The Unofficial XKEYSCORE User Guide



E92 – ADET Consultant, Booz Allen Hamilton

The Unofficial XKEYSCORE User Guide	
Creating Queries	
Classic Queries	
Multisearch:	
Classic Searches (A-Z)	6
Creating a WorkFlow	
Searching - Tips and Tricks	
Which Query Is best for Me?	

Derived From: NSA/CSSM 1-52 Dated: 20070108 Declassify On: 20320108 TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108

Creating Queries

Clicking on Search at the top of the screen will bring up a list of searches in the Navigation Menu:



The Search screen has cascading menus of different Searches: Classic, Common, Dictionary Hits, File Transfer, Multisearch, Network Management, User Activity, VoIP, and Wireless.

Classic Queries:

Within the Classic Menu there are three folders: MultiSearch, Classic A-M, and Classic N-Z.

Multisearch:

Expand the Multisearch folder by clicking on the plus sign:

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



Multisearch IP Address:

The Multisearch IP Address query allows you to search on an IP address into seven different searches. Think of it as a federated query using an IP address. The Multisearch IP Address query searches on:

- User Activity ۲
- Phone Number Extractor
- **Email Addresses** •
- **Extracted Files** •
- **HTTP** Activity ۲
- Full Log
- Web Proxy •

Refer to some of the individual searches below for more information about specific queries

Creating a MultiSearch IP Address Query:

When you have filled in your query name, justified it, entered an IP address, selected your search engines and sites the last thing is to submit the query. If you select "Merge Results", then all of your individual queries will be merged into one consolidated result.

"Why would I want to merge my results?"

If you wanted to see all of the activity together to get a 'big picture' look at the IP address, regardless of the activity or application that is on the IP. The New GUI's results screens allow you to filter your results easily which may make viewing your results more intuitive. See "Viewing Your Results" in this Guide.

"What would I want to NOT merge my results?"

Viewing the results individually allows you to focus on a particular activity or result (e.g. Documents or email addresses).

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

Multisearch MAC Address:

The **Multisearch MAC Address** query is exactly the same as the IP address query except it only allows you to search on a MAC address. Follow the same instructions as the **Multisearch IP Address** query above but replace the IP address with your MAC address(es).

Fields Show Hidden Search F	ields Clear Search Values Reload Last Search Values					
Multiple Search: Mac Address						
Query Name:						
Justification:						
Additional Justification:	~					
Miranda Number:						
Dat e time:	1 Day 💽 Start: 2009-01-22 🖸 00:00	Multisearch MAC Address looks jus	C st			
Mac Address:		Ike the Multisearc	ch ,			
Content Must Exist;		except you must no	้าพ			
Max Results for a Single DB:	✓	search on a MAC	2			
Search Forms Clear	 User Activity Phone Number Extractor Email Addresses Extracted Files HTTP Activity Full Log Web Proxy 					
Save in my Favorites	No					
Load From my Favorites	✓					

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

Multisearch Username:

As you may have guessed, the **Multisearch Username** query is exactly the same as the IP Address Query and the MAC Address except it only allows you to search on a target's Username. Follow the same instructions as the **Multisearch IP Address** query above but replace the IP address with your Username(s).

Fields • Show Hidden Search	Fields Clear Search Values Reload Last Search	h Values	
Multiple Search: Us	ername		
Query Name:	Abujihan		
Justification:	ic: target in afganistan		
Additional ustification:		¥	
Míranda Number:			
Datetime:	Custor 💌 Start: 2009-01-3	22 🖪 00:00	Type in the username and domain (without the "@" symbol)
Jsemane;	abujihac		(without the @ symbol)
Domain:	yanoo.com		
Content Must Exist:			
Max Results for a Singlo DB:		*	
Search Forms Clear	 ✓ User Activity ✓ Email Addresses ✓ Full Log ✓ Logins and Passwords 		
Save in my Favorites	No	¥	

Loac From my Fayorites			¥
	-	(xks-central.corp.nsa.ic.gov:q0)	

"What is a Username?"

A "Username" in XKEYSCORE queries is the portion before the "@" symbol in an email address.

