Monitoring Government Surveillance Capabilities by means of Transparency tools

Riccardo Coluccini @ORARiccardo
Fabio Pietrosanti @fpietrosanti

e-Privacy XXI 23-24 Giugno 2017

ITALY

Watch How Government Spyware Infects a Computer in This Leaked Demo Video

EFF and ACLU Expose Government's Secret Stingray Use in Wisconsin Case

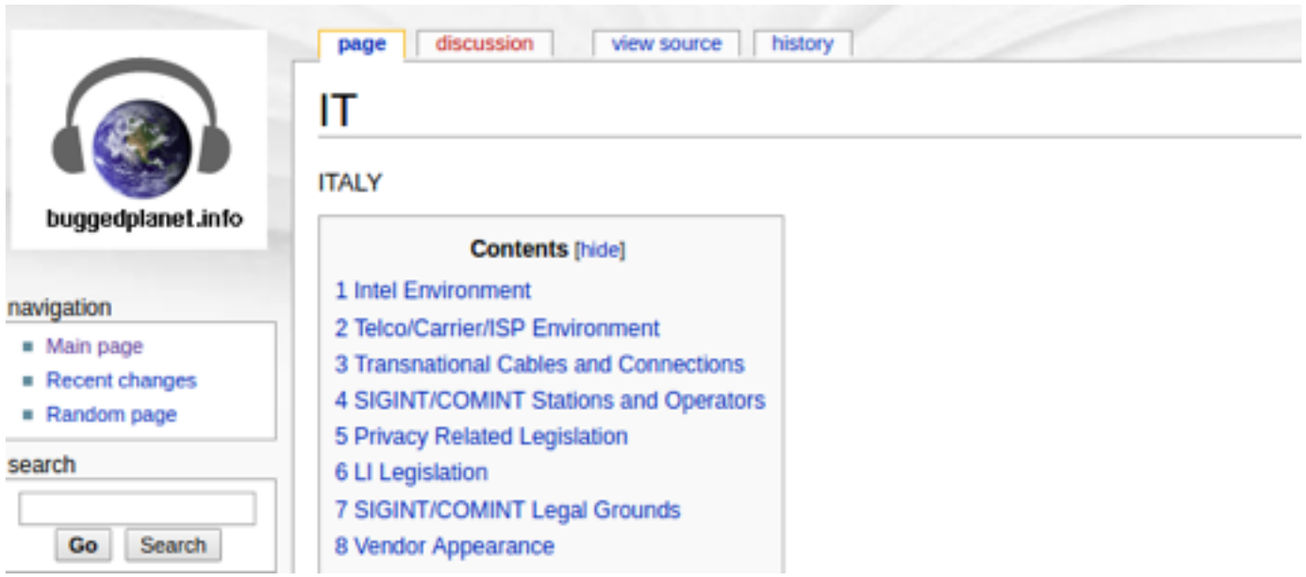
Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families

World's largest internet exchange sues Germany over mass surveillance

Outline

- OSINT
- Early findings
- Peculiar cases (IMSI-catcher, RCS,…)
- What’s next?

