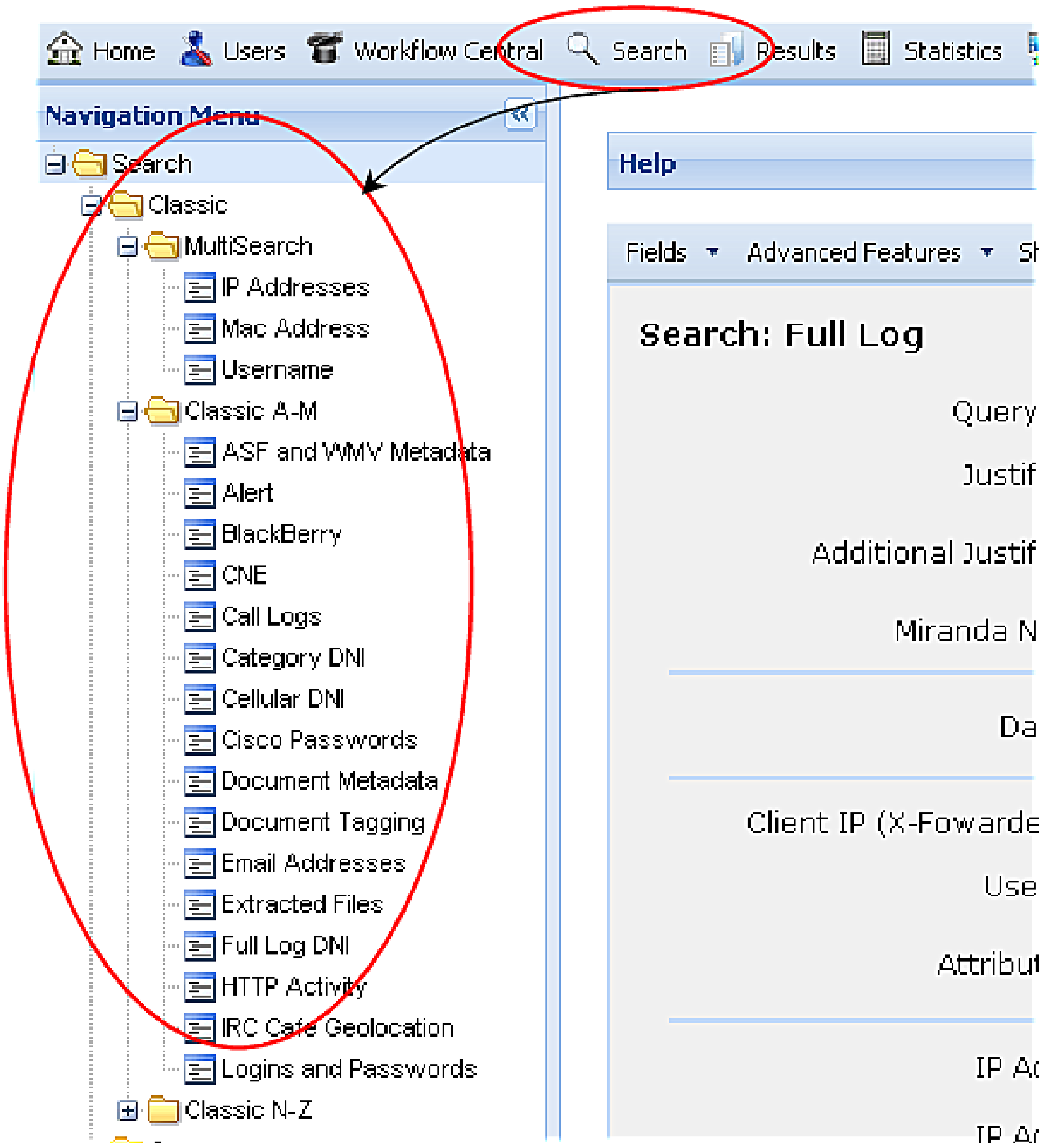
The Unofficial XKEYSCORE User Guide

[redacted]
E92 – ADET
Consultant, Booz Allen Hamilton

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

Creating Queries

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



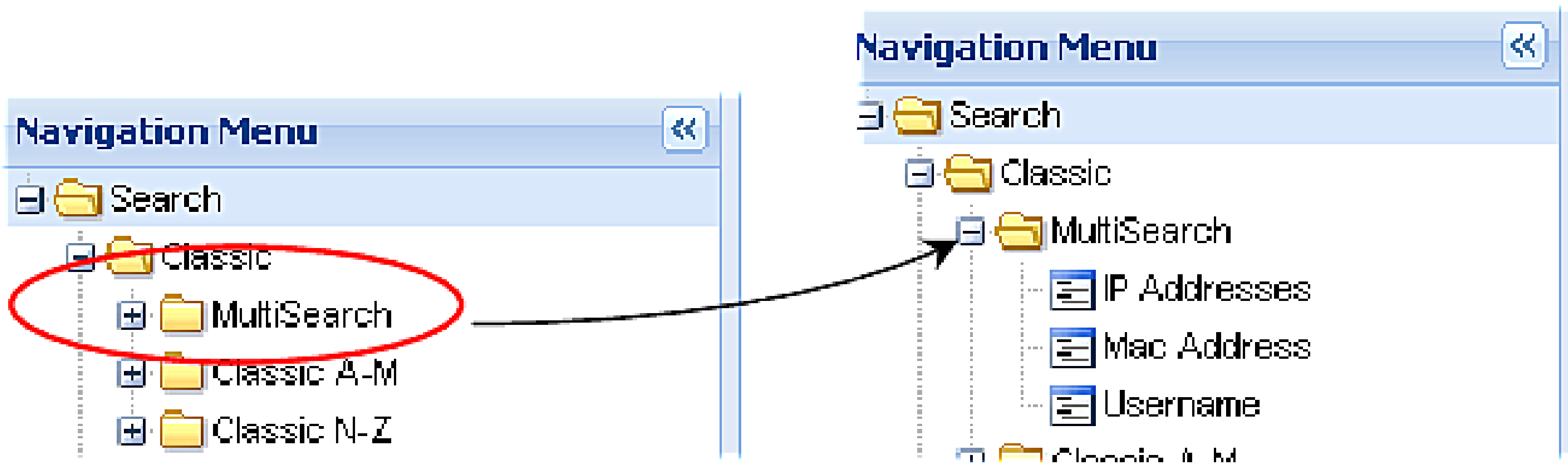
The Search screen has cascading menus of different Searches: Classic, Common, Dictionary Hits, File Transfer, Multisearch, Network Management, User Activity, VoIP, and Wireless.

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:



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
- Phone Number Extractor
- Email Addresses
- Extracted Files
- HTTP Activity
- Full Log
- Web Proxy

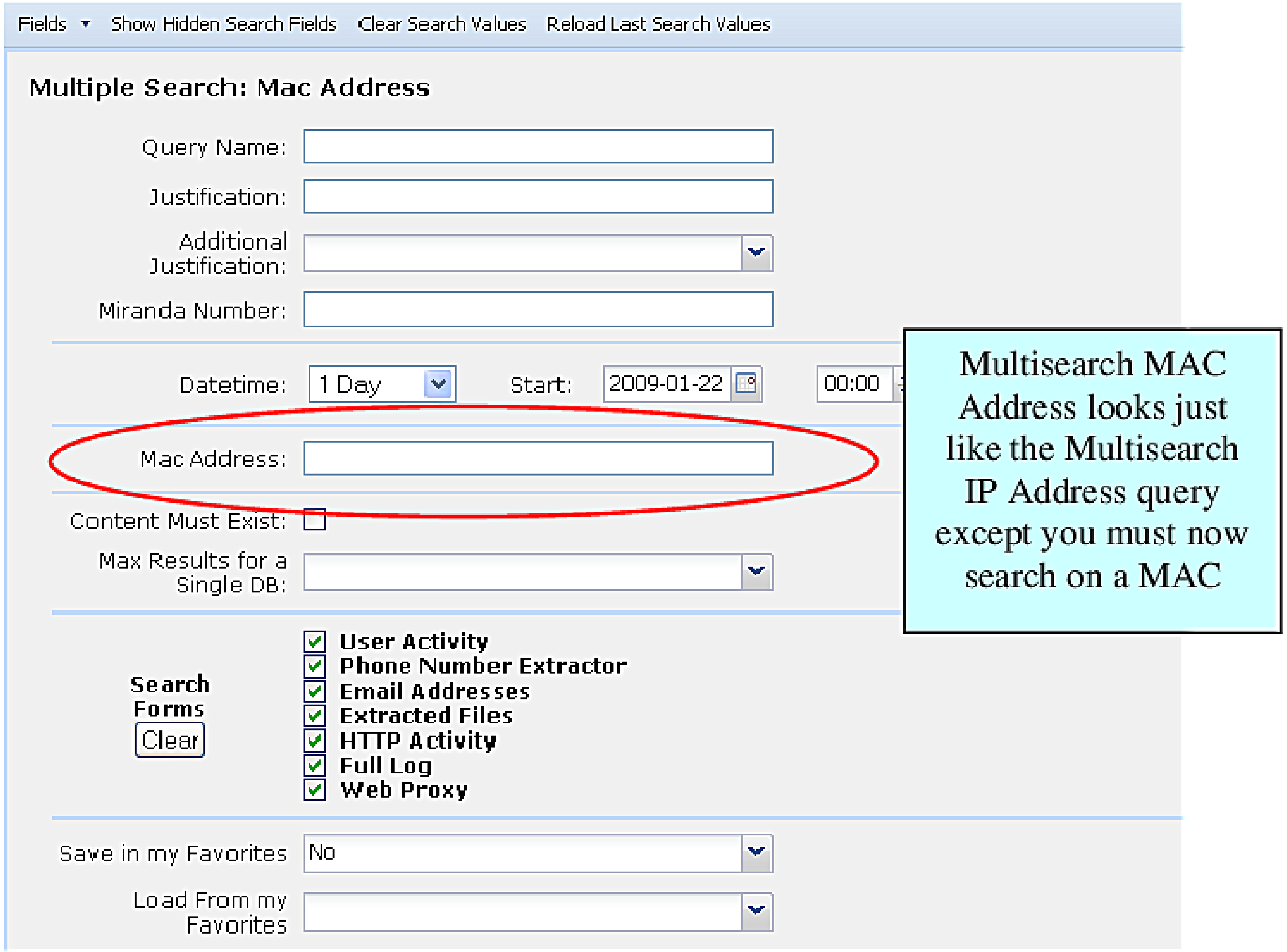
Refer to some of the individual searches below for more information about specific queries

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).

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).



Multiple Search: Mac Address

Query Name:

Justification:

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-01-22 00:00

Mac Address:

Content Must Exist: □

Max Results for a Single DB:

Search Forms
☑ User Activity
☑ Phone Number Extractor
☑ Email Addresses
☑ Extracted Files
☑ HTTP Activity
☑ Full Log
☑ Web Proxy

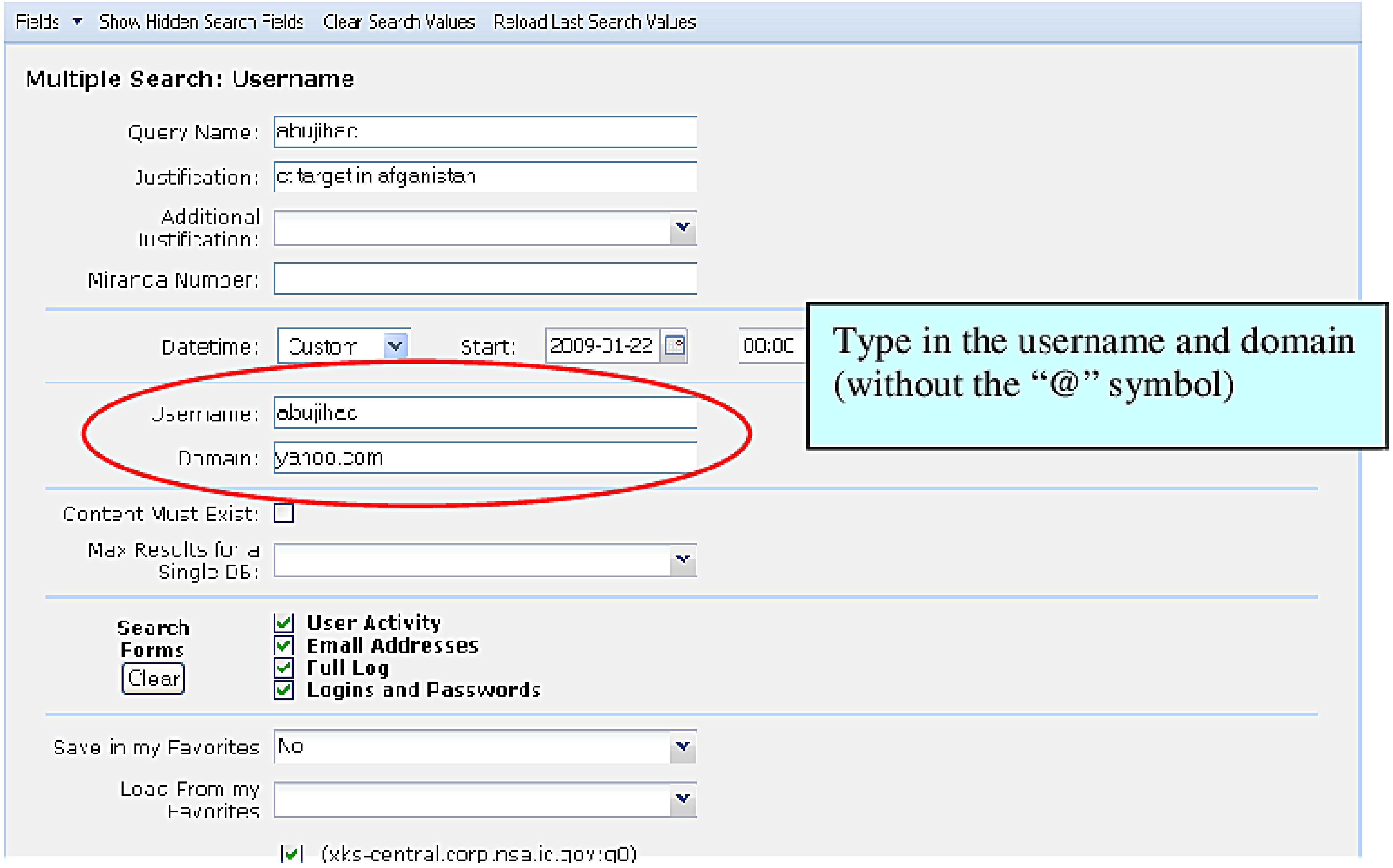
Save in my Favorites: No

Load From my Favorites:

Multisearch MAC Address looks just like the Multisearch IP Address query except you must now search on a MAC

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).