For example:

Abujihad@hotmail.com:

Username = abujihad Domain = yahoo.com

5

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

Classic Searches (A-Z)

There are 32 different searches between the A-M and N-Z searches. This guide will cover some of the most common searches. You will notice that most of the fields of the searches are the same and each individual query will be unique because based on its query name. For example, the **Extracted Files** search has fields that are only applicable to file attachments (e.g., file names, file extensions) and the **Email Addresses** query has fields for email addresses (e.g., username and domains). All of the Classic queries will have common fields like Ports, IP addresses, Countries, SIGADS, and CaseNotations that you can use to



Audresses are the	piug-
ins unique to each	query.

	40 <i>1</i>	:		Tc 💌	
	Countr Countr		The Ema to que	ail Address que rying on email	ery is catered addresses
Tie o	is ▼ Advanced Features ▼ Show Lidten earch: Phone Number Extra	leaxhFelcs Clea⊨Search Ionr	The Pl	hone Number	Query has
			F		
	Jery Name:				
	_ Listificat an:				
	Addiringal 1 isrification:				
1	Miranda Namber:				
1	נהר זוורהל	tionh 🗹 Storts	2008-12-24 📑 🛛	300 \$ Ston: 2009-01-28	*
	Enorg & imbra				
	Number Type:				
	Churty Jode:		I		
	Arn 1:	1			
	IP ≜ddress:			Ficm 💌	
	IP Address:			-v 💌	
	-1017:			Fich 😣	
	יחר:			- n 💌	
	Or unity:		~	zi m 🖃	
	Country:		Y	T₂ ~	

6

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

Email Addresses Query:

One of the most common queries is (you guessed it) an **Email Address Query** searching for an email address. To create a query for a specific email address, you have to fill in the name of the query, justify it and set a date range then you simply fill in the email address(es) you want to search on and submit.

That would look something like this...

Fields 💌 Advanced Features 💌 Show Hidder	Search Fields Clear Search Values Relcad Last Search Values
Search: Email Addresses	
Query Name:	abujihad
Just ficatior :	ct target in n africa
Addit on al Just ficatior :	v
Miranda Number:	
Datetime:	1 Mnnth () Start: 2008-12-24 🖪 00:00 🖴 🤅
Email Username:	abujihad
@Dcmair :	yahoo.com

NOTE: You DO NOT have to know an email address to use the **Email Address Query**. You can also search on an IP address*, domain name**, country, port, casenotation, protocol, SIGAD, MAC address, PID and more. If you search on something other-than an

email address (e.g., an IP address), your results will be all of the email addresses seen on those IPs.

* The IP must be hosted OUTSIDE 5-eyes countries

** The Domain MUST be foreign owned. Check WHOIS and NSLOOKUP for more info on your domain before-hand

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

Extracted Files Query:

1. <u>To find a specific file (i.e., if you already know the file name)</u>: For example, if you noticed a file name in your target's inbox and you never actually got the file attachment. This is VERY common for webmail collection because the attachment is often not put into PINWALE with the email.

Fields 🔹 Advanced Features 🔹 Show Hidden	Search Fields Clear Search Values Reload Last Search Values				
Search: Extracted Files					
Overy Name:	rth: esearch				
Justification:	Iranian Nuke files				
Additional Justification:	~				
Miranda Number:					
Datetime:	Cusion 💌 Start: 2008-01-24 💽 00:00 😴 Stop 2009-0				
Extractec Filename:	nuc eorindairy2343.pdf				
Extension:					
File Type (MIME Type):					
Is Obfuscated yes/no):					
Obfuscated Real File Extension:					
Ella tine for Dich					

2. To search for all files or specific file types on a particular area or on a network. (E.g.,

IP address). This is a GREAT query if you have a foreign mail server and want to see what files are collected on that IP address.

Reid. 🔹 Advanced Features 🔻 Show Hiddar	n Search Fields - Clear Search Yalues - P.elbad Last Search Values	
Scarch: Extracted Files		
Query Name	cíFí e se ar th	
Additional Justification		
Miranda Numcer		
Datesime	Cuntom	If you leave the Extracted Filenames
E: tracted Flaname		field blank, you are wildcarding the
Extension		search to look for ALL files names
File Type (MIME Type)		
Obfuscated Real File Extension		The IP Address of the mail server
Fila Size on Di≤k		you found using NSLookup in
Liata File Creatad		Foxtrall or your non-attrib Airgap
File Last Access		field
File Last Modified		пска
IP Address	2105.227.7J Ether	
JP Asdress	TJ .	

