Alibi Informatico

Maria Ausilia Napoli Spatafora[1], Mattia Litrico[2]

Sommario
Con la presenza e l'utilizzo sempre più massiccio di dispositivi elettronici ed informatici, si delinea un nuovo tipo di alibi: il cosiddetto alibi informatico. Questo report intende fornire una dimostrazione di come sia molto semplice crearsi un falso alibi informatico (anche in assenza di competenze informatiche specifiche) e che l'analisi tecnica dei dispositivi dell'indagato possa non far cadere tale alibi.

[1] *Dipartimento di Matematica e Informatica, Università degli Studi di Catania, ausilianapoli@gmail.com*
[2] *Dipartimento di Matematica e Informatica, Università degli Studi di Catania, mattialitrico@gmail.com*

Indice

Introduzione

Il ricorso sempre più massiccio all'uso di strumenti elettronici, informatici e telematici per lo svolgimento di attività lavorative e ricreative, ha determinato una enorme produzione di dati digitali. La pervasività della tecnologia elettronico-informatica ha comportato, pertanto, un sensibile aumento dei casi in cui i computer e gli apparati di comunicazione digitali vengono utilizzati come mezzo per commettere reati e, nel contempo, vengono sottoposti, anche in casi di commissione di reati non prettamente informatici, ad analisi forense al fine di trovare tracce utili alle indagini[1].
È accaduto che tracce informatiche sono servite a dimostrare l'assoluta estraneità dell'indiziato alle accuse formulate nei suoi confronti perché sospettato di essere l'autore materiale del reato; tuttavia, è accaduto, altresì, che un falso alibi sia stato costruito ad arte ricorrendo a tecniche di anti forensics.
L'analisi tecnica di un alibi informatico è del tutto equivalente ad una evidenza digitale e, conseguentemente, possono essere ascritte le stesse peculiarità e lo stesso modus operandi, relativamente all'acquisizione, al trattamento, all'analisi e alla conservazione, tipici della prova digitale.
Relativamente alla variabile tempo, l'alibi può essere contemporaneo o meno all'evento criminoso; per il primo caso è utile la classificazione che Calabrò et Al.[1] hanno fornito per quelle tracce informatiche e non prodotte ad arte:

1. l'imputato ha generato direttamente tracce informatiche su dispositivi distanti dalla scena del crimine;
2. un sistema informatizzato ha eseguito "automaticamente" azioni ed eventi pianificati che, producendo tracce informatiche, simulano la presenza e l'interazione dell'imputato in un luogo diverso dalla scena del crimine;
3. un terzo, persona fisica o sistema automatico, ha registrato tracce che potrebbero giustificare la presenza dell'imputato in luoghi diversi dalla scena del crimine;
4. un terzo, un complice, ha eseguito azione, per nome e per conto dell'imputato, che producono tracce informatiche su dispositivi distanti dalla scena del crimine.

Il nostro obiettivo è di fornire una realizzazione dell'ultimo caso per mezzo delle due fasi, creazione e smontaggio dell'alibi.

1. Creazione dell'alibi

In data 8 aprile 2019 alle ore 17:40 circa la squadra mobile di Catania ha arrestato Giuseppe Tobalo, detto "Pippuzzo", con l'accusa di omicidio plurimo premeditato accadutosi lo stesso giorno intorno alle 17:00: l'imputato è accusato di aver ucciso la propria ex fidanzata (Loredana Idelo) e i suoi genitori in seguito alla rottura del loro rapporto.
Tobalo non si era rassegnato all'idea della fine della loro relazione e ha deciso così di porre fine alla vita dell'ex e dei genitori che, secondo lui, avevano sostenuto la scelta della figlia: questo è il movente dell'omicidio secondo il GIP Sebastiano Battiato.
Durante l'interrogatorio in commissariato Tobalo afferma da subito e con fermezza di essere innocente ed estraneo ai fatti perché durante l'evento criminoso si trovava a casa propria al pc per navigare su internet e connettersi ai propri profili social.

