



RAGGRUPPAMENTO OPERATIVO SPECIALE CARABINIERI

Reparto Indagini Telematiche



***Sviluppo delle capacità investigative nel
contrasto alla criminalità organizzata attraverso
l'analisi e l'acquisizione di evidenze digitali per
le esigenze operative del Raggruppamento
Operativo Speciale dei Carabinieri***

-ACQUISTO DI SISTEMI PER L'ANALISI FORENSE-

Capitolato tecnico

Rel. 2.0

SOMMARIO

1	<i>Premessa</i>	3
2	<i>Elementi della fornitura</i>	3
2.1	<i>Dispositivo di protezione dalla scrittura (WB)</i>	3
2.2	<i>Software per l'analisi forense (SW-PC)</i>	3
2.3	<i>Software per l'analisi forense di dispositivi mobili (SW-MOB)</i>	4
2.4	<i>Hardware per l'analisi forense di dispositivi mobili (HW-MOB)</i>	5
2.5	<i>Software per l'analisi di web artifacts (SW-WEB)</i>	6
3	<i>Dotazioni</i>	6
3.1	<i>Dotazione RITEL</i>	6
3.2	<i>Dotazione avanzata</i>	7
3.3	<i>Dotazione media</i>	7
3.4	<i>Dotazione base</i>	7
3.5	<i>Quantitativi</i>	7
4	<i>Addestramento</i>	8
5	<i>Termini di fornitura e collaudi</i>	9
6	<i>Servizi di installazione e configurazione</i>	10
7	<i>Garanzia</i>	10
8	<i>Fatturazione</i>	10
9	<i>Personale</i>	10
10	<i>Informazioni riservate</i>	10
11	<i>Modalità d'accesso</i>	11
12	<i>Responsabilità per danno</i>	11
13	<i>Documento Unico di Valutazione dei Rischi Interferenti - DUVRI</i>	11
14	<i>Comunicazioni</i>	12

1 Premessa

L'Amministrazione intende dotare il Raggruppamento Operativo Speciale dell'Arma dei Carabinieri di idoneo materiale e relativo addestramento per il compimento di indagini nel settore della Digital Forensics.

2 Elementi della fornitura

Nel seguito verranno elencate le caratteristiche minime obbligatorie degli elementi della fornitura, rimandando le peculiarità opzionali al documento di specifica degli elementi di valutazione tecnico-economica.

2.1 Dispositivo di protezione dalla scrittura (WB)

- a. Possibilità di collegare nativamente dispositivi USB 2/3
- b. Interfaccia verso l'host computer in USB 3.0
- c. Dotazione completa di alimentatore e cavi USB
- d. Garanzia 3 anni

2.2 Software per l'analisi forense (SW-PC)

- a. Analisi dei filesystem Windows (NTFS, FAT16, FAT32, exFAT, CDFS), Linux (Ext2, Ext3, Reiser, JFS) ed Apple Machintosh (HFS, HFS+ e APFS)
- b. Capacità di indicizzazione dei dati per una ricerca rapida
- c. Capacità di effettuare ricerche binarie
- d. Capacità di mostrare l'anteprima del contenuto dei formati di file più comuni
- e. Capacità di esecuzione da dispositivi USB senza necessità di installazione (modalità portable)
- f. Supporto ai linguaggi di scripting
- g. Capacità di effettuare acquisizioni remote via rete tramite agente
- h. Capacità di porre in sola lettura di dispositivi USB collegati e bloccare qualsiasi tentativo di scrittura (write blocking)
- i. Supporto nativo per la crittografia EFS, Bitlocker, McAfee, Checkpoint, PGP, Safeguard
- j. Capacità di esecuzione distribuita

2.3 Software per l'analisi forense di dispositivi mobili (SW-MOB)

- a. Sistemi operativi supportati nativamente:
 - Android (tutte le versioni)
 - iOS (tutte le versioni)
 - Blackberry OS
 - Windows Phone
 - Windows Mobile
- b. Capacità di accesso ed estrazione:
 - Logica (minimo 8000 dispositivi)
 - File System (minimo 5000 dispositivi)
 - Fisica, senza necessità di preventiva acquisizione delle prerogative di amministratore (rooting) del dispositivo (minimo 5000 dispositivi)
 - Bypass della protezione (minimo 4000 dispositivi)

