RELAZIONE CONSULENZA TECNICA INFORMATICA

OGGETTO:
Verifica dell'eventuale presenza di materiali di proprietà dell'azienda committente ACME Corporation all'interno del disco dell'azienda ricorrente GMBH srl.

COMMITTENTE:
Prof. Alessandro Amoroso

CONSULENTI TECNICI: Federica La Piana, Stefano Balla, Dario Floris

Bologna 2/01/2020

RELAZIONE TECNICA

DISPOSITIVI SOTTOPOSTI ALL' ANALISI

Model: `USB Flash Disk USB Device`
Numero seriale:`BK1410220003502`
Data Size:`3824 MB`
MD5 checksum: `f3de0b4867ae6798a91483ae47654569`
SHA1 checksum:
`e3f07d72ce522fcb0491ff5161cfe18a1bd58428`

Model: `HITACHI_DK23EA-30B`
Numero seriale: `G91428`
Data Size:`30005 MBytes (30 GB)`
MD5 checksum: `da8f17eda1c82710e5f848b63c4baae0`
SHA1 checksum:
`b4ce77d263cc9627d0e70db12b0bfc2206cdc6bc`

OBIETTIVI

L'obiettivo dell'indagine consiste nell'acquisire sia la memoria di massa che il disco interno del pc portatile sequestrato. Determinare quindi l'eventuale presenza di file testuali o porzioni di essi, rinvenuti nella memoria usb fornita dall'azienda ACME, all'interno del materiale informatico sequestrato all'azienda GMBH. Secondo la disposizione del giudice, verrà presa come oggetto dell'indagine anche l'analisi delle

mail, al fine di stabilire se i file siano stati inviati da un ex dipendente dell'azienda ACME.

METODOLOGIA

Acquisizione del supporto USB

Al fine di acquisire i dati presenti nel supporto USB di proprietà dell'azienda ACME è stato utilizzato un *Write Blocker Tableau T8U*, un dispositivo hardware di sola lettura collegato ad un computer e al supporto USB.
Tramite il programma di acquisizione dati *Ftk Imager 4.2.1* è stata generata l'immagine forense del dispositivo USB fornito dalla parte committente. Grazie alle specifiche tecniche del software è stato possibile estrarre i metadati, contenenti: le date di creazione, di modifica, di ultimo accesso, il formato, dimensione.
A seguito della creazione dell'immagine, il programma genera la scheda tecnica contenente i metadati dell'immagine, i digest in formato MD5,SHA1 e il risultato della verifica degli hash disponibile in sez. 'DISPOSITIVI SOTTOPOSTI ALL' ANALISI'.

Acquisizione del disco

L'acquisizione della memoria G91428 è stata realizzata attraverso il software Guy Manager presente all'interno della distribuzione Linux Deft Zero. Per l'immagine prodotta è stato poi calcolato e verificato l'hash, indicato in sez. 'DISPOSITIVI SOTTOPOSTI ALL' ANALISI'.

Analisi dei dispositivi

Al fine di effettuare l'analisi dei file di testo presenti nel supporto USB consegnato dall'azienda ACME, è stato utilizzato il software *Autopsy 4.9.1* che consente la visione, l'analisi e la classificazione delle informazioni presenti nei dispositivi informatici.
Dopo aver caricato l'immagine del supporto USB dell'azienda ACME nel programma, sono stati estratti file di testo al fine di identificare il contenuto della ricerca.
Di seguito viene mostrato il report generato dal programma contenente le informazioni dei file di testo.

