



Analyzing Mobile/Cellular DNI in XKEYSCORE

May 2009

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

DERIVED FROM: NSA/CSSM 1-52



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)



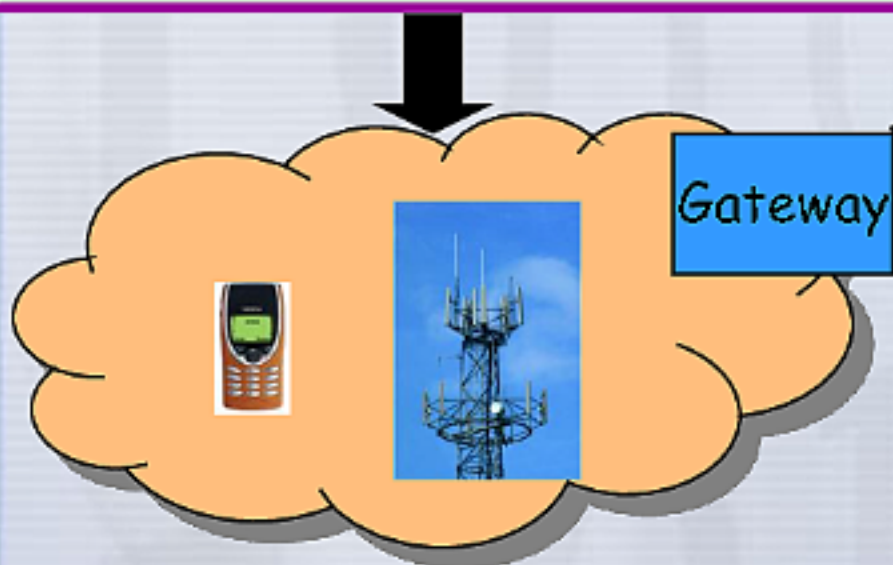
Mobile DNI

- 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



Internet

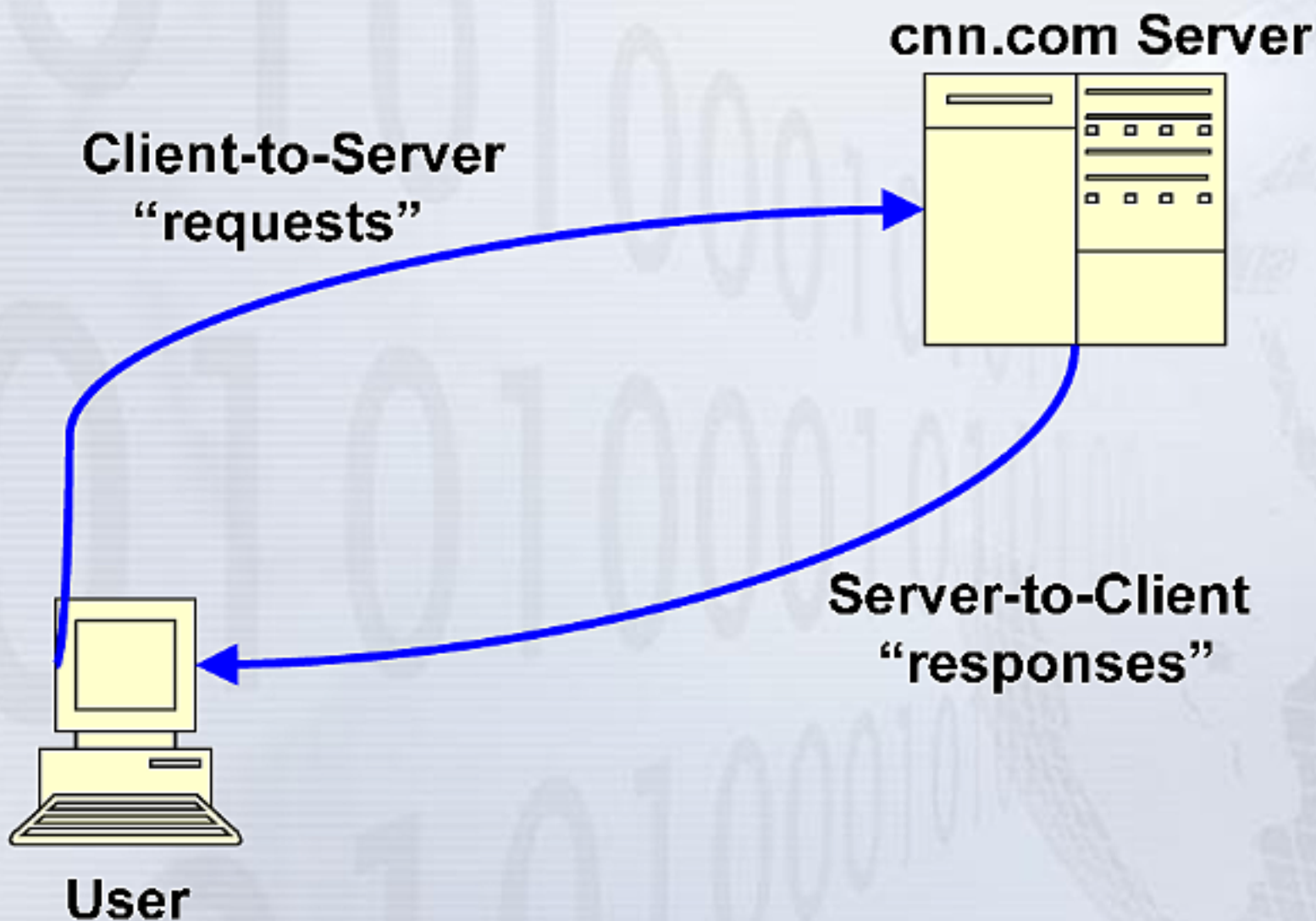
Looks like regular DNI but with "hints" that the source is a cell phone

