



Phone Number Extractor

October 2009

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

DERIVED FROM: NSA/CSSM 1-52



Where are Phone Numbers seen in DNI?

- Phone Numbers are located in MANY parts of DNI traffic
 - “Contact Us” parts of web pages
 - Signature Lines
 - Address Books
 - “Leaked” as METADATA in Mobile HTTP traffic
 - Collected as converged data from GPRS/CDMA/WLL traffic
 - Collected in signaling of VOIP traffic

Phone Numbers in “Content”



- Looking inside the body of content, the Phone Number Extractor Looks for:
 - Telephony-related terms in the body of traffic and parses out any digits after that
 - Ex: “Tel:” or “Mobile” or “Fax” or “ ”
 - Note that all punctuation is removed.
 - i.e. (92) 928.555-555 becomes 92928555555



Phone Numbers on Websites

- Many times phone numbers are in the body of a website
 - “Contact-Us”
 - Craigslist-like websites listing items for sale
 - Forums, etc...
- Traffic can be TO or FROM Port 80

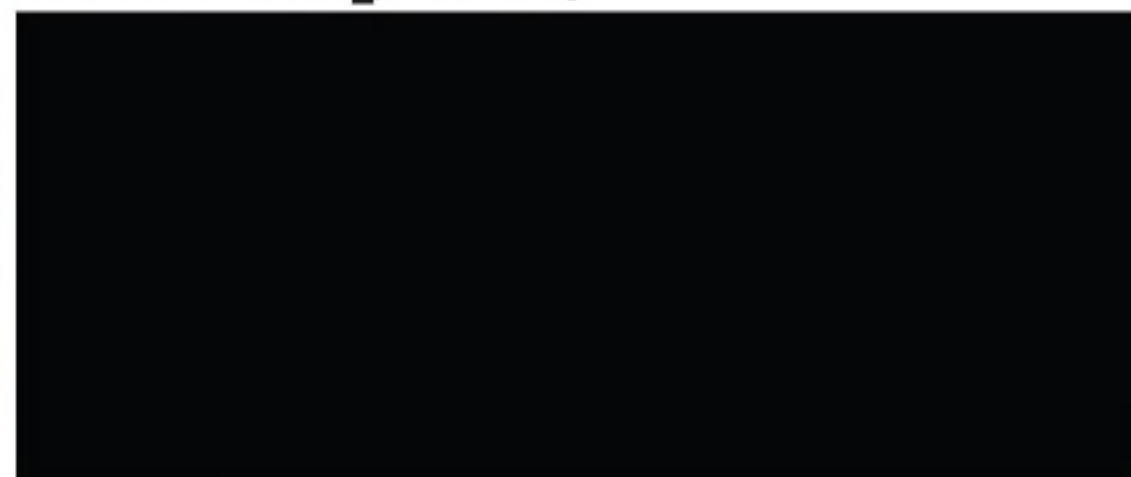


Normalization problems



- When a phone number is in the “body” of traffic, like a signature block or a “contact us” line on a webpage, it **doesn't have to be normalized**.
- XKS will extract the number exactly how it appears (minus punctuation and leading 0's) which can create problems.
- Look what happens to the '0' happen here:

Best Regards,



telephone



mobile



Phone Numbers on Websites

Search: Phone Number Extractor

Query Name:

Justification:

[Recent Justification](#)

Additional Justification:

Query

Miranda Number:

Datetime:

Start:

Stop

Phone Number:

Port:

Port:



Country:

Country:

Phone Numbers on Websites



Results

Phone Number	Highlights	Number Type	Fm Couhtr	Fm Port	To Country	To Port
[REDACTED]	 	telephone	US	80	IR	4179

Send to: Download Session | Mode: Full Sessio | Enter text to search

۸۷/۹/۲۱

Laptop PII

PII MMX- Ram 196-Hard 30GB-CDRom دارای باتری سالم و در حد نو و دارای ساخت ژاپن . . .
 Windows XP IBM 210000 سیستم عامل

