Cybercrime e Forensics

Datamatic Sistemi & Servizi

DFA OPEN DAY 2015

Agenda

- Cybersecurity Market
- Chi siamo
- Cosa facciamo
- Nuovi trend del Cybersecurity: Moblile, Cloud, Social
- Demo

Cybersecurity Market

4 giugno 2015

Usa, massiccio attacco hacker agli uffici federali

Secondo il "Washington Post" e il "Wall Street Journal" l'operazione sarebbe stata opera di hacker di stanza in Cina

00:23 - Una massiccia violazione a opera di hacker è stata messa segno ai danni di alcuni uffici federali americani e Washington è già a lavoro per stabilire l'entità dell'attacco. Lo riferisce la Associated Press. Secondo una fonte informata citata dall'agenzia americana, è stato colpito l'ufficio risorse umane del governo.

8

10

"2011: il fatturato dell'industria "Cybercrime" è superiore al fatturato dello spaccio di droga, traffico degli esseri umani e di armi!"

Varie fonti(ex. UN, USDOJ, INTERPOL, 2011)

Stima del fatturato 2011: 6-12 BLN USD$/year

«Il Cybercrime è il 4° crimine economico»……

da tecnologico è divenuto un problema di business….

PriceWaterhouseCoopers LLC
Global Economic Crime Survey 2014

Cybersecurity Market: Considerazioni

- Istituzioni private, pubbliche e civili divengono sempre più dipendenti dai sistemi informativi e più vulnerabili dagli attacchi sempre più sofisticati di criminali informatici.

- L'informatica è ormai parte irrinunciabile della NOSTRA vita (smartphone, tablet, PC ecc.)

- App sempre più connesse…la prossima rivoluzione è IoX (Internet of Things…il tuo frigo parlerà con il tuo cellulare!)

TUTTO STA DIVENTANDO DIGITALE

Cybercrime: cos'è?

L'**esecuzione di crimini**, mediante l'**ausilio di mezzi informatici**, al fine di **acquisire illegalmente le informazioni** per poter **commettere degli illeciti.**

Furto di Identità
o Personal Info

Furto di Credit Identity
o Financial Info: login bancari, CC/CVV, «fullz», etc

Hacking
o verso e-commerce, e-banking, Credit Processing Centers

Industrial Espionage Malware
o Virus, Worm, Spyware, Key Loggers, Rogue AV, Botnets, Mobile

Hacking su commissione
Attacchi DDoS
o Blackmail, Hacktivism

Spam
Counterfeiting
o medicinali, luxury, prodotti & servizi

Gambling
o Riciclaggio di denaro
o Finti siti e/o non autorizzati (i.e. Italia -> da AAMS)

Porno generico / Pornografia minorile / infantile
o fake sites, etc

Datamatic Sistemi & Servizi : Chi siamo?

- Nata nel 1984 come divisione di Datamatic
- Divenuta Società per Azioni nel 2004
- Presenza commerciale a Milano, Roma, Torino, Napoli, Catania, Bari
- 5 Business Units
- Offerta basata su Prodotti, Servizi, Formazione, Supporto
- Partner Commerciale dei principali leader di mercato
- Certificata ISO 9001
- Fornitore registrato dai più importanti gruppi e consorzi Italiani

Cosa Facciamo

- Portiamo in Italia e mettiamo a disposizione delle Forze dell'Ordine e degli Investigatori che operano nel mercato della Sicurezza e del Cybercrime, le più innovative tecnologie Hardware e Software disponibili nel mondo, atte a contrastare i crimini informatici e ad individuare chi ha perpetrato attività illecite.

I nostri Partner....

cellebrite
delivering mobile expertise

VERITY SYSTEMS

AccessData
A Pioneer in Digital Investigations Since 1987

TABLEAU

Logicube

ELCOMSOFT
PROACTIVE SOFTWARE

SONICWALL

RIMAGE™

MAGNET FORENSICS

QUALYS®

CISCO

GLOBO™


OXYGEN FORENSICS
Helping good people to make this world safer

DELL REGISTERED PARTNER

Nuovi Trend : Mobile, Social, Cloud

- In Italia 97 milioni di abbonamenti mobile attivi: il 58% in più rispetto al totale della popolazione (158%), ossia **una persona su due ha due SIM** mentre la media europea è del 139%.
- Enorme quantità di utenti mobile ma soprattutto l'**impressionante numero degli utenti Facebook attivi rispetto agli utenti internet** (il rapporto è vicino al 73%).
- **293 milioni di utenti attivi** sui Social media in Europa – il 40% della popolazione totale – e il 66% di questi vi accede tramite dispositivo mobile.
- I dati italiani sono in linea con la media europea: gli utenti attivi sono il 42% della popolazione e il 62% di questi utenti accede ai social tramite dispositivo mobile.