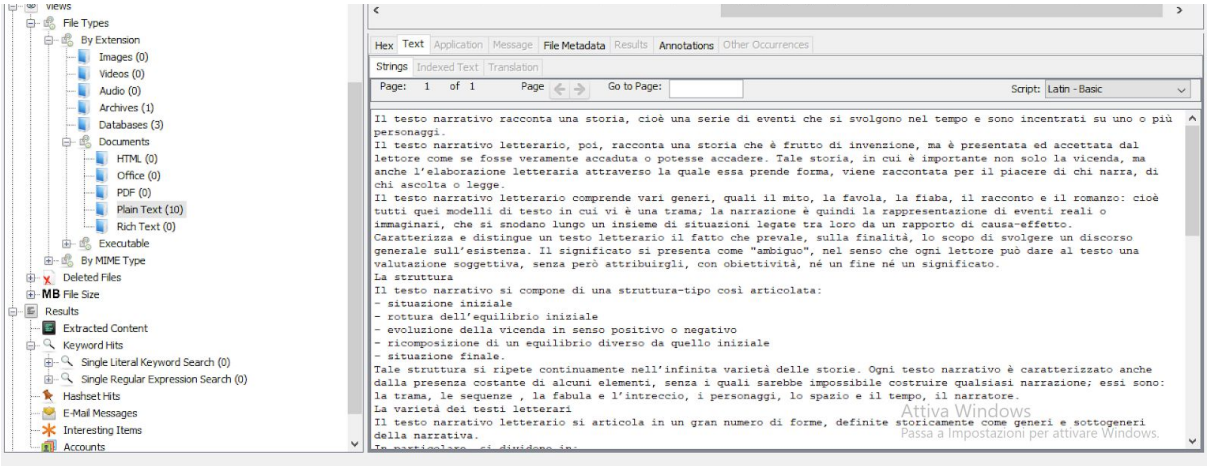
Contains files that were tagged with one of the following:Bookmark

Tag	File	Comment	User Name	Modified Time	Changed Time	Accessed Time	Created Time	Size (Bytes)	Hash
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/5857tgfghfhf.txt		Federica	2019-12-05 14:25:06 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:30 CET	3095	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/aeroporto.txt		Federica	2019-12-05 14:28:18 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:30 CET	5206	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/pensier2.txt		Federica	2019-12-05 14:26:10 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:30 CET	6501	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/presentaz bol.txt		Federica	2019-12-05 14:21:44 CET	0000-00-00 00:00:00	2019-12-10 00:00:00 CET	2019-12-07 15:43:30 CET	3653	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/priv 3.txt		Federica	2019-12-05 14:57:12 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:31 CET	5206	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/silvia.txt		Federica	2019-12-05 14:28:56 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:31 CET	7139	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/sto narr insieme.txt		Federica	2019-12-05 14:21:54 CET	0000-00-00 00:00:00	2019-12-10 00:00:00 CET	2019-12-07 15:43:31 CET	2496	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/test lett.txt		Federica	2019-12-05 14:19:06 CET	0000-00-00 00:00:00	2019-12-10 00:00:00 CET	2019-12-07 15:43:31 CET	6921	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/test seminario 2.txt		Federica	2019-12-05 14:23:02 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:31 CET	2452	null
Bookmark	/img_flash_disk_case_3.E01/vol_vol6/vam 14.txt		Federica	2019-12-05 14:27:26 CET	0000-00-00 00:00:00	2019-12-07 00:00:00 CET	2019-12-07 15:43:31 CET	4503	null

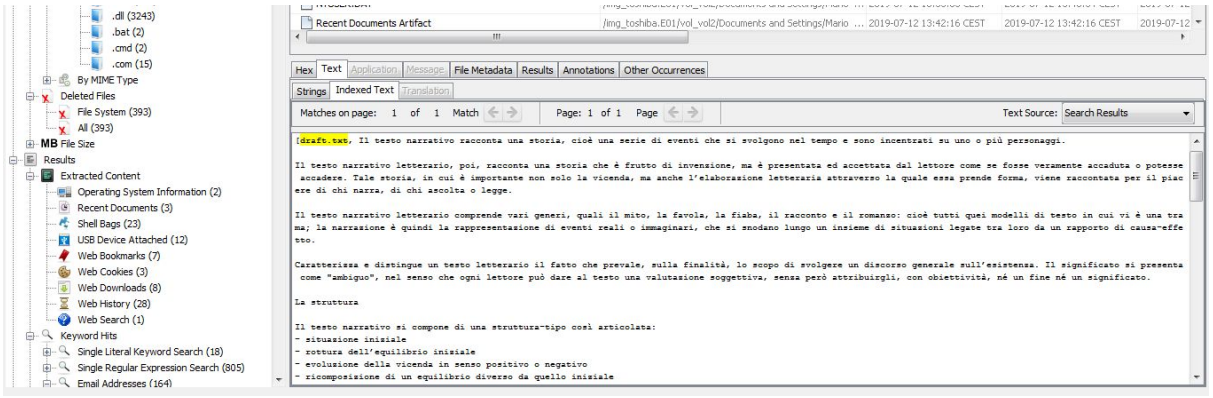
Lo stesso procedimento è stato eseguito per l'immagine del disco dell'azienda GMBH.

