



Raggruppamento Carabinieri Investigazioni Scientifiche

Reparto Tecnologie Informatiche

L'Arma dei Carabinieri ed i
Crimini ad alta tecnologia

Narni, 15 maggio 2009

Magg. CC Ing. Marco Mattiucci



Reparto Tecnologie Informatiche



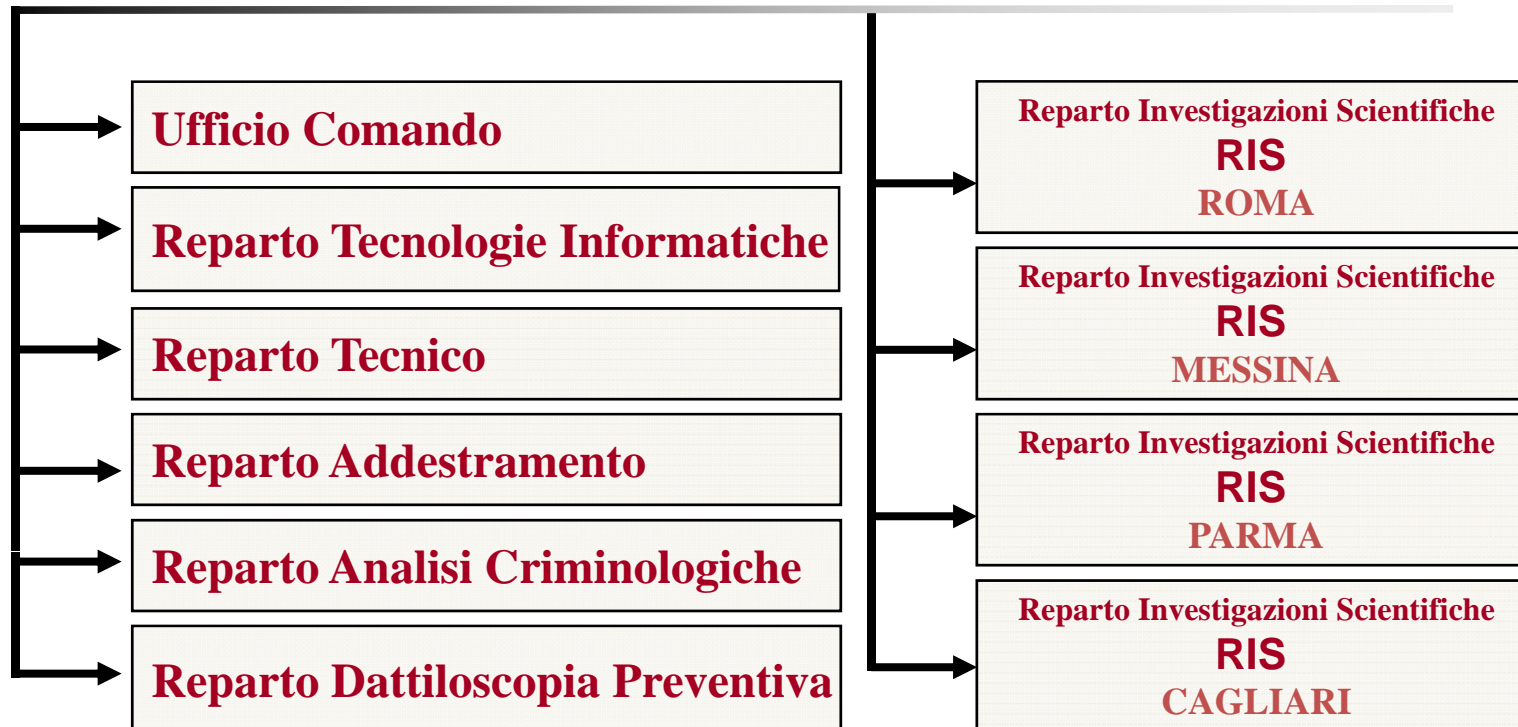
-
- Formalmente istituito nel 2006 fonda la sua prassi tecnico/investigativa su una consolidata esperienza che parte nel 1998
 - Tale esperienza è nata dall'esigenza di affrontare repertamento ed analisi, sia sulla scena del crimine che in laboratorio, di sistemi digitali, a scopo di indagine di PG



Reparto Tecnologie Informatiche



La struttura ordinativa in cui è inserito:

