

CORSO DI ALTA FORMAZIONE

L'attività del Consulente Tecnico e del Perito nei giudizi civili e penali: questioni processuali e case study

Stefano Martinazzo

Dipartimento di Forensic Accounting, Internal Audit & Litigation - AXERTA S.p.A.

Dottore Commercialista, Ordine di Milano

Revisore Legale dei Conti

ODCEC di Bologna

21 novembre 2022

DATA BASE RELAZIONALI... (1999-2005)

Anagrafiche

Microsoft Access - [Autori : Tabella]

	Nome	Cognome	Nazi
+	Francesco	de Franchis	Italiana
+	Jack P.	Friedman	statun
+	John	Downes	statun
+	Jordan Elliot	Goodman	statun
+	Abate	Mario	italiana
+	Giuseppe	Di Dio	italiana

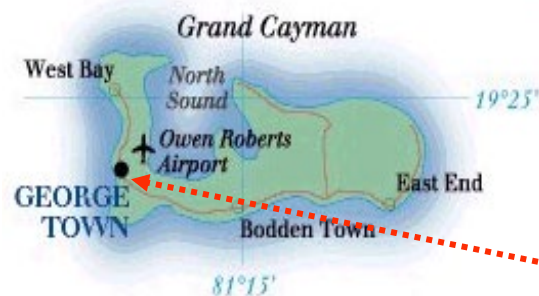
Conto Corrente

IDCC: 24 NumeroConto: Jg-12346 Banca: Banca dello Stato del C
NomeConto: Anguria Corrispondenza presso: Cairo
DivisaConto: \$ Data Apertura:

Note:

Persone collegate: Società collegate: Documenti di riferimento: Operazioni collegate:

Persona:	Ruolo:
Mario Abate	Intestatario

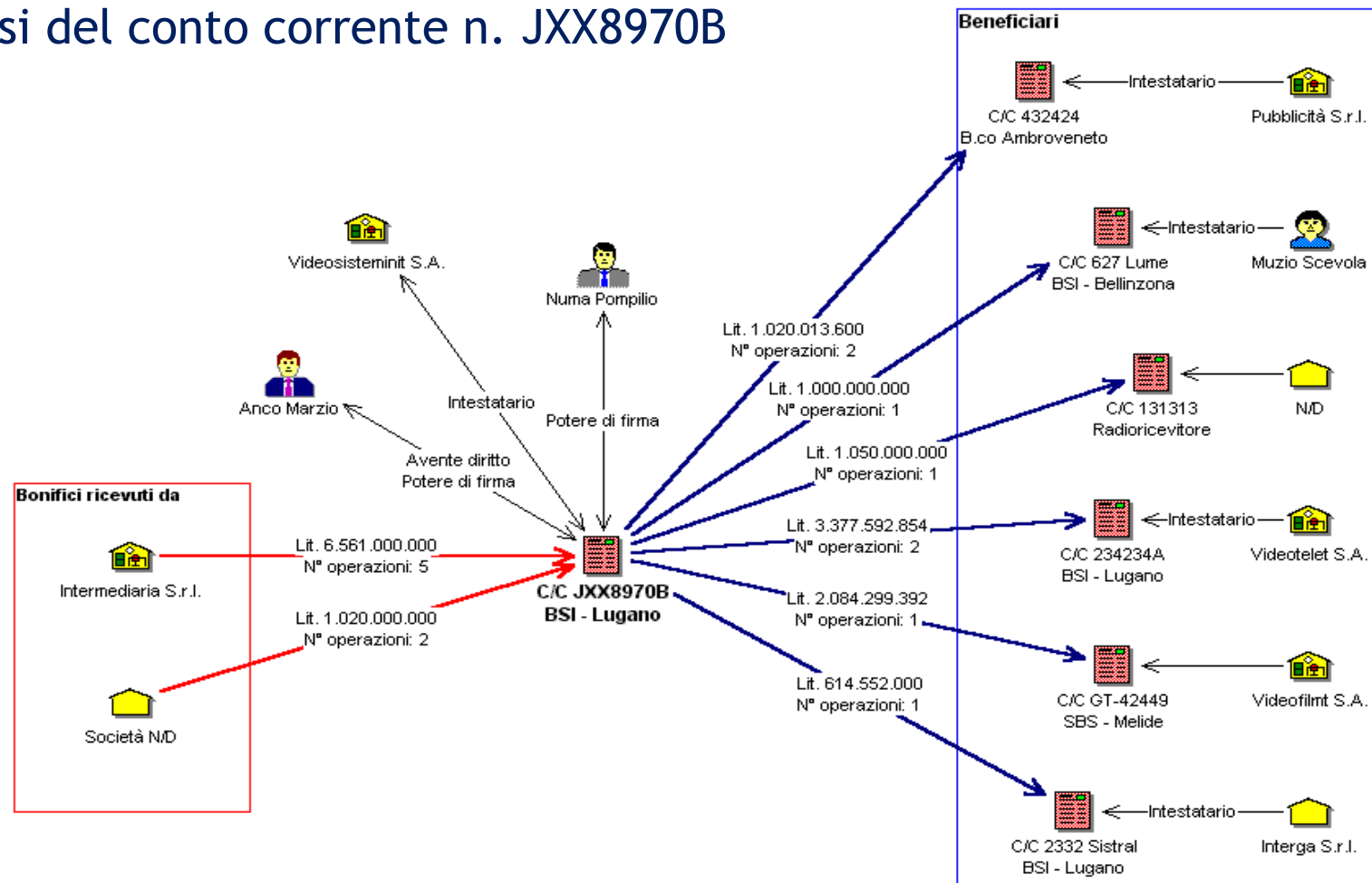


Microsoft Access - [Operazioni : Tabella]

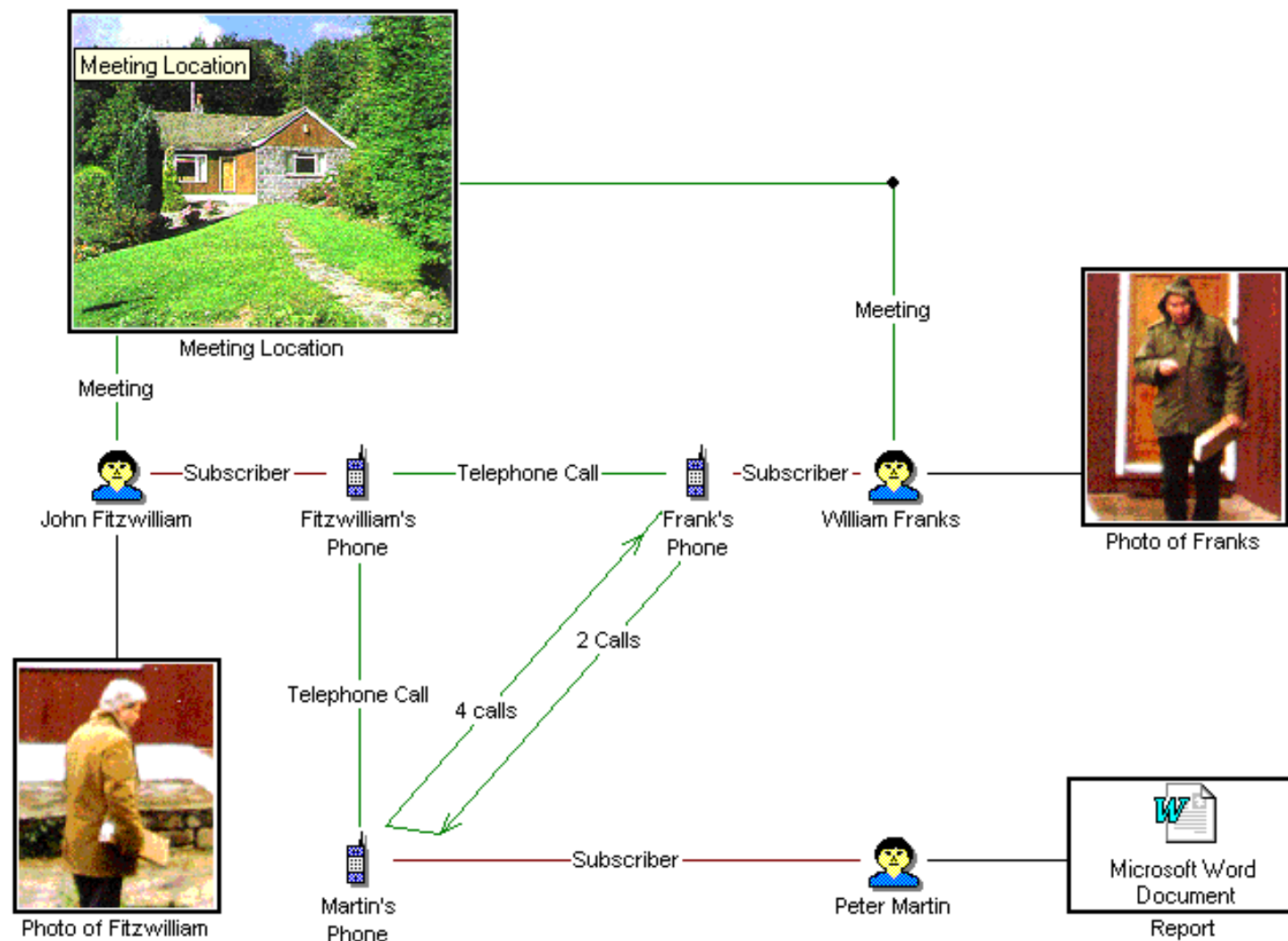
ContoCorrenteBeneficiario	ModalitàPaga	DataOperazione	ImportoLire	Causale
2.0 23-8	Bonifico	16/08/95	1.049.800.000	Swift Transfer Or
270660.0_1.0	Bonifico	14/09/95	L. 1.199.800.000	Swift Transfer Or
864_67-7	Bonifico	14/12/95	L. 1.299.800.000	
366	Bonifico	29/12/95	L. 1.749.800.000	Swift transfer ord
206-00-0427293	Bonifico	27/12/95	L. 1.749.981.000	Fattura 1/A

