(TS//SI//REL)VPN SigDev Basics

[redacted]

S31244 - OTTERCREEK

Overall Classification:

TOP SECRET//COMINT//REL TO USA, FVEY

(U) What is a VPN?

- (U) A Virtual Private Network or VPN is a computer network that uses encryption to securely connect remote users/networks over an otherwise insecure network, usually the public internet.
- (U) Common Types:
  - PPTP, IPSec, SSL
- (U) Public Key Encryption
  - Diffie-Hellman, RSA

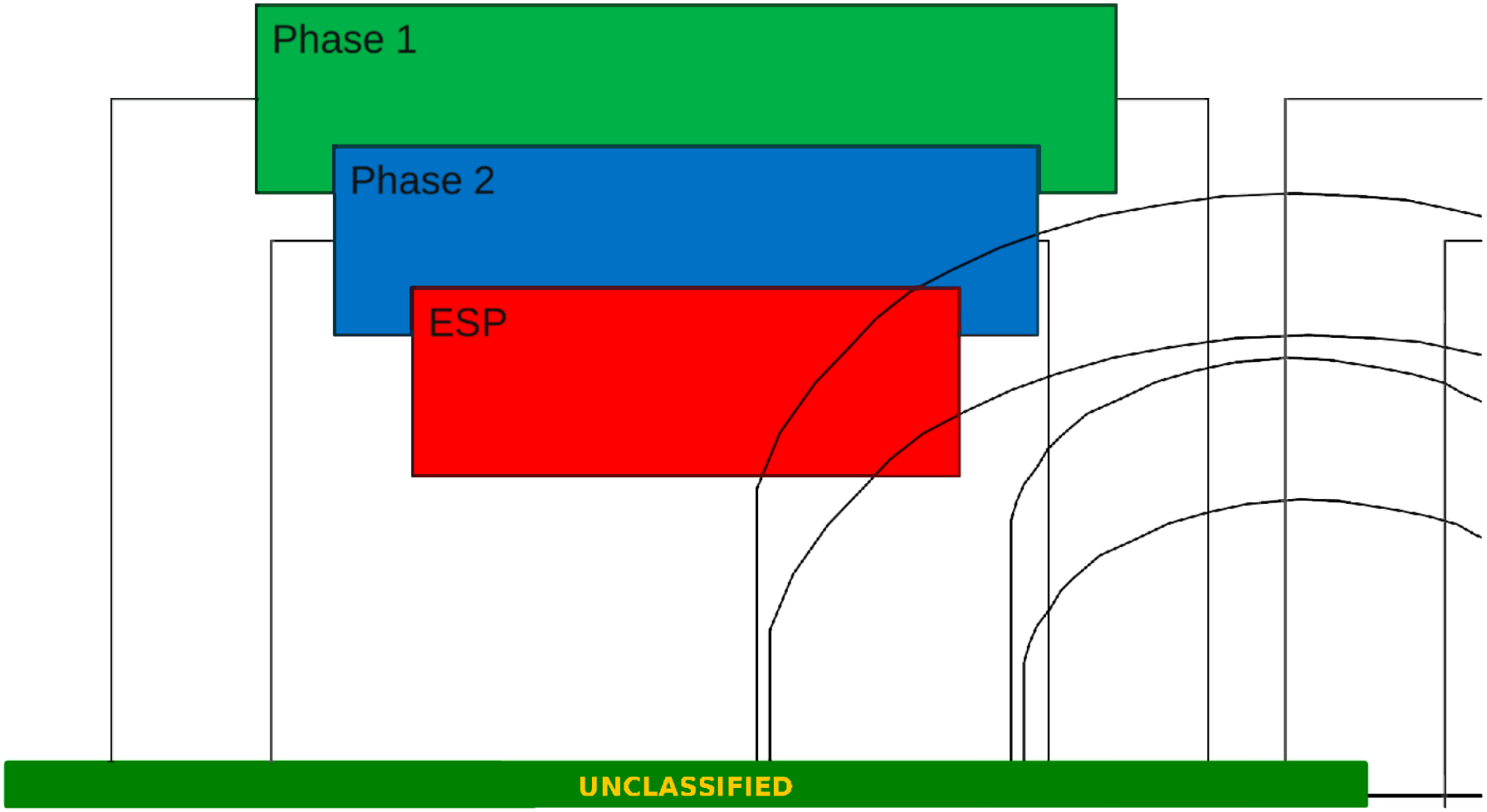
(U) PPTP

- (U) Microsoft Point-to-Point Tunneling Protocol
- (U) Control Channel
  - TCP port 1723
- (U) Data Channel
  - GRE-Next Protocol 47
- (U) RFC 2637, RFC 3078

(U) IPSec

- (U) Authentication
  - Pre-shared key (PSK) or Public key certificates
- (U) ISAKMP/IKE packets are used for key exchange and to establish the secure connection
  - UDP port 500, 4500; TCP port 500
- (U) ESP packets contain the encrypted data
  - IP Next Protocol 50; UDP port 500
- (U) RFC2402, RFC2406, RFC2409, RFC4306, RFC2408

(U) IPSec in a nutshell

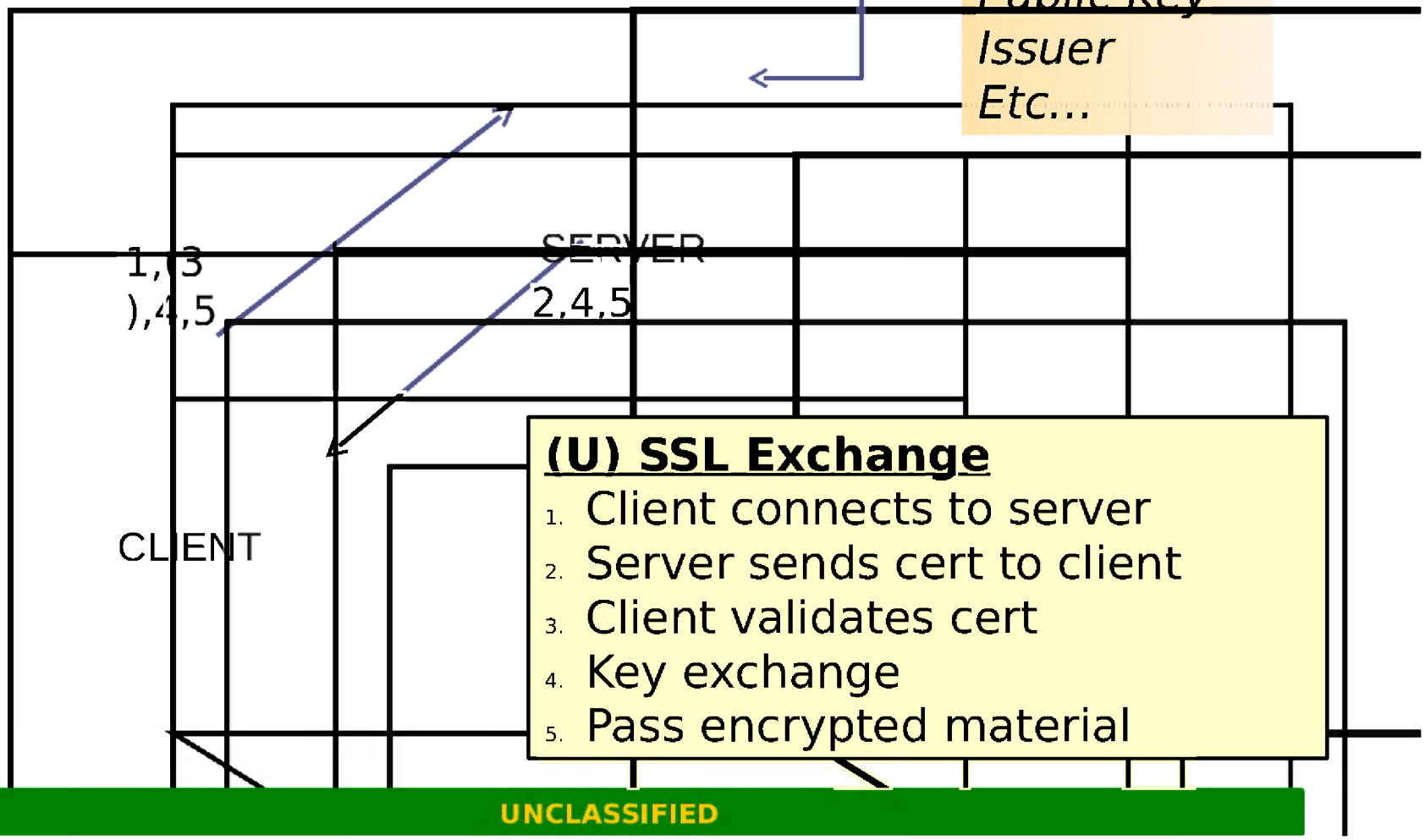


(U) SSL/TLS

- (U) Secure Sockets Layer/Transport Layer Security
- (U) WARNING! e-commerce = tons of uninteresting SSL traffic
- (U) Common ports: TCP ports 443, 995
- (U) RFC2246, RFC4346, RFC5246
  - [redacted]

