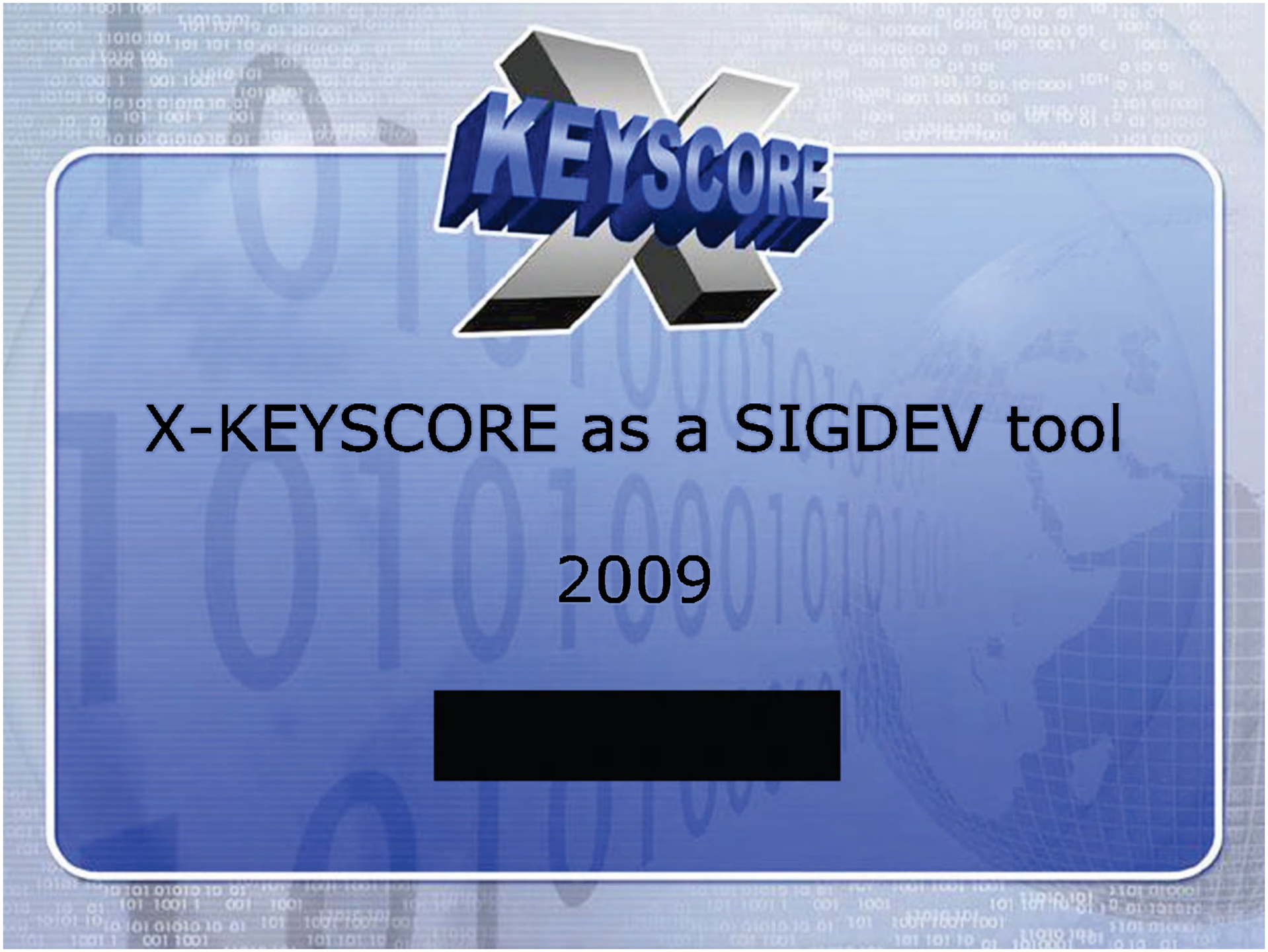

KEYSCORE
X-KEYSCORE as a SIGDEV tool
2009
[redacted]

What is X-KEYSCORE?

What is XKEYSCORE?

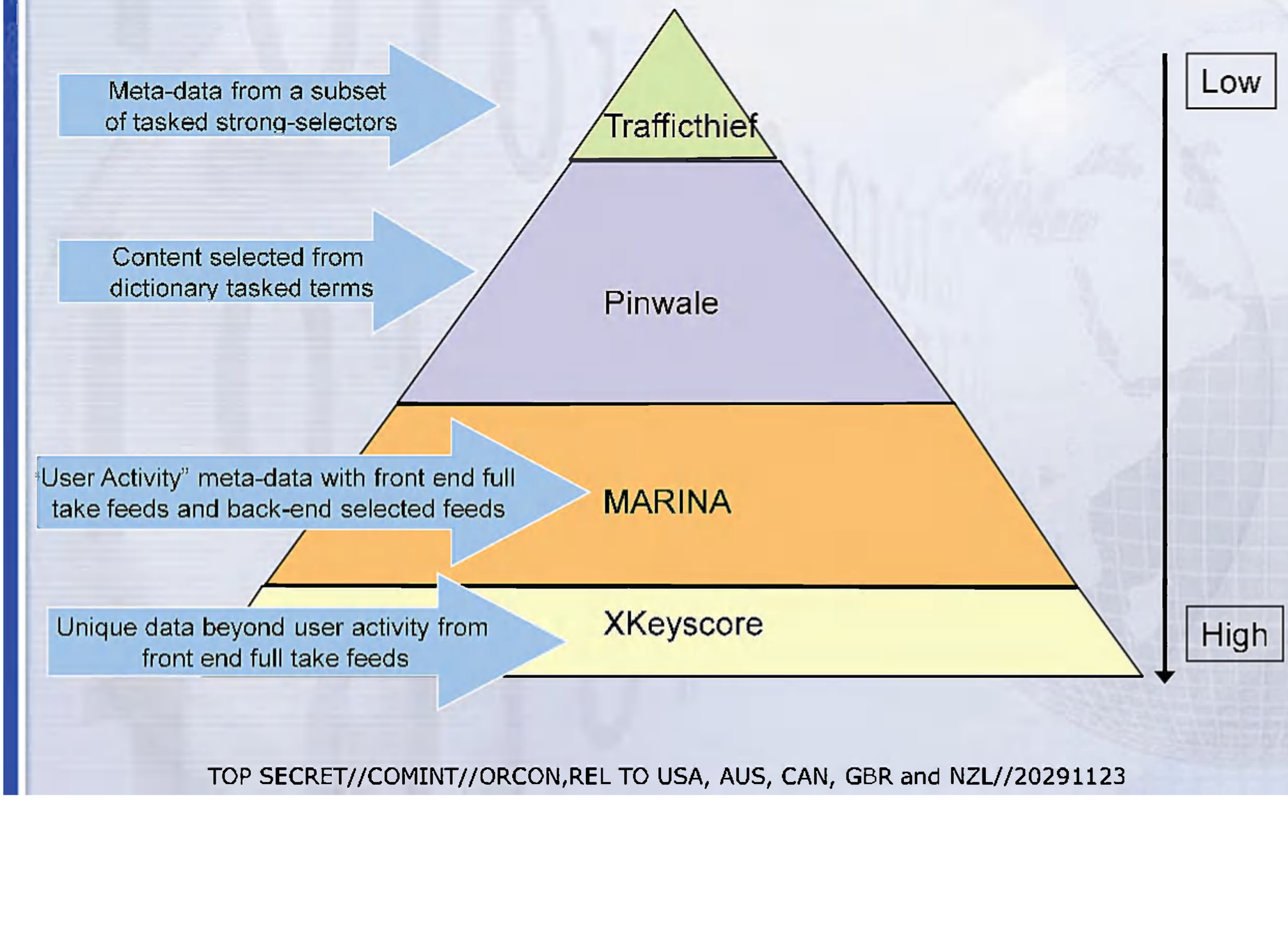
A (DNI) SIGDEV Tool

It gives you the ability to discover things that you otherwise wouldn't have seen