Dovrà essere fornita sia la lista aggiornata alla versione corrente contenente marca e modello dei dispositivi che la garanzia circa l'effettuazione dei test per ognuno di essi.
- c. Disabilitazione e riattivazione del blocco utente
- d. Disattivazione della sequenza di blocco e del codice PIN per almeno 300 dispositivi Android, inclusi Samsung Note 4, Galaxy Tab, Galaxy S5, Galaxy Mini, LG G4, Nexus 5, Galaxy S6
- e. Supporto all'estrazione fisica per dispositivi Android Qualcomm mediante la funzionalità EDL e con eventuale bypass del blocco utente
- f. Capacità' di estrazione e analisi di dispositivi di fabbricazione cinese dotati di connettori non standard
- g. Acquisizione fisica mediante bootloader appositamente sviluppato dal costruttore (è pertanto esclusa la possibilità di utilizzo di bootloader di terze parti), senza l'impiego di tecniche di rooting ed senza alterazione del contenuto informativo del reperto
- h. Clonazione SIM/USIM card
- i. Capacità di visualizzare i dati della configurazione delle SIM acquisite
- j. Recupero dei dati cancellati da database SQLite 3
- k. Possibilità di eseguire ricerche personalizzabili dall'utente sui database SQLite 3 usati dalla App installate nei dispositivi mobili in

esame

- l. Funzionalità di identificazione di malware eventualmente presenti nei dispositivi esaminati
- m. Presenza di un set di accessori, adattatori e cavi contenuti in una borsa appositamente progettata

2.4 Hardware per l'analisi forense di dispositivi mobili (HW-MOB)

HW-MOB dovrà possedere tutte le caratteristiche già citate al precedente punto 2.3 ed in aggiunta:

- a. L'apparato è di tipo portatile (ovvero fruibile sia in laboratorio sia all'esterno), contiene l'applicazione per l'acquisizione ed è comprensivo di accessori, adattatori e cavi. E' composto da uno chassis appositamente progettato ed ingegnerizzato dal costruttore per gli scopi di acquisizione forense dei dati da dispositivi mobili ed è contenuto in apposita custodia rinforzata
- b. Capacità di eseguire estrazione e analisi dei dati in contemporanea
- c. Display touch screen capacitivo a colori
- d. Dotazione di Batteria Li-Ion interna ricaricabile in caso di assenza di alimentazione
- e. Tecnologie di rete: Wi-Fi, Bluetooth, Ethernet 1Gbit porta RJ45
- f. Porte USB 3.0: minimo 4
- g. Porta seriale
- h. Posizionamento GPS
- i. Lettore integrato SIM con supporto per: SIM, Micro SIM, Nano SIM e lettore di schede SD per SD, SDHC, MMC, SDXC
- j. Possibilità di ripristino delle impostazioni di fabbrica
- k. Rilevazione automatica del modello del dispositivo mobile oggetto dell'estrazione
- l. Funzione di identificazione del dispositivo mobile in esame per fornitore, modello, IMEI
- m. Possibilità di inserimento dei dettagli dell'indagine
- n. Filtro predefinito dell'utente che permetta di estrarre e visualizzare solo una parte dei contenuti del dispositivo, in base all'intervallo di tempo o alle informazioni specifiche del soggetto (persona, email, telefono)
- o. Presenza di tastiera virtuale per la digitazione del testo

- p. Aggiornamento della licenza software mediante rete o porta USB
- q. Possibilità di ricezione di notifiche automatiche in caso di aggiornamenti e nuove versioni dell'applicazione quando l'unità di estrazione portatile è collegata alla rete
- r. Funzionalità di autenticazione per consentire l'accesso ai soli utilizzatori autorizzati

