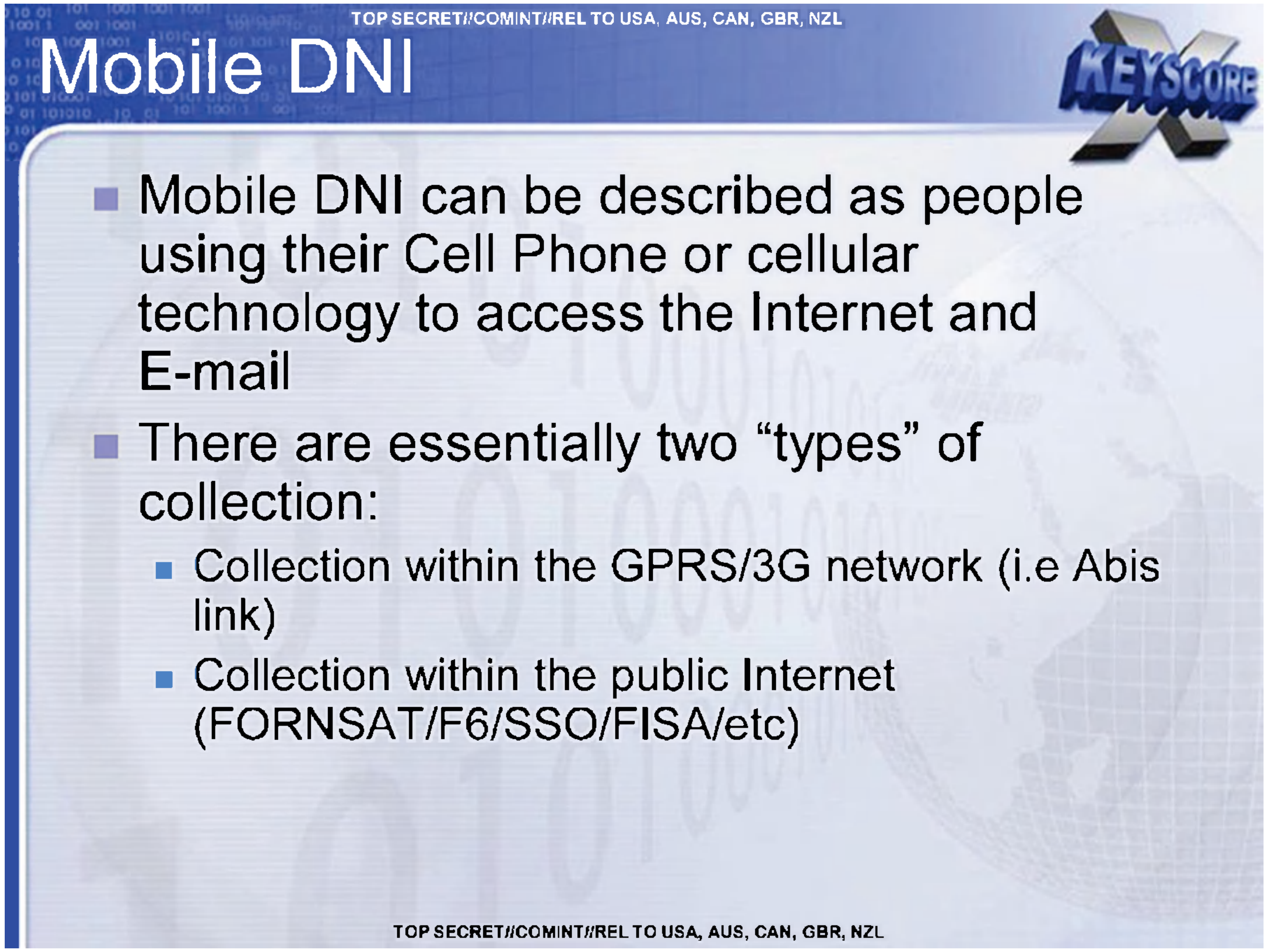
Analyzing Mobile/Cellular DNI in XKEYSCORE

May 2009

Derived From: NSA/C[illegible]
Dated: 2007[illegible]
Declassify On: 20291123

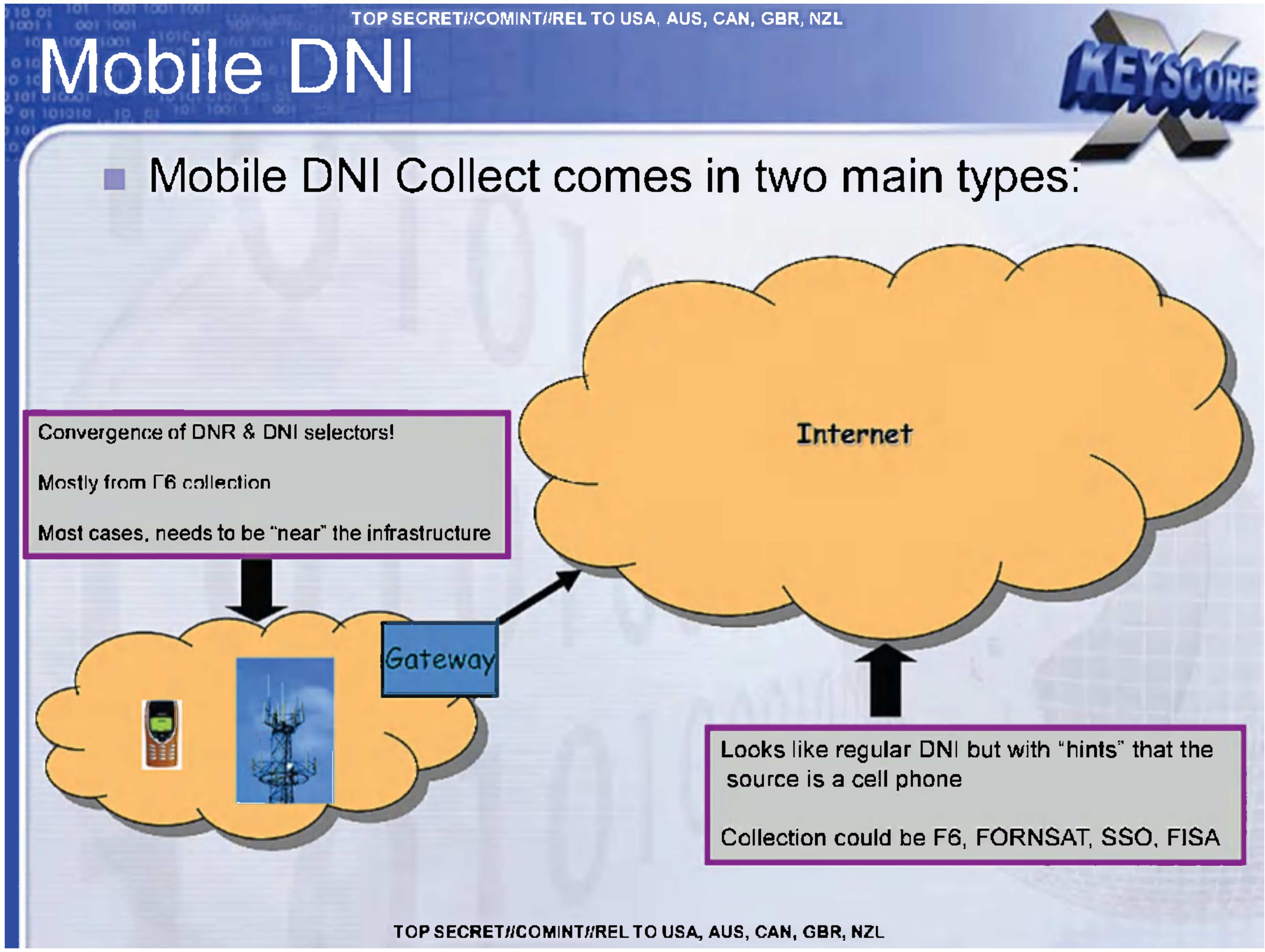
[redacted]CSSM 1-52

08



Mobile DNI

- Mobile DNI can be described as people using their Cell Phone or cellular technology to access the Internet and E-mail
- There are essentially two “types” of collection:
  - Collection within the GPRS/3G network (i.e Abis link)
  - Collection within the public Internet (FORNSAT/F6/SSO/FISA/etc)



Mobile DNI

- Mobile DNI Collect comes in two main types:

Convergence of DNR & DNI selectors!