What makes XKS so good at SIGDEV?

- XKS gives analysts unique access to terabytes of content and meta-data
- Typically sites select and forward to PINWALE less than 5% of the DNI they're processing
- The rest of that data used to be dropped but is now being retained temporarily and made available to analysts through X-KEYSCORE
- As an example, at one our sites XKS sees more data per day than all of PINWALE

DNI Discovery Options



"Slowing down the Internet"

- XKS goal is to store the full-take content for 3-5 days, effectively "slowing down the Internet" so that analysts can go back and recover sessions that otherwise would have been dropped by the front end
- Meta-data is saved off longer, with the goal of 30 days retention
- A lot of analysis can be done through meta-data only (MARINA is meta-data only)

XKS Storage Times

- Front end storage is limited by resources and policy restrictions and will vary by site
- At some sites, the amount of data we receive per day (20+ Terabytes) can only be stored for as little as 24 hours based on available resources
- Other sites have legal or policy restrictions that limit the amount of time we can store data (if we can at all)
- It's a rolling buffer where new data comes in and pushes the oldest data out

How can I "save off" XKS data?

- Content that is "interesting" can be pulled out of X-KEYSCORE and pushed to Agility or PINWALE or any other database for longer retention

- Workflows can be set up to automatically harvest content out of XKS before it ages off

- The goal, however, is to use X-KEYSCORE to discover new things, that will end up on tasking for future collection

How do I access XKS data?

- It's important to know that XKS queries meta-data tables only
- Results from the meta-data tables are then linked back to the original piece of content
- Goal of the system is to extract a wide range of meta-data for users to query

What kind of meta-data is produced?

KEYSCORE

- Classic A-M
  - ASF and WMV Metadata
  - Alert
  - BlackBerry
  - CNE
  - Call Logs
  - Category DNI
  - Cellular DNI
  - Cisco Passwords
  - Document Metadata
  - Document Tagging
  - Email Addresses
  - Extracted Files
  - Full Log DNI
  - HTTP Activity
  - IRC Cafe Geolocation
  - Logins and Passwords
- Classic N-Z
  - Network Logs
  - PDF Metadata
  - PILBEAM
  - Phone Number Extractor
  - RBGAN
  - REGISTRY
  - RTP
  - Radius Logs
  - RealMedia Metadata
  - SIP
  - TOR Log
  - Tech Strings in Documents
  - User Activity
  - WLAN
  - Web Proxy
  - Wireshark

Examples of "simple" Plug-ins

Plug-in	DESCRIPTION
E-mail Addresses	Indexes every E-mail address seen in a session by both username and domain
Extracted Files	Indexes every file seen in a session by both filename and extension
Full Log	Indexes every DNI session collected. Data is indexed by the standard N-tupple (IP, Port, Casenotation etc.)
HTTP Parser	Indexes the client-side HTTP traffic (examples to follow)
Phone Number	Indexes every phone number seen in a session (e.g. address book entries or signature block)

Examples of "advanced" Plug-ins

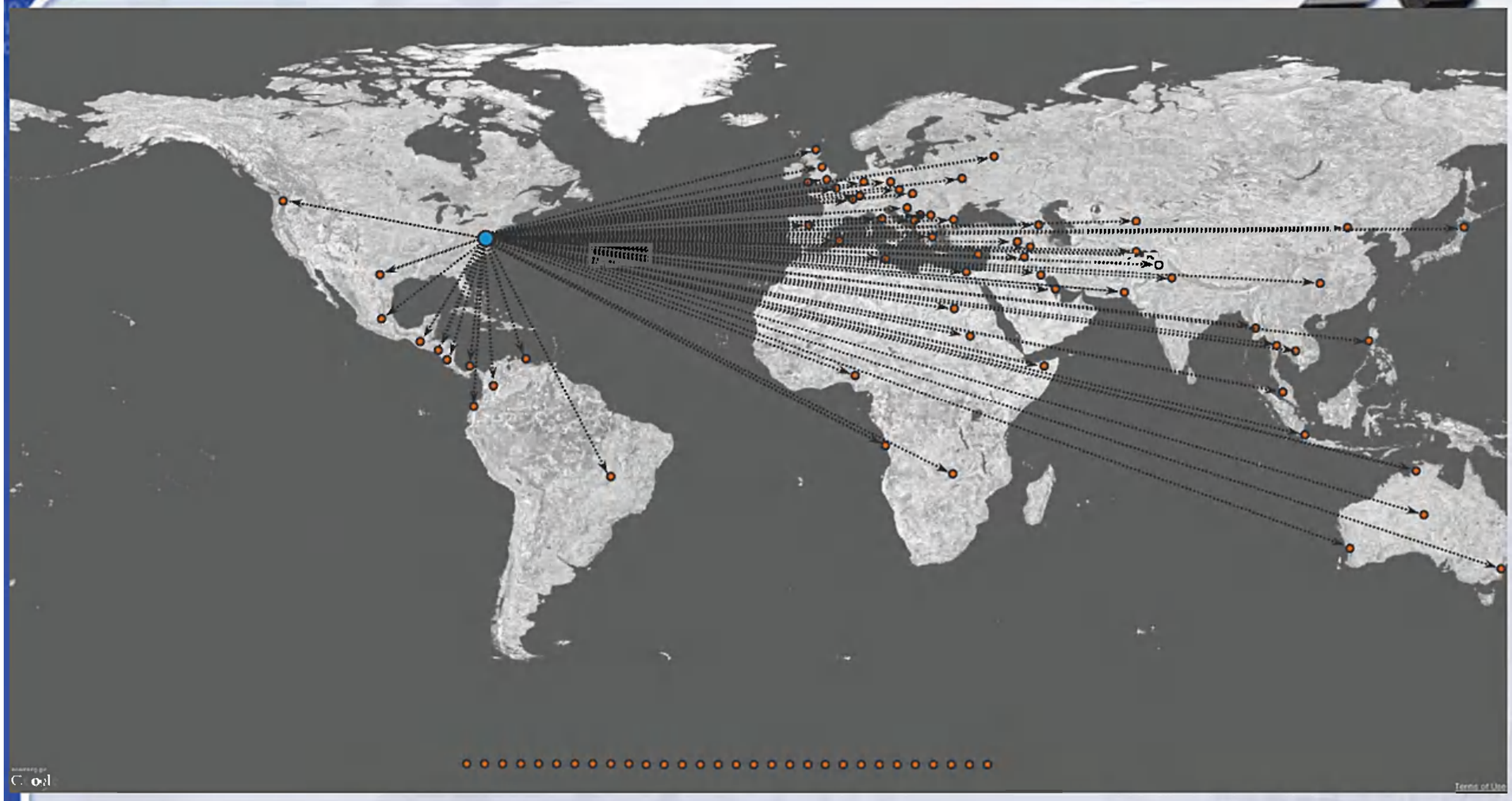
Plug-in	DESCRIPTION
User Activity	Indexes the Webmail and Chat activity to include username, buddylist, machine specific cookies etc. (AppProc does the exploitation)
Document meta-data	Extracts embedded properties of Microsoft Office and Adobe PDF files, such as Author, Organization, date created etc.