VISUAL INTELLIGENCE ANALIYSIS... (2004)

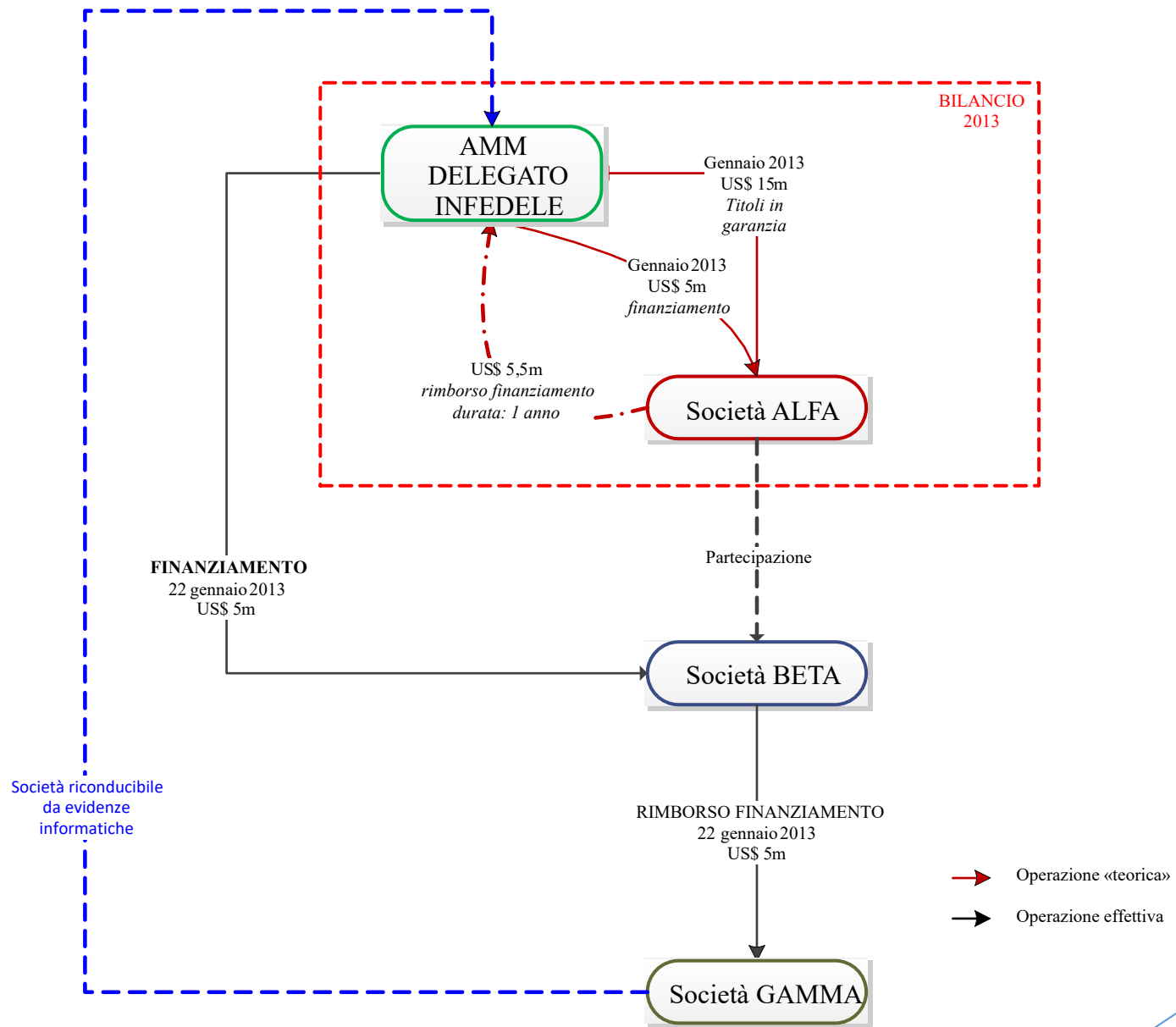
Analisi del conto corrente n. JXX8970B



VISUAL INTELLIGENCE ANALYSIS... (2004)



OPERAZIONE FINANZIAMENTO



PROBLEMATICHE

- 1) QUESITI TECNICI SEMPRE PIU' ARTICOLATI
- 2) IMMENSA MOLE DI DATI AZIENDALI CONTENUTA NEI DISPOSITIVI DIGITALI DA ESAMINARE
- 3) DATI NON ORGANIZZATI PROVENIENTI DA PIATTAFORME DIVERSE
- 4) DATI ARCHIVIATI NEL CLOUD E/O SU SERVER PRESERNTI IN ALTRI PAESI
- 5) FLUSSI DI DENARO IN CRIPTOVALUTE E UTILIZZO DEL DARK WEB
- 6) FORMAZIONE MULTIDISCIPLINARE (LINGUE, INFORMATICA, LEGALE/GIURIDICA ECCETERA)
- 7) RIDUZIONE DEL TEMPO A DISPOSIZIONE DEL CT
- 8) RIDUZIONE DEL BUDGET A DISPOSIZIONE DEL CT

ESEMPIO DI QUESITO INFORMATICO E IN MATERIA CONTABILE:

"il consulente informatico proceda:

- ***ad effettuare la copia forense del materiale informatico sequestrato durante le operazioni di perquisizione e sequestro svolte dalla PG delegata;***
- ***a recuperare i file e i messaggi di posta elettronica cancellati e/o danneggiati;***
- ***a decifrare eventuali file protetti da password;***
- ***a convertire i file in formato immagine contenenti testo in formato ricercabile (mediante processi di OCR);***
- ***a rendere fruibili le informazioni estratte dai sistemi informativi affinché sia possibile effettuare un'attività di ricerca;***
- ***ad identificare eventuali altri dispositivi digitali e caselle o server di posta elettronica, allo stato non oggetto di provvedimento di sequestro, contenenti dati elettronici utili alle indagini."***

"il consulente contabile, esaminato il contenuto dei dispositivi digitali indicizzati e resi ricercabili dal consulente tecnico informatico, nonché tutta la documentazione depositata in atti, comprese le annotazioni redatte dalla polizia giudiziaria operante, i verbali di sommarie informazioni testimoniali, gli atti delle procedure fallimentari, nonché, ove ritenuto necessario, l'ulteriore documentazione di natura societaria e aziendale detenuta presso professionisti terzi, accerti:

INFORMATICA FORENSE: LE TRE FASI

1. *ACQUISIZIONE INFORMATICA DEI DISPOSITIVI DIGITALI*
2. *ESTRAZIONE INFORMATICA DEI DATI DIGITALI*
3. *ANALISI INFORMATIZZATA DEL MATERIALE ACQUISITO AL PP*

ACQUISIZIONE DEI DISPOSITIVI INFORMATICI

E' la fase dell'acquisizione informatica dei dispositivi digitali.

Il CT informatico in questa fase redige un verbale delle operazioni compiute, indicando gli elementi che assicurano l'utilizzabilità del dato digitale in sede dibattimentale (calcolo del codice hash, inserimento di time stamp e firma digitale, realizzazione di copie di sicurezza cautelate in buste antieffrazione eccetera)

Il dato informatico, affinché possa essere utilizzato, deve essere acquisito:

- ▶ Con software/hardware di acquisizione aggiornati e certificati
- ▶ Attraverso protocolli che assicurino che il dato acquisito sia:
 - ▶ Completo (non vi possono essere acquisizioni parziali)
 - ▶ Integro (non deve essere stato corrotto dall'operazione di acquisizione)
 - ▶ Fruibile e leggibile (accessibile alle parti del processo)
 - ▶ Affidabile e imm modificabile (tipico nei sistemi contabili)
 - ▶ Ripetibile applicando i medesimi criteri di acquisizione

ESTRAZIONE DEL DATO DIGITALE

Successivamente alla fase di acquisizione il CT informatico dovrà estrarre:

- ▶ i file acquisiti nei vari formati Microsoft Office, mdb, pdf, immagini, video, audio, archivi compressi eccetera
- ▶ i messaggi posta elettronica (privata e aziendale);
- ▶ i messaggi inviati con altri strumenti alternativi alla posta elettronica (chat, web mail, skype ecc.);
- ▶ il contenuto di smartphone, ipad, ipod, iwatch, sistemi di navigazione eccetera.