Verifica presenza artefatti nel contenuto del disco.

Poichè i file recuperati dal supporto USB risultano in formato testuale, come prima cosa è stata analizzata sistematicamente la sezione *Documents* del disco che comprende i file in formato HTML, Office, Plain Text, PDF, Rich Text.
Nello specifico, è stata fatta una ricerca per parole-chiave utilizzando inizialmente come chiave di ricerca parole presenti all'interno dei file recuperati dal supporto USB dell'azienda committente.
Successivamente, è stata effettuata una ricerca utilizzando i nomi dei file presenti nel dispositivo USB.
La ricerca per parole presenti nel contenuto ha effettivamente trovato un riscontro nella sezione Plain Text. In particolare, risulta che il file intitolato "*test lett.txt*" presente nel supporto USB dell'azienda committente sia identico al file "*draft.txt*" presente nella sezione plain text del disco dell'azienda GMBH.
Di seguito vengono mostrati i file "*test lett.txt*" e "*draft.txt*" che presentano lo stesso contenuto.



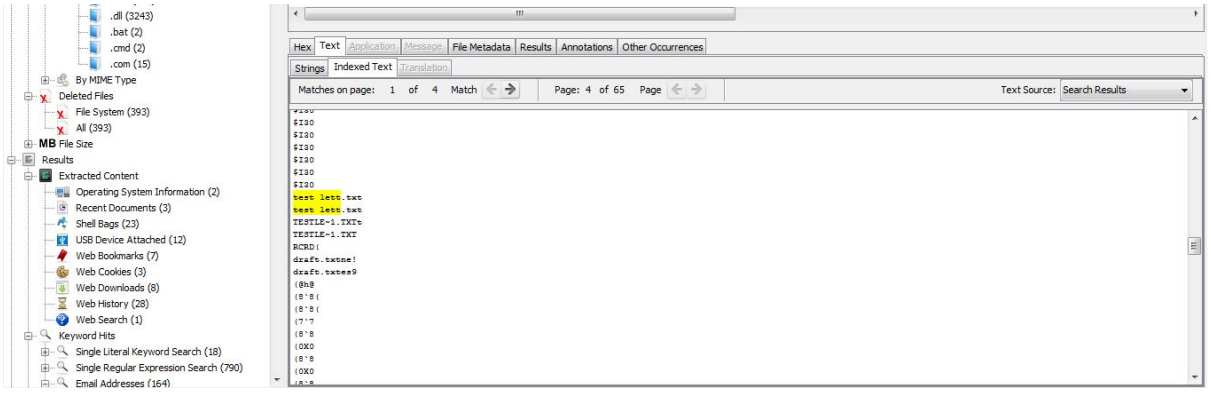
[test lett.txt]



[draft.txt]

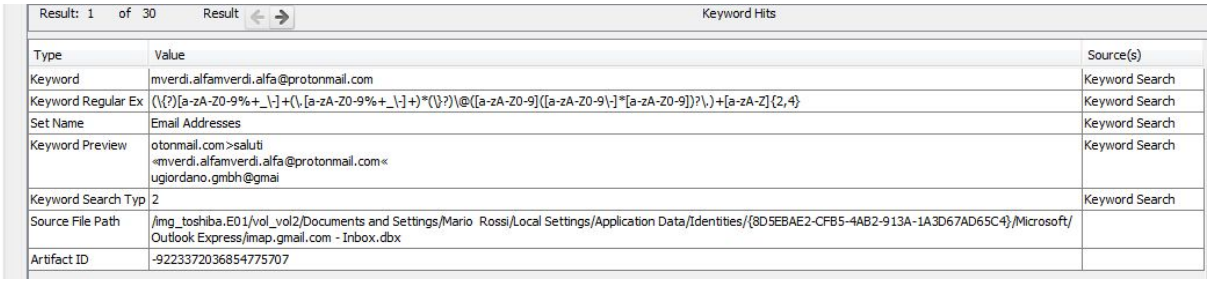
Sempre per mezzo di una ricerca per parole chiave, digitando il nome originale del file in questione, questo compare come allegato in una mail il cui mittente è "*mverdi.alfamverdi.alfa@protonmail.com"* e il destinatario è "*ugiordano.gmbh.gmail"* ricevuta in data 2019-07-12 ore 13:42:05.