Plug-ins

- A single session may contain entries in multiple meta-data tables
- For example, if a single session had a user E-mailing an attached word document the following plug-ins would extract meta-data:

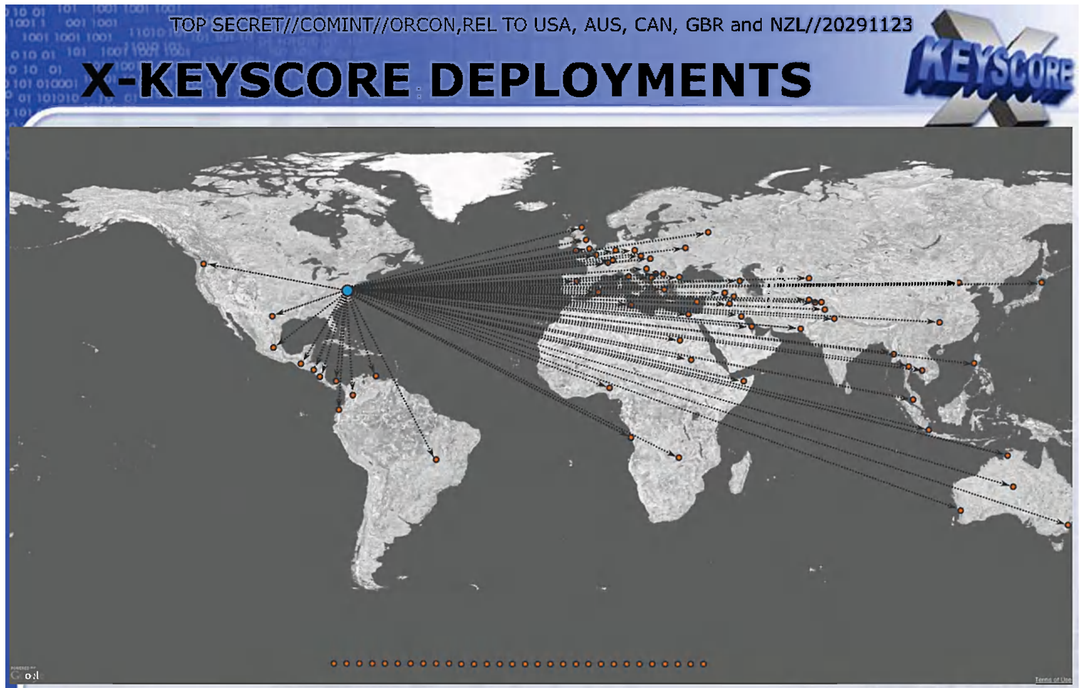
Plug-in	Would have extracted…
Full Log	…bare minimum meta-data like To/From IP address, ports, casenotation, sigad etc.
E-mail Addresses	…any E-mail addresses seen on that page (including inside the attached word file)
Extracted Files	…the filename and extension of the attachment
Document Meta-data	…in addition to the filename and extension, any embedded properties of the word document like Author, last author, organization, date created, date last modified etc.

X-KEYSCORE DEPLOYMENTS



125 Sites

X-KEYSCORE DEPLOYMENTS



125 Sites

AppIds and Fingerprints

- X-KEYSCORE produces an application id for each session processed
- Currently almost 1300 Appids in 28 categories
- An Appid is meant to identify a session as a particular application
- Fingerprints are an extensible way of tagging sessions
- Ex: A session Appid'd as mail/smtp might also contain fingerprints for encryption if used in the email

AppIds and Fingerprints

Ex: E-Mails with encryption

From: "Launchpad OpenPGP Key Confirmation" <noreply@launchpad.net> **[Save Address] [Block Sender]**

To: [redacted]
Cc:
Subject: Launchpad: Confirm your OpenPGP Key
Date: Wed, 31 Dec 2008 10:04:16 -0000

-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.6 (GNU/Linux)

Application	AppID (+Fingerprints)
mail/webmail/outblaze	mail/webmail/outblaze has_fingerprint encryption/pgp encryption/pgp/message

spfMVPZsl1vpg67VdHFUprgv0JprnjQlb73gWmhbOUrZzyGdDRla9CcFzJA7OIL
3XyCrlniniJ4/c98+khDazh1XY/S7yNi38Wrlkd3GOz9DFFl1Nu31nwjh3+nc0pv
OlyztsQzLFB/8+qJrPvmK8fzz7tWp2djxyfMGoAYNAf/QOohR0BjqTgOUlqLRVrE
eEFivrMOnBxf60SHlFra7LpZlsTUFpBJNAkgguk7m8fJ0dMrnU0V5MeM1x8GuWv5+
Uk4bBwwZ1VpEVHCyGuv6ux+V+KpSkQtDwdhlp12SZ2SUrn1upnVB9lfcnlhWvxZp
LaY3mXqNWhyhzFPFxkhUwqzd/rMxrCJucfXGaeisSizZDlQOWxTSwe7BwvG8Bvnr
QEQVKY30WWg+2pDTPrKq3uEqOwj9JY7KTPMrf2gZLNABDuCJm5lRALZqqETTg4dh
xV0r9+2ZLtyGDXQhLMyBElYns4+jiP1rd3E+TW7JVUe/dPluyC4DwOUPklwuHcC+
StLAuQHMS6RkB4aDNdi6QG9kEWvjq2PvfuMIBWo5jJ8RFoDSx8q5t1ukgeCxr6xr
Q4eTmOFTlA71G312Xa7ZniOzyxiWZ4CAbhHLF+3baFD3lb4/EFmRvPBdqy6wUyHD
Z5EXyHDzl4XlDyEe/aomEqAsUqPs8MZirHHzpbaS3LbG5B5VKAKU59bENpf/KOgT
a3lUAeQ1t6xLzgToVdfhEkPj5bxODrWcZtHeTEt1nV+3pc2P58+QICDOETiDCA/j
dhG2brUwbxny6Ap7fU5e1ALU3ryoXKvt9eCXZHooY/p9QIC3koHCWptGD6gKCxlt
KW/K5M+HkxhHy4V7Wb137CStzeLda8BdU43Kh0ZQWWjK7pDXKKhHLYIGlawRScQa
e6J+y4JR1KKyXiXY94Erxa/P0FzuYV/QCJUDpqWFR22bXuy4FhkosLWM8G+UBHVt
UfgRxq8as60DhBDWy08eLEAdE92TVffJgXOvAOzTqBrP7uZi/Q7ABFFGTQ9n
=N4CJ
-----END PGP MESSAGE-----