2.5 Software per l'analisi di web artifacts (SW-WEB)

- a. Analisi dei filesystem Windows (NTFS, FAT16, FAT32, exFAT, CDFS), Linux (Ext2, Ext3) ed Apple Machintosh (HFS, HFS+)
- b. Capacità di indicizzazione dei dati per una ricerca rapida
- c. Capacità di effettuare ricerche binarie
- d. Identificazione della navigazione web dei seguenti browser: Internet Explorer, Chrome, Firefox, Safari
- e. Capacità di Identificazione delle Chat di Skype, MSN, Facebook
- f. Supporto nativo per la crittografia EFS, Bitlocker e McAfee
- g. Possibilità di esportare dati ed analizzarli tramite applicazione nativa senza necessità di licenza

3 Dotazioni

Al fine di meglio attagliare gli strumenti tecnici alle esigenze investigative dei Reparti centrali e periferici della catena Anti Crimine, sono stati individuati i seguenti requisiti:

- Dotazione RITEL
- Dotazione avanzata
- Dotazione media
- Dotazione base

di seguito meglio definite.

3.1 Dotazione RITEL

Di seguito le specifiche tecniche della dotazione:

N.	Elemento	Quantità	Anni di supporto aggiuntivi al primo
1	WB	3 (tre)	
2	SW-PC	2 (due)	1 (uno)
3	SW-WEB	2 (due)	1 (uno)
4	SW-MOB	2 (due)	1 (uno)

5	HW-MOB	3 (tre)	1 (uno)
---	--------	---------	---------

3.2 Dotazione avanzata

Di seguito le specifiche tecniche della dotazione:

N.	Elemento	Quantità	Anni di supporto aggiuntivi al primo
1	WB	2 (due)	
2	SW-PC	1 (uno)	1 (uno)
3	SW-WEB	1 (uno)	1 (uno)
4	SW-MOB	1 (uno)	1 (uno)
5	HW-MOB	1 (uno)	1 (uno)

3.3 Dotazione media

Di seguito le specifiche tecniche della dotazione:

N.	Elemento	Quantità	Anni di supporto aggiuntivi al primo
1	WB	1 (uno)	
2	SW-PC	1 (uno)	1 (uno)
3	SW-WEB	1 (uno)	1 (uno)
4	SW-MOB	1 (uno)	1 (uno)
5	HW-MOB	1 (uno)	1 (uno)

3.4 Dotazione base

Di seguito le specifiche tecniche della dotazione:

N.	Elemento	Quantità	Anni di supporto aggiuntivi al primo
1	WB	1 (uno)	
2	SW-PC	1 (uno)	1 (uno)
3	SW-WEB	1 (uno)	1 (uno)
4	SW-MOB	1 (uno)	1 (uno)

3.5 Quantitativi

L'Amministrazione richiede:

- numero 1 (una) **dotazione RITEL** in favore del Reparto Indagini Telematiche di Roma;
- numero 5 (cinque) **dotazioni avanzate** in favore dei seguenti comandi:
 - o Reparto AC di Napoli;

- Reparto AC di Reggio Calabria;
- Reparto AC di Palermo;
- Reparto AC di Milano
- Sezione AC di Padova
- numero 4 (quattro) **dotazioni medie** in favore dei seguenti comandi:
 - Sezione AC di Cagliari;
 - Sezione AC di Bologna;
 - Sezione AC di Trento;
 - Sezione AC di Perugia;
- numero 16 (sedici) **dotazioni base** in favore dei seguenti comandi:
 - Sezione AC di Salerno;
 - Sezione AC di Bari;
 - Sezione AC di Catanzaro
 - Sezione AC di Catania;
 - Sezione AC di Brescia;
 - Sezione AC di Firenze;
 - Sezione AC di Genova;
 - Sezione AC di Torino;
 - Sezione AC di Lecce;
 - Sezione AC di Potenza;
 - Sezione AC di Messina;
 - Sezione AC di Caltanissetta;
 - Sezione AC di Ancona;
 - Sezione AC di Campobasso;
 - Sezione AC di L'Aquila;
 - Sezione AC di Udine.

