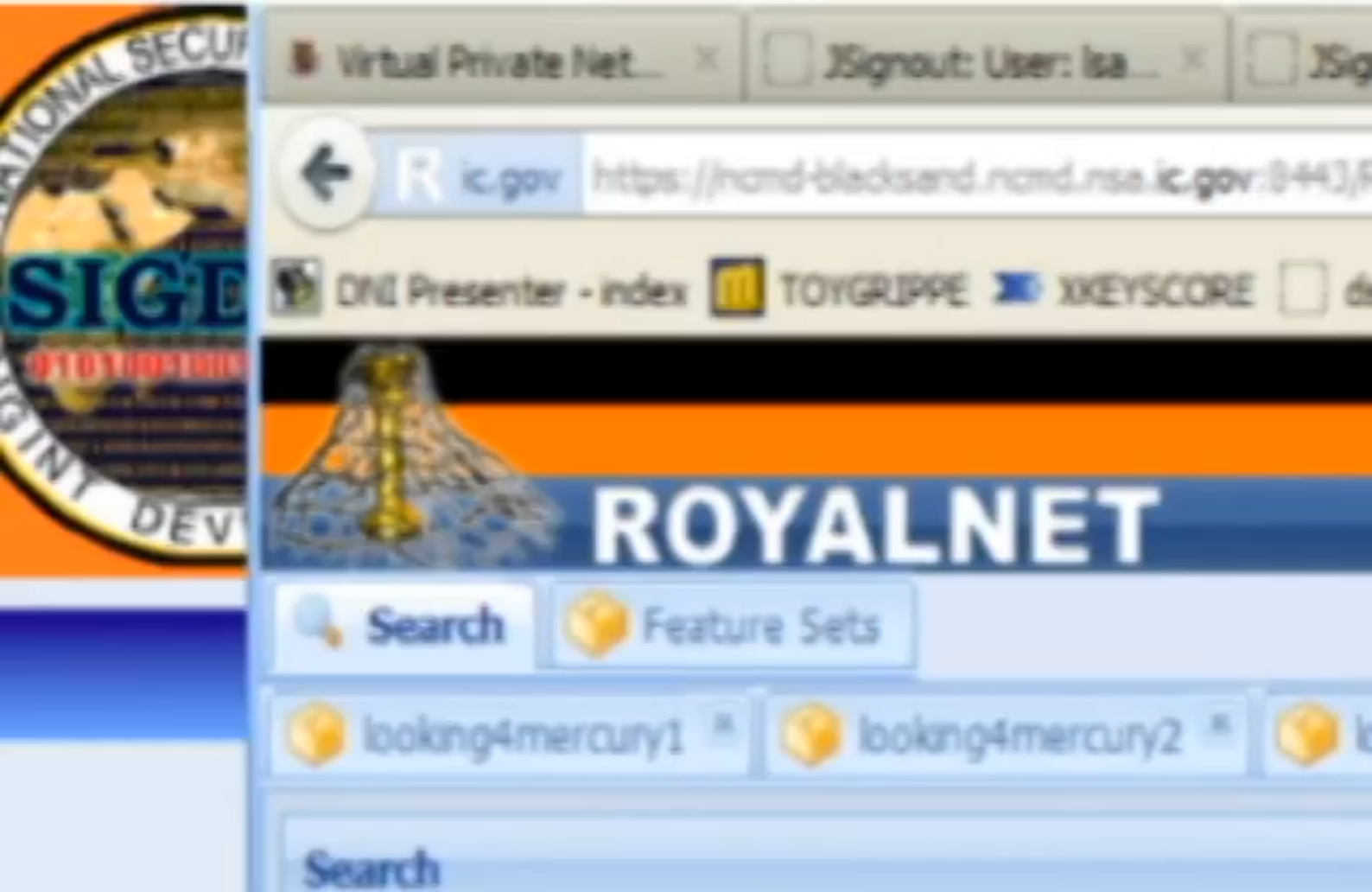


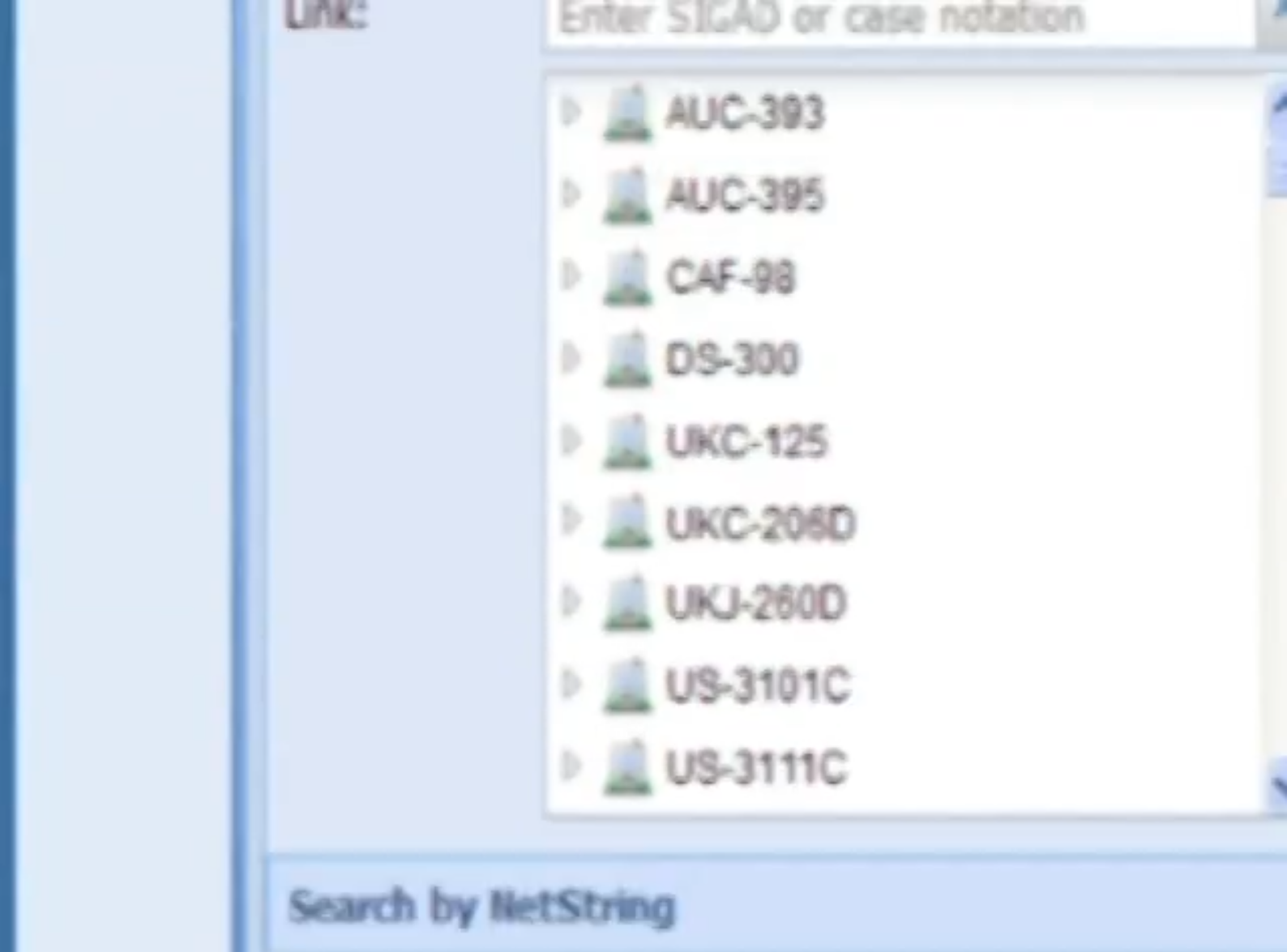
Creating a Feature Set

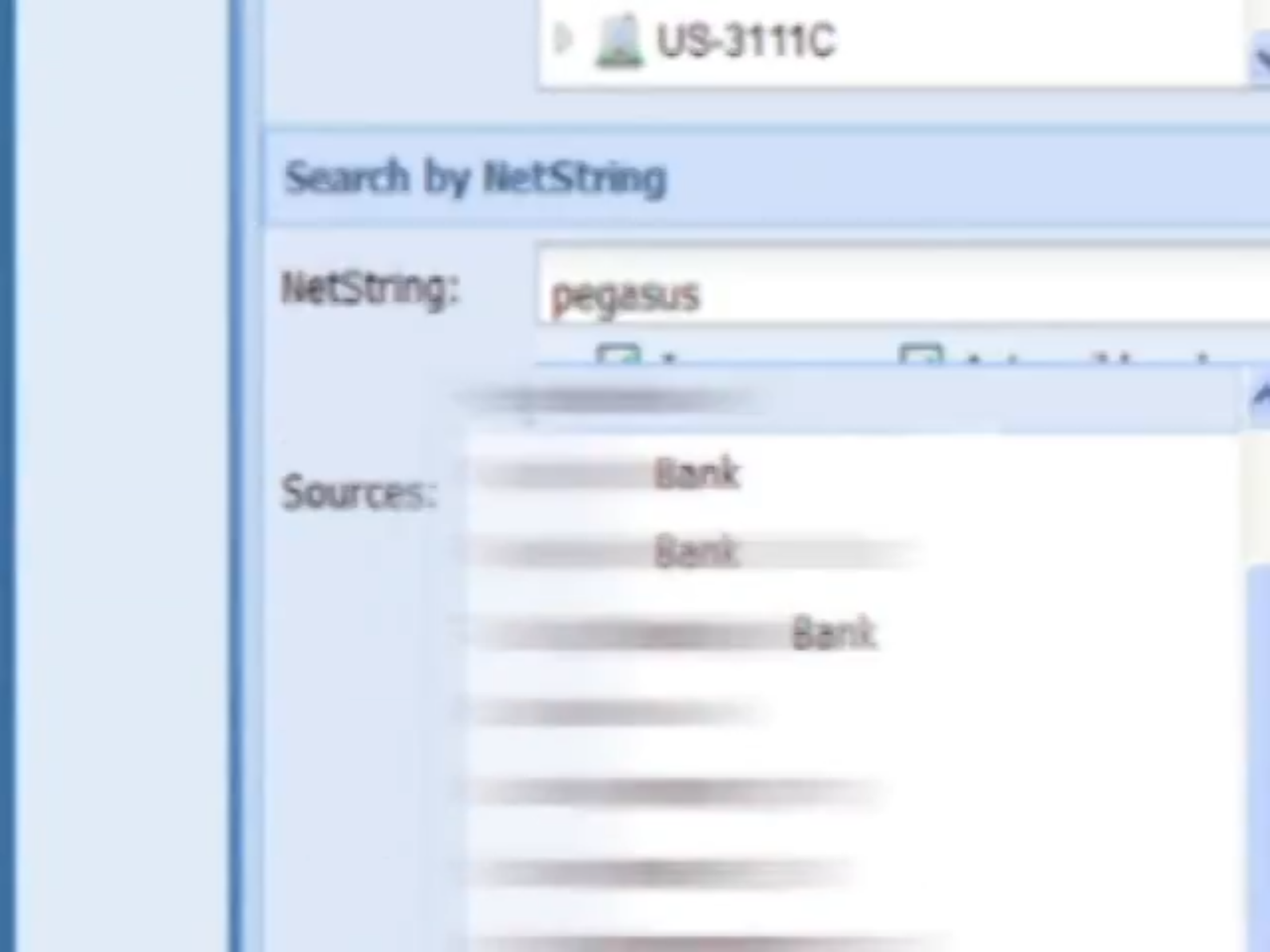


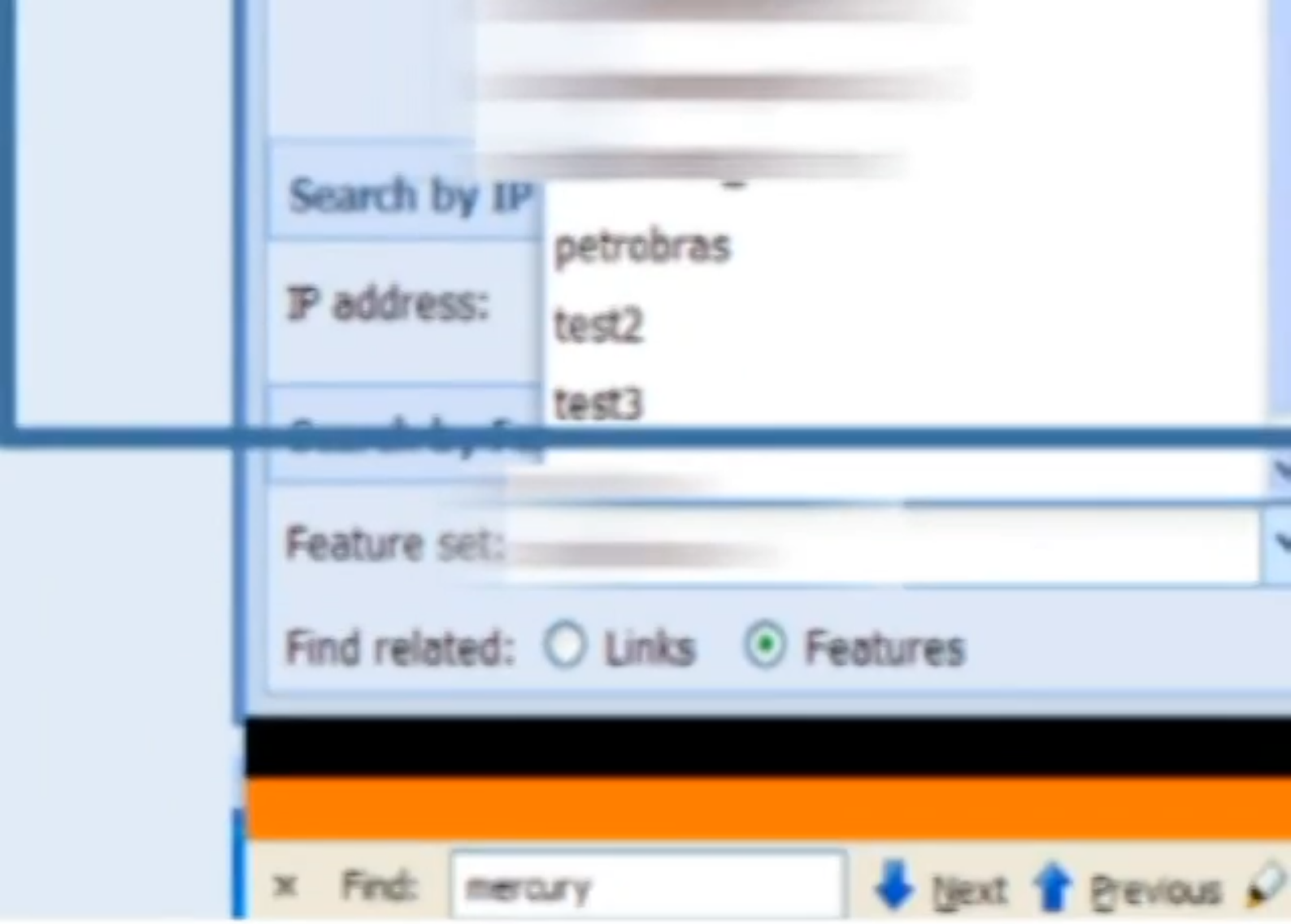

Search by IP Address/Range
IP address:
Enter IP address, range or CIDR
Search by Feature Set
Feature set:
French MFA
petrobras


Add
Rename
Delete
Name
Features
French MFA
Bank
Bank
Bank
petrobras
Category
X.400 address
DNS server nar
SNMP commur


Virtual Private Net...
JSignout: User: lsa...
ic.gov
https://nsnd-blacksand.nsnd.nsa.ic.gov:8443/
DNI Presenter - index
TOYGRIPPE
XKEYSCORE
ROYALNET
Search
Feature Sets
looking4mercury1
looking4mercury2
Search


Enter SIGAD or case notation
AUC-393
AUC-395
CAF-98
DS-300
UKC-125
UKC-206D
UKJ-260D
US-3101C
US-3111C
Search by NetString

