UNIVERSITÀ DI BOLOGNA

Dipartimento di Informatica - Scienza e Ingegneria
Corso di Laurea Magistrale in Informatica

Progetto corso di Digital Forensics
A.A. 2024/25

23Bottles S.p.A. vs Partolini S.r.l.

Relazione parte Convenuta

Davide De Rosa — Matricola: 0001186536
Marco Coppola — Matricola: 0001170490
Valerio Pio De Nicola — Matricola: 0001170425

Indice

1 Informazioni amministrative **3**

2 Svolgimento dell'indagine **4**
2.1 Obiettivo della relazione 4
2.2 Sommario esecutivo 5

3 Acquisizioni forensi **6**
3.1 PC Portatile Compaq 6
3.2 Chiavetta USB 6

4 Svolgimento delle Analisi **7**
4.1 Ricerca per codici Hash 7
4.2 Ricerca per email e keyword 8
4.2.1 Posta inviata.dbx 9
4.2.2 Posta eliminata.dbx 9
4.2.3 Bozze.dbx 9
4.2.4 Posta in arrivo.dbx 9
4.3 Ricerca per dispositivi collegati 9
4.4 Ricerca nei log di sistema 9
4.4.1 Cambi di data e ora 10
4.4.2 Accessi al sistema 10
4.5 Ricerca nei registri di sistema 10
4.6 Ricerca per file 11

5 Timeline degli eventi **15**

6 Risultati delle Analisi **18**
6.1 Analisi USB 18
6.2 Analisi HDD 18

7 Conclusioni **21**

8 Materiale **22**
8.1 Materiale depositato 22
8.1.1 001_Richiesta informazioni sulle opzioni di spedizione.eml 22
8.1.2 002_Richiesta informazioni sulle opzioni di spedizione.eml 23
8.1.3 003_Solito.eml 24
8.1.4 004_Conferma della Proposta e Richiesta di Preventivi.eml 24
8.1.5 005_Solito.eml 25

8.1.6 006_Conferma della Proposta e Richiesta di Preventivi.eml 26
8.1.7 _Quantitativo Totale di Merce per Spedizione.eml 26
8.1.8 Quantitativo Totale di Merce per Spedizione-3.eml 27
8.1.9 Quantitativo Totale di Merce per Spedizione-2.eml 28
8.1.10 Solito.eml 28
8.1.11 Reclamo per Mancanza di Merce alla Consegna.eml 29
8.1.12 Reclamo per Mancanza di Merce alla Consegna-2.eml 30
8.1.13 Reclamo per Mancanza di Merce alla Consegna-3.eml 31
8.1.14 Preventivo.docx 32
8.1.15 Consegna.pdf 33
8.2 Materiale acquisito 34
8.2.1 Seagate HDD 500GB 34
8.3 Informazioni aggiuntive 35
8.3.1 Informazioni HDD 35
8.3.2 Informazioni "Laura" 35
8.3.3 Informazioni Hard Disk collegato 35

1. Informazioni amministrative

L'azienda **23Bottles S.p.A.**, d'ora in poi *23Bottles*, decide di presentare istanza di ricorso nei confronti dell'azienda di trasporti **Partolini S.r.l.**, d'ora in poi *Partolini*, sostenendo che quest'ultima non abbia garantito il servizio di trasporto pattuito contrattualmente. Tale supposizione nasce da un recente scambio di e-mail tra 23Bottles e uno dei clienti, il quale afferma di aver ricevuto da Partolini un numero inferiore di unità dei prodotti di 23Bottles rispetto a quanto richiesto.

L'azienda 23Bottles ha inoltre depositato al momento della presentazione della richiesta di ricorso, una *memoria USB* contenente le e-mail scambiate con il cliente e le fatture fornite da Partolini. Questo materiale costituisce *patrimonio aziendale riservato*, ed è l'oggetto del ricorso.

Il Giudice ha autorizzato il sequestro del materiale informatico, qualsiasi supporto in grado di immagazzinare dati, in possesso dall'azienda Partolini. Si deve analizzare il materiale sequestrato, ossia il computer portatile detenuto dalla segretaria, che fungeva da tramite di 23Bottles e lo spedizioniere dell'azienda Partolini.

Il materiale sequestrato è stato fisicamente consegnato ai consulenti tecnici delle parti. Il contenuto della memoria USB è reperibile presso il sito *Virtuale* del corso.

Il Giudice ha posto il seguente quesito, al quale i consulenti delle parti e del Giudice sono chiamati a rispondere:

> *"Considerando che oggigiorno le aziende si avvalgono di una serie di servizi per la gestione delle proprie attività. Queste aziende possono essere vittime di frodi: in queste situazioni, investono risorse finanziarie in servizi che promettono beneici ma, al contrario, causano danni all'attività. Si chiede agli specialisti forensi di veriicare la veridicità delle affermazioni di parte attrice sulla base del materiale depositato e quello sequestrato."*

2. Svolgimento dell'indagine

Viene premesso che il materiale d'indagine del caso consiste in due supporti di memorizzazione dati:

- La memoria USB depositata da 23Bottles, denominata d'ora in poi *USB*, contenente le email scambiate tra 23Bottles e Partolini e i due file inerenti al preventivo ed alla consegna;
- L'Hard Disk del PC sequestrato alla segretaria di Partolini, denominato d'ora in poi *HDD*, contenente i dati del computer utilizzato dalla segretaria dell'azienda Partolini.

2.1. Obiettivo della relazione

La presente relazione fornisce un'analisi dettagliata delle criticità emerse nella documentazione presentata dalla controparte durante il procedimento investigativo.
L'obiettivo è identificare eventuali discrepanze o incongruenze che potrebbero incidere sulla validità delle prove. Il documento è strutturato per esaminare in modo approfondito ogni elemento contestato, offrendo una valutazione basata su prove concrete.

Sebbene l'analisi riguardi esclusivamente la documentazione fornita dalla controparte, non si esclude la possibilità di interpretazioni differenti rispetto a quanto prospettato. I fatti oggetto dell'indagine potrebbero essere letti in modi diversi a seconda delle circostanze.
Nel contesto dell'indagine, il Giudice ha autorizzato il sequestro del materiale informatico in uso presso Partolini, inclusi dispositivi di memorizzazione dati. Particolare attenzione è stata rivolta al computer portatile utilizzato dalla segretaria, che fungeva da intermediaria nei rapporti tra 23Bottles e Partolini.
Il materiale sequestrato è stato successivamente affidato ai consulenti tecnici delle parti per le opportune verifiche.
Inoltre, i file contenuti nella memoria USB depositata da 23Bottles sono disponibili per l'analisi.

2.2. Sommario esecutivo

L'indagine ha seguito tre fasi distinte:

1. **Acquisizione USB** [8.1]: inizialmente, è stata condotta un'analisi dei dati contenuti nella memoria USB fornita da 23Bottles, al fine di ottenere una panoramica completa degli eventi e delle comunicazioni. Tale attività ha previsto la sintesi delle email e l'analisi degli eventi associati. Durante questa fase, sono stati identificati gli indirizzi email di rilevanza ai fini della dinamica investigativa.
   Inoltre, si è resa necessaria l'analisi di email cifrate, che sono state successivamente decifrate per permettere un'indagine approfondita dei contenuti. Infine, è stato possibile ricostruire gli eventi in una linea temporale, garantendo una comprensione dettagliata della sequenza degli avvenimenti e delle interazioni tra le parti coinvolte.

2. **Acquisizione HDD** [8.2.1]: successivamente, è stata eseguita un'acquisizione forense dell'hard disk del computer utilizzato dalla segretaria dell'azienda Partolini, per garantire l'integrità dei dati raccolti e prevenire la contaminazione delle prove.

3. **Analisi comparativa**: per concludere, è stata condotta un'analisi comparativa dei dati, confrontando le informazioni presenti nella memoria USB con quelle acquisite dal computer di Partolini. L'obiettivo di questa fase è stato quello di identificare corrispondenze o discrepanze, al fine di confermare o confutare le affermazioni avanzate da 23Bottles.

Questo approccio ha permesso di condurre un'analisi forense rigorosa e completa, fornendo una panoramica dettagliata dei fatti e delle circostanze oggetto della controversia legale.

3. Acquisizioni forensi

3.1. PC Portatile Compaq

In conformità all'autorizzazione del Giudice per il sequestro del materiale informatico appartenente all'azienda Partolini, questa sezione descrive il processo di analisi del materiale confiscato.
Tra gli elementi sequestrati vi è il computer portatile utilizzato dalla segretaria, figura chiave nell'intermediazione tra l'azienda Partolini e 23Bottles.

Per acquisire l'immagine forense del computer, abbiamo inizialmente smontato il dispositivo ed estratto il disco. Abbiamo successivamente collegato il write blocker – modello *Tableau TK8U* – al computer e successivamente il disco al write blocker, seguendo la sequenza prestabilita. Una volta alimentati i dispositivi, abbiamo avviato **FTK Imager**[1].

Abbiamo eseguito una verifica preliminare dell'integrità del dispositivo tramite FTK Imager. Il valore hash ottenuto ha confermato che non erano state apportate modifiche al dispositivo sorgente, permettendoci così di procedere con la creazione dell'immagine forense.

Per il formato dell'immagine, abbiamo scelto il **formato E01**, considerato il più adatto alle esigenze investigative del caso.

3.2. Chiavetta USB

La chiavetta USB fornita da 23Bottles è stata acquisita utilizzando FTK Imager come volume logico, permettendoci di ottenere anche i diversi Hash dei documenti presenti al suo interno.

Viene ignorato il contenuto della cartella __MACOSX, directory di sistema aggiunta automaticamente da MacOS quando si comprime o archivia un insieme di file.

[1] FTK Imager, strumento gratuito fornito da *AccessData*, offre diverse funzionalità, tra cui la possibilità di generare un valore hash per il dispositivo sorgente, creare un'immagine forense e successivamente calcolare un altro valore hash per verificare l'integrità del processo, assicurando l'assenza di modifiche al dispositivo originale.