8

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

Logins and Passwords

1. If you already know the login and/or password.

Query Name:	Luginslu A ghan P]	
Justification:	Afghanistan network mai server password	If you know the	logins or passwords,
Additional Justification:		query on them as 1	long as they are unique
Miranda Number:		and will comp	ly with USSID-18.
Datetime:	1 Month 💌 Start: 2008-12-24 🖪 0	00.00 🖴 Stop 2009-01-23 🕅	
User Name:	admin		
Eassword:	w2o1		
Do nain;]	
IP AJURES:		Frum 💌	
IP Address:		To 🕑	
Pii I:		Fran 💌	
Pot:		Το	

"Where would I find passwords to use in this query?"

- Passwords can be found in TUNINGFORK (e.g., FoggyBottom), passed in the content of emails or text messages, or from previous XKEYSCORE queries.
- 2. Trying to discover logins and passwords on a network? NOTE: Logins and passwords are valuable tools to enable Tailored Access Operations (TAO).

"What tools would I use to get the network information like a Mail Server, or Name Server?"

NS Lookups tools on NSA net such as FOXTRAIL and Open Source tools such as robtex.com, centralops.net, and network-tools.com are a GREAT START. They provide you with IP addresses for domains. You can then query on the foreign-hosted IP addresses.

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

Fields 🕐 Auxanusu Factures 🔹 Shuw Hidden Search Fields - Claar Search Values - Reluad Last Search Values					
Search: Logins and Password	Search: Logins and Passwords				
Query Name: Just fication: Additional Just fication: Miranda Number: Datesime:	I oginsforAignaniP Afghanistan network meil server passwo	rds			
Jser Name: Password: Domain: IF Address: IF Address:		If you are trying to FIND logins and and you know the IP address for the then search on the IP!! Your results will be LOGIN PASSWORDS!	d passwords te network, NS and		

Phone Number Extractor

The **Phone Number Extractor** query looks through the content of an email for phone numbers. This is very similar to a PINWALE DoPhone query except the traffic that XKEYSCORE finds may be survey (i.e., unselected, non-tasked data) and might not be in PINWALE. XKEYSCORE may be your only hope at finding an email address for a target where you only have their phone number as lead information.

1. <u>Already have a phone number</u>? If all you have to start with as lead information is a phone number, you may find it useful to query on that phone number and see if anyone sent an email with that number in the signature line.

Field	ls 🔻 Advanced Features 💌 Show Hidden	Search Fields Clear Search Values Reload Last Search Values
se	earch: Phone Number Extrac	tor
	Query Name: Justification:	Afghan Afghanistan phone number ct target
	Additional Justification:	~
	Miranda Number:	
	Datetime:	1 Month 🔽 Start: 2008-12-24 🖸 00:00 🛟 Stop
	Phone Number:	
	Number Type:	
	Country Code:	
	Area:	
	IP Address:	From 💌
	IP Address:	To 💌

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

2. <u>Looking for any phone numbers on a network</u>? Quite often you know the mail server IP address and could use some telephone numbers to task?

Felds - Advanced Features - Show Holden	Search Fields - Clear Search Values - Reload Last Search Values
Search: Phone Number Extra	ctor
QJery Name:	Alghan
Justif cation:	Afghanistan phone number attarget
Additional Justification:	
Miranda Number:	
Datetime:	I fvonih 📝 Start: 2008-12-24 🗹 00:00 ♣ Stop: 2009-01-23 🖸 23:59 ♣ 🌍
Phone Number:	
Number Type:	
Cuuntry Cude:	
Area:	
IP Address:	
(P Address:	
5 J	

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

3. Looking for a phone number without the country code (non-normalized)? It's possible a target will pass their phone number without the country code (e.g. a signature line with "Tel: 5354658"). In that case, XKEYSCORE will not find the number with the country code so you must create a query that looks for fewer digits but still complies with USSID-18. This is not a 100% solution* but ANDing your query with a country or IP address would certainly be more compliant. See example below:

Phone Number: Number Type: Country Code: Area:		The number you enter here isn't normalized because you expect to see it in traffic without the country code. To make this USSID-18 Compliant you must AND this with something
IP Address:	From 💌	like a country or IP address.
IP Address;	Το 💌	5
Purl;	From 💌	This example shows traffic in/out of
Port;	lo 👻	Pakistan
Country:	P<	
Phone Number:		
Nunber Type:		This example shows traffic
Country Code:		in/out of a particular
Area:		network/IP Address



*If you ask XKEYSCORE to give you all Pakistani traffic, it's doing an NKB lookup on all Pakistani registered IP addresses. Geolocation of IP addresses is not 100% accurate at this time. Unofficial estimates say asking for all of Country X's traffic will find between 50-60% of the actual traffic. (That's more than 0%, though, right?)