Thanks,

AppIds and Fingerprints

KEYSCORE

Ex: Airline E-Tickets

Subject:	**Airblue E-Ticket - JGDTGSWB**
From:	Airblue Reservations <website@airblue com>;
To:	[redacted]
Date:	Nov 18, 2008 10:41:54 AM

E-TICKET airblue

Reservation No. [redacted]

Application	AppID (+Fingerprints)
mail/webmail/yahoo	mail/webmail/yahoo has_fingerprint travel/airbiue

[redacted]

Phone 1: [redacted]
Phone 2:

AZ2749951 21 6876 5648 15E

Travel Coupon(s) PHOTO ID REQUIRED AT CHECK-IN

[redacted]

21 6876 5648 / 1 ED 610 Peshawar Dubai 29 NOV 08 12:00 O YA90O 15.505.00 OK

Transactions history details:

Date/Time	Method	Location	Description	Amount
18-Nov-2008 3:41 PM	Travel Agency	Khaleej Express- Pew Muhammed Younas, Main Branch	Ticket Sale	Rs 15,505.00

AppIds and Fingerprints

Ex: Extremist Forum Private Messages

HTTP Header Information	Content Type: HTTP/POST/Form-Data
POST /vb/private.php?do=insertpm &pmid= HTTP/1.1	
Accept:	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Referer:	[redacted]
Accept-Language:	en-gb
Content-Type:	application/x-www-form-urlencoded
UA-CPU:	x86
Accept-Encoding:	gzip, deflate
User-Agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; FDM)

Application	AppID (+Fingerprints)
mail/webmail/vbulletin/private_message.insert	**mail/webmail/vbulletin/private_message/insert has_fingerprint forum.extremist/al-faloja**

recipients	[redacted]
bccrecipients	
title	خبر مهم
message	شنت كتيبة المواجهات التابعة لحركة الشباب المجاهدين-يفضل الاخضاء يوم الإثنين 08 محرم 1430 هـ الموافق لـ:05-01-2009م هجوما مباشرا وعنيفا على مصنع الباسئا للقوات الصليبية الإثيوبية في مقديشو،وشاركت كتيبة المدفعيات في العملية المباركة حيث قامت بقصف المصنع بوابل من الصواريخ والمدفعيات. واستخدم المجاهدون في الهجوم أساليب قتالية غير مسبوقة مما أرغم على فوات العدو الذاجع من دفاعاتها في الشارع العام المؤدي إلى المصنع،وحينما اجتمعوا على حجرهم فاجأتهم كتيبة المدفعيات بقصف عنيف ودقيق وتوقع خسائر بشرية جسيمة في صفوف القوات الصليبية ولله الحمد والمنة

X-KEYSCORE Workflows

- X-KEYSCORE workflows are standing queries that run on set intervals during the day (usually once a day)
- After action reports can E-mail the results of the workflow, parse out data to mailorder to other databases and more
- New GUI's Workflow Central makes it easy to create and manage your workflows

XKS Workflows: Easy to Create!

This system is audited for USSID 18 and Human Rights Act compliance

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, and NZL//20320108

XKEYSCORE Welcome: dtstua2 switch users

Home | Admin | Users | Workflow Central | Search | Results | Statistics | Preferences | Help

Navigation Menu

- Explorer
  - Home
  - Admin
  - Users
  - Workflow Central
    - Request
    - All Workflows
    - My Workflows
  - Search
    - Classic
      - MultiSearch
        - IP Addresses
        - Mac Address
        - Username
      - Classic A-M
        - ASF and WMV Metada
        - Alert
        - BlackBerry
        - CNE
        - Call Logs

Welcome to the *Beta* release of the *New* XKEYSCORE Home Page!