4. Svolgimento delle Analisi

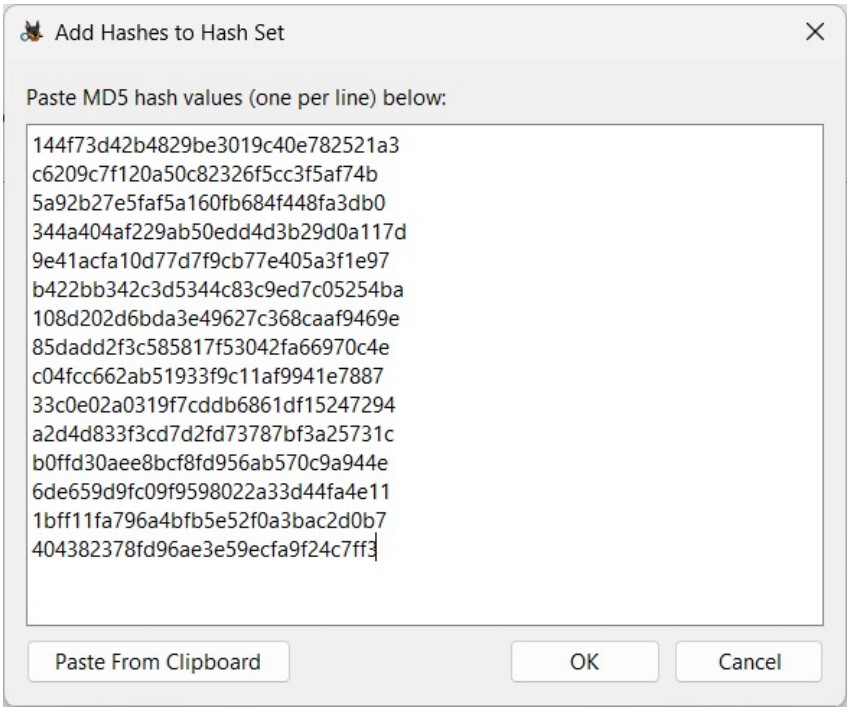
Lo strumento principale utilizzato nel processo di analisi è **Autopsy**, strumento gratuito fornito da *SLEUTH KIT LABS*. Tale strumento ha permesso di analizzare l'immagine dell'HDD acquisita in precedenza, tramite diverse funzionalità disponibili al suo interno.

Di seguito vengono riportate tutte le analisi effettuate sull'immagine.

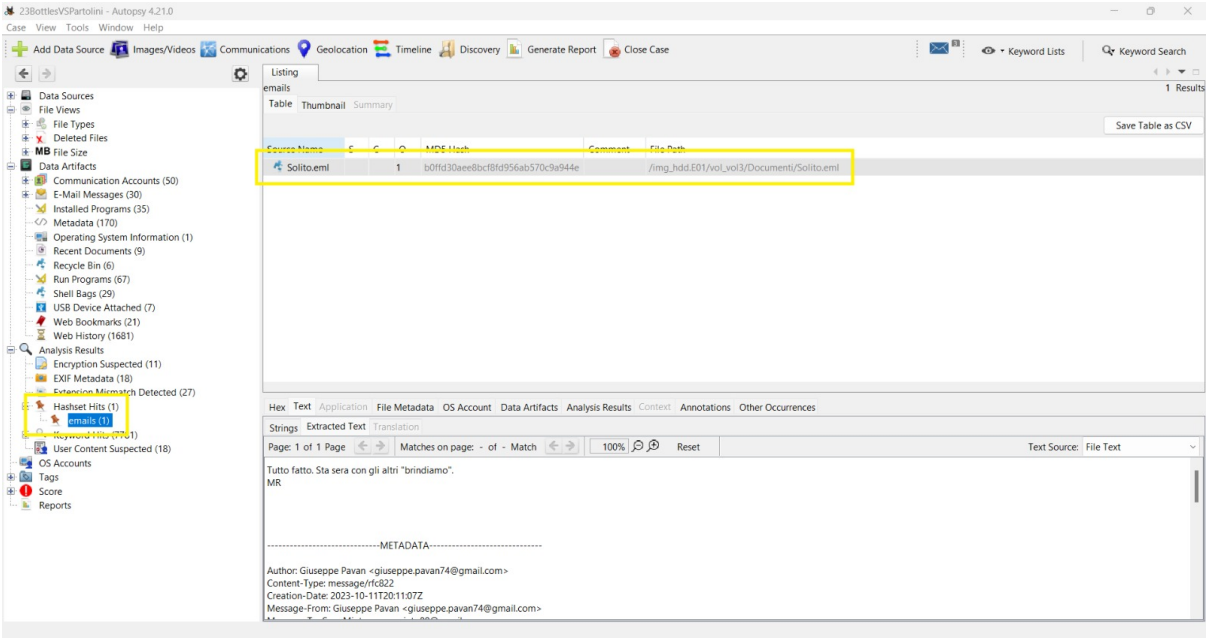
4.1. Ricerca per codici Hash

Un primo approccio di analisi è stato quello di cercare una corrispondenza, tramite ricerca per codici hash, tra i file presenti sulla memoria USB e l'HDD acquisito.

Viene quindi creato un **Hash Set** all'interno di Autopsy per effettuare la ricerca su tutti gli **MD5** inerenti ai file presenti nella USB.



Una volta salvato l'Hash Set, Autopsy esegue la **ricerca tramite Hash** all'interno dell'HDD trovando **soltanto un unico Hashset Hit**.



L'Hashset Hit riguarda l'unica email trovata all'interno dell'HDD sequestrato, ovvero la email "**Solito.eml**" [8.1.10].

4.2. Ricerca per email e keyword

Non avendo trovato tutte le corrispondenze tra USB e HDD abbiamo effettuato una ricerca tramite email e keyword, utilizzando tutte le parole chiave inerenti alle email ed ai documenti presenti nella memoria USB. Alcune delle keyword utilizzate sono:

- Cinzia Zingaro
- Partolini
- 23Bottles
- Consegna
- Pavan

Alcune degli indirizzi email trovati sull'HDD sono:

- andrea.zanatta@TTBottles.com
- giulia.zingaro@partolini.com
- sara.minto80@gmail.com
- giuseppe.pavan74@gmail.com

Questo ci ha portato a trovare le restanti email nei **database offline** di *Microsoft Outlook*:

- Posta inviata.dbx
- Posta eliminata.dbx
- Bozze.dbx
- Posta in arrivo.dbx

Nel dettaglio, vengono specificate le diverse email trovate per ogni database offline:

4.2.1 Posta inviata.dbx

- 002_Richiesta informazioni sulle opzioni di spedizione.eml [8.1.2]
- 003_Solito.eml [8.1.3]
- 006_Conferma della Proposta e Richiesta di Preventivi.eml [8.1.6]
- Quantitativo Totale di Merce per Spedizione-2.eml [8.1.9]
- Reclamo per Mancanza di Merce alla Consegna-2.eml [8.1.12]

4.2.2 Posta eliminata.dbx

- 005_Solito.eml [8.1.5]
- Quantitativo Totale di Merce per Spedizione-3.eml [8.1.8]
- Reclamo per Mancanza di Merce alla Consegna.eml [8.1.11]

4.2.3 Bozze.dbx

- Quantitativo Totale di Merce per Spedizione-3.eml [8.1.8]

4.2.4 Posta in arrivo.dbx

- 001_Richiesta informazioni sulle opzioni di spedizione.eml [8.1.1]
- 004_Conferma della Proposta e Richiesta di Preventivi.eml [8.1.4]
- Solito.eml [8.1.10]
- Reclamo per Mancanza di Merce alla Consegna-3.eml [8.1.13]

4.3. Ricerca per dispositivi collegati

Con l'utilizzo della sezione *USB Device Attached* di Autopsy abbiamo potuto osservare il collegamento al computer di Laura di un hard disk esterno (*Western Digital My Passport WDBPKJ* [8.3.3]), con log di collegamento **01/05/2023 9:52:36 GMT**.

4.4. Ricerca nei log di sistema

Osservando i log di sistema all'interno della directory
`C:/Windows/System32/winevt/Logs/` è stato possibile osservare diversi eventi.

4.4.1 Cambi di data e ora

Tramite il file **System.evtx** sono stati osservati diversi cambi di data e ora effettuati dall'utente Laura. Di seguito alcuni dei log sospetti:

- **Da** 2002-01-11 **a** 2023-10-04 → *Salto di 21 anni*
- **Da** 2023-10-06 **a** 2023-05-01 → *Retrocesso di 5 mesi*
- **Da** 2023-10-23 **a** 2023-10-18 → *Retrocesso di 5 giorni*
- **Da** 2023-10-24 **a** 2023-10-23 → *Retrocesso di 1 giorno*
- **Da** 2023-05-01 **a** 2024-05-01 → *Avanzato di 1 anno*

4.4.2 Accessi al sistema

Tramite il file **Security.evtx** sono stati osservati diversi **Logon** al sistema. Di seguito alcuni dei log:

- **Nome account**: LAURA-PC$ – **Tipo di accesso**: 5 – **Data**: 01/05/2023 9:52:39
- **Nome account**: LAURA-PC$ – **Tipo di accesso**: 2 – **Data**: 01/05/2023 9:52:42
- **Nome account**: LAURA-PC$ – **Tipo di accesso**: 5 – **Data**: 01/05/2023 9:52:43
- **Nome account**: NULL SID – **Tipo di accesso**: 3 – **Data**: 01/05/2023 9:52:46
- **Nome account**: LAURA-PC$ – **Tipo di accesso**: 5 – **Data**: 01/05/2023 9:52:53
- **Nome account**: LAURA-PC$ – **Tipo di accesso**: 5 – **Data**: 01/05/2023 9:54:47

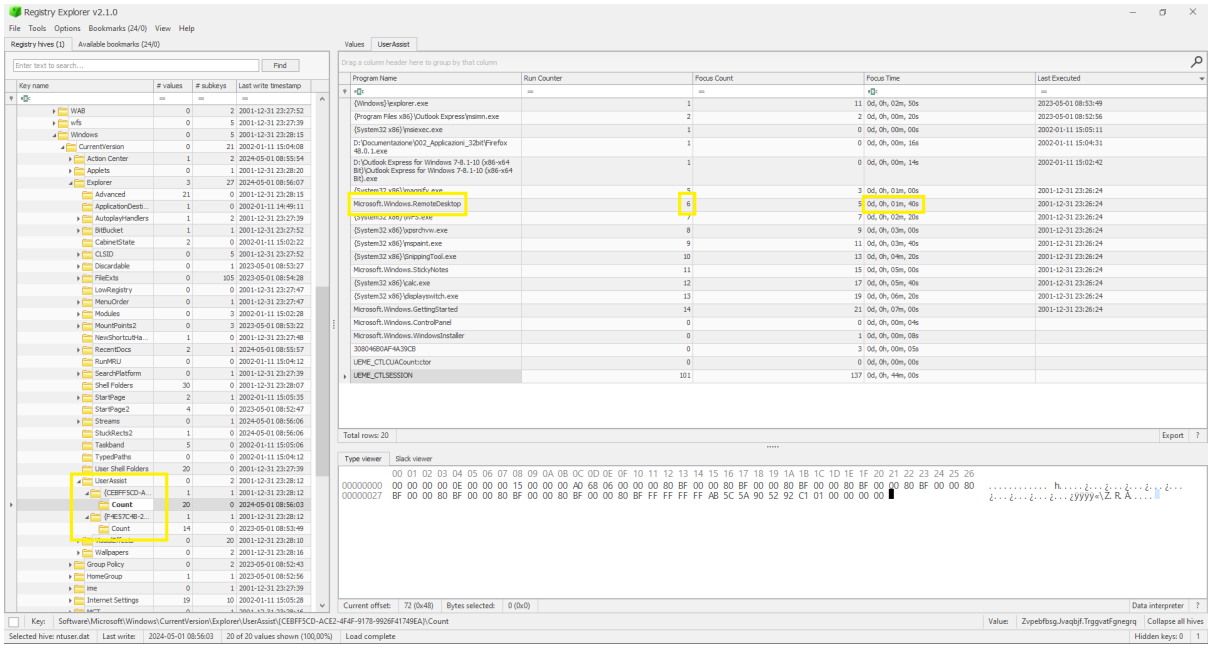
Vengono di seguito spiegati brevemente i diversi tipi di accesso:

- **Tipo 2**: utente che accede fisicamente al pc, tramite schermata di login
- **Tipo 3**: utente che accede da remoto via rete
- **Tipo 5**: login effettuato da servizi di Windows

4.5. Ricerca nei registri di sistema

Per osservare al meglio i registri di sistema abbiamo utilizzato il software **Registry Explorer**, strumento gratuito offerto da *ericzimmerman*.
Il focus principale è stato sugli hive presenti nella directory `C:/Windows/System32/config`. Nello specifico, abbiamo analizzato *sam*, *system*, *security* e *software*. Analizzandoli non abbiamo trovato informazioni rilevanti.