4 Addestramento

Attesa la complessità degli strumenti tecnici oggetto di acquisizione, la formazione del personale operante deve costituire parte integrante e qualificante della fornitura. Si rende pertanto necessaria l'erogazione dei seguenti corsi, presenti nel catalogo ufficiale dei costruttori e tenuti da partner da essi certificati (Authorized Training Partners):

1. Corso di addestramento per l'utilizzazione di Software per l'analisi forense (43 corsi totali) di cui:

- Corso SW-PC base, per complessive 4 giornate addestrative in favore di 33 (trentatre) militari;
 - Corso SW-PC avanzato, per complessive 8 giornate addestrative in favore di 10 (dieci) militari;
2. Corso di addestramento per l'utilizzazione di software per l'acquisizione e l'analisi forense di dispositivi mobili (32 corsi totali) di cui:
- Corso SW-MOB base, per complessive 3 giornate addestrative in favore di 20 (venti) militari;
 - Corso SW-MOB avanzato, per complessive 5 giornate addestrative in favore di 12 (dodici) militari;
3. Corso di addestramento per l'utilizzazione di Unità hardware dedicata all'acquisizione ed interfacciamento con l'operatore che agevoli le fasi di estrazione dati (tablet, notebook ecc. – 10 corsi totali):
- Corso HW-MOB base, per complessive 3 giornate addestrative in favore di 10 (dieci) militari;

I corsi si terranno presso le strutture che il Raggruppamento Operativo Speciale renderà disponibili (aula multimediale per complessivi 22 postazioni) presso la propria sede in Roma.

5 Termini di fornitura e collaudi

L'operatore economico aggiudicatario dovrà approntare alla verifica di conformità l'intera fornitura entro 60 giorni solari a decorrere dal giorno successivo alla data di ricezione, tramite posta elettronica certificata, della comunicazione attestante l'avvenuta registrazione del contratto presso gli organi di controllo.

Entro la medesima tempistica, la società contraente dovrà consegnare l'intera fornitura presso le sedi dei Reparti CC indicati nel punto 3.5 del presente capitolato tecnico, nelle quantità e dotazioni previste.

Apposita commissione nominata dal Comando Generale dell'Arma dei Carabinieri, dopo aver ricevuto conferma da tutti i Reparti dell'avvenuta consegna dell'intera fornitura, eseguirà – presso n. 4 Reparti CC individuati a campione – la verifica di conformità dei beni consegnati.

L'esecuzione dei corsi di addestramento dovrà essere erogata presso la sede del ROS di "Ponte Salario" di Roma, entro 60 giorni solari dal giorno successivo alla ricezione, tramite posta elettronica certificata, della comunicazione dell'avvenuta favorevole verifica di conformità della fornitura, da parte dell'Ufficio Sistemi Informativi del Comando Generale dell'Arma dei Carabinieri. Conclusi interamente i corsi previsti, la società aggiudicataria dovrà darne comunicazione a mezzo P.E.C. all'Ufficio Sistemi Informativi ed al Centro Unico Contrattuale del Comando Generale dell'Arma dei Carabinieri.

6 Servizi di installazione e configurazione

Gli operatori presso i Reparti sono addestrati all'installazione ed alla configurazione degli apparati in fornitura, pertanto non sono richiesti servizi di tale genere.

7 Garanzia

La società contraente s'impegna a garantire il prodotto in fornitura per almeno 24 mesi, decorrente dalla favorevole verifica di conformità della fornitura. Il servizio di garanzia sarà reso disponibile su segnalazione degli utenti finali, o su richiesta del Raggruppamento Operativo Speciale, mediante chiamata ad un numero telefonico che la società dovrà mettere a disposizione dell'Amministrazione entro la medesima tempistica prevista per la consegna dei materiali in fornitura e che dovrà essere operativo dal lunedì al venerdì dalle 09.00 alle 18.00 esclusi festivi. Gli interventi in garanzia dovranno essere effettuati entro 3 giorni solari dalla chiamata.

