Nell'ipotesi di un accadimento drammatico per l'uso dello smartphone durante la guida, è possibile applicare il metodo scientifico alle investigazioni digitali quando nei procedimenti penali occorra stabilire se l'incidente stradale è originato dalla condotta negligente del conducente e, nella fattispecie, a causa proprio dell'utilizzo dello smartphone.

di Roberto Rocchetti

DISTRAZIONE DA SMARTPHONE NELL'OMICIDIO STRADALE. ANALISI DELLE EVIDENZE DIGITALI SULL'ORA ESATTA

Roberto ROCCHETTI, specialista laureato in Scienze della Informazione, è Consulente Tecnico del Pubblico Ministero in materia di Digital Forensics.

In una recente campagna di sensibilizzazione per i giovani tra i 18 e i 29 anni[1], l'Automobile Club Italiano ha riportato che 3 incidenti stradali su 4 sono dovuti a distrazione e l'uso dello smartphone è stato indicato tra le prime cause di distrazione alla guida. Ad esempio, ipotizzando che l'auto viaggi ad una velocità di 130 km orari, una distrazione da smartphone di 1,5 secondi determina una guida non sorvegliata per un tratto di oltre 54 metri.

In tema, il 25 marzo 2016 è entrata in vigore la legge n.41 - 23 marzo 2016, che ha introdotto nell'ordinamento penale i reati di cui agli articoli 589 bis e 590 e 590 bis c.p., rispettivamente per omicidio stradale e lesioni personali stradali gravi e gravissime. La legge fa rientrare indirettamente l'uso dello smartphone nell'articolo 590 *"[…]Se i fatti di cui al secondo comma sono commessi con violazione delle norme sulla disciplina della circolazione stradale[…]"*.

Nell'ipotesi di un accadimento drammatico, è possibile applicare il metodo scientifico alle investigazioni digitali quando nei procedimenti penali occorra stabilire se l'incidente stradale è originato dalla condotta negligente del conducente e, nella fattispecie, a causa dell'utilizzo dello smartphone durante la guida.

Per cercare eventuali responsabilità del conducente si dovrà porre una particolare attenzione al:

1. concetto di *simultaneità* di un evento reale rispetto a dispositivi digitali che registrano l'evento;
2. la validazione e *normalizzazione* dei dati cronologici rispetto al sistema dell'ora esatta UTC;
3. l'identificazione dell'*ora esatta UTC* dell'incidente;
4. la costruzione della *catena di relazioni causa-effetto* partendo dall'evidenza digitale che registra il fatto.

A partire dallo smartphone, l'investigatore digitale dovrà individuare tutte le sorgenti di dati utili all'indagine e procedere all'estrazione, categorizzazione, normalizzazione e validazione dei dati. Le evidenze digitali normalizzate rispetto all'ora esatta (nel formato UTC) permetteranno di identificare eventi precedenti al momento dell'impatto. I dati selezionati saranno usati dal Consulente Tecnico per cercare le relazioni causa-effetto. Il successo dipenderà dalla capacità del CT di individuare tutte le sorgenti di dati utili alla indagine e dalla conoscenza del processi digitali interni ad ogni sistema periziato. I riferimenti bibliografici puntelleranno le singole osservazioni peritali. Il lavoro sarà completo quando sarà possibile costruire la catena delle relazioni causa-effetto passando dal contesto digitale a quello originatrice situato nel mondo reale.

Il Consulente Tecnico (CT) dovrà porre attenzione a quei dati cronologici che hanno una data e ora di registrazione del dato (*timestamp*) prossimi all'orario dell'incidente. Il *timestamp* può essere relativo all'inizio o alla fine di un evento digitale; viene sempre ricavato dall'orologio interno del sistema digitale e la sua rappresentazione può avere differenti formati come "data:hh:mm" o "data:ora:mm:ss", con l'eventuale precisione di un miliardesimo di secondo.

Nel caso di uno smartphone Microsoft, una fotografia scattata ad 1/100 di secondo avrà un *timestamp* corrispondente al momento iniziale dello scatto con la precisione di fabbrica impostata ad un secondo; Il *timestamp* di una telefonata avrà invece l'orario dell'inizio tecnico della conversazione con la precisione di un secondo. Nella catena delle relazioni tra i dati cronologici l'approssimazione sarà imposta dal dato con minor risoluzione temporale. Andranno cercate anche informazioni GPS per identificare se possibile anche le coordinate terrestri del luogo in cui il dato è stato generato. La ricerca dovrà essere estesa a tutti i sistemi che possono aver tracciato eventi utili alla validazione dei dati cronologici estratti dai reperti.

