KEYSCORE

Email Address vs User Activity

24 June 2009

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20291123

DERIVED FROM: NSA/CSSM 1-52

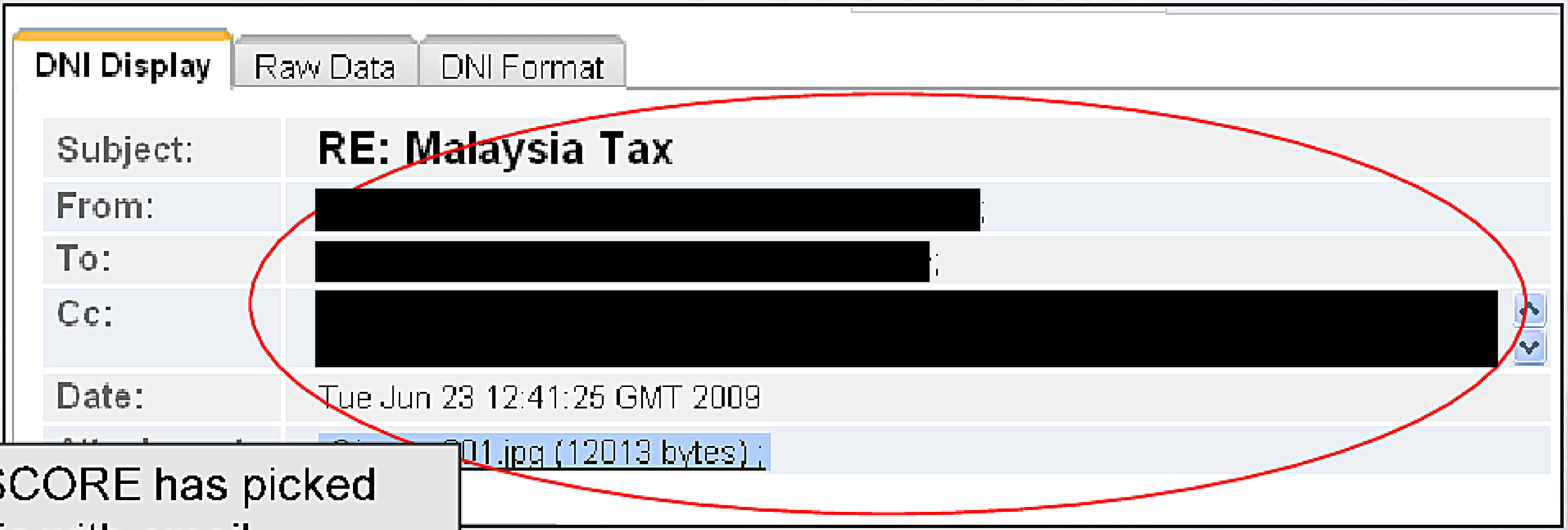
08

Email Addresses

- The Email Address search allows you to search on:
  - Full Email Address
    - **Do not** search on/wildcard JUST the username, always include a specific domain
  - Foreign-hosted domains (e.g. @cnc.cn)
- The query searches within bodies of emails, webpages and documents for….(you guessed it)…Email Addresses
  - To, From, CC, BCC lines..
  - “Contact Us” pages on websites
  - Signature blocks

Email Address

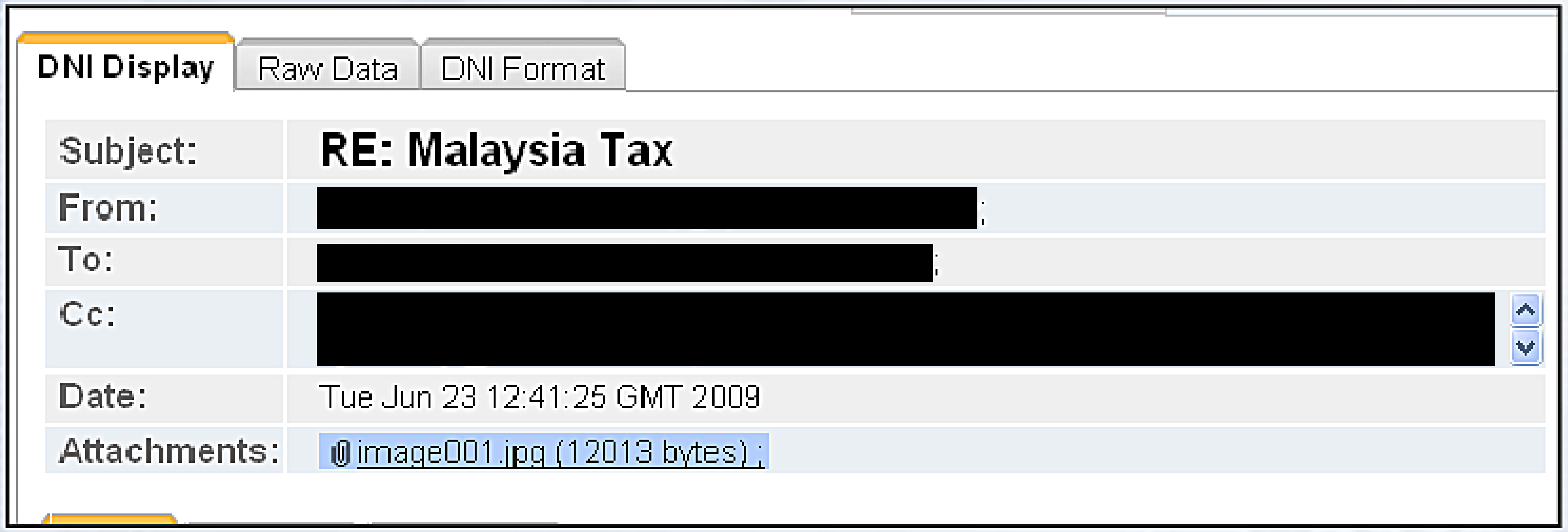
- Email Addresses are found in many parts of traffic



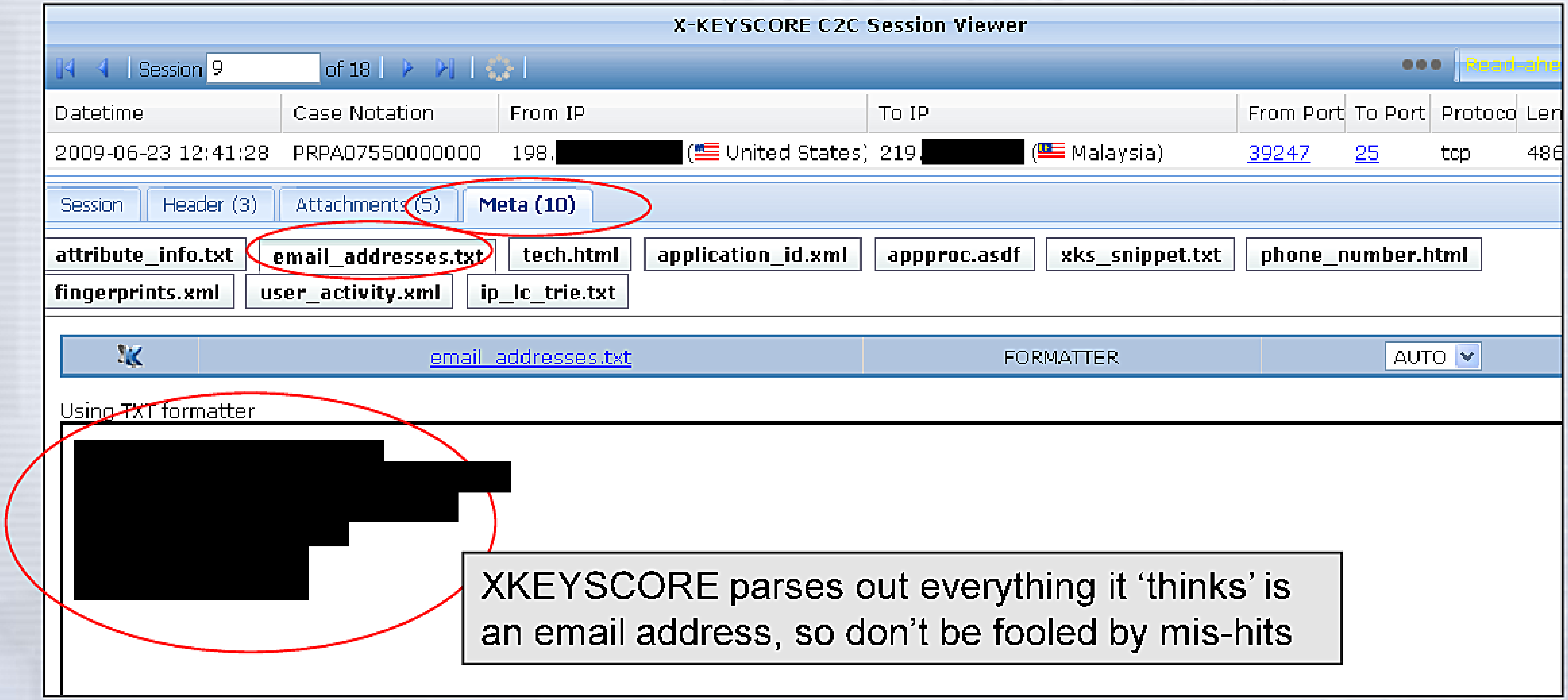
Subject:	RE: Malaysia Tax
From:	[redacted] ;
To:	[redacted] ;
Cc:	[redacted]
Date:	Tue Jun 23 12:41:25 GMT 2009
[illegible]	[illegible]01.jpg (12013 bytes) ;

