VIDEOFORENSICS: OBIETTIVI NELLE OPERAZIONI DI ACQUISIZIONE DI UN FILMATO

di Antonmarco Catania

In questo articolo intendiamo individuare gli obiettivi che si deve porre una best practice quando si propone come metodologia di acquisizione di un sistema di videosorveglianza.
I criteri guida da seguire sono sostanzialmente due. Il primo attiene alla capacità di mantenere nel tempo la robustezza della prova informatica, assicurando la genuinità dei reperti. Il secondo, quello di raccogliere, fin da subito, informazioni e dati di contesto, che permettano di esprimere le più accurate valutazioni sui reperti, nella ricostruzione di eventi e nell'identificazione di persone o cose.
Quando si tratta di sistemi di videosorveglianza, la "genuinità del reperto" non può essere assicurata solo in relazione al dato digitale. Devono essere considerati altri aspetti, che tratteremo in questo articolo.

GENUINITÀ DEI DATI DIGITALI

Un sistema di videosorveglianza è costituito da un insieme eterogeneo di apparati hardware. L'acquisizione dei dati digitali contenuti nei singoli componenti del sistema, deve essere realizzata seguendo le best practices più opportune, in relazione alla componente del sistema in questione, di "computer forensics", "mobile forensics", "network forensics" etc.
Questo presupposto, che dovrebbe essere scontato, purtroppo non lo è quando si tratta di filmati prelevati da sistemi di videosorveglianza.
Genuinità dei filmati
Quando si realizza un'acquisizione da un sistema di videosorveglianza, si è interessati alle informazioni contenute all'interno di un video. Bisogna fare attenzione che la genuinità del dato digitale acquisito, contenente il video, non implichi automaticamente, ai fini probatori, la genuinità delle informazioni contenute nel video stesso. La creazione di video "falsi originali", in particolare, costituisce una tipica operazione di anti-forensics.

GENUINITÀ DEI FOTOGRAMMI

All'interno di sistemi di videosorveglianza potrebbero essere archiviati volutamente o ritrovati anche singoli fotogrammi. Analogamente a quanto detto per i filmati, si rende necessario verificarne l'autenticità.

GENUINITÀ DELLA "TIMELINE"

Altro aspetto cruciale, che è necessario salvaguardare durante la fase di acquisizione di un sistema di videosorveglianza, è la fedeltà della "timeline".

In questa fase non deve essere trascurata l'acquisizione di ogni "dato rilevante", che può contribuire a definire una "timeline", che metta in relazione le informazioni contenute nei filmati con l'asse reale dei tempi. Anche pochi minuti o secondi di differenza possono definire scenari completamente diversi in una ricostruzione dei fatti.

RACCOLTA DEI DATI DI CONTESTO

Un sistema di videosorveglianza non viene mai sequestrato completamente. Al più viene sequestrato il videoregistratore digitale. Tipicamente non vengono sequestrati le telecamere o altri elementi che costituiscono il sistema stesso. Questi elementi potrebbero però contenere informazioni preziose, che devono essere acquisite.

Un sistema di videosorveglianza, indipendentemente da quale che sia la tecnologia di cui è composto, è certamente una fonte di informazione ricchissima. Le informazioni contenute in ogni componente del sistema, oltre i video, ne rappresentano il contesto informativo.

In conclusione l'obiettivo di una corretta acquisizione, tramite la raccolta di tutti i dati di rilevanti disponibili, è quello di offrire alla successiva fase di accertamento tutte quelle informazioni necessarie a ricostruire il contesto nel quale si trovava il dato digitale disponibile, in modo da permettere valutazioni con un maggiore indice di confidenza. ■

CORSO DI INTRODUZIONE ALLA VIDEOFORENSICS

Modulo I – *4 Ottobre 2012*

Trezzano s/N Milano – *via C. Colombo 23*

ore 9.00 Registrazione

ore 9.15 Saluti, introduzione della giornata e breve overview sul corso

Dott.ssa Daniela Duranti – *Marketing Manager GSG International*

ore 9.20 Perché la Videoforensics

Dott. Antonmarco Catania – *Esperto in videosorveglianza e Consulente Tecnico Ufficio n.11788 del Tribunale di Milano*

ore 9.30 Cenni di Digital Forensics

Dott. Antonmarco Catania – *Esperto in videosorveglianza e Consulente Tecnico Ufficio n.11788 del Tribunale di Milano*

ore 10.15 Norma tecnica CEI EN - 50.132 10.15

Dott. Antonmarco Catania – *Esperto in videosorveglianza e Consulente Tecnico Ufficio n.11788 del Tribunale di Milano*

ore 10.45 Coffee break

ore 11.00 VIDEOFORENSICS Linee guida per l'acquisizione, la raccolta dei dati rilevanti e l'analisi di un sistema di videosorveglianza

Dott. Antonmarco Catania – *Esperto in videosorveglianza e Consulente Tecnico Ufficio n.11788 del Tribunale di Milano*

ore 13.00 Pausa Pranzo

ore 14. Panoramica normativa di riferimento: *Digital evidence* e processo penale: la l. 48/2008 e i "reati informatici" – Codice dell'Amministrazione digitale e documento informatico" (D. Lgs 82/2005) – Il Codice per la protezione dei dati personali (D. Lgs 196/1993) e gli strumenti di investigazione difensiva (art. 391 bis e ss. C.p.p.) - cenni giurisprudenziali (leading cases Garlasco e Vierika)

Avv. Ivan Francesco Behare – *Esperto in digital forensics, Patrocinante presso la Corte di cassazione*

ore 16.00 Panoramica sui tool

Dott. Ing. Ludovico Paveri Fontana – *Progettista in ambito videosorveglianza ed Esperto in sistemi di analisi videoforense*

ore 16.30 Manipolazione

Dott. Ing. Ludovico Paveri Fontana – *Progettista in ambito videosorveglianza ed Esperto in sistemi di analisi videoforense*

ore 17.15 Case History

Dott. Antonmarco Catania – *Esperto in videosorveglianza e Consulente Tecnico Ufficio n.11788 del Tribunale di Milano*

ore 17.45 ONVIF e la videoforensics

Ing. Gabriele Scarparo – *Software Project Leader esperto di ONVIF ed elaborazione audio*

ore 18.15 Q&A e conclusione del modulo I

S NEWS È MEDIA PARTNER UFFICIALE DELL'INIZIATIVA