(U) SSL in a nutshell

Certificate
Subject
Validity
Public Key
Issuer
Etc…



(U) SSL Exchange

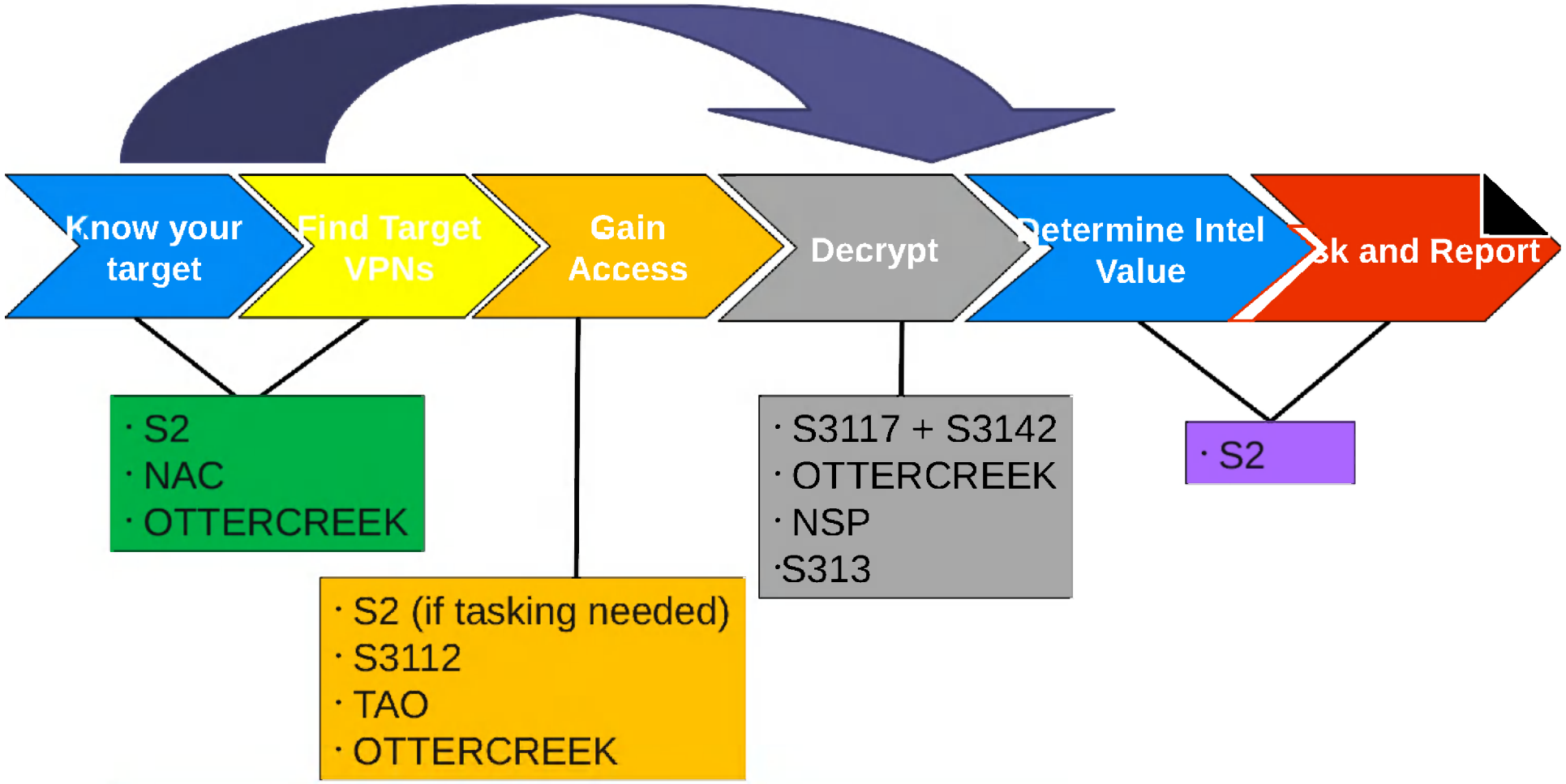
1. Client connects to server
2. Server sends cert to client
3. Client validates cert
4. Key exchange
5. Pass encrypted material

(TS//SI/REL) Who works VPNs?

- (TS//SI//REL) VPN Working Group (go vpn) [redacted]
  - S2, SSG, CES (OTTERCREEK, NSP, S31322, S3117, S3112), TAO, etc.
- (TS//SI//REL) Alias: [redacted]

  (Board alias: [redacted])
- (TS//SI//REL) Meets every other Thursday at 1300

(TS//SI/REL) Who works VPNs?



(TS//SI//REL) So you think your target is using a VPN...

(TS//SI//REL) SigDev Tools

(TS//REL) VPN Specific

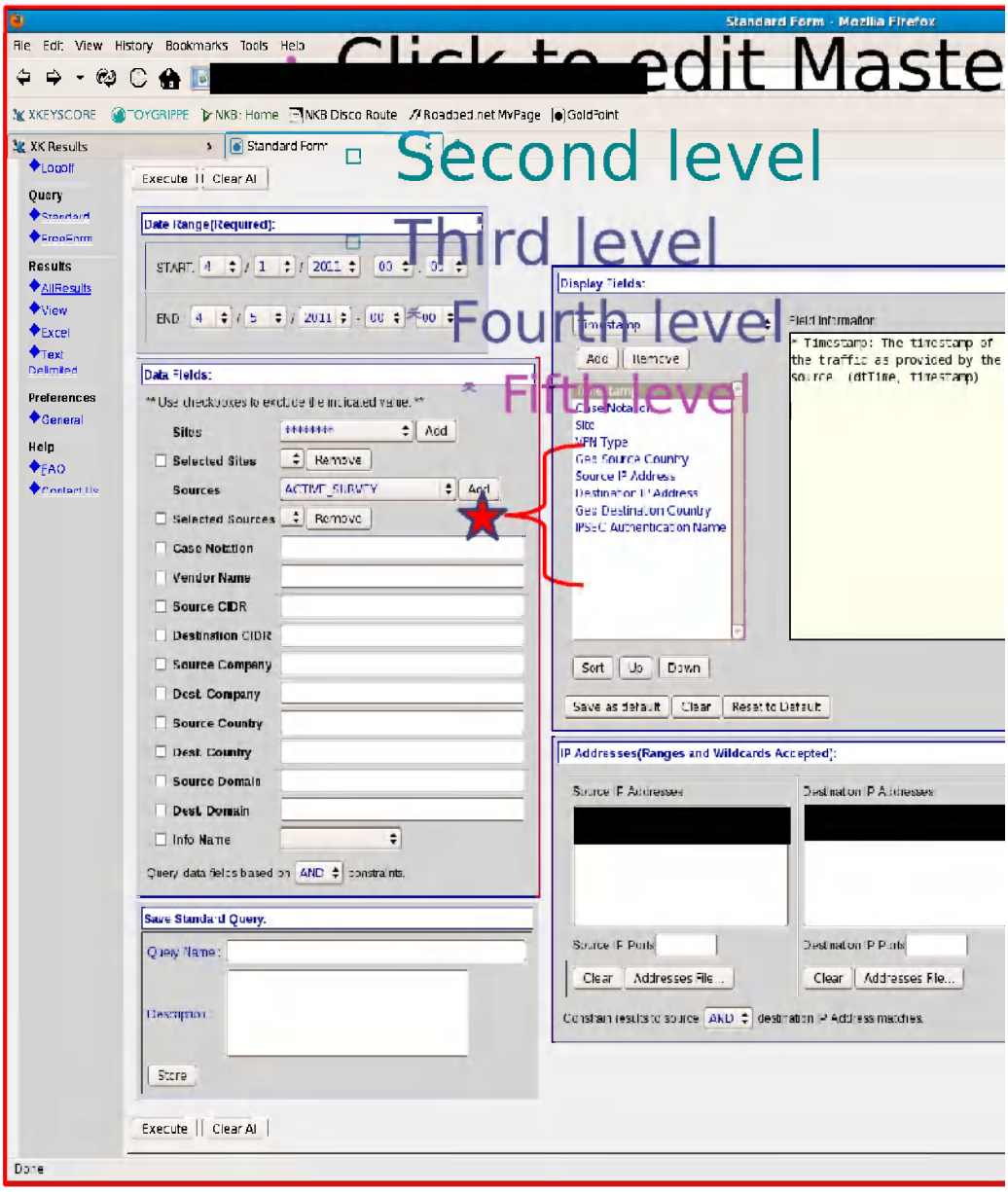
- ~~BLEAKINQUIRY~~
- **DISCOROUTE**
- **TOYGRIPPE**