1 http://www.aci.it/archivio-notizie/notizia.html?tx_ttnews%5Btt_news%5D=1825&cHash=96771b8a5963bed51beac69bc68de8c0

Il lavoro del CT dovrà proseguire riposizionando i dati validati sulla linea del tempo dell'ora esatta. Dovrà essere stimata l'ora dell'incidente stradale rispetto all'ora esatta affinché possa essere stabilito se un evento imputabile al conducente è accaduto prima o dopo l'impatto stradale. In ogni sistema digitale il *timestamp* di un evento è l'orario ricavato dall'orologio interno detto *system clock*. Conseguenza di questo fatto è il possibile disallineamento dei dati cronologici rispetto all'ora esatta UTC e anche rispetto ad altri dispositivi che hanno "osservato" il medesimo evento.

Ritorna alla mente il problema della *simultaneità* di un evento rispetto ad due o più osservatori. La definizione della *simultaneità* di Einstein contenuta nella *teoria della relatività speciale* afferma che *il tempo è relativo* ed è locale ad ogni sistema a cui si riferisce. La teoria viene applicata nei sistemi astrofisici e subatomici, nel mondo in cui viviamo è stata fatta usa semplificazione tramite il *sistema dell'ora esatta*, usato in ambito civile in tutto il mondo e basato su un sistema distribuito di *orologi atomici* detto *UTC* (*Tempo Coordinato Universale*) il quale ammette un errore di un secondo ogni cinque miliardi di anni cioè 0,000000000000000006 secondi.
Nei sistemi digitali la generazione della data e dell'ora dipende da un dispositivo elettronico. Il software che se ne prende cura è il *Network Time Protocol* (NTP). Si chiama *NTP client* il servizio software in grado di verificare in rete l'esistenza di un orologio di riferimento esterno (detto *NTP Server*) ed eseguire periodici allineamenti. Anche un *NTP server* avrà bisogno di ricevere l'ora esatta da un sistema analogo ma più in alto nella gerarchia, solitamente un sistema dell'ora esatta.

Ad esempio, una telefonata è registrata in momenti diversi a seconda del punto in cui la si osserva. Riferendoci al modello in cui la chiamata è inizialmente originata dallo smartphone dell'utente, la chiamata viene presa in gestione dalla rete e la chiamata viene aperta dal destinatario, in questi punti di osservazione si possono avere *timestamp*.
Negli smartphone la precisione varia da un secondo a un miliardesimo di secondo a seconda della applicazione usata. È necessario pertanto rapportare tutti i dati cronologici ad un sistema unico di riferimento, cioè l'UTC. Per validare i *timestamp*, il Consulente Tecnico dovrà determinare una stima dello scostamento temporale rispetto all'ora esatta UTC e scartare il dato ove tale stima non fosse calcolabile.

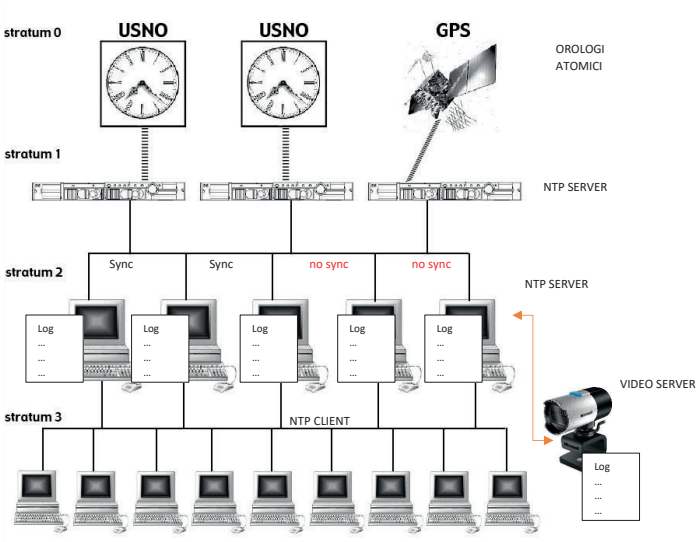

***Figura 1** - Una infrastruttura digitale che implementa correttamente il servizio NTP. Lo Stratum levels definisce la distanza dall'orologio di riferimento.*

Supponiamo che un grave incidente sia stato causato da una automobilista il quale, non accorgendosi di un cantiere stradale, investe gravemente alcune auto in prossimità del cantiere con passeggeri a bordo. Supponiamo inoltre che l'incidente sia stato ripreso da una sistema di videosorveglianza: nel filmato il conducente non sembra tentare alcuna frenata o manovra d'emergenza. Il conducente si salva ma non dimostra segni di malessere. Una delle ipotesi più verosimili che il PM potrà verificare è la *distrazione alla guida da uso dello smartphone*.