OSINT

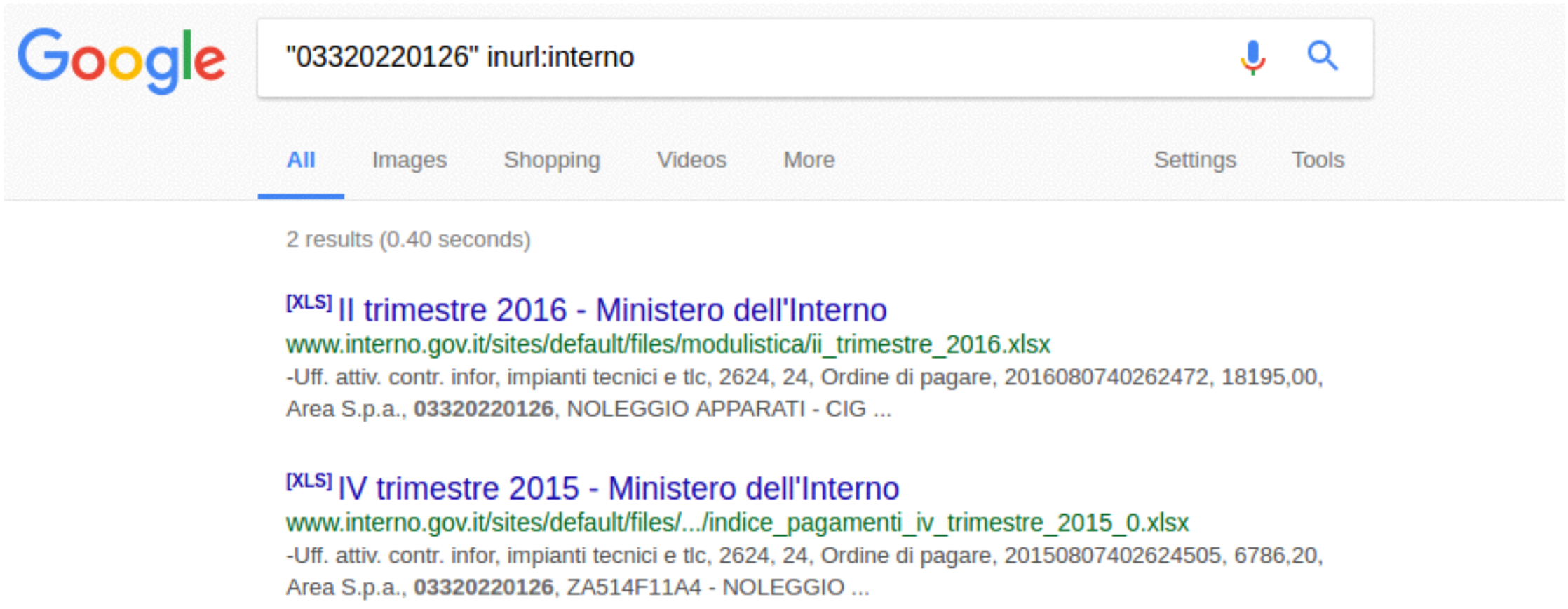


buggedplanet.info

sii.transparencytoolkit.org

OSINT

- Advanced Google Search



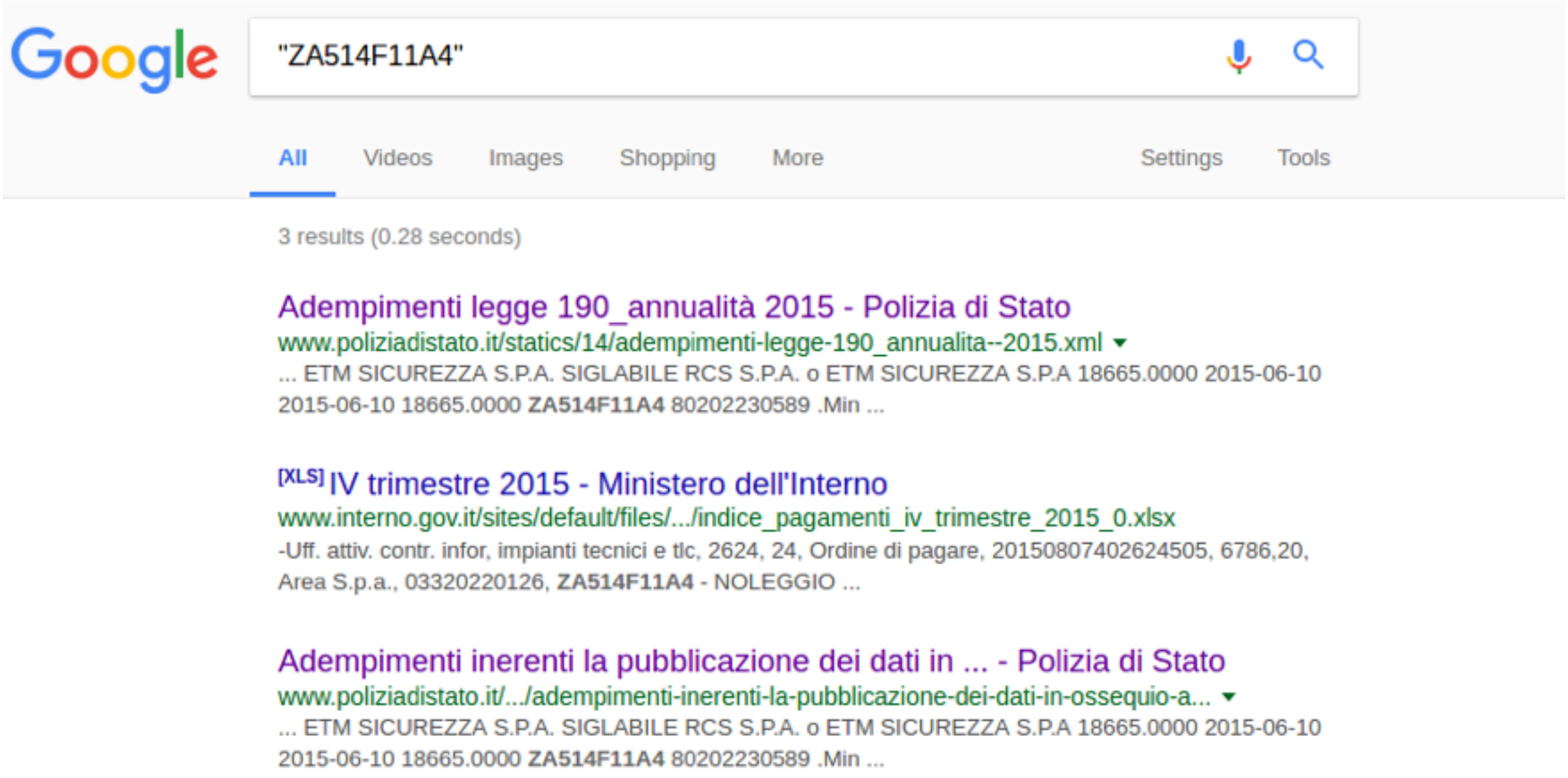
OSINT

- Payments by Ministry of Interior

IMPORTO TOTALE TITOLO	BENEFICIARIO TIT.	C.F. BENEFICIARIO TIT.	CAUSALE TITOLO
18195,00	Area S.p.a.	03320220126	NOLEGGIO APPARATI - CIG Z1918DC17A
18195,00	Area S.p.a.	03320220126	NOLEGGIO APPARATI - CIG Z1918DC17A
18195,00	Area S.p.a.	03320220126	NOLEGGIO APPARATI - CIG Z1918DC17A
18195,00	Area S.p.a.	03320220126	NOLEGGIO APPARATI - CIG Z1918DC17A

OSINT

- Advanced Google Search



OSINT

- Public Procurement datasets


```
▼<legge190:pubblicazione xmlns:legge190="legge190_1_0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  ▼<metadata>
    ▼<titolo>
      Pubblicazione dati ai sensi dell'art. 1 comma 32 legge n. 190/2012
    </titolo>
  ▼<abstract>
      Pubblicazione dati ai sensi dell'art. 1 comma 32 legge n. 190/2012
    </abstract>
    <dataPubbicazioneDataset>2017-01-03</dataPubbicazioneDataset>
    <entePubblicatore>Ministero dell'Interno</entePubblicatore>
    <dataUltimoAggiornamentoDataset>2017-02-08</dataUltimoAggiornamentoDataset>
    <annoRiferimento>2017</annoRiferimento>
    <urlFile>http://opendataavcp.interno.it/L190/80202230589</urlFile>
    <licenza>-</licenza>
  </metadata>
```

