Procedimento R.G. n. 42/2024

Tribunale di Bologna

Descrizione Giudiziale

SPA

vs

SRL

Giuseppe Spathis

Emanuele Di Sante

Matteo Fontana

10 Dicembre 2024

Indice

1. Scopo di questa relazione

La presente relazione riporta i risultati dell'analisi preliminare dei dati digitali acquisiti nell'ambito del procedimento R.G. numero 42/2024, avviato su richiesta dell'Autorità Giudiziaria. Tale analisi è stata condotta al fine di fornire al Giudice una descrizione dettagliata a riguardo del materiale informatico sottoposto a sequestro e delle evidenze emerse durante l'analisi.
Il procedimento è stato avviato a seguito del ricorso presentato dalla società SRL nei confronti della società SPA, con l'accusa di appropriazione indebita di materiale riservato appartenente a SRL. Tra i materiali oggetto di indagine figurano un computer portatile, sequestrato presso l'azienda SPA e detenuto dal titolare di quest'ultima, e una memoria USB, fornita dalla società SRL e contenente disegni industriali di rilevante valore aziendale, che costituiscono patrimonio riservato di SRL e rappresentano l'oggetto del ricorso. SRL sospetta che tali disegni siano stati illecitamente inviati tramite email da un ex dipendente interno all'azienda.
La relazione mira, inoltre, a rispondere ai quesiti posti dal Giudice, verificando la possibile presenza dei dati riservati contenuti nella memoria USB all'interno del disco rigido del computer sequestrato e accertando la/le modalità di diffusione.

2. Metodologia

La presente descrizione si è articolata in due fasi principali.
La prima ha previsto l'acquisizione forense dei dati provenienti dal computer portatile sequestrato e dalla memoria USB depositata dall'azienda SRL. Le operazioni di acquisizione sono state svolte garantendo l'integrità delle prove digitali, mediante l'utilizzo di strumenti certificati conformi agli standard di catena di custodia (vedi cap. 3 per ulteriori dettagli).
Mentre nella seconda fase, i dati sono stati sottoposti a un'analisi sommaria utilizzando il software Autopsy, versione 4.21.0, con l'intento di ottenere una panoramica preliminare utile ai fini del presente procedimento.
Successivamente, la fase di ricerca delle informazioni si è concentrata su diverse tecniche d'indagine. Tra queste, la ricerca per parole chiave ha avuto particolare importanza: alcuni termini sono stati utilizzati per analizzare sia i nomi dei file sia i loro contenuti (vedi cap. 6.1 per ulteriori dettagli). Parallelamente, altre sezioni specifiche sono state esplorate per raccogliere ulteriori informazioni: i metadati sono stati esaminati per comprendere la struttura e la cronologia dei file, la sezione di Autopsy "web downloads" ha fornito informazioni sui file scaricati tramite il web e "deleted files" ha permesso il recupero di elementi cancellati. Inoltre, la sezione di Autopsy "extension mismatch detected" è stata analizzata per identificare possibili alterazioni nell'estensione dei file rispetto al loro contenuto effettivo.
Ciò ha portato le risultanze e conclusioni riportate in seguito.

3. Acquisizioni forensi

Si è acquisita in copia forense:

1. Il contenuto del computer del titolare della società SPA.

2. Il contenuto della chiavetta USB depositata dalla società SRL contenente l'oggetto del ricorso.

3.1 Computer del titolare dell'azienda SPA

Il computer in esame è stato acquisito tramite il comando `dd` dal sistema Kali Linux avviato in modalità live per garantire la non alterazione delle prove digitali. È stata acquisita una copia integrale della memoria di massa del disco rigido presente nel dispositivo, comprensiva di tutti i suoi settori, inclusi quelli non allocati e le aree potenzialmente cancellate. Si faccia riferimento alla sezione 6.2 per ulteriori dettagli.

3.2 Chiavetta USB dell'azienda SRL

L'acquisizione della chiavetta USB è stata condotta seguendo una procedura analoga a quella utilizzata per il computer portatile. Anche in questo caso, il comando dd è stato eseguito su un sistema Kali Linux avviato in modalità live. Si faccia riferimento alla sezione 6.2 per ulteriori dettagli.

4. Risultanze

A seguito del processo di analisi del disco sono stati rinvenuti diversi file e metadati significativi, che offrono indicazioni riguardanti la presenza del materiale oggetto del ricorso. La tabella sottostante rappresenta le informazioni relative ai file di interesse ritrovati nell HDD del pc analizzato.