تهران: تلفن: [REDACTED]

۸۷/۹/۲۱

آکبند با یک سال گارانتی ارتقاک Dell 500

Farsi: "TEL"

Phone Numbers in SIG Blocks



- Signature lines are SELECTOR-RICH environments (Emails, phones, names, titles, etc..)
 - Many SIG blocks have extraneous characters/numbers
 - XKS ignores dashes, parenthesis, etc..
 - XKS only parses out the numbers after



Phone Numbers in SIG Blocks

Search: Phone Number Extractor

Query Name:

Justification:

[Recent Justificatio](#)

Query

Additional Justification:

Miranda Number:

Datetime: Start: Stop:

Phone Number:

Phone Numbers in SIG Blocks



Results

State	ID	Phone Number	Highlights	Number Type	Fm Country	Fm Port	To Country	
	1640	[REDACTED]		fax	US	80	LB	2

Notation	From IP	To IP	From Port	To Port	Protocol
00000M0000	209 [REDACTED] (United States)	85 [REDACTED] (Lebanon)	80	28678	TCP

nts (11) Meta (11)

Send to: Download Session | Mode: Full Session | Options | Search: Enter text to search

deduct from the price? vo to be submitted by contractor taking into consideration any abo
 related to works already executed + submit separately offer for marble to be supplied by
 self

Ø I would like to change the ceramic tiles for the two other bathrooms. What is the
 m2 I need to buy and how much you will deduct from the price? Under assessment by contrac
 into consideration any abortive works related to works already executed.

Ø Master Bedroom bathroom, I would like to make it bigger and to cahnge the locati
 of the Toilet Seat + have doubel sinks.

As at this stage all end-user's requests are clear, we kindly ask you to give the releva
 maximum within a couple of days.

Thanks and Best regards

[REDACTED]
 Development Manager
 [REDACTED]
 Tel: [REDACTED]
 Fax: [REDACTED]

You can view our new projects on
 [REDACTED]

Phone Numbers in HTTP GETs



- HTTP GET Requests contain many “leaked” phone numbers from the providers
 - GPRS activity commonly seen with DNR selectors

Phone Numbers in HTTP GETs



Search: Phone Number Extractor

Query Name:

Justification:

[Recent Justif](#)

Additional Justification:

Query

Miranda Number:

Datetime: Start:

Phone Number:

Port:

Port:

Country:

Phone Numbers in HTTP GETs



Results

Phone Number	Highlights	Number Type	Fm Countr	Fm Port	To Country	To Port
[REDACTED]		telephone	IR	57875	US	80
[REDACTED]		telephone	IR	57875	US	80

```

Mode: Full Session | Options | Search Content: Enter text to search
AUTO FORMATTER: app_id= unknown/port80/http_www Viewer= ASCII format

2.2.1 Profile/MIDP-2.0 Configuration/CLDC-1.1
accept-application: x-wap-application:wml.ua,x-wap-application:mms.ua
Content-length: 0
Via: WTP/1.1 twwap7.mtnirancell.ir (Nokia_WAP_Gateway 4.1/CD20/4.1.113)
X-Network-info: GPRS, [REDACTED] unsecured
X-Nokia-msisdn: [REDACTED]
X-Nokia-CONNECTION_MODE: TCP
X-Nokia-BEARER: GPRS
X-Nokia-GATEWAY_ID: NWG/4.1/Build113
x-nokia.wia.accept.original: application/xhtml+xml,text/html,application/vnd.w
Connection: close

```



Phone Numbers in HTTP POSTs

- Many times a phone number is submitted in an HTTP “POST” session
 - If a person fills in a form or replies to an email, the information in the body will be collected

Phone Numbers in HTTP POSTs



Fields ▾ Advanced Features ▾ Show Hidden Search Fields Clear Search Values Reload Last Search Values