E' stato successivamente analizzato anche il file **NTUSER.dat**, presente nella directory `C:/Users/Laura`. Tramite l'utilizzo di Registry Explorer abbiamo potuto osservare diverse entry, tra cui una che fa riferimento all'utilizzo di un software di Accesso Remoto.



Inoltre, all'interno di NTUSER.dat, è stato riscontrato l'ultimo accesso dell'utente Laura al computer, in data *01/05/2023 9:56:10*.

4.6. Ricerca per file

Durante l'analisi del contenuto del filesystem effettuata con Autopsy, è stato evidenziato come sospetto il file **Important Document.zip**, presente nella directory `C:/Users/Laura/Desktop`. Il motivo della segnalazione del file è dovuto ad un'alta entropia dei suoi contenuti, suggerendo che il file fosse criptato.
Eseguendo infatti il comando per calcolare l'entropia del contenuto di un file:

```
ent Important Document.zip
```

si ottiene il valore **7.999983** bits per byte, indicando che i bit sono distribuiti uniformemente nel contenuto, quasi vicino al massimo teorico di 8.

Supponendo dunque che il file fosse criptato abbiamo provato ad identificare il tipo di cifratura utilizzando **hashcat**, eseguendo il comando:

```
hashcat Important Document.zip
```

L'assenza di header o di una lunghezza specifica del file non suggeriscono una tipologia specifica di cifratura, indicando dunque che si tratta di una full-text-encryption effettuata con algoritmi come **VeraCrypt** o **TrueCrypt**.
Data la numerosità di algoritmi di cifratura di questo tipo abbiamo deciso di non procedere con la decifrazione del contenuto in bruteforce, ma piuttosto analizzare altre strade.

Il sistema operativo Windows permette agli utenti di cifrare un file con una chiave che è generata a partire dalle informazioni di login dell'utente. La cifratura del file appare trasparente all'utente in quanto dopo aver effettuato il login il file viene "*sbloccato*". In eventuali acquisizioni forensi dunque il file verrà mostrato nella sua natura criptata.

Per poter accedere al file è dunque necessario effettuare il login come Laura. Abbiamo deciso di effettuare il boot del disco.

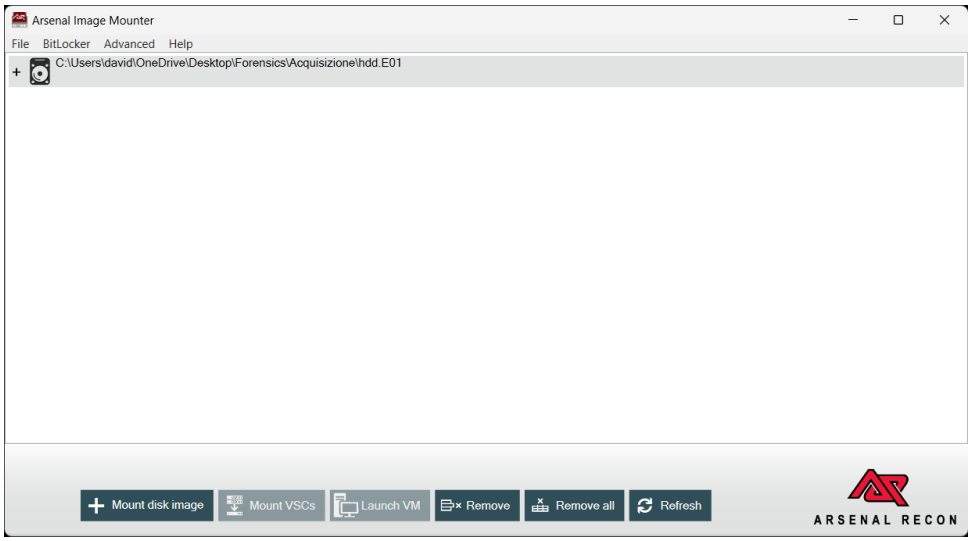
A partire da un'immagine **E01** non è immediato il processo di boot, abbiamo quindi effettuato diversi tentativi:

FTKImager + VirtualBox

Abbiamo utilizzato FTKImager per espandere l'immagine nelle sue totali dimensioni di '500GB' in modo da poter montare fisicamente il disco sulla nostra macchina locale.
In seguito abbiamo utilizzato il tool **VBoxManage.exe** per poter generare un file **.vmdk** che facesse da link per la macchina virtuale con il disco montato.
La creazione del file .vmdk non è però andata a buon fine.

Arsenal Image Mounter + VMWare Workstation

Il secondo tentativo è stato quello di utilizzare **Arsenal Image Mounter** per creare il disco su cui eseguire il boot della VM. La peculiarità di Arsenal è che riesce a montare il disco partendo da un E01, con scrittura abilitata, mantenendolo offline.



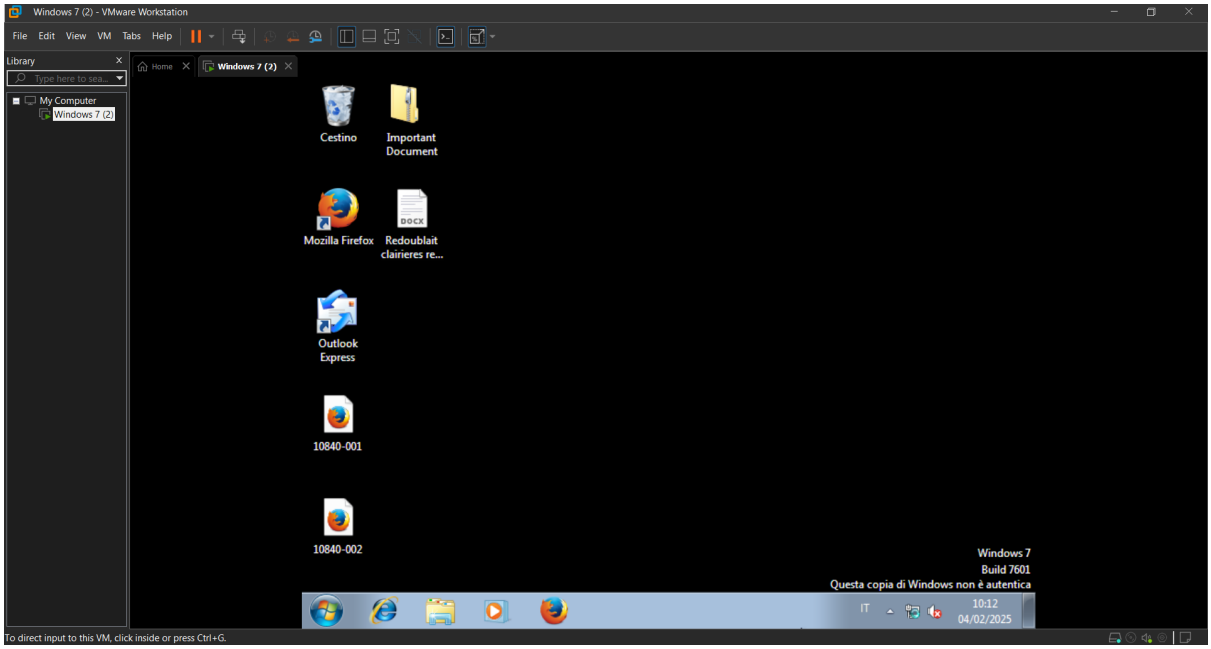
Per evitare che il file E01 venisse modificato abbiamo specificato una posizione di write cache dove i cambiamenti effettuati sulla VM vengono salvati.
Arsenal ha dunque montato il disco offline **PhysicalDrive1** da cui siamo riusciti a creare la virtual machine utilizzando **VMWare Workstation**.

Durante la creazione della VM abbiamo dovuto configurare diversi parametri. In questa fase sono stati effettuati diversi tentativi (non funzionanti). Dopo svariate ore e prove siamo arrivati ad una combinazione di parametri funzionanti, confermati anche da valori trovati su Autopsy:

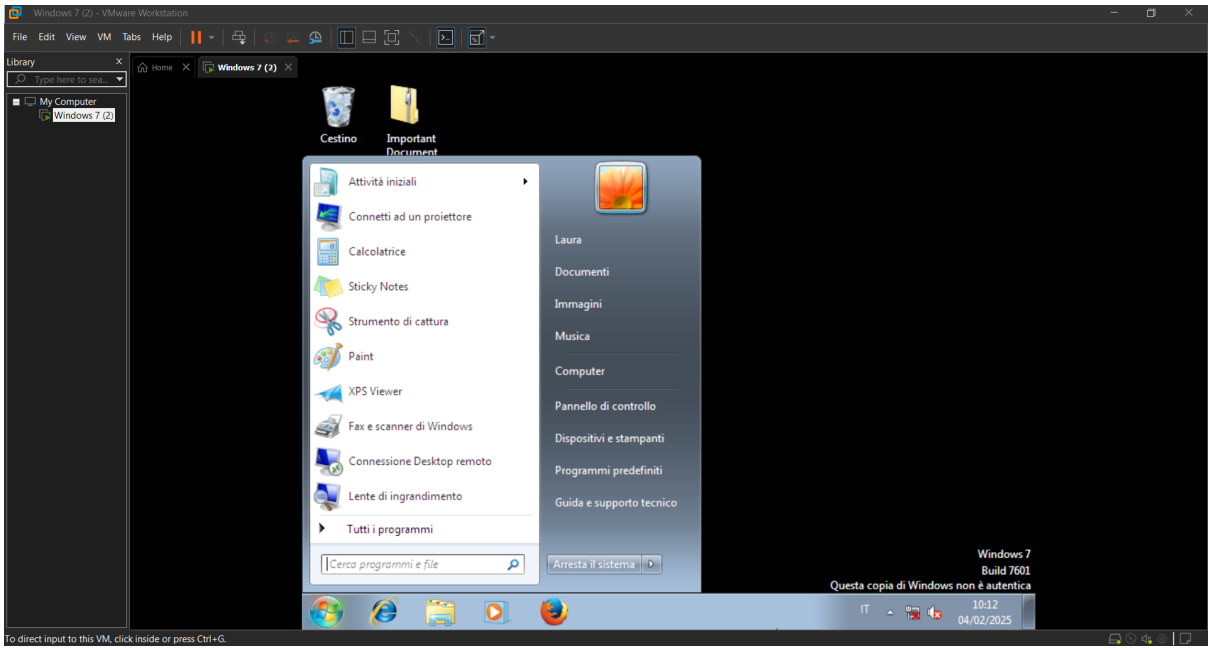
- **Distribuzione del Sistema Operativo**: Windows 7 Professional
- **Architettura**: x86 32Bit
- **Interfaccia Disco**: SATA