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

HTTP Parser

The **HTTP Parser** query looks for web activity (remember, HTTP = web) on a particular link. This query is useful for several reasons. Firstly, if you know a particular website and want to see if a foreign target visits it (e.g. an extremist web forum URL, or maps.google.com). Secondly, this query enables you to query on a network IP(s), casenotation, or country and see what websites we don't know about (survey-type query).

Here are two examples

1. <u>If you know the particular website the target visits</u>. For this example, I'm looking for everyone in Sweden that visits a particular extremist web forum.

Search: HTTP Activity		
Query Name:	HTTP in Sweden	
Justification:	SwedishExtremist website visitors	
Additional Justification:	×	The website LIPL (aka "host) is
Miranda Number:		entered in with a wildcard to
Datetime:	1 Week 🔽 Start: 2009-01-20 🖸 0	account for "www" and "mail" other hosts.
НТТР Туре:	×	To comply with USSID-18 you
Host:	*al-hisbah.com	must AND that with some

Scroll down to enter a c	country code (Sweden is	other information like an IP or	
Country:	9-	Lither V	country
Country:		¥ 10 ¥	

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

2. <u>If you don't know the website but you know the network information (IP)</u>. For this example, I'm querying on a network IP block to see all of the websites the target visits.

Search: IITTP Activity	
Query Name:	WebUseIrenians
Justification:	Websiles For ranian University
Additional Justification:	v
Miranda Number:	
Datetime:	1 Week 👱 Start; 20 ⊆01-20 🖸 00:00 🚓 Stop: 2009-01-27 🖸
HTTP Type;	~
Host:	
UKL Path:	
URL Args:	The website LIRLs (hosts) are
Search Terms;	left blank to wildcard those
'LancLege*:	fields.
Character Encoding:	V
Contert Stort:	
Content Stop:	
Contert Intal	
Referer:	
X Forwarded For:	

To comply with USSID-18 you AND that with some other information like an IP or

country		
\leq	IP Address:	210. Either 💌
	IP Address:	То 💌
	Port:	From 💌
	Port:	Το 💌

Results from an HTTP Parser query

This shows what the results from a query look like for an HTTP Parser query:

	12	<u>ں</u>	JM (()						
-	-Site	17 -	Later the	Deterine End	FTP Type	Host	UNL YORN	URL WHE	Search Terms
3	<u>لم</u>	1	2009-01-22 11:46:25	2409-01-27 11:48:25	past	f-gaming.com	.s.stat.php		
□	E	2	2009-01-27 11:19:15	2009-01-27-1110-00	hoar	memi žu tu	Aistat.php		
	E	3	2409-01-27 11:55:45	2008-01-27 11:55:49	Vilast	candy-cou ntry.com	.newpapaka/s		
Π	E	4	2009-01-27 11:39:58	2009-01-27 11:40:08	hoar	mambauru	Asstat.php		
Π	E\$	5	2009-01-27 11:25:12	2009-01-27 11:25:14	past 🔪	candy-country.com	ленрара ка /з		
⊡		<u>e</u>	2009-01-27 11:09:41	2409-01-27 11:09:42	past \	mambauru	A-stat.php		
⊡	E.	I	2009-01-22 11:29:47	2409-01-27 11:23:51	past 🚶	manibauru	Arstatiphp		
⊡	M	1	2009-01-27 11:00:32	2409-01-27 11:06:32	response				

Example 1 above shows a person was visiting <u>www.f-gaming.com/s/stat.php</u>

Host = f-gaming.com

URL Path = /s/stat/php

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

Document Metadata

Document Metadata query allows you to search on document authors, organization, encryption*, and many other things about a document. This is extremely helpful if you have found a file attachment from a target (e.g. Brick-and-mortar targets, person, or Organization) and you want to see all of the other files they have sent. With the Document Metadata query you don't have to know the email address of the person sending the document, you just have to know the document's properties.

*Most Microsoft Office allows uses to encrypt files by clicking Tools -> Options -> Security and password protecting the files. The Document Metadata query looks for that type of encryption. It doesn't look for PGP or other 3rd party encryption.