Dovrà inoltre:

- ▶ recuperare i file e i messaggi di posta elettronica cancellati («data carving»);
- ▶ aprire/decifrazione i file protetti da password;
- ▶ rendere i file in formato pdf e tiff ricercabili (con procedura OCR);
- ▶ creazione di un ambiente di ricerca unico affinché il CT economico-finanziario e contabile possa compiere gli accertamenti richiesti dall'AG.

ESTRAZIONE INFORMATICA DELLA CONTABILITA'

Rispetto alle metodologie classiche di estrazione dei dati, ora è possibile clonare il sistema gestionale contabile.

Attività:

- ▶ analisi del sistema gestionale-contabile in uso in azienda;
- ▶ Verifica dell'architettura, della struttura e della quantità di dati memorizzati in funzione dell'arco temporale da estrarre;
- ▶ definizione delle procedure di estrazione dei dati (in formato pdf, xls o txt);
- ▶ estrazione dei dati contabili seguendo i riconosciuti protocolli di informatica forense;
- ▶ Creazione di un database che «replica» il sistema gestionale contabile, finalizzato all'interrogazione e all'estrazione dei dati (schede contabili, partitari, bilanci di verifica, piano dei conti, libro giornale, eccetera).

ANALISI INFORMATIZZATA DEL DATO

La terza fase riguarda:

- ▶ la valutazione del materiale digitale acquisito (finalizzata ad individuare possibili difetti nella procedura di acquisizione);
- ▶ l'individuazione di ulteriori supporti informatici sfuggiti all'acquisizione (PC, chiavette USB, HD esterni, DVD, CD, flash memory, SandDisk, SIM card eccetera).
- ▶ le caratteristiche dei file al momento dell'acquisizione attraverso l'esame dei «metadati» (dimensione, formato, ultimo salvataggio, data di creazione, ultima data di stampa, identificazione del proprietario e dell'autore, del software utilizzato per creare il file eccetera);
- ▶ L'UTILIZZO DI SOFTWARE INVESTIGATIVI (Magnet Axion, DTSearch, Intella, Exterro-FTK, Autopsy Digital Forensics, X-Ways, Cellebrite Inspector eccetera)