Multiple Search: Username

Query Name: abujihad

Justification: c: target in afganistan

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2009-01-22 00:00

Username: abujihad

Domain: yahoo.com

Content Must Exist: □

Max Results for a Single DB:

Search Forms

☑ User Activity

☑ Email Addresses

☑ Full Log

☑ Logins and Passwords

Save in my Favorites: No

Load From my Favorites:

☑ (xks-central.corp.nsa.ic.gov:q0)

Type in the username and domain (without the "@" symbol)

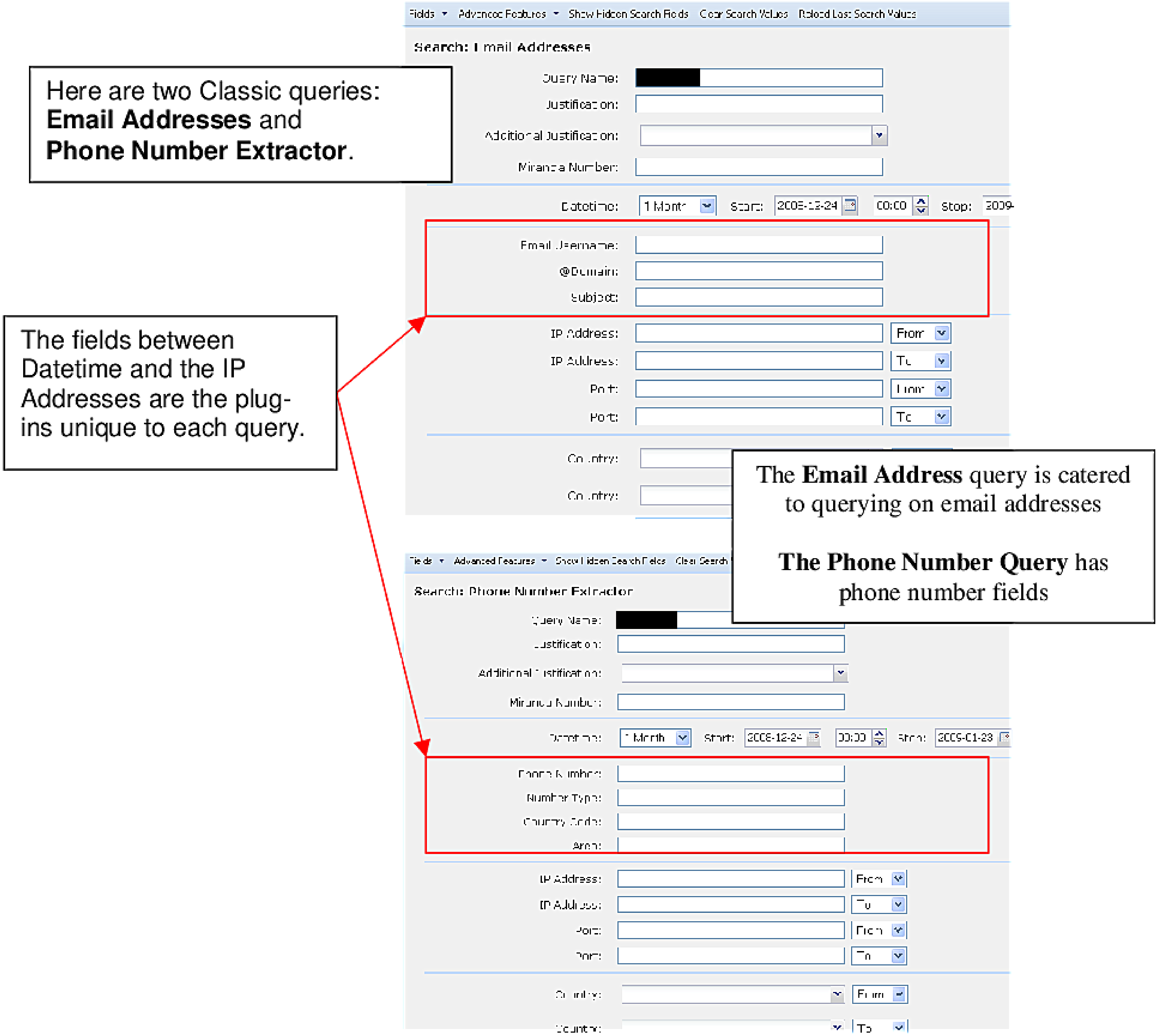
"What is a Username?"
A "Username" in XKEYSCORE queries is the portion before the "@" symbol in an email address.

For example:

Abujihad@hotmail.com: Username = abujihad
Domain = yahoo.com

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



Here are two Classic queries: **Email Addresses** and **Phone Number Extractor**.

The fields between Datetime and the IP Addresses are the plug-ins unique to each query.

The **Email Address** query is catered to querying on email addresses

The Phone Number Query has phone number fields

Search: Email Addresses

Query Name: [redacted]
Justification:
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00 Stop: 2009-
Email Username:
@Domain:
Subject:
IP Address: From
IP Address: To
Port: From
Port: To
Country:
Country:

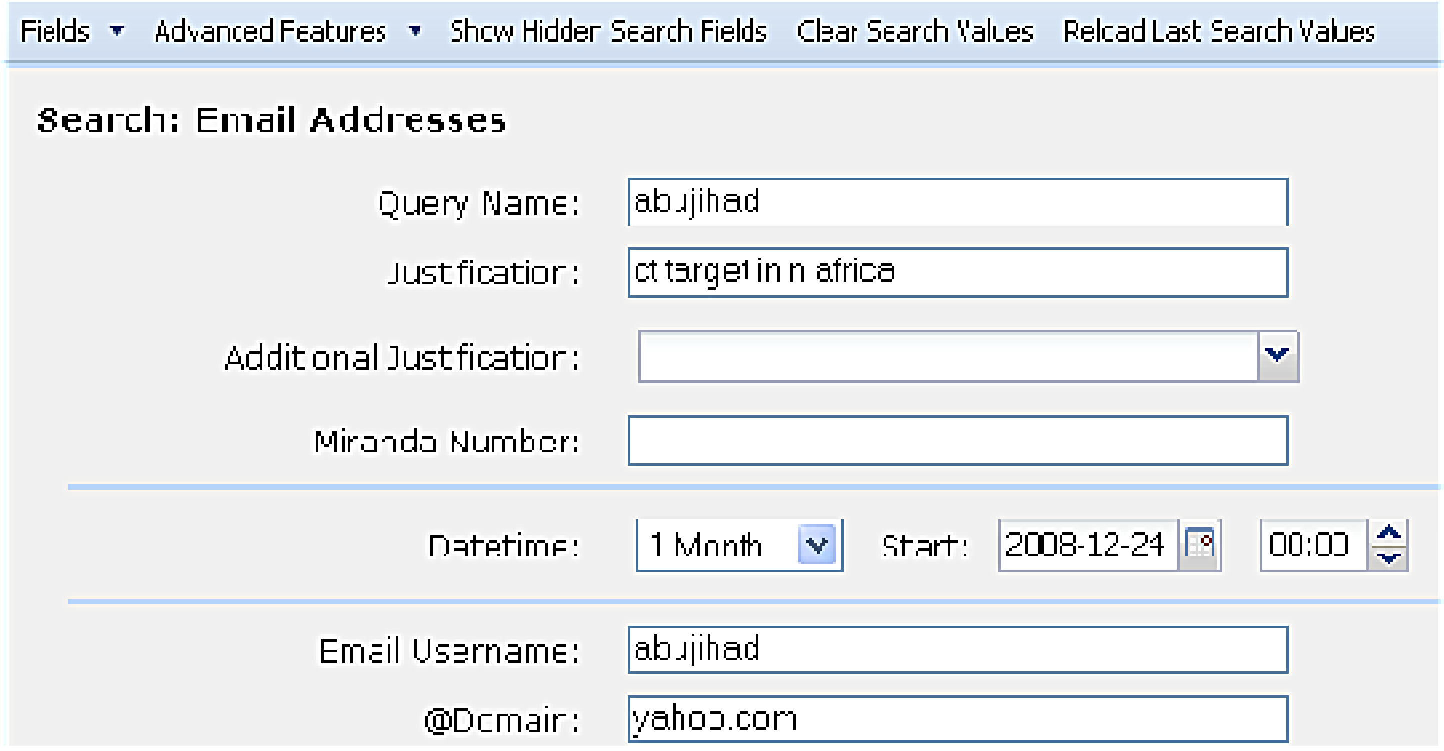
Search: Phone Number Extractor

Query Name: [redacted]
Justification:
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00 Stop: 2009-01-23
Phone Number:
Number Type:
Country Code:
Area:
IP Address: From
IP Address: To
Port: From
Port: To
Country: From
Country: To

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…



Search: Email Addresses

Query Name: abujihad

Justification: ct target in n africa

Additional Justification:

Miranda Number:

Datetime: 1 Month Start: 2008-12-24 00:00

Email Username: abujihad

@Domain: yahoo.com

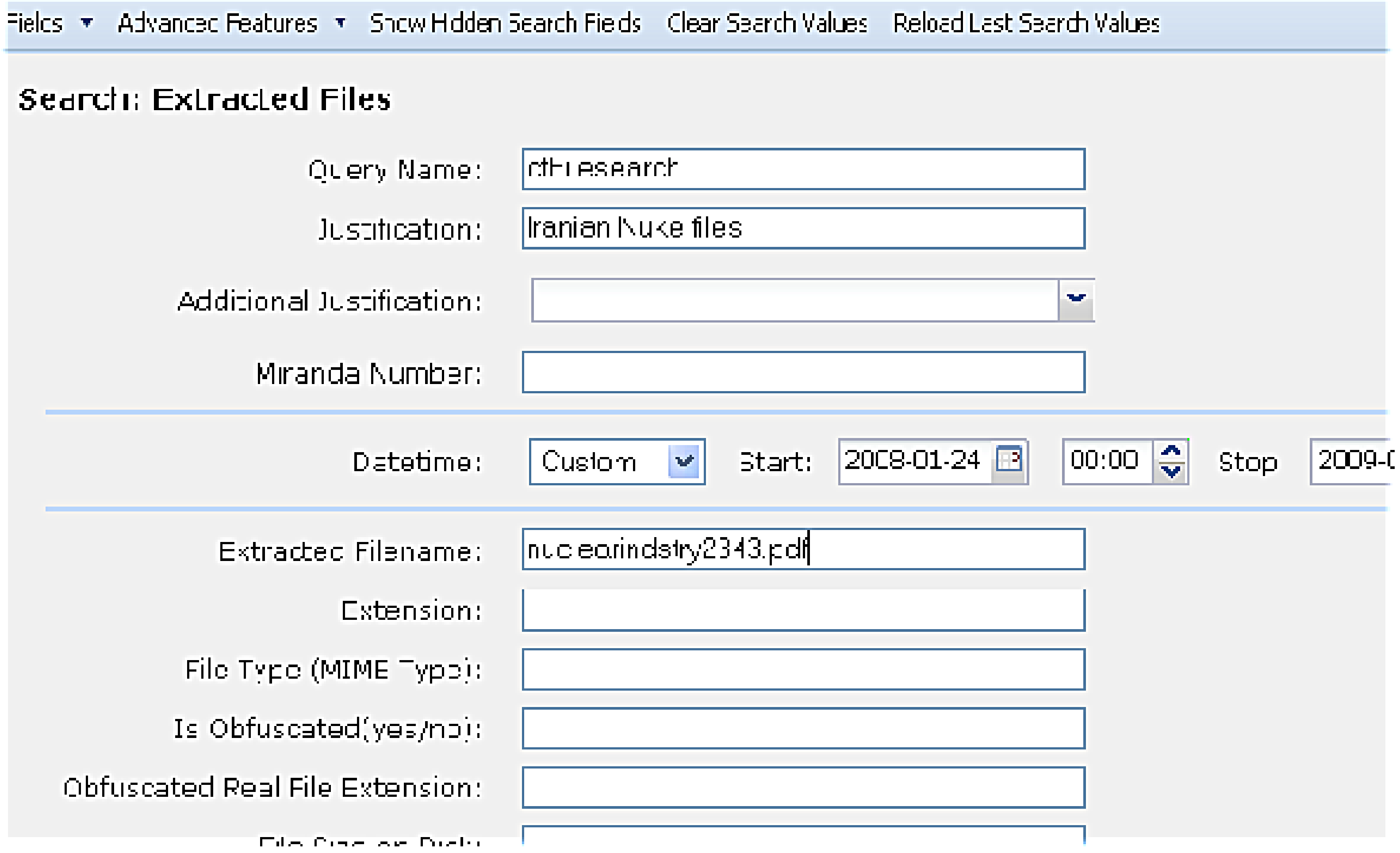
NOTE: You DO NOT have to know an email address to use the **Email Address Query**. You can also search on an IP address*, domain name**, country, port, casenotation, protocol, SIGAD, MAC address, PID and more. If you search on something other-than an email address (e.g., an IP address), your results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

Extracted Files Query:

1. To find a specific file (i.e., if you already know the file name): 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.



Search: Extracted Files

Query Name: ctFilesearch

Justification: Iranian Nuke files

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2008-01-24 00:00 Stop 2009-

Extracted Filename: nuclearindstry2343.pdf

Extension:

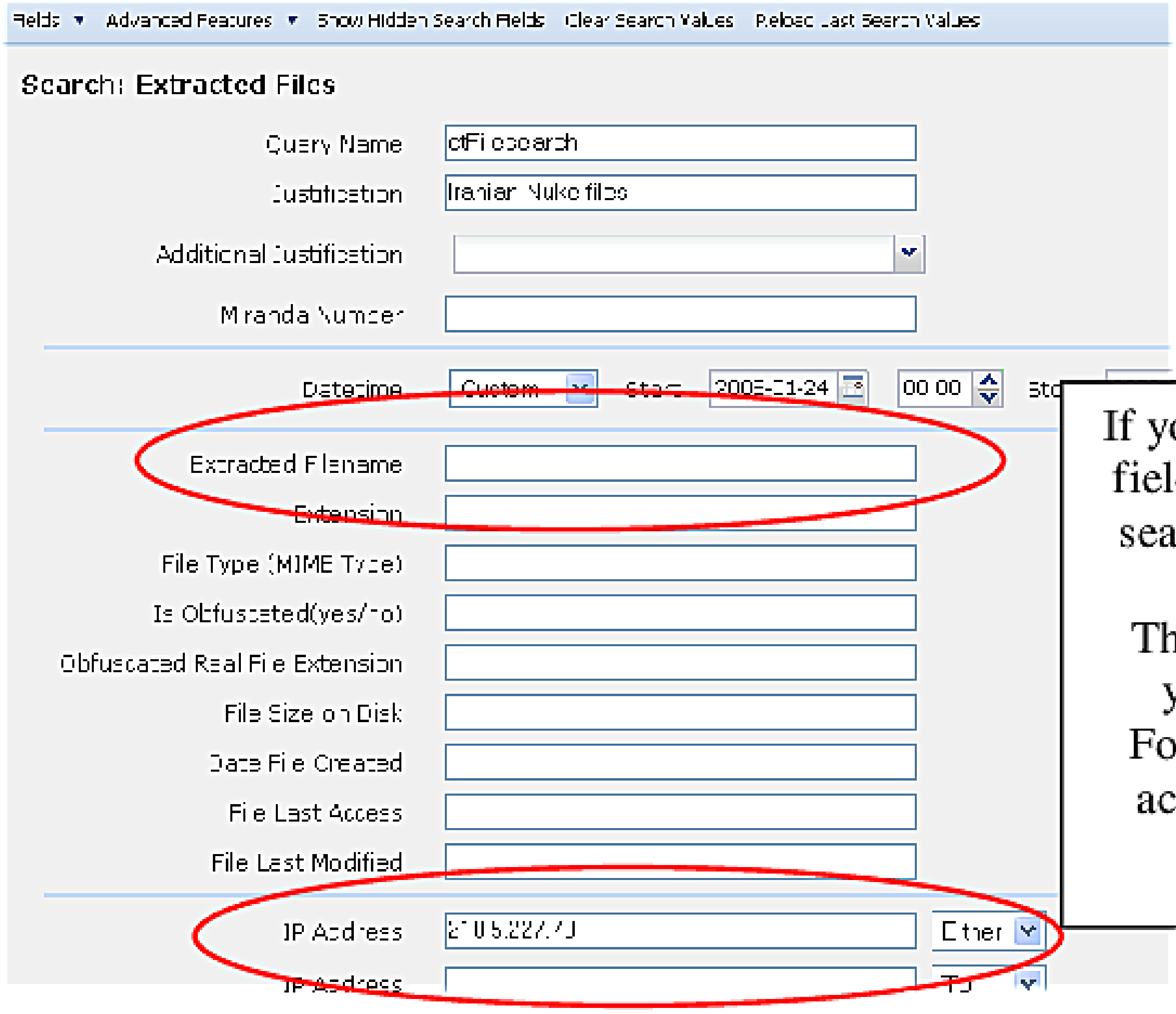
File Type (MIME Type):

Is Obfuscated(yes/no):

Obfuscated Real File Extension:

File Size on Disk:

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.