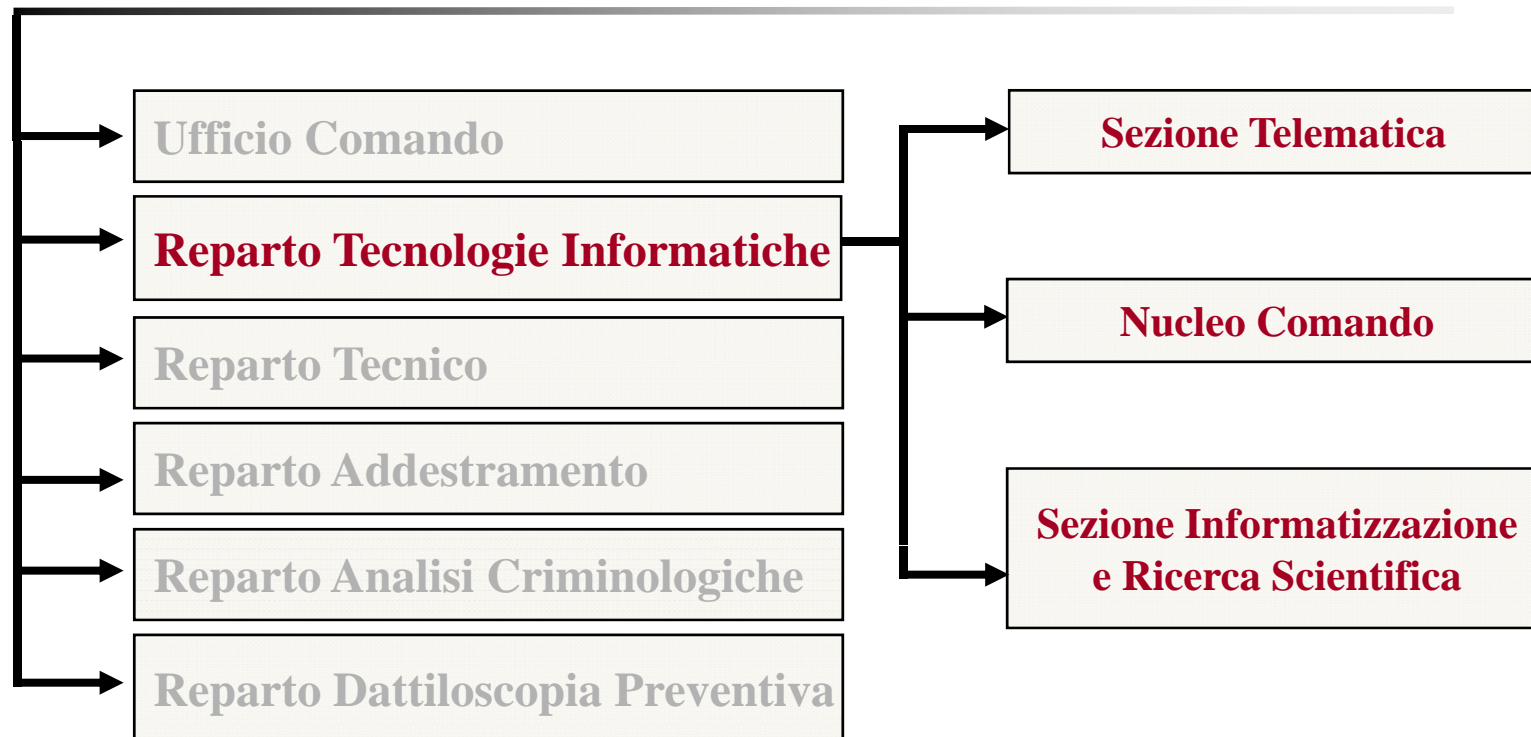




Reparto Tecnologie Informatiche



La struttura ordinativa del Reparto:





La Sezione Telematica



-
- Inserita dapprima nei contesti del Reparto Tecnico, poi del RIS di Roma ed infine nel Reparto Tecnologie Informatiche
 - Tra i suoi compiti istitutivi lo svolgimento di indagini tecniche su tutti i reperti che afferiscano a sistemi digitali ma sempre e solo POST-MORTEM



La Sezione Telematica



-
- La Sezione si occupa quindi della **branca informatica della criminalistica** e dato che opera solo post-mortem e su qualsiasi tipo di sistema digitale il suo naturale campo di applicazione è la: **DIGITAL FORENSICS**.
 - *“...the science of recovering digital evidence from digital systems under forensically sound conditions using accepted methods.” (NIST)*



Digital Forensics...