Collection could be F6, FORNSAT, SSO, FISA



HTTP Activity

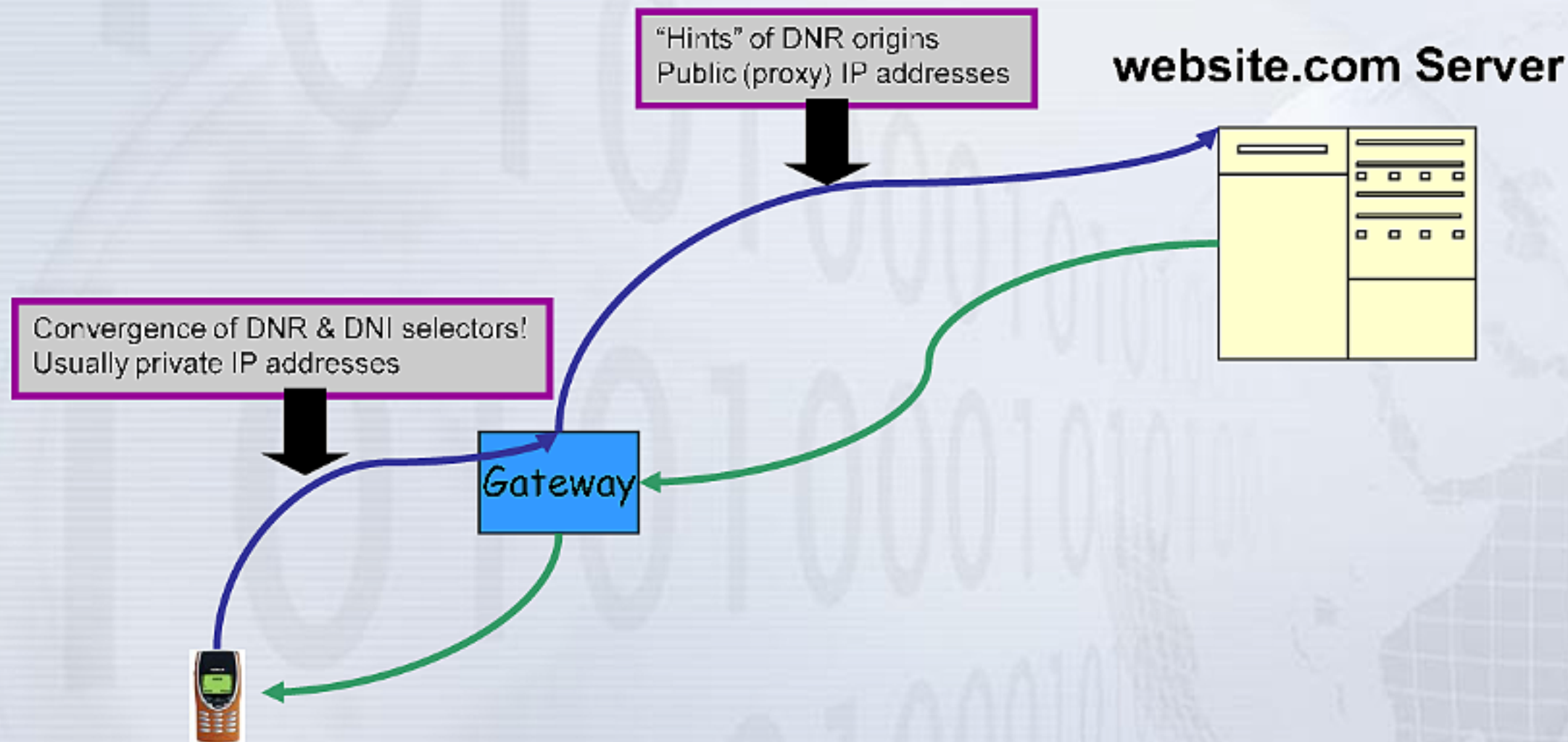
- HTTP activity comes in two types:





Mobile DNI: HTTP Activity

- HTTP activity comes in two types:





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

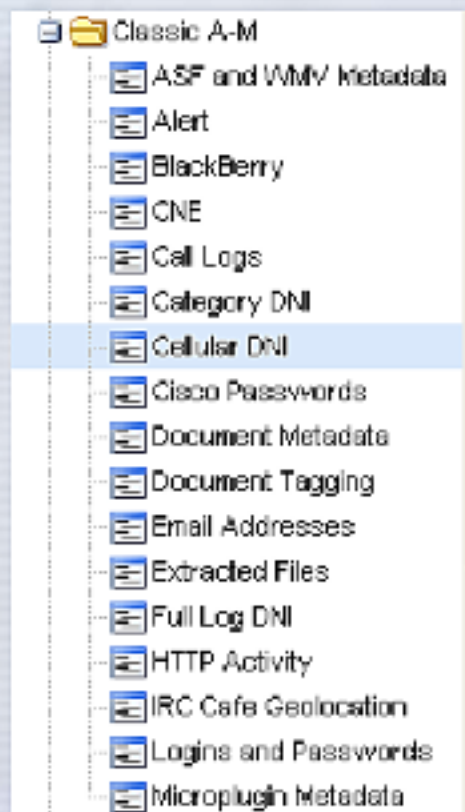
- DNR & DNI meta-data will be together:

USER_A	ACTIVITY	USER_B	COOKIE	ACTIVE_USER	ACTIVE_USER_IP	ACTIV...
[REDACTED]	server to client	[REDACTED]	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	XXX
[REDACTED] <yahoo>	logged in (email)	[REDACTED]	<input type="checkbox"/> 2 possible <ul style="list-style-type: none"> • c1b09e4e<TLLI> • 418056101353054<IMSI> 	[REDACTED] <yahoo>	[REDACTED]	XXX
[REDACTED]	seen with machine ID	<input type="checkbox"/> Show (2) Values	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	XXX
[REDACTED] <yahoo>	seen with machine ID	<input type="checkbox"/> Show (2) Values	<input type="checkbox"/> 2 possible	[REDACTED] <yahoo>	[REDACTED]	XXX
[REDACTED]	previous IP	[REDACTED]	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	XXX



Mobile DNI: Converged collection

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



Query Name:	<input type="text" value="distus2_4"/>
Justification:	<input type="text"/>
Additional Justification:	<input type="text" value="v"/>
Miranda Number:	<input type="text"/>
Datetime:	1 Week <input type="text"/> Start: 2009-05-06 <input type="text"/> 00:00 <input type="text"/> Stop: 2009-05-13 <input type="text"/> 23:59 <input type="text"/>
Interface:	<input type="text"/>
Hit Status:	<input type="text"/>
IMSI:	<input type="text"/>
KI:	<input type="text"/>
TMSI:	<input type="text"/>
IMEI:	<input type="text"/>
MCC:	<input type="text"/>



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<yahooEcookie>	9rvueuh4slr97<yahooBcookie>	[REDACTED]<yahoo>	[REDACTED]	AF
20090506 192654Z			[REDACTED]<yahoo>	seen with machine ID	9rvueuh4slr97<yahooEcookie>	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<yahooEcookie>	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	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	██████████@yahoo	mail/webmail/yahoo	mail/webmail/yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile



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=Na2nwYzHyTU&tsrc=yahoo&r=284440439

Cookie	Browser
SP=v=1&a=1; Y=v=1&n=d8kcgij1f38g6&l=	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”

ID: sess_orig_proc

Type: HTTP-GET [Printer Friendly Version](#)

DNI Display Raw Data DNI Format

Services ▾

```
GET /p/messenger?c=Na2awYzHyTU &tsrc=ResourceServlet?name=yahoo &r=284440439 HTTP/1.1
```

Host:	intl.m.yahoo.com				
Accept:	text/javascript, text/ecmascript, application/x-javascript, text/html, application/vnd.wap.xhtml+xml, 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				
Cooki	<table border="1"> <tr> <td>SP</td> <td>v=1 a=1</td> </tr> <tr> <td>Y</td> <td>v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED]) iz=1700 r=i4 lg=en-US (Language/content: English)</td> </tr> </table>	SP	v=1 a=1	Y	v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED]) iz=1700 r=i4 lg=en-US (Language/content: English)
SP	v=1 a=1				
Y	v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED]) iz=1700 r=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+xml, multipart/mixed, text/vnd.wap.wml, application/vnd.wap.wmlc, application/vnd.wap.wmlscriptc, 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”

Yahoo B Cookie

MSISDN

B	2lflaEh50f1jl 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 NokiaE63-1/100.21.110; Profile/MIDP-2.0 Configuration 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=0woNpDRlqNR&z=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	mssrv-mspnt
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

api.apple.mail.go.yahoo.com

Browser

iPhone Mail (5H11)

Cookie:

Y	v=1 n=57secjd2aqi8h l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: female, Birth year: 1977, Postal 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=EAApZI__STMfoCu8IWEdATmIg---C d=c2wBTIRVNEFURTF0ekEwT0RNeE9EYy0BYQFRQUUBZwFUTEZVQITV F6egFDU0IDS0JnV0EBdGhwATBkVXVFQw--
path	/
domain	yahoo.com

User-Agent:

iPhone Mail (5H11)