Figura 1. L'abitazione di Loredana Idelo e dei suoi genitori dove è avvenuto l'omicidio

1.1 L'alibi

Giuseppe Tobalo non è una persona sprovveduta e dai vari servizi televisivi aveva compreso quanto siano determinanti e utili le prove digitali, e aveva così deciso di usarle a proprio favore per lo scopo criminale. Avendo competenze informatiche basilari, decise di farsi aiutare da una persona molto fidata e poco sospettabile: la suo ex compagna di scuola Giovanna Carta.
Giovanna Carta è stata da sempre riconoscente a Giuseppe Tobalo per avergli salvato la vita durante la gita scolastica: da quel momento, infatti, Carta disse a Tobalo che aveva un enorme debito nei confronti di quest'ultimo, e Tobalo pensò che questo era il momento giusto per chiedere indietro il favore.
Giuseppe Tobalo chiese all'ex compagna di utilizzare il proprio pc praticando attività sui social e non solo, mentre lui metteva in atto la propria resa dei conti. Carta accettò.

2. La consulenza tecnica

Procedimento penale nˆ 19/285 RGNR - 19/117 GIP relativo all'omicidio plurimo della famiglia Idelo in data 08/04/2019 presso Catania (CT). Con tale incarico si è proceduto alla contestuale nomina del collegio peritale composto da:

- LITRICO MATTIA - afferente al Dipartimento di Matematica e Informatica dell'Università di Catania;
- NAPOLI SPATAFORA MARIA AUSILIA - afferente al Dipartimento di Matematica e Informatica dell'Università di Catania.

La riunione è stata svolta il giorno 9 aprile 2019 presso il Tribunale di Catania.

Quesito Nell'udienza preliminare del 08/04/2019 il GIP formulava al Collegio Peritale il seguente quesito: ***"accertino l'alibi informatico fornito dall'indagato Giuseppe Tobalo in merito all'omicidio avvenuto il 08/04/2019 della famiglia Idelo presso Catania. Si proceda alle seguenti operazioni:***

1. ***Acquisizione del contenuto della memoria volative del PC Lenovo, modello G50-70;***

2. ***Redazione di una timeline, a partire dalle ore 16:40, che indichi con il maggior dettaglio e la maggiore precisione cronologica le attività svolte sul già citato dispositivo.***

Si verifichi la circostanza che l'indagato Giuseppe Tobalo abbia utilizzato il proprio dispositivo per svolgere attività web."

Premesse tecniche La memoria volatile è una memoria informatica che, a differenza della memoria non volatile, necessita dell'alimentazione elettrica continua al fine di mantenere memorizzate le informazioni. Un esempio è la memoria RAM che si trova in tutti i PC [2].
La RAM (Random Access Memory) è, infatti, un tipo di memoria volatile caratterizzata dal permettere l'accesso diretto a qualunque indirizzo di memoria con lo stesso tempo di accesso. Nella memoria RAM vengono copiati (caricati) i programmi che la CPU deve eseguire. Una volta chiuso il programma le modifiche effettuate, se non opportunatamente salvate sul disco rigido o su altra memoria non volatile verranno perse. Per le sue caratteristiche, la RAM viene usata come memoria principale nei dispostivi quali Personal Computer [3].
Un memory DUMP è un processo nel quale il contenuto della memoria viene visualizzato e conservato in caso di crash dell'applicazione o del sistema. Tipicamente il memory dump fornisce informazioni sull'ultimo stato di programmi, applicazioni e del sistema prima che venissero terminati a causa del crash, e mostra quindi l'elenco di tutti i processi attivi, annesse le tabelle dei file aperti (es. cronologia del browser), nell'istante in cui viene effettuato il memory dump [4].