- **Memoria RAM**: 1Gb
- **Numero Processori**: 1

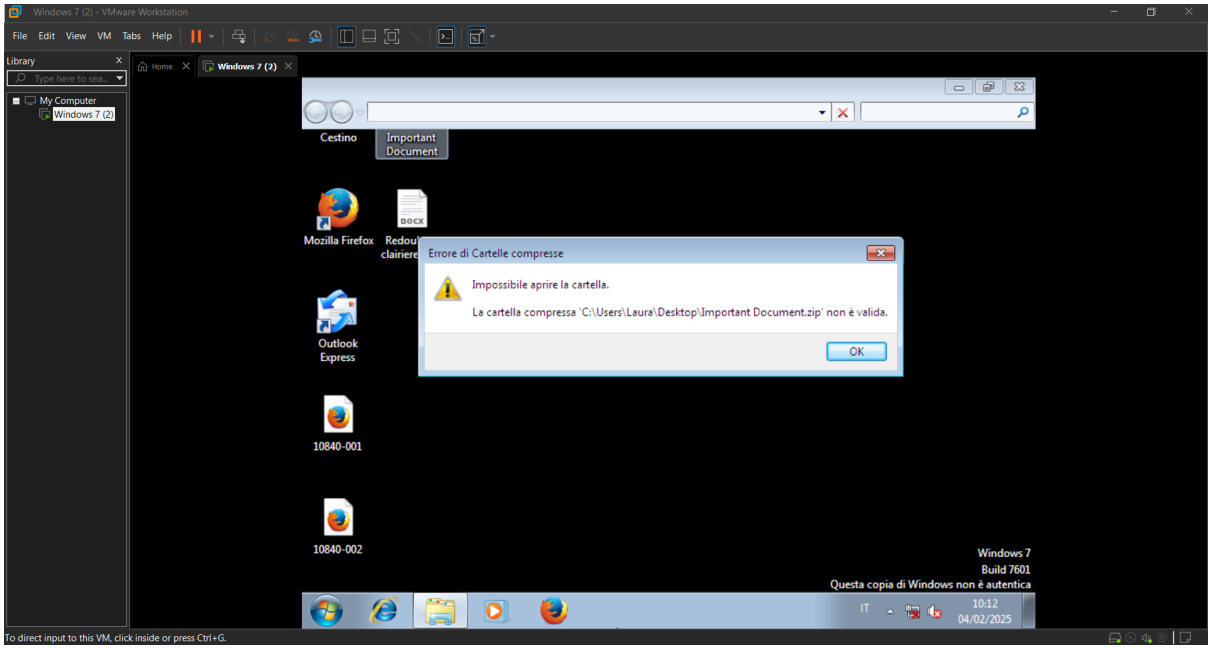
Con questi parametri, la VM ha effettuato un boot funzionante senza schermate **BSOD** che precedentemente hanno invalidato i diversi tentativi effettuati.



E' possibile osservare l'utente Laura.



Provando quindi ad aprire il file Important Document.zip dall'utente Laura notiamo il messaggio di errore restituito.



5. Timeline degli eventi

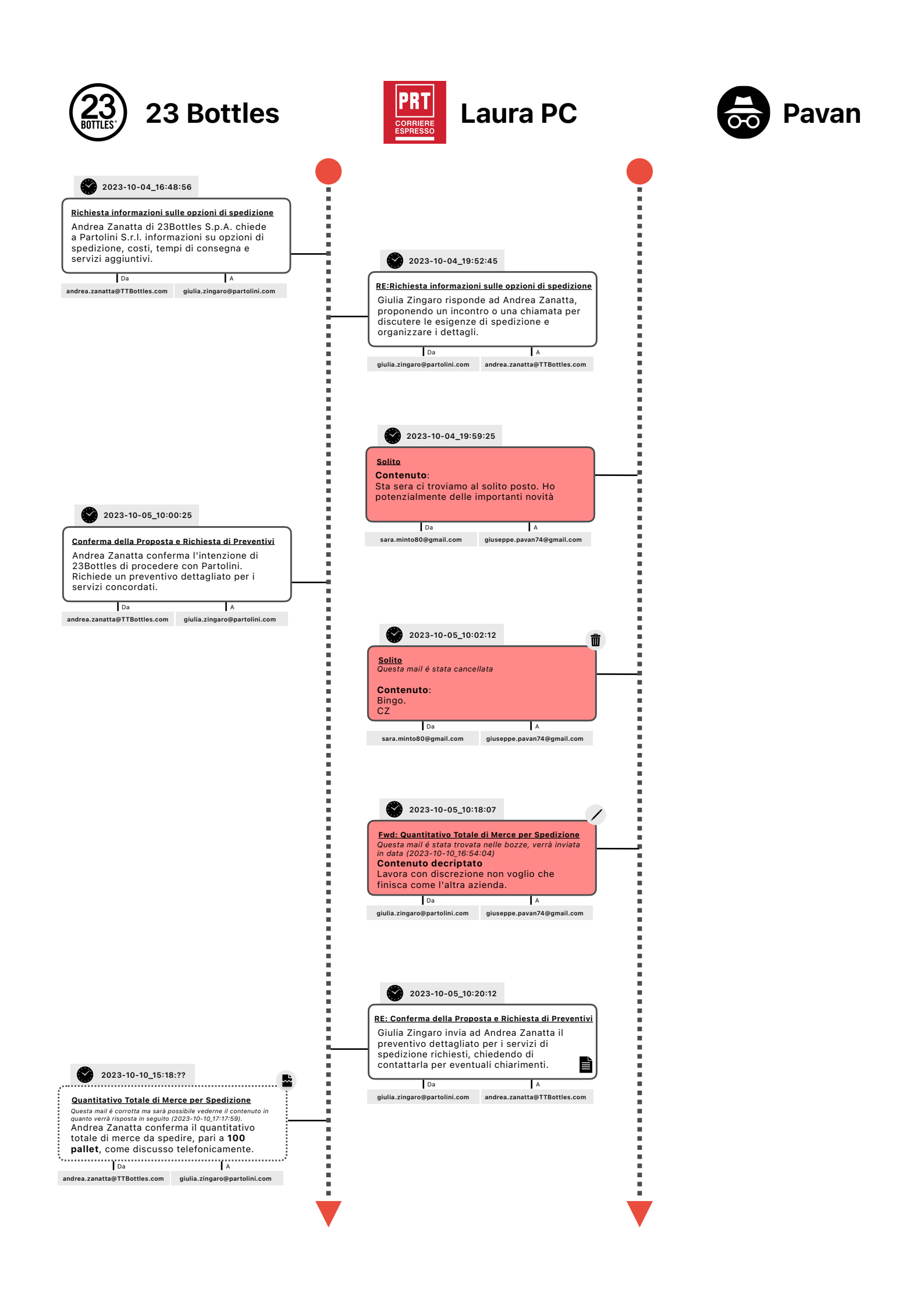
Vengono rappresentate le comunicazioni tra le tre entità principali del caso divise in:

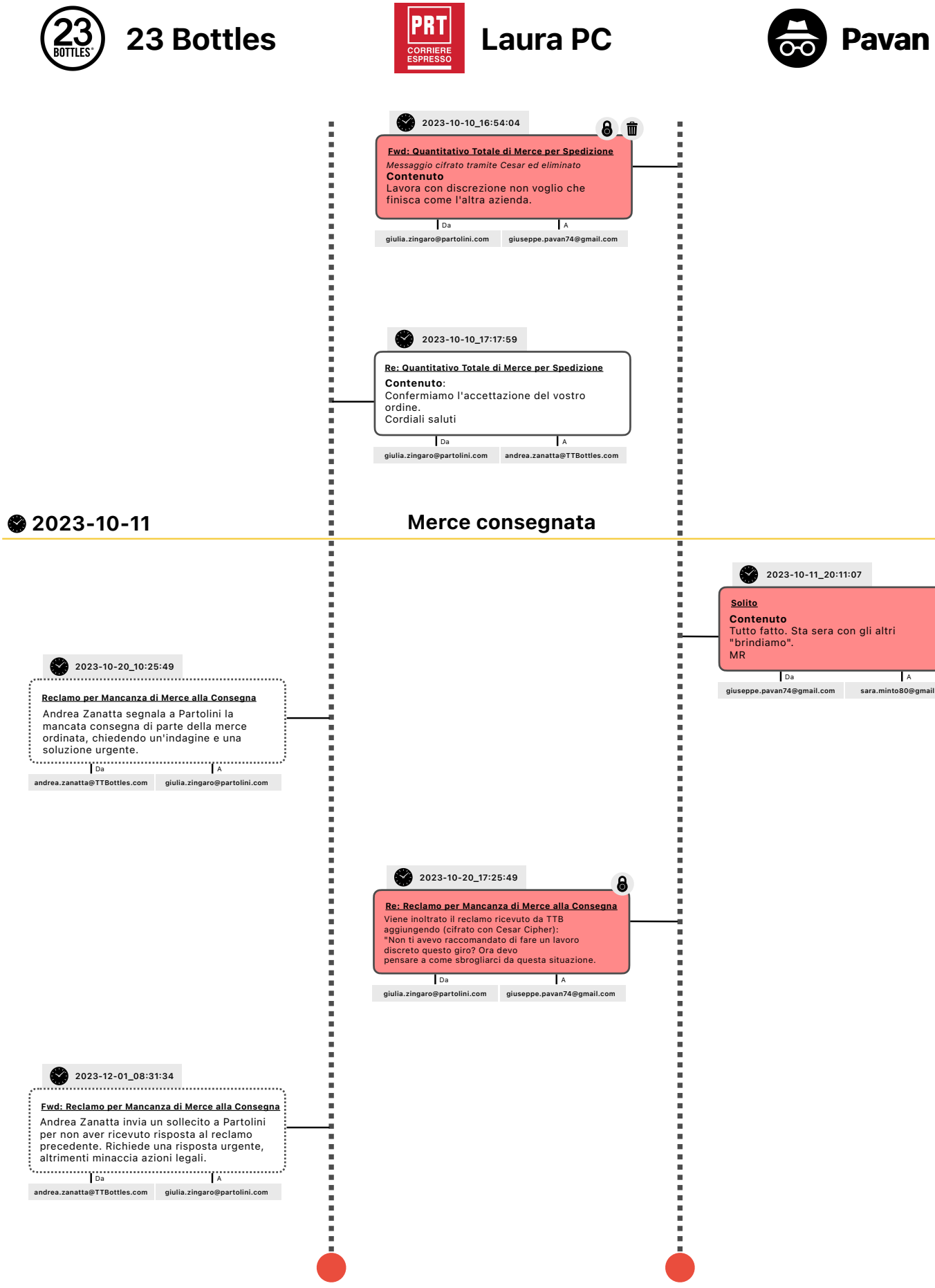
- **23Bottles**: l'azienda che ha intrapreso la causa contro Partolini
- **Laura PC**: il PC sequestrato a Partolini
- **Giuseppe Pavan**: uno sconosciuto che ha comunicato con l'utente *Laura* durante il periodo di interesse

Gli elementi con sfondo bianco sono le normali comunicazioni di business tra 23Bottles e Partolini, mentre quelli con sfondo rosso sono le comunicazioni sospette tra l'utente Laura e Pavan.