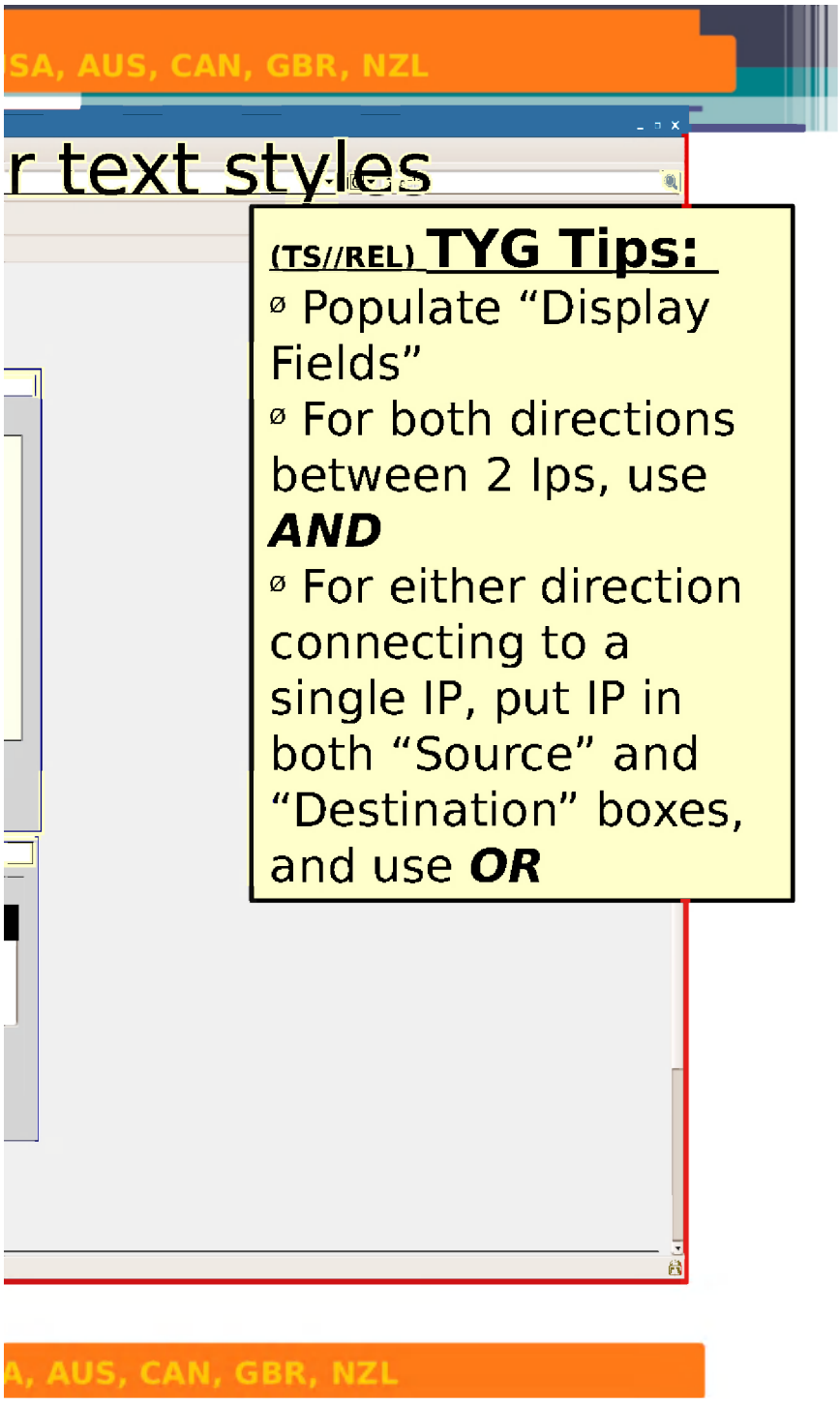
(TS//REL) Also useful

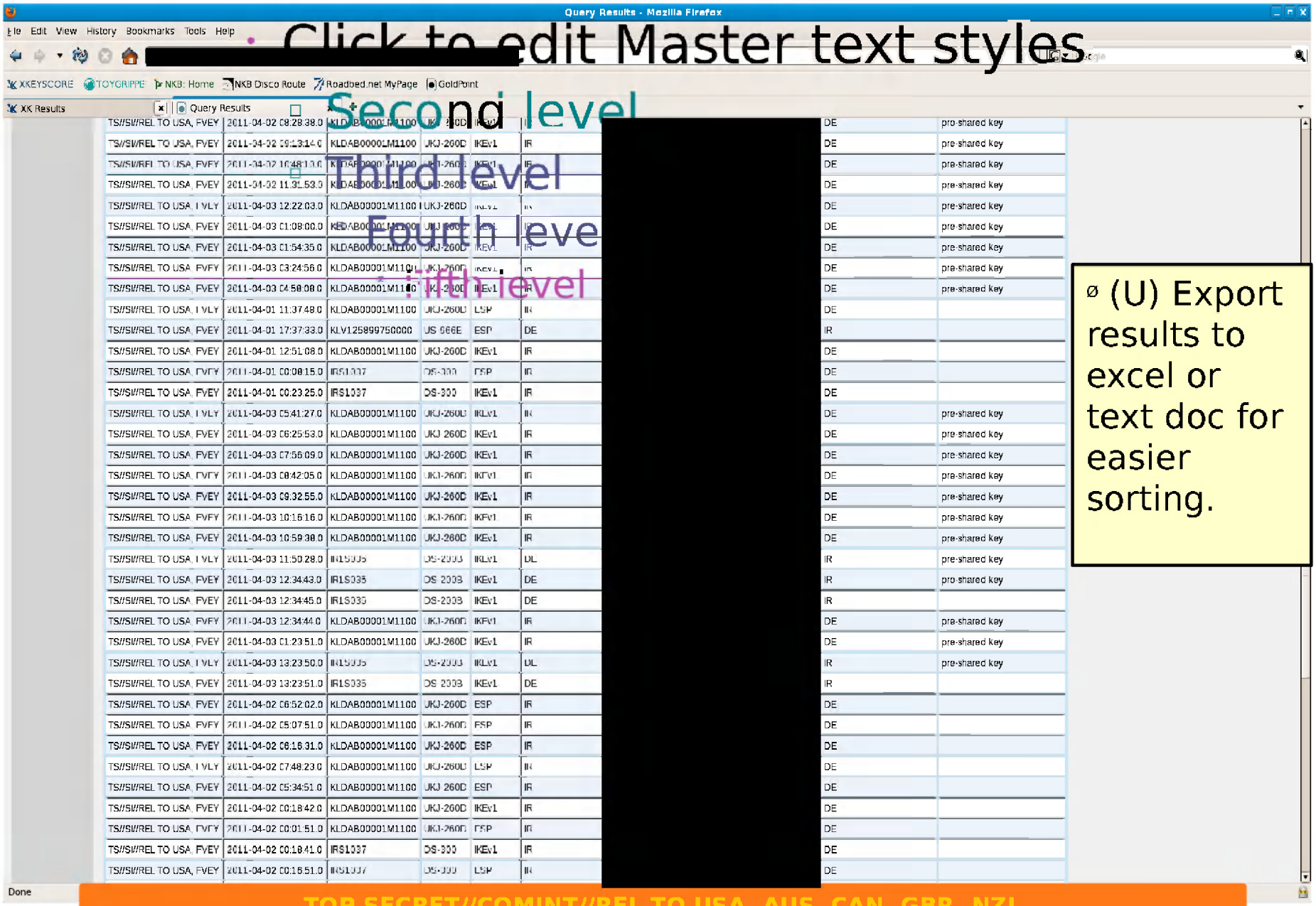
- MARINA
- MASTERSHAKE
- NKB
- PINWALE
- RENOIR
- TREASUREMAP
- TUNINGFORK
- **XKEYSCORE**

(TS//SI//REL) TOYGRIPPE

- (TS//SI//REL) Database of VPN metadata
  - IPSec, PPTP, ViPNet


Standard Form - Mozilla Firefox
Click to edit Maste
Second level
Third level
Fourth level
Fifth level
XKEYSCORE
NKB: Home
NKB Disco Route
Roadbed.net MyPage
GoldPoint
XK Results
Standard Form
Logoff
Query
Standard
FreeForm
Results
AllResults
View
Excel
Text
Delimited
Preferences
General
Help
FAQ
Execute
Clear All
Date Range[Required]:
START: 4 / 1 / 2011 00 : 00
END 4 / 5 / 2011 : 00 : 00
Data Fields:
** Use checkboxes to exclude the indicated value. **
Sites
Add
Selected Sites
Remove
Sources
Selected Sources
Case Notation
Vendor Name
Source CIDR
Destination CIDR
Source Company
Dest. Company
Source Country
Dest. Country
Source Domain
Dest. Domain
Info Name
Query data fields based on AND constraints.
Save Standard Query.
Query Name:
Description:
Store
Display Fields:
Timestamp
Add
Remove
Case Notation
Site
VPN Type
Geo Source Country
Source IP Address
Destination IP Address
Geo Destination Country
IPSEC Authentication Name
Field Information
* Timestamp: The timestamp of the traffic as provided by the source. (dtTime, Timestamp)
Sort
Up
Down
Save as default
Clear
Reset to Default
IP Addresses(Ranges and Wildcards Accepted):
Source IP Addresses
Destination IP Addresses
Source IP Ports
Destination IP Ports
Clear
Addresses File...
Constrain results to source AND destination IP Address matches
Done


SA, AUS, CAN, GBR, NZL
r text styles
(TS//REL) TYG Tips:
ø Populate “Display Fields”
ø For both directions between 2 Ips, use AND
ø For either direction connecting to a single IP, put IP in both “Source” and “Destination” boxes, and use OR
A, AUS, CAN, GBR, NZL



ø (U) Export results to excel or text doc for easier sorting.