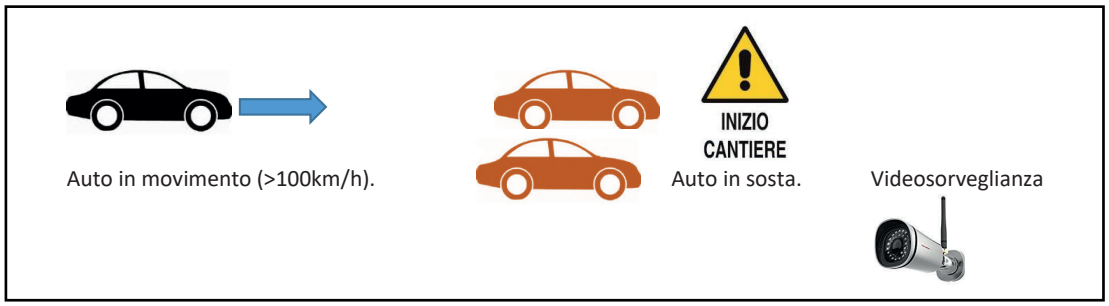

***Figura 2** - Scenario dell'incidente stradale.*

Nel caso in esame si dovranno acquisire in modalità forense (ex art 360 c.p.p.) i dati dello smartphone dell'automobilista (lasciando la SIM interna), i tabulati telefonici, il filmato. Si dovranno estrarre tutti le registrazioni degli eventi ascrivibili all'uso interattivo dello smartphone e procedere con la validazione e normalizzazione delle evidenze rispetto all'ora esatta UTC; ciò dovrà avvenire nel più breve tempo possibile per evitare la cancellazione automatica di alcuni dati utili alla indagine.

Si dovrà determinare l'ora esatta dell'incidente e rapportare le evidenze a quell'ora distinguendo eventi precedenti o successivi. A tale scopo i dati cronologici dovranno essere normalizzati uno ad uno, sulla linea del tempo dell'ora esatta.
La stima dello scarto temporale ∂ di un *timestamp*, richiederà l'analisi della configurazione NTP per verificare quale sistema sia stato usato per aggiornare l'ora. Sarà obbligatorio analizzare i file di log per riscontrare la presenza di eventi di sincronizzazione dell'orologio interno rispetto all'ora dell'NTP server con attenzione agli eventi del periodo di indagine. Si dovrà verificare se l'ora dell'NTP server era stata allineata a UTC.

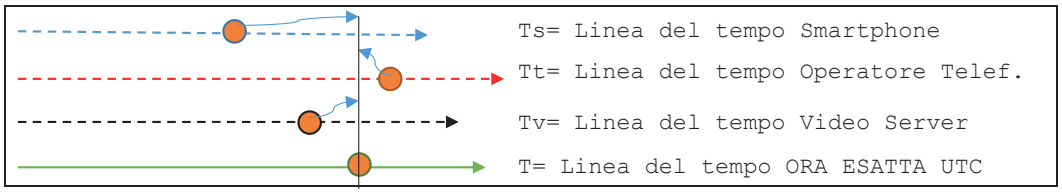

***Figura 3** - Differenze tra diversi system clock e UTC nella rilevazione dell'orario di un evento istantaneo.*

Per normalizzare il *timestamp* a UTC si dovrà applicare la formula: $t_{ora\ esatta} = t_{evento} + \partial$

Per determinare l'ora esatta dell'incidente si procederà dal file video che ha ripreso l'incidente, tipicamente un file AVI, H.264 o Mp4. Generalmente le riprese video riportano impresso il *timestamp* nella forma "data:ora:minuti". Individuato il fotogramma dell'impatto dell'auto il passo successivo sarà quello di determinare l'orario dell'impatto nel modo più preciso calcolando i secondi ed i decimi di secondo. Per sapere se il file video riporta l'ora esatta UTC si analizzeranno i registri log degli eventi NTP a partire dal video server. Tipicamente questi server cancellano i propri log file dopo alcuni giorni e in tal caso potrebbe essere necessario eseguire il recupero forense dai log cancellati dagli hard disk. Per validare l'orario del filmato saranno utili anche gli schemi della architettura dei video server e dei sistemi NTP, i file di log del video server e i file di log dei sistemi di monitoraggio della infrastruttura informatica, questi ultimi potrebbero rivelarci informazioni del funzionamento dei sistemi NTP.