2.1 Analisi Forense

2.1.1 Acquisizione

In data 08/04/2019 alle ore 17.45 il Collegio Peritale ha acquisito il PC di Giuseppe Tobalo ed effettuato il memory dump della memoria RAM con il software open source DumpIt v. 1.3.2.2011041 su pc con Windows 10x64 Home versione 1803. Ne è stata fatta una copia forense del suddetto memory dump con hash SHA-256 `540B952E6FD88481EEDED64890BD383F700229C5E8184BF0279B9F5E19576B4F` in data 08/04/2019 alle ore 20.00.

2.1.2 Analisi tecnica

In prima istanza si è proceduto ad analizzare il memory dump con il software open source Volatility v. 2.6.1. Tale software è capace di estrarre dal dump della RAM la lista dei processi attivi, ma necessita che venga impostato il profilo corretto per procedere all'analisi: tale profilo è altamente dipendente dal Sistema Operativo e dal kernel presente sulla macchina sulla quale è stato effettuato il dump ed è necessario impostarlo correttamente perché il software apprende come il Sistema Operativo memorizza i propri dati.
Il memory dump è stato effettuato su una macchina con Windows 10 e tra i profili forniti dall'applicativo non è stato trovato quello confacente e così questa forma di analisi non si è potuta svolgere.

Successivamente è stato utilizzato un ulteriore software di analisi: Belkasoft Evidence Center 9.4. Si tratta di un software commerciale che, dall'analisi del dump, ha estratto la cronologia web ed effettuato il recupero delle immagini presenti in RAM.

Timeline Per la ricostruzione della timeline, dall'analisi delle immagini non sono state estratte informazioni rilevanti. Bensì la cronologia del browser si è rilevata molto utile in tal senso. Il browser utilizzato è Google Chrome e la tabella 1 mostra le pagine web visitate dalle 16.40 del 08/04/2019 fino al momento dell'esecuzione del dump.
Osservati i tempi di navigazione e non trovata alcuna traccia di automatismi, è verosimile che l'attività sul web sia stata svolta da un soggetto umano.

Tabella 1. Tabella della cronologia web

URL	Data e Ora
https://www.google.it/?gws_rd=ssl	16:48:15
https://www.google.com/search?q=MAC&oq=MAC&aqs=chrome..69i57j69i61l2j35i39j0l2.2599j0j7&sourceid=chrome&ie=UTF-8	16:48:30
https://www.packtpub.com/	16:51:16
https://www.packtpub.com/#	16:51:25
https://www.packtpub.com//?login=1	16:51:43
https://www.youtube.com/	17:31:47
https://www.youtube.com/watch?v=BPNTC7uZYrI	17:32:16
https://twitter.com/	17:36:26
https://twitter.com/	17:36:29
https://www.youtube.com/watch?=1G4isv_Fylg	17:36:32
https://twitter.com/	17:36:39
https://twitter.com/login	17:36:41
https://twitter.com/login	17:40:57
https://twitter.com/sessions	17:40:58
https://t.co/3CX8VOdizy	17:41:30
https://www.lercio.it/il-60-dei-sardi-fa-finta-di-capirsi-quando-parlano-tra-loro/	17:41:31
https://www.lercio.it/revenge-porn-emendamento-lega-sara-reato-pubblicare-foto-dellex-accompagnate-da-testi-di-gio-evan/	17:42:08
https://www.youtube.com/watch?v=5NV6Rdv1a3I	17:42:32

2.2 Conclusioni

L'analisi forense ha trovato delle evidenze digitali che confermano attività umana sul web nel pc dell'indagato Giuseppe Tobalo perché non sono state riscontrate tracce di automatismi in grado di simulare attività sul PC e i tempi di navigazione sono confacenti alle abilità umane. Si tratta della cronologia web del browser utilizzato nella quale sono stati trovate pagine web di social network e di siti di informazione. Sono state recuperate dal memory dump anche immagini salvate automaticamente dal PC, ma dall'analisi delle quali non si è evidenziato alcun riscontro in grado di fornire informazioni utili. Per motivi tecnici non è stato possibile effettuare ulteriori analisi sul memory dump come l'analisi dei processi attivi che avrebbe potuto fornire utili informazioni.