-
- **Digital Evidence:** attenzione! Non si può tradurre “*prova digitale*”...
 - **Forensically sound conditions:** massima salvaguardia dei dati e completo logging
 - **Accepted methods:** ...dalla comunità scientifica internazionale



La Sezione Telematica



- Nel 2008 ha svolto 500 indagini tecniche coinvolgendo tra i casi consueti:
 - Circa 5000 Tbyte di dati analizzati;
 - Oltre 400 cellulari e 500 SIM;
 - Oltre 600 Hard Disk e 200 pendrive;
 - Circa 200 siti web e 300 email address;
 - Alcune decine di sistemi elettronici speciali;
 - Almeno 200 carte plastiche di pagamento.



La Sezione Telematica



-
- Settori di indagine:
 - Computer Forensics;
 - Mobile Forensics;
 - Network & Internet Forensics;
 - Debit & Credit card frauds;
 - Electronic Forensics.



Reparto Tecnologie Informatiche



La struttura ordinativa del Reparto:





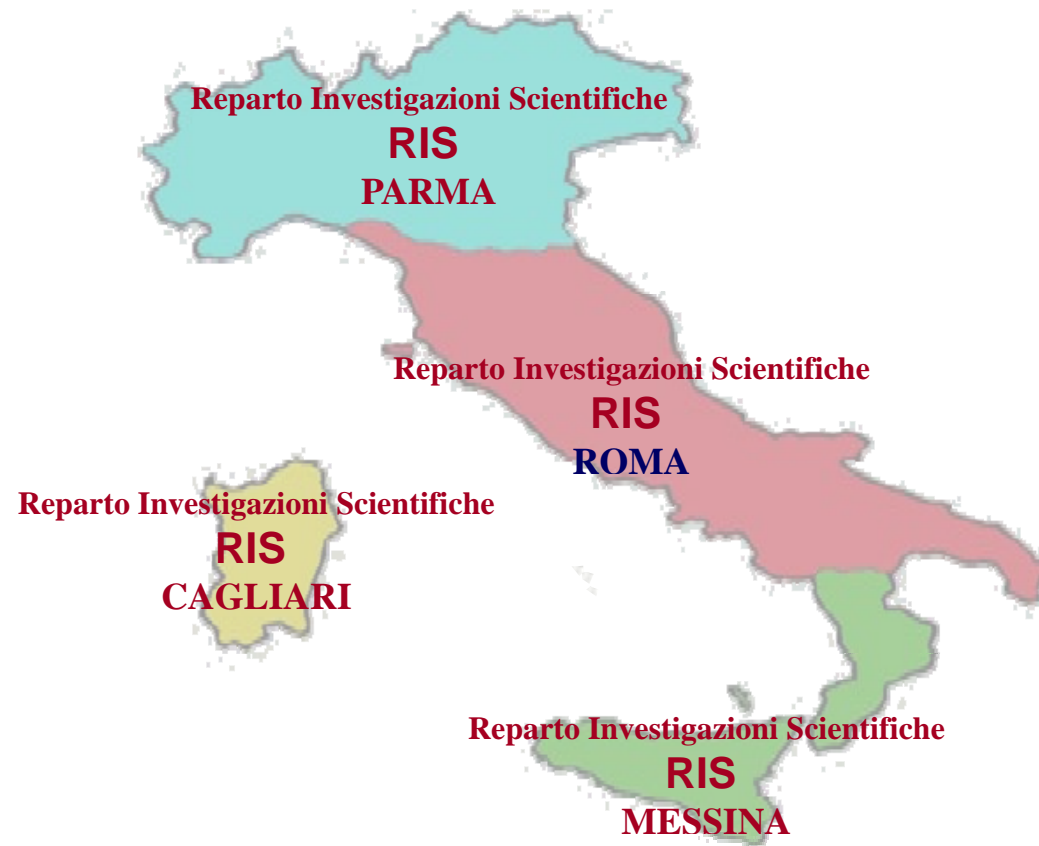
La Sezione I.R.I.S.



-
- Gestione del collegamento telematico tra i RIS in Italia;
 - Gestione delle banche dati scientifiche;
 - Ricerca di nuovi strumenti e metodologie per le indagini nel Digital Forensics e nella sicurezza digitale ed elettronica;
 - Studio delle garanzie per la privacy sui dati informatici nelle indagini tecniche
-



Competenza areale dei RIS





Competenza areale RTI





I settori di indagine tecnica



-
- **Computer Forensics:** copia “forense” ed analisi di memorie di massa (semipermanenti e permanenti)
 - **Data recovery:** recupero di file cancellati;
 - **Data carving:** recupero e ricostruzione di parti di file cancellati anche parzialmente sovrascritti;
 - **Data analysis:** filtraggio e correlazione dei dati ai fini investigativi.