Early Findings

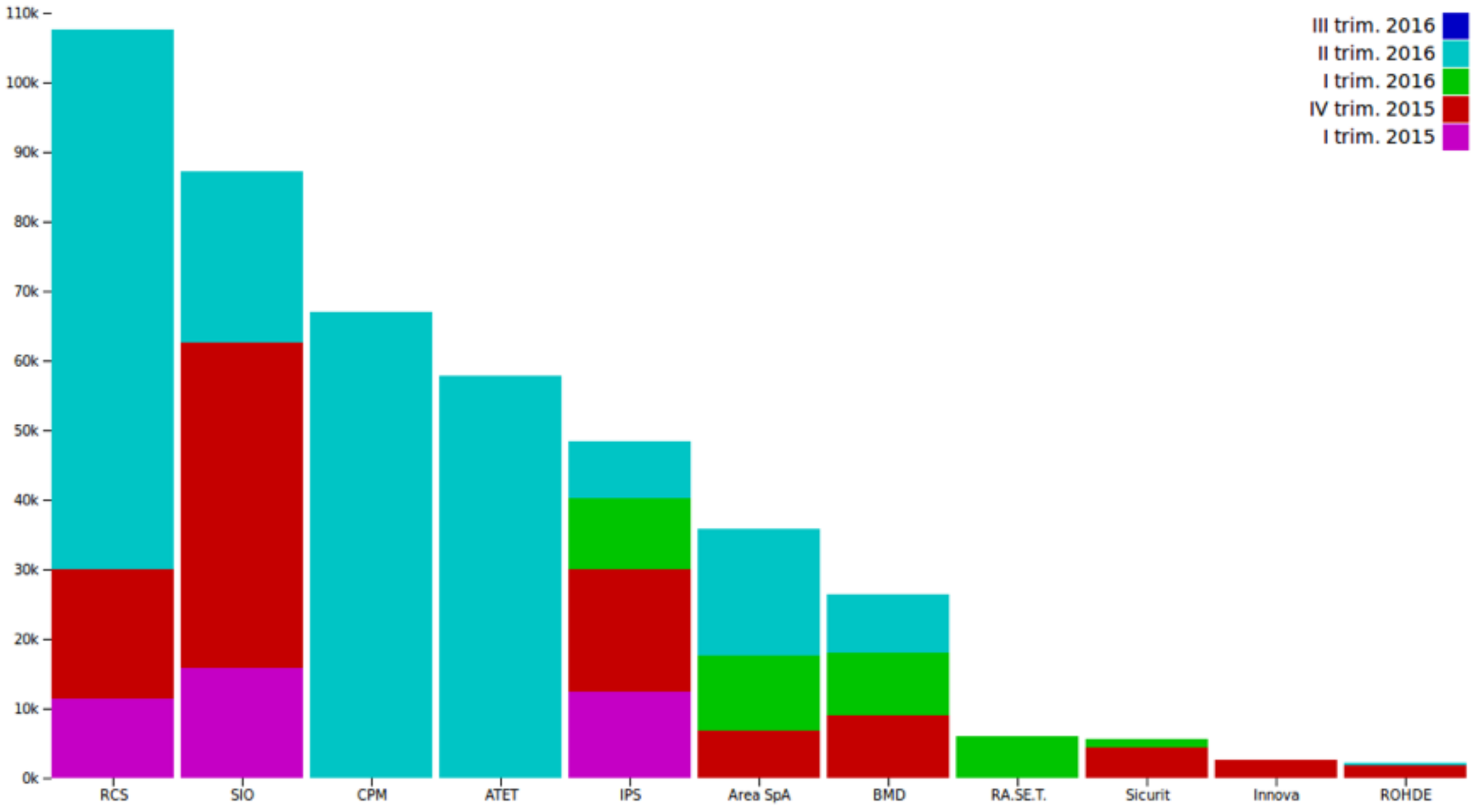
- Surveillance Companies

Società	Partita IVA
Araknos	06930301004
Area Spa	03320220126
BEA srl	07081770013//00507430015
DIGINT	05769010967
Endoacustica	06836020724
Expert System	02608970360
GR Sistemi	03396400966
Hacking Team	03924730967
Innova	01056020322
IPS Intelligence	02021190596
Leonardo	00881841001
Loquendo	08137760016
Midland Europe	02944320122
RCS	07715580630
RESI	05633751002
Sio Spa	04154970968
SPEI 2000	05394150964
Spektra Europe	02700210129
Vitrociset	04424091009

Società	Partita IVA
CSH & MPS	05557460820
Radiotrevisan	
Italarms Srl	02872730151
ATET SpA	02557620016
NSA Italia S.R.L	11972570151
RA.SE.T. S.R.L.	04873851002
CTE INTERNATIONAL S.R.L.	01671970364// 01410320350
Smiths Detection Italia S.R.L.	
SICURIT ALARMITALIA S.P.A	03475570150
Selavio Security Systems	06993720017
AV NET di Scarantino	01831070493
CPM ELETTRONICA SRL	08351181006
BMD S.R.L.	11303341009
AUS.TECH. S.R.L.	04751051006
SELEX ES S.P.A.	10111831003
ROHDE & SCHWARZ ITALIA	02156670156
TELECOM ITALIA SPA	00488410010
Cy4gate	13129151000
HDS Sistemi SpA	05348521005
Yarix srl	03614930265
4N6 srl	03531200982

Early Findings

- Expenditures



Peculiar cases

- Invoices

BENEFICIARIO TIT.	C.F. BENEFICIARIO TIT.	CAUSALE TITOLO	IMPORTO TITOLO ASSOCIATO AL DOCUMENTO
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	100,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	100,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	25,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	100,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	100,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	90,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	195,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	195,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	195,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	195,00
Area S.p.a.	3320220126	ZA514F11A4 - NOLEGGIO APPARATI	190,00

BENEFICIARIO TIT.	C.F. BENEFICIARIO TIT.	CAUSALE TITOLO	IMPORTO TITOLO ASSOCIATO AL DOCUMENTO
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	2240,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	160,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	156,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	956,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	160,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	160,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00
IPS S.p.a	202119059[illegible]6	INTERCETTAZIONI	52,00

IMSI-catchers

- Who are the participants?


```
<oggetto>FORNITURA SISTEMA IMSI CATCHER</oggetto>
<sceltaContraente>02-PROCEDURA RISTRETTA</sceltaContraente>
▼<partecipanti>
 ▼<partecipante>
    <codiceFiscale>02872730151</codiceFiscale>
    <ragioneSociale>ITALARMS S.R.L.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>11303341009</codiceFiscale>
    <ragioneSociale>BMD S.R.L.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>04751051006</codiceFiscale>
    <ragioneSociale>AUS.TECH. S.R.L.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>02557620016</codiceFiscale>
   ▼<ragioneSociale>
      ATET AZIENDA TORINESE ELETTRONICA TELECOMUNICAZIONI SPA
    </ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>00507430015</codiceFiscale>
    <ragioneSociale>B.E.A. S.R.L.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>01671970364</codiceFiscale>
    <ragioneSociale>C.T.E. INTERNATIONAL S.R.L.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>10111831003</codiceFiscale>
    <ragioneSociale>SELES ES S.P.A.</ragioneSociale>
  </partecipante>
 ▼<partecipante>
    <codiceFiscale>02156670156</codiceFiscale>
    <ragioneSociale>ROHDE & SCHWARZ ITALIA SPA</ragioneSociale>
 ▼<partecipante>
    <codiceFiscale>00488410010</codiceFiscale>
    <ragioneSociale>TELECOM ITALIA SPA</ragioneSociale>
```

IMSI-catchers

MODULARIO
INTERNO 314

MOD. 4 P.S.C.