If you have questions or bug reports please go to XKEYSCORE New GUI Forum

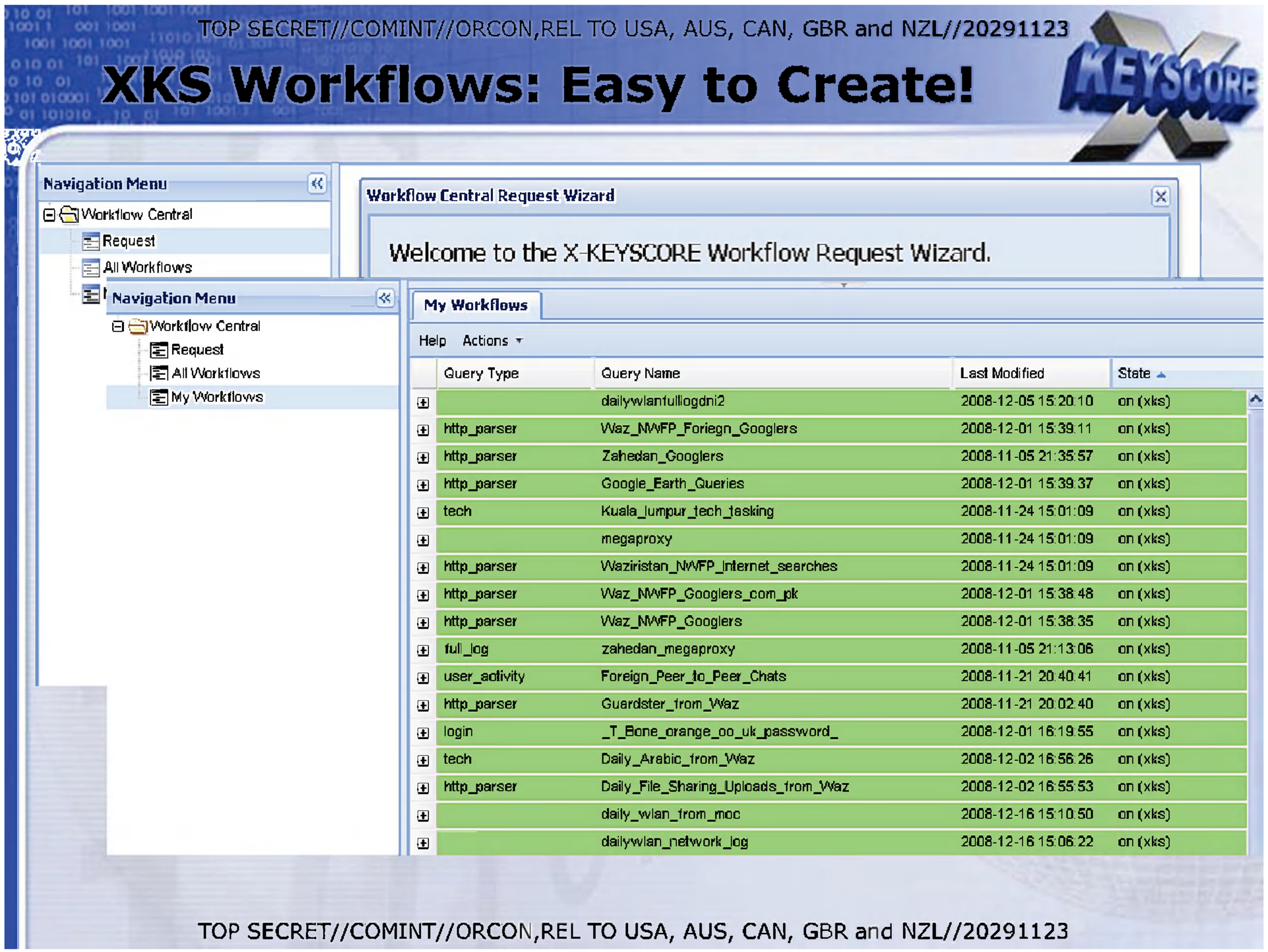
News

(U//FOUO) New XKEYSCORE GUI

(U//FOUO) XKEYSCORE is working on a new GUI that has now reached an open Beta state. Follow the link below to try it out. Your account and preferences will automatically be transfered when you log in. Please view these training videos to acclimate yourself with the new layout and features. Some features have not yet been completed but will still be available in the original GUI. Try the new XKEYSCORE GUI (Beta)!

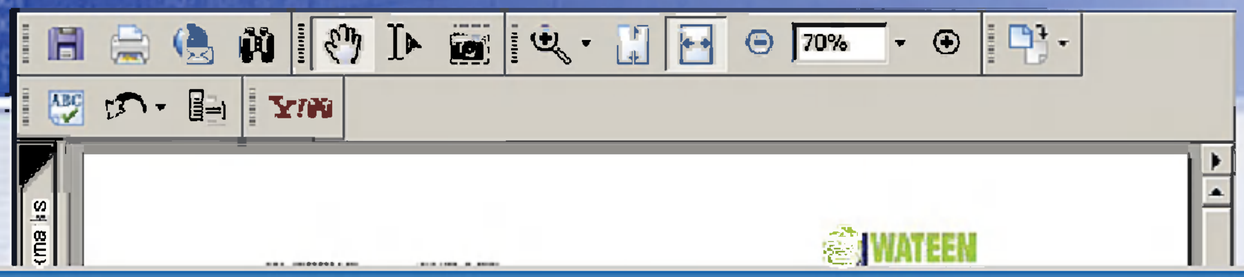
(U//FOUO) If you find bugs please report them **ONLY** in the XKEYSCORE Forums under the New GUI section, which can be found here. We will try to fix any bugs as quickly as possible, but when experiencing a problem revert back to the original GUI until we can fix it.

XKS Workflows: Easy to Create!

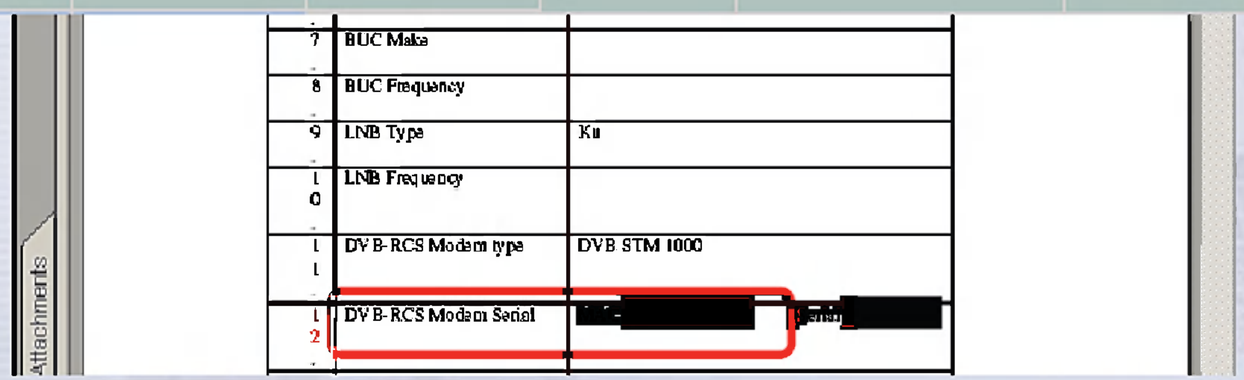


Context-Aware Tagging

- Provides for the ability to task and scan for terms only when they appear inside the body of documents like Microsoft Office or Adobe PDFs
- EX: We want to find technical documents regarding WIMAX networks but tasking the term 'WIMAX' to Cadence would flood PINWALE with hits. What if we only look for the term within documents?



ID	DATETIME	DATETIME END	TECH NAME	TECH VALUE	TECH FILENAME
1	2008-01-01 04:55:00	2008-01-01 04:55:01	wireless	WIMAX	NIB Ranchor Line KHI.doc
2	2008-01-01 04:55:00	2008-01-01 04:55:01	satellite	DVB	NIB Ranchor Line KHI.doc
3	2008-01-01 04:55:00	2008-01-01 04:55:01	mac	[redacted]	NIB Ranchor Line KHI.doc



Context-Aware Tagging

KEYSCORE

- E
  li
  b

Event T

email_t

Fm City

KLOSTE

Subject:	NFF-66024-GCC-KHI
From:	[redacted]
To:	[redacted]
Cc:	[redacted]
Date:	Tue Dec 30 10:57:48 GMT 2008

HTML | Plain Text | Attachment

IMEI: [redacted]

Model: 6300

WON: 66024

ASC: GCC-KHI

Symptom: 4100

Comments: no fault found phone is working properly kindly confirm the fault in detail when and in which condition it creates problem related to mention symptom

[redacted]
GSM Repair Engineer
[redacted]
Tel:
Mob:
Fax:

Context-Aware Scanning

- Tasking is so flexible that it can include regular expressions (REGEXs) with few or no anchor points
- Ex: Can we find documents that have MAC addresses in them?
- The following Regex looks for MAC addresses:
- "(00|01|02|04|08|10|3C|44):(?=[\d:]{0,12}[a-f])([\da-f]{2}):([\da-f]{2}):([\da-f]{2}):([\da-f]{2}):([\da-f]{2})"

Context-Aware Scanning

- Supports full foreign language tagging and querying
- Ex look for common Arabic expressions in E-mails coming from the Pakistan tribal regions:

UIS Webmail Display Windows Live Mail Beta Active user: Unknown

From: [redacted] ([redacted]@gmail.com)

Medium risk You may not know this sender. Mark as safe | Mark as unsafe

Sent: Thu 1/01/09 12:07 PM

To: [redacted]