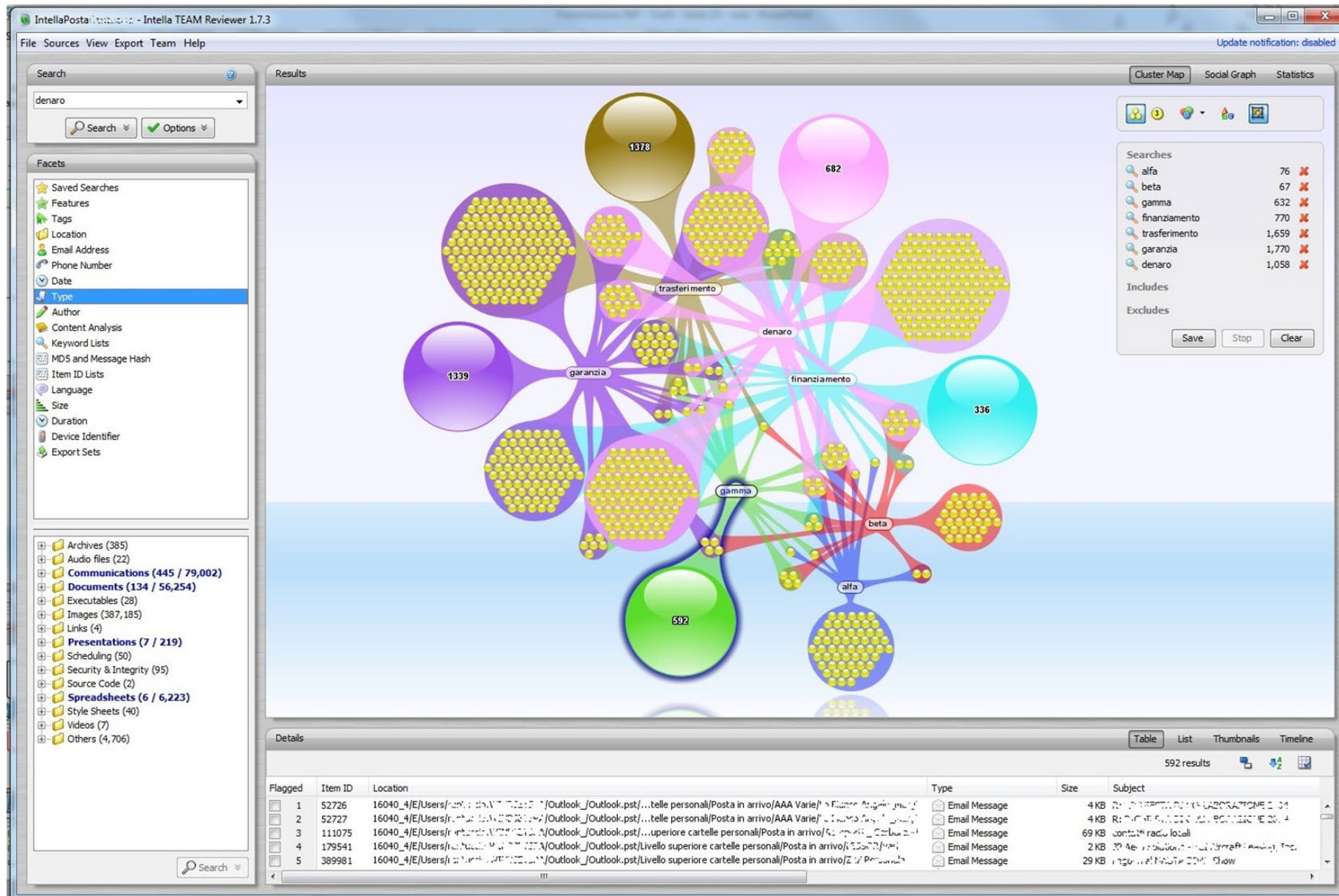
Qualche dato su indagini fatte

- ▶ Procura di Catania (2012-2013):
 - ▶ Wind Jet:
 - ▶ PC/server/HD acquisiti: n. 63
 - ▶ Smartphone: n. 7
 - ▶ Gestionali contabili: n. 5
 - ▶ File esaminati: circa 1 milione
 - ▶ Email esaminate: circa 100.000
- ▶ Procura di Civitavecchia (2018-2019):
 - ▶ Alitalia SAI:
 - ▶ Dimensione dei dati digitali esaminati: 18 terabyte
 - ▶ File esaminati: poco più di 90 milioni
 - ▶ Email esaminate: circa 4.000.000

Qualche dato su indagini fatte

- ▶ Procura di Catania (2021):
 - ▶ ??:
 - ▶ File esaminati: circa 12 milioni
 - ▶ File cancellati e recuperati: circa 100.000
 - ▶ Email esaminate: circa 900.000
 - ▶ Documenti pdf e Microsoft Office esaminati: circa 800.000
 - ▶ Immagini esaminate: circa 6.400.000
 - ▶ Audio esaminati: n. 11.000 di cui rilevanti 500

IL SOFTWARE INVESTIGATIVO



Evidence

								
Total Count	575,272	1,095	1,088	50,380	2,431	346,528	8,295	51,345
Deduplicated	330,448	689	686	11,732	1,825	153,442	5,296	30,127
	All Items	Encrypted	Decrypted	OCRed	Exception items	Irrelevant	Extraction Unsupported	Recovered

Types

Communication

E-mail	128,920
 Email Message	99,588
 Delivery Status Notification	16,712
 Email Headers	12,620
Contacts	3,695
 vCard File	3,695
Other communications	7
 Outlook Rule Message	7

User activity

Scheduling	2,212
 iCalendar/vCalendar File	2,212
www	3
 Internet Location (URL)	3

Documents

Word processing	41,375
 PDF Document	37,049
 Microsoft Word Document	4,199
 Rich Text Document	104
 OpenDocument Text	20
 Microsoft Publisher Document	2
 Acrobat Forms Data Format	1
Presentations	92
 Microsoft PowerPoint Presentation	92
Spreadsheets	2,041
 Microsoft Excel Workbook	2,037
 OpenDocument Spreadsheet	2
 OpenOffice Spreadsheet	2
Graphics	1,796
 AutoCAD DWG File	1,795
 Adobe Photoshop Image	1
Other documents	10,433
 Plain Text Document	9,660
 HTML Document	511
 AutoCAD Template	152