"How do I find a document's properties?"

The easiest way to see this is to open a MS Office document and click on File -> Properties. To find the document properties for a file you target sent, the easiest way is to view the file in Agility and click on Properties.

Finding your target's file properties

If you can view the target's document in Agility, click on the Properties tab to show the target's Organization and/or Author. If the fields are unique or random enough you can query on the term itself. If the Organization or Author aren't enough to comply with USSID-18, then you must AND that query with supporting information (IP or Country).

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

Displaying MS Word document in Agility:

entre de la la la la color de la	1195	ERRET GERMAN FORMER	2156 (SECING / 200291191)	1-1-1	1.1.1
2월 1월에 1월에 100k (월요즘).일이는 180k [1	107.5	elker, yeb mintyykkeri ne e			
	Fin	0.5(34)	Sing 24	Fire (b) Type : 7	Free
3		5030032.026	13 FM Canbre or Tearl Case	2 India	71
9		V15600711	1.12.78	1 best/icm	and
U		50500B305	25 Fbl Tes vice the Dutic	3873 opplodier.hold	i-then bos
12		015600771	22 -18 der: k	fud application to	244 214
~		PRINCIPAL INC.		F) opplodier."ex	ne bos
5		01,8200	0000	The appoint of	70 MPC
	· · · · · · · · · · · · · · · · · · ·		3898	application/octet-	-strear
*]	the standard and		150		
Depis, pignal Roy, SY Picadar (Properties	Control Carl Trater	Colocod Dec Sea	🧹 462	application/msivo	rd 🐧 📋
	Dag	ument Properti			
Category			50	application/mswo	rd
Сопрану					
HiddenSlideCount	a				
LineCount	243				
LinksUp To Date	13.58				
Мападат					
MMClipCount	(25)				
NoteCount	29				
ParagraphCount	18				
PresentationTarget					n –
ScaleCrap	1.58				
SlideCount	8				
AppName	M crosol. woru				
Author		>			
ChargeterCount	352.2				
Comments					
Out Owned at	G/12/2008 3:13:3	00 A M		Author =	
UBIECrebied	the second se	and the second se			
SecurityLevel	rone		I ant	Author -	

To create a query in	XKEYSCORE from	this information:
----------------------	-----------------------	-------------------

Search: Document Metadata	
Query Name:	foriegndocuments
Justification:	Swedish CT Target
Additional Justification:	~
Miranda Numper:	
Datstime:	1 Week 🔽 Start: 2009-01-20 🖸 00 00 🗘 Stud: 2009-01
Document Type:	
Encrypted?:	
Corrupted?:	
Filename:	
Extension:	
"Subject":	
Creation Time;	
Last Modified Time:	
'Unique I <u>D* [fultent]</u> ;	
Author:	GoGo
Last Author:	

16

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

View of document properties of PDFs in Agility:



To create a query in XKEYSCORE using this information:

Search: Document Metadata	
Query Name:	furiegnducuments
Justification:	Swedish CT Target
Additional Justification:	▼
Miranda Numher:	
Datetime:	1 Week 💽 Start: 2009-01-20 🖸 00:00 🗘 Stop: 2009-01-27
Document Type:	pd.
Encrypted?:	
Corrupted ?:	
Fiename:	
Extension:	
* Subject *:	
Creation Tma:	
* ast Modified Tma*:	Author =
Un que <u>ID [fulltext]</u> ;	
Author:	

17

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

Creating a WorkFlow

Workflows are periodic queries you can set up that run at specified times. They are great for sustained targets because they query the database for you (e.g. every night) and you can easily view the recently collected traffic without having to create a new query each day. They are also very helpful if you are performing target discovery on a network and haven't seen much traffic yet on a selector. A workflow for an email address can bridge the gap between when you discover the selector (and you task it to UTT/Cadence) and when it actually makes it to the appropriate dictionaries).

It's important to understand that a normal (ad hoc) query is submitted when you hit Submit. Workflows, on the other hand, are created then submitted to the XKEYSCORE team for review. The XKEYSCORE team does not review it for USSID-18 compliance (that's up to you); they only review it to ensure your query won't strain the system with too complex a query.