Ministero dell'Interno

DIPARTIMENTO DELLA PUBBLICA SICUREZZA
Direzione Centrale della Polizia Criminale

DISCIPLINARE DI GARA

CIG n.5208849E29

"Gara d'appalto,ai sensi del D. Lgs. 163 del 12 aprile 2006 e ss.mm.ii., con procedura ristretta (artt. 54 e 55 punto 6) e accelerata (art.70, comma 11, lett. a e b), per l'acquisizione di un sistema IMSI Catcher per il monitoraggio e la localizzazione di terminali radiomobili in tecnologia 2G/3G/LTE - 4G"

IMSI-catchers

- Specs

l'impiego di un unico kit trasportabile[4], impiegabile ed alimentabile con autoveicoli commerciali. Di seguito è descritta la composizione di massima in cui si deve articolare la fornitura del sistema:

- unità centrale IMSI Catcher 2G/3G/LTE-4G; l'unità, composta da uno o più cestelli, si intende comprensiva del ricevitore GPS, dei nodi di simulazione delle stazioni radio base e dei moduli radio-goniometrici utili all'espletamento del Direction Finding;
- PC portatile per la gestione del sistema e l'esecuzione delle attività di monitoraggio e localizzazione; nel seguito del documento denominato anche "PC di gestione" o "interfaccia locale";
- dotazione di backup (costituita da un PC aggiuntivo e un HD immagine predisposto con tutto il software necessario);
- modulo radiogoniometrico; sottosistema, integrato con l'IMSI Catcher, utile alla esecuzione della localizzazione dei terminali;
- antenne e cavetterie varie;
- contenitore per il trasporto mobile degli apparati succitati;
- manuale d'installazione (formato cartaceo ed elettronico);
- manuale d'uso (formato cartaceo ed elettronico);
- cartografia nazionale geo-referenziata ed in formato elettronico;
- kit di alimentazione per autoveicolo;

IMSI-catchers

- Specs

Id.	FUNZIONALITA' RICHIESTE
R.4	La simulazione delle celle di radio-copertura deve poter avvenire anche su più RAT simultaneamente. Il fornitore deve indicare il numero massimo di nodi contemporaneamente simulabili per RAT. Il numero minimo di nodi contemporaneamente simulabili richiesto varia a seconda della scelta implementativa delle stazioni radio base; in tecnologia MSR/SDR/singleRAN si richiede di poter simulare almeno **3 nodi** contemporaneamente impostabili via software nella tecnologia e nella banda di frequenza di volta in volta necessaria nel corso della missione; in tecnologia tradizionale si richiedono almeno **2 nodi 2G**, **2 nodi 3G** ed **1 nodo LTE-4G**; qualora venisse offerto un solo nodo LTE-4G questo dovrà poter operare nelle bande oggetto di licenza sul territorio nazionale per tale tecnologia. In caso di stazioni radio implementate per via MSR/SDR/singleRAN, l'impostazione della RAT in cui avviene la simulazione di cella deve poter essere eseguita dall'operatore in campo senza la necessità di alcuna installazione hardware o software, ma semplicemente per mezzo di una configurazione del sistema in tempo reale per mezzo del PC di gestione/interfaccia locale.