Nome File	**Percorso**	**Hash md5**	**Hash SHA256**
Dc7.pdf	`/img_acq.img/vol_vol2/WINDOWS/system32/`	8222271c02ea45d5a794829757e7a1b5	6b18239374b9c228813b2019370f56b3c27cf03478f6309e563a84a124221142
tavola_5.dll	`/img_acq.img/vol_vol2/WINDOWS/system32/tavola_5.dll`	8222271c02ea45d5a794829757e7a1b5	6b18239374b9c228813b2019370f56b3c27cf03478f6309e563a84a124221142
tavola_5.pdf	`/img_acq.img/vol_vol2/Documents and Settings/pinco/My Documents/tavola_5.pdf`	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
imap.gmail.com - Inbox.dbx	`/img_acq.img/vol_vol2/Documents and Settings/pinco/Local Settings/Application`	5bdecaa66bd3a33e4a0ded267aed0d42	3f8fc1bc107aa209402069cca8c685086e32514465dd7536232e85763d2f331d

Nome File	Percorso	Hash md5	Hash SHA256
	Data/Identities/{02DF6D25-D836-4F57-B441-1C0E07BF8F46}/Microsoft/Outlook Express/imap.gmail.com - Inbox.dbx		

4.1 Documenti rinvenuti

4.1.1 Dc7.pdf

È stato riscontrato che il file *Dc7.pdf*, corrisponde visivamente al file *tavola 5.pdf* presente sulla chiavetta USB consegnata dall'azienda SRL. La somiglianza visiva tra i due documenti è evidente, inclusi segni scritti a mano, che appaiono identici.
La presenza del file *dc7.pdf:Zone.identifier* (con valore di ZoneId=4) nella sezione *Web Downloads* di Autopsy, indica che il documento in questione è stato scaricato dal web. Il valore *Zoneid* equivalente a 4 evidenzia la provenienza da "URL con restrizioni".

4.1.2 tavola_5.dll

All'interno della cartella "System32" è stato rinvenuto un file con estensione .dll ma file type riportato nei metadati corrispondente ad "application/pdf". Una volta ispezionato tramite il tool "application" di Autopsy, questo documento corrisponde visivamente al file proprietario dell'azienda tavola_5.pdf presente nella chiavetta USB, come nel caso del documento descritto nella sezione 4.1.1, presentando corrispondenze anche dei segni a mano presenti nella seconda pagina del documento.

4.1.3 tavola_5.pdf

È stato trovato nel disco rigido del pc il file *tavola_5.pdf* nella sottosezione di Autopsy "File System" di "Deleted Files"; essendo stato eliminato, nei metadati si riscontra avere size 0, essere in una porzione non allocata del file system e campi "Modified", "Accessed", "Created", "Changed" uguali a 0000-00-00 00:00:00.

4.2 Ricerca per parole chiave

Di seguito riportiamo una ricerca che abbiamo effettuato nell'HDD del pc tramite l'apposito tool di Autopsy.
La ricerca «tavol» ha individuato 17 file; di questi, i file rilevanti ai fini dell'analisi sono i seguenti:

- *Dc7.pdf* e *tavola_5.pdf*, di cui si è già parlato nella sezione 4.1.
- *imap.gmail.com - Inbox.dbx*, utile per l'analisi delle email, ulteriori informazioni dettagliate sono presenti nella sezione 4.3.

- *$LogFile*, è particolarmente utile poiché, tenendo traccia delle attività svolte sul computer, è possibile individuare attività legate ai file contenenti i disegni in oggetto.

4.3 Mail rinvenute

Tramite l'analisi del contenuto estratto da Autopsy, relativo al file *imap.gmail.com - Inbox.dbx*, sono state esaminate le email ricevute all'indirizzo di posta elettronica mtoscani.spa@gmail.com . L'attenzione è stata rivolta, in particolare, a specifiche comunicazioni ricevute dall'indirizzo adirosa.srl@gmail.com . Tra queste, risulta di particolare rilevanza una email che include come allegato il file denominato *tavola_5.pdf,* come evidenziato in Figura 1.
Data la dicitura "srl" presente all'interno dell'indirizzo mail adirosa.srl@gmail.com è possibile che esso appartenga ad un dipendente dell'azienda SRL.