	XKEYSCORE
🏦 Home 🗻 Users 🖀 Workflow Central 🔍 Search 🔟 Results 📓 Statistics	🌄 Preferences 🕜 Help
Navigation Menu 🛛 👘 Histo: Query Type 📧	
🖻 🔄 Results 🔹 👘 Clear Selection	

The first step in creating a Workflow is click on Workflow Central:

Then click on Request on the left to start the Workflow Request Wizard, and then click Next.

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

orkflow Central Request Wizard
Welcome to the X KEYSCORE Workflow Request Wizard.
This wizard will guide you through the process of creating a Workflow.
A Workflow is an standing query that will execute at a specified time or interval. In addition, a workflow can execute follow-on actions once the query has completed. Follow-on actions are scripts that perform certain tasks such as sending email or creating a summary of the results through specified SQL queries.
Upon completion of this wizard the workflow will be submitted for approval.
Cancel 4 Frev

Next, select the search type you want to create from the pull-down menu. For this, I'm selecting an **Extracted Files** query. These queries are essentially the Classic A-M and N-

Z queries you have seen in the Classic Search screens. The only difference is an **Extracted Files** workflow will start looking for extracted files in the future and an ad hoc **Extracted Files** query will search in past/previous collection.



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

Next, fill in the name of your query ("AfghanFiles"), the auditor-compliant justification, and how often you want the query to run. I recommend offsetting the time from the default of midnight (2400) by a few hours (before of after). For this, I'm selecting 0400. Then hit NEXT.

know central request wizord			
Basic Information			
Query Name: Query Justification: Additional Justification: Micarue Number:	ntiles gətin afçhanistan		
Run ∋very 24 ¥ H	turs - Starting at	400	
Recourring Search One Time S	oarch		_
Basic Features Help			
			 _

In the Add Search Fields window, you will select the search criteria that you want to search on. In this example, I'm looking for specific file attachment (DOC or PDF or XLS or PPT) on a specific Afghanistan IP address.

You must hit the green "+" symbol to enter the search criteria.

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

Add Search Fields Search Field Search Value Remove Extension DOC or PEF or XLS or FPT Image: Comparison of the provided and the provided a	alow central Request 4	Wizard		
Search Field Search Value Remove Extension DOC or PDF or XLS or FPT Image: Comparison of the comparison	Add Search Fields			
Extension DOC or PDF or XLS or FPT From IP Address CR To IP Acdress 203 Datetime Image: Comparison of the search Single Field Search Multiple Field Search Search Value Help Image: Comparison of the search	Search Field		Search Value	Remove
From IP Address CR To IP Address 203 Datetime Image: Comparison of the second o	Extension		DOC or PDF or XLS or FPT	*
Datetime Single Field Search Multiple Field Search Search Value Help	From IP Address CR To I	P Acdress	203	2
Single Field Search Multiple Field Search Search Value Help	Datetime		·	-
Search Value Help	Single Field Search	Multiple Field Search		
	Search Value Help	~		

Click Next

<u>Single Field Search</u> only searches in one field (e.g. File Extensions)

<u>Multiple_Field_Search</u> allows you to search on several fields (e.g., *To IP* AND *From IP*)

Add Search Fields	-
Search Field	s
Extension	D
From IP Address OR To IP Address	2
File Last Modified From IP Address To IP Address From Port To Port	
Single Field Search Multiple Field Search	
Search Value Help	

Next, you will select the sites where you want your query to run. Scroll down in this window to use the convenient "Select All" or "Uncheck All" buttons.

NOTE: If your selector is NOFORN, you must DESELECT sites that are 2nd/3rd party.

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

	Texas (mr1vwa1.tex.f.nsa:xs_web_db) TIMBERLINE (timberline:xs_web_db) xks voip 1 (xksvoip1:q0) xks voip 2 (xksvoip2:q0)		
	Yakıma mıssion system (j<2kəyscore2a.yrs.f.nsa:xs_web_db) Content must exist Check All Incheck All		
_	Basic Features Help		
< Car	ncel 🖣 Prev 🔰 Next Su	bnit)

Click Next

Follow-on Actions tell XKEYSCORE to do things after it runs your query. For example, it can email you with the results, or it can send them to Agility, or any combination of the two. For this example, I want XKEYSCORE to email me telling me I have results and I want it to download my results to Agility. Make sure you select Send to Agility if you want the same.

tiow Central Request	Wizard		0
Follow-on Actions			
Would you like to ac	ld any follow on actions		
O ND			
⊙ Y∋s			
Surpl	Script Arguments		Ali
Directual Sessions	User .D		-
	Crnal To	Birisa.ic.gov	
	Food Subject:	You have results!	
	Emai Content:	Go check Aginy My man	
	ROWR:		
	Filename:		
	Mai Qıcer Trigr∠ph:		
	GZIP:	Compress Contents	
	Send To Aglity	Send To Acility	
<u> </u>			

Click the Green Add symbol, and then click next when finished. On the next screen, enter any comments you wish (optional) and click Next

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

Lastly, click SUBMIT. Your query isn't active yet. The XKEYSCORE team will review it and you will have to check back later and turn the query ON or OFF as you wish.