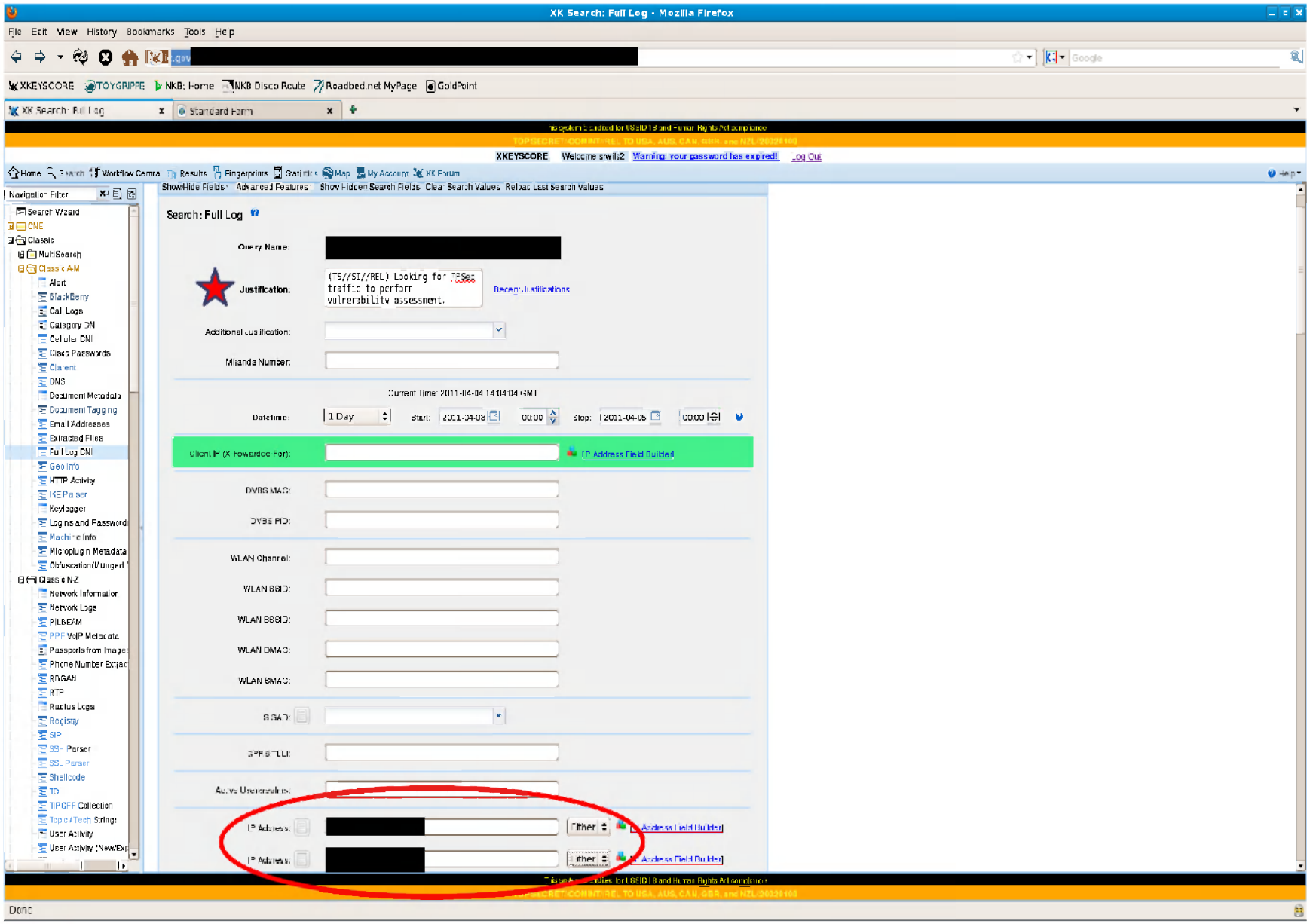
(TS//SI//REL) XKEYSCORE

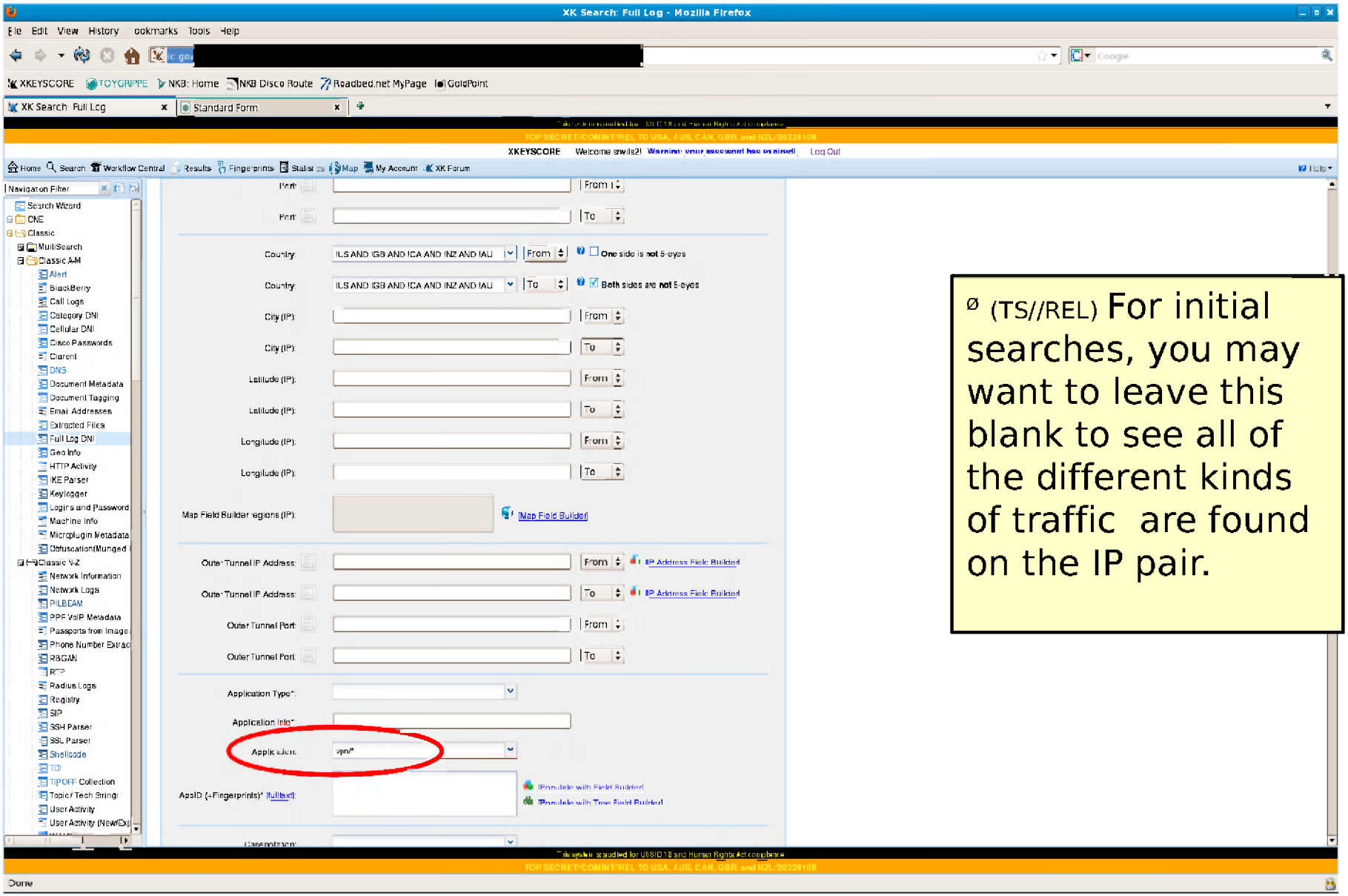
(TS//REL) Fingerprints

- IPSec
  - vpn/esp
  - vpn/isakmp
- PPTP
  - vpn/pptp*
- SSL
  - network_encyption/ssl

