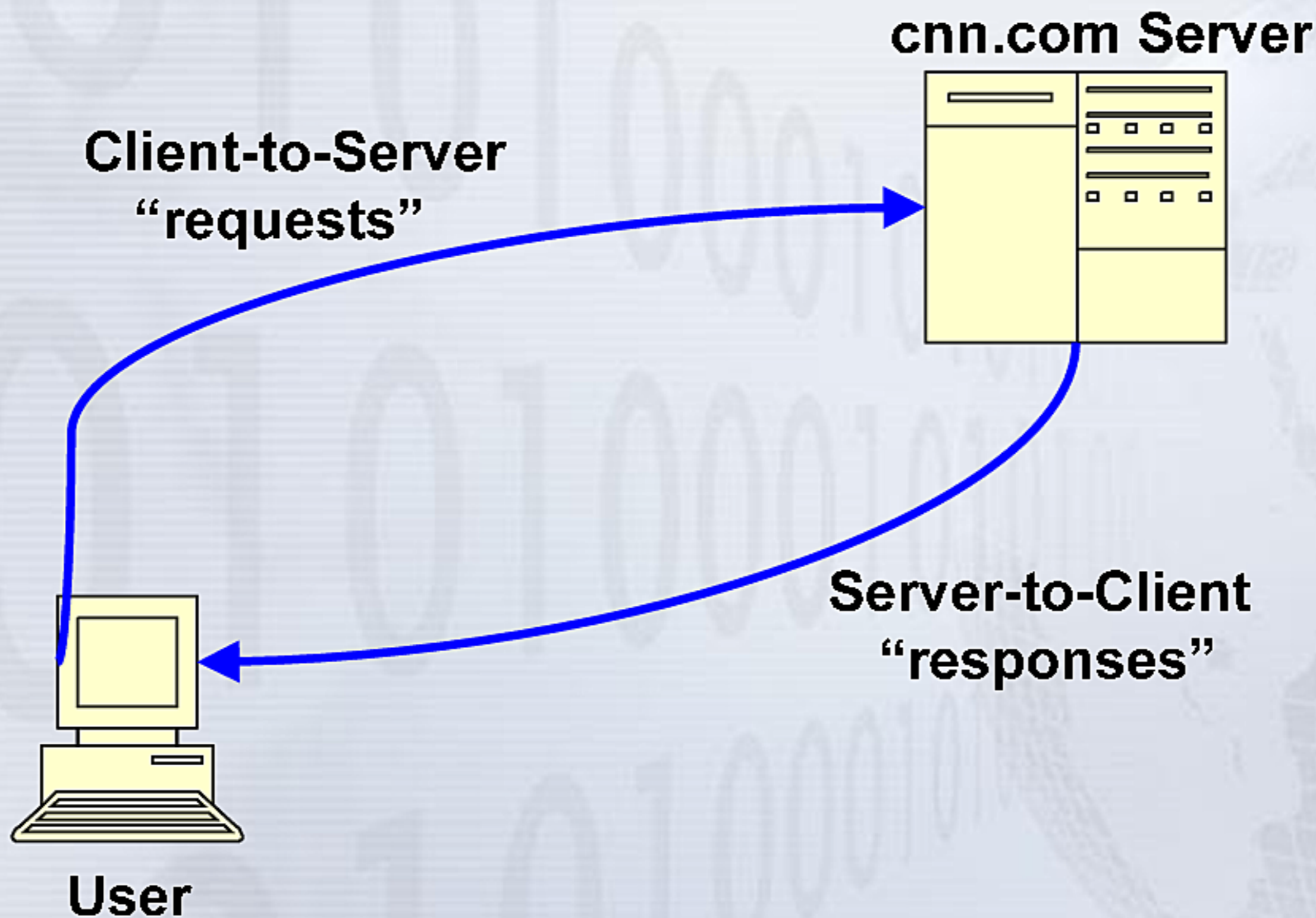# HTTP Activity in XKEYSCORE

March 2009

HTTP Activity

- HTTP Activity is essentially all web-based activity from a user's internet browser (with some exceptions)

- It includes, web-surfing, Internet Searching (like Google), Mapping Website (Google Earth/Maps) etc.