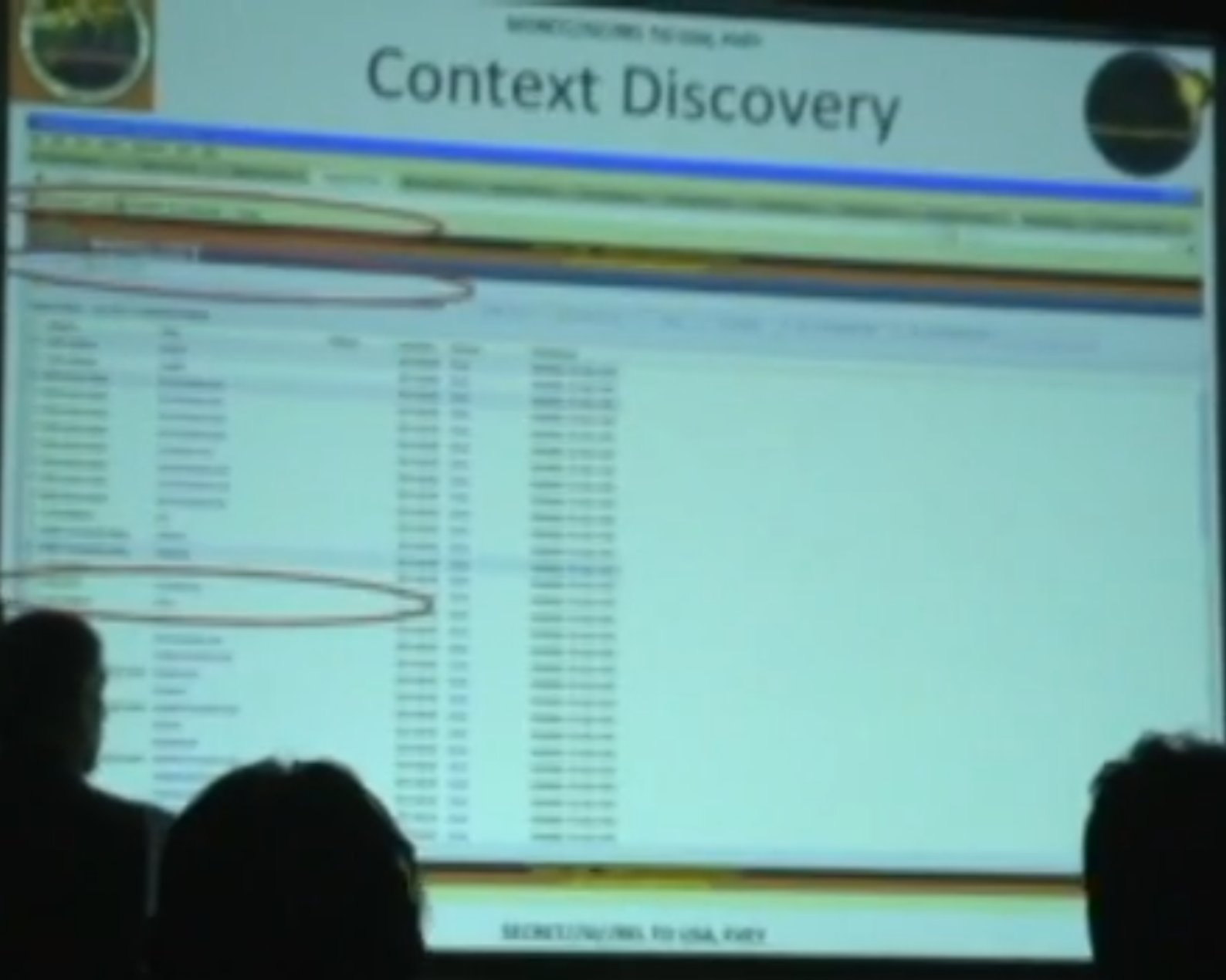

US-3111C
Search by NetString
NetString:
pegasus
Sources:
Bank
Bank
Bank


Search by IP
petrobras
IP address:
test2
test3
Feature set:
Find related:
Links
Features
Find:
mercury
Next
Previous

huawei | huawei_test | Huawei

Address	# Features
	1
10 [redacted] 0	1
	1
10 [redacted] 80	2
	1
10.7 [redacted]	1
10 [redacted] 5	1
	2

	1
10 80	2
	1
10.7	1
10 5	1
	2
	2
10.12	2
10.19 9	1
10	1
	1
16.3	2
.103	2
.106	2


Context Discovery

Realms in Analyst Tools