السلام عليكم ورحمة الله وبركاته

X-KEYSCORE SIGDEV

- **X-KEYSCORE's full take database of meta-data and content make it an powerful SIGDEV tool**
- **Many DNI applications don't contain strong selectors that allow traffic to be collected**
  - **Web surfing**
  - **Internet searching**
  - **Anonymous file uploading/downloading**
- **The variety of applications processed and meta-data available make X-KEYSCORE an ideal starting point for DNI development**

X-KEYSCORE SIGDEV

- **Scenario 1: Persona Analysis**
- **Goal to identify the "user session"**
- **Help answer the question : What did my target do while he was online?**
- **We may know from TRAFFICTHIEF, PINWALE or MARINA that our target was online at a given time and from a given IP address, so we can then search in X-KEYSCORE for everything that happened "around" that event.**

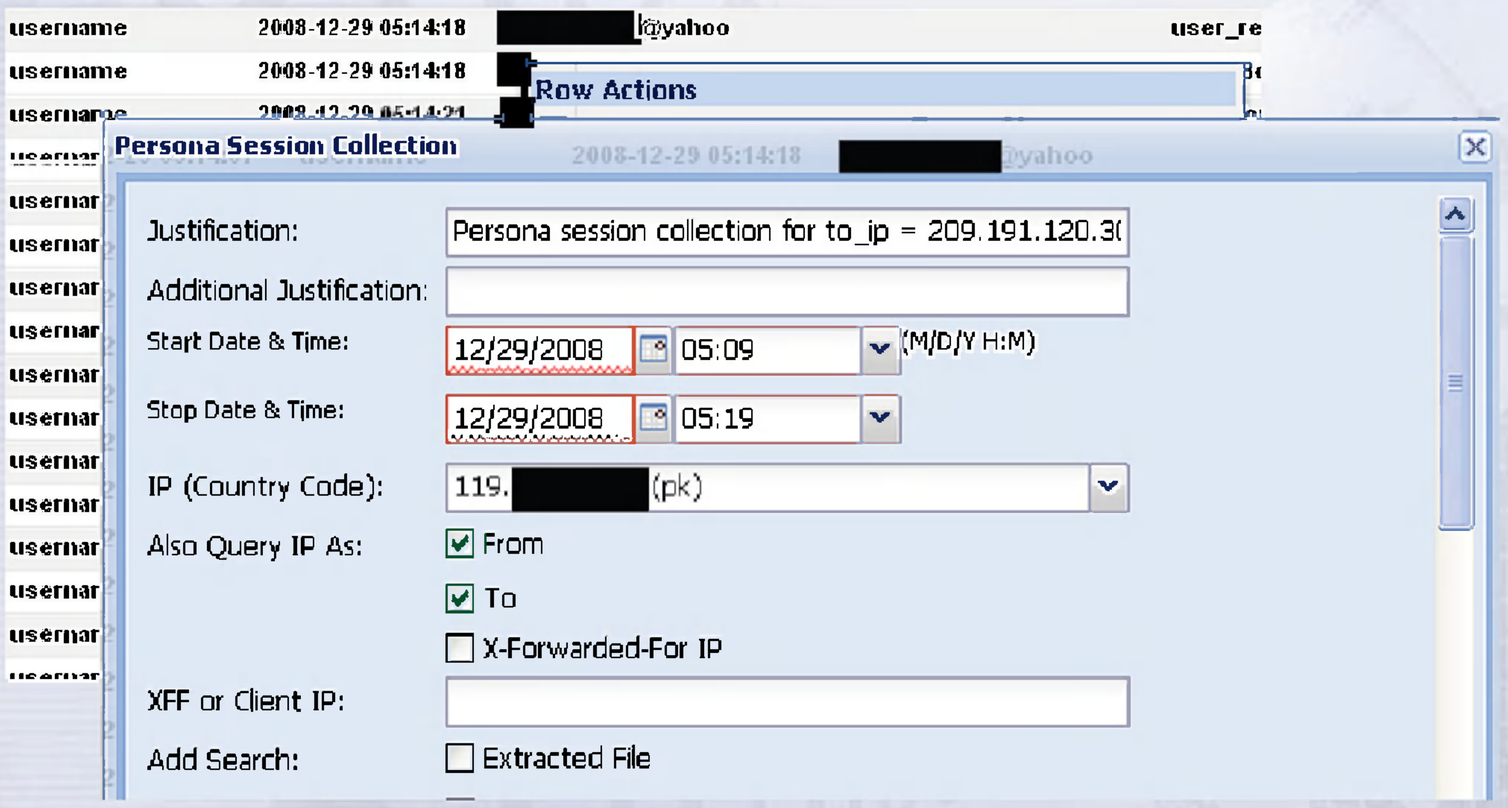
XKS SIGDEV: Persona Analysis

TS ▲	ACTIVE_USER	ACTIVE_USER_IP	ACTI
20081229 051406Z	[redacted]<yahoo>	119 [redacted]	PK
20081229 051406Z			
20081229 051406Z			
20081229 051407Z			
20081229 051409Z			
20081229 051410Z			
20081229 051410Z			
20081229 051410Z			
20081229 051411Z			
20081229 051414Z			
20081229 051415Z			
20081229 051420Z			
20081229 051420Z			
20081229 051421Z			
20081229 051426Z			