Search: Phone Number Extractor

Query Name:

Justification:

[Recent Justifications](#)

Additional Justification:

Miranda Number:

Datetime: Start: Stop:

Phone Number:

Port:

Port:

Country:

Query



Phone Numbers in HTTP POSTs

Phone Number	Highlights	Number Type	Fm Countr	Fm Port	To Country	To Port	S
[REDACTED]		mobile	IR	3511	US	80	C

Results

From IP	To IP	From Port	To Port	Protocol	Length
92. [REDACTED] (Iran)	209. [REDACTED] (United States)	3511	80	TCP	13476

```

ments (2)
Download Session | Mode: Full Session | Options | Search Content: Enter text to search
POST /mail/?ui=2&ik=367371b1d8&at=xn3j30ni9gjyfueofsjzpxq6ubnbom&view=up&act=sd&jsid=plrevt7
Host: mail.google.com
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.3) Gecko/20090824 Firef
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: fa
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded; charset=
Referer: http://mail.google.com/mail/?ui=2&view=js&name=vmMKYU.en.&am=!Hln0yYGL2
Cookie: S=gmail=D8-U_bh5VJXMxnqp5vUunA:gmproxy=Q5n_Xd7qetw-95daj8ynMA; GX=DQAAAHoAAABcX4IyR%
Pragma: no-cache
Cache-Control: no-cache

to=[REDACTED]&cc=&bcc=&subject=Re%3A%2

```

No Phone Number in the POST Metadata



Phone Numbers in HTTP POSTs

Results

Phone Number	Highlights	Number Type	Fm Countr	Fm Port	To Country	To Port	S
[REDACTED]		mobile	IR	3511	US	80	C

The phone number was in the body of the POST (i.e. a reply to an email)

Session | Header (3) | Meta (10) | Attachments (2)

Formatter: AUTO | Send to: Download Session | Mode: [REDACTED]

Quick Clicks

- Session
- Attachments
 - web
 - html
 - unknown_152.x-www-form-t
 - unknown
 - text
 - document_body.email_0.txt
- One-Click Searches
 - Find opposite side of session
 - 92 [REDACTED] 3511 ->
 - 209 [REDACTED] : 80
 - Find traffic on
 - 209 [REDACTED]

unknown_152. [REDACTED]

Virus scan results

Using HTML formatter

2009/10/3 [REDACTED]

Thanks Dear Hubert,

I tried to call from Here, But is very Difficult to Call UK from Here.

Could pls. Give my Contact or Skpye to Him to Call me urgently:

Skype: [REDACTED]

Mobile: [REDACTED]