Nella maggior parte dei casi criminali c'è sicuramente coinvolto un dispositivo digitale e molto probabilmente questo sarà mobile.

Cloud Analyser

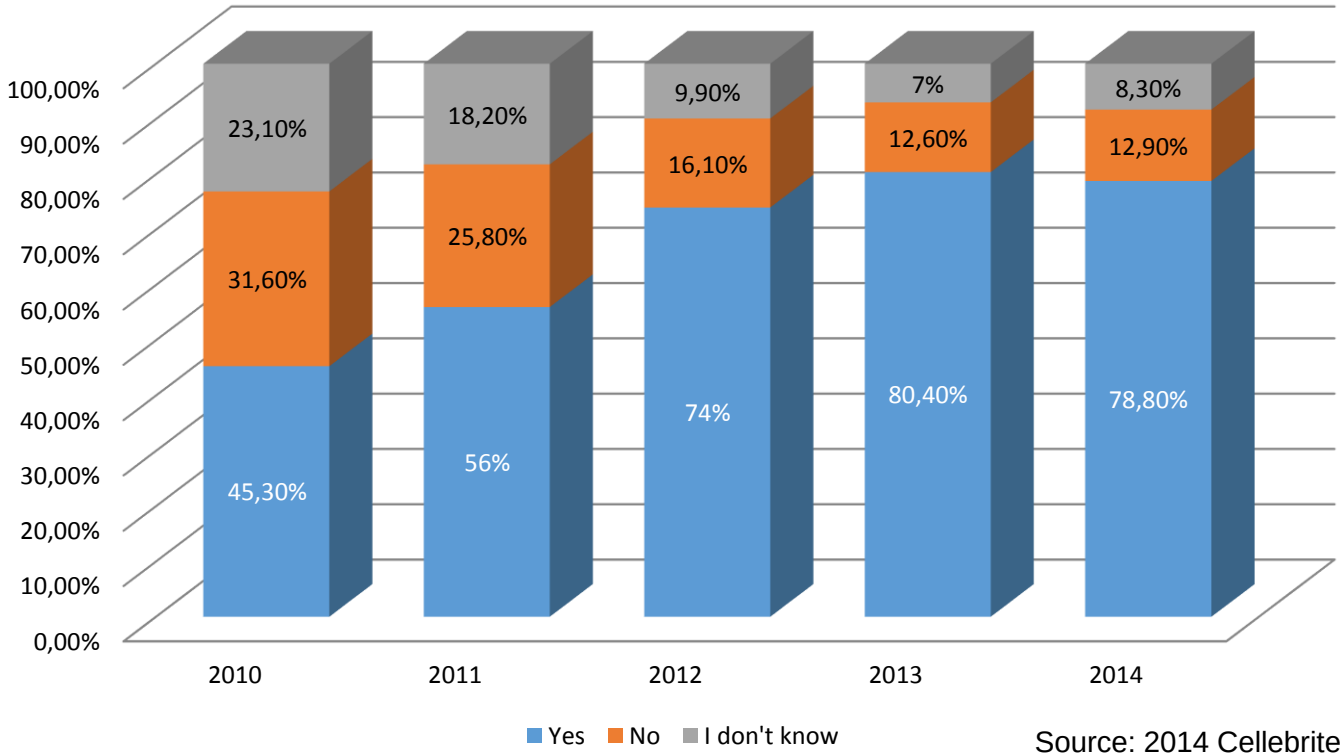
Cellebrite

Cosa si intende per Cloud?

Dati ospitati da un provider di servizi remoti.

- **Social media** - Facebook, Twitter, Google+
- **Web mail** - Gmail, Yahoo, Outlook
- **Storage services** - Google Drive, Dropbox, Box
- **Instant messaging service** - Kik, Whatsapp
- **E-commerce** - Amazon, Ebay

Social media possono aiutare a risolvere il caso?