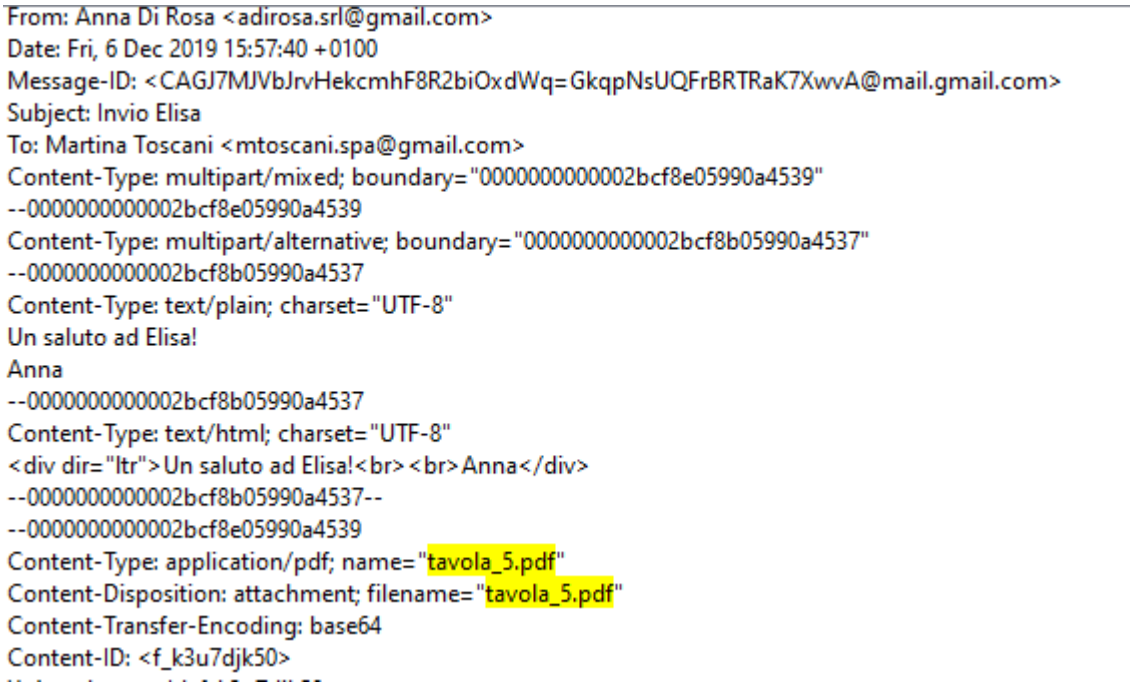

Figura 1: screenshot del file imap.gmail.com - Inbox.dbx aperto tramite il tool application di Autopsy. Viene mostrato lo scambio di messaggi avvenuto tra mtoscani.spa@gmail.com e adirosa.srl@gmail.com e il corrispettivo invio del file tavola_5.pdf come allegato.

5. Conclusioni

Attraverso le diverse tecniche di Digital Forensics sono stati trovati i seguenti file rilevanti:

- Dc7.pdf
- tavola_5.dll
- tavola_5.pdf
- imap.gmail.com - Inbox.dbx

Nel file *imap.gmail.com - Inbox.dbx* si evince che sia stato inviato il file *tavola_5.pdf* da Anna di Rosa, sospetta dipendente dell'azienda SRL come si evince dal suo indirizzo di posta elettronica adirosa.srl@gmail.it , a Martina Toscani.
Inoltre è stato eliminato un file *tavola_5.pdf*, dal nome corrispondente al file inviato da Anna,

mentre i file tavola_5.dll e Dc7.pdf corrispondono in contenuto al documento tavola_5.pdf presente nella chiavetta depositata.
In conclusione quindi è evincibile che il contenuto del documento tavola_5.pdf presente nel portatile sequestrato sia stato inviato tramite email a Martina Toscani e che, successivamente, sia stato collocato all'interno della cartella "system32" con il nome di *tavola_5.dll,* mentre una copia corrispondente dal nome *Dc7.pdf* sia stata invece cestinata.
La presenza di un file eliminato, denominato *tavola_5.pdf* in uno spazio non allocato del disco rigido del pc, segnala che un file dal medesimo nome è stato presente nel computer.

6. Appendici

6.1 Spiegazione dettagliata ricerca per parole chiave

La ricerca per parole chiave avviene sia tra i nomi dei file, sia nel loro contenuto. La ricerca per nome dei file individua i file che nel proprio nome contengono una, o più, parole chiave e la ricerca per contenuto dei file, invece, analizza ogni file cercando al suo interno le parole chiave. È opportuno evidenziare, infine, che la ricerca delle parole chiave non fa distinzione tra caratteri maiuscoli e minuscoli, sia nel nome sia nel contenuto dei file. Vale la pena segnalare che un singolo file potrebbe essere riportato più volte tra i risultati delle ricerche perché contenente più di una parola chiave.

6.2 Spiegazione dettagliata acquisizioni forensi

L'acquisizione è stata effettuata con Kali Linux 2024.3 Live 32 bit (disponibile da https://www.kali.org/get-kali/#kali-live) avviando il sistema in Forensics mode.
la versione del tool `dd` utilizzato è la 9.4, ed il comando lanciato è stato

```
sudo dd if=/dev/sda
of=/media/kali/9C33-6BBD/forensics_acquisizione/acq.img bs=512
conv=noerror,sync status=progress iflag=fullblock
```

Lo stesso tool è stato usato per acquisire i contenuti della chiavetta, con la medesima versione e modalita' di Kali linux:

```
sudo dd if=/dev/sdd
of=/media/kali/9C33-6BBD/forensics_acquisizione/usb.img bs=512
conv=noerror,sync status=progress iflag=fullblock
```

I dettagli dell'acquisizione sono riassunti nella seguente tabella:

Nome Immagine	Origine	Metodologia	Riferimento	hash
acq.img	Computer portatile DELL mod. Latitude D520 PP17L Serial number 1Q64M2J	Kali Linux 2024.3 Live dd (coreutils) 9.4	3.1	MD5 CE2DFF5FCCB74BC9A91E8EB84C52A0A5 SHA1 FA783D6A52CCAEA029F1164E39D89C39DAA8D553

usb.img	USB depositata dall'azienda SRL	Kali Linux 2024.3 Live dd (coreutils) 9.4	3.2	MD5 FBA4A109EB378FCE01755EFC0EA66126 SHA1 02709E413600DC7FD5C642B882B855A1EECB1F93