- Most of this data will not contain a strong selector like E-mail address

HTTP Activity

- HTTP activity comes in two types:

cnn.com Server

**Client-to-Server
"requests"**

**Server-to-Client
"responses"**

User

HTTP Activity

- How do you know which side you're looking at?
- Client-to-Server requests are generally small in size and are computers talking to other computers
- Server-to-Client responses larger and are what web-pages look like at home
- So if you're looking at something that looks like a web-page its Server-to-Client

HTTP Activity Examples

KEYSCORE

Client-to-Server request:

TOP SECRET//COMINT//20320108

ID: sess_orig_proc

Type: HTTP-GET   🖨 Printer Friendly Version

DNI Display   Raw Data   DNI Format

Services ▾

GET /Hezbollah-Terrorism-Judith-Palmer-Harik/dp/1860648932 HTTP/1.1	
User-Agent:	Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US) AppleWebKit/525.19 (KHTML, like Gecko) Chrome/1.0.154.48 Safari/525.19
Referer:	http://www.google.com.pk/search?hl=en&q=wretten books on hizbollah&btnG=Google Search&meta=
Accept:	text/xml,application/xml,application/xhtml xml,text/html;q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Encoding:	gzip,deflate,bzip2,sdch
Cookie:	ubid-main=185-5525816-8765531
	apn-user-id=P1YXY7QF1PUYQ5
Accept-Language:	en-US,en
Accept-Charset:	ISO-8859-1,*,utf-8
Host:	www.amazon.com
Connection:	Keep-Alive

HTTP Activity Examples

Server-to-Client Response:

HTTP Activity

- XKS HTTP Activity Meta-data differs greatly depending on which side of traffic we're collecting

- In nearly all cases it's better to have client-to-server traffic

HTTP Activity Client-to-Server

KEYSCORE

```
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%28co
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

HTTP Activity Server-to-Client

HTTP Activity – HTTP Types

- Meta-data will also tell you which side of traffic you're looking at

- Client-to-server has two main types:

HTTP Type
get

HTTP Type
post

- Server-to-client has only one:

HTTP Type
response

HTTP Activity – Get vs Post

- A 'GET' is you requesting data from the server (most web surfing)

- A 'POST' is you sending data to the server (i.e. signing in, filling out a form, uploading a file etc.)

XKS SIGDEV: HTTP Traffic

Example: Lets look for all Arabic font Google queries coming out of the tribal areas of Pakistan

Information needed is contained in HTTP Activity meta-data

XKS SIGDEV: HTTP Traffic

TS ▲	USERID	PHONE	USER_A		ACTIVITY	USER_B	
20081119 074259Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074259Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074304Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074316Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074316Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074316Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦

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

20081119 0743̶1̶6̶Z			████████████	\<emailAddr\>	logged in (email)	116.	🚦
20081119 074357Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074357Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074357Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074357Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074358Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074358Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074358Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074358Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦
20081119 074511Z			████████████	\<emailAddr\>	logged in (email)	116.████████	🚦

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)
============================================================|

               SEARCHES

============================================================
www.google.com
---------------
 116.█          2008-11-19 18:54:20 : al qaida (en, en-GB) (1)
 116.█          2008-11-19 07:36:49 : The al-Ikhlas network (cybertrans from Arabic) (1)
 116.█          2008-11-19 07:37:07 : (referer) the al-Ikhlas network (cybertrans from Arabic) (3)
 116.█          2008-11-19 08:03:17 : Forum bride/'Arus (cybertrans from Arabic) (1)
 116.█          2008-11-19 08:05:51 : Forum love/gram (cybertrans from Arabic) (1)
 116.█          2008-11-19 08:06:52 : (referer) forum love/gram (cybertrans from Arabic) (1)
 116.█          2008-11-19 15:01:00 : The hills jihadist without inflicting (cybertrans from Arabic) (10)
 116.█          2008-11-19 15:14:13 : (referer) the hills jihadist without inflicting (cybertrans from Arabic) (6)
 116.█          2008-11-19 15:33:19 : Waziristan (cybertrans from Arabic) (1)
 116.█          2008-11-19 04:24:44 : Scandals (cybertrans from Arabic) (2)
 116.█          2008-11-19 04:24:59 : (referer) scandals (cybertrans from Arabic) (1)
 116.█          2008-11-19 04:29:29 : News (cybertrans from Arabic) (1)
 116.█          2008-11-19 04:30:04 : Forum soil (cybertrans from Arabic) (1)
 116.█          2008-11-19 04:31:51 : (referer) forum soil (cybertrans from Arabic) (1)
                  </and>
```