Inoltre, analizzando i file di log, risulta un'operazione di modifica del titolo del file da "*test.lett.txt*" a "*draft.txt"*.



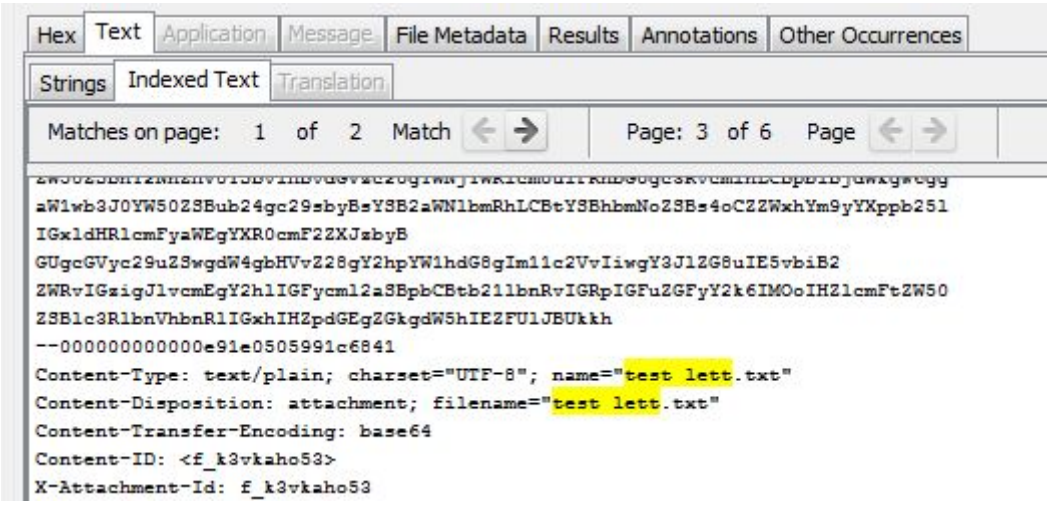
Per quanto riguarda gli altri testi, non sembrano essere presenti nel disco dell'azienda ricorrente, tuttavia, all'interno della cartella *Documents* in cui è stato rinvenuto il file draft.txt risultano presenti i file "44444.txt", "appunti 3.txt", "armonia nel tes.txt", "notturno.txt" e "silence.txt".

Analizzandone i metadati risultano essere frutto di una copia massiva, il che ha portato l'indagine verso l'analisi delle email, discussa nel paragrafo successivo.
Di seguito vengono mostrate le meta-informazioni relative alle email in questione.



Result: 1 of 30 Result — Keyword Hits

Type	Value	Source(s)
Keyword	mverdi.alfamverdi.alfa@protonmail.com	Keyword Search
Keyword Regular Ex	(\{?)[a-zA-Z0-9%+_\-]+(\.[a-zA-Z0-9%+_\-]+)*(\}?)\@([a-zA-Z0-9][a-zA-Z0-9\-]*[a-zA-Z0-9])?\.)+[a-zA-Z]{2,4}	Keyword Search
Set Name	Email Addresses	Keyword Search
Keyword Preview	otonmail.com>saluti «mverdi.alfamverdi.alfa@protonmail.com« ugiordano.gmbh@gmai	Keyword Search
Keyword Search Typ	2	Keyword Search
Source File Path	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/Local Settings/Application Data/Identities/{8D5EBAE2-CFB5-4AB2-913A-1A3D67AD65C4}/Microsoft/Outlook Express/imap.gmail.com - Inbox.dbx	
Artifact ID	-9223372036854775707	



Hex | Text | Application | Message | File Metadata | Results | Annotations | Other Occurrences