XKEYSCORE has picked up traffic with email addresses in it..

Email Address



Subject:	RE: Malaysia Tax
From:	[redacted];
To:	[redacted];
Cc:	[redacted]
Date:	Tue Jun 23 12:41:25 GMT 2009
Attachments:	image001.jpg (12013 bytes) ;



Datetime	Case Notation	From IP	To IP	From Port	To Port	Protoco	Len
2009-06-23 12:41:28	PRPA07550000000	198.[redacted] (United States)	219.[redacted] (Malaysia)	39247	25	tcp	486

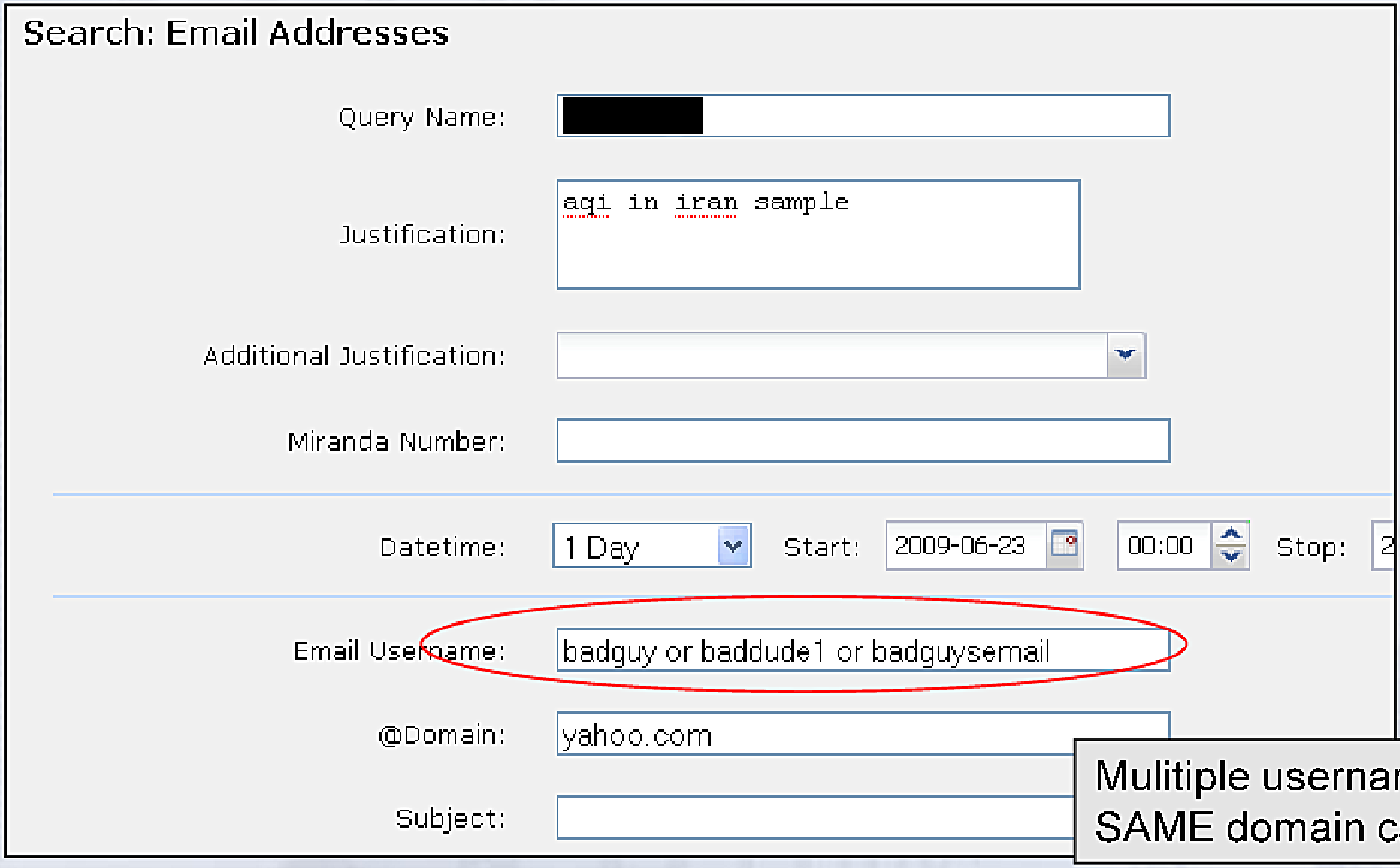
Using TXT formatter

[redacted]

XKEYSCORE parses out everything it 'thinks' is an email address, so don't be fooled by mis-hits

Creating Email Address Queries

- Enter usernames and domains into query



Search: Email Addresses

Query Name: [redacted]