Per collocare gli elementi sulla timeline è stato utilizzato il **Time Zone GMT**, convertendo tutti i timestamp delle email trovate in quella time zone.
Gli orari precisi sono stati trovati all'interno dei metadati delle diverse email utilizzando la data di ricezione del Server SMTP.

Viene quindi di seguito mostrata una **timeline** grafica.


23 Bottles
Laura PC
Pavan
2023-10-04_16:48:56
Richiesta informazioni sulle opzioni di spedizione
Andrea Zanatta di 23Bottles S.p.A. chiede a Partolini S.r.l. informazioni su opzioni di spedizione, costi, tempi di consegna e servizi aggiuntivi.
Da
A
andrea.zanatta@TTBottles.com
giulia.zingaro@partolini.com
2023-10-04_19:52:45
RE:Richiesta informazioni sulle opzioni di spedizione
Giulia Zingaro risponde ad Andrea Zanatta, proponendo un incontro o una chiamata per discutere le esigenze di spedizione e organizzare i dettagli.
Da
A
giulia.zingaro@partolini.com
andrea.zanatta@TTBottles.com
2023-10-04_19:59:25
Solito
Contenuto:
Sta sera ci troviamo al solito posto. Ho potenzialmente delle importanti novità
Da
A
sara.minto80@gmail.com
giuseppe.pavan74@gmail.com
2023-10-05_10:00:25
Conferma della Proposta e Richiesta di Preventivi
Andrea Zanatta conferma l'intenzione di 23Bottles di procedere con Partolini. Richiede un preventivo dettagliato per i servizi concordati.
Da
A
andrea.zanatta@TTBottles.com
giulia.zingaro@partolini.com
2023-10-05_10:02:12
Solito
Questa mail é stata cancellata
Contenuto:
Bingo.
CZ
Da
A
sara.minto80@gmail.com
giuseppe.pavan74@gmail.com
2023-10-05_10:18:07
Fwd: Quantitativo Totale di Merce per Spedizione
Questa mail é stata trovata nelle bozze, verrà inviata in data (2023-10-10_16:54:04)
Contenuto decriptato
Lavora con discrezione non voglio che finisca come l'altra azienda.
Da
A
giulia.zingaro@partolini.com
giuseppe.pavan74@gmail.com
2023-10-05_10:20:12
RE: Conferma della Proposta e Richiesta di Preventivi
Giulia Zingaro invia ad Andrea Zanatta il preventivo dettagliato per i servizi di spedizione richiesti, chiedendo di contattarla per eventuali chiarimenti.
Da
A
giulia.zingaro@partolini.com
andrea.zanatta@TTBottles.com
2023-10-10_15:18:??
Quantitativo Totale di Merce per Spedizione
Questa mail é corrotta ma sarà possibile vederne il contenuto in quanto verrà risposta in seguito (2023-10-10_17:17:59).
Andrea Zanatta conferma il quantitativo totale di merce da spedire, pari a 100 pallet, come discusso telefonicamente.
Da
A
andrea.zanatta@TTBottles.com
giulia.zingaro@partolini.com


23 Bottles
Laura PC
Pavan
2023-10-10_16:54:04
Fwd: Quantitativo Totale di Merce per Spedizione
Messaggio cifrato tramite Cesar ed eliminato
Contenuto
Lavora con discrezione non voglio che finisca come l'altra azienda.
Da
giulia.zingaro@partolini.com
A
giuseppe.pavan74@gmail.com
2023-10-10_17:17:59
Re: Quantitativo Totale di Merce per Spedizione
Contenuto:
Confermiamo l'accettazione del vostro ordine.
Cordiali saluti
Da
giulia.zingaro@partolini.com
A
andrea.zanatta@TTBottles.com
2023-10-11
Merce consegnata
2023-10-11_20:11:07
Solito
Contenuto
Tutto fatto. Sta sera con gli altri "brindiamo".
MR
Da
giuseppe.pavan74@gmail.com
A
sara.minto80@gmail.com
2023-10-20_10:25:49
Reclamo per Mancanza di Merce alla Consegna
Andrea Zanatta segnala a Partolini la mancata consegna di parte della merce ordinata, chiedendo un'indagine e una soluzione urgente.
Da
andrea.zanatta@TTBottles.com
A
giulia.zingaro@partolini.com
2023-10-20_17:25:49
Re: Reclamo per Mancanza di Merce alla Consegna
Viene inoltrato il reclamo ricevuto da TTB aggiungendo (cifrato con Cesar Cipher):
"Non ti avevo raccomandato di fare un lavoro discreto questo giro? Ora devo pensare a come sbrogliarci da questa situazione.
Da
giulia.zingaro@partolini.com
A
giuseppe.pavan74@gmail.com
2023-12-01_08:31:34
Fwd: Reclamo per Mancanza di Merce alla Consegna
Andrea Zanatta invia un sollecito a Partolini per non aver ricevuto risposta al reclamo precedente. Richiede una risposta urgente, altrimenti minaccia azioni legali.
Da
andrea.zanatta@TTBottles.com
A
giulia.zingaro@partolini.com

6. Risultati delle Analisi

Di seguito vengono illustrati i diversi risultati ottenuti durante l'indagine forense.

6.1. Analisi USB

All'interno della memoria USB depositata dall'azienda 23Bottles sono stati rinvenuti diversi file, come annunciato in precedenza:

- **13 email**, tra cui:
  - 7 email scambiate tra 23Bottles e Partolini. I due indirizzi con i quali sono avvenute le comunicazioni sono *andrea.zanatta@TTBottles.com* e *giulia.zingaro@partolini.com* [8.1.1] [8.1.2] [8.1.4] [8.1.6] [8.1.9] [8.1.11] [8.1.13]
  - 2 email scambiate tra Giulia Zingaro e Giuseppe Pavan, con email codificate in quasi tutte le comunicazioni. I due indirizzi con i quali sono avvenute le comunicazioni sono *giulia.zingaro@partolini.com* e *giuseppe.pavan74@gmail.com* [8.1.8] [8.1.12]
  - 3 email scambiate tra Sara Minto e Giuseppe Pavan. I due indirizzi con i quali sono avvenute le comunicazioni sono *sara.minto80@gmail.com* e *giuseppe.pavan74@gmail.com* [8.1.3] [8.1.5] [8.1.10]
  - 1 email corrotta, alla quale si può risalire tramite la risposta ricevuta successivamente. I due indirizzi con i quali è avvenuta la comunicazione sono *andrea.zanatta@TTBottles.com* e *giulia.zingaro@partolini.com* [8.1.7]
- **2 file**, tra cui:
  - Un documento chiamato **Preventivo** [8.1.14] con estenzione *.docx*, nel quale è presente il preventivo per la consegna effettuata da Partolini per 23Bottles
  - Un documento chiamato **Consegna** [8.1.15] con estenzione *.pdf*, nel quale è presente la conferma di ricezione dell'ordine

6.2. Analisi HDD

Tramite la ricerca per codici hash, email e keyword viene evidenziata la presenza di tutte le email depositate da 23Bottles.

Dall'esame delle comunicazioni emerse durante l'indagine, è stato possibile quindi ricostruire una serie di eventi che offrono una visione più chiara delle dinamiche tra 23Bottles e Partolini, oltre che di alcune interazioni interne a quest'ultima.

Le prime email tra Andrea Zanatta, rappresentante di 23Bottles, e Giulia Zingaro, referente di Partolini, sembrano rientrare in un normale contesto di trattativa commerciale. In particolare, la richiesta iniziale di informazioni [8.1.1] e la successiva conferma di interesse per una collaborazione [8.1.2], avvenute il 4 ottobre 2023, indicano una fase di avvio regolare della contrattazione tra le parti.
Tuttavia, accanto a queste comunicazioni ufficiali, emergono parallelamente altri scambi di email tra indirizzi personali che suggeriscono una gestione meno trasparente della vicenda. In particolare, alle ore 19:59:25 GMT dello stesso giorno, viene inviata un'email con oggetto "Solito" dall'indirizzo *sara.minto80@gmail.com* a *giuseppe.pavan74@gmail.com* [8.1.3].
Il messaggio fa riferimento a un incontro in un luogo abituale per discutere di "novità importanti". È rilevante notare che la firma riportata è "CZ", sebbene non corrisponda al nome associato all'indirizzo email. Questo schema si ripete in ulteriori scambi successivi.

Il 5 ottobre 2023, alle 10:00:25 GMT, Andrea Zanatta scrive a Giulia Zingaro per esprimere apprezzamento per la collaborazione in corso e per richiedere preventivi dettagliati sui servizi discussi [8.1.4]. La risposta di Giulia Zingaro, inviata alle 10:20:12 GMT, contiene il documento richiesto. [8.1.6].
Poco prima, alle 10:02:12 GMT, ovvero due minuti dopo la ricezione dell'email di Zanatta, Sara Minto invia a Giuseppe Pavan un altro messaggio con oggetto "Solito", scrivendo solamente "Bingo" firmato "CZ". [8.1.5].

Il 10 ottobre 2023, alle 15:18 GMT, Andrea Zanatta conferma via email un ordine di 100 pallet, facendo riferimento a un accordo telefonico precedente. Poco dopo, alle 16:54:04 GMT, Giulia Zingaro scrive un'email codificata utilizzando il cifrario di Cesare a Giuseppe Pavan, sottolineando l'importanza della discrezione e richiamando ad una maggiore attenzione. [8.1.8].
Nello stesso giorno, viene rinvenuto un documento di presa in consegna della merce, firmato da Marco Rizzoli e contenuto tra i materiali informatici depositati da 23Bottles [8.1.15]. La data del documento coincide con quella dell'ultima email con oggetto "Solito" inviata da Giuseppe Pavan a Sara Minto, in cui, firmandosi "MR", fa riferimento a un brindisi per celebrare il "lavoro svolto" [8.1.10].