Workflow Values Workflow XML

HTTP Activity – URLs

- ■ Many targets use Free File Sharing Websites to pass messages.

- ■ Example we may see a message like this:

From: badguy@yahoo.com

To: someotherbadguy@yahoo.com

Hey dude check out this file:

http://www.sendspace.com/file/1gojft

- ■ Lets use X-KEYSCORE to find who else might have viewed that file

HTTP Activity – URL Structure

KEYSCORE

- ## XKS breaks up URL's into their components:

http://www.google.com/search?hl=ar&lr=&q=terrorism&start=10&sa=N

www.google.com is the 'host'

aka everything between the http:// and the first/**search is the 'url path' everything after www.blah.com and before the ?**

hl=ar&lr=&q=terrorism&start=10&sa=N

is the 'url argument' aka everything after the ?

terrorism is the 'search term'

XKS SIGDEV: HTTP Traffic

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

XKS SIGDEV: HTTP Traffic

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

Datet
2008

XKS HTTP Meta-data: 'Atiyah

- (TS//SI//OC/REL TO USA, AUS, CAN, GBR, NZL) During his Internet session, 'Atiyah queried on himself, "Shaykh 'Atiyatallah," and on the name "Khalid al-Habib." (3/OO/7878-08)

- (TS//SI//OC/REL TO USA, AUS, CAN, GBR, NZL) During his session on 16 September, 'Atiyah used a U.S. search engine to search for information on himself and a possible associate. 'Atiyah submitted Arabic queries for an alias of his, "'Atiyahtallah", and his real name, "Jamal Ibrahim Ishtaywi". 'Atiyah also queried for "A Revealing View." (COMMENT: This is likely a reference to the book he recently wrote entitled "Lebanese Hezballah and the Palestinian Issue - A Revealing View.") 'Atiyah also queried for "'Ali 'Iwad al-Harabi" (no further information). On 17 September, 'Atiyah searched again on the title of his book. (3/OO/7151-08)

XKS HTTP Meta-data: 'Atiyah

- (TS//SI//OC/REL TO USA, AUS, CAN, GBR, NZL) During the 1035Z to 1143Z online activity, 'Atiyah down-loaded the VoIP application Skype to his private computer. During an earlier online session from approximately 0902Z to 0935Z, either 'Atiyah or his wife, Jamila, also down-loaded Skype onto her private computer. (3/OO/10570-07)

- (TS//SI//OC/REL TO USA, AUS, CAN, GBR, NZL) Although much of 'Atiyah's online activity is communication, he is also a "news hound." While located in Sanandaj, 'Atiyah daily visited several online international news sites, such as Qatar-registered al-Jazeera news website, and Arabic language versions of U.S.-based and U.K.-based news organizations. Also, 'Atiyah frequently visits religious sites, such as the Saudi Arabia-registered islamtoday.net. (3/OO/21045-07)

XKS Enabled: Google Earth Exploitation