Justification: aqi in iran sample

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-06-23 00:00 Stop: 2

Email Username: badguy or baddude1 or badguysemail

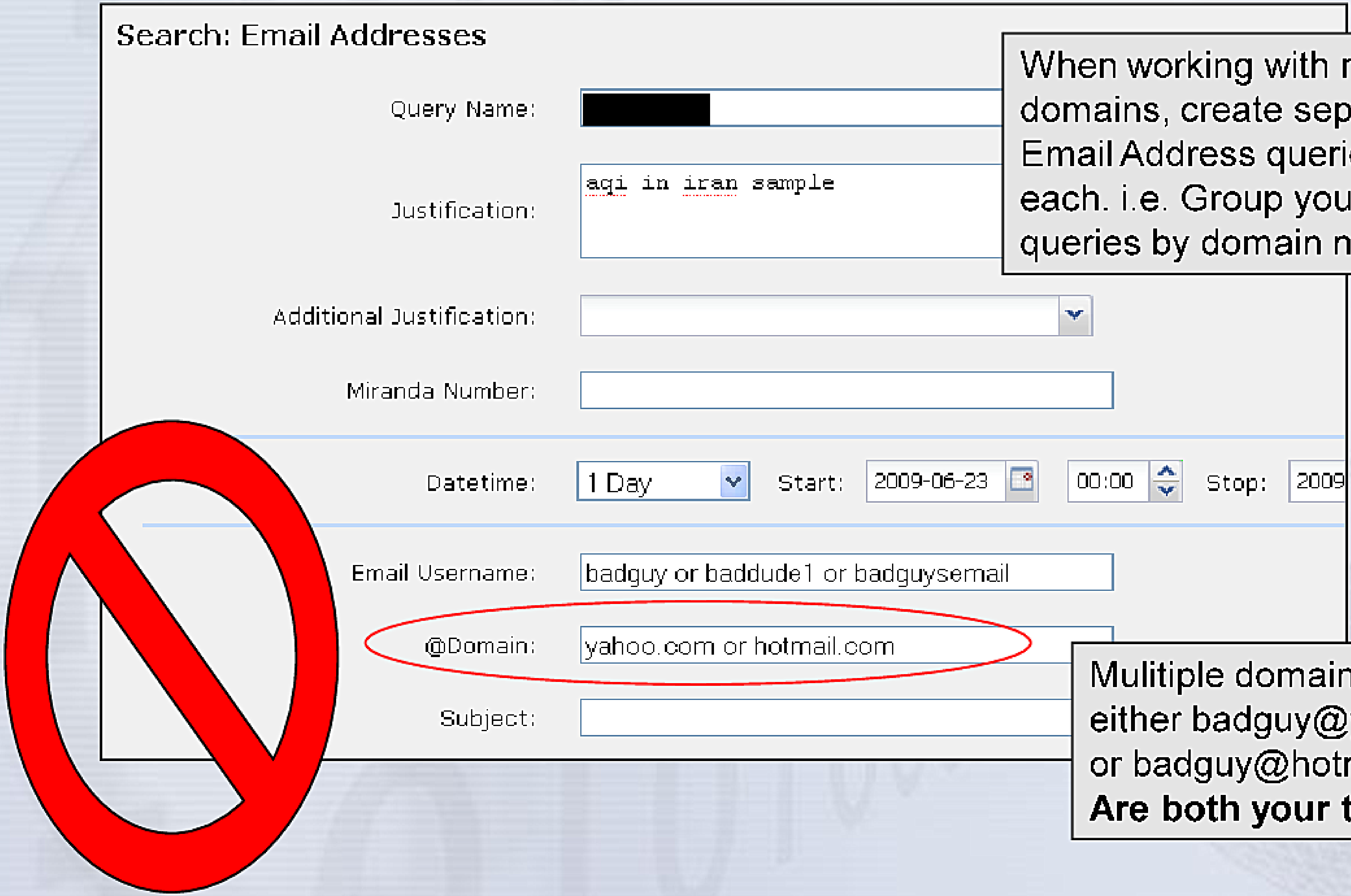
@Domain: yahoo.com

Subject:

Mulitiple usernames from SAME domain can be OR'd

Creating Email Address Queries

- BE VERY CAREFUL of OR'ing domains



Search: Email Addresses

Query Name: [redacted]

Justification: aqi in iran sample

Additional Justification:

Miranda Number:

Datetime: 1 Day Start: 2009-06-23 00:00 Stop: 2009

Email Username: badguy or baddude1 or badguysemail

@Domain: yahoo.com or hotmail.com

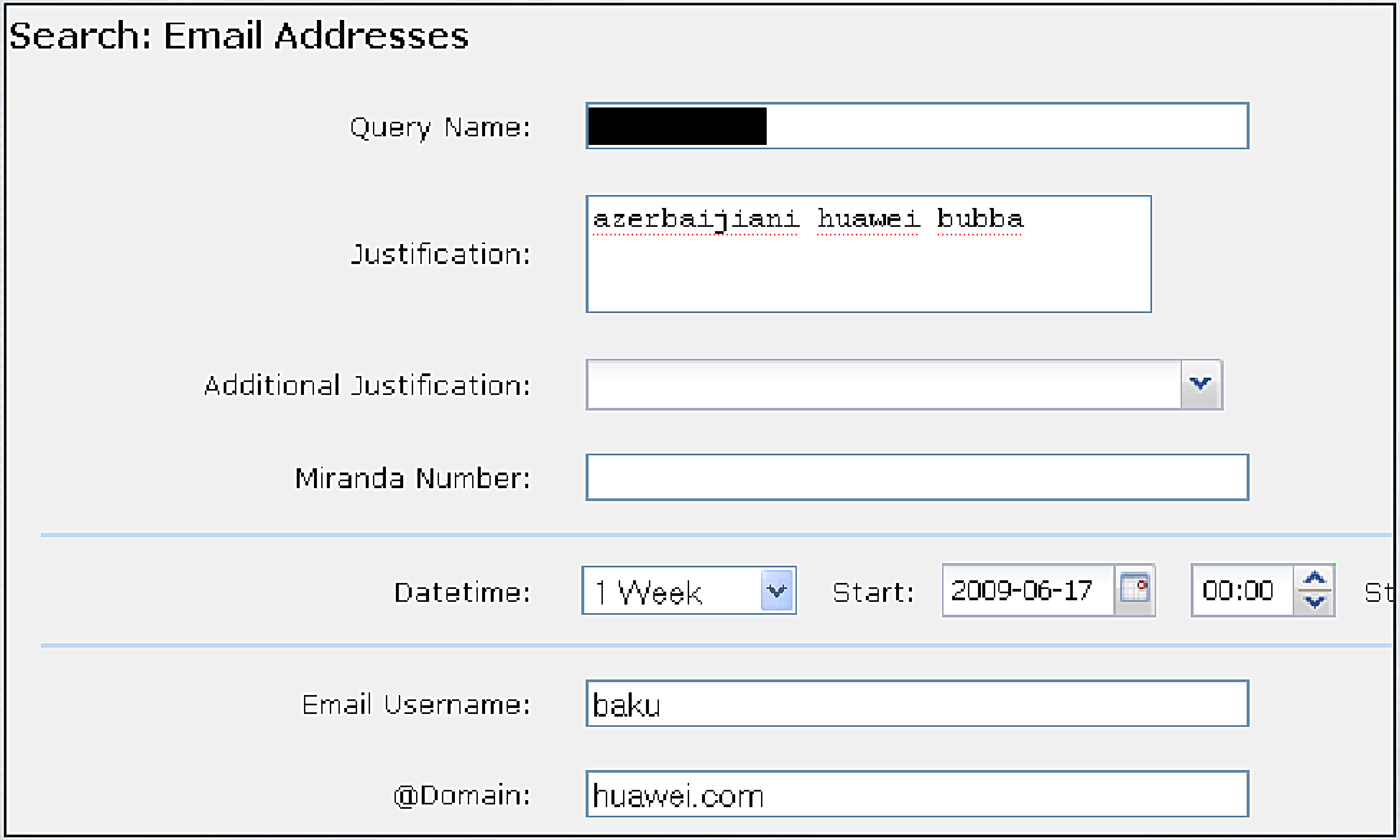
Subject:

When working with multiple domains, create separate Email Address queries for each. i.e. Group your queries by domain names.

Mulitiple domains means either badguy@yahoo.com or badguy@hotmail.com. **Are both your targets?**

Email Address

- Sample Search: baku@huawei.com



Search: Email Addresses

Query Name: [redacted]

Justification: azerbaijiani huawei bubba

Additional Justification:

Miranda Number:

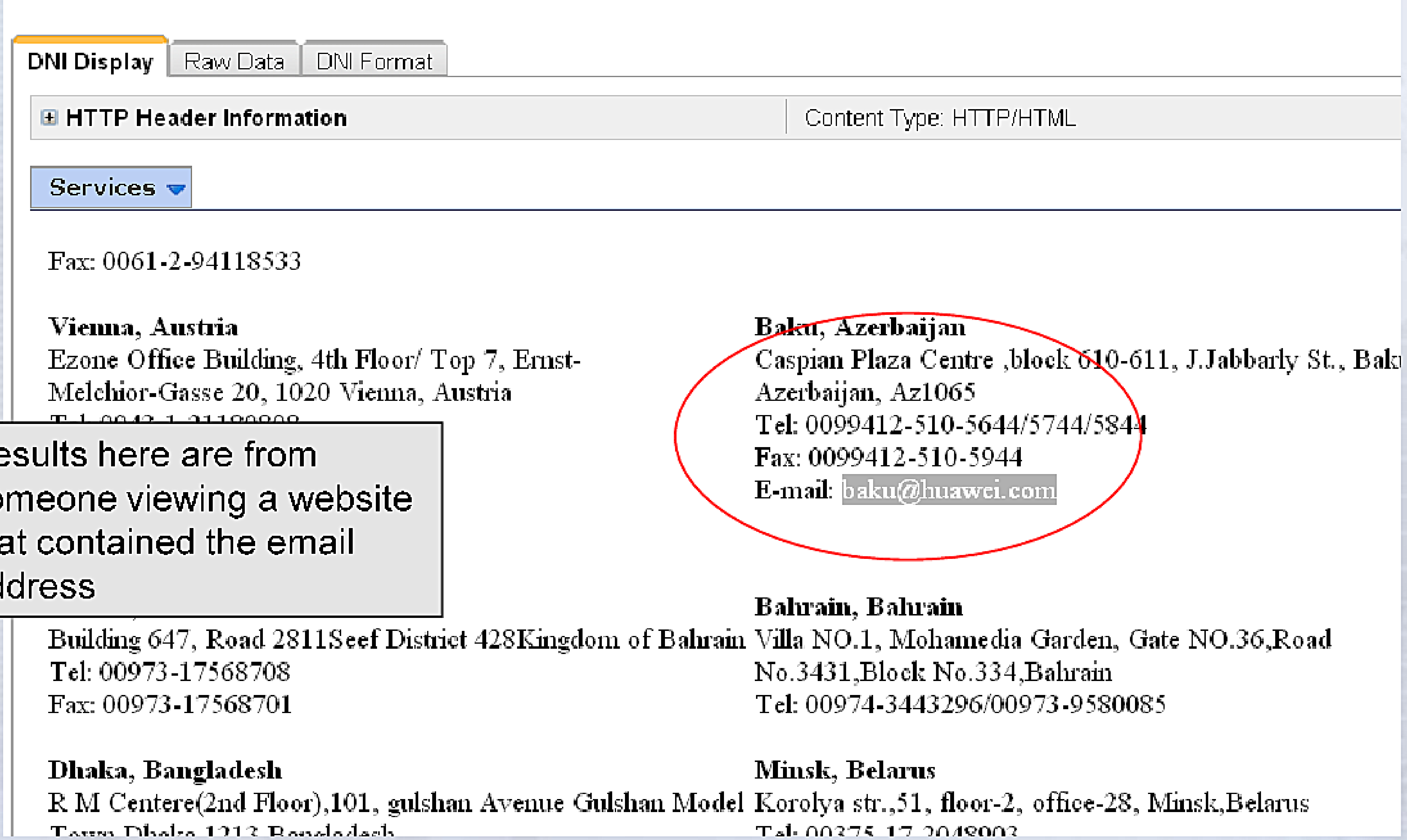
Datetime: 1 Week Start: 2009-06-17 00:00 St

Email Username: baku

@Domain: huawei.com

Email Address

- Email Addresses are found in many parts of traffic



Fax: 0061-2-94118533

Vienna, Austria
Ezone Office Building, 4th Floor/ Top 7, Ernst-Melchior-Gasse 20, 1020 Vienna, Austria
Tel: 0043-1-31180808

Baku, Azerbaijan
Caspian Plaza Centre ,block 610-611, J.Jabbarly St., Baku
Azerbaijan, Az1065
Tel: 0099412-510-5644/5744/5844
Fax: 0099412-510-5944
E-mail: baku@huawei.com

Building 647, Road 2811Seef District 428Kingdom of Bahrain
Tel: 00973-17568708
Fax: 00973-17568701

Bahrain, Bahrain
Villa NO.1, Mohamedia Garden, Gate NO.36,Road No.3431,Block No.334,Bahrain
Tel: 00974-3443296/00973-9580085

Dhaka, Bangladesh
R M Centere(2nd Floor),101, gulshan Avenue Gulshan Model Town Dhaka 1213 Bangladesh

Minsk, Belarus
Korolya str.,51, floor-2, office-28, Minsk,Belarus
Tel: 00375-17-2048903

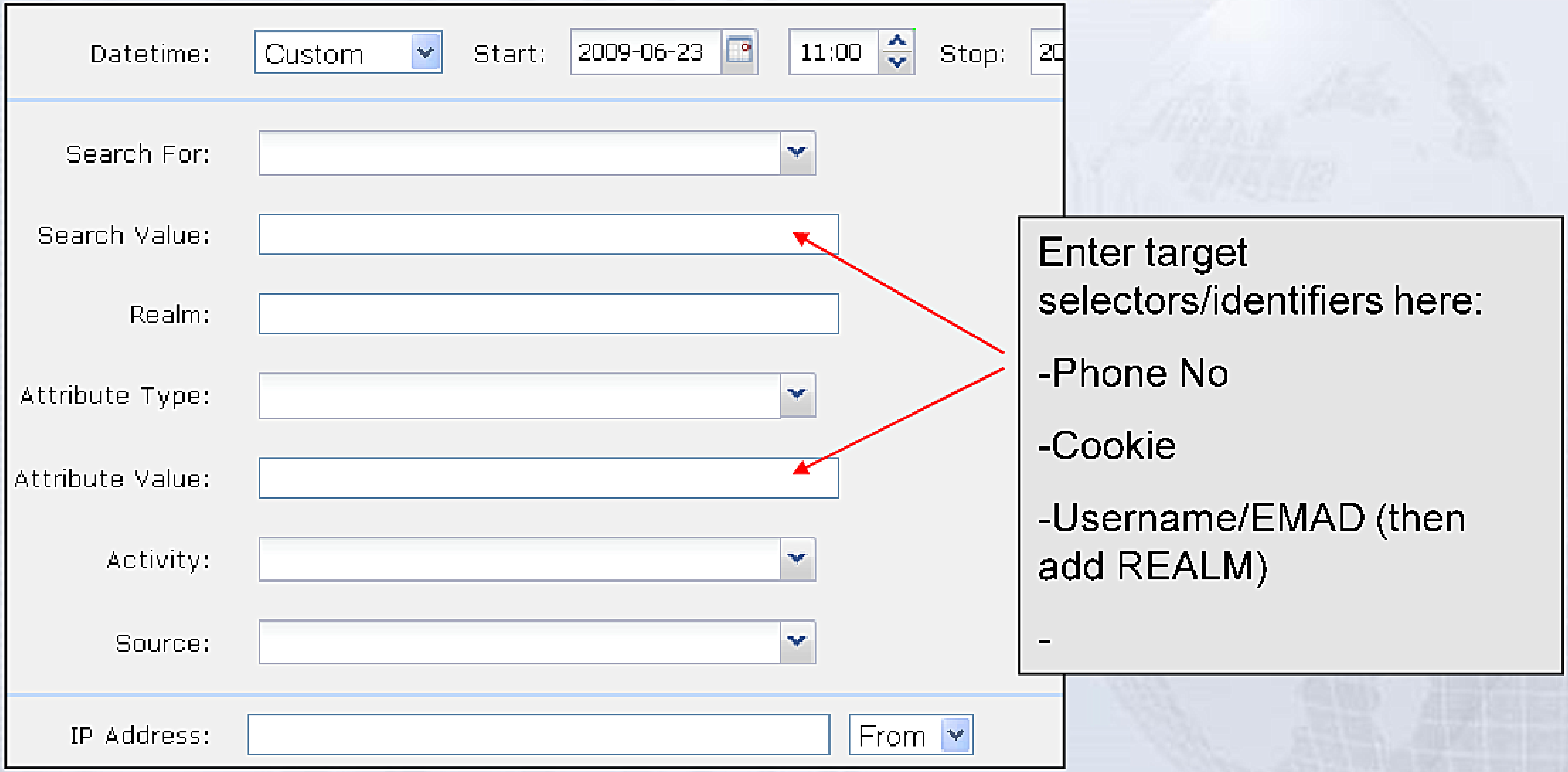
Results here are from someone viewing a website that contained the email address

User Activity Query

- User Activity query is based on APPROC collection (such as chat, webmail, etc)
- Allows more flexible search criteria than Email Address query
  - Can search on: Cookies, numeric logins (e.g. web forums & OSN), VoIP selectors, webcam first images, Webmail profile information from registration (birthdays), general usernames

Creating User Activity Queries

- The fields in a User Activity query can be confusing



Datetime: Custom Start: 2009-06-23 11:00 Stop: 20

Search For:

Search Value:

Realm:

Attribute Type:

Attribute Value:

Activity:

Source:

IP Address: From

Enter target selectors/identifiers here:

-Phone No

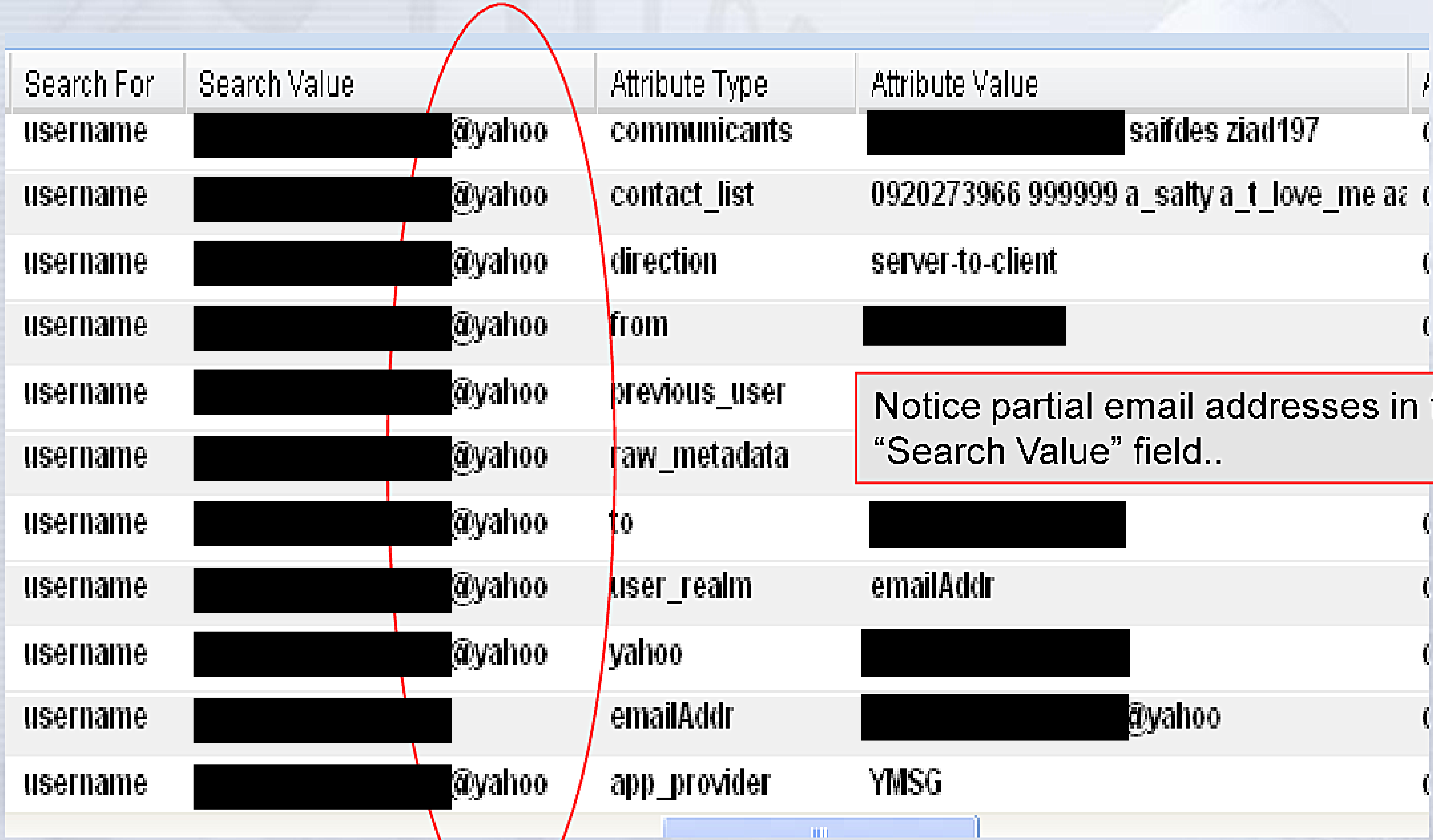
-Cookie

-Username/EMAD (then add REALM)

-

Creating User Activity Queries

- The fields in a User Activity query can be confusing



Search For	Search Value	Attribute Type	Attribute Value
username	[redacted]@yahoo	communicants	[redacted] saifdes ziad197
username	[redacted]@yahoo	contact_list	0920273966 999999 a_salty a_t_love_me aa
username	[redacted]@yahoo	direction	server-to-client
username	[redacted]@yahoo	from	[redacted]
username	[redacted]@yahoo	previous_user	
username	[redacted]@yahoo	raw_metadata	
username	[redacted]@yahoo	to	[redacted]
username	[redacted]@yahoo	user_realm	emailAddr
username	[redacted]@yahoo	yahoo	[redacted]
username	[redacted]	emailAddr	[redacted]@yahoo
username	[redacted]@yahoo	app_provider	YMSG

Notice partial email addresses in the “Search Value” field..

Creating User Activity Queries

- Scenario:

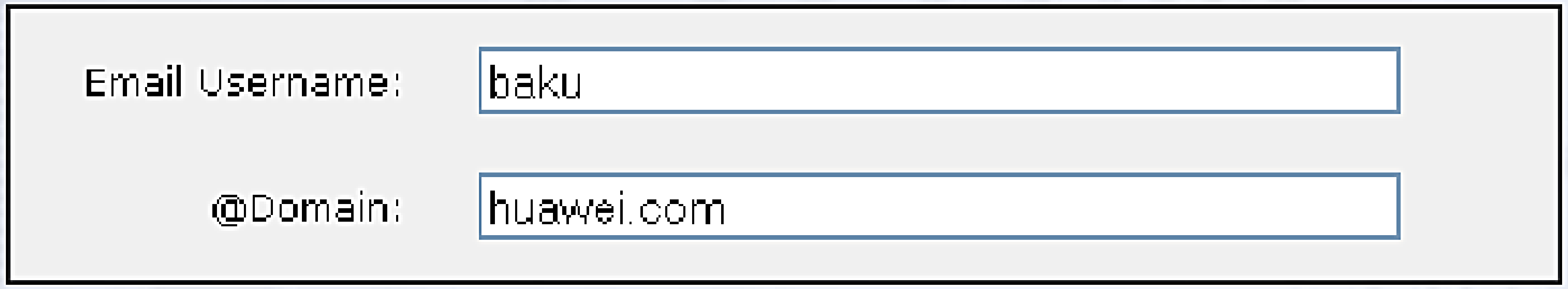
  You have a target's email address:

  - [redacted]@hotmail.com
    - Known: One email address
    - Unknown: Alternate ID's, IPs, Location, Photo, etc… (lots of stuff)

Where do we begin?

I want to….

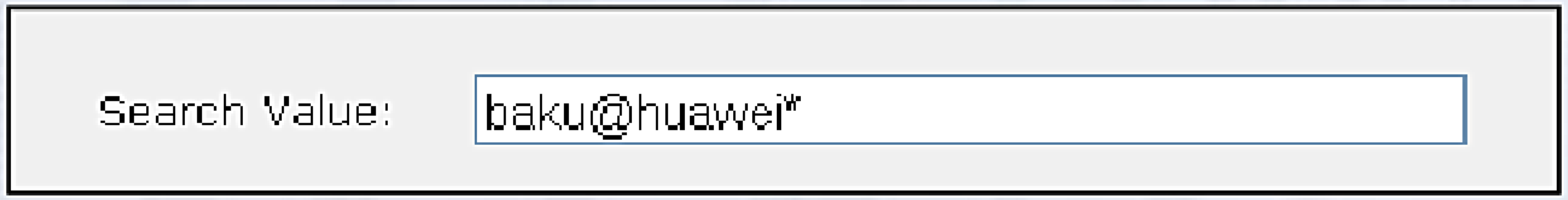
- I have an Email Address and want to see if it's being collected?
  - Do an **Email Address** query on username and domain



Email Username: baku

@Domain: huawei.com

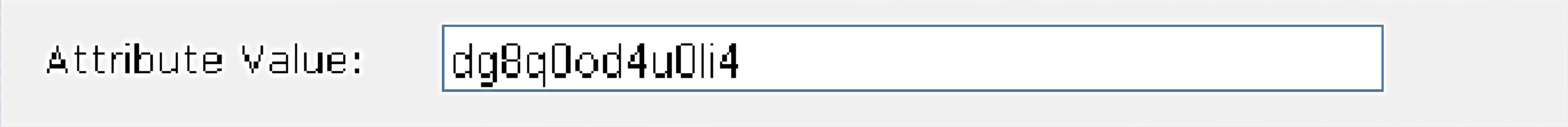
  - Do a **User Activity** query on the email address in the "Selector Value"