8 Fatturazione

La società contraente potrà emettere fattura conseguentemente alla comunicazione formale dell'Amministrazione attestante il favorevole esito delle operazioni di verifica di conformità e dell'avvenuta effettuazione dei corsi. Fatture pervenute anticipatamente a tale comunicazione non saranno prese in considerazione ai fini del pagamento.

La fattura dovrà essere trasmessa, in formato elettronico, con il meccanismo "SPLIT PAYMENT", ai sensi di quanto disposto dal nuovo art.17-ter del D.P.R. n.633/1972, attraverso il sistema di interscambio (SDI).

9 Personale

La Società garantisce sin dalla firma del contratto che tutti gli interventi di fornitura ed assistenza saranno effettuati impiegando esclusivamente personale regolarmente assunto ed inquadrato a termine di legge, e nel rispetto delle norme antinfortunistiche in materia.

La Ditta contraente si impegnerà a far rispettare al proprio personale le norme comportamentali e quelle di sicurezza in vigore all'interno dei Comandi dell'Arma.

L'Arma si riserva la facoltà di richiedere ed ottenere, a proprio insindacabile giudizio, la sostituzione del personale che abbia violato dette norme comportamentali e di sicurezza.

10 Informazioni riservate

Qualsiasi notizia, documento, informazione, concernente direttamente o indirettamente il lavoro svolto o l'organizzazione e l'attività dell'Arma che venisse a conoscenza della Ditta contraente o

del suo personale, in relazione ai servizi prestati, dovrà essere trattato come materiale riservato e non potrà essere comunicato a terzi neanche parzialmente.

Sono escluse dalle condizioni suddette le notizie, o informazioni che siano o divengano di dominio pubblico, o che siano già state portate a conoscenza della Ditta contraente da terzi a valido titolo.

É in ogni caso esclusa la duplicazione o riproduzione o asportazione di documentazione dell'Arma, anche qualora contenesse notizie già di pubblico dominio. Detto obbligo sopravviverà per un periodo di almeno due anni dalla data di cessazione del rapporto tra la Ditta contraente e l'Arma.

11 Modalità d'accesso

Nel caso si rendesse necessario, la ditta dovrà comunicare al Reparto Indagini telematiche del Raggruppamento Operativo Speciale dei Carabinieri l'elenco nominativo del personale che sarà incaricato di accedere ai locali dell'Amministrazione, al fine di consentire all'Ufficio di adempiere ai previsti controlli di sicurezza.

Tale elenco con la relativa documentazione dovrà essere aggiornato con i nuovi inserimenti di personale, anche per sostituzione temporanea di altro personale.

12 Responsabilità per danno

Sono a carico della Ditta contraente tutti gli oneri ed i rischi connessi ad eventuali danni a persone o cose provocati dalla Ditta stessa o dal suo personale nell'esecuzione dell'attività di manutenzione o comunque durante la loro permanenza all'interno di locali dell'Arma.

Per quanto riguarda gli eventuali danni causati agli utenti finali dell'Arma ed imputabili alla Ditta contraente, essi saranno regolamentati dalle Direttive Comunitarie e dalle leggi italiane in materia.

É quindi a carico della Ditta contraente il risarcimento delle eventuali spese giudiziali sostenute dall'Arma e degli eventuali danni da questa subiti, relativamente alle due fattispecie sopra riportate.

13 Documento Unico di Valutazione dei Rischi Interferenti - DUVRI

Le parti, in osservanza di quanto disposto dal D.Lgs. 81/08 non hanno provveduto a predisporre il DUVRI, avendo valutato, in relazione all'attività oggetto dell'appalto, l'assenza di rischi interferenti in quanto trattasi di mera fornitura di apparati senza alcun correlato servizio di installazione.

Pertanto le parti convengono che i costi per l'azzeramento dei rischi interferenti sono pari a zero.

14 Comunicazioni

Tutte le comunicazioni scambiate con l'Amministrazione si intendono inviate mediante Posta Elettronica Certificata.