Ulteriori dettagli emergono in seguito al reclamo presentato da Andrea Zanatta il 20 ottobre 2023 [8.1.11]. In questa comunicazione, il rappresentante di 23Bottles segnala che un cliente non ha ricevuto l'intera fornitura prevista e sollecita un'indagine per chiarire le cause del problema. Propone inoltre di risolvere la questione con una spedizione urgente della merce mancante per ridurre al minimo l'impatto sulle attività aziendali.
Nello stesso giorno, alle 15:25:49 GMT, Giulia Zingaro scrive un'email a Giuseppe Pavan, il cui contenuto decodificato – anche qui con cifrario di Cesare – lascia intendere la possibilità di problematiche tra i due dipendenti. Nel messaggio, Zingaro si lamenta infatti di aver consigliato a Pavan di agire con discrezione e si rammarica di dover ora trovare una soluzione alla situazione [8.1.12].

Infine, il primo dicembre alle 08:31:34 GMT, Andrea Zanatta invia un'ultima email a Giulia Zingaro per sollecitare una risposta alla sua precedente richiesta. Esprime la delusione per la mancata comunicazione e sottolinea che, in assenza di chiarimenti immediati, 23Bottles prenderà provvedimenti legali [8.1.13].

Inoltre, alla luce dei dati raccolti, si evidenzia come la sezione USB Device Attached di Autopsy abbia mostrato il collegamento, in data 01/05/2023 alle ore 9:52:36 GMT, di un hard disk esterno [8.3.3]. Tale collegamento, unitamente agli eventi registrati nei log di sistema, ha consentito di ricostruire una serie di operazioni che, seppur anomale, non risultano direttamente riconducibili ad un comportamento scorretto da parte di Partolini.

In particolare, l'analisi dei log di sistema in `C:/Windows/System32/winevt/Logs/` ha rivelato numerosi cambi di data e ora effettuati dall'utente Laura, con variazioni temporali significative (ad es. un salto di 21 anni e retrocessi di mesi e giorni). Inoltre, l'esame del file **Security.evtx** ha registrato vari accessi al sistema, con evidenza di:

- Accessi fisici (Tipo 2) effettuati tramite la schermata di login.
- Accessi remoti (Tipo 3) e login effettuati dai servizi di Windows (Tipo 5).

Un ulteriore elemento critico è rappresentato dal file **Important Document.zip** presente nella directory `C:/Users/Laura/Desktop`.
L'alta entropia del file (misurata a circa 7.999983 bits per byte) indica una cifratura totale, coerente con l'utilizzo di algoritmi di full-text encryption (ad es. VeraCrypt o TrueCrypt) supportati da Windows tramite la cifratura basata sulle informazioni di login. Nonostante i tentativi di decifrazione tramite strumenti come `hashcat` e vari approcci di boot del disco in ambiente virtuale, il file è rimasto inaccessibile. Questa inaccessibilità implica che il contenuto di **Important Document.zip** non può essere analizzato e, di conseguenza, non fornisce ulteriori elementi probatori utili a supportare le tesi della parte attrice.
In assenza di evidenze chiare e verificabili provenienti da tale file, non è possibile ricostruire con piena affidabilità eventuali discrepanze o errori nella gestione del trasporto da parte di Partolini.

Alla luce di questi elementi, si conferma che il materiale analizzato non fornisce basi sufficienti per attribuire a Partolini responsabilità per eventuali errori nella gestione del trasporto, rafforzando così la posizione difensiva dell'azienda.

7. Conclusioni

Dall'analisi forense condotta sul materiale raccolto, è possibile trarre le seguenti conclusioni, che rafforzano la posizione difensiva di Partolini:

1. **Validità delle Comunicazioni Ufficiali:** le email scambiate tra 23Bottles e Partolini, registrate con le date e gli orari indicati dai server di posta elettronica, testimoniano una fase iniziale di trattativa commerciale regolare (ad es. [8.1.1], [8.1.2]). Tali comunicazioni ufficiali risultano affidabili, mentre le ulteriori email scambiate tramite indirizzi personali sembrano riferirsi a dinamiche interne non per forza riconducibili alle operazioni logistiche.

2. **Evidenze di Accessi e Operazioni sul Sistema:** l'analisi del collegamento di un hard disk esterno [8.3.3] in data 01/05/2023, unitamente ai log di sistema in `C:/Windows/System32/winevt/Logs/`, ha rivelato numerosi cambi di data e accessi al sistema, con variazioni temporali significative (ad esempio, un salto di 21 anni e retrocessi di mesi e giorni) effettuati dall'utente Laura.

3. **Inaccessibilità del File Important Document.zip:** il file presente nella directory `C:/Users/Laura/Desktop` mostra un'alta entropia (circa 7.999983 bits per byte) e risulta cifrato mediante algoritmi di full-text encryption (ad es. VeraCrypt o TrueCrypt). Nonostante i tentativi di decifrazione tramite `hashcat` e varie procedure di boot in ambiente virtuale, il contenuto del file è rimasto inaccessibile. Tale circostanza implica che il file non fornisce elementi probatori aggiuntivi a supporto delle tesi della parte attrice, impedendo una ricostruzione completa di eventuali discrepanze nella gestione del trasporto.

Complessivamente, il materiale analizzato – includendo le comunicazioni ufficiali, i log di sistema e il file cifrato – non fornisce basi sufficienti per dimostrare un comportamento scorretto o un inadempimento contrattuale da parte di Partolini.

Pertanto, alla luce di quanto emerso dall'indagine forense, si ritiene che il materiale evidenzi, pur la presenza di alcuni elementi anomali, la regolarità delle operazioni svolte da Partolini.
In assenza di ulteriori prove chiare e verificabili, non è possibile attribuire a Partolini responsabilità per eventuali errori nella gestione del trasporto, rafforzando così la posizione difensiva dell'azienda.

8. Materiale

8.1. Materiale depositato

8.1.1 001_Richiesta informazioni sulle opzioni di spedizione.eml

From: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
To: Giulia Zingaro <*giulia.zingaro@partolini.com*>
Date: 4 ottobre 2023, 16:48:56 GMT
Subject: Richiesta informazioni sulle opzioni di spedizione

Gentile Partolini S.r.l,
Mi presento, sono Andrea Zanatta di 23Bottles S.p.A e come suo rappresentate sono attualmente alla ricerca di un partner affidabile per gestire le spedizioni delle nostre bottiglie e vorremmo ottenere maggiori informazioni sui servizi offerti dalla vostra azienda. Le caratteristiche principali che ci interessano includono:

- Tipologie di spedizioni disponibili (nazionali/internazionali, spedizioni particolari, ecc.)
- Costi e tariffe relative alle diverse opzioni di spedizione
- Tempi di consegna stimati
- Eventuali servizi aggiuntivi offerti (assicurazione, tracciamento, ecc.)

Saremmo grati se poteste fornirci una panoramica dettagliata dei vostri servizi e delle eventuali personalizzazioni disponibili per adattarsi alle esigenze della nostra attività.

Se possibile, vorremmo anche organizzare una chiamata o un incontro per discutere più approfonditamente delle nostre esigenze e delle vostre soluzioni.

Resto in attesa di ricevere le informazioni richieste e spero di avere l'opportunità di instaurare una proficua collaborazione con la vostra azienda.

Grazie per la vostra attenzione.

Cordiali saluti,
Andrea Zanatta
23Bottles S.p.A
Telefono: 347 3214254

MD5 checksum	5a92b27e5faf5a160fb684f448fa3db0
SHA-256 checksum	491867cc035d42c618498e19a85e258b543e8b45c582811212b8f8f6b09e2ad3

8.1.2 002_Richiesta informazioni sulle opzioni di spedizione.eml

From: Giualia Zingaro <*giulia.zingaro@partolini.com*>
To: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
Date: 4 ottobre 2023, 19:52:45 GMT
Subject: Re: Richiesta informazioni sulle opzioni di spedizione

Gentile Andrea Zanatta,
Grazie per averci contattato e per l'interesse dimostrato nei confronti dei nostri servizi di spedizione per le vostre bottiglie.
Siamo entusiasti della possibilità di discutere in dettaglio le vostre esigenze e le soluzioni che possiamo offrire. Saremmo lieti di organizzare un incontro o una chiamata telefonica per fornirvi tutte le informazioni necessarie e comprendere meglio le vostre aspettative.
Per quanto riguarda l'appuntamento, preferite una chiamata telefonica o un incontro di persona presso la nostra sede? Siamo flessibili e disposti a adattarci alla vostra disponibilità per garantire un incontro proficuo.
Se avete delle preferenze riguardo alla data e all'orario, vi chiedo cortesemente di fornirci delle opzioni in modo da organizzare al meglio il nostro calendario. Resto in attesa delle vostre indicazioni e non vedo l'ora di poter discutere delle nostre proposte in modo più dettagliato.
Grazie ancora per l'opportunità di collaborare.
Cordiali saluti,
Cinzia Zingaro

Il giorno mer 04 ott 2023 alle ore 17:49 Andrea Zanatta <andrea.zanatta@TTBottles.com> ha scritto:
>
> Gentile Partolini S.r.l,
>
> Mi presento, sono Andrea Zanatta di 23Bottles S.p.A e come suo rappresentate sono attualmente alla ricerca di un partner affidabile per gestire le spedizioni delle nostre bottiglie e vorremmo ottenere maggiori informazioni sui servizi offerti dalla vostra azienda. Le caratteristiche principali che ci interessano includono:
>
> - Tipologie di spedizioni disponibili (nazionali/internazionali, spedizioni particolari, ecc.)
> - Costi e tariffe relative alle diverse opzioni di spedizione
> - Tempi di consegna stimati
> - Eventuali servizi aggiuntivi offerti (assicurazione, tracciamento, ecc.)
>
> Saremmo grati se poteste fornirci una panoramica dettagliata dei vostri servizi e delle eventuali personalizzazioni disponibili per adattarsi alle esigenze della nostra attività.
>
> Se possibile, vorremmo anche organizzare una chiamata o un incontro per discutere più approfonditamente delle nostre esigenze e delle vostre soluzioni.
>
> Resto in attesa di ricevere le informazioni richieste e spero di avere l'opportunità di instaurare una proficua collaborazione con la vostra azienda.
>
> Grazie per la vostra attenzione.
>
> Cordiali saluti,
> Andrea Zanatta
> 23Bottles S.p.A
> Telefono: 347 3214254

MD5 checksum	344a404af229ab50edd4d3b29d0a117d
SHA-256 checksum	041a2665a861dff6448bd6401a3d099f2630a39c20e42b9a1abe0b35d656a16f

8.1.3 003_Solito.eml

From: Sara Minto <*sara.minto80@gmail.com*>
To: Giuseppe Pavan <*giuseppe.pavan74@gmail.com*>
Date: 4 ottobre 2023, 19:59:25 GMT
Subject: Solito

Sta sera ci troviamo al solito posto. Ho potenzialmente delle importanti novità.
CZ

MD5 checksum	9e41acfa10d77d7f9cb77e405a3f1e97
SHA-256 checksum	e1b525f1f48e2c836f22e901b3234d25fefa1af8ae5fd6d4cc5aa0a2997372eb

8.1.4 004_Conferma della Proposta e Richiesta di Preventivi.eml

From: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
To: Giulia Zingaro <*giulia.zingaro@partolini.com*>
Date: 5 ottobre 2023, 10:00:25 GMT
Subject: Conferma della Proposta e Richiesta di Preventivi

Gentile Cinzia Zingaro,

Desidero esprimere la mia gratitudine per l'incontro durante il quale abbiamo discusso approfonditamente le nostre esigenze relative alla gestione delle spedizioni per le nostre bottiglie.