Mostly from F6 collection

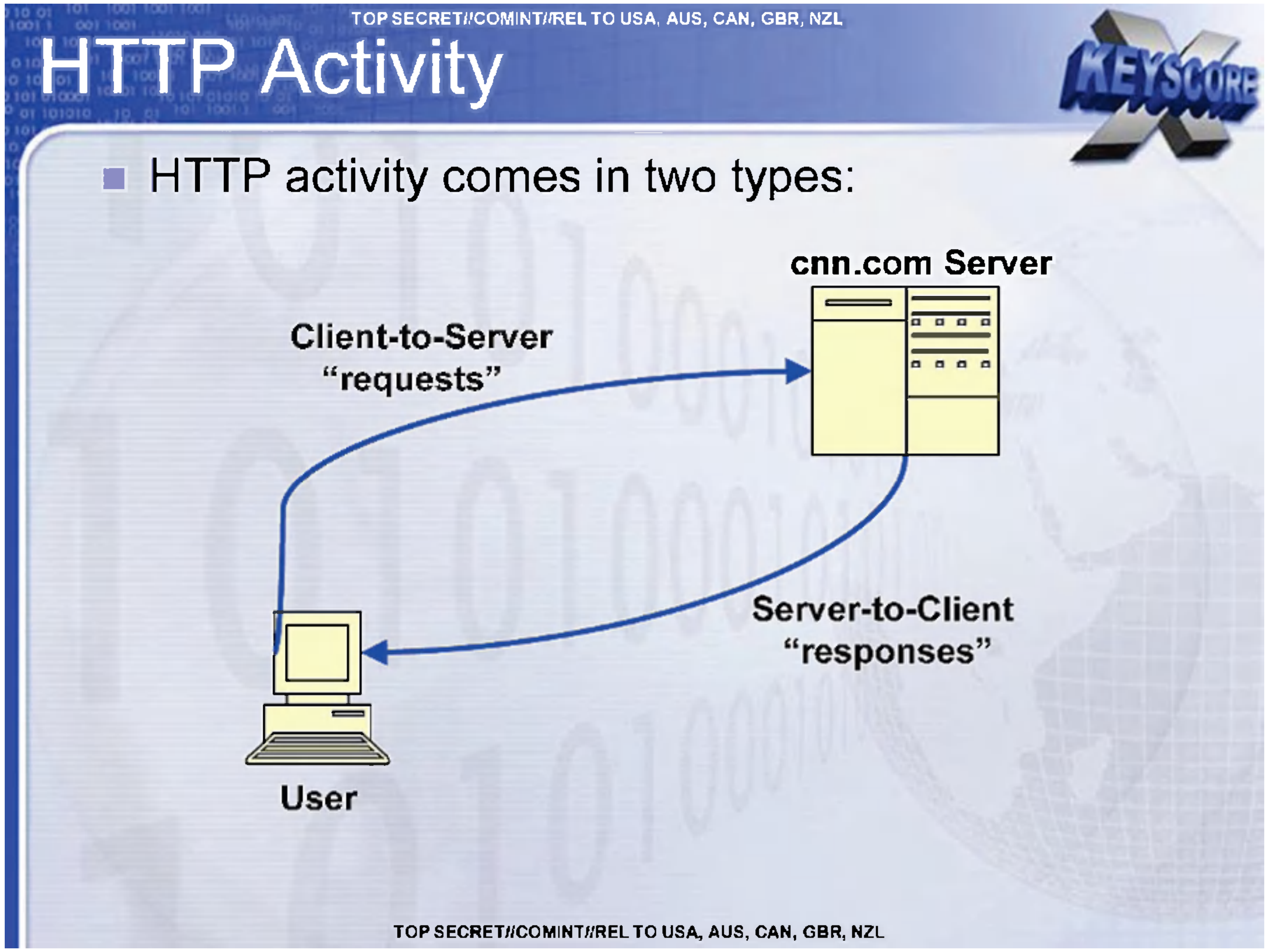
Most cases, needs to be "near" the infrastructure

Gateway

Internet

Looks like regular DNI but with "hints" that the source is a cell phone

Collection could be F6, FORNSAT, SSO, FISA



HTTP Activity

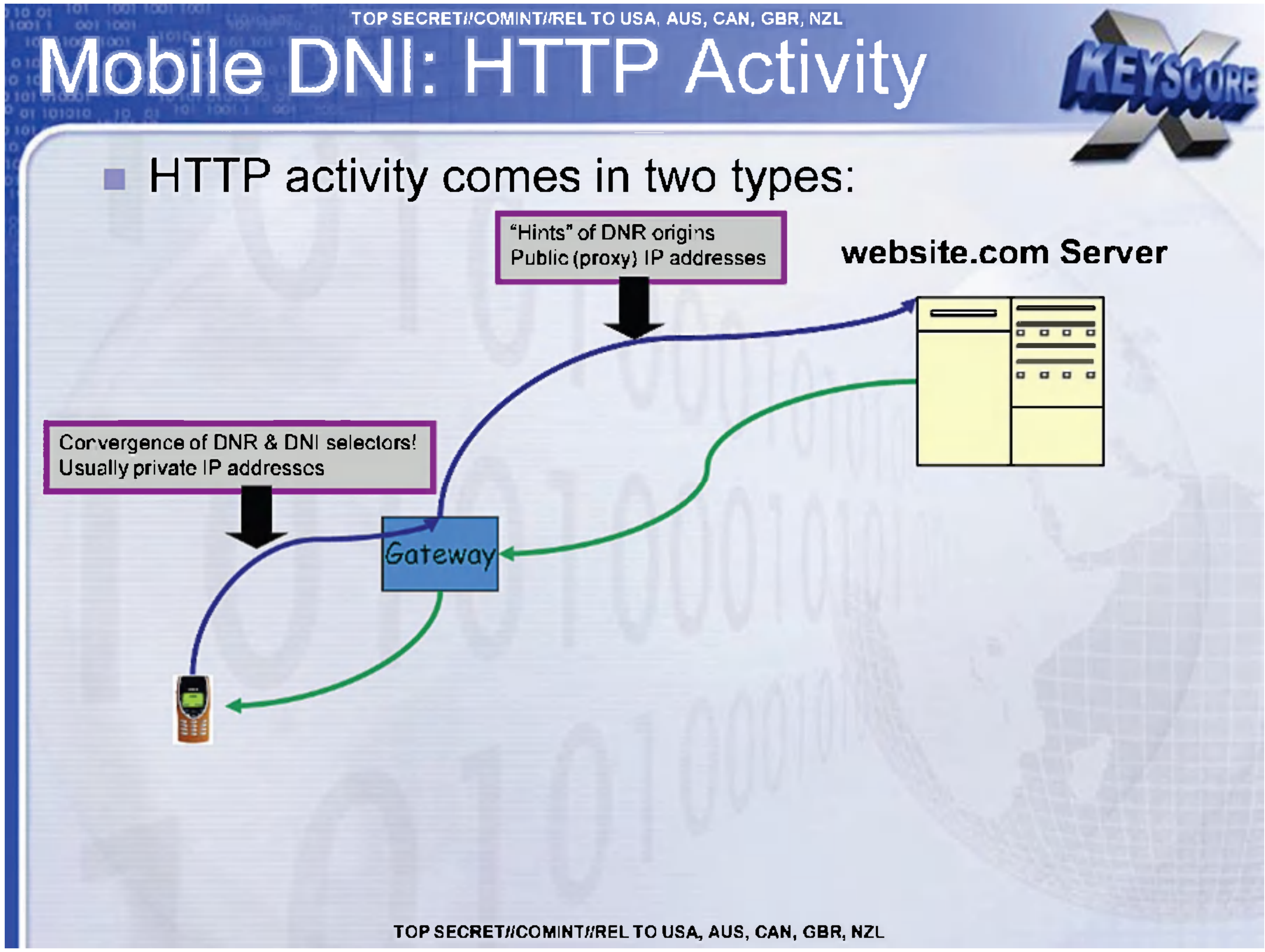
- HTTP activity comes in two types:

cnn.com Server

Client-to-Server
“requests”