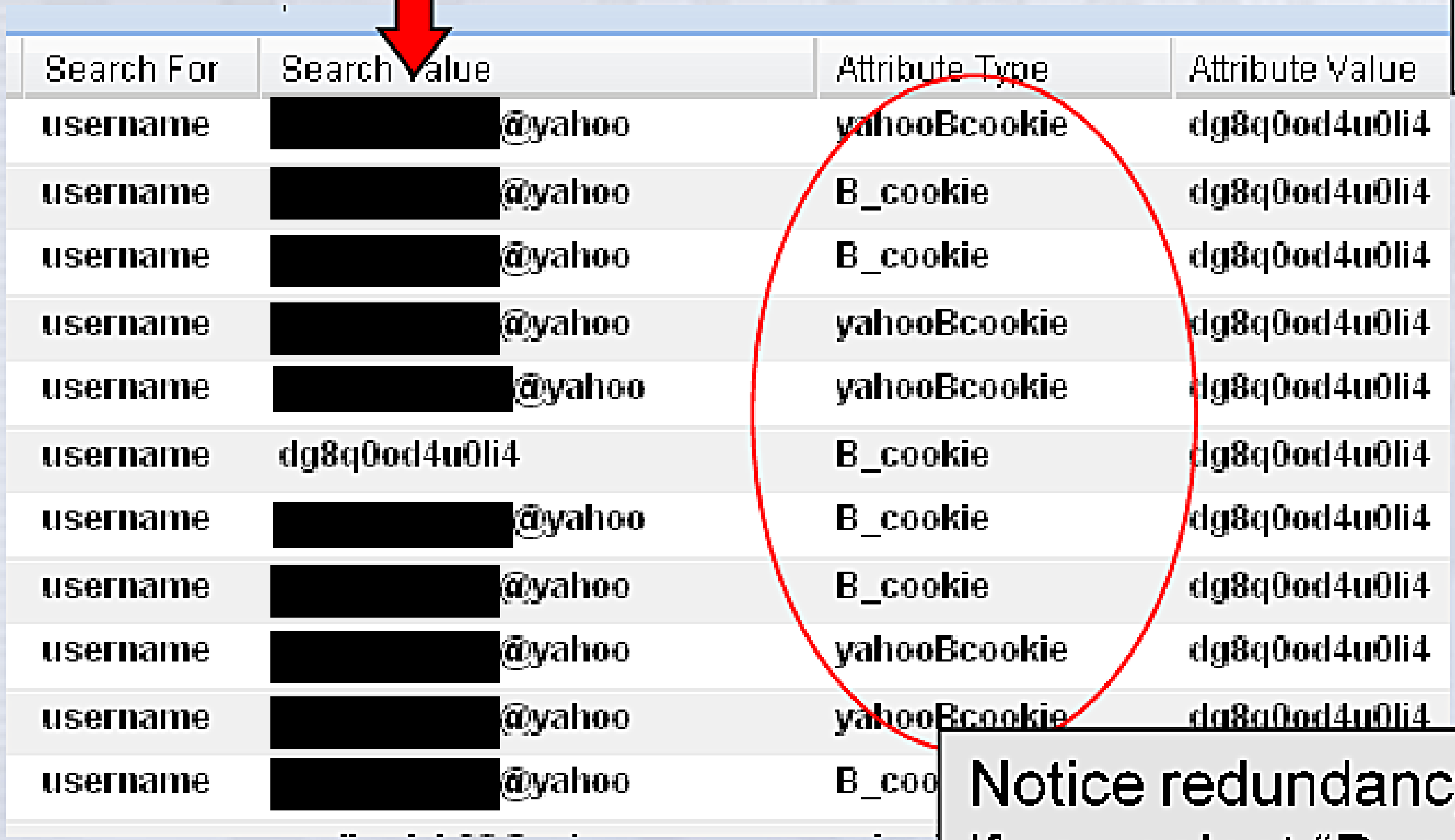
Search Value: baku@huawei*

I want to….

- I have a Cookie and want to see what other accounts access this computer
  - Do TWO separate **User Activity** query on the cookies
  - 1.



Attribute Value: dg8q0od4u0li4



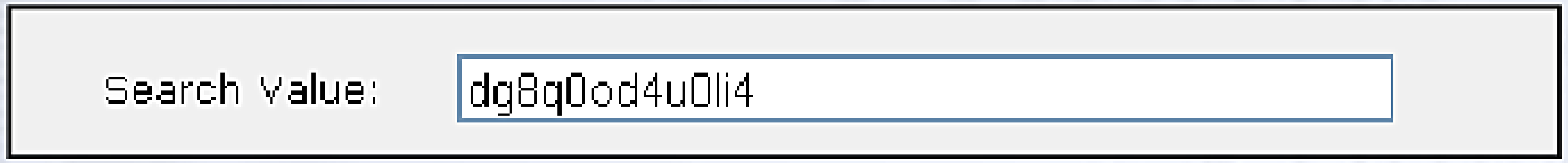
Search For	Search Value	Attribute Type	Attribute Value
username	[redacted]@yahoo	yahooBcookie	dg8q0od4u0li4
username	[redacted]@yahoo	B_cookie	dg8q0od4u0li4
username	[redacted]@yahoo	B_cookie	dg8q0od4u0li4
username	[redacted]@yahoo	yahooBcookie	dg8q0od4u0li4
username	[redacted]@yahoo	yahooBcookie	dg8q0od4u0li4
username	dg8q0od4u0li4	B_cookie	dg8q0od4u0li4
username	[redacted]@yahoo	B_cookie	dg8q0od4u0li4
username	[redacted]@yahoo	B_cookie	dg8q0od4u0li4
username	[redacted]@yahoo	yahooBcookie	dg8q0od4u0li4
username	[redacted]@yahoo	yahooBcookie	dg8q0od4u0li4
username	[redacted]@yahoo	B_coo	

Brings back THESE results…

Notice redundancy.. So you MAY miss traffic if you select "B_cookie" or "yahooBcookie" (don't know why)

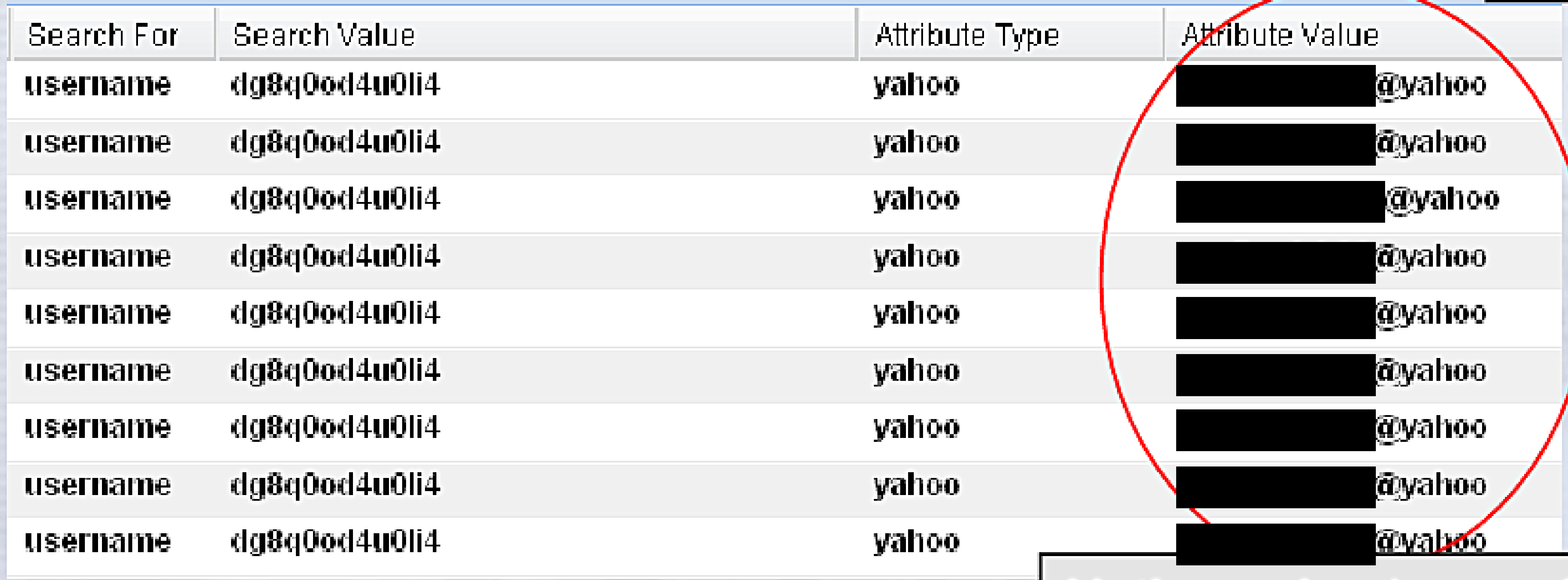
I want to….