Sulla base dei dettagli condivisi e dei requisiti emersi, desidero confermare la nostra intenzione di procedere con la vostra azienda per la gestione delle spedizioni. Abbiamo valutato positivamente le soluzioni proposte e riteniamo che la vostra competenza e l'approccio personalizzato siano in linea con le nostre necessità.
Per poter procedere ulteriormente, vi chiedo cortesemente di inviarci i preventivi dettagliati relativi ai servizi discussi durante l'incontro. La chiarezza e la completezza delle informazioni fornite ci aiuteranno a prendere una decisione informata e a stabilire una collaborazione efficace.

Grazie ancora per l'attenzione.

Cordiali saluti,
Andrea Zanatta
23Bottles S.p.A
Telefono: 347 3214254

MD5 checksum	b422bb342c3d5344c83c9ed7c05254ba
SHA-256 checksum	244af17358b613976dd643c35f7fca8eeca26da0d2b5e8cb63a288f170ba2297

8.1.5 005_Solito.eml

From: Sara Minto <*sara.minto80@gmail.com*>
To: Giuseppe Pavan <*giuseppe.pavan74@gmail.com*>
Date: 5 ottobre 2023, 10:02:12 GMT
Subject: Solito

Bingo.
CZ

MD5 checksum	108d202d6bda3e49627c368caaf9469e
SHA-256 checksum	31025d53abfc5ae166741a01f0ac52ca2337f677ebd9ffb51d2f7f8a2cef7c61

8.1.6 006_Conferma della Proposta e Richiesta di Preventivi.eml

From: Giulia Zingaro <*giulia.zingaro@partolini.com*>
To: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
Date: 5 ottobre 2023, 10:20:12 GMT
Subject: Re: Conferma della Proposta e Richiesta di Preventivi
Attachment: Preventivo.docx

Gentile Andrea,
Spero questa email vi trovi bene.
Desidero ringraziarvi per l'opportunità di poter discutere delle nostre esigenze di spedizione durante il recente incontro. Come concordato, vi invio in allegato il preventivo dettagliato per i servizi di spedizione offerti dalla nostra azienda.
Vi prego di esaminare attentamente il preventivo e, in caso di domande o necessità di chiarimenti, non esitate a contattarmi. Siamo aperti a discutere ulteriori dettagli o a fornire informazioni supplementari qualora ce ne fosse bisogno.
Cordiali saluti,
Cinzia Zingaro

Il giorno gio 05 ott 2023 alle ore 11:00 Andrea Zanatta <andrea.zanatta@TTBottles.com> ha scritto:
>
> Gentile Cinzia Zingaro,
>
> Desidero esprimere la mia gratitudine per l'incontro durante il quale abbiamo discusso approfonditamente le nostre esigenze relative alla gestione delle spedizioni per le nostre bottiglie.
>
> Sulla base dei dettagli condivisi e dei requisiti emersi, desidero confermare la nostra intenzione di procedere con la vostra azienda per la gestione delle spedizioni. Abbiamo valutato positivamente le soluzioni proposte e riteniamo che la vostra competenza e l'approccio personalizzato siano in linea con le nostre necessità.
>
> Per poter procedere ulteriormente, vi chiedo cortesemente di inviarci i preventivi dettagliati relativi ai servizi discussi durante l'incontro. La chiarezza e la completezza delle informazioni fornite ci aiuteranno a prendere una decisione informata e a stabilire una collaborazione efficace.
>
> Grazie ancora per l'attenzione.
>
> Cordiali saluti,
> Andrea Zanatta
> 23Bottles S.p.A
> Telefono: 347 3214254

MD5 checksum	85dadd2f3c585817f53042fa66970c4e
SHA-256 checksum	edde101b000675005d507683c548f20e04bb9bd5ab16cca65d1e4ce1affa25bb

8.1.7 _Quantitativo Totale di Merce per Spedizione.eml

Il contenuto della mail non è presente essendo corrotta.

MD5 checksum	c04fcc662ab51933f9c11af9941e7887
SHA-256 checksum	50ddb3d6d2e4f1b1f7768ffc21c29efe99a8af065f0a5fe77c7175ff65aba74f

8.1.8 Quantitativo Totale di Merce per Spedizione-3.eml

From: Giulia Zingaro <*giulia.zingaro@partolini.com*>
To: Giuseppe Pavan <*giuseppe.pavan74@gmail.com*>
Date: 10 ottobre 2023, 16:54:04 GMT Subject: Fwd: Quantitativo Totale di Merce per Spedizione

Shcvyh jvu kpzjylgpvul uvu cvnspv jol mpupzjh jvtl s'hsayh hgplukh.

———- Forwarded message ———
Da: Andrea Zanatta <andrea.zanatta@TTBottles.com>
Subject: Quantitativo Totale di Merce per Spedizione
To: Giulia Zingaro <giulia.zingaro@partolini.com>

Hssh jvyalzl haalugpvul kp Whyavspup Z.y.s,

Klzpklyv jvumlythyl ps xbhuapahapcv avahsl kp tlyjl jol pualukphtv zwlkpyl bapspgghukv p cvzayp zlycpgp. Kvwv bu'haaluah chsbahgpvul klssl uvzayl zjvyal l klssl ypjoplzal pu hyypcv, hiiphtv jhsjvshav jol ps xbhuapahapcv

=J3 mvukhtluahsl wly uvp nhyhuapyl buh nlzapvul hjjbyhah l lmmpjplual klssh tlyjl l klssl ylshapcl zwlkpgpvup.

Cp ypunyhgphtv wly s'haalugpvul l sh cvzayh hzzpzalugh uls nhyhuapyl buh jvyylaah nlzapvul klp uvzayp vykpup kp zwlkpgpvul. Ylzaphtv kpzwvupipsp wly bsalypvyp pumvythgpvup v wly xbhszphzp hnnpvyuhtluav ylshapcv h xblzah xbhuapa=J3=H0.

Nyhgpl hujvyh wly sh cvzayh jvsshivyhgpvul.

Jvykphsp zhsbap,
Hukylh Ghuhaah
23Ivaaslz Z.w.H
Alslmvuv: 347 3214254

MD5 checksum	33c0e02a0319f7cddb6861df15247294
SHA-256 checksum	04df760b872c7ba1817bcf4953a2a7fda9784ede4d2ba595e5c49ccdbabc0156

Contenuto decifrato tramite cifratura di Cesare facendo shift di 7 posizioni a destra:
`Lavora con discrezione non voglio che finisca come l'altra azienda.`
Il restante contenuto cifrato del messaggio fa riferimento a [8.1.9]

8.1.9 Quantitativo Totale di Merce per Spedizione-2.eml

From: Giulia Zingaro <*giulia.zingaro@partolini.com*>
To: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
Date: 10 ottobre 2023, 17:17:59 GMT
Subject: Re: Quantitativo Totale di Merce per Spedizione

Confermiamo l'accettazione del vostro ordine.
Cordiali saluti,
Cinzia Zingaro

Il giorno mer 10 ott 2023 alle ore 16:18 Andrea Zanatta <andrea.zanatta@TTBottles.com> ha scritto:

> Alla cortese attenzione di Partolini S.r.l,
>
> Desidero confermare il quantitativo totale di merce che intendiamo spedire
> utilizzando i vostri servizi. Dopo un'attenta valutazione delle nostre
> scorte e delle richieste in arrivo, abbiamo calcolato che il quantitativo
> totale da spedire ammonta a 100 pallet come da accordi presi per telefono.
>
> È fondamentale per noi garantire una gestione accurata e efficiente della
> merce e delle relative spedizioni.
>
> Vi ringraziamo per l'attenzione e la vostra assistenza nel garantire una
> corretta gestione dei nostri ordini di spedizione. Restiamo disponibili per
> ulteriori informazioni o per qualsiasi aggiornamento relativo a questa
> quantità.
>
> Grazie ancora per la vostra collaborazione.
>
> Cordiali saluti,
> Andrea Zanatta
> 23Bottles S.p.A
> Telefono: 347 3214254
>

MD5 checksum	a2d4d833f3cd7d2fd73787bf3a25731c
SHA-256 checksum	2b35b07b17d9a3555079e5f4c8af64b30c529e368748421092f4fda7e0b1d348

8.1.10 Solito.eml

From: Giuseppe Pavan <*giuseppe.pavan74@gmail.com*>
To: Sara Minto <*sara.minto80@gmail.com*>
Date: 11 ottobre 2023, 20:11:07 GMT
Subject: Solito

Tutto fatto. Sta sera con gli altri "brindiamo".
MR

MD5 checksum	b0ffd30aee8bcf8fd956ab570c9a944e
SHA-256 checksum	5c1c92a63d1d32f78448abad0f3d46e28fa622c16ce28bc1e9622d7e516ce36f

8.1.11 Reclamo per Mancanza di Merce alla Consegna.eml

From: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
To: Giulia Zingaro <*giulia.zingaro@partolini.com*>
Date: 20 ottobre 2023, 10:25:49 GMT
Subject: Reclamo per Mancanza di Merce alla Consegna

Gentile Partolini S.r.l.,

Mi rivolgo a voi in merito all'ordine della azienda che rappresento per segnalare una situazione di estrema delusione e disagio a causa della mancanza di parte della merce prevista.

Al momento della ricezione della consegna, il cliente ha riscontrato che una parte del prodotto non erano inclusi nel carico come previsto e concordato nella nostra ordine di acquisto.

In qualità di vostro cliente, ci aspettavamo un servizio accurato e una gestione impeccabile degli ordini effettuati. La mancanza di parte della merce compromette non solo la nostra operatività, ma anche la fiducia nei confronti dei vostri servizi.