Server-to-Client
“responses”

User

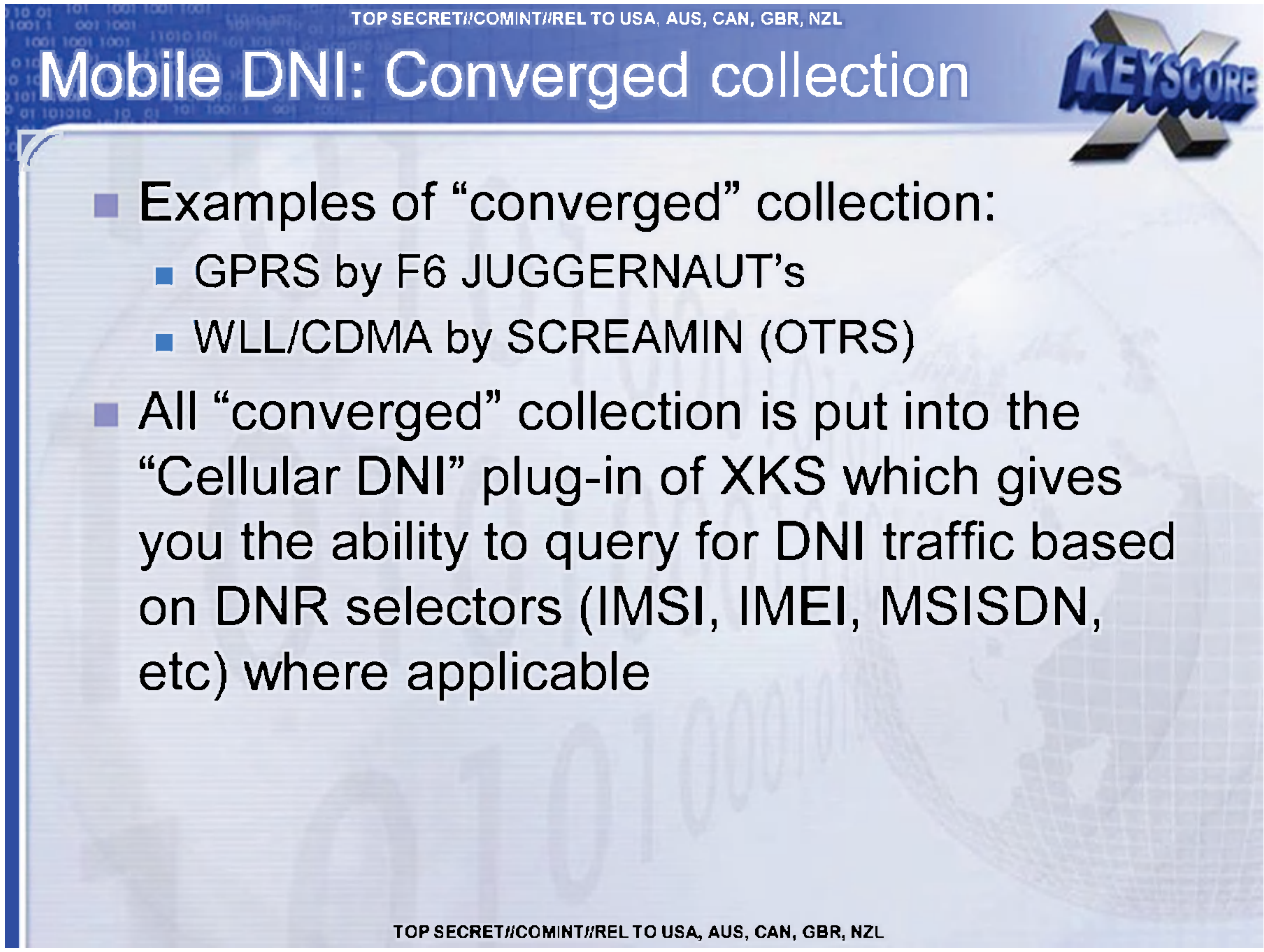


Mobile DNI: HTTP Activity

- HTTP activity comes in two types:

"Hints" of DNR origins
Public (proxy) IP addresses

Convergence of DNR & DNI selectors!
Usually private IP addresses

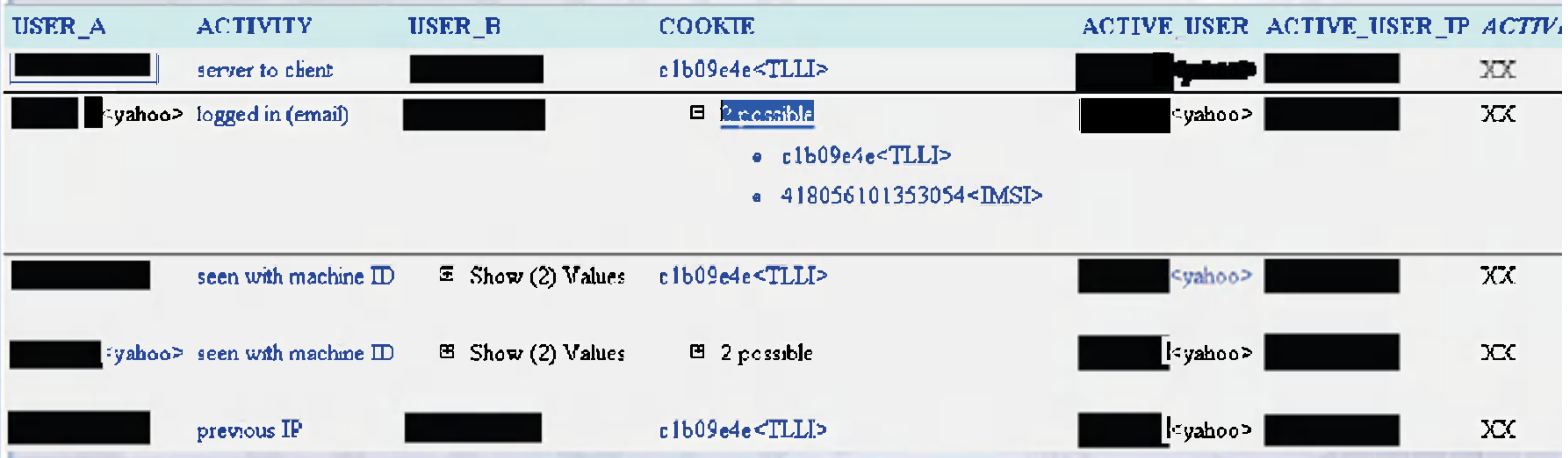


Mobile DNI: Converged collection

- Examples of "converged" collection:
  - GPRS by F6 JUGGERNAUT's
  - WLL/CDMA by SCREAMIN (OTRS)
- All "converged" collection is put into the "Cellular DNI" plug-in of XKS which gives you the ability to query for DNI traffic based on DNR selectors (IMSI, IMEI, MSISDN, etc) where applicable

Mobile DNI: Converged collection

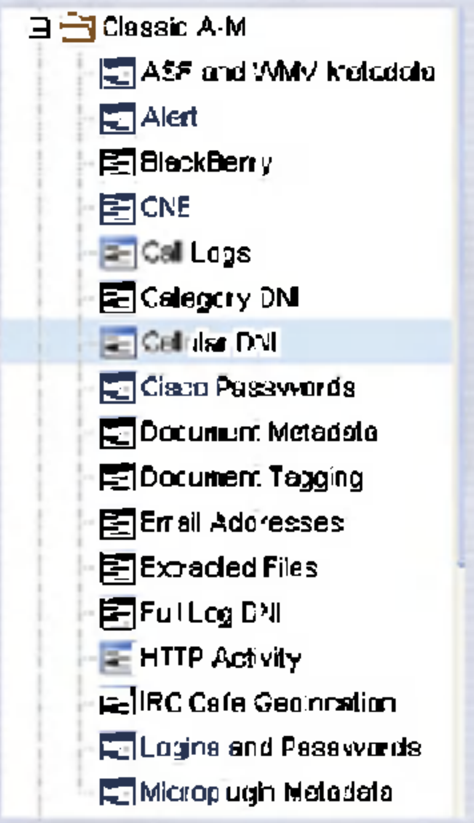
- DNR & DNI meta-data will be together:

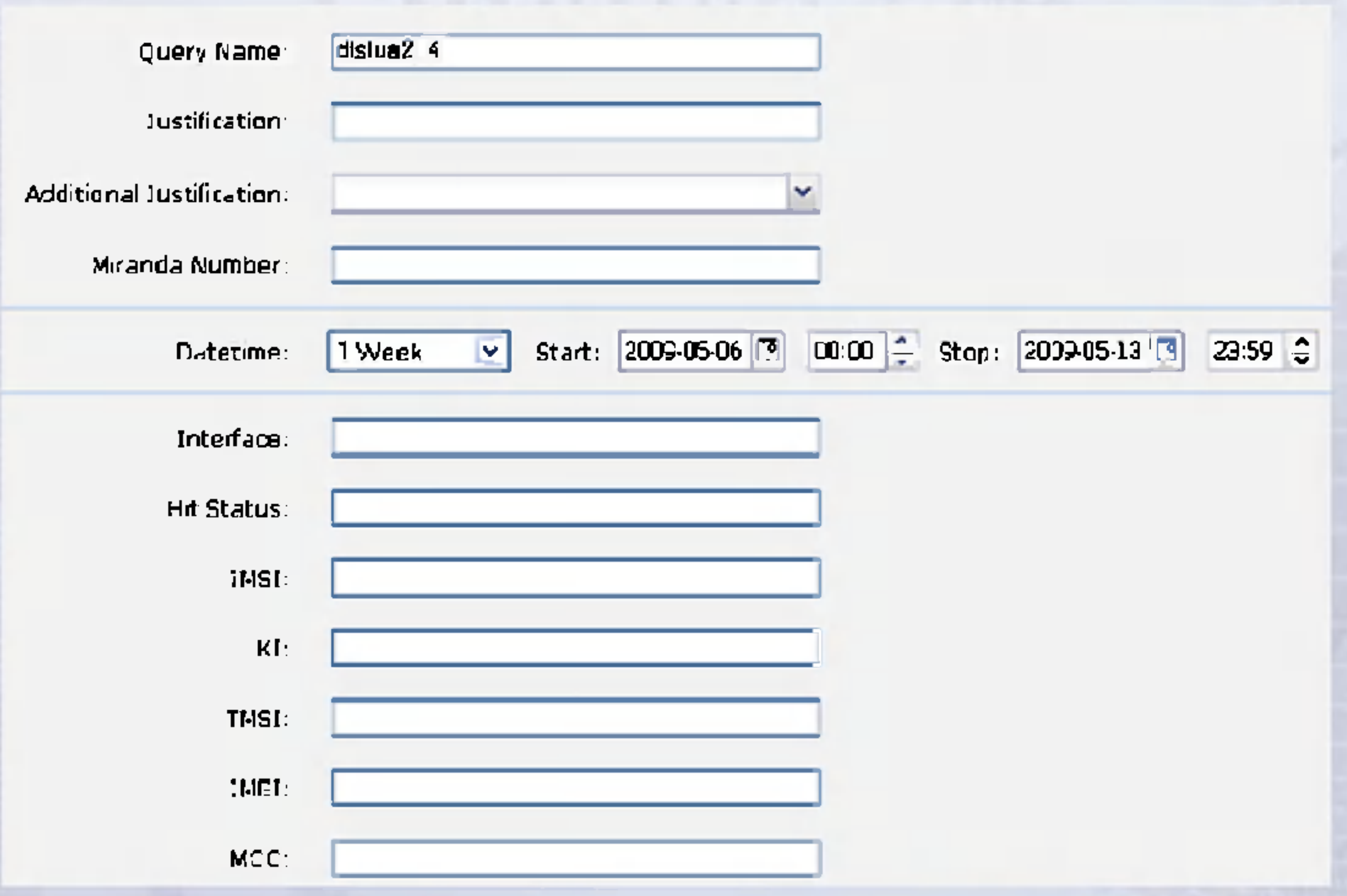


USER_A	ACTIVITY	USER_B	COOKIE	ACTIVE_USER	ACTIVE_USER_IP	ACTIV
[redacted]	server to client	[redacted]	c1b09e4e<TLLI>	[redacted]	[redacted]	XX
[redacted] [redacted]<yahoo>	logged in (email)	[redacted]	⊟ 2 possible • c1b09e4e<TLLI> • 418056101353054<IMSI>	[redacted]<yahoo>	[redacted]	XX
[redacted]	seen with machine ID	⊞ Show (2) Values	c1b09e4e<TLLI>	[redacted]<yahoo>	[redacted]	XX
[redacted]<yahoo>	seen with machine ID	⊞ Show (2) Values	⊞ 2 possible	[redacted]<yahoo>	[redacted]	XX
[redacted]	previous IP	[redacted]	c1b09e4e<TLLI>	[redacted]<yahoo>	[redacted]	XX

Mobile DNI: Converged collection

- X-KEYSCORE's Cellular DNI plug-in allows you to query on the DNR selectors for Persona Analysis