- I have a Cookie and want to see what other accounts access this computer
  - Do TWO separate **User Activity** query on the cookies
  - 2.



Search Value: dg8q0od4u0li4

Brings back THESE results…

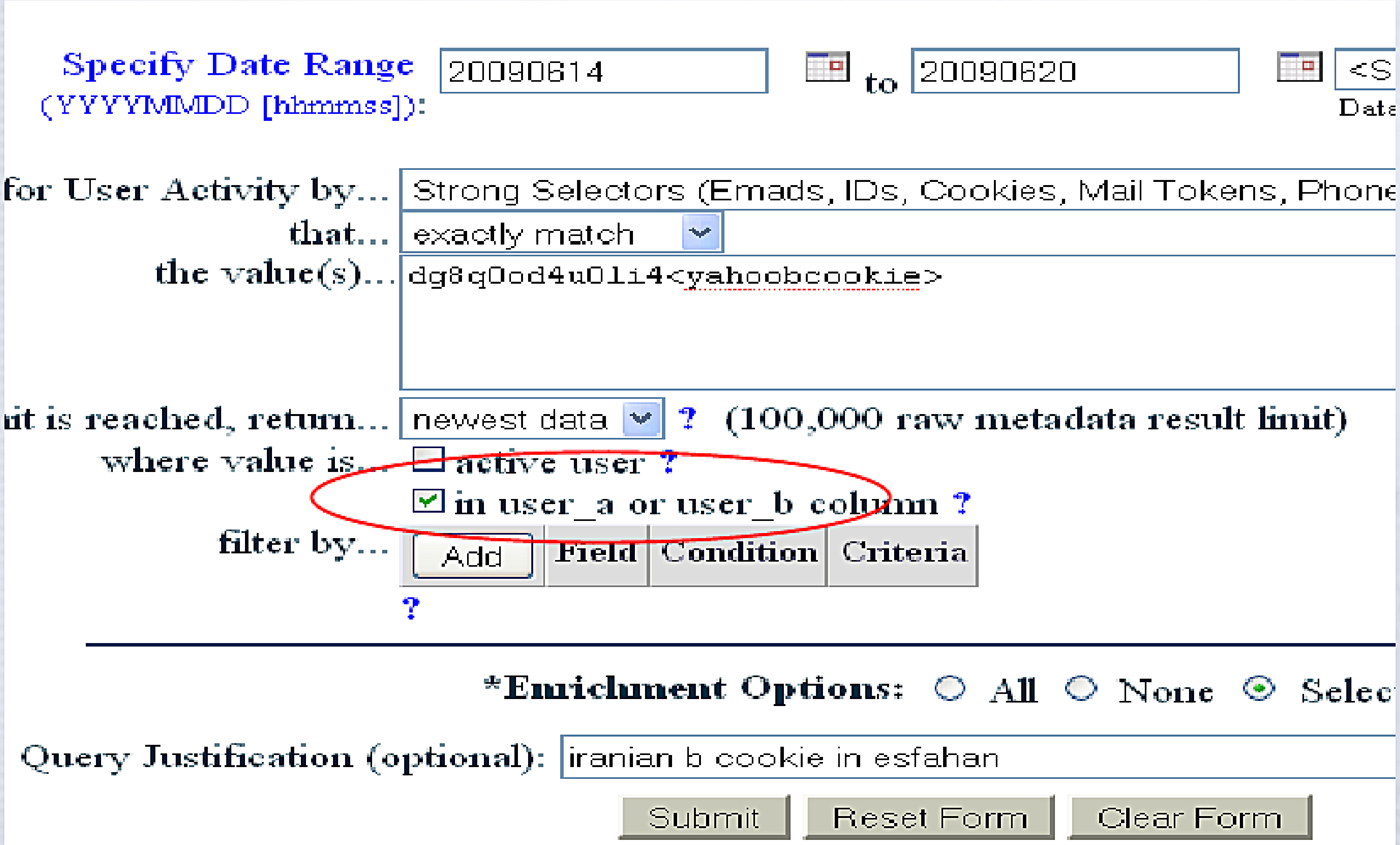


Search For	Search Value	Attribute Type	Attribute Value
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo

Notice redundancy.. So you MAY miss traffic if you select “B_cookie” or “yahooBcookie” (don’t know why)

I want to….

- I have a Cookie and want to see what other accounts access this computer
  - Do a Marina query on the cookie as well (why not)?



Specify Date Range (YYYYMMDD [hhmmss]): 20090614 to 20090620 <S
Date

for User Activity by… Strong Selectors (Emads, IDs, Cookies, Mail Tokens, Phone

that… exactly match

the value(s)… dg8q0od4u0li4<yahoobcookie>

it is reached, return… newest data ? (100,000 raw metadata result limit)

where value is… □ active user ?
☑ in user_a or user_b column ?

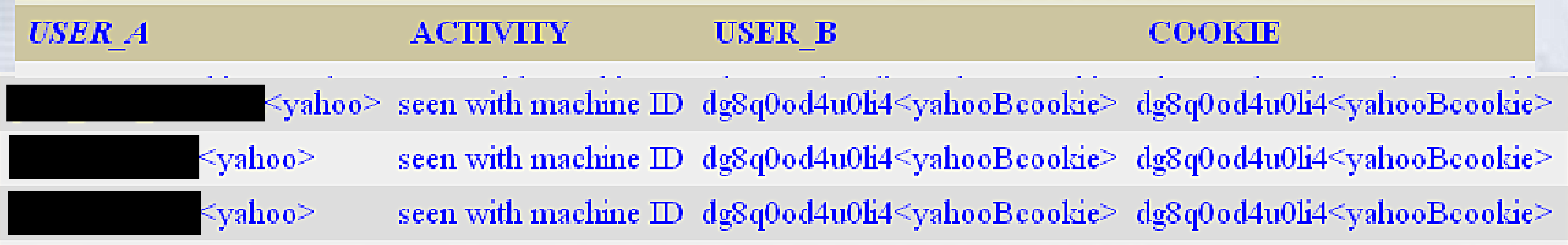
filter by… Field Condition Criteria
?

*Enrichment Options: ○ All ○ None ● Selec

Query Justification (optional): iranian b cookie in esfahan

I want to….

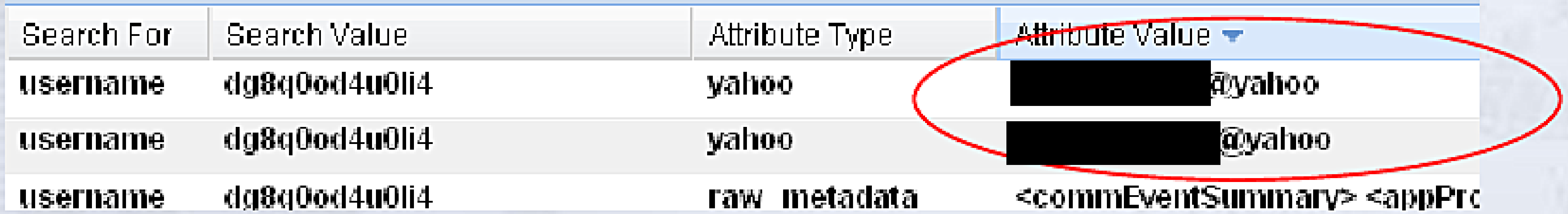
- I have a Cookie and want to see what other accounts access this computer
  - Do a Marina query on the cookie as well (why not)?