G-I Genuest	Hé	ep Actions 🔨				
My Worktows		Query Туре	Guery Name	Last Modified	Stete 🔺	Actions
	1±	phone_ runiber	HERNANDEZION	2009-01-19-21.47.40	u r (aks)	
	Œ	phone_number	laras_phones	2009:01 19 21:47:40	01 (%kɛ)	
	t±	phone number	SWEDISTPHORES Cruz	2009-01-19 21:47:40	on (xks)	<u>े 🗶 🔾 ह</u>
	G	phone_number	Fr MFA Doc 2008	2009-01-19 21:47:21	off	97028
	÷	phone_number	iragi_Nela2006_telecom	2009-01-19 21:47:21	011	2×0/28
	Œ	phone_number	MutindThones	2009-01-19 21:47:21	off	280/8
	G	http_rarser	pakisten/F_KRI	2009-01-19 21:47:21	off	280/28
	Œ	http_parser	VYebrorum 2.0	2009-01-19 21:47:21	off	2*0/5
	G	http_rarset	web thun?	2009-01-19 21 47 71	off	280/28
	1e	l pijtoTrausei	Emul usty	2009-01-19/21.47.21	off	9×021
		phone_number	ZTØ_OPSUMVERCLEA	2009-01-19 21:47:51	off	480/8

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

Searching - Tips and Tricks

The Official XKEYSCORE Frequently Asked Questions page is located here: <u>http://xkeyscore.rl.r.nsa/redmine/wiki/xkeyscore/FAQ</u>. Here are some other tips/tricks that may be useful

1. Underscores in usernames:

If your selector has an underscore in it, you must precede the underscore with a backslash. For example: **abu_jihad** would become searched as **abu_jihad**. If you leave the underscore in the query without the backslash, you are wildcarding a single character (see below).

<u>To search on:</u> abu_jihad@hotmail.com: Bad query: Abu_jihad Good query: Abu_jihad

If you search on "abu_jihad" (without the backslash), you could bring back "abu1jihad", "abuTjihad", "abuSjihad", "abu-jihad", etc... because you are wildcarding that character and therefore you would be pulling on an entirely different selector.

2. To search on a range of IP addresses:

IP Address Range: 202.82.86.224 - 202.82.86.244

Becomes this XKEYSCORE Query (entered in the IP Address as To, From, or Either): regex:202\.82\.86\.22[4-9] OR regex:202\.82\.86\.23[0-9] OR regex:202\.82\.86\.24[0-4]

OPERATOR	DESCRIPTION	USAGE
!	Not Equal Comparison	beginning of word (i.e. !joe and !sam)
or	Logical OR (Search for multiple values)	between words (i.e. osama or laden)
and	Logical AND (Search for combination value matches)	between words (ie. *osama* and *laden*) takes precedence over ORs
*	Multiple Character Wildcard	anywhere in word (i.e. *osam*bin*laden)
-	Single Character Wildcard	anywhere in word (i.esambin_laden)
>	Greater Than Comparison	beginning of word (i.e. >00080 and <00111)
<	Less Than Comparison	beginning of word (i.e. >00080)
regex:	REGEX Expression	(i.e. to retrieve only numbers: regex:[0-9]*)

3. Boolean Search Descriptions (Wildcards, ANDs, ORs, etc):

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

Which Query is best for me?

Quite often the most difficult part of using XKEYSCORE is deciding which query to use at which time. Here's a rough guide to help you decide.

Do you have an IP Address and want to learn more about that network





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

Do you have an Email Address or Foreign Domain And want to learn more about it?

Which XKEYSCORE Query is Best for Me?



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

Do you have a phone number for your target and want to learn their email address?

Which XKEYSCORE Query is Best for Me?



The PHONE NUMBER EXTRACTOR query and search on the PHONE NUMBER(S).

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