Chiediamo cortesemente un'indagine immediata su questa questione e vi preghiamo di fornirci una spiegazione dettagliata sul motivo per cui la merce specificata non è stata inclusa nella consegna. Inoltre, vi chiediamo di proporre delle soluzioni per risolvere prontamente questa situazione, come ad esempio la spedizione urgente della merce mancante o altre alternative che possano attenuare l'impatto di questa mancanza sulla nostra attività.

A questo proposito, vi chiedo cortesemente di confermare la ricezione di questa comunicazione e di informarci tempestivamente sulle azioni che intendete intraprendere per risolvere questa situazione.

Attendiamo con urgenza una vostra risposta e la vostra azione per risolvere questo inconveniente.

Cordiali saluti,
Andrea Zanatta
23Bottles S.p.A
Telefono: 347 3214254

MD5 checksum	6de659d9fc09f9598022a33d44fa4e11
SHA-256 checksum	85b08316d29c5eee75e100cea3dc195a81b868633e4c7e0b07511e46e6e82522

8.1.12 Reclamo per Mancanza di Merce alla Consegna-2.eml

From: Giulia Zingaro <*giulia.zingaro@partolini.com*>
To: Giuseppe Pavan <*giuseppe.pavan74@gmail.com*>
Date: 20 ottobre 2023, 17:25:49 GMT
Subject: Re: Reclamo per Mancanza di Merce alla Consegna

Uvu ap hclcv yhjjvthukhav kp mhyl bu shcvyv kpzjylav xblzav npyv? Vyh klcv wluzhyl h jvtl ziyvnsphyjp kh xblzah zpabhgpvul.

Mi rivolgo a voi in merito all'ordine della azienda che rappresento per segnalare una situazione di estrema delusione e disagio a causa della mancanza di parte della merce prevista.

Al momento della ricezione della consegna, il cliente ha riscontrato che una parte del prodotto non erano inclusi nel carico come previsto e concordato nella nostra ordine di acquisto.

In qualità di vostro cliente, ci aspettavamo un servizio accurato e una gestione impeccabile degli ordini effettuati. La mancanza di parte della merce compromette non solo la nostra operatività, ma anche la fiducia nei confronti dei vostri servizi.

Chiediamo cortesemente un'indagine immediata su questa questione e vi preghiamo di fornirci una spiegazione dettagliata sul motivo per cui la merce specificata non è stata inclusa nella consegna. Inoltre, vi chiediamo di proporre delle soluzioni per risolvere prontamente questa situazione, come ad esempio la spedizione urgente della merce mancante o altre alternative che possano attenuare l'impatto di questa mancanza sulla nostra attività.

A questo proposito, vi chiedo cortesemente di confermare la ricezione di questa comunicazione e di informarci tempestivamente sulle azioni che intendete intraprendere per risolvere questa situazione.

Attendiamo con urgenza una vostra risposta e la vostra azione per risolvere questo inconveniente.

MD5 checksum	1bff11fa796a4bfb5e52f0a3bac2d0b7
SHA-256 checksum	e9b051588715c1d3be35b76e44bad599ac372e6c9142ab747bd3e3d32cf67aaf

Contenuto decifrato tramite cifratura di Cesare facendo shift di 7 posizioni a destra:
`Non ti avevo raccomandato di fare un lavoro discreto questo giro? Ora devo pensare a come sbrogliarci da questa situazione.`

8.1.13 Reclamo per Mancanza di Merce alla Consegna-3.eml

From: Andrea Zanatta <*andrea.zanatta@TTBottles.com*>
To: Giulia Zingaro <*giulia.zingaro@partolini.com*>
Date: 01 dicembre 2023, 08:31:34 GMT
Subject: Fwd: Reclamo per Mancanza di Merce alla Consegna

Alla cortese attenzione di Partolini S.r.l.,

Mi rivolgo nuovamente a voi in seguito alla comunicazione che riporto di seguito.

Siamo delusi nel constatare che non abbiamo ricevuto alcuna risposta o chiarimento in merito alla nostra precedente comunicazione. Come vostro cliente, ci aspettavamo una pronta e attenta considerazione dei nostri dubbi e delle nostre richieste.

Questa mancanza di risposta ci ha causato disagio e incertezza, in quanto avevamo posto delle questioni rilevanti che richiedevano una vostra attenzione immediata per poter procedere con le nostre attività in modo efficiente e coerente.

Riteniamo che una comunicazione tempestiva e chiara sia fondamentale per mantenere una relazione di fiducia e collaborazione tra le nostre aziende. Vi chiediamo pertanto di considerare l'importanza della vostra risposta e di fornirci una spiegazione o un chiarimento in merito alla nostra comunicazione precedente.

Vi preghiamo di trattare questa richiesta con la massima urgenza e di garantire una risposta completa e dettagliata, altrimenti dovremmo procedere per vie legali.

Resto in attesa di ricevere una vostra pronta risposta.

Grazie per la vostra attenzione e collaborazione.

Andrea Zanatta

23Bottles S.p.A

Telefono: 347 3214254

——— Forwarded message ———
Da: Andrea Zanatta <andrea.zanatta@TTBottles.com>
Date: ven 20 ott 2023 alle ore 11:25
Subject: Reclamo per Mancanza di Merce alla Consegna
To: Giulia Zingaro <giulia.zingaro@partolini.com>

Gentile Partolini S.r.l.,

Mi rivolgo a voi in merito all'ordine della azienda che rappresento per segnalare una situazione di estrema delusione e disagio a causa della mancanza di parte della merce prevista.

Al momento della ricezione della consegna, il cliente ha riscontrato che una parte del prodotto non erano inclusi nel carico come previsto e concordato nella nostra ordine di acquisto.

In qualità di vostro cliente, ci aspettavamo un servizio accurato e una gestione impeccabile degli ordini effettuati. La mancanza di parte della merce compromette non solo la nostra operatività, ma anche la fiducia nei confronti dei vostri servizi.

Chiediamo cortesemente un'indagine immediata su questa questione e vi preghiamo di fornirci una spiegazione dettagliata sul motivo per cui la merce specificata non è stata inclusa nella consegna. Inoltre, vi chiediamo di proporre delle soluzioni per risolvere prontamente questa situazione, come ad esempio la spedizione urgente della merce mancante o altre alternative che possano attenuare l'impatto di questa mancanza sulla nostra attività.

A questo proposito, vi chiedo cortesemente di confermare la ricezione di questa comunicazione e di informarci tempestivamente sulle azioni che intendete intraprendere per risolvere questa situazione.

Attendiamo con urgenza una vostra risposta e la vostra azione per risolvere questo inconveniente.

Cordiali saluti,
Andrea Zanatta
23Bottles S.p.A
Telefono: 347 3214254

MD5 checksum	404382378fd96ae3e59ecfa9f24c7ff3
SHA-256 checksum	d7701a1d13a591b8f7e9d1e80579258a5f9dcda77ef636491d98ce69d633ae16

8.1.14 Preventivo.docx

Preventivo # 1072

Partolini S.r.l

CLIENTE: 23Bottles S.p.A

DESCRIZIONE	QUANTITÀ	PREZZO	SUBTOTALE	IVA
Gestione spedizione	8	133,00	1.064,00	234,08 (22%)
Servizio di tracciamento	1	620,00	620,00	136,40 (22%)
Servizio di tracciamento (Sconto 10%)	1	-62,00	-62,00	-13,64 (22%)

SUBTOTALE	1.622,00 €
IVA	356,84 €
Totale	**1.978,84 €**

MD5 checksum	c6209c7f120a50c82326f5cc3f5af74b
SHA-256 checksum	16905c277627c83f4062059d0769d982f9882c2e646df0399dfefbf1e1462123

8.1.15 Consegna.pdf

Ricevuta di Consegna Merce

Dati del Cliente:

Nome dell'Azienda/Cliente: 23Bottles

Indirizzo: Milano, via 23 Settembre

Città, CAP: Milano, 20019

Telefono: 347 8012309

Dettagli della Consegna:

Data della Consegna: 11 Ottobre 2023

Descrizione della Merce: 100 pallet di bottiglie, ogni pallet contiene 25 pezzi.

Quantità: 2500

Condizioni della Merce: Nulla da riportare

Note: _____

Accettazione della Merce:

Con la presente, confermo di aver ricevuto la merce sopra descritta nelle condizioni indicate. Accetto la responsabilità di custodirla e assicurarmi che sia in buone condizioni fino al suo utilizzo o alla sua destinazione finale.

Firma del Responsabile o Dipendente: Marco Rizzoli

Nome del Responsabile o Dipendente: Marco Rizzoli

Data: 10 Ottobre 2023

MD5 checksum	144f73d42b4829be3019c40e782521a3
SHA-256 checksum	725c17ef07d38545dfbc90872e89a6b3078fc2665e968bbdb13427b54a197496

8.2. Materiale acquisito

8.2.1 Seagate HDD 500GB

Modello	500GB Seagate Laptop Thin
Codice Seriale	W625FZAT
MD5 Checksum	808b681e557864a91568a4d6de42f2c9
SHA-1 Checksum	093eeddb84cf7c73d63ffc83f06244f3d7a2c6b7
Size (bytes)	500107862016
Numero di Partizioni	4

Partizione 1

Partizione	Vol1
Descrizione	Non allocata
Settore iniziale	0
Lunghezza in settori	2048

Partizione 2

Partizione	Vol2
Descrizione	NTFS/ExFAT
Settore iniziale	2048
Lunghezza in settori	204800

Partizione 3

Partizione	Vol3
Descrizione	NTFS/ExFAT
Settore iniziale	206848
Lunghezza in settori	959339537

Partizione 4

Partizione	Vol4
Descrizione	Non allocata
Settore iniziale	959546385
Lunghezza in settori	17226783

8.3. Informazioni aggiuntive

8.3.1 Informazioni HDD

Sistema operativo: Windows 7 Professional Service Pack 1
Architettura processore: x86
Nome: LAURA-PC

Versione Outlook: Outlook Express for Windows 7-8.1-10 (x86-64 Bit)

8.3.2 Informazioni "Laura"

Login: Laura
Home Directory: *C:/Users/Laura*
SID: S-1-5-21-3222981709-1565221779-1341311900-1000

Profilo Outlook Express (contenuto del file Laura.wab):

- {4586BA90-4EE6-4BD0-BEAF-1EDC08CB6D21}
- {4586BA90-4EE6-4BD0-BEAF-1EDC08CB6D21}

Il precedente valore indica il contatto dell'identità principale, ovvero Laura.

8.3.3 Informazioni Hard Disk collegato

Devide Make: Western Digital Technologies, Inc.
Devide Model: My Passport (WDBPKJ)
Devide ID: 5758333241353143454E3755
MD5 checksum: d6e903ffa4b6652c1058fd79202ab570
SHA-256 checksum: ca3bc22d72afc0195e3e931e4ceaa8f7ebfad721b7918ab5941643d582436f56