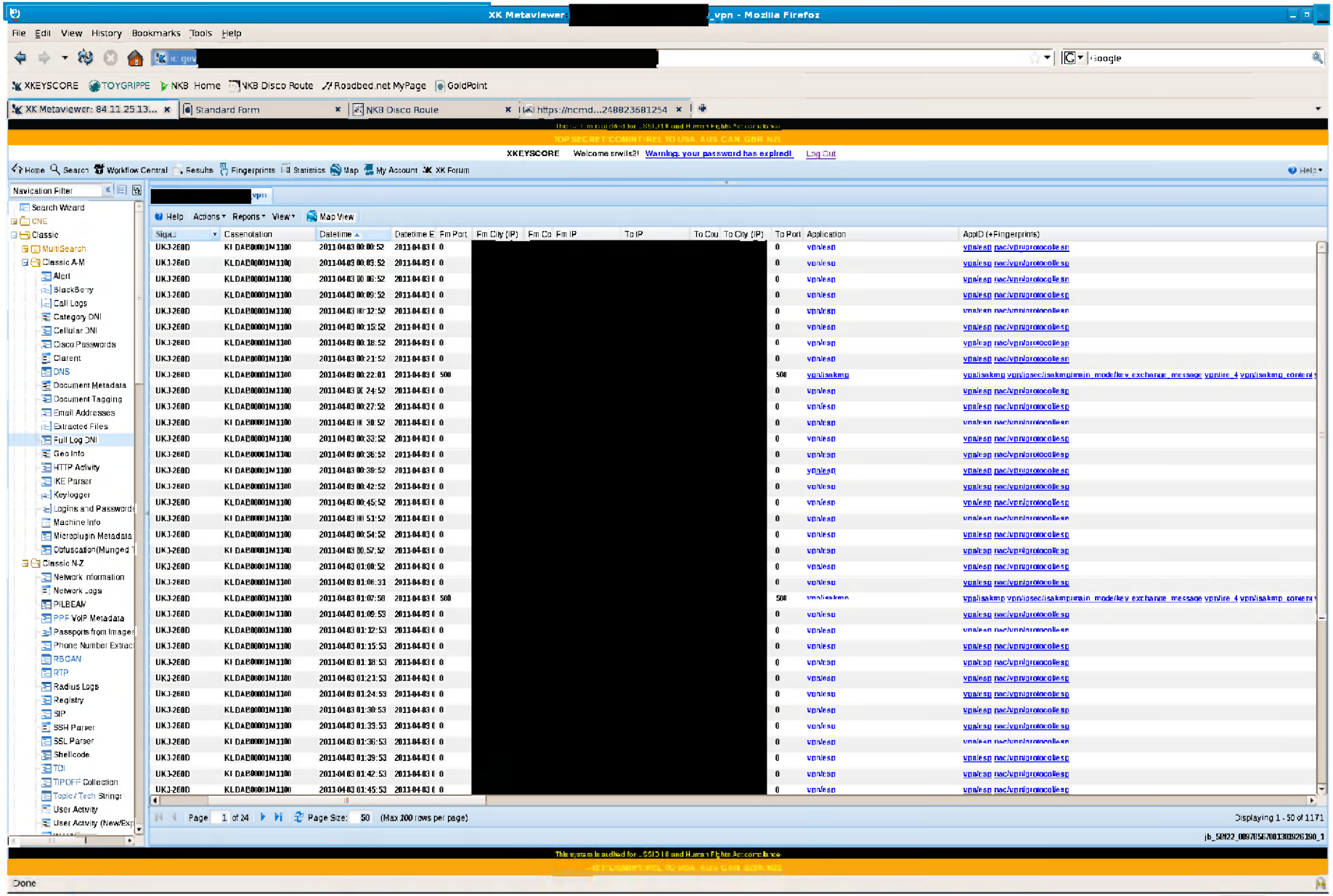
(TS//REL) Search Forms

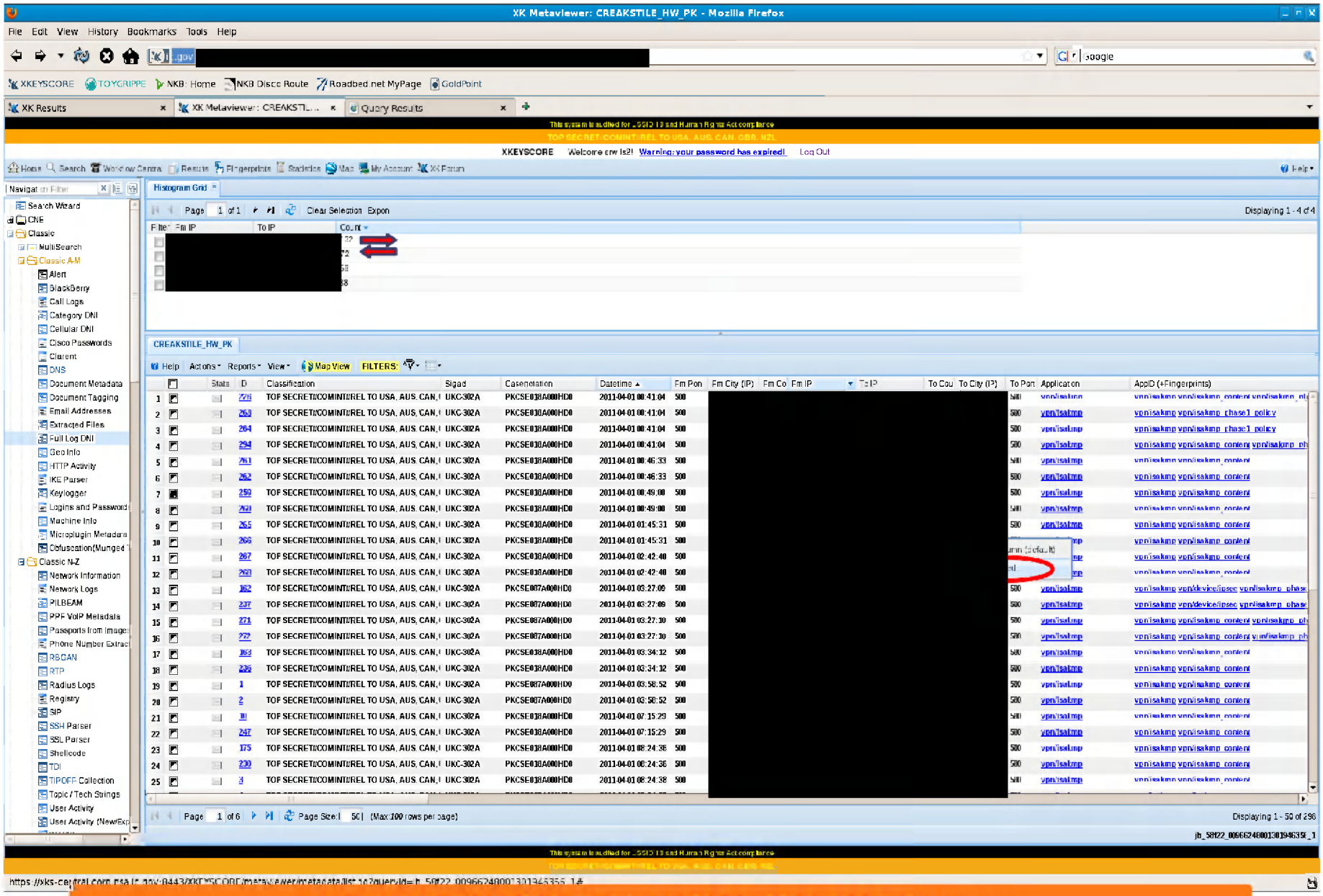
- Start with **FULL DNI**
  - **vpn/***
  - **network_encrytion/***
- IPSec
  - IKE Parser
- SSL
  - SSL Parser


XK Search: Full Log - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE
Welcome sw#i2!
Warning: your password has expired!
Log Out
Search: Full Log
Query Name:
Justification:
(TS//SI//REL) Looking for TASec traffic to perform vulnerability assessment.
Recent Justifications
Additional Justification:
Milanda Number:
Current Time: 2011-04-04 14:04:04 GMT
Datetime:
1 Day
Start:
2011-04-03
00:00
Stop:
2011-04-05
00:00
Client IP (X-Forwarded-For):
IP Address Field Builder
DVBS MAC:
DVBS PID:
WLAN Channel:
WLAN SSID:
WLAN BSSID:
WLAN DMAC:
WLAN SMAC:
IP Address:
Either
Done



ø (TS//REL) For initial searches, you may want to leave this blank to see all of the different kinds of traffic are found on the IP pair.