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

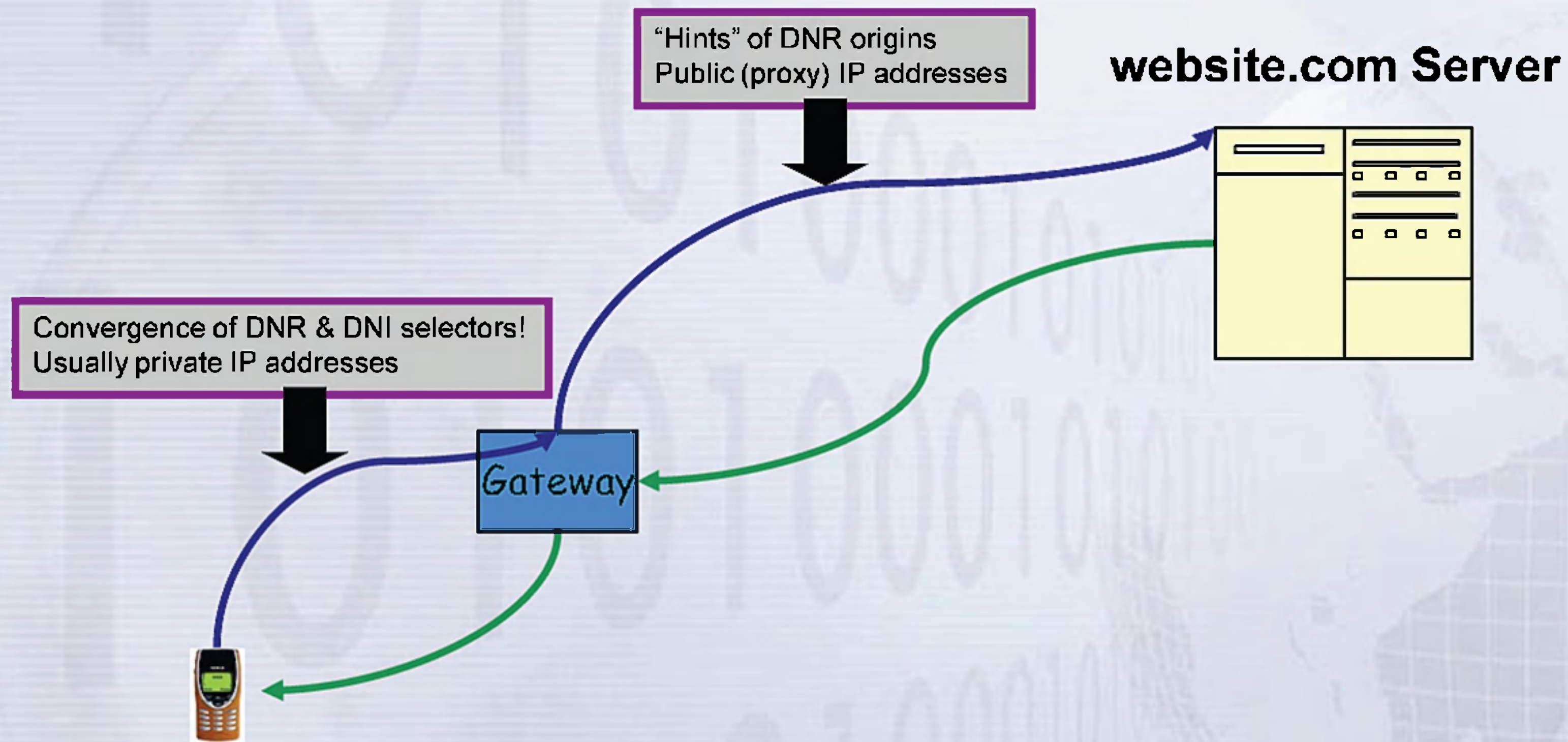


Looks like regular DNI but with "hints" that the source is a cell phone
Collection could be F6, FORNSAT, SSO, FISA



Mobile DNI: HTTP Activity

- HTTP activity comes in two types:





Phone Numbers From Converged Collection

USER_A	ACTIVITY	USER_B	COOKIE	ACTIVE_USER	ACTIVE_USER
<yahoo>	seen with machine ID	<IMSI>	<IMSI>	<yahoo>	202

Phone Number:

Results

Datetime	Datetime End	Phone Number	Number Type	Country Code	Area
2009-10-05 17:12:59	2009-10-05 17:12:59		imsi	pk	Mobilink
2009-10-05 17:13:49	2009-10-05 17:13:55		imsi	pk	Mobilink
2009-10-05 17:13:11	2009-10-05 17:13:11		imsi	pk	Mobilink
2009-10-05 17:16:07	2009-10-05 17:16:07		imsi	pk	Mobilink
2009-10-05 17:15:16	2009-10-05 17:15:18		imsi	pk	Mobilink
2009-10-05 17:16:17	2009-10-05 17:16:17		imsi	pk	Mobilink
2009-10-05 17:18:28	2009-10-05 17:18:28		imsi	pk	Mobilink
2009-10-05 17:18:28	2009-10-05 17:18:28		imsi	pk	Mobilink
2009-10-05 17:19:11	2009-10-05 17:19:11		imsi	pk	Mobilink