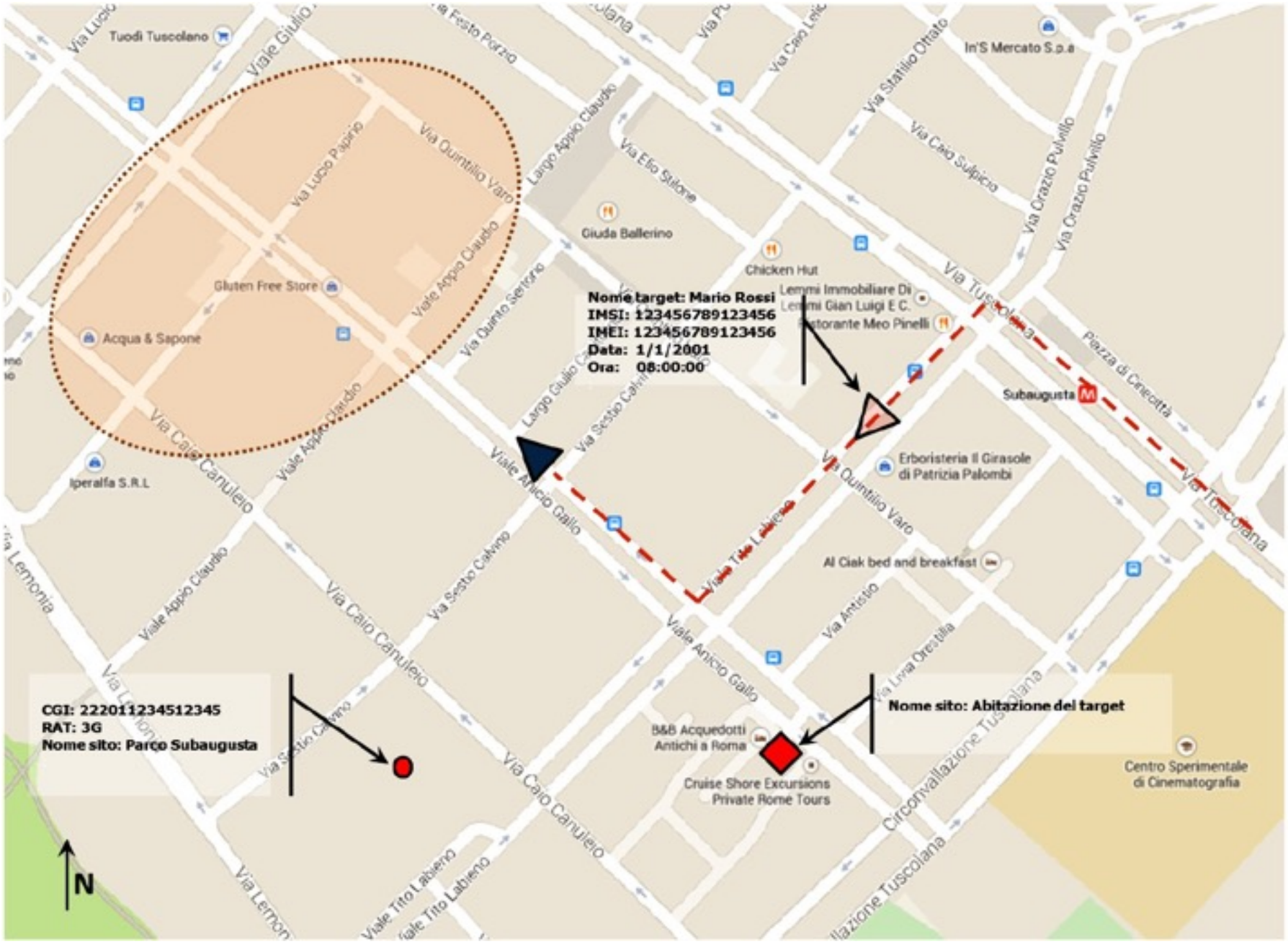
IMSI-catchers

- Specs

Id.	FUNZIONALITA' RICHIESTE
I.5	Il fornitore deve indicare le possibili combinazioni di tecnologia di partenza e arrivo in cui il sistema è in grado di indurre il terminale ad effettuare il *downgrade* radio (es: 3G✉2G, 4G✉3G ...), qualora tale prestazione sia fornita dalla soluzione proposta.

R.8	Tutti i terminali mobili nelle tecnologie 2G/3G/LTE-4G commercializzate sul territorio nazionale e presenti nell'area di copertura del sistema, inclusi i dispositivi concepiti per la sola navigazione dati (c.d. tablet, dongle o chiavetta internet), dovranno essere censiti dallo strumento (le informazioni minime acquisite sono IMSI ed IMEI del terminale). Nella modalità attiva di base (ossia quella mirata alla sola rilevazione dei terminali mobili presenti nell'area coperta dal sistema), a valle dell'acquisizione dei dati di identità del terminale, i MS dovranno essere rilasciati alla rete reale.

IMSI-catchers



Cellbrite UFED

SUPPORTO AVANZATO PER DISPOSITIVI

Leader nel settore dell'accesso ai dati mobili in combinazione con un sistema operativo più potente fornisce un'esperienza di estrazione, senza necessità di manutenzione, in accordo con i procedimenti delle scienze forensi. Frequenti aggiornamenti software per garantire una compatibilità costante con i dispositivi più recenti non appena introdotti sul mercato.

NUOVE E POTENTI FUNZIONI

- Porta per mini schermi
- Windows 10 personalizzato

IL VANTAGGIO DI UFED TOUCH2 – CARATTERISTICHE IN RISALTO

Cellebrite continua a impostare lo standard del settore per le soluzioni di analisi forense digitale. UFED Touch2 riflette proprio queste caratteristiche, fornendo vantaggi ai professionisti forensi e agli investigatori:

Cellbrite UFED

Nello specifico, all'interno di questo lotto è inclusa la fornitura di:

(1) **n. 60 apparati Cellebrite UFED Ultimate Touch (nuovi) versione rinforzata (*ruggedized*)** o eventuali nuove versioni dello stesso *kit*, completo di:

(a) **unità hardware dedicata all'acquisizione** ed interfacciamento con l'operatore che agevoli le varie fasi di estrazione dati. Lo strumento deve offrire la massima maneggevolezza e facilità d'uso nelle operazioni di estrazione. La fase di analisi vera e propria, infatti, potrà essere condotta in un secondo momento in laboratorio;