XK Metaviewer: [redacted]_vpn - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE TOYGRIPPE NKB Home NKB Disco Route Roadbed.net MyPage GoldPoint
XK Metaviewer: 84.11.25.13... Standard Form NKB Disco Route https://ncmd...248823681254
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL
XKEYSCORE Welcome srwils2! Warning: your password has expired! Log Out
Home Search Workflow Central Results Fingerprints Statistics Map My Account XK Forum Help
Navigation Filter
Search Wizard
CNE
Classic
MultiSearch
Classic A-M
Alert
BlackBerry
Call Logs
Category DNI
Cellular DNI
Cisco Passwords
Clarent
DNS
Document Metadata
Document Tagging
Email Addresses
Extracted Files
Full Log DNI
Geo Info
HTTP Activity
IKE Parser
Keylogger
Logins and Passwords
Machine Info
Microplugin Metadata
Obfuscation(Munged
Classic N-Z
Network Information
Network Logs
PILBEAM
PPP VoIP Metadata
Passports from Images
Phone Number Extract
RBGAN
RTP
Radius Logs
Registry
SIP
SSH Parser
SSL Parser
Shellcode
TDI
TIPOFF Collection
Topic / Tech String
User Activity
User Activity (New/Exp
[redacted] vpn
Help Actions Reports View Map View
Sigact Casenotation Datetime Datetime E Fm Port Fm City (IP) Fm Co Fm IP To IP To Cou To City (IP) To Port Application AppID (+Fingerprints)
UKJ-26OD KLDAE00001M1100 2011-04-03 00:00:52 2011-04-03 0 0 0 vpn/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:03:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:06:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:09:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:12:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:15:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:18:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:21:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:22:01 2011-04-03 0 500 500 vpn/isakmp vpn/isakmp vpn/ipsec/isakmp/main_mode/key_exchange_message vpn/ike_4 vpn/isakmp_content
UKJ-26OD KLDAE00001M1100 2011-04-03 00:24:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:27:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:30:52 2011-04-03 0 0 0 vpn/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:33:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:36:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:39:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:42:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:45:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:51:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:54:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 00:57:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:00:52 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:06:31 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:07:58 2011-04-03 0 500 500 vpn/isakmp vpn/ipsec/isakmp/main_mode/key_exchange_message vpn/ike_4 vpn/isakmp_content
UKJ-26OD KLDAE00001M1100 2011-04-03 01:09:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:12:53 2011-04-03 0 0 0 vpn/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:15:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:18:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:21:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:24:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:30:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:33:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:36:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:39:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:42:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
UKJ-26OD KLDAE00001M1100 2011-04-03 01:45:53 2011-04-03 0 0 0 vpn/esp nac/vpn/protocol/esp
Page 1 of 24 Page Size: 50 (Max 100 rows per page)
Displaying 1 - 50 of 1171
This system is audited for ...SSIS 18 and Human Rights Accordance
Done


XK Metaviewer: CREAKSTILE_HW_PK - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE
XK Results
Query Results
XKEYSCORE
Log Out
Histogram Grid
CREAKSTILE_HW_PK
Help Actions Reports View Map View FILTERS:
Classification
Sigad
Datetime
Application
AppID (+Fingerprints)

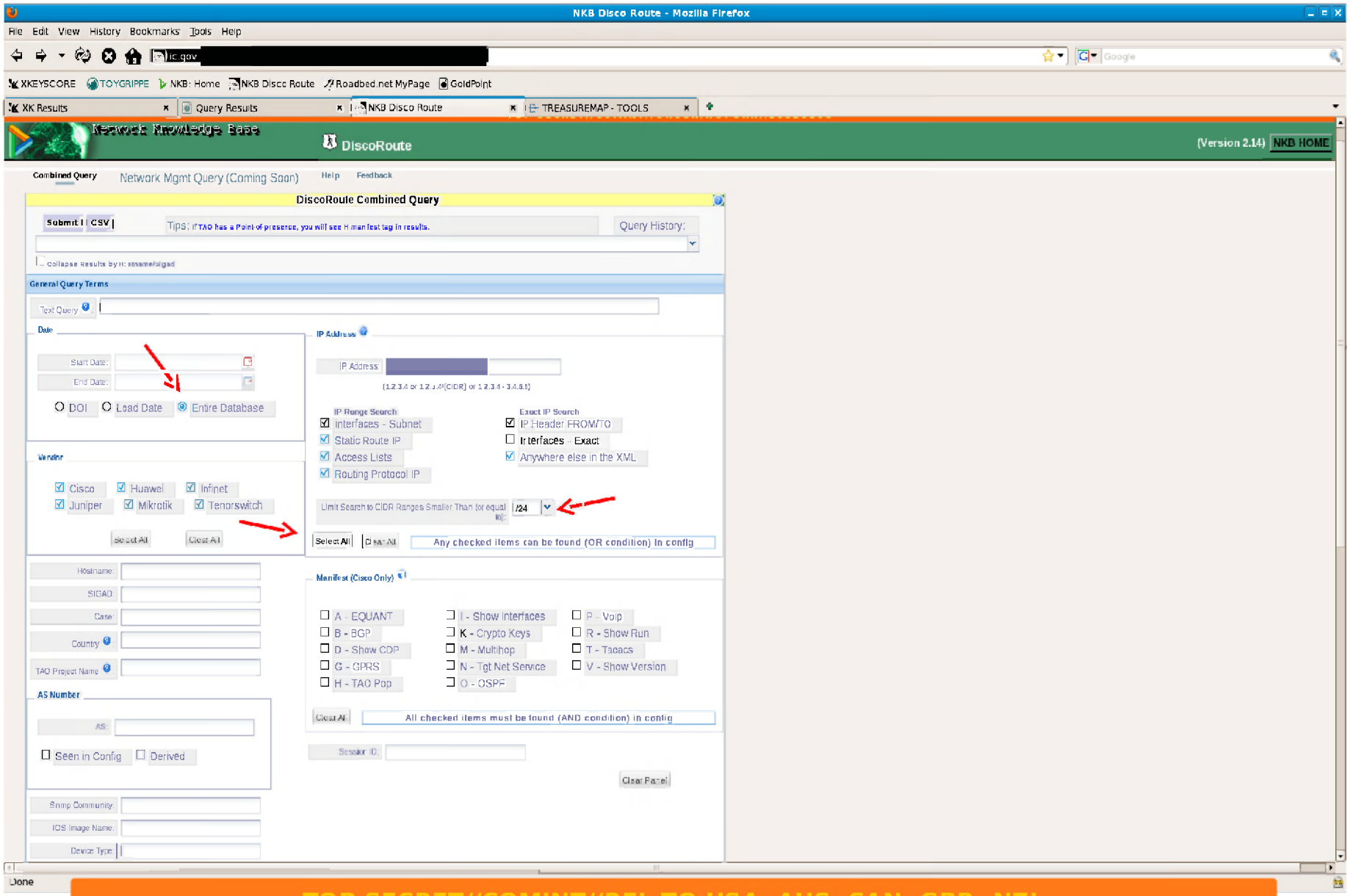
(TS//SI//REL) PINWALE

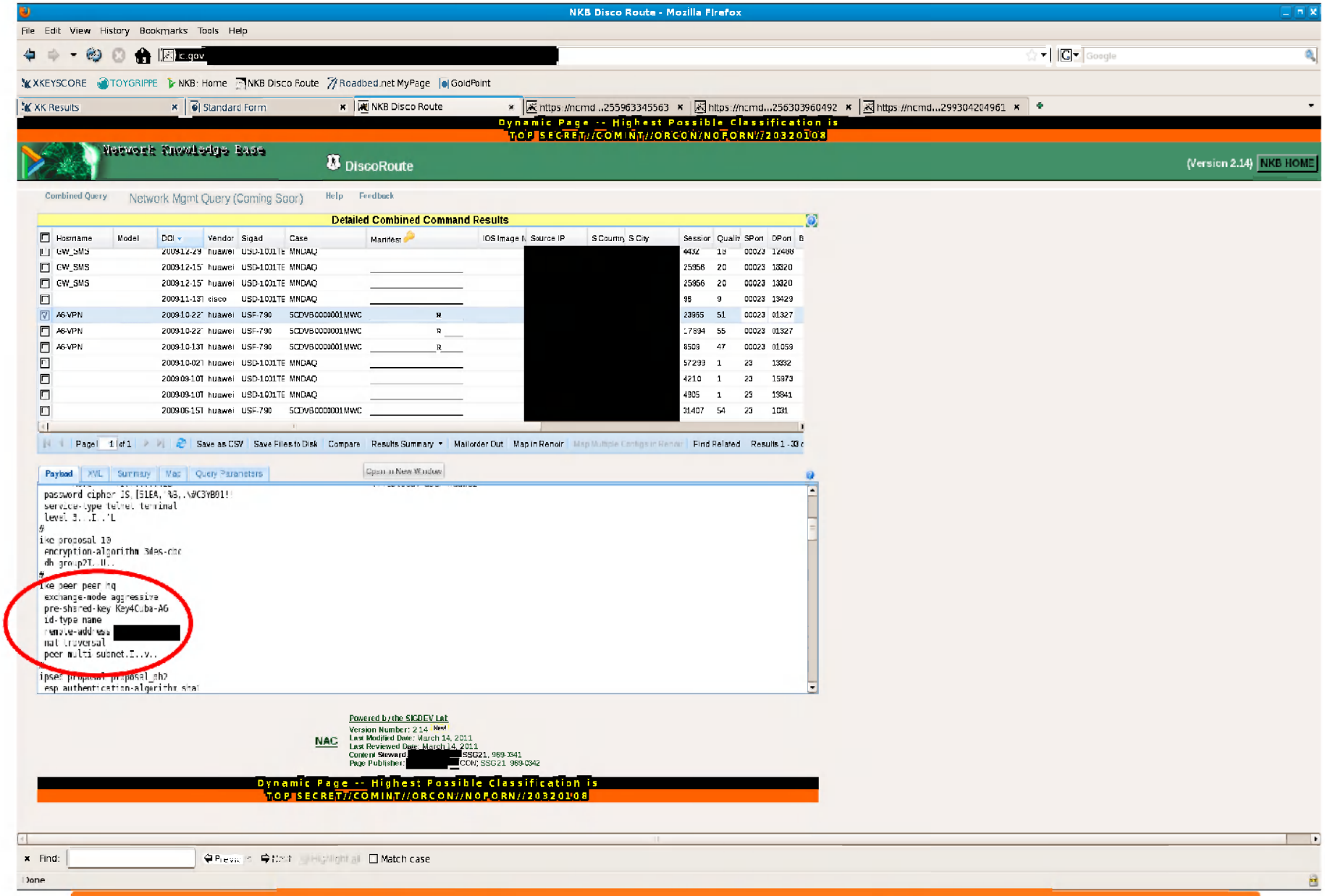
- (TS//SI/REL) Both VPN traffic and Sys Admins passing information about VPN setup

