



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



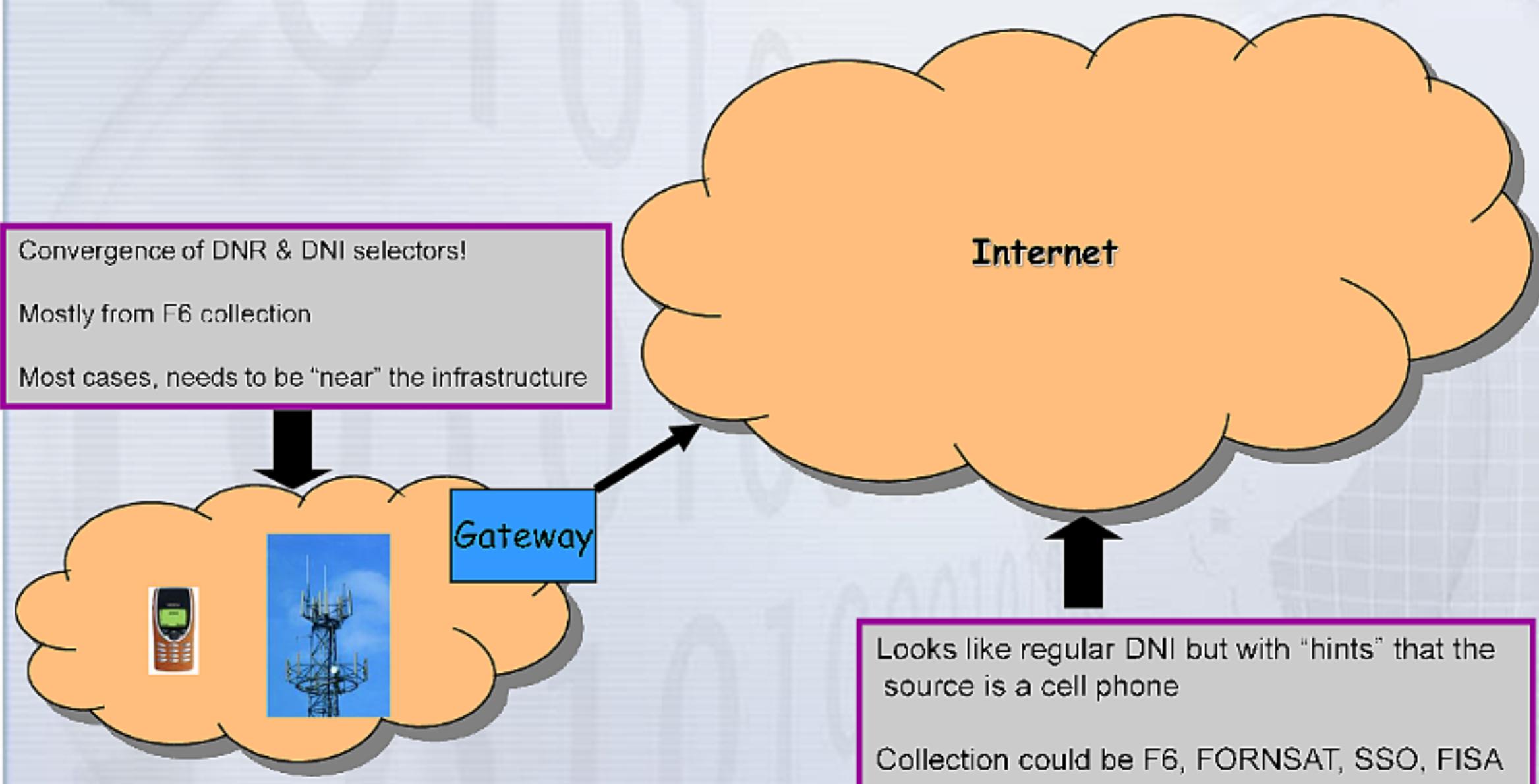
Mobile DNI