I settori di indagine tecnica



-
- **Computer Forensics**: il più “anziano” ed assestato scientificamente dei settori, coinvolge:
 - **Data mining**: ricerca dei dati a fini decisionali;
 - **Password cracking**;
 - **Tracking**: navigazione internet, email, ecc.
 - **Events correlation**: date ed orari di eventi, attività criminali svolte, ecc..



I settori di indagine tecnica



-
- **Mobile Forensics:** copia “forense” ed analisi di:
 - **SIM:** recupero di dati rubrica e di comunicazione nonché di SMS evidenti e cancellati;
 - **Mobile Equipment:** recupero di dati PIM, multimediali e di comunicazione nonché di SMS/MMS evidenti e cancellati;
 - **Removable Media:** ...computer forensics!



I settori di indagine tecnica



-
- **Mobile Forensics**: il più “attivo” ed investigativamente valido dei settori, coinvolge:
 - **Localization**: tracciamento della posizione (GPS);
 - **Data mining**: ricerca dei dati a fini decisionali;
 - **Events correlation**: date ed orari di eventi, attività criminali svolte, ecc..



I settori di indagine tecnica



-
- **Network and Internet Forensics:** copia “forense” ed analisi di dati presenti su reti di computer:
 - **Email:** tracciamento del mittente;
 - **Siti web:** tracciamento servizi, utenti, provider, chiusura delle pagine, ecc.;
 - **IM, chat & File sharing:** rilevazione dati e posizioni fisiche;
 - **Social networking:** tracciamento servizi, utenti e chiusura dei servizi.



I settori di indagine tecnica



-
- **Network and Internet Forensics:** il più “ampio” dei settori, coinvolge:
 - **Localization:** tracciamento della posizione;
 - **Data mining:** ricerca dei dati a fini decisionali;
 - **Events correlation:** date ed orari di eventi, attività criminali svolte, ecc.;
 - **Investigation...**



I settori di indagine tecnica



-
- **Debit & Credit Card Frauds:** analisi di carte plastificate di pagamento e dei sistemi illegali per la loro duplicazione:
 - **Bancomat (carte di debito):** clonazione fisica;
 - **Carte di credito:** clonazione fisica e virtuale;
 - **Carte prepagate:** clonazione fisica e virtuale;
 - **ATM, POS:** alterazione dei sistemi di prelievo e pagamento.



I settori di indagine tecnica



-
- **Electronic Forensics:** repertamento ed analisi di sistemi elettronici non noti funzionalmente e/o internamente:
 - **Inneschi a distanza:** cellulari modificati;
 - **Sistemi di controllo:** attuatori e rilevatori;
 - **Sensori:** spie elettroniche hardware e software;
 - **Virus, Trojan e Malware** su dispositivi embedded (es. palmtop).



La Sezione Telematica



-
- **Il metodo di indagine (1):**
 - Preservazione attenta della catena di custodia;
 - Documentazione di tutte le attività svolte, dalla strumentazione (LOG) alle deduzioni (reasoning) alla redazione del referto tecnico.
 - Uso di tool hardware/software standard;
 - Uniformazione del metodo per il personale tecnico che svolge le indagini;



La Sezione Telematica



-
- **Il metodo di indagine (2):**
 - Esercizi collaborativi con equipollenti laboratori esteri in EU e USA;
 - Lifelong learning sia in ambito di Forze di Polizia che in quello universitario;
 - Approccio basato sulla copia “forense” dei dati;
 - Approccio garantista: un fatto è avvenuto solo se ci sono evidenze certe mentre dimostrare che un fatto NON è avvenuto si ritiene complesso.
-



La Sezione Telematica



- **Il metodo di repertamento:**
 - Sulla scena del crimine solo in casi estremi;
 - Chi reperta non coincide con chi analizza il reperto;
 - Si evita l'analisi diretta sulla scena del crimine;
 - Laddove risulti indispensabile si effettua la copia "forense" dei dati sulla scena del crimine.



Raggruppamento Carabinieri Investigazioni Scientifiche

Reparto Tecnologie Informatiche

FINE PRESENTAZIONE

<http://www.marcomattiucci.it>