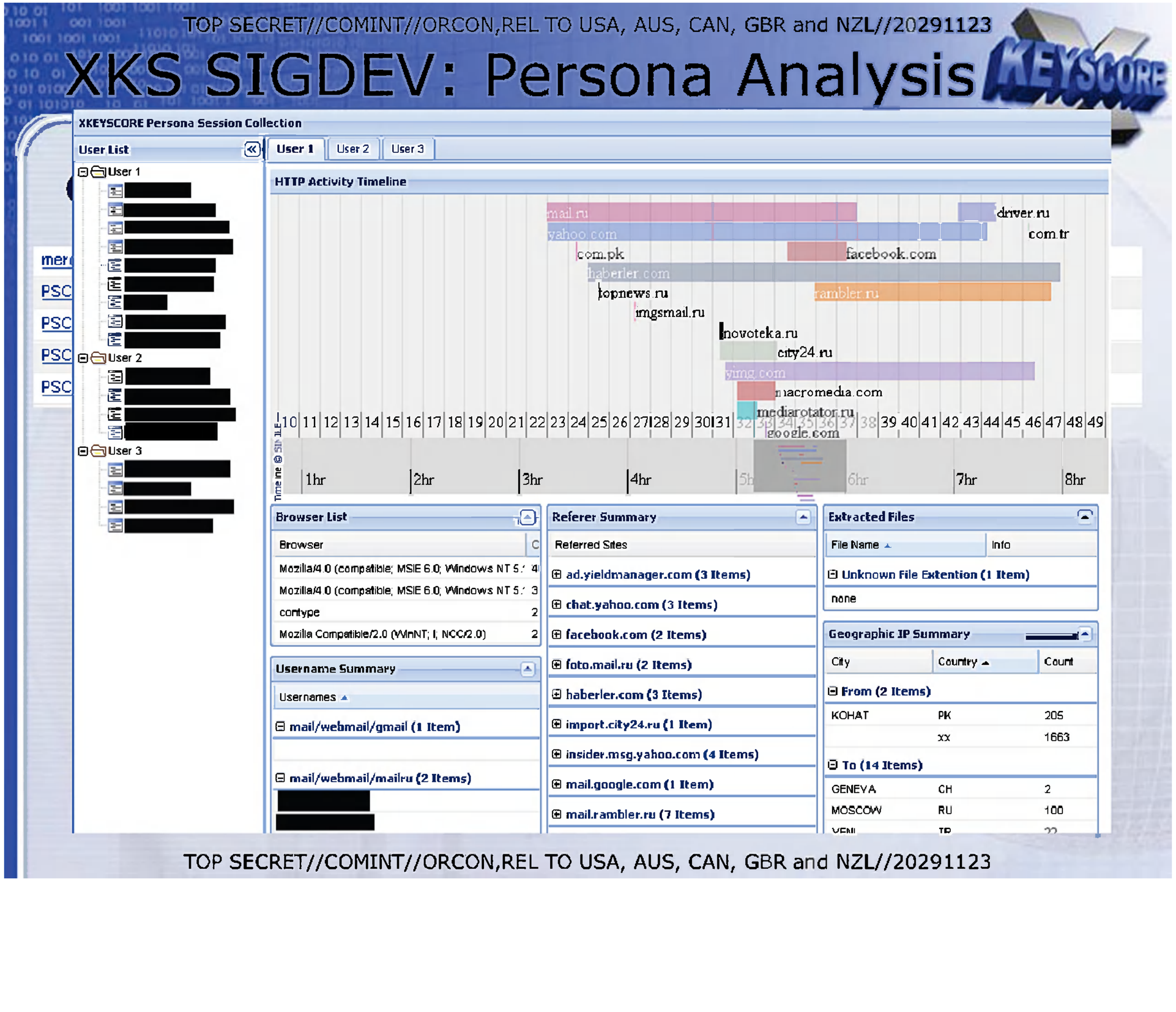
Datetime ▲	Search For	Datetime End	Search Value	Fm IP	To IP
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]	119.[redacted]	[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:07	username	2008-12-29 05:14:18	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]	119.[redacted]	[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:09	username	2008-12-29 05:14:21	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo	119.[redacted]	209.[redacted]
2008-12-29 05:14:10	username	2008-12-29 05:14:50	[redacted]@yahoo		

XKS SIGDEV: Persona Analysis

Coming soon: XKS PSC query builder/viewer



XKS SIGDEV: Persona Analysis



XKS SIGDEV: Persona Analysis

Coming soon: XKS PSC query builder/viewer

Username Summary

Usernames

- mail/webmail/gmail (1 Item)
- mail/webmail/mailru (2 Items)
  - [redacted]
  - [redacted]
- mail/webmail/mailru/post (1 Item)
  - [redacted]
- mail/webmail/rambler (2 Items)
- mail/webmail/rambler/post (1 Item)
- mail/webmail/yahoo (5 Items)
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

Web Searches

Terms	Search Engines
(None) (1 Item)	
none	

Traffic Summary

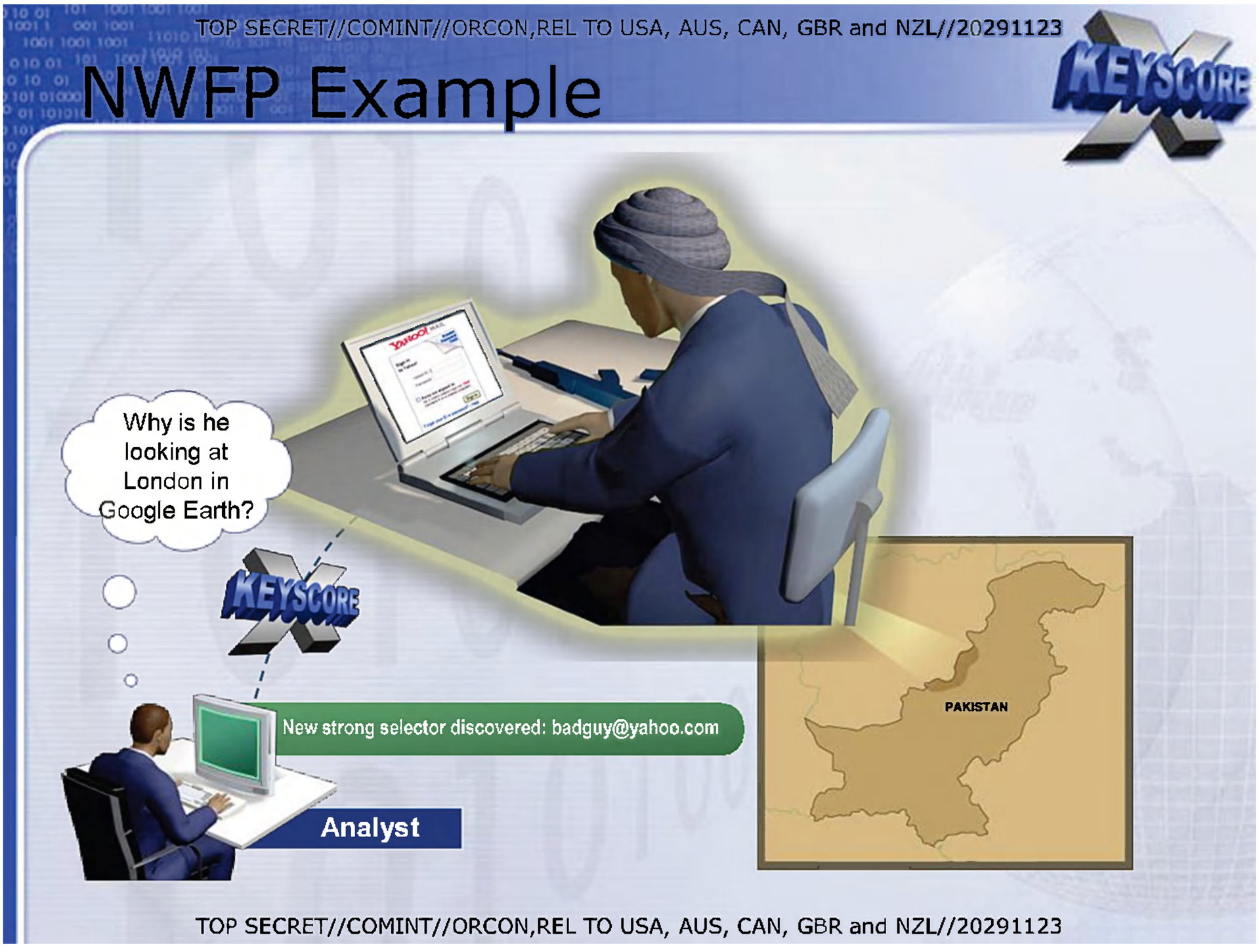
AppID or Fingerprint	C
advertisement	2
http	6
mail	1
news	2
social	1
unknown	1