(b) **kit completo di cavi di connessione:** le unità di supporto tecnico alle indagini devono essere attrezzate per interfacciarsi con i dispositivi rinvenuti sullo scenario operativo;

(c) ***software UFED Physical Analyzer* per l'analisi forense dei dati estratti:** l'apparato di estrazione deve essere corredato di apposito *software* in grado di analizzare le evidenze digitali rinvenute nelle memorie dei dispositivi acquisiti, con particolare riguardo alla ricostruzione delle strutture dati contenute in una copia fisica (*physical dump*) delle memorie;

(d) ***software UFED Phone Detective* per l'individuazione guidata del modello del dispositivo da analizzare:** gli operatori dovranno essere guidati nella procedura di acquisizione fin dalla corretta identificazione del tipo di dispositivo sotto indagine;

(e) ***software UFED Link Analysis*** per l'analisi di correlazione delle informazioni estratte dai dispositivi;

(f) ***chassis* rinforzato (*ruggedized*) di protezione dell'apparato**: per garantire un uso ottimale delle apparecchiature, devono essere necessariamente forniti supporti per la prevenzione di *shock* meccanici (*case* imbottiti,

IP Interception

OGGETTO	AGGIUDICATARIO	IMPORTO
2013		
MANUTENZIONE SISTEMI DI INTERCETTAZIONE	RCS ETM SICUREZZA SPA	33212
2014		
MANUTENZIONE N. 3 SISTEMI INTERCETTAZIONE INTERNET	RCS ETM SICUREZZA SPA	24500
2015		
MANUTENZIONE SISTEMI INTERCETTAZIONE INTERNET	RCS ETM SICUREZZA SPA	34800
2016		
FORNITURA N. 4 SISTEMI MONITORAGGIO AUDIO DIGITALE PER AUTOVEICOLI	AREA SPA	10719
Manutenzione sistemi intercettazione internet	RCS ETM SICUREZZA S.P.A.	42000
PR.366.00F.001 (AgA) - servizio di manutenzione e assistena sistema SFERA	RCS SPA	27000
RICONOSCIMENTO DI DEBITO PER NOLEGGIO APPARATI	RCS ETM SICUREZZA S.P.A.	4100
RICONOSCIMENTO DI DEBITO PER NOLEGGIO APPARATI	RCS ETM SICUREZZA S.P.A.	18469.4
RICONOSCIMENTO DI DEBITO PER NOLEGGIO APPARATI	RCS ETM SICUREZZA S.P.A.	22175
RICONOSCIMENTO DI DEBITO PER NOLEGGIO APPARATI	RCS SPA	24432
		2017
NOLEGGIO APPARATI	RCS ETM SICUREZZA S.P.A.	23836

IP Interception

Dati aggiornati al: 31/08/2016

Progetto

RCS ETM SICUREZZA

Cod. PIAI*049452/0013/0030*A-1247-P

Scarica in formato vettoriale | Istruzioni

Descrizione | Beneficiari | Obiettivi

Ambito/i	Beni e attività culturali ???
Descrizione	Il progetto prevede la realizzazione di un nuovo sistema di monitoraggio per il supporto alle Autorità Giudiziarie nelle attività di indagine e di repressione del crimine. Il sistema è basato sulla realizzazione di apparati per l'intercettazione legale di dati su rete di accesso con tecnologia ADSL, chiamati Sonde ADSL. Assieme ad essi il progetto prevede lo sviluppo di un apparato Mediation Device per la collezione e trasporto dei dati intercettati verso le procure e di un terzo apparato chiamato Provisioning Management System, per la configurazione e gestione delle sonde. A tal fine sono state individuate le seguenti funzionalità d'interesse: intercettazione di tutto il traffico relativo ad un utente identificato mediante attacco di utente attraverso l'impiego di sonde ADSL; intercettazione di tutto il traffico da/per un sito predefinito attraverso uno specifico sviluppo del software; identificazioni di sessioni d'interesse ed intercettazione delle stesse. Le caratteristiche principali previste per il sistema sono: trasparenza, sicurezza, utilizzo dei protocolli sicuri per il trasferimento dei dati sensibili; mantenimento dei dati sensibili nelle sonde e involucri sicuri difficilmente manomettibili.
Costo totale	911.600,00 euro

IP Interception

Data approvazione	**20/03/2006**	
Inizio attività	Data prevista **01/05/2005**	Data effettiva **01/05/2005**
Fine attività	Data prevista **13/07/2007**	Data effettiva **13/07/2007**
Costo totale	**911.600,00 euro**	
Contributo pubblico	Totale **133.661,00 euro**	Ammesso PON R&C **13.366,10 euro**
Erogazioni	Totale **120.294,90 euro**	Importo PON R&C **-** Data ultima erogazione PON R&C **14/01/2015**