2.3 Allegati tecnici

Si allegano i seguenti file prodotti durante la consulenza dai software utilizzati:

1. **Memory dump**:

   NOME: `DESKTOP-J0UME12-20190408-154503.raw`

   DIMENSIONE: `9921626112 bytes (9462 MB)`

   SHA-256: `540B952E6FD88481EEDED64890BD383F700229C5E8184BF0279B9F5E19576B4F`

2. **Report software Belkasoft**:

   NOME: `DESKTOP-J0UME12-20190408-154503.raw.docx`

   DIMENSIONE: `23261101 bytes (22 MB)`

   SHA-256: `F76E41A856D4CFCEC4053DF33589C8615B22ED606DDE939795C7DAD6C052062`

Conclusioni

L'idea iniziale era di smascherare l'alibi dell'indagato riscontrando nel pc la presenza di un malware che registrava video da webcam; dal ritrovamento e dalla successiva analisi di questi video, si evidenziava che la persona ad aver utilizzato il pc di Tobalo, era bensì la sua complice Carta.
Purtroppo l'analisi non ha evidenziato ciò poiché non è stato possibile analizzare la lista dei processi in esecuzione sul pc tramite il software Volatility che necessita del profilo corretto (dipendente da Sistema Operativo e kernel della macchina sulla quale viene effettuato il dump). Non sono stati trovati altri software free con i quali poter effettuare questa analisi e tra i software commerciali è stato usato Belkasoft Evidence Center che, però, non permette di effettuare l'operazione desiderata. Le difficoltà con Volatility sono state riscontrate su due piattaforme di Sistemi Operativi (Ubuntu 18.10 e Windows 10, entrambe a 64 bit) per le quali era stato appositamente creato lo script che da linea di comando (bash per Ubuntu 18.10 1 e powershell per Windows 10 2) registrava i video in esecuzione all'avvio del pc.
Da ciò si evince che la creazione ad arte di un alibi informatico è semplice (anche senza competenze e strumenti particolari) e resistente all'analisi tecnica qualora non si hanno tutti gli strumenti adatti e le giuste intuizioni.

Listing 1. Malware scritto in linguaggio bash per Ubuntu 18.10

```
#! /bin/bash
DIRECTORY=/tmp/.SeeYou
while :
do
      if [ ! -d "$DIRECTORY" ]; then
            mkdir $DIRECTORY
      fi
      current_time=$(date "+%s")
      path=$DIRECTORY/
         ↪ outfile_$current_time.avi
      #echo $path
      streamer -q -c /dev/video0 -f
         ↪ rgb24 -r 3 -t 00:01:00 -o
         ↪ $path
      sleep 60
done
```

Listing 2. Malware scritto in linguaggio powershell per Windows 10

```
$path = ".\SeeYou"
if(![System.IO.File]::Exists($path)){
      mkdir $path
}
$format = ".mp4"
while($true){
      $timestamp = Get-Date -Format o |
         ↪ foreach {$_ -replace ":",
         ↪ "-"}
      $output = $path+"\"+$timestamp+
         ↪ $format
      .\ffmpeg\bin\ffmpeg.exe -f dshow
         ↪ -s 320x240 -r 30 -vcodec
         ↪ mjpeg -t 60 -i video="Lenovo
         ↪  EasyCamera" $output
      Start-Sleep -s 60
}
```

Riferimenti bibliografici

[1] S. Fratepietro M. Ianulardo G. Nicosia V. Calabrò, G. Costabile. L'alibi infomartico: Aspetti tecnici e giuridici.

[2] Wikipedia, memoria volatile. https://it.wikipedia.org/wiki/Memoria_volatile.

[3] Wikipedia, ram. https://it.wikipedia.org/wiki/RAM.

[4] Techopedia, memory dump. https://www.techopedia.com/definition/20663/memory-dump.