Il CT dovrà richiedere gli stessi dati anche all'operatore telefonico il quale potrebbe rilasciare anche le attestazioni e certificazioni della qualità e correttezza degli orari impressi sui tabulati telefonici relativi al periodo di indagine.
Anche i moderni smartphone implementano NTP e UTC, ciononostante l'accertamento dell'eventuale disallineamento dell'orologio interno è in generale limitato dalla configurazione di fabbrica che fa un uso minimale dei log. Questa limitazione può essere aggirata incrociando i dati dello smartphone con i tabulati telefonici. Ad esempio si dovrà individuare sullo smartphone una telefonata T_1 effettuata poco prima dell'incidente stradale e ricercarla sui tabulati telefonici dell'operatore. Dopo aver accertato che i tabulati riportino l'ora esatta, si potrà calcolare lo scarto temporale:

$$\partial = (\text{orari UTC di } T_1 \text{ dai tabulati telefonici}) - (\text{orario } T_1 \text{ dal registro smartphone})$$

da cui

$$t_{ora\ esatta\ timestamp\ smartphone} = t_{timestamp\ smartphone} + \partial$$

Ad esempio, se l'ultima telefonata prima dell'incidente fosse stata registrata sullo smartphone alle 10:59:57 e sui tabulati alle 11:00:02, la correzione ∂ = 5 secondi.
Applicando questo metodo a tutte le sorgenti di dati il CT potrà riallineare i dati cronologici all'ora esatta UTC. Nell'esempio seguente i dati del registro chiamate dello smartphone indicano che al momento dell'impatto il conducente era al telefono e precisamente dalle ore 11:00:02 (*timestamp* registrato dallo smartphone e normalizzato alle 11:00:02). La linea azzurra indica il tempo UTC dell'ora esatta, in giallo l'evento della ultima telefonata prima dell'incidente riallineato all'ora esatta. In rosso l'ora stimata dell'incidente ed in arancio l'errore di stima dell'ora dell'incidente.

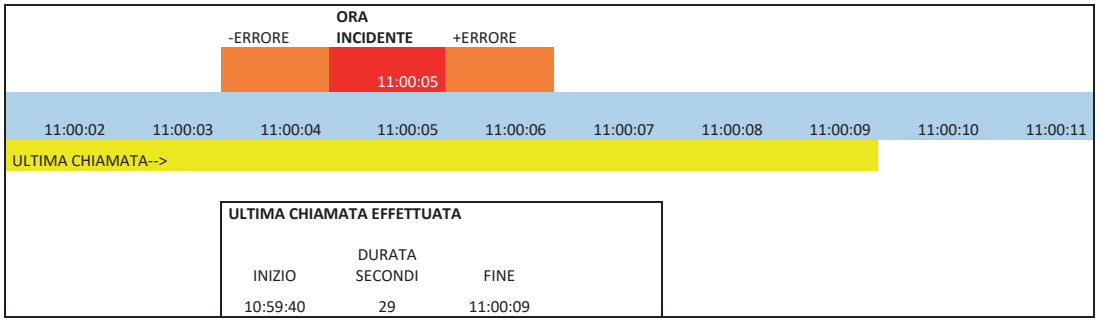

***Figura 4** - Differenze tra diversi system clock e UTC nella rilevazione dell'orario di un evento istantaneo.*

Per ricostruire la catena causa-effetto il CT dovrà infine verificare la relazione tra evento digitale e reale includendo inizialmente tutti i casi possibili per arrivare a selezionare un fatto reale specifico. Per ciascuna evidenza digitale validata e di interesse si dovranno identificare le possibili causa originatrici nel mondo reale.

Nella Digital Forensics il cammino dal digitale al reale è davvero lungo e non sempre lineare; per essere completato con successo dal Consulente Tecnico è richiesta l'adozione di una metodica specifica per il contesto legale in cui si opera, supporto di ausiliari specializzati in tecnologie proprietarie in cui non ci sono riferimenti bibliografici, software specifico e se necessario programmato dal CT, letteratura, prove di laboratorio, precisione nella validazione dei dati, conoscenza nell'identificazione dello spazio delle possibilità e nel processo di ricostruzione delle catene causa-effetto. La relazione tecnica sarà davvero completa se sarà descritto al PM o al Giudice l'eventuale spazio di incertezza ancora esistente. ©