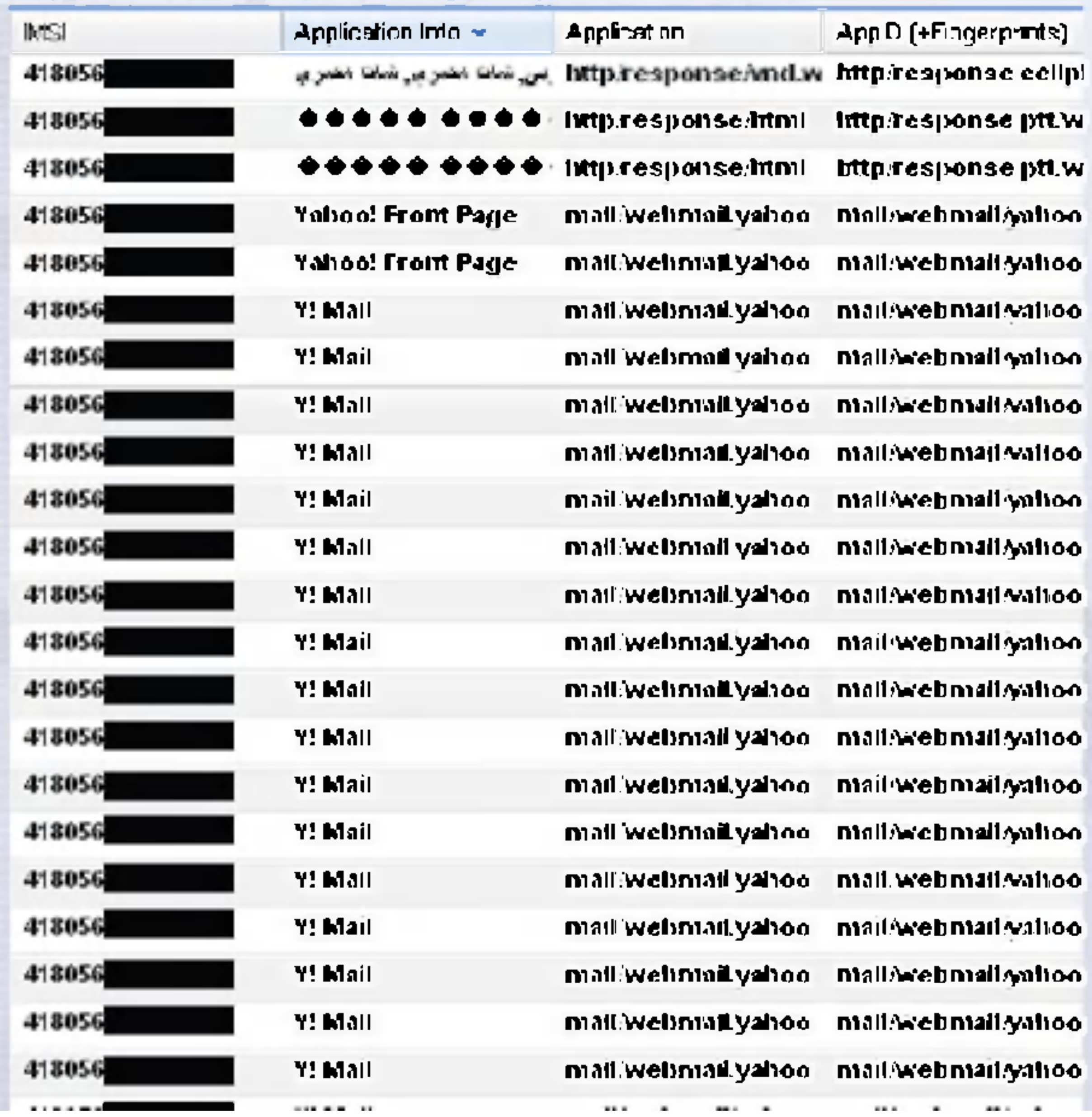




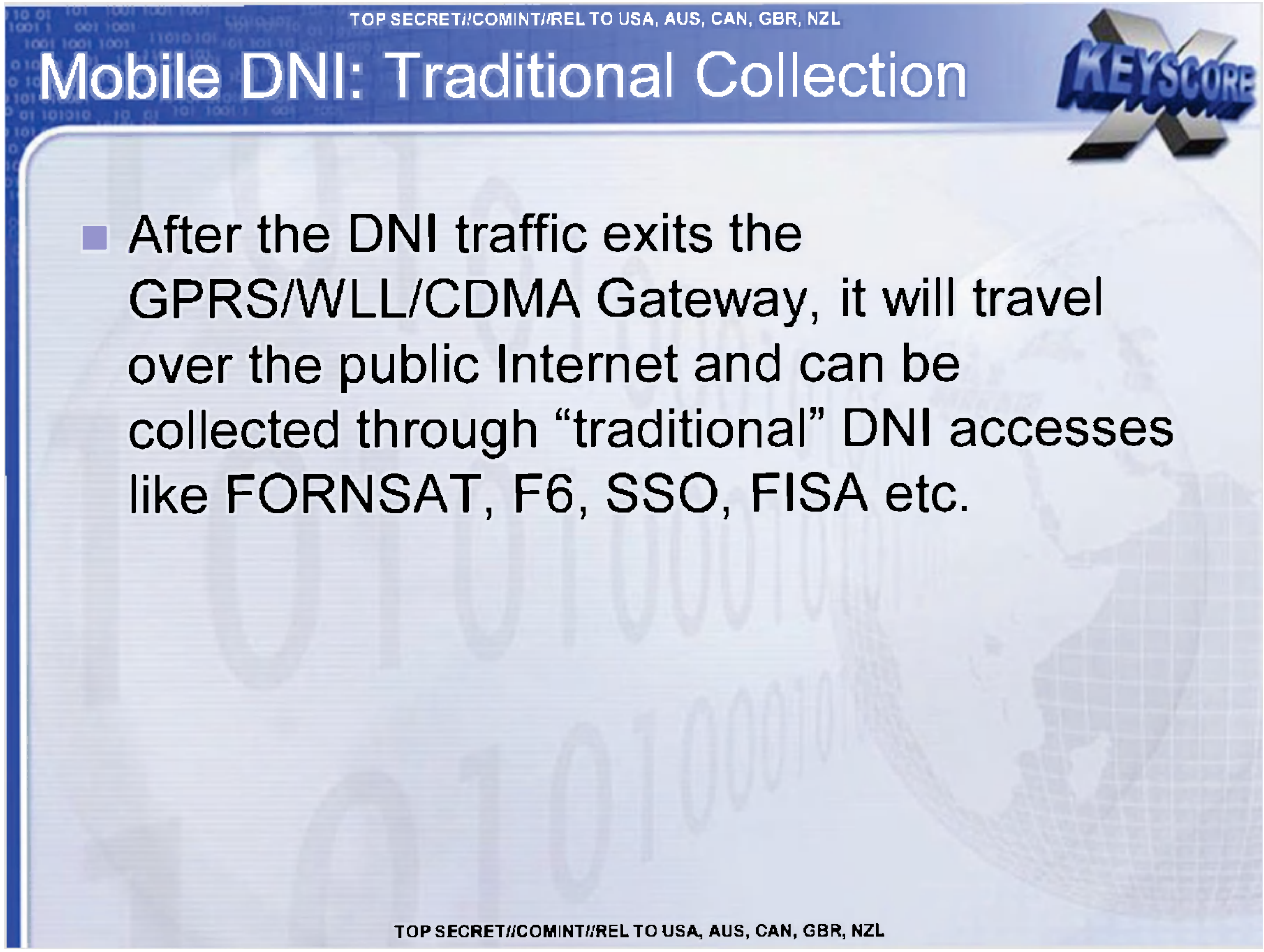
Query Name:	dislua2 4
Justification:	
Additional Justification:	
Miranda Number:	
Datetime:	1 Week Start: 2009-05-06 00:00 Stop: 2009-05-13 23:59
Interface:	
Hit Status:	
IMSI:	
KI:	
TMSI:	
IMEI:	
MCC:	

Mobile DNI: Converged collection

- By taking the IMSI we found in MARINA we can identify all of the DNI traffic (webmail, web-surfing etc.) that originated from that same mobile subscriber



IMSI	Application Info	Application	AppID (+Fingerprints)
418056[redacted]	[illegible]	http.response/and.w	http/response cellpl
418056[redacted]	●●●●●● ●●●●	http.response/html	http/response ptt.w
418056[redacted]	●●●●●● ●●●●	http.response/html	http/response ptt.w
418056[redacted]	Yahoo! Front Page	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Yahoo! Front Page	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail.webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo
418056[redacted]	Y! Mail	mail.webmail.yahoo	mail/webmail/yahoo

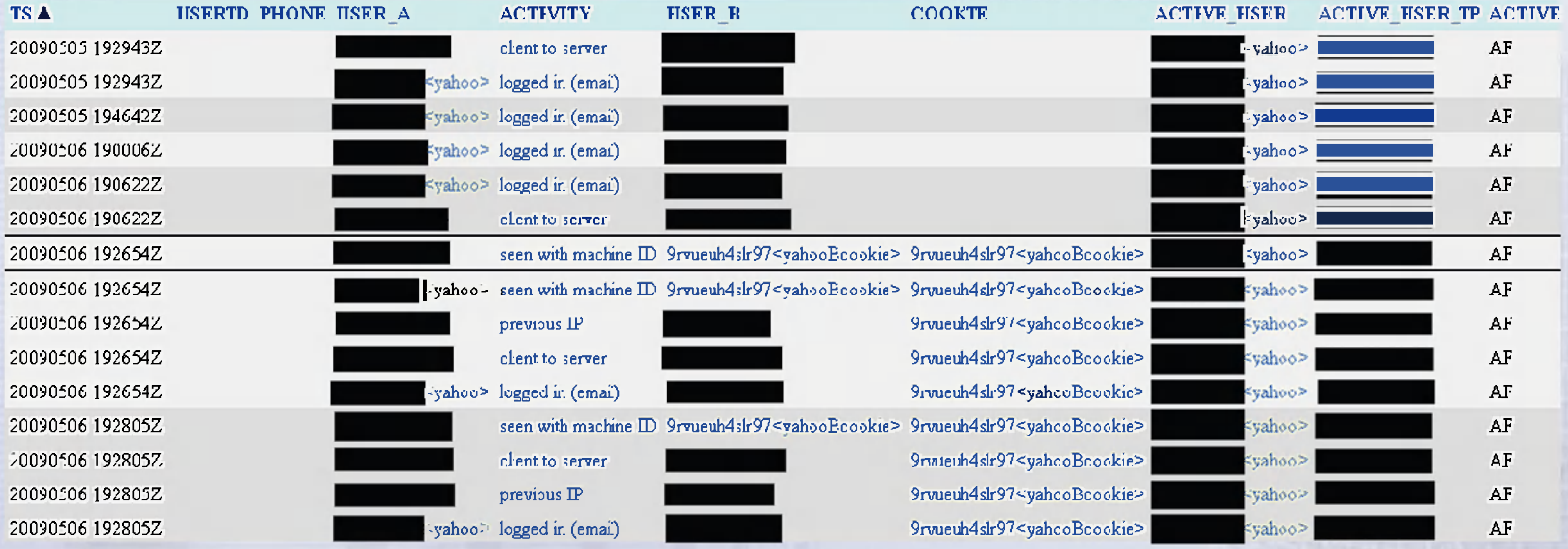


Mobile DNI: Traditional Collection

- After the DNI traffic exits the GPRS/WLL/CDMA Gateway, it will travel over the public Internet and can be collected through “traditional” DNI accesses like FORNSAT, F6, SSO, FISA etc.