Media

Images	375,080
 JPEG Image	129,259
 PNG Image	127,524
 TIFF Image	113,652
 GIF Image	1,642
 WMF Image	1,376
 EMF Image	1,172
 BMP Image	451
 Icon	3
 WebP Image	1
Video	46
 Windows Media Video Clip	16
 AVI Video Clip	13
 MPEG Video Clip	8
 MPEG-4 Video File	6
 3GPP Multimedia File	3
Audio	114
 WAV Audio Clip	112
 MIDI Audio Clip	2

Containers

E-mail container	 Microsoft
Databases	 Microsoft
Archives	 Zip Archiv
	 Gzip Archi
	 Rar Archiv
	 Microsoft
	 7-Zip Arch
	 InstallShie
Wrappers	 OLE 2.0 C

PII in Metadata

Type	Values	
@ Email Address	16,582	
Phone Number	149	
Chat Account	0	
Creator	1,322	
Contributor	576	

Social media

 Ask.fm	0	 Instagram	0	 Twitter	0
 ClassMates	0	 LinkedIn	0	 VK	0
 Facebook	0	 Meetup	0	 Vine	0
 Flickr	0	 Pinterest	0	 YouTube	0
 Google+	0	 Tumblr	0		

Top 10 email addresses

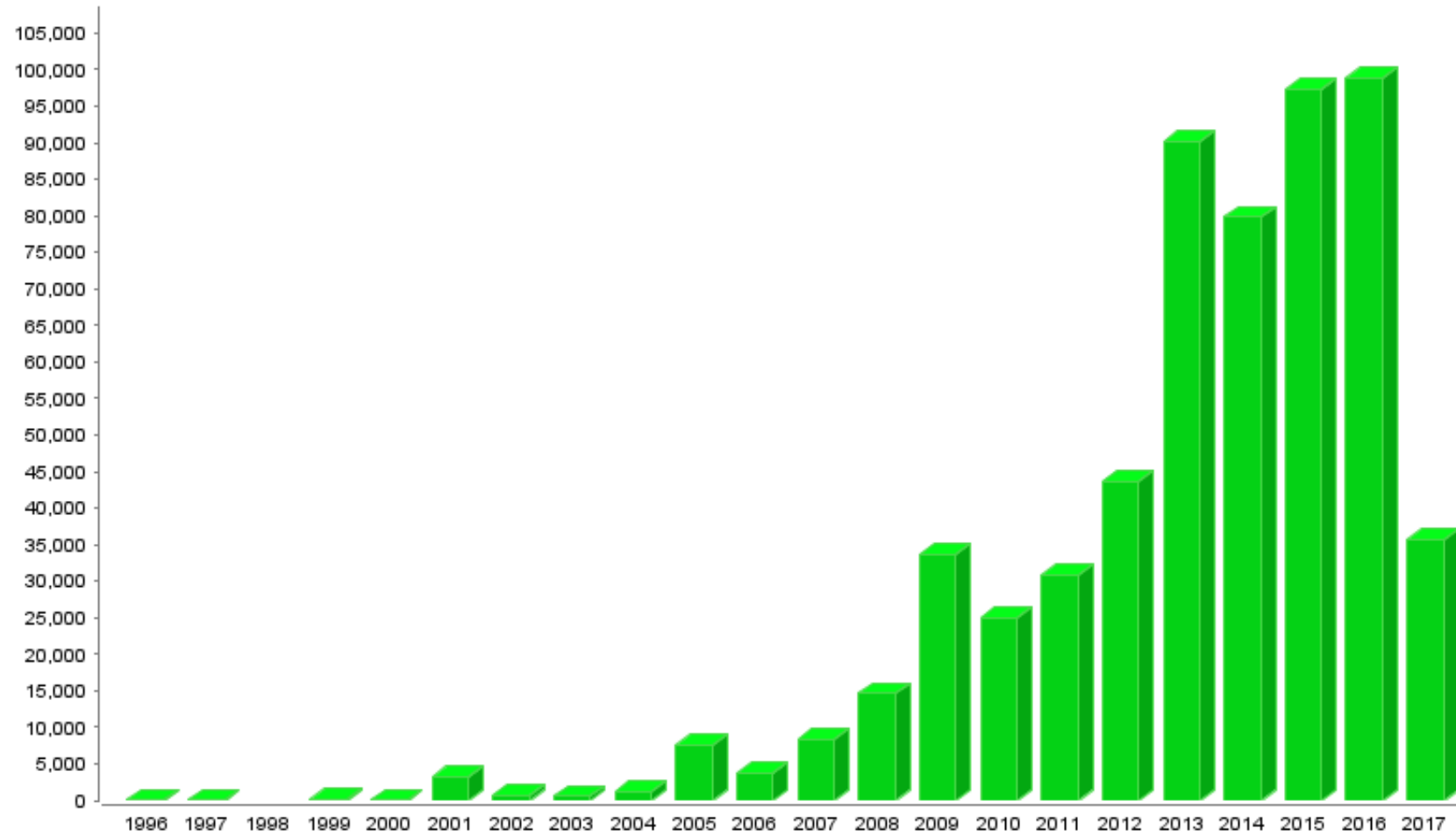
Email Address	Number of e...	Deduplic...
██████████@rosario.it	78,248	75,862
/o=windom/ou=first administrative group/cn=recipients/c...	77,623	72,942
mailer-daemon@mailrelay1.rossoxweb.com	10,357	10,228
postmaster@██████████.it	9,353	7,931
.	7,727	7,585
/o=windom/ou=first administrative group/cn=recipients/c...	6,528	6,445
/o=windom/ou=first administrative group/cn=recipients/c...	4,808	4,741
davide@██████████.it	3,992	3,864
renato@██████████.it	3,093	3,027
/o=windom/ou=first administrative group/cn=recipients/c...	2,695	2,638