Domain Summary

Subdomains

- adinterax.com (2 Items)
- adriver.ru (1 Item)
- akamai.net (1 Item)
- bn5.ru (1 Item)
- city24.ru (1 Item)
- com.pk (1 Item)
- com.tr (1 Item)
- facebook.com (2 Items)
- fbcdn.net (1 Item)
- gismeteo.ru (1 Item)
- google.com (1 Item)
- haberler.com (3 Items)
- imgsmail.ru (1 Item)
- macromedia.com (3 Items)
- mail.ru (7 Items)

NWFP Example



XKS SIGDEV: HTTP Traffic

Example: I **font Google queries co** **reas of Pakistan**

Informatic **in HTTP Activity m**

Fm IP	To IP	Fm Port	To Port
116.[redacted]	65.[redacted]	1233	80

Row Actions
- View Session
- View Session (New Window)
- Show All Row Values
- Mark Metadata row as Important

Query Marina for IP: 116.58.126.162
Datetime: 2008-12-29 07:21:42 (+/-) 3 hours
OK Cancel

- Un-Check where Fm IP Equals '116.[redacted]
- NKB Lookup
- Query Marina

Host	
www.g[redacted]	

Fm Country (IP)	Fm
PK	BA[redacted]

istan:WLL:PTCL

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

XKS SIGDEV: HTTP Traffic

KEYSCORE

TS ▲	USERID	PHONE	*USER_A*		*ACTIVITY*	USER_B
20081119 074259Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074259Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074304Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074316Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074316Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074316Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]

START_TIME	STOP_TIME	DURATION	CALL_DONE	IP_ADDRESS	USERID	PHONE_MAC_ADD
20081119 073141Z	20081119 092841Z	0d 01:57:00	UNK	116.[redacted]	[redacted]	[redacted]

[redacted]			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074357Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074357Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074357Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074357Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074358Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074358Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074358Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074358Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]
20081119 074511Z			[redacted]	<emailAddr>	logged in (email)	116[redacted]

TOP SECRET//COMINT//ORCON,REL TO USA, AUS, CAN, GBR and NZL//20291123

XKS SIGDEV: HTTP Traffic

Now make that into a workflow

```
=====================================================
!                    X-KEYSCORE EMAILER                    !
=====================================================
QUERY NAME: Waz_NWFP_Foriegn_Googlers
 current time: 2008-11-20 07:15:15 GMT
 submitted at: 2008-11-20 03:55:03 GMT
 has 14 result(s)
=============================================================
                  SEARCMES
=============================================================
www.google.com
--------------
 116.[redacted] 2008-11-19 18:54:20 : al qaida (en, en-GB) (1)
 116.[redacted] 2008-11-19 07:36:49 : The al-Ikhlas network (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 07:37:07 : (referer) the al-Ikhlas network (cybertrans from Arabic) (3)
 116.[redacted] 2008-11-19 08:03:17 : Forum bride/'Arus (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 08:05:51 : Forum love/gram (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 08:06:52 : (referer) forum love/gram (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 15:01:00 : The hills jihadist without inflicting (cybertrans from Arabic) (10)
 116.[redacted] 2008-11-19 15:14:13 : (referer) the hills jihadist without inflicting (cybertrans from Arabic) (6)
 116.[redacted] 2008-11-19 15:33:19 : Waziristan (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 04:24:44 : Scandals (cybertrans from Arabic) (2)
 116.[redacted] 2008-11-19 04:24:59 : (referer) scandals (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 04:29:29 : News (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 04:30:04 : Forum soil (cybertrans from Arabic) (1)
 116.[redacted] 2008-11-19 04:31:51 : (referer) forum soil (cybertrans from Arabic) (1)
```

Workflow Values | Workflow XML

X-KEYSCORE SIGDEV

- EX: Targets pass links to videos, use XKS to discover new targets who have viewed those videos

In HB 00215-09, he promises that the newest video will be ready very soon, and then sends these two links:

http://www.load.to/[redacted]
http://www.files.to/get/[redacted]

Datetime: 2 Weeks Start: 2008-12-23 00:00 Stop: 2009-01-06 23:59

HTTP Type:

Host: www.files.to

URL Path: /get/[redacted]

X-KEYSCORE SIGDEV

TS ▲	USERID	PHONE	*USER_A*	*ACTIVITY*	USER_B
20081231 224606Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224949Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224949Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224949Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224952Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224952Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 224952Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 225018Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]
20081231 225021Z			[redacted] <emailAddr>	logged in (email)	59.[redacted]

X-KEYSCORE SIGDEV

How to find technical documents of interest

One Idea: Take advantage of the properties exploited as meta-data by X-KEYSCORE like the Author and Organization

Lets look for all documents where the organization field is the company we're interested in, ex: Warid Telecom

Filename	Extension	Author	Last Author	Organization
PAR_MPBH_GUJ_To troubleshoot MPBH end for BSC23.doc	doc	[redacted]	[redacted]	Warid Telecom (Pvt.) Ltd.
PAR_MPBH_GUJ_To troubleshoot MPBH end for BSC23.doc	doc	[redacted]		Warid Telecom (Pvt.) Ltd.
wp for bbs troubleshooting 30-12-08.doc	doc	[redacted]	[redacted]	Warid Telecom (Pvt.) Ltd.
wp for bbs troubleshooting 30-12-08.doc	doc	[redacted]		Warid Telecom (Pvt.) Ltd.
Flexo Signs.xls	xls	[redacted]	[redacted]	Warid Telecom (Pvt.) Ltd.
Flexo Signs.xls	xls	[redacted]		Warid Telecom (Pvt.) Ltd.
LOI Warid for 3443 and 3444 Shortcodes.doc	doc	[redacted]	[redacted]	Warid Telecom (Pvt.) Ltd.
LOI Warid for 3443 and 3444 Shortcodes.doc	doc	[redacted]		Warid Telecom (Pvt.) Ltd.
Sohail Malik.xls	xls	[redacted]	[redacted]	Warid Telecom (Pvt.) Ltd.

Many of these files may have not been selected, because either there was no strong selector associated or the strong selector(s) weren't tasked for collection

Questions?

[redacted]@nsa

xkeyscore@nsa

HTTP Activity


```
GET /search?tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next HTTP/1.1
Accept: */*
Referer: http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: search.bbc.co.uk
Cookie: BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2f4%2e0%20%28cc
Cache-Control: max-stale=0
Connection: Keep-Alive
X-BlueCoat-Via: 66808702E9A98546
```

Host	URL Path	URL Args
search.bbc.co.uk	/search	tab=urdu&order=sortboth&q=musharraf&start=3&scope=urdu&link=next

Search Terms	Language	Browser	Via
musharraf	en	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)	66808702E9A98546

Referer
http://search.bbc.co.uk/search?tab=urdu&order=sortboth&q=musharraf&start=2&scope=urdu

Cookie
BBC-UID=b479a5f4ad230a53063d513630203acb22684634a0e0b164c45f96efc054cf950Mozilla%2f4%2e0%20%28com

Query Hierarchy