Mobile DNI: Traditional Collection

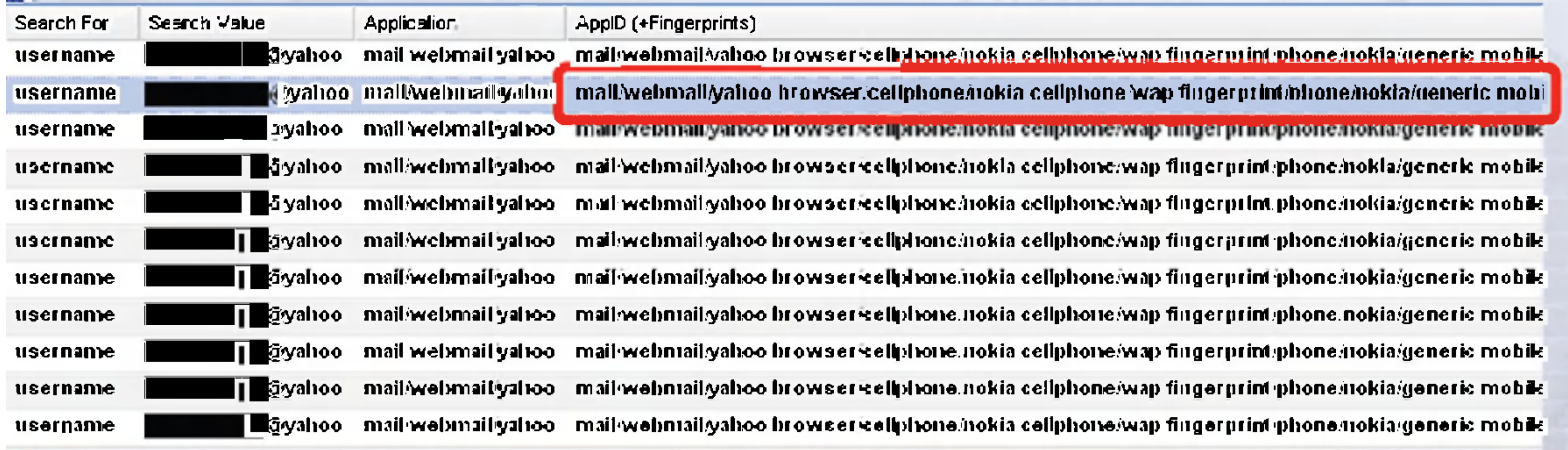
- Sometimes its difficult to tell if your target is using a cell phone to access his E-mail
- MARINA currently provides little or no “hints”



TS ▲	USERID	PHONE	USER_A	ACTIVITY	USER_B	COOKIE	ACTIVE_USER	ACTIVE_USER_IP	ACTIVE
20090505 192943Z			[redacted]	client to server	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090505 192943Z			[redacted] <yahoo>	logged in (email)	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090505 194642Z			[redacted] <yahoo>	logged in (email)	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090506 190006Z			[redacted] <yahoo>	logged in (email)	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090506 190622Z			[redacted] <yahoo>	logged in (email)	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090506 190622Z			[redacted]	client to server	[redacted]		[redacted] <yahoo>	[redacted]	AF
20090506 192654Z			[redacted]	seen with machine ID	9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192654Z			[redacted] <yahoo>	seen with machine ID	9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192654Z			[redacted]	previous IP	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192654Z			[redacted]	client to server	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192654Z			[redacted] <yahoo>	logged in (email)	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192805Z			[redacted]	seen with machine ID	9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192805Z			[redacted]	client to server	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192805Z			[redacted]	previous IP	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF
20090506 192805Z			[redacted] <yahoo>	logged in (email)	[redacted]	9rvueuh4slr97<yahooBcookie>	[redacted] <yahoo>	[redacted]	AF

Mobile DNI: Traditional Collection

- X-KEYSCORE "User Activity" provides *some* hints
- Note the fingerprint of browser/cellphone/nokia

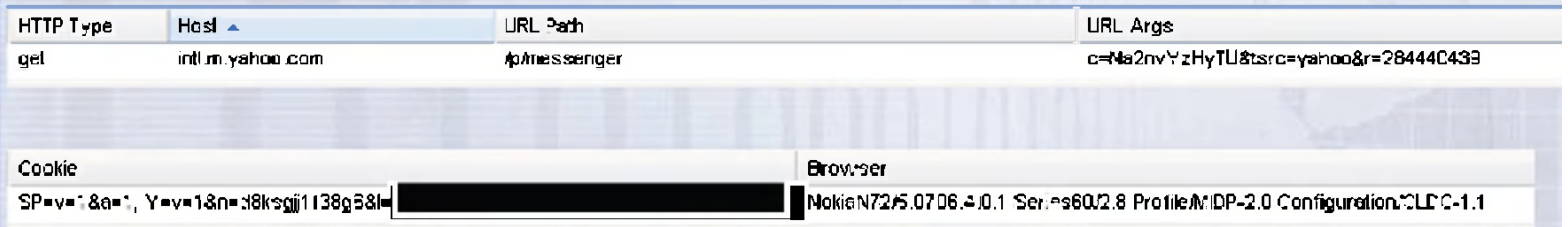


Search For	Search Value	Application	AppID (+Fingerprints)
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yaho	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobi
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil
username	[redacted]@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobil

Mobile DNI: Traditional Collection

- X-KEYSCORE "HTTP Activity" also provides some hints!
- Note the hostname of intl.m.yahoo.com and user agent of:

  NokiaN72/5.0706.4.0.1 Series60/2.8 Profile/MIDP-2.0 Configuration/CLDC-1.1

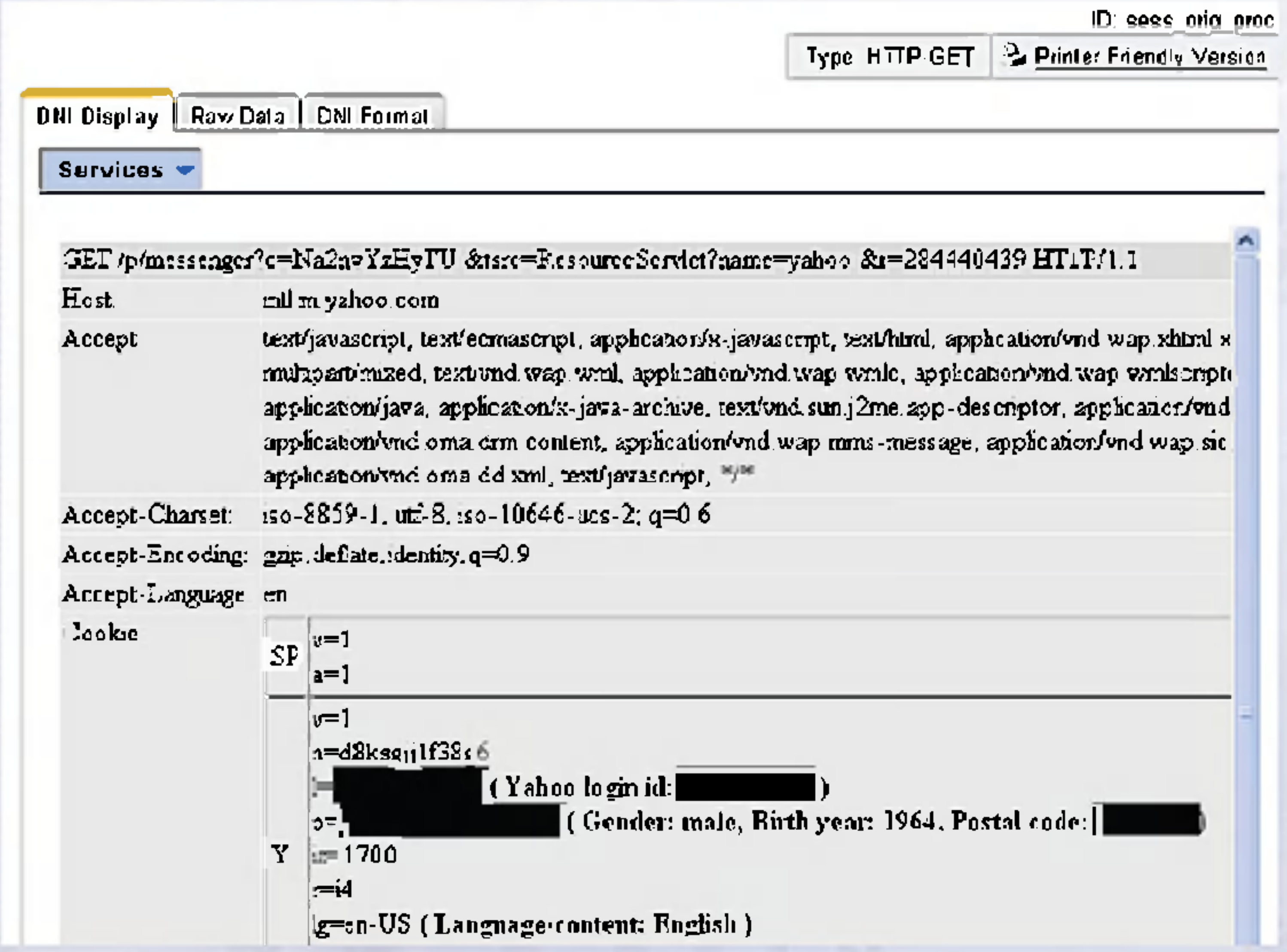


HTTP Type	Host ▲	URL Path	URL Args
get	intl.m.yahoo.com	/p/messenger	c=Na2nvYzHyTU&tsrc=yahoo&r=284440439

Cookie	Browser
SP=v=1&a=1, Y=v=1&n=d8ksgjj1138g38l=[redacted]	NokiaN72/5.0706.4.0.1 Series60/2.8 Profile/MIDP-2.0 Configuration/CLDC-1.1

Mobile DNI: Traditional Collection

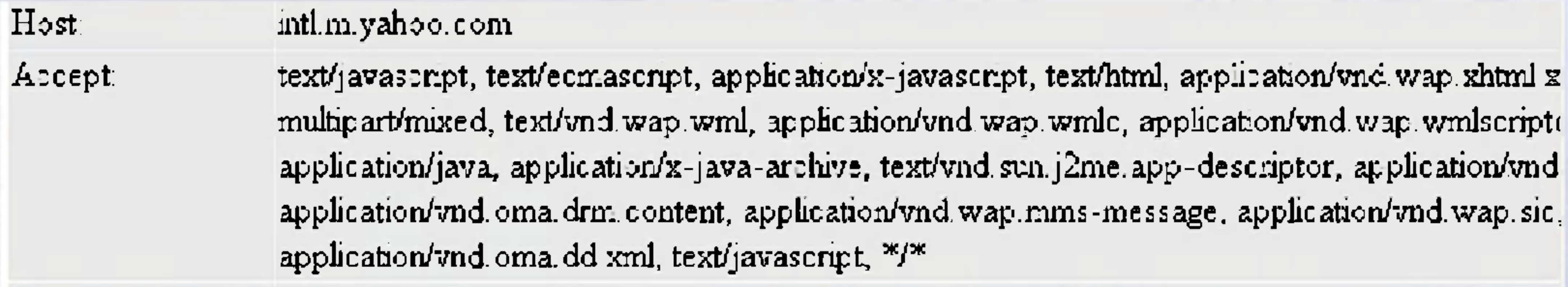
The content also provides some “hints”



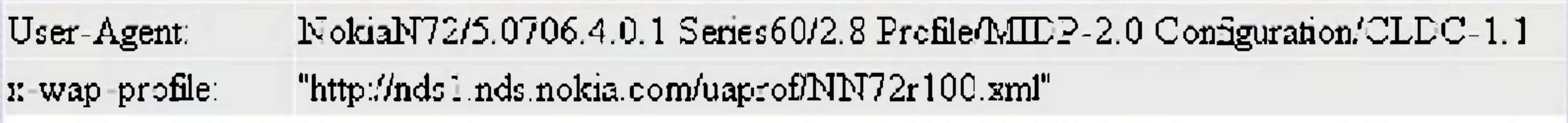
```
GET /p/messenger?c=Na2a=YzHyTU &tsrc=ResourceServlet?name=yahoo &r=284440439 HTTP/1.1
Host              mail.m.yahoo.com
Accept            text/javascript, text/ecmascript, application/x-javascript, text/html, application/vnd.wap.xhtml+x
                  multipart/mixed, text/vnd.wap.wml, application/vnd.wap.wmlc, application/vnd.wap.wmlscript
                  application/java, application/x-java-archive, text/vnd.sun.j2me.app-descriptor, application/vnd
                  application/vnd.oma.drm.content, application/vnd.wap.mms-message, application/vnd.wap.sic
                  application/vnd.oma.dd.xml, text/javascript, */*
Accept-Charset:   iso-8859-1, utf-8, iso-10646-ucs-2; q=0.6
Accept-Encoding:  gzip, deflate, identity, q=0.9
Accept-Language   en
Cookie       SP   v=1
                  a=1
             Y    v=1
                  n=d8ksqj1f38s6
                  l=[redacted]( Yahoo login id: [redacted] )
                  p=[redacted]( Gender: male, Birth year: 1964, Postal code: [redacted])
                  r=1700
                  i=i4
                  lg=en-US ( Language content: English )
```

HTTP Activity Examples

The content also provides some “hints”



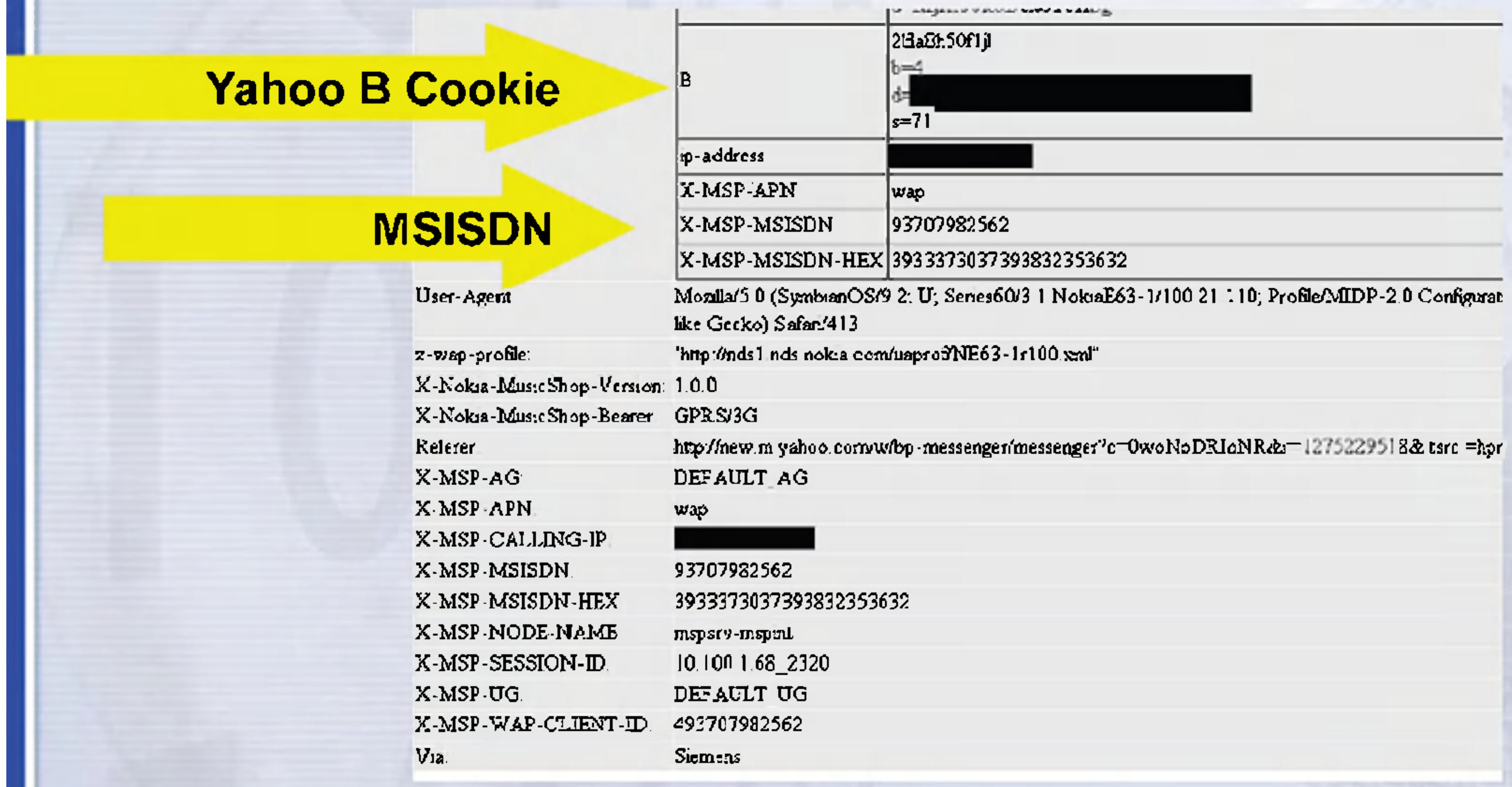
Host:	intl.m.yahoo.com
Accept:	text/javascript, text/ecmascript, application/x-javascript, text/html, application/vnd.wap.xhtml x multipart/mixed, text/vnd.wap.wml, application/vnd.wap.wmlc, application/vnd.wap.wmlscript application/java, application/x-java-archive, text/vnd.sun.j2me.app-descriptor, application/vnd application/vnd.oma.drm.content, application/vnd.wap.mms-message, application/vnd.wap.sic, application/vnd.oma.dd xml, text/javascript, */*