Secret tenders

Programmi	*Sigla identificativa del programma*	*Esigenza operativa*	*Quantità*	*Onere globale previsto (1)*
AMMODERNAMENTO SISTEMA ARACNE FASE II – LOTTO 5 OPZIONALE	P. PERF. - SCHEDA 4	POTENZIAMENTO ED AMMODERNAMENTO SISTEMI COMINT	N.A. euro	€ 245.860,50
L'ACQUISIZIONE DEL SUPPORTO NECESSARIO AL POTENZIAMENTO DEL SISTEMA COSA	---	POTENZIAMENTO ED AMMODERNAMENTO SISTEMI COMINT	N.A. euro	€ 487.043,52
PIATTAFORMA DI CYBER INTELLIGENCE MALWARE ANALYSIS - CLESSIDRA	---	POTENZIAMENTO ED AMMODERNAMENTO SISTEMI COMINT	N.A. euro	€ 498.514,97
ACQUISIZIONE DEL SISTEMA DI SELEZIONE DEL TRAFFICO INTERCETTATO "BEAGLE" E DEL SISTEMA DI RAPPRESENTAZIONE DEL TRAFFICO "SPEECH TO TEXT" - INTEGRAZIONE IVA DAL 21 % AL 22 %	SMD 20/2014	POTENZIAMENTO ED AMMODERNAMENTO SISTEMI COMINT	N.A. euro	€ 4.286,10
L'AMMODERNAMENTO SISTEMI INFORMATICI DEL C.I.I.	---	AMMODERNAMENTO E POTENZIAMENTO DEI SISTEMI INFORMATICI	N.A. euro	€ 504.907,25
AMMODERNAMENTO SISTEMI ELINT - SOFIA	---	POTENZIAMENTO ED AMMODERNAMENTO SISTEMI COMINT	N.A. dollari	€ 1.800.000,00

Secret tenders

- BEAGLE

EXPERT SYSTEM SUITE:
Beagle - Netwatcher

A. Presentation

1. Tools

Beagle
Beagle is an innovative solution that allows to perform detailed analyses of all the significant information contained in the text. It supplements the basic semantic net with highly customizable modules to monitor the specific information sources and find connections among documents available in different formats.

Netwatcher
NetWatcher is an advanced software agent that performs targeted searches on Internet and Intranet, offering the opportunity of setting customized search criteria, and communicating the results to the user via e-mail and Web pages. Thanks to the continuous monitoring of the specified sources, the user can receive automatically the results of the search and then file the results.

What's next?

- FOIA requests

1. L'istanza di accesso generalizzato presentata il **15.05.2017** , con la quale la s.v. ha richiesto l'estrazione di copia telematica mediante trasmissione in P.E.C., è stata **accolta** Si rende disponibile, pertanto, la sottoelencata documentazione:
   - Fattura n. 1114000040 del 20.01.2014 di €. 1.074,09;
   - Fattura n. 1114000041 del 20.01.2014 di €, 1.074,09;
   - Fattura n. 1114000042 del 20.01.2014 di €. 295,00;
   - Fattura n. 1114000043 del 20.01.2014 di €[i]. 295,00:
   - Fattura n. 1114000044 del 20.01.2014 di €. 287,92;
   - Fattura n. 1116001795 del 29.01.2016 di €. 2.171,60;
   - Fattura n. 1116001796 del 29.01.2016 di €. 2.830,40;
   - Fattura n. 1116001797 del 29.01.2016 di € 1.952,00;
   - Fattura n. 1116001798 del 29.01.2016 di €. 2.830,40;
   - [ii]Fattura n.1116001799 del 29.01.2016 di €. 1.0952,00;
   - Fattura n. 1116001800 del 29.01.2016 di €. 244,00;
   - Fattura n. 1116001801 del 29.01.2016 di €. 244,00;
   - Fattura n. 1116001802 del 29.01.2016 di €. 244,00;
   - Fattura n. 1116001803 del 29.01.2016 di €, 244,00;
2. *(altre eventuali comunicazioni dirette esclusivamente all'interessato).*

1. Si inviano, pertanto, i documenti messi a disposizione e si precisa che la ricezione a mezzo P.E.C. della presente comunicazione, comprensiva dei suoi allegati, costituirà avvenuto esercizio del diritto di accesso.
2. Il responsabile del procedimento è: *(si identifica nel Capo Servizio Amministrativo del Reparto Autonomo del Comando Generale dell'Arma dei Carabinieri).*

What's next?

- FOIA requests to obtain:
    - Invoices
        - Technical and economic offers
- Expand the database of companies
- Monitor Government expenditures

Thank you!

- Contacts

riccardo.coluccini@vice.com

fabio.pietrosanti@logioshermes.org

e-Privacy XXI 23-24 Giugno 2017