Search: Extracted Files

Query Name: ctFilesearch

Justification: Iranian Nuke files

Additional Justification:

Miranda Number:

Datetime: Custom Start: 2008-01-24 00:00 Sto

Extracted Filename:

Extension:

File Type (MIME Type):

Is Obfuscated(yes/no):

Obfuscated Real File Extension:

File Size on Disk:

Date File Created:

File Last Access:

File Last Modified:

IP Address: [illegible] Either

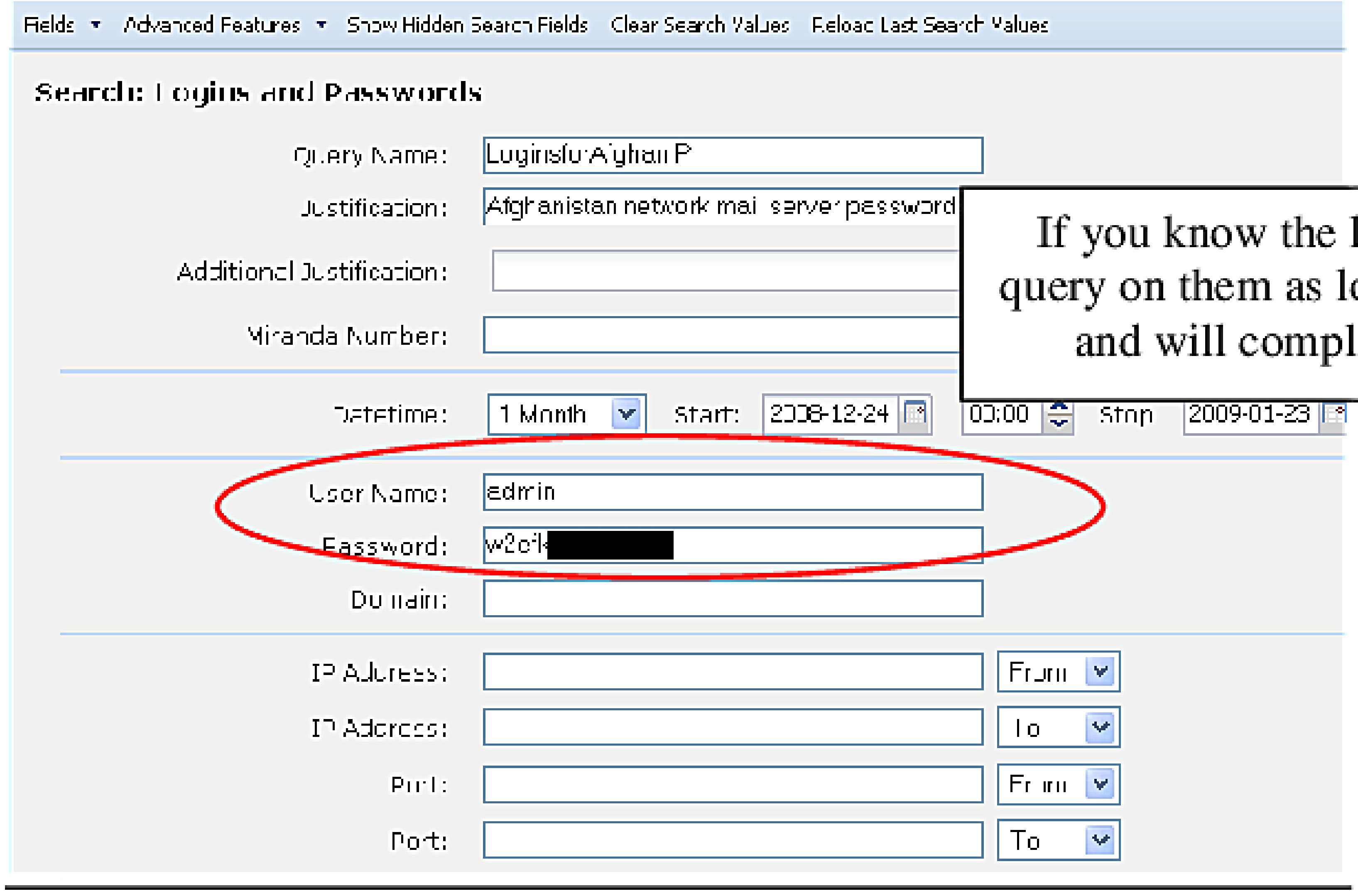
IP Address: To

If you leave the Extracted Filenames field blank, you are wildcarding the search to look for ALL files names

The IP Address of the mail server you found using NSLookup in Foxtrail or your non-attrib Airgap account goes in the "IP Address" field

Logins and Passwords

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



Search: Logins and Passwords

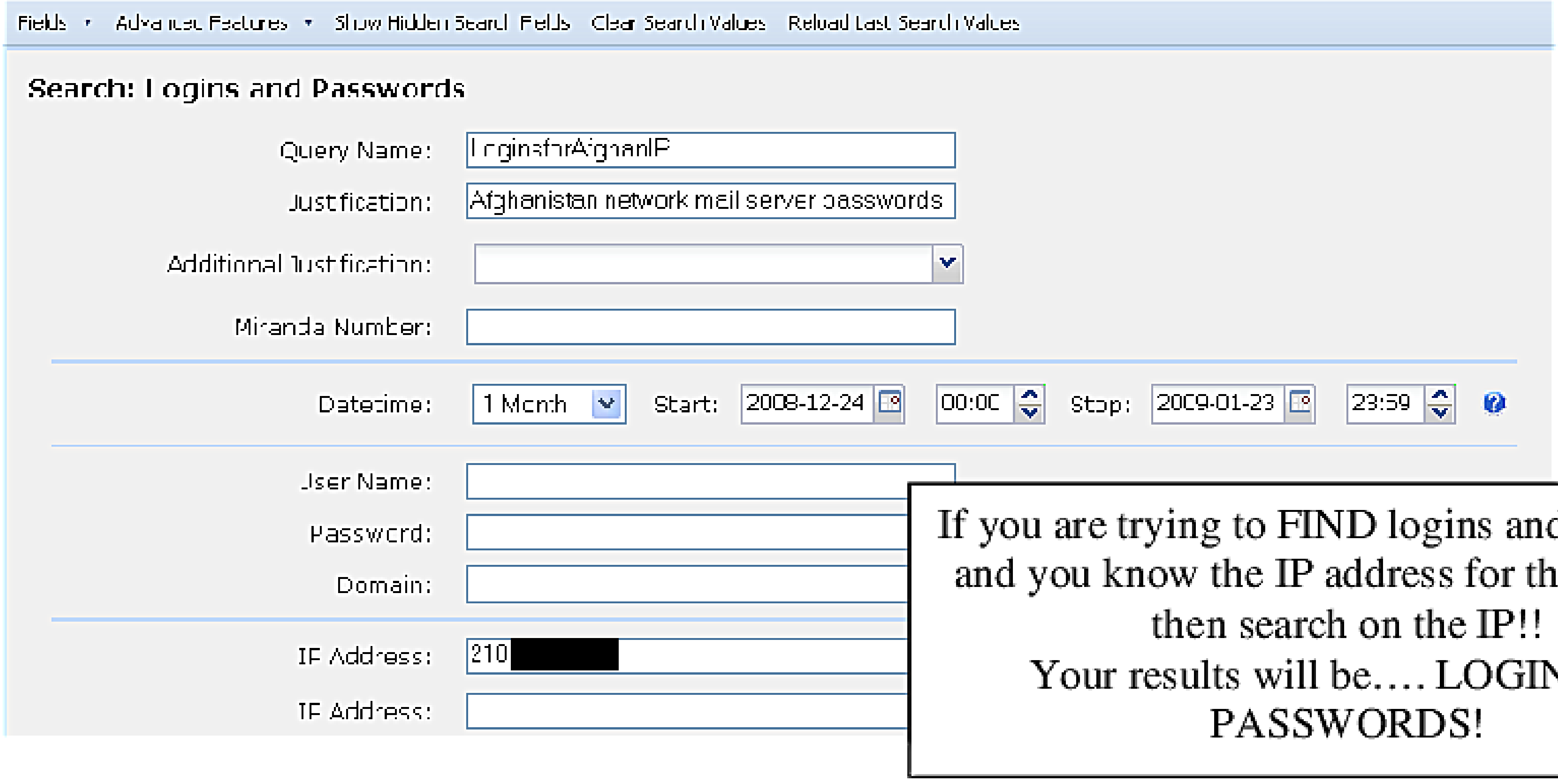
Query Name: LoginsforAfghanP
Justification: Afghanistan network mail server password
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00 Stop: 2009-01-23
User Name: admin
Password: w2o'k[redacted]
Domain:
IP Address: From
IP Address: To
Port: From
Port: To

If you know the logins or passwords, query on them as long as they are unique and will comply with USSID-18.

"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. <u>Trying to discover logins and passwords on a network</u>? 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.



Search: Logins and Passwords

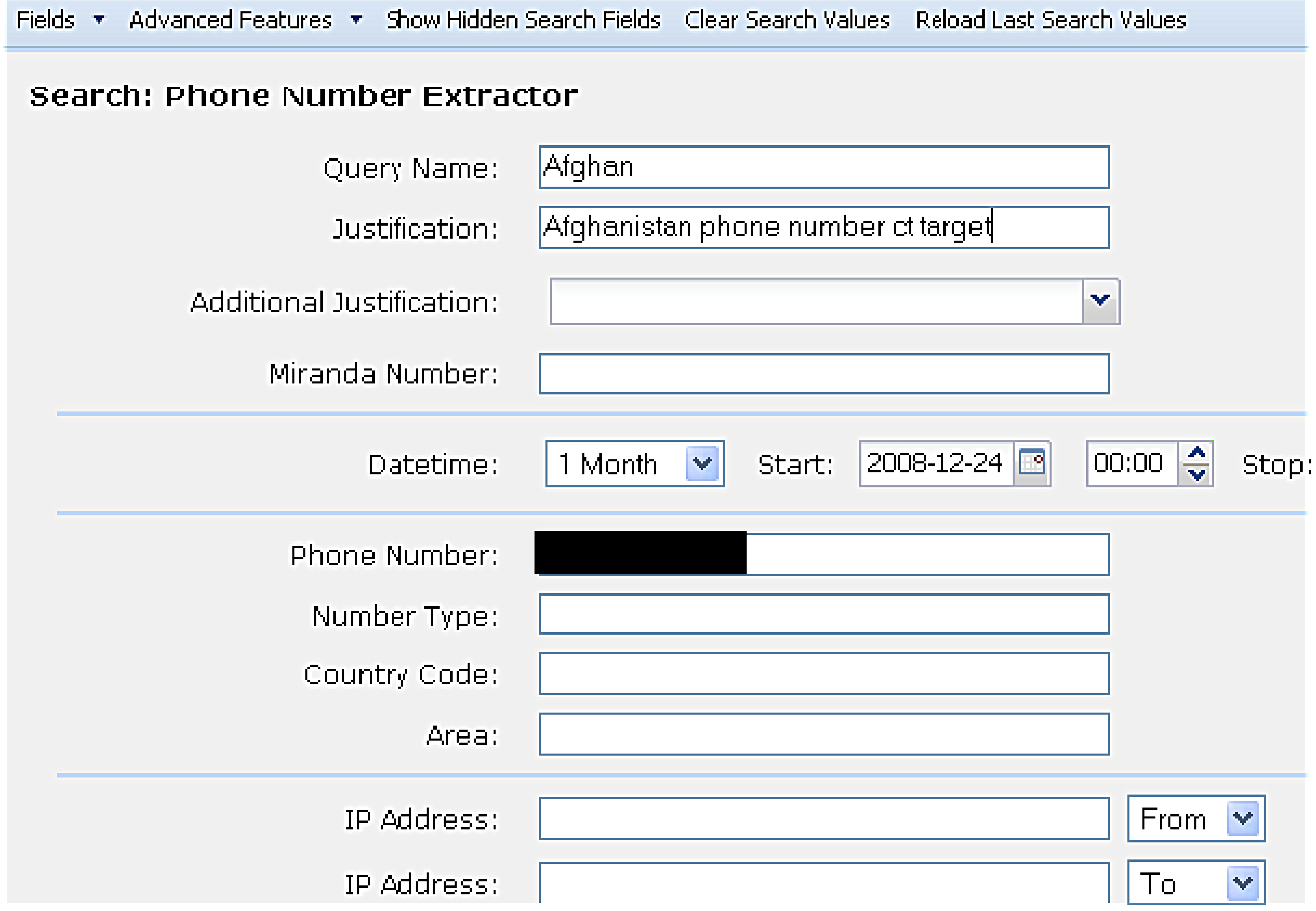
Query Name: LoginsforAfghanIP
Justification: Afghanistan network mail server passwords
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00 Stop: 2009-01-23 23:59
User Name:
Password:
Domain:
IP Address: 210[redacted]
IP Address:

If you are trying to FIND logins and passwords and you know the IP address for the network, then search on the IP!!
Your results will be…. LOGINS and PASSWORDS!

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.

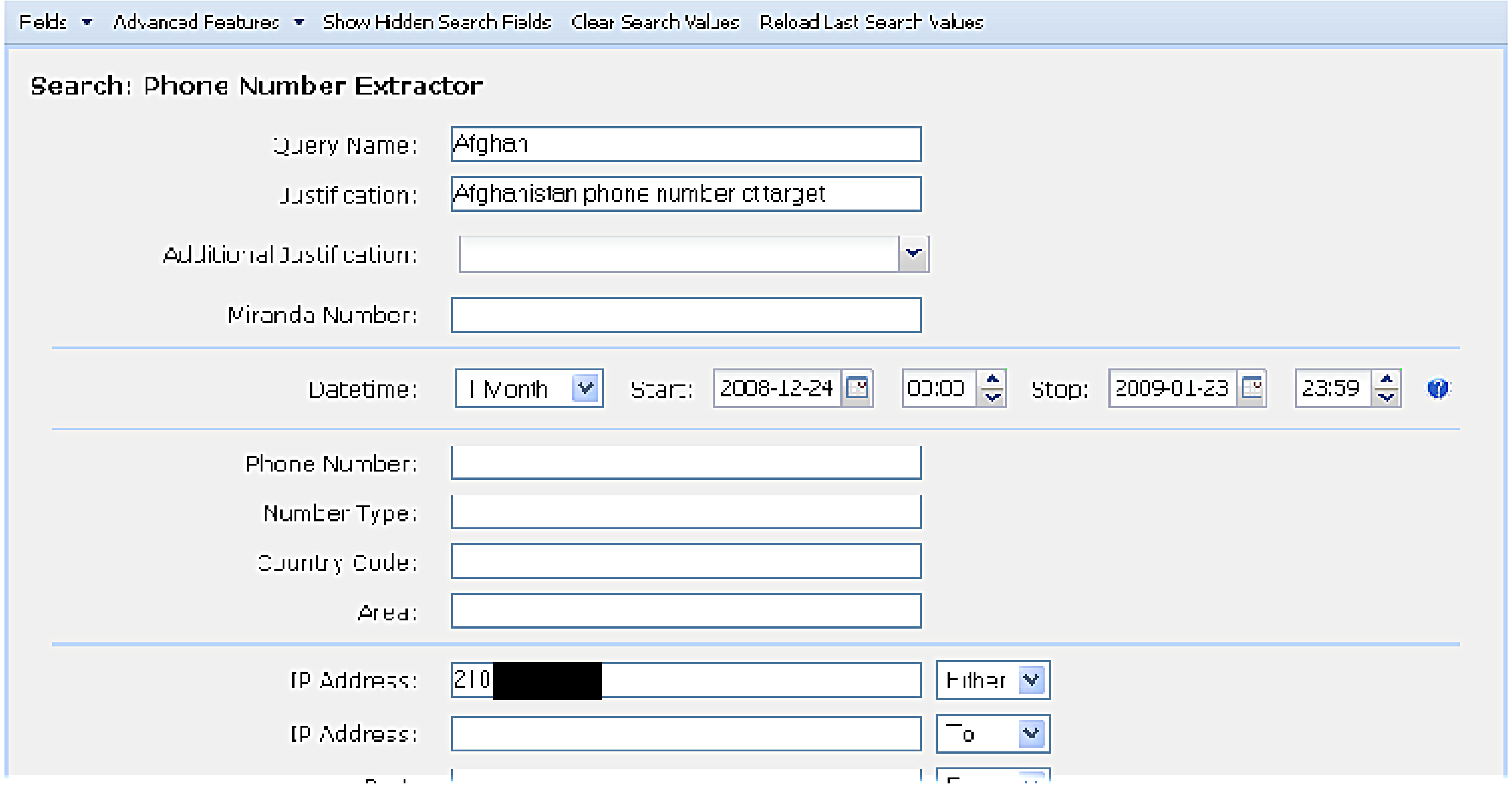
1. Already have a phone number? If all you have to start with as lead information is a phone number, you may find it useful to query on that phone number and see if anyone sent an email with that number in the signature line.