Strings | Indexed Text | Translation

Matches on page: 1 of 2 Match — Page: 3 of 6 Page

```
aW1wb3J0YW50Z3Bub24gc29sbyBsYSB2aWNlbmRhLCBtYSBhbmNoZSBs4oCZZWxhYm9yYXppb251
IGxldHRlcmFyaWEgYXR0cmF2ZXJzbyB
GUgcGVyc29uZSwgdW4gbHVv228gY2hpYW1hdG8gIm11c2VvIiwgY3J1ZG8uIE5vbiB2
ZWRvIGzigJlvcmEgY2hlIGFycml2aSBpbCBtb21lbnRvIGRpIGFuZGFyY2k6IMOoIHZlcmFtZW50
ZSBlc3RlbnVhbnRlIGxhIHZpdGEgZGkgdW5hIEZFUlJBUkkh
--000000000000e91e0505991c6841
Content-Type: text/plain; charset="UTF-8"; name="test lett.txt"
Content-Disposition: attachment; filename="test lett.txt"
Content-Transfer-Encoding: base64
Content-ID: <f_k3vkaho53>
X-Attachment-Id: f_k3vkaho53
```

VERIFICA DELLO SCAMBIO DEL MATERIALE SOSPETTO TRAMITE EMAIL

In seguito ad una ricerca per parole chiave, utilizzando i titoli dei file di testo rinvenuti nel dispositivo USB dell'azienda ACME, è risultata una corrispondenza all'interno del file "*imap.gmail.com - Inbox.dbms*", ovvero il file che contiene le mail ricevute.
Più specificatamente, dalla ricerca risulta che il giorno Venerdì, 06 Dec 2019 08:26:04, dall'indirizzo di posta "*verdi.alfa@protonmail.com*" è

stato inviato un messaggio all'indirizzo di posta "*ugiordano.gmbh@gmail.com*" contenente come allegato un file intitolato "test lett.txt".
L'indirizzo "*ugiordano.gmbh@gmail.com*" risulta essere l'unica casella di posta attiva sul dispositivo sequestrato.
Nella stessa modalità sono stati inviati altri documenti testuali rinvenuti poi nella cartella *Documents* del dispositivo sequestrato, per tali documenti però non è stata riscontrata alcuna corrispondenza con i file forniti dalla parte committente.
Seguendo un'analisi approfondita delle mail sono state rinvenute tracce di contatto fra l'indirizzo di posta "*ugiordano.gmbh@gmail.com*", "*verdi.alfa@protonmail.com*" e un terzo indirizzo "*mbellucci.acme@gmail.com*" in data Venerdì, 6 Dicembre, 2019 ore 10:29 AM, nel file "*Outbox.dbx"*.
Alla luce delle prove disponibili non è però possibile stabilire la natura delle relazioni fra essi.

APPENDICE

File Name	Hash MD5	Path
imap.gmail.com - Inbox.dbms	12354b0b121ef3560eb91f38e45c8a31	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/Local Settings/Application Data/Identities/{8D5EBAE2-CFB5-4AB2-913A-1A3D67AD65C4}/Microsoft/Outlook Express/imap.gmail.com - Inbox.dbx
Outbox.dbx	db2885486ff0fbcc1af436d553a92450”	“/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/Local Settings/ApplicationData/Identities/{8D5EBAE2-CFB5-4AB2-913A-1A3D67AD65C4}/Microsoft/Outlook Express/Outbox.dbx

Documents		“/img_toshiba.E01/vol_vol2/DocumentsandSettings/Mario Rossi/My Documents/”
Draft.txt	43617c9ff52e5dd2cb9f2c6435540105	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My
44444.txt	7f67106e8d7524925ca36f2bd757744e	img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My Documents/44444.txt
Notturno.txt	766444341fd444dd040985346ecf0041	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My Documents/notturno.txt
Armonia nel tes.txt	668e92e552255e6f21286566e9d8a2ba	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My Documents/armonia nel tes.txt

Appunti 3.txt	45d4d8bfdf991169a46a550565d2ad03	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My Documents/notturno.txt
Silence.txt	39c5b1bb68ddbc82df1aa3b38d517270	/img_toshiba.E01/vol_vol2/Documents and Settings/Mario Rossi/My Documents/silence.txt