User-Agent:	NokiaN72/5.0706.4.0.1 Series60/2.8 Profile/MIDP-2.0 Configuration/CLDC-1.1
x-wap-profile:	"http://nds1.nds.nokia.com/uaprof/NN72r100.xml"

Mobile DNI: Traditional Collection

Sometimes there are even more “hints”



B	2l3a8t50f1jl
	b=4
	d=[redacted]
	s=71

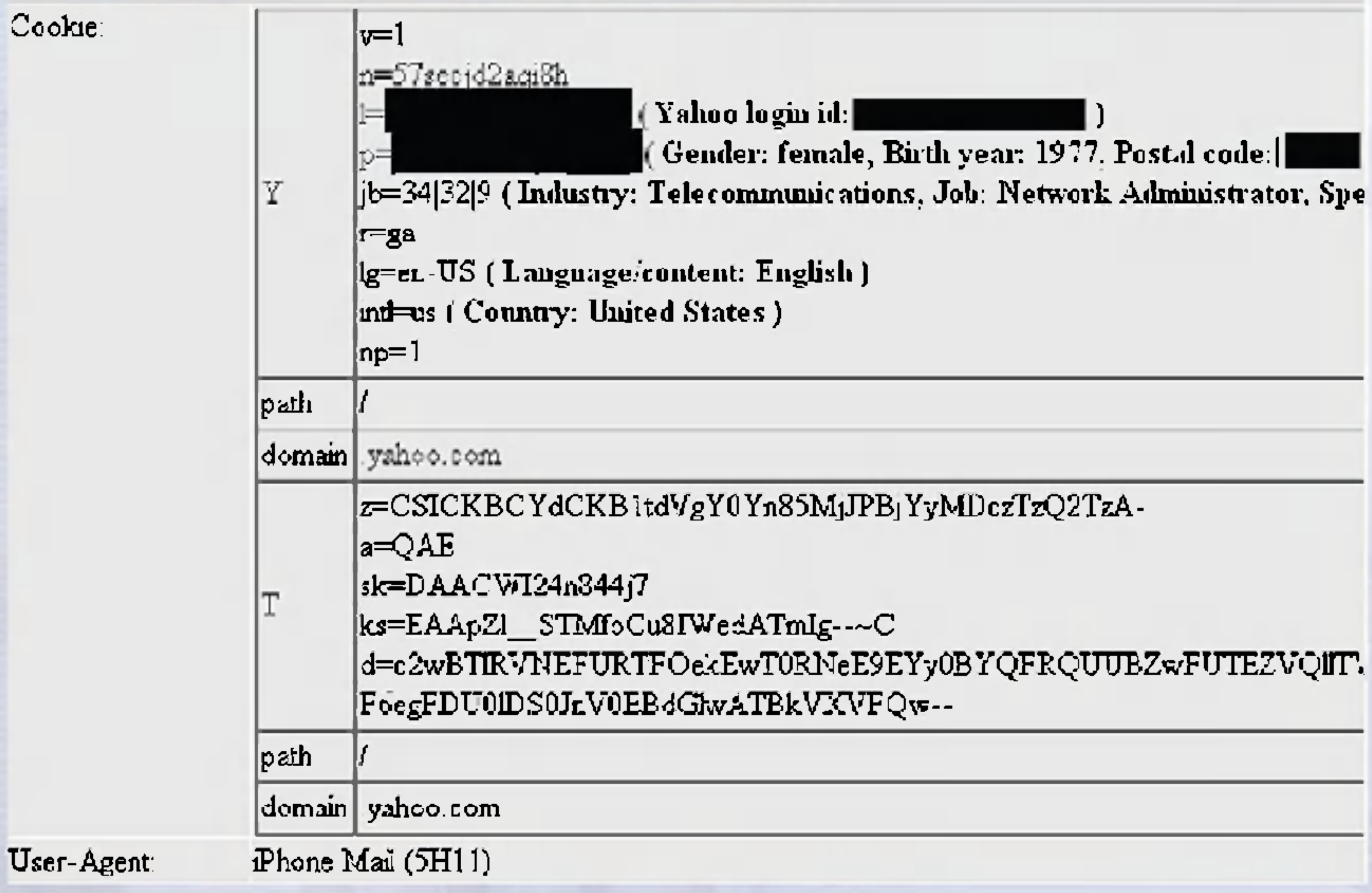
ip-address	[redacted]
X-MSP-APN	wap
X-MSP-MSISDN	93707982562
X-MSP-MSISDN-HEX	3933373037393832353632

User-Agent	Mozilla/5 0 (SymbianOS/9 2: U; Series60/3 1 NokiaE63-1/100 21 :10; Profile/MIDP-2.0 Configurat like Gecko) Safari/413
z-wap-profile:	"http://nds1 nds nokia com/uaprof/NE63-1r100.xml"
X-Nokia-MusicShop-Version:	1.0.0
X-Nokia-MusicShop-Bearer	GPRS/3G
Referer	http://new.m yahoo.com/w/bp-messenger/messenger?c=OwoNoDRIoNR&t=1275229518& tsrc =hpr
X-MSP-AG	DEFAULT_AG
X-MSP-APN	wap
X-MSP-CALLING-IP	[redacted]
X-MSP-MSISDN	93707982562
X-MSP-MSISDN-HEX	3933373037393832353632
X-MSP-NODE-NAME	mspsrv-msprnl
X-MSP-SESSION-ID	10.100 1.68_2320
X-MSP-UG	DEFAULT_UG
X-MSP-WAP-CLIENT-ID	493707982562
Via	Siemens

HTTP Activity Examples

IPhone Users!

Host	Browser
api.apple.mail.go.yahoo.com	iPhone Mail (5H11)



Cookie:	Y	v=1
		n=57sccjd2aqi8h
		l=[redacted] (Yahoo login id: [redacted])
		p=[redacted] (Gender: female, Birth year: 1977, Post.d code:| [redacted]
		jb=34|32|9 (Industry: Telecommunications, Job: Network Administrator, Spe
		r=ga
		lg=en-US (Language/content: English)
		intl=us (Country: United States)
		np=1

	path	/
	domain	.yahoo.com

	T	z=CSICKBCYdCKB1tdVgY0Yn85MjJPBjYyMDczTzQ2TzA-
		a=QAE
		sk=DAACWI24n844j7
		ks=EAApZl__STMfoCu8IWedATmIg--~C
		d=c2wBTlRVNEFURTFOekEwT0RNeE9EYy0BYQFRQUUBZwFUTEZVQllT
		FoegFDU0lDS0JzV0EBdGlwATBkVXVFQw--

	path	/
	domain	yahoo.com
User-Agent:	iPhone Mail (5H11)	