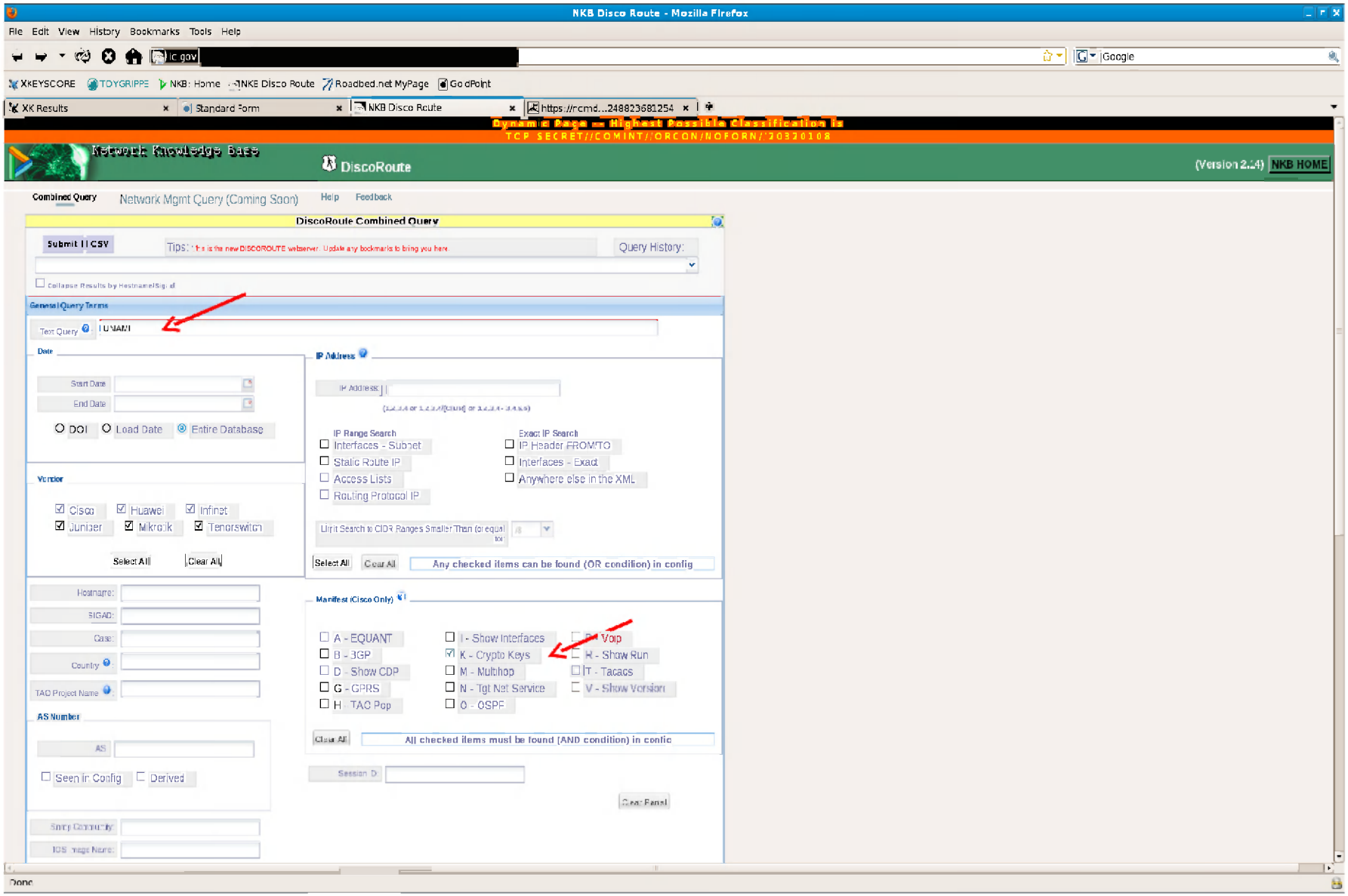
- (TS//SI/REL) IP addresses and port numbers (ex. AP 00500) ******Document Zone = C2C***
- (TS//SI/REL) Display 'DZ Protocol SRC Port','DZ Protocol DEST Port', 'Next Protocol Name'

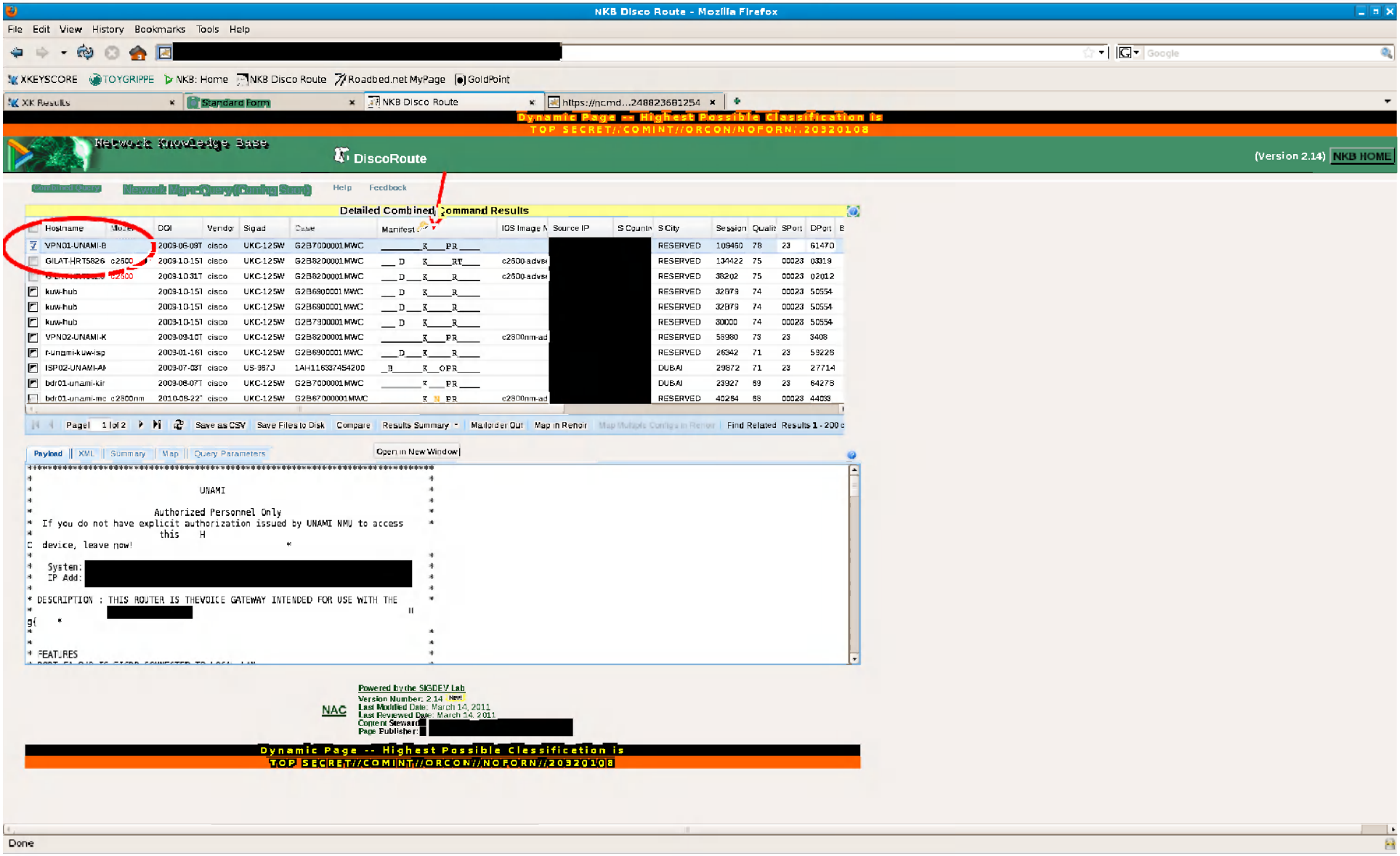
(TS//SI//REL) DISCOROUTE

- (TS//SI/REL) Router configuration data
  - From passive and active collection
  - Key terms to search for within configs:
  - ‘crypto map’, ‘isakmp’, ‘ipsec’, ‘pre-shared-key’