Top 10 host names

Host name	Number of emails	Deduplicated
rosario.it	86,912	84,356
mailrelay1.rossoxweb.com	10,367	10,238
libero.it	7,526	7,049
gmail.com	6,743	6,510
studio██████████.it	6,583	6,301
alice.it	2,909	2,815
credem.it	2,878	2,847
fas-fumane.com	2,680	2,622
██████████.com	1,439	1,042
virgilio.it	1,431	1,327



Timeline



Keyword Search

Enter Keyword Search...

Options

Search

Facet Search

★ Saved Searches

Features

Tags

Identities

Custodians

Location

@ Email Address

Phone Number

Chat Account

Recipient Count

31 Date

Type

Author

Content Analysis

Email Thread

Near-Duplicates

Keyword Lists

MD5 and Message Hash

Item ID Lists

Language

Size

Duration

Device Identifier

Export Sets

returns all documents that contain the word "intella" in their title. The following field names are available:

text - searches in the text of the document or email

title - searches in document titles and email subjects

path - searches in file and folder names

summary - searches in descriptions, metadata keywords, etc.

agent - searches in authors, contributors and email senders and receivers

from - searches in email From fields

sender - searches in email Sender fields

to - searches in email To fields

cc - searches in email Cc fields

bcc - searches in email Bcc fields

headers - searches in the raw email headers

rawdata - searches in the document raw data

comment - searches in the comments made by reviewers

export - searches in the export IDs of the documents that are part of any export set

Facet Search

★ Saved Searches

Features

caratteristiche

- Encrypted (1,095)
- Decrypted (1,088)
- Unread (1,314)
- Empty Documents (31,989)
- Has Duplicates (298,042)
- Has Shadow Copies (0)
- Has Geolocation (295)
- Downloaded from Internet (0)
- OCRed (50,380)
- Has Imported Text (0)
- Content Analysed (0)
- Exception Items (2,431)
- Extraction Unsupported (8,295)
- Text Fragments Extracted (0)
- Irrelevant (346,528)
- Threaded (0)
- Recovered (51,345)
- Attached (108,228)
- Has attachments (51,188)
- Embedded images (342,702)
- Tagged (0)
- Flagged (0)
- Commented (0)
- Previewed (50)
- Opened (37)
- Exported (0)
- Redaction (0)
- Batched (0)
- Top-level parents (110,620)
- Item stubs (2)
- W4 Delta (0)
- Analyzed for Near-Duplicates (0)
- Has Near-Duplicates (0)
- All Items (575,272)

Stefano Martinazzo

Dipartimento di Forensic Accounting, Internal Audit & Litigation

Dottore Commercialista, Ordine di Milano

Revisore Legale dei Conti

stefano.martinazzo@axerta.it

ODCEC di Bologna

21 novembre 2022

Stefano Martinazzo

Dipartimento di Forensic Accounting, Internal Audit & Litigation - AXERTA S.p.A.

Dottore Commercialista, Ordine di Milano

Revisore Legale dei Conti

stefano.martinazzo@axerta.it