Search: Phone Number Extractor

Query Name: Afghan
Justification: Afghanistan phone number ct target
Additional Justification:
Miranda Number:
Datetime: 1 Month Start: 2008-12-24 00:00 Stop:
Phone Number: [redacted]
Number Type:
Country Code:
Area:
IP Address: From
IP Address: To

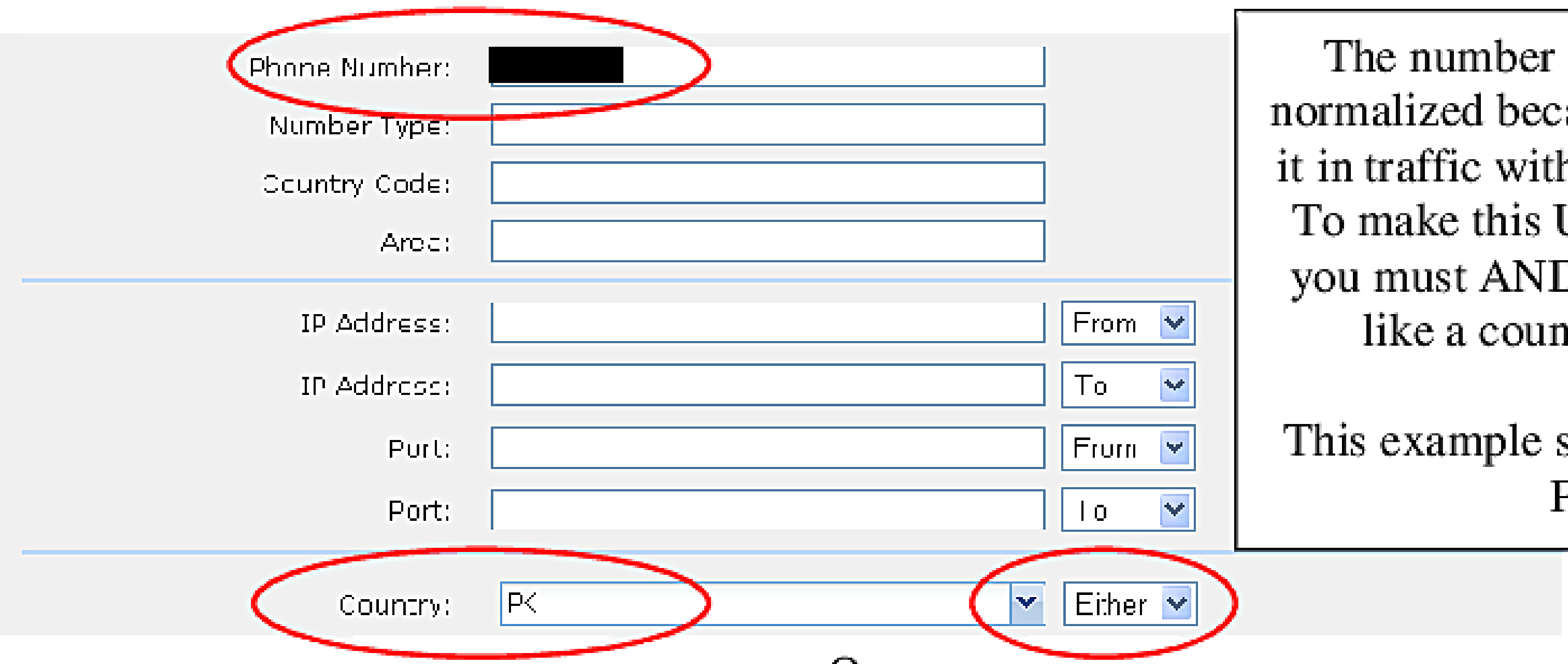
2. Looking for any phone numbers on a network? Quite often you know the mail server IP address and could use some telephone numbers to task?



Search: Phone Number Extractor

Query Name:	Afghan						
Justification:	Afghanistan phone number cttarget						
Additional Justification:							
Miranda Number:							
Datetime:	1 Month	Start:	2008-12-24	00:00	Stop:	2009-01-23	23:59
Phone Number:							
Number Type:							
Country Code:							
Area:							
IP Address:	210 [redacted]	Either					
IP Address:		To					

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:

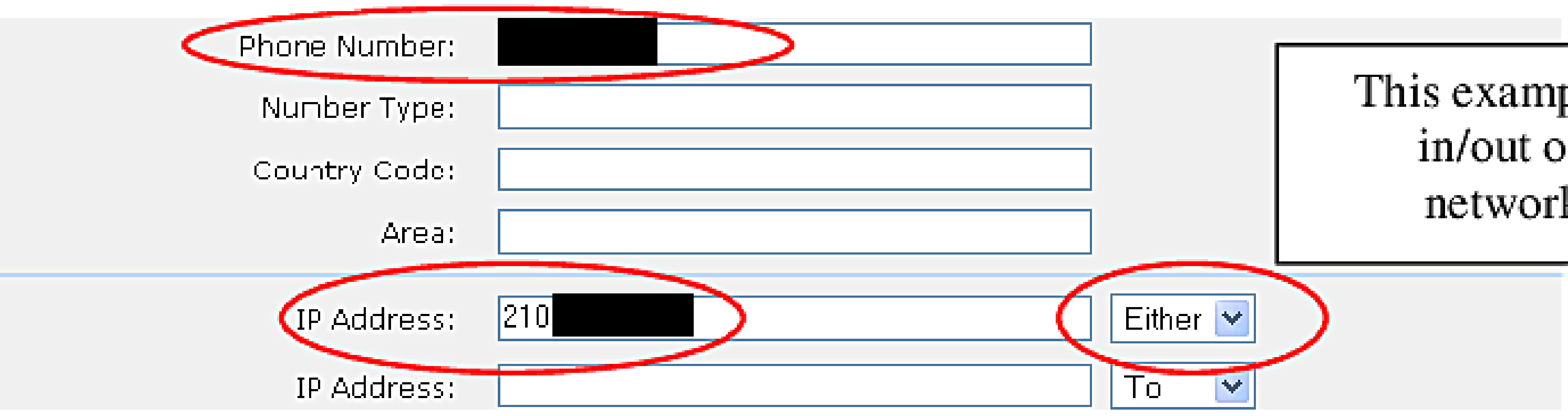


Phone Number:	[redacted]	
Number Type:		
Country Code:		
Area:		
IP Address:		From
IP Address:		To
Port:		From
Port:		To
Country:	PK	Either

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 like a country or IP address.

This example shows traffic in/out of Pakistan

Or



Phone Number:	[redacted]	
Number Type:		
Country Code:		
Area:		
IP Address:	210[redacted]	Either
IP Address:		To

This example shows traffic in/out of a particular network/IP Address

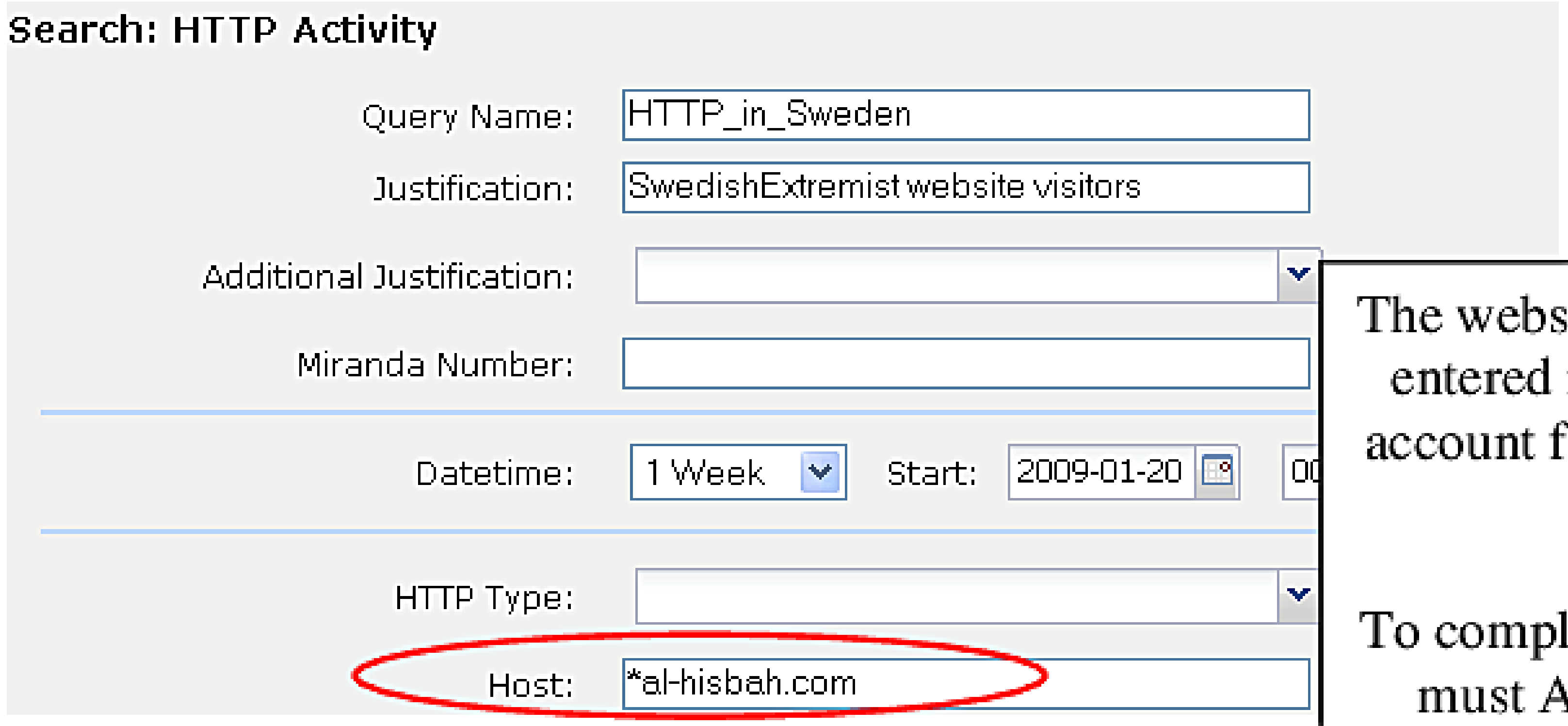
*If you ask XKEYSCORE to give you all Pakistani traffic, it's doing an NKB lookup on all Pakistani registered IP addresses. Geolocation of IP addresses is not 100% accurate at this time. Unofficial estimates say asking for all of Country X's traffic will find between 50-60% of the actual traffic. (That's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

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:

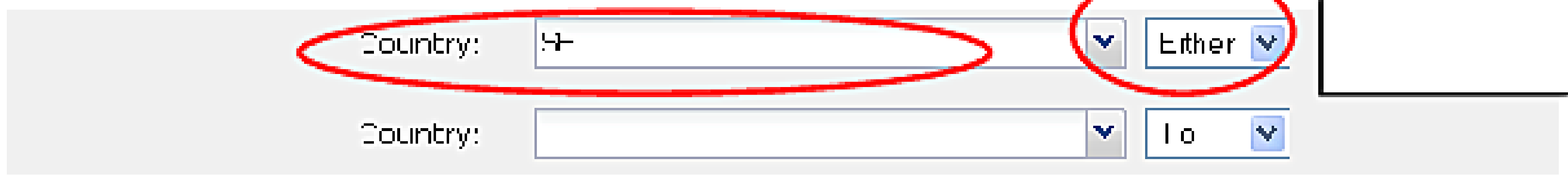
Miranda Number:

Datetime: 1 Week Start: 2009-01-20 00

HTTP Type:

Host: *al-hisbah.com

Scroll down to enter a country code (Sweden is selected



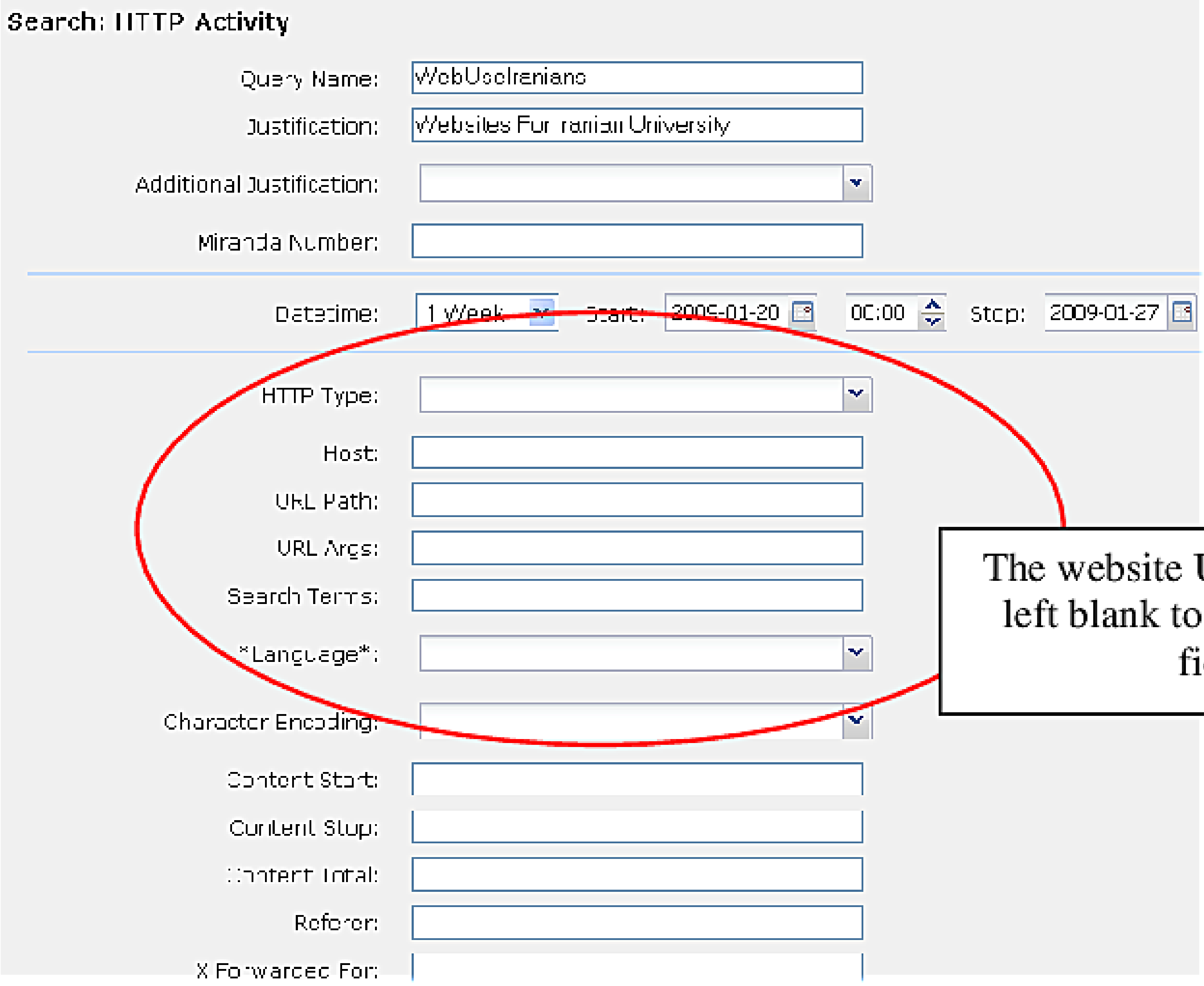
Country: SE Either

Country: To

The website URL (aka "host) is entered in with a wildcard to account for "www" and "mail" other hosts.

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

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.

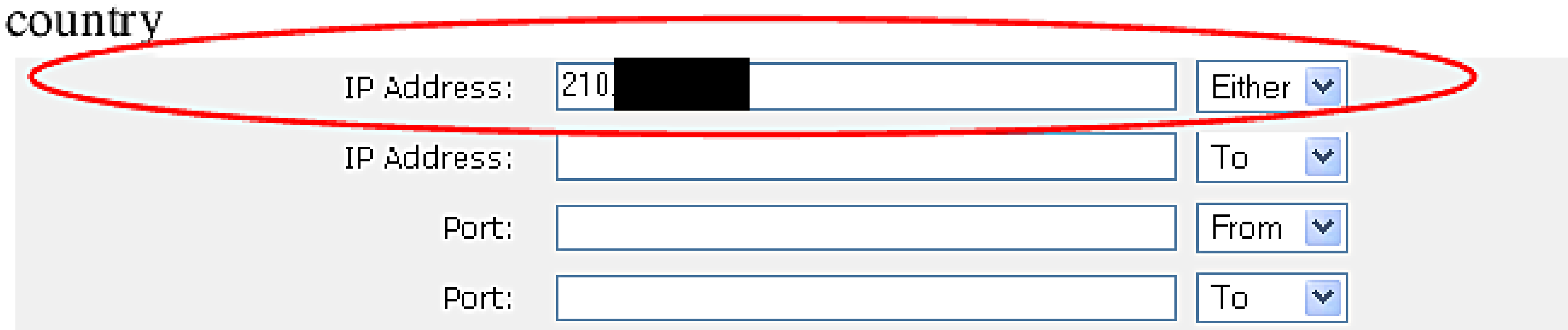


Search: HTTP Activity

Query Name:	WebUseIranians
Justification:	Websites For Iranian University
Additional Justification:	
Miranda Number:	
Datetime:	1 Week Start: 2009-01-20 00:00 Stop: 2009-01-27
HTTP Type:	
Host:	
URL Path:	
URL Args:	
Search Terms:	
Language:	
Character Encoding:	
Content Start:	
Content Stop:	
Content Total:	
Referer:	
X Forwarded For:	

The website URLs (hosts) are left blank to wildcard those fields.

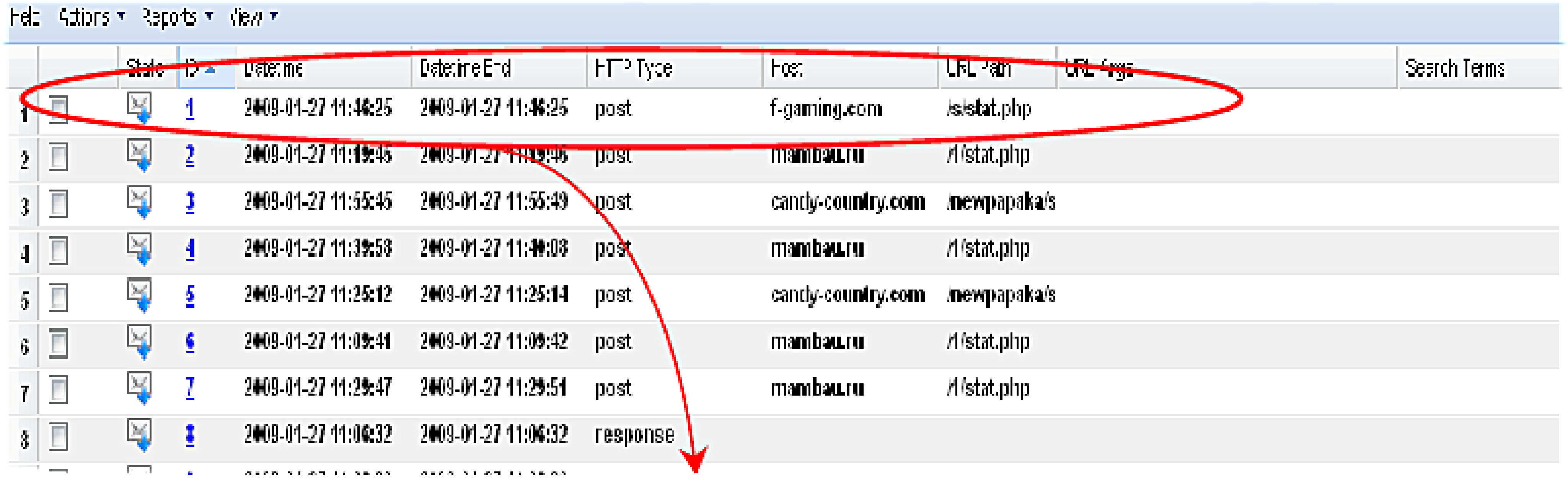
To comply with USSID-18 you AND that with some other information like an IP or country



IP Address:	210.[redacted]	Either
IP Address:		To
Port:		From
Port:		To

Results from an HTTP Parser query

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



		State	ID	Datetime	Datetime End	HTTP Type	Host	URL Path	URL Args	Search Terms
1	□		1	2009-01-27 11:46:25	2009-01-27 11:46:25	post	f-gaming.com	/s/stat.php		
2	□		2	2009-01-27 11:19:45	2009-01-27 11:19:46	post	mambau.ru	/l/stat.php		
3	□		3	2009-01-27 11:55:45	2009-01-27 11:55:49	post	candy-country.com	/newpapaka/s		
4	□		4	2009-01-27 11:39:58	2009-01-27 11:40:08	post	mambau.ru	/l/stat.php		
5	□		5	2009-01-27 11:25:12	2009-01-27 11:25:14	post	candy-country.com	/newpapaka/s		
6	□		6	2009-01-27 11:09:41	2009-01-27 11:09:42	post	mambau.ru	/l/stat.php		
7	□		7	2009-01-27 11:29:47	2009-01-27 11:29:51	post	mambau.ru	/l/stat.php		
8	□		8	2009-01-27 11:06:32	2009-01-27 11:06:32	response				

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

Host = f-gaming.com

URL Path = /s/stat/php

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.

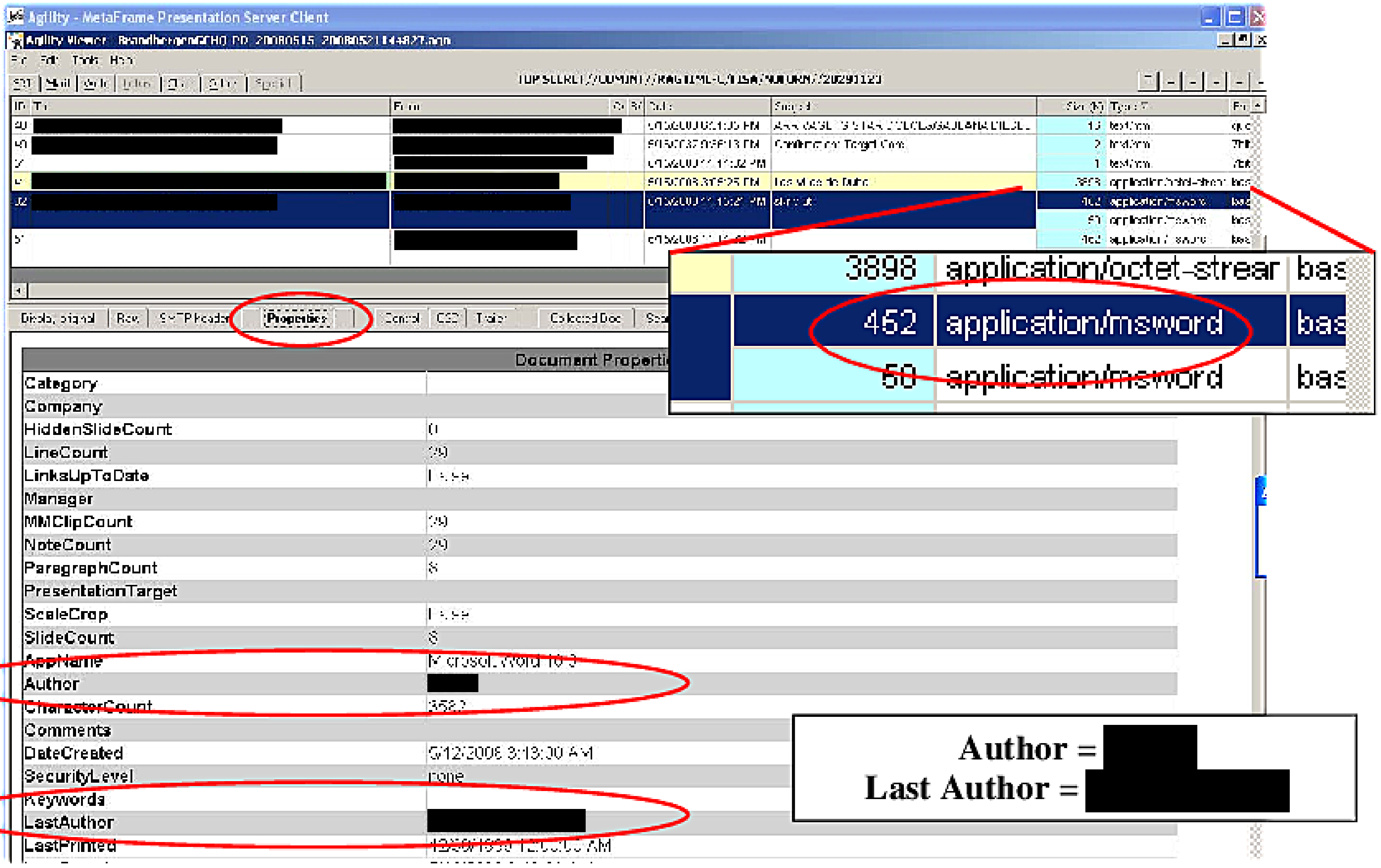
*Most Microsoft Office allows uses to encrypt files by clicking Tools -> Options -> Security and password protecting the files. The Document Metadata query looks for that type of encryption. It doesn't look for PGP or other 3rd party encryption.

> **"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).

Displaying MS Word document in Agility:

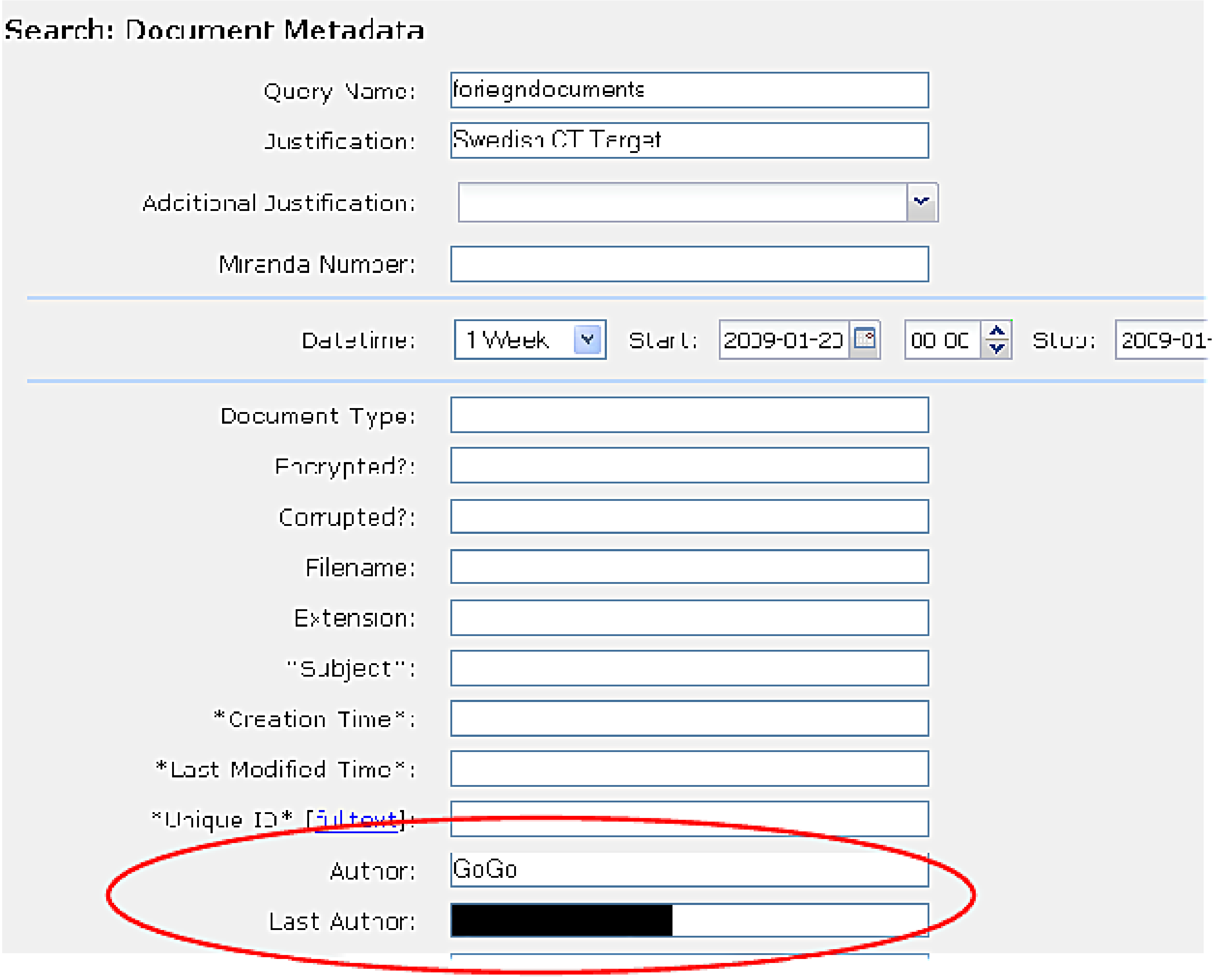


3898	application/octet-strear
452	application/msword
50	application/msword

Category	
Company	
HiddenSlideCount	0
LineCount	29
LinksUpToDate	False
Manager	
MMClipCount	29
NoteCount	29
ParagraphCount	8
PresentationTarget	
ScaleCrop	False
SlideCount	8
AppName	Microsoft Word 10.0
Author	[redacted]
CharacterCount	3582
Comments	
DateCreated	5/12/2008 3:13:00 AM
SecurityLevel	none
Keywords	
LastAuthor	[redacted]
LastPrinted	12/30/1899 12:00:00 AM

Author = [redacted]
Last Author = [redacted]

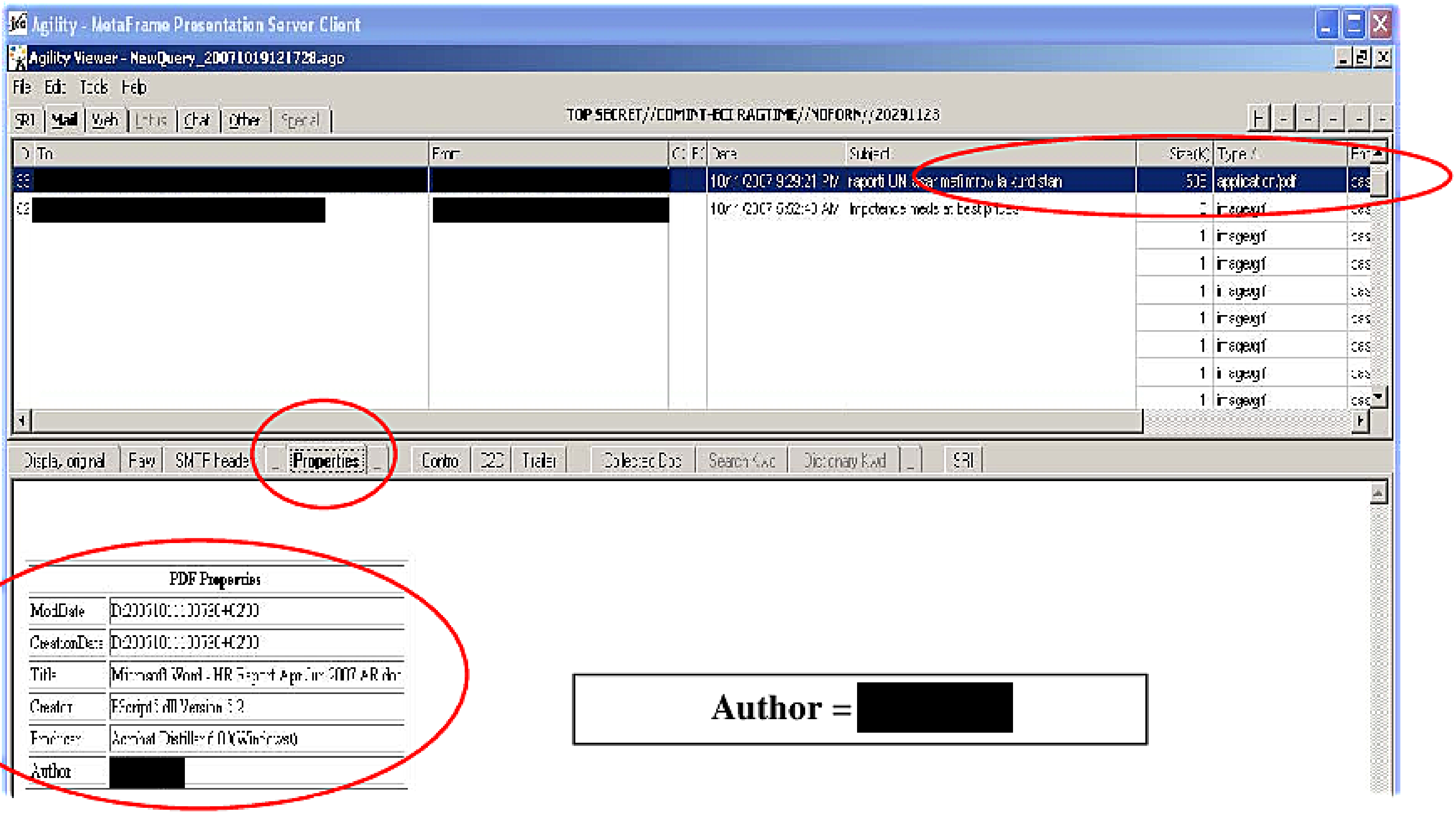
To create a query in XKEYSCORE from this information:



Search: Document Metadata

Query Name: foriegndocuments
Justification: Swedish CT Target
Additional Justification:
Miranda Number:
Datetime: 1 Week Start: 2009-01-20 00 00 Stop: 2009-01-
Document Type:
Encrypted?:
Corrupted?:
Filename:
Extension:
"Subject":
Creation Time:
Last Modified Time:
Unique ID [fulltext]:
Author: GoGo
Last Author: [redacted]

View of document properties of PDFs in Agility:


Agility - MetaFrame Presentation Server Client
Agility Viewer - NewQuery_20071019121728.ago
File Edit Tools Help
SRI Mail Web Lotus Chat Other Special
TOP SECRET//COMINT-ECI RAGTIME//NOFORN//20291123
Display original Raw SMTP header Properties Contro 220 Trailer Collected Docs Search Kwd Dictionary Kwd SRI

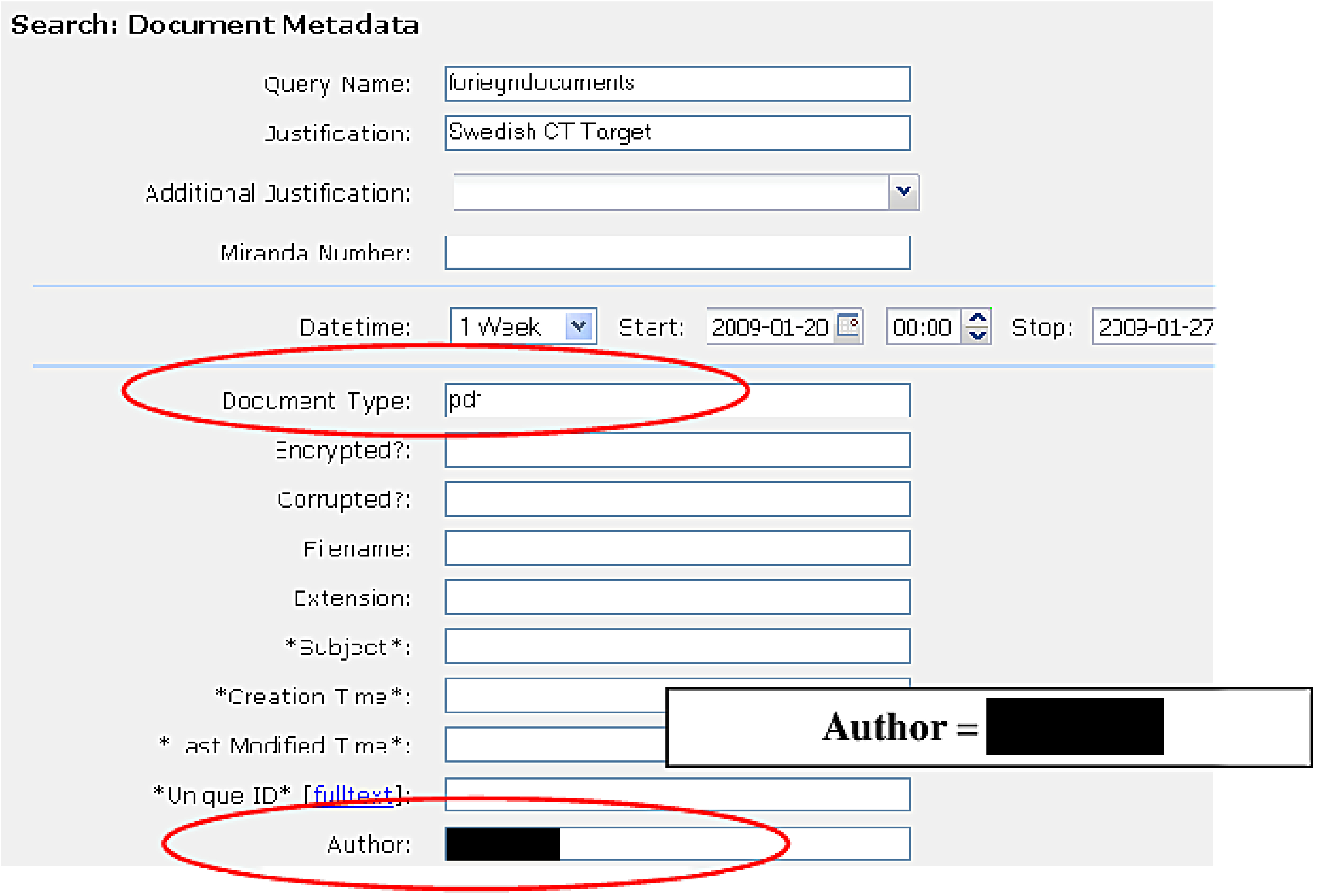
ID	To	From	Date	Subject	Size(K)	Type
33	[redacted]	[redacted]	10/11/2007 9:29:21 PM	raporti UN [illegible]	503	application/pdf
02	[redacted]	[redacted]	10/11/2007 5:02:40 AM	Importance [illegible]	2	image/gif
					1	image/gif
					1	image/gif
					1	image/gif
					1	image/gif
					1	image/gif
					1	image/gif
					1	image/gif

PDF Properties

ModDate	D:20071011100730+0200
CreationDate	D:20071011100730+0200
Title	Microsoft Word - HR Report Apr-Jun 2007 AR.doc
Creator	PScript5.dll Version 5.2
Producer	Acrobat Distiller 6.0 (Windows)
Author	[redacted]

Author = [redacted]

To create a query in XKEYSCORE using this information:



Search: Document Metadata

Query Name: foreigndocuments
Justification: Swedish CT Target
Additional Justification:
Miranda Number:
Datetime: 1 Week Start: 2009-01-20 00:00 Stop: 2009-01-27
Document Type: pdf
Encrypted?:
Corrupted?:
Filename:
Extension:
Subject:
Creation Time:
Last Modified Time:
Unique ID [fulltext]:
Author: [redacted]

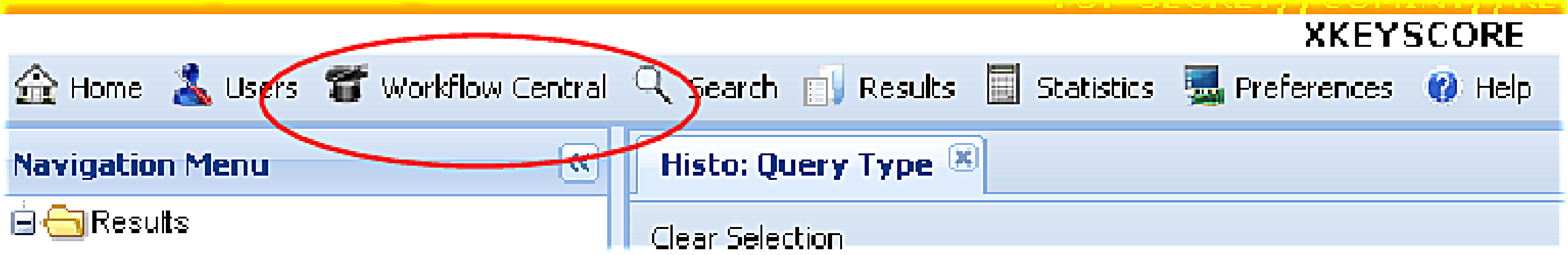
Author = [redacted]

Creating a WorkFlow

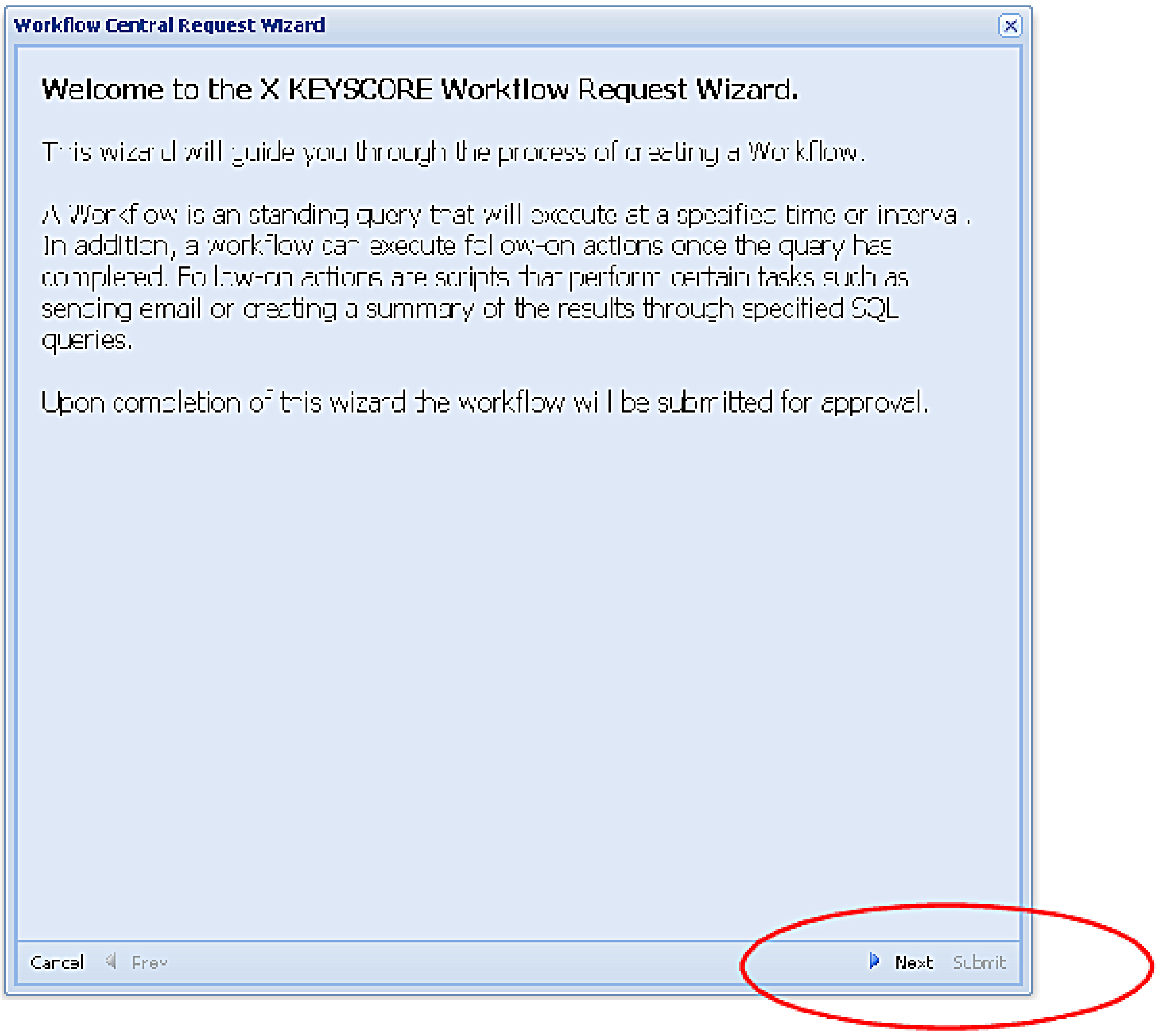
Workflows are periodic queries you can set up that run at specified times. They are great for sustained targets because they query the database for you (e.g. every night) and you can easily view the recently collected traffic without having to create a new query each day. They are also very helpful if 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.

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.



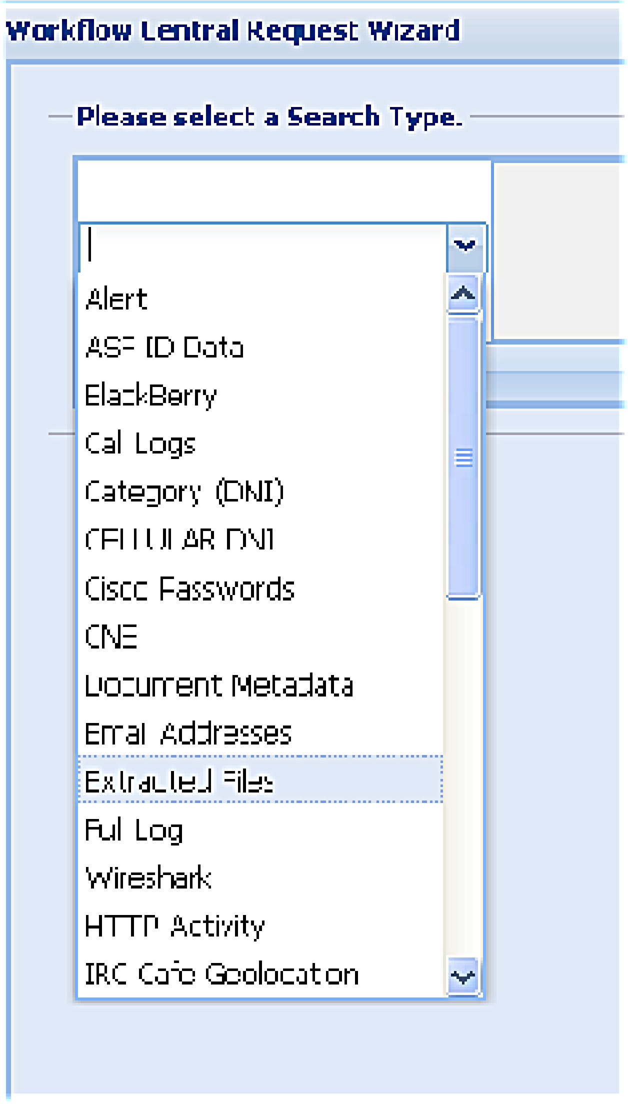
Welcome to the X KEYSCORE Workflow Request Wizard.

This wizard will guide you through the process of creating a Workflow.

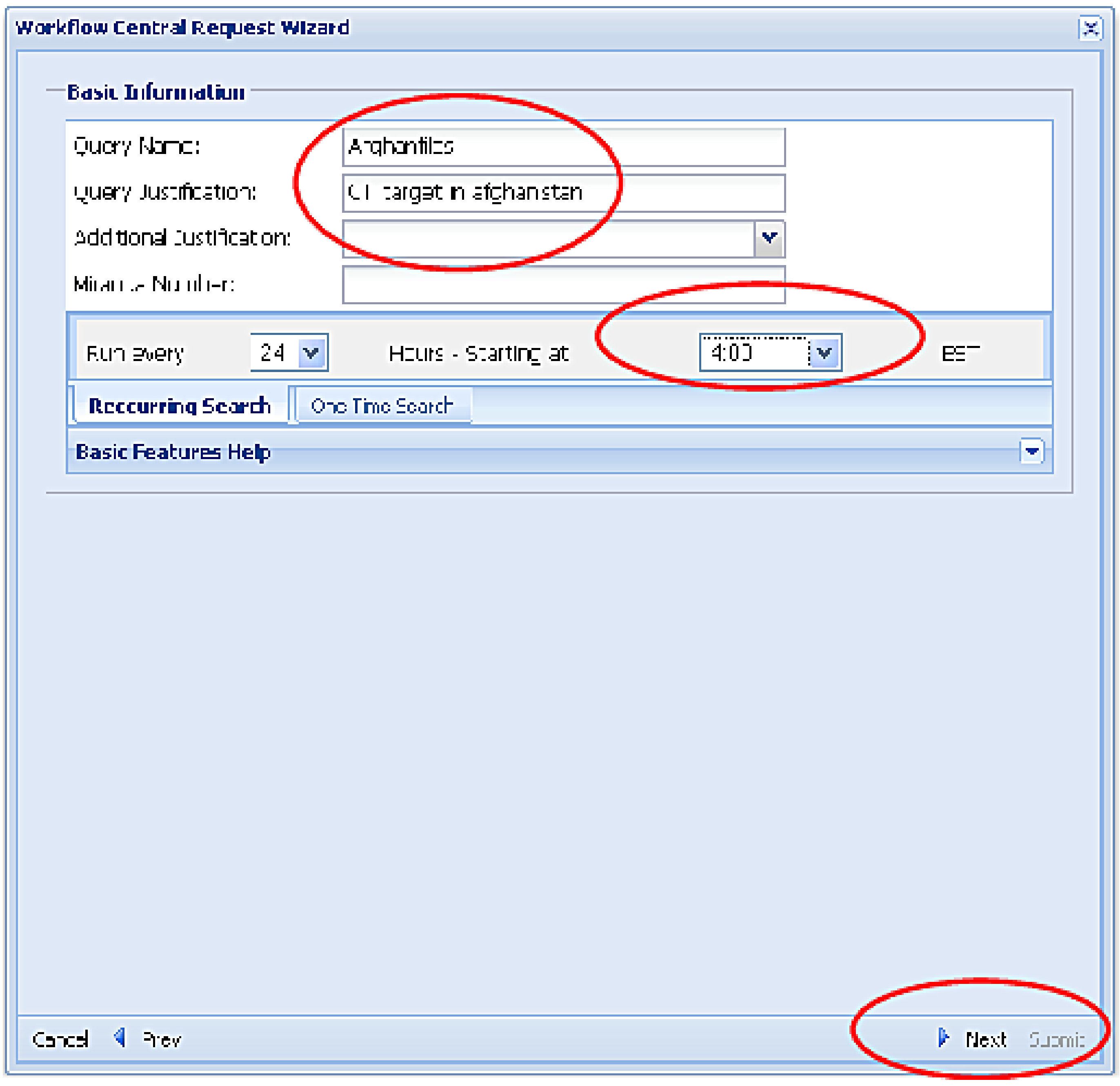
A Workflow is an standing query that will execute at a specified time or interval. In addition, a workflow can execute follow-on actions once the query has completed. Follow-on actions are scripts that perform certain tasks such as sending email or creating a summary of the results through specified SQL queries.

Upon completion of this wizard the workflow will be submitted for approval.

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.



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.



Workflow Central Request Wizard

Basic Information

Query Name: Afghanfiles

Query Justification: CT target in afghanstan

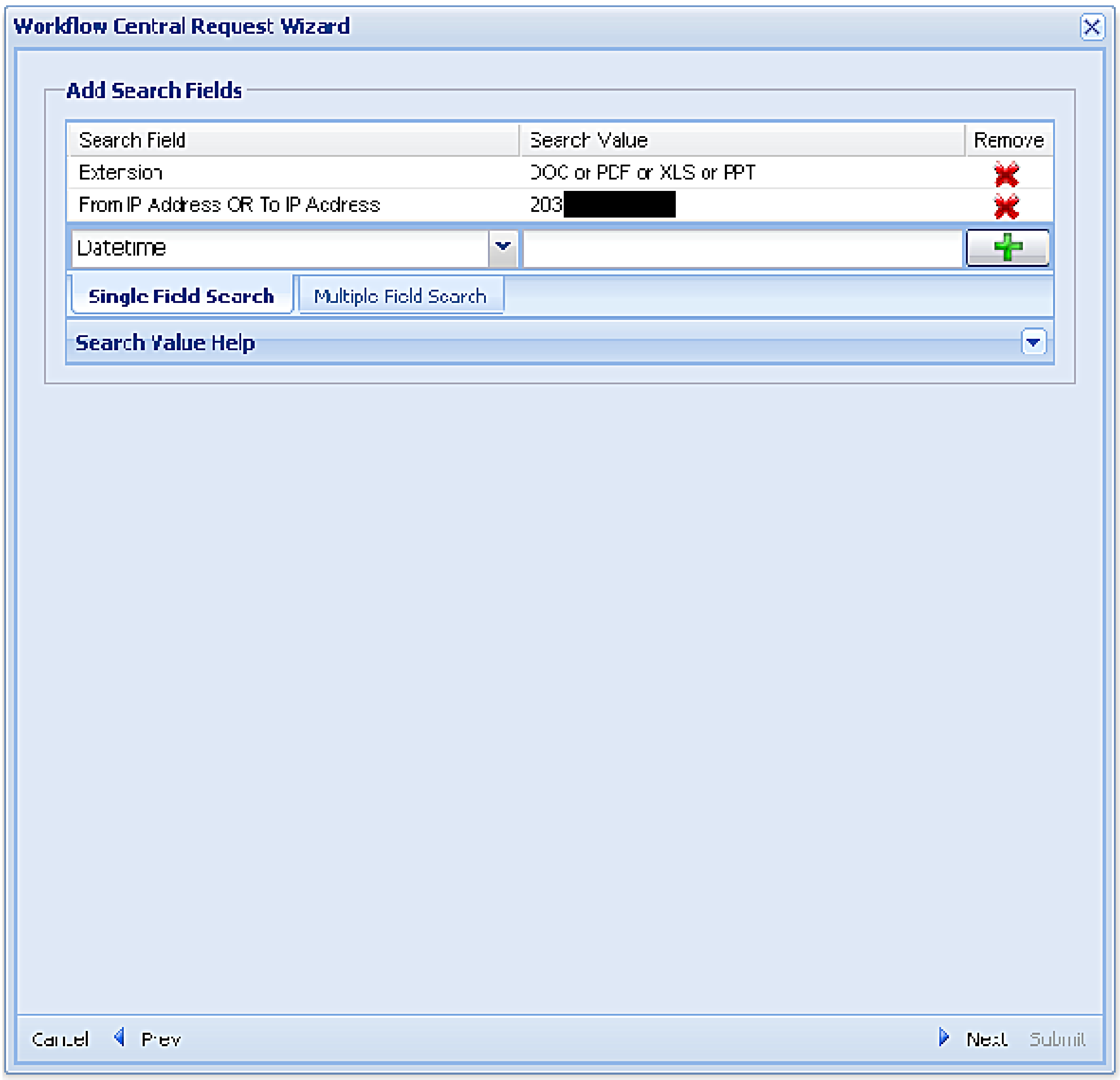
Additional Justification:

Miranda Number:

Run every 24 Hours - Starting at 4:00 EST

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.

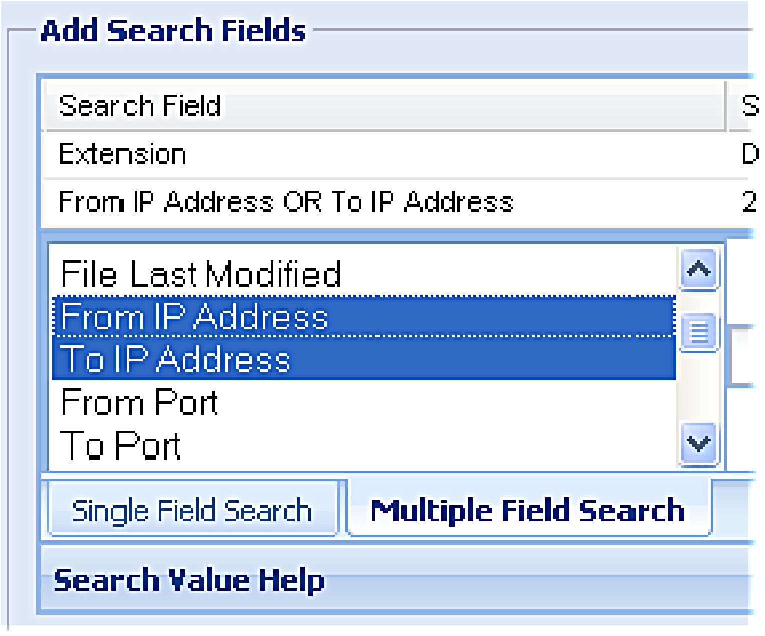


Search Field	Search Value	Remove
Extension	DOC or PDF or XLS or PPT	✖
From IP Address OR To IP Address	203[redacted]	✖

Click Next

Single Field Search only searches in one field (e.g. File Extensions)

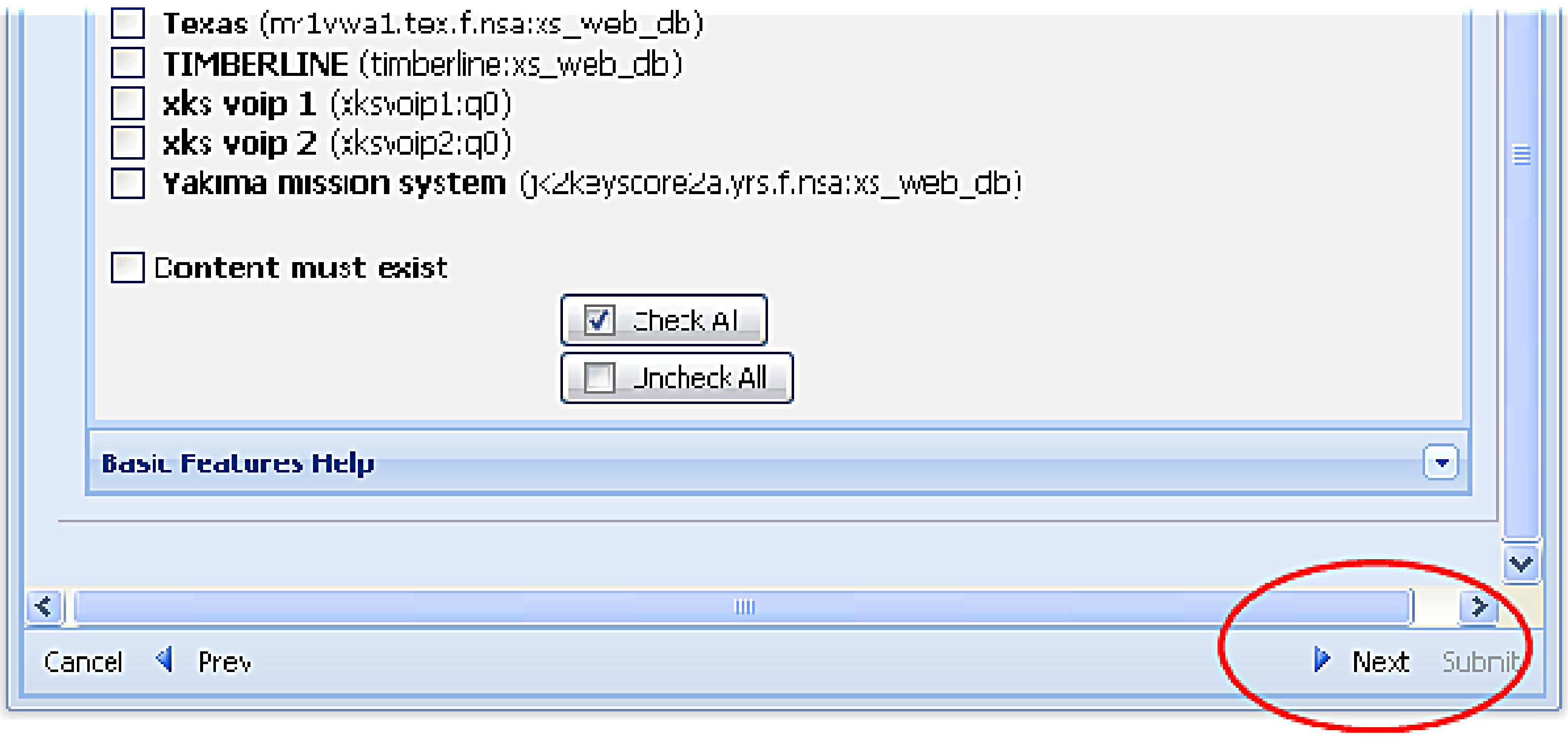
Multiple Field Search allows you to search on several fields (e.g., *To IP* **AND** *From IP*)



Search Field	S
Extension	D
From IP Address OR To IP Address	2

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.

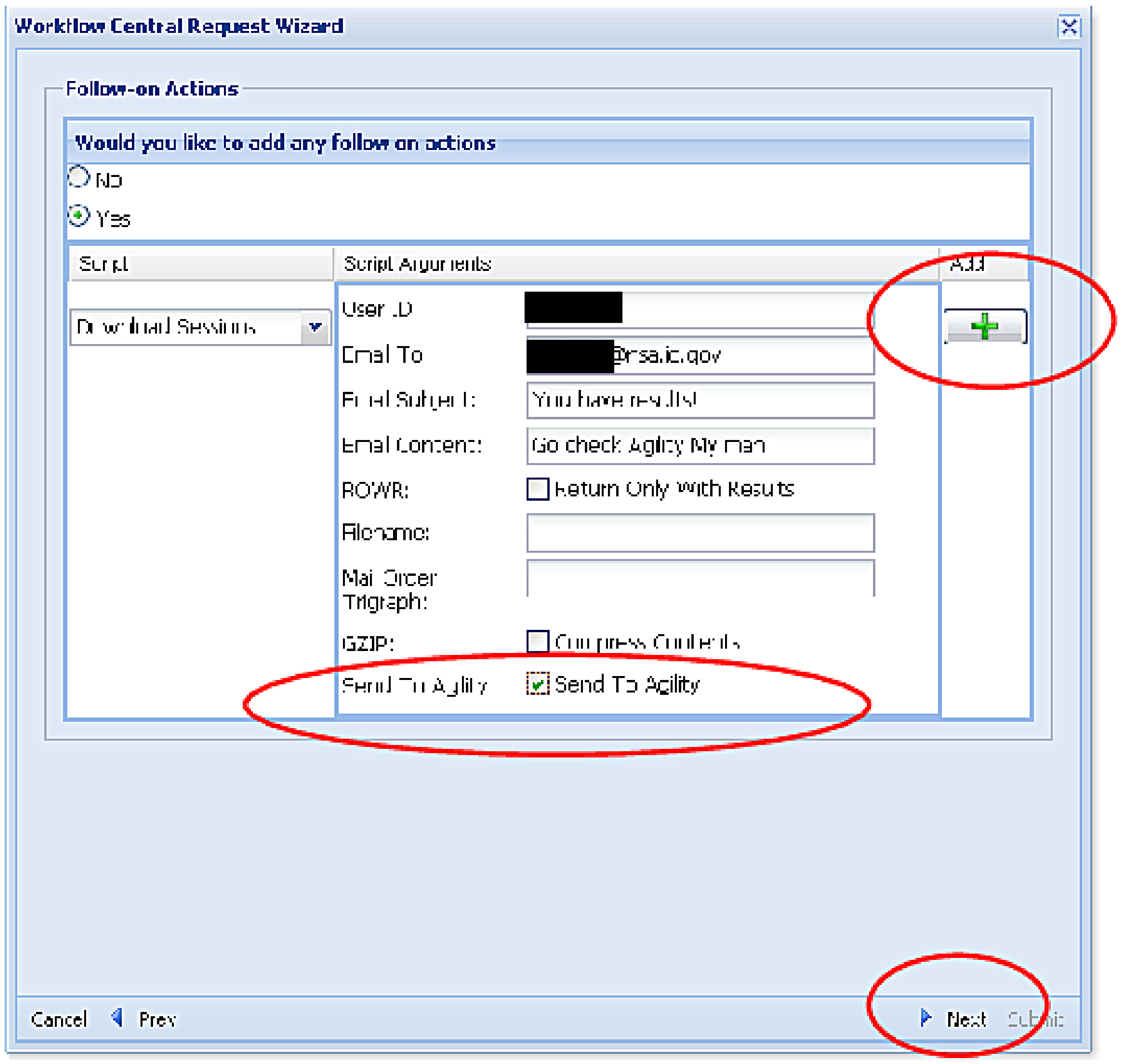


- □ **Texas** (m1vwa1.tex.f.nsa:xs_web_db)
- □ **TIMBERLINE** (timberline:xs_web_db)
- □ **xks voip 1** (xksvoip1:q0)
- □ **xks voip 2** (xksvoip2:q0)
- □ **Yakima mission system** (xk2keyscore2a.yrs.f.nsa:xs_web_db)

□ Content must exist

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.