NKB Disco Route - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint
XK Results
Query Results
NKB Disco Route
TREASUREMAP - TOOLS
Network Knowledge Base
DiscoRoute
(Version 2.14)
NKB HOME
Combined Query
Network Mgmt Query (Coming Soon)
Help
Feedback
DiscoRoute Combined Query
Submit!
CSV
Tips: If TAO has a Point-of-presence, you will see H man test tag in results.
Query History:
General Query Terms
Text Query
Date
Start Date:
End Date:
DOI
Load Date
Entire Database
Vendor
Cisco
Huawei
Infinet
Juniper
Mikrotik
Tenorswitch
Select All
Clear All
IP Address
IP Address:
IP Range Search
Interfaces - Subnet
Static Route IP
Access Lists
Routing Protocol IP
Exact IP Search
IP Header FROM/TO
Interfaces - Exact
Anywhere else in the XML
Limit Search to CIDR Ranges Smaller Than (or equal to):
/24
Select All
Clear All
Any checked items can be found (OR condition) in config
Hostname:
SIGAD:
Case:
Country
TAO Project Name
AS Number
AS:
Seen in Config
Derived
Snmp Community:
IOS Image Name:
Device Type:
Manifest (Cisco Only)
A - EQUANT
B - BGP
D - Show CDP
G - GPRS
H - TAO Pop
I - Show Interfaces
K - Crypto Keys
M - Multihop
N - Tgt Net Service
O - OSPF
P - Voip
R - Show Run
T - Tacacs
V - Show Version
Clear All
All checked items must be found (AND condition) in config
Session ID:
Clear Panel
Done


NKB Disco Route - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint
XK Results
Standard Form
NKB Disco Route
Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108
Network Knowledge Base
DiscoRoute
(Version 2.14) NKB HOME
Combined Query
Network Mgmt Query (Coming Soon)
Help
Feedback
Detailed Combined Command Results
Hostname Model DOI Vendor Sigad Case Manifest IOS Image Source IP S Country S City Session Quality SPort DPort
GW_SMS huawei USD-1031TE MNDAQ
GW_SMS huawei USD-1031TE MNDAQ
GW_SMS huawei USD-1031TE MNDAQ
cisco USD-1031TE MNDAQ
A6-VPN huawei USF-790 SCDVB0000001MWC
A6-VPN huawei USF-790 SCDVB0000001MWC
A6-VPN huawei USF-790 SCDVB0000001MWC
huawei USD-1031TE MNDAQ
huawei USD-1031TE MNDAQ
huawei USD-1031TE MNDAQ
huawei USF-790 SCDVB0000001MWC
Page 1 of 1
Save as CSV
Save Files to Disk
Compare
Results Summary
Mailorder Out
Map in Renoir
Find Related
Payload
XML
Summary
Mac
Query Parameters
password cipher
service-type telnet terminal
level
!
ike proposal 10
encryption-algorithm
dh group2
!
ike peer peer_ng
exchange-mode aggressive
pre-shared-key Key4Cuba-A6
id-type name
remote-address
nat traversal
peer multi subnet
ipsec proposal
esp authentication-algorithm sha1
Powered by the SIGDEV Lab
NAC
Version Number: 2.14
Last Modified Date: March 14, 2011
Last Reviewed Date: March 14, 2011
Content Steward
Page Publisher:
Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108
Find:
Match case
Done


NKB Disco Route - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GodPoint
XK Results
Standard Form
NKB Disco Route
Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON/NOFORN//20320108
Network Knowledge Base
DiscoRoute
(Version 2.4)
NKB HOME
Combined Query
Network Mgmt Query (Coming Soon)
Help
Feedback
DiscoRoute Combined Query
Submit
CSV
Tips:
Query History:
Collapse Results by Hostname/Sig. id
General Query Terms
Text Query
EQUANT
Date
Start Date
End Date
DOI
Load Date
Entire Database
IP Address
IP Address
IP Range Search
Interfaces - Subnet
Static Route IP
Access Lists
Routing Protocol IP
Exact IP Search
IP Header FROM/TO
Interfaces - Exact
Anywhere else in the XML
Limit Search to CIDR Ranges Smaller Than (or equal to)
Select All
Clear All
Any checked items can be found (OR condition) in config
Vendor
Cisco
Huawei
Infinet
Juniper
Mikrotik
Tenorswitch
Select All
Clear All
Hostname:
SIGAD:
Case:
Country
TAO Project Name
AS Number
AS
Seen In Config
Derived
Manifest (Cisco Only)
A - EQUANT
B - 3GP
D - Show CDP
G - GPRS
H - TAO Pop
I - Show Interfaces
K - Crypto Keys
M - Multihop
N - Tgt Net Service
O - OSPF
R - Show Run
T - Tacacs
V - Show Version
Clear All
All checked items must be found (AND condition) in confic
Session ID
Clear Panel
Done


NKB Disco Route - Mozilla Firefox
File Edit View History Bookmarks Tools Help
XKEYSCORE TOYGRIPPE NKB: Home NKB Disco Route Roadbed.net MyPage GoldPoint
XK Results
Standard Form
NKB Disco Route
https://ncmd...248823681254
Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON/NOFORN//20320108
Network Knowledge Base
DiscoRoute
(Version 2.14)
NKB HOME
Help
Feedback
Detailed Combined Command Results
Hostname
VPN01-UNAMI-B
GILAT-HRT5826
kuw-hub
VPN02-UNAMI-K
r-unami-kuw-isp
ISP02-UNAMI-AI
bdr01-unami-kir
bdr01-unami-mc
RESERVED
Page1 1 of 2
Save as CSV
Save Files to Disk
Compare
Results Summary
Mail order Out
Map in Reroir
Find Related
Payload
XML
Summary
Map
Query Parameters
Open in New Window
UNAMI
Authorized Personnel Only
If you do not have explicit authorization issued by UNAMI NMU to access
this H
device, leave now!
System:
IP Add:
DESCRIPTION : THIS ROUTER IS THEVOICE GATEWAY INTENDED FOR USE WITH THE
FEATURES
NAC
Powered by the SIGDEV Lab
Version Number: 2.14
Last Modified Date: March 14, 2011
Last Reviewed Date: March 14, 2011
Content Steward:
Page Publisher:
Dynamic Page -- Highest Possible Classification is
TOP SECRET//COMINT//ORCON//NOFORN//20320108
Done

(U) Others

- (TS//REL) NKB
- (TS//REL) TUNINGFORK
- (TS//REL) TREASUREMAP
- (TS//REL) RENOIR
- (TS//REL) MASTERSHAKE
- (TS//REL) ROADBED
- (TS//REL) ~~BLEAKINQUIRY~~

AUS, CAN, GBR, NZL

(TS//SI//REL) Basic VPN rules of thumb

(TS//REL) If you have an IP address…

- Check TOYGRIPPE and XKS
  - Look for paired traffic
- For IPSec, check sys admin chatter for PSK (DISCOROUTE; PINWALE; MARINA)
- Share your data with OTTERCREEK for vulnerability assessment (XKEYSCORE or DROPBOX)
- Submit tasking

(TS//REL) If you don't …

- Look in DISCOROUTE
- Query Sys Admins in PINWALE and MARINA
- Check your targets TAO projects

EITHER WAY,
JOIN THE
VPN WORKING GROUP
FOR ALL OF YOUR
VPN SIGDEV NEEDS

(U//FOUO) Useful Links

- (TS//SI//REL) VPN Working Group (go vpn) [redacted]
- (TS//SI//REL) OTTERCREEK (go VPN XFT)
  [redacted]
  - VPNXFT DROPBOX

[redacted]

- (TS//SI//REL) Network Security Products (go NSP)
  [redacted]

(U) Questions?

[redacted]

OTTERCREEK

[redacted]