- 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

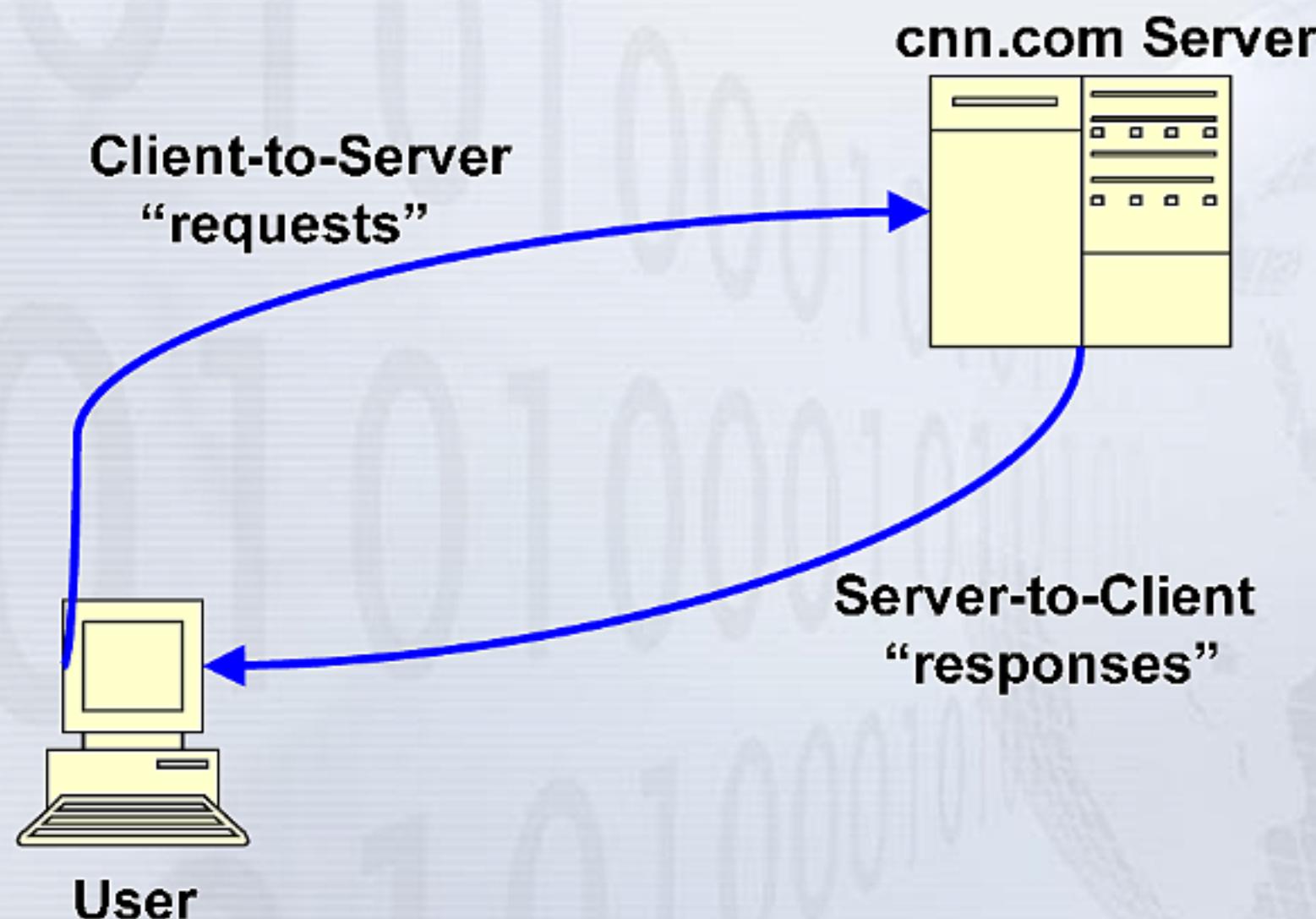
- Mobile DNI Collect comes in two main types:





HTTP Activity

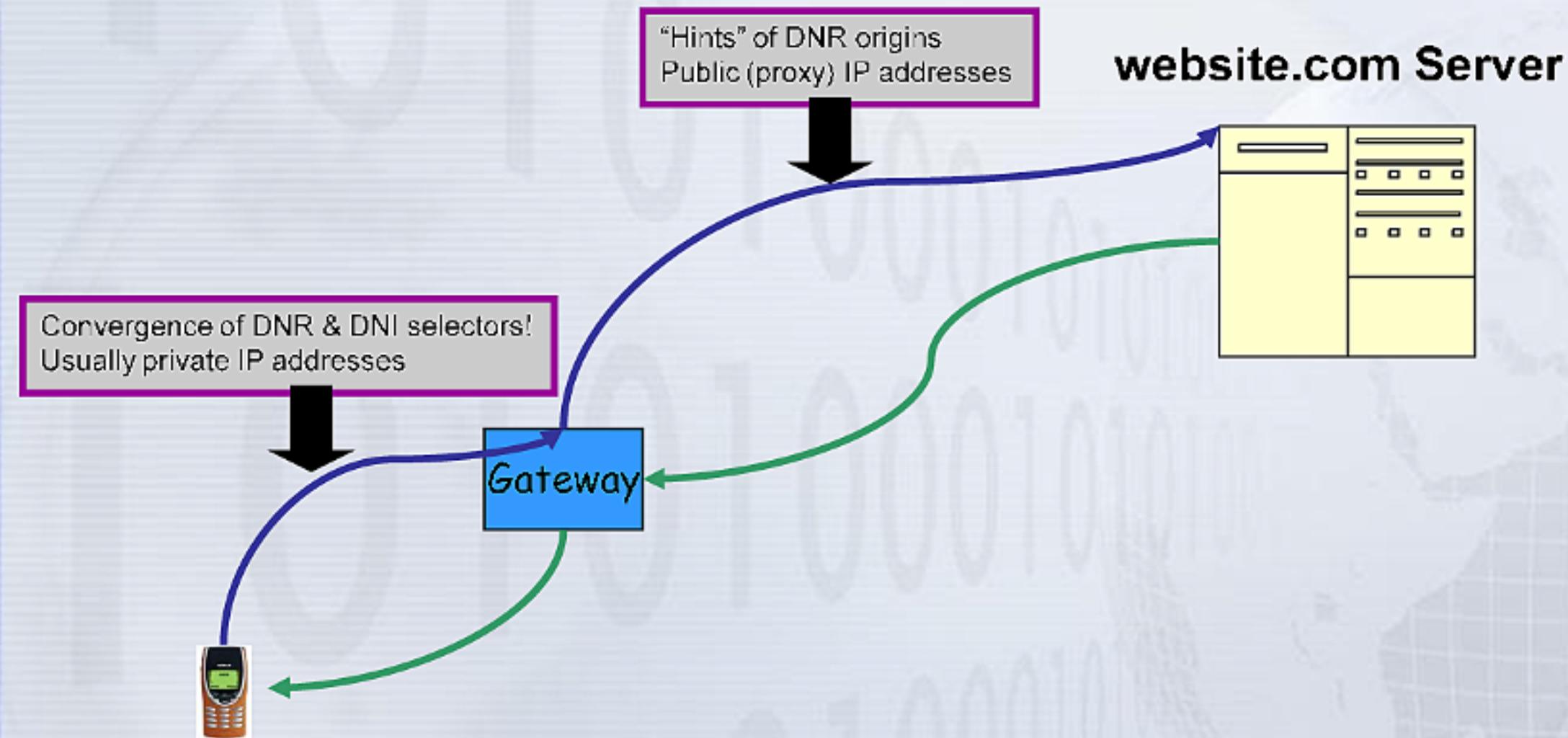
- HTTP activity comes in two types:





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	ACTIVI
[REDACTED]	server to client	[REDACTED]	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	DOC
[REDACTED] <yahoo>	logged in (email)	[REDACTED]	<input type="checkbox"/> 2 possible <ul style="list-style-type: none"> • c1b09e4e<TLLI> • 418056101353054<IMSI> 	[REDACTED] <yahoo>	[REDACTED]	DOC
[REDACTED]	seen with machine ID	<input checked="" type="checkbox"/> Show (2) Values	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	DOC
[REDACTED] <yahoo>	seen with machine ID	<input checked="" type="checkbox"/> Show (2) Values	<input type="checkbox"/> 2 possible	[REDACTED] <yahoo>	[REDACTED]	DOC
[REDACTED]	previous IP	[REDACTED]	c1b09e4e<TLLI>	[REDACTED] <yahoo>	[REDACTED]	DOC



Mobile DNI: Converged collection

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

The screenshot shows a software interface for querying mobile data. On the left is a sidebar menu with a tree view under 'Classic A-M'. The 'Cellular DNI' node is selected and highlighted in blue. Other nodes include 'ASF and Wmv Metadata', 'Alert', 'BlackBerry', 'CNE', 'Call Logs', 'Category DNI', 'Cisco Passwords', 'Document Metadata', 'Document Tagging', 'Email Addresses', 'Extracted Files', 'Full Log DNI', 'HTTP Activity', 'IRC Cafe Geolocation', 'Logins and Passwords', and 'Micropugin Metadata'. To the right is a main query form with various input fields:

- Query Name:
- Justification:
- Additional Justification:
- Miranda Number:
- Datetime: Start: Stop:
- 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



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_R	COOKIE	ACTIVE_USER	ACTIVE_USER_IP	ACTIVE
20090505 192943Z				client to server					AF
20090505 192943Z				<yahoo> logged in. (email)					AF
20090505 194642Z				<yahoo> logged in. (email)					AF
20090506 190006Z				<yahoo> logged in. (email)					AF
20090506 190622Z				<yahoo> logged in. (email)					AF
20090506 190622Z				client to server					AF
20090506 192654Z				seen with machine ID 9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahcoBcookie>				AF
20090506 192654Z				<yahoo> seen with machine ID 9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahcoBcookie>				AF
20090506 192654Z				previous IP		9rvueuh4slr97<yahcoBcookie>			AF
20090506 192654Z				client to server		9rvueuh4slr97<yahcoBcookie>			AF
20090506 192654Z				<yahoo> logged in. (email)		9rvueuh4slr97<yahcoBcookie>			AF
20090506 192805Z				seen with machine ID 9rvueuh4slr97<yahooBcookie>	9rvueuh4slr97<yahcoBcookie>				AF
20090506 192805Z				client to server		9rvueuh4slr97<yahcoBcookie>			AF
20090506 192805Z				previous IP		9rvueuh4slr97<yahcoBcookie>			AF
20090506 192805Z				<yahoo> logged in. (email)		9rvueuh4slr97<yahcoBcookie>			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 mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@yahoo	mail/webmail@yahoo	mail/webmail@yahoo browser/cellphone/nokia cellphone/wap fingerprint/phone/nokia/generic mobile
username	[REDACTED]@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=Na2nvYzHyTU&tsrc=yahoo&r=284440439

Cookie	Browser
SP=v=1&a=1; Y=v=1&n=d8lcsgjj1f38g68l= [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”

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

DNI Display Raw Data DNI Format

Services ▾

GET /p/messenger?c=Na2nvYzHyTU &src=ResourceServlet?name=yahoo &r=284440439 HTTP/1.1

Host	in1.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						
Cookie	<table border="1"><tr><td>SP</td><td>v=1 a=1</td></tr><tr><td></td><td>v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED])</td></tr><tr><td>Y</td><td>i=1700 r=i4 lg=en-US (Language/content: English)</td></tr></table>	SP	v=1 a=1		v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED])	Y	i=1700 r=i4 lg=en-US (Language/content: English)
SP	v=1 a=1						
	v=1 n=d8ksgjj1f38g6 l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: male, Birth year: 1964, Postal code: [REDACTED])						
Y	i=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.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”

Yahoo B Cookie

MSISDN

B	21fa3h50f1jl 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
x-wap-profile	"http://nds1.nds.nokia.com/uaprof?NE63-1r100.xml"
X-Nokia-Music-Shop-Version	1.0.0
X-Nokia-Music-Shop-Bearer	GPRS/3G
Referer	http://new.m.yahoo.com/w/bp-messenger/messenger?c=0woNpDRIqNR&r=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	mspdrv-mspmt
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:

	v=1 n=57secjd2aqi8h l=[REDACTED] (Yahoo login id: [REDACTED]) p=[REDACTED] (Gender: female, Birth year: 1977, Postal code: [REDACTED]) Y jb=34 32 9 (Industry: Telecommunications, Job: Network Administrator, Spe r=ga lg=en-US (Language/content: English) mt=us (Country: United States) np=1
path	/
domain	.yahoo.com
T	z=CSICKBCYdCKB1tdVgY0Yn85MjJPBjYyMDczTzQ2TzA- a=QAE sk=DAACWI24n844j7 ks=EAApZl__STMfoCu8IWedATmIg---C d=c2wBTRVNEFURTFoekEwT0RNneE9EYy0BYQFRQUUEZwFUTEZVQlITv F6egFDU01DS0JnV0EBdGhwATBkVXVFQw--
path	/
domain	.yahoo.com
User-Agent:	iPhone Mail (5H11)