USER_A	ACTIVITY	USER_B	COOKIE
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>

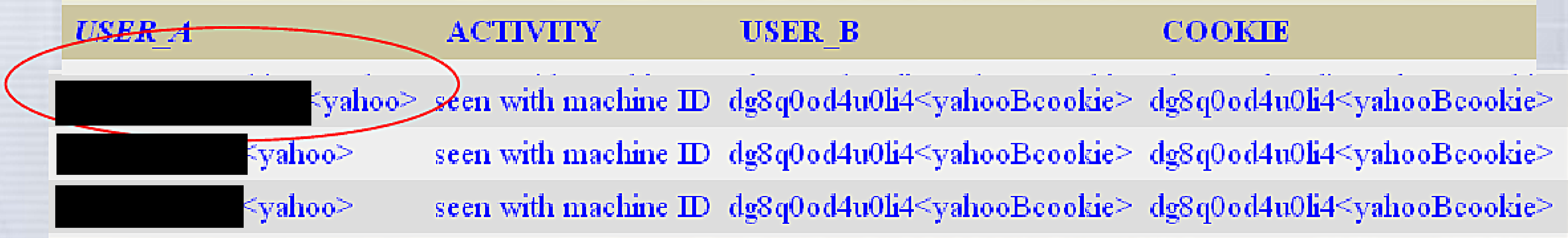
I want to….

- So let's put the cookie query all together…
  - Between Marina and XKS, I should have an idea of all the accounts..
    - Results pulling on dg8q0od4u0li4 as a Search Value



Search For	Search Value	Attribute Type	Attribute Value
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	yahoo	[redacted]@yahoo
username	dg8q0od4u0li4	raw_metadata	<commEventSummary> <appPrc

    - Plus my Marina results

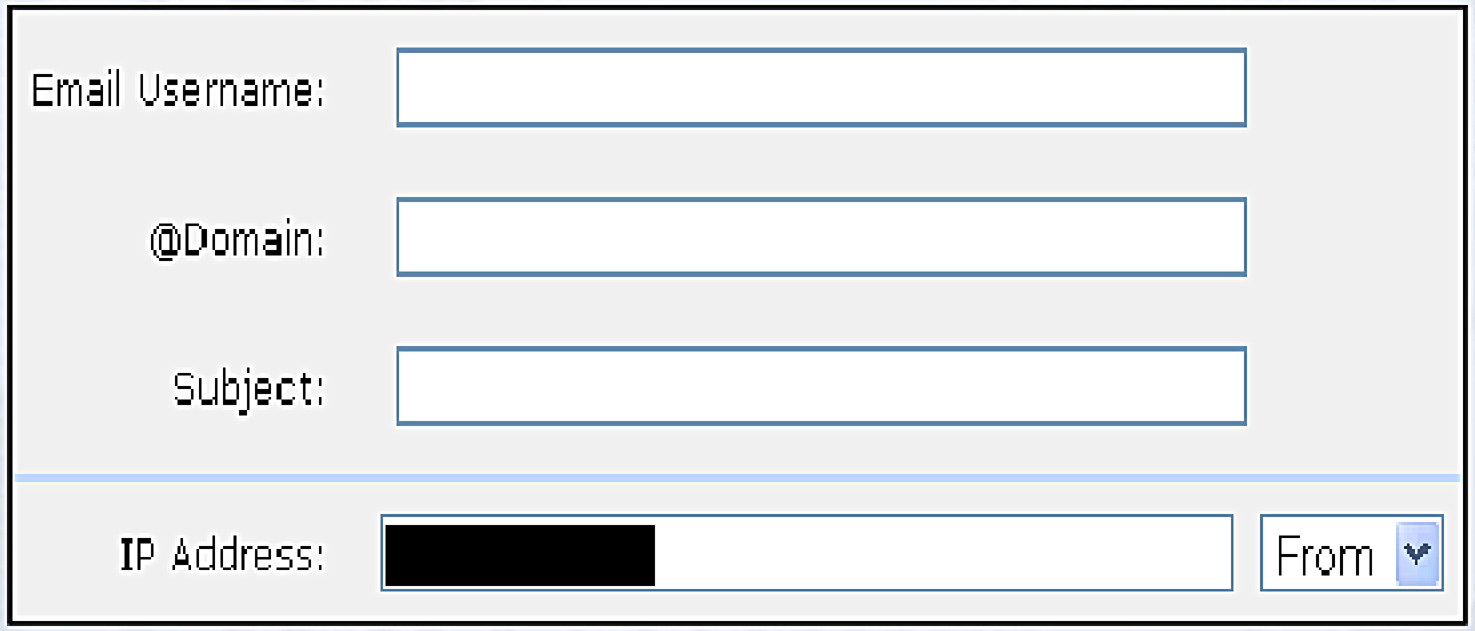


USER_A	ACTIVITY	USER_B	COOKIE
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>
[redacted]<yahoo>	seen with machine ID	dg8q0od4u0li4<yahooBcookie>	dg8q0od4u0li4<yahooBcookie>

RESULTS: Three users on the a computer..

I want to….

- I have an IP address and want to know what users/accounts are collected in that network? (I.E. a Café's IP address, or mail/web server for an organization)
  - Do an **Email Address** query on the IP address



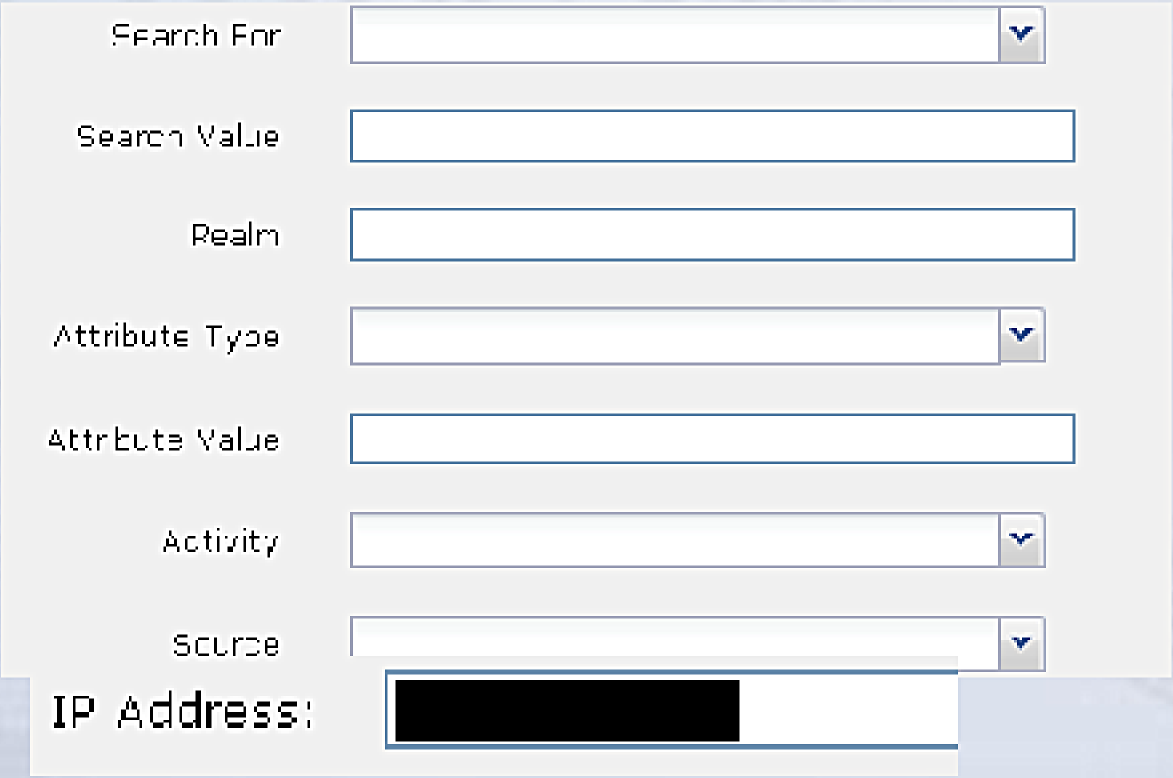
Email Username:

@Domain:

Subject:

IP Address: [redacted] From

  - Do a **User Activity** query on the IP address



Search For

Search Value

Realm

Attribute Type

Attribute Value

Activity

Source

IP Address: [redacted]

Moral of the story

- Email Address query looks for the @ symbol in traffic
- User Activity search allows you to query on more than just an email address