Workflow Central Request Wizard

Follow-on Actions

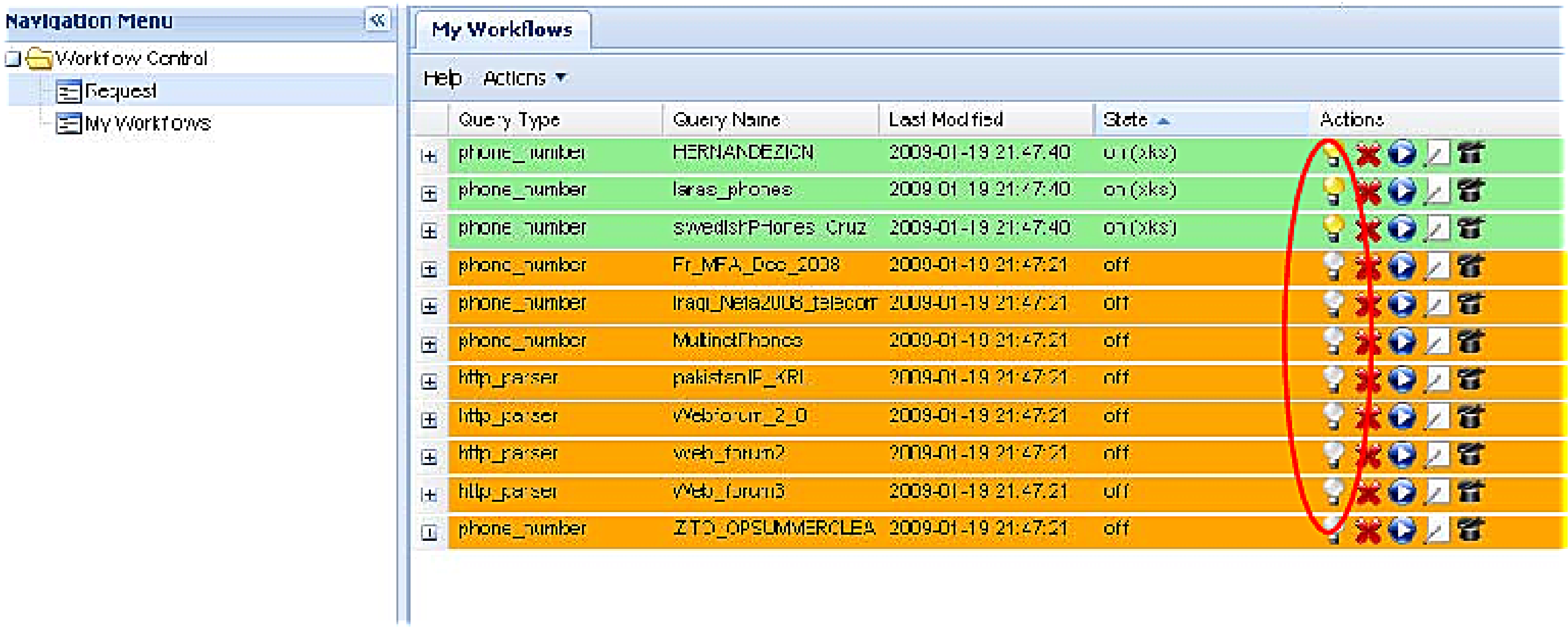
Would you like to add any follow on actions

○ No
● Yes

Script	Script Arguments		Add
Download Sessions	User ID	[redacted]	+
	Email To	[redacted]@nsa.ic.gov	
	Email Subject:	You have results!	
	Email Content:	Go check Agility My man	
	ROWR:	□ Return Only With Results	
	Filename:		
	Mail Order Trigraph:		
	GZIP:	□ Compress Contents	
	Send To Agility	☑ Send To Agility	

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

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.



Query Type	Query Name	Last Modified	State ▲	Actions
phone_number	HERNANDEZION	2009-01-19 21:47:40	on (xks)	
phone_number	laras_phones	2009-01-19 21:47:40	on (xks)	
phone_number	swedishPHones_Cruz	2009-01-19 21:47:40	on (xks)	
phone_number	Fr_MFA_Doc_2008	2009-01-19 21:47:21	off	
phone_number	Iraqi_Nets2008_telecom	2009-01-19 21:47:21	off	
phone_number	MultinatPhones	2009-01-19 21:47:21	off	
http_parser	pakistanIP_KRI	2009-01-19 21:47:21	off	
http_parser	Webforum_2_0	2009-01-19 21:47:21	off	
http_parser	web_forum2	2009-01-19 21:47:21	off	
http_parser	Web_forum3	2009-01-19 21:47:21	off	
phone_number	ZTO_OPSUMMERCLEA	2009-01-19 21:47:21	off	

Searching - Tips and Tricks

The Official XKEYSCORE Frequently Asked Questions page is located here: http://xkeyscore.r1.r.nsa/redmine/wiki/xkeyscore/FAQ. 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).

To search on: 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 "abu**1**jihad", "abu**T**jihad", "abu**S**jihad", "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]

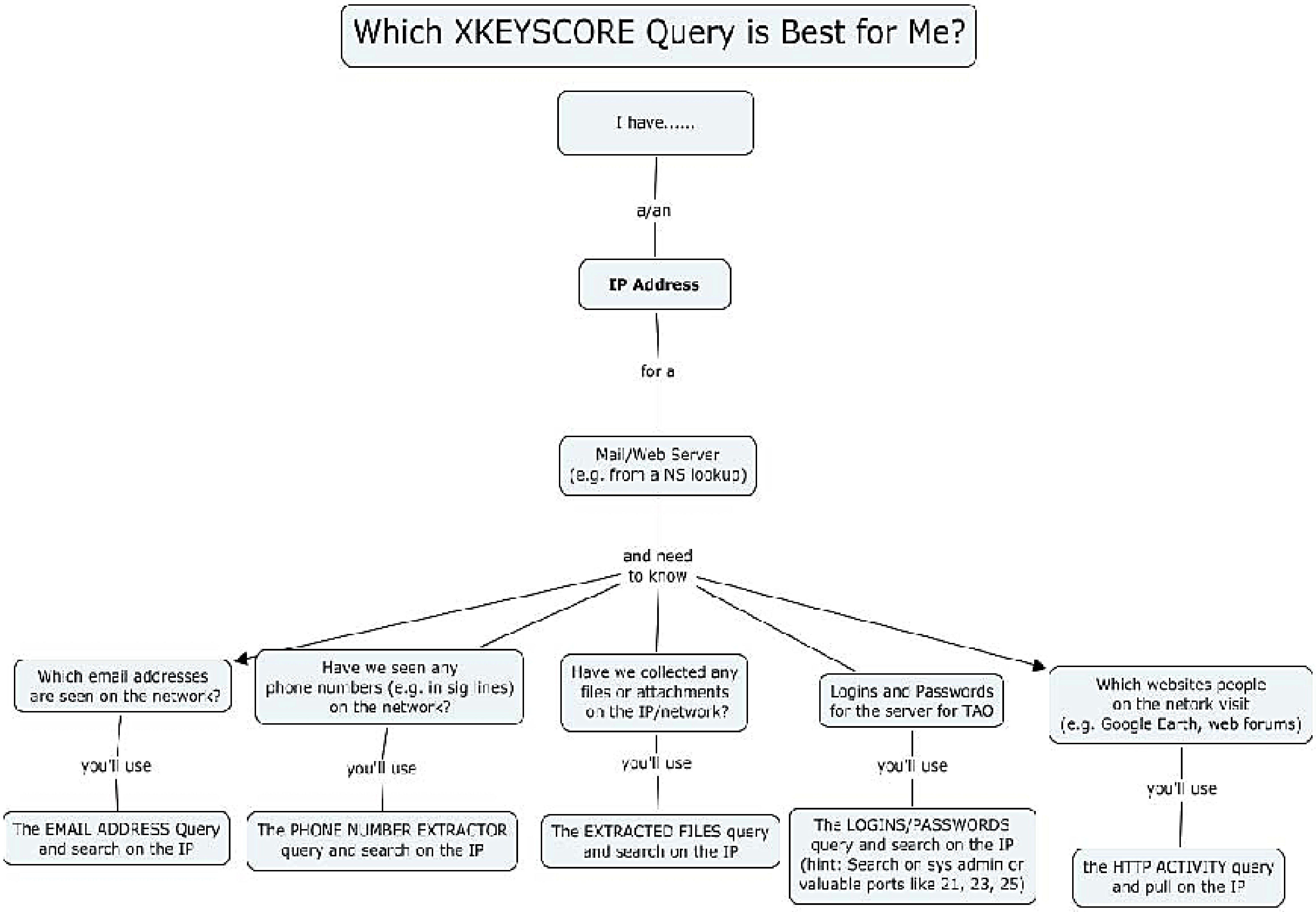
3. Boolean Search Descriptions (Wildcards, ANDs, ORs, etc):

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.e. _sam__bin_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]*)

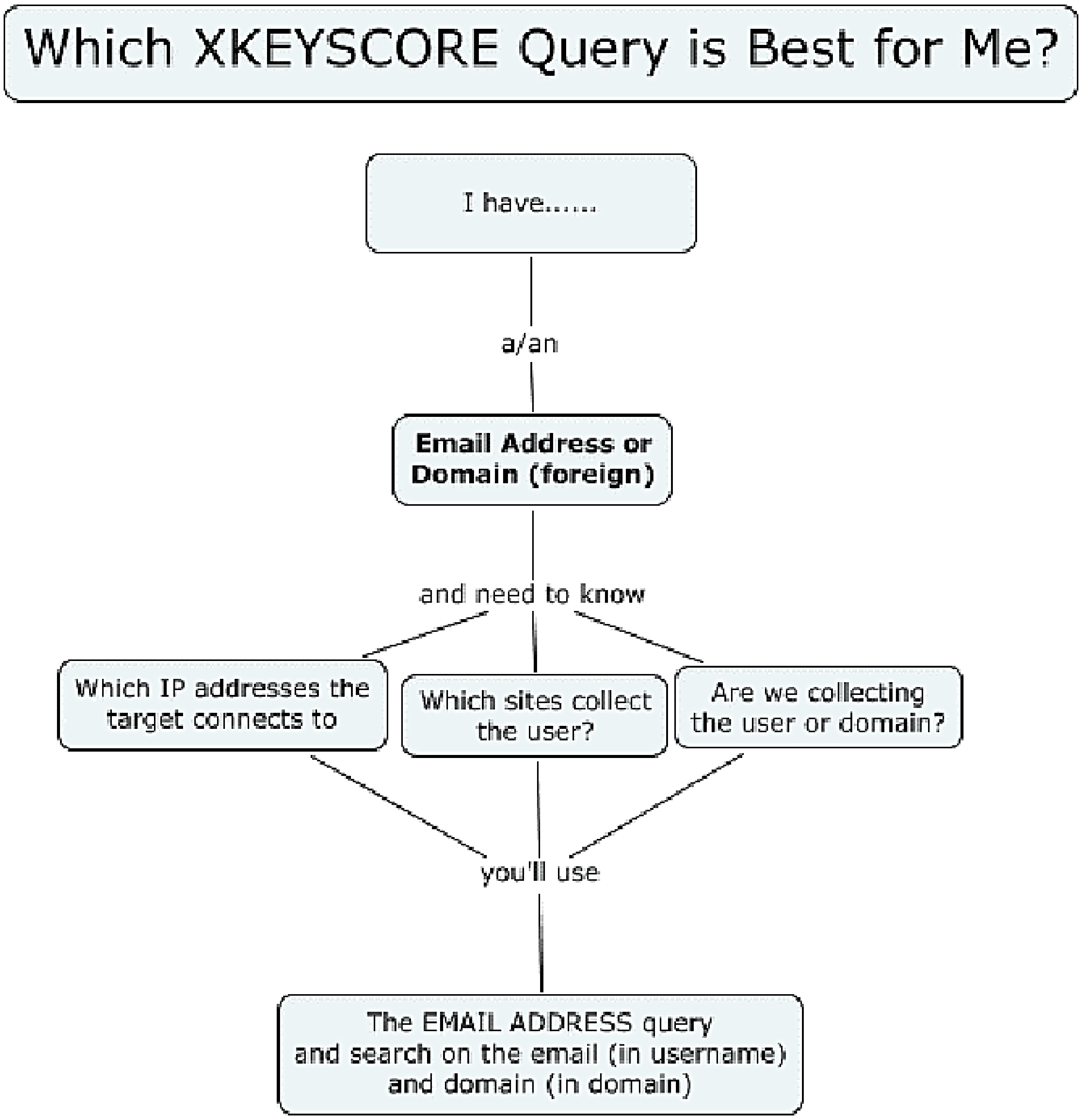
Which Query is best for me?

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.

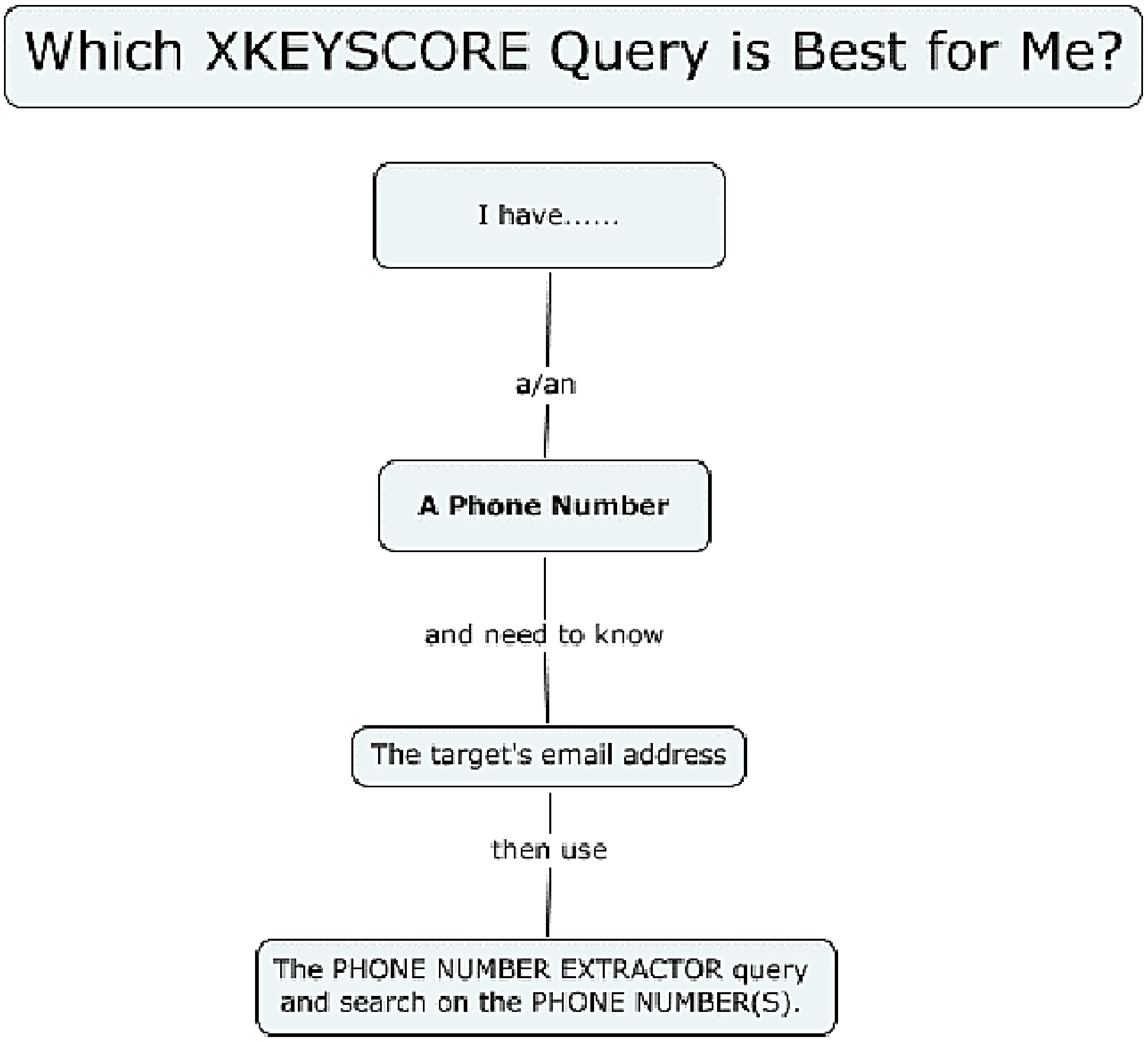
Do you have an IP Address and want to learn more about that network


Which XKEYSCORE Query is Best for Me?
I have......
a/an
IP Address
for a
Mail/Web Server (e.g. from a NS lookup)
and need to know
Which email addresses are seen on the network?
you'll use
The EMAIL ADDRESS Query and search on the IP
Have we seen any phone numbers (e.g. in sig lines) on the network?
you'll use
The PHONE NUMBER EXTRACTOR query and search on the IP
Have we collected any files or attachments on the IP/network?
you'll use
The EXTRACTED FILES query and search on the IP
Logins and Passwords for the server for TAO
you'll use
The LOGINS/PASSWORDS query and search on the IP (hint: Search on sys admin or valuable ports like 21, 23, 25)
Which websites people on the netork visit (e.g. Google Earth, web forums)
you'll use
the HTTP ACTIVITY query and pull on the IP

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


Which XKEYSCORE Query is Best for Me?
I have......
a/an
Email Address or Domain (foreign)
and need to know
Which IP addresses the target connects to
Which sites collect the user?
Are we collecting the user or domain?
you'll use
The EMAIL ADDRESS query and search on the email (in username) and domain (in domain)

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



Which XKEYSCORE Query is Best for Me?

I have......

a/an

A Phone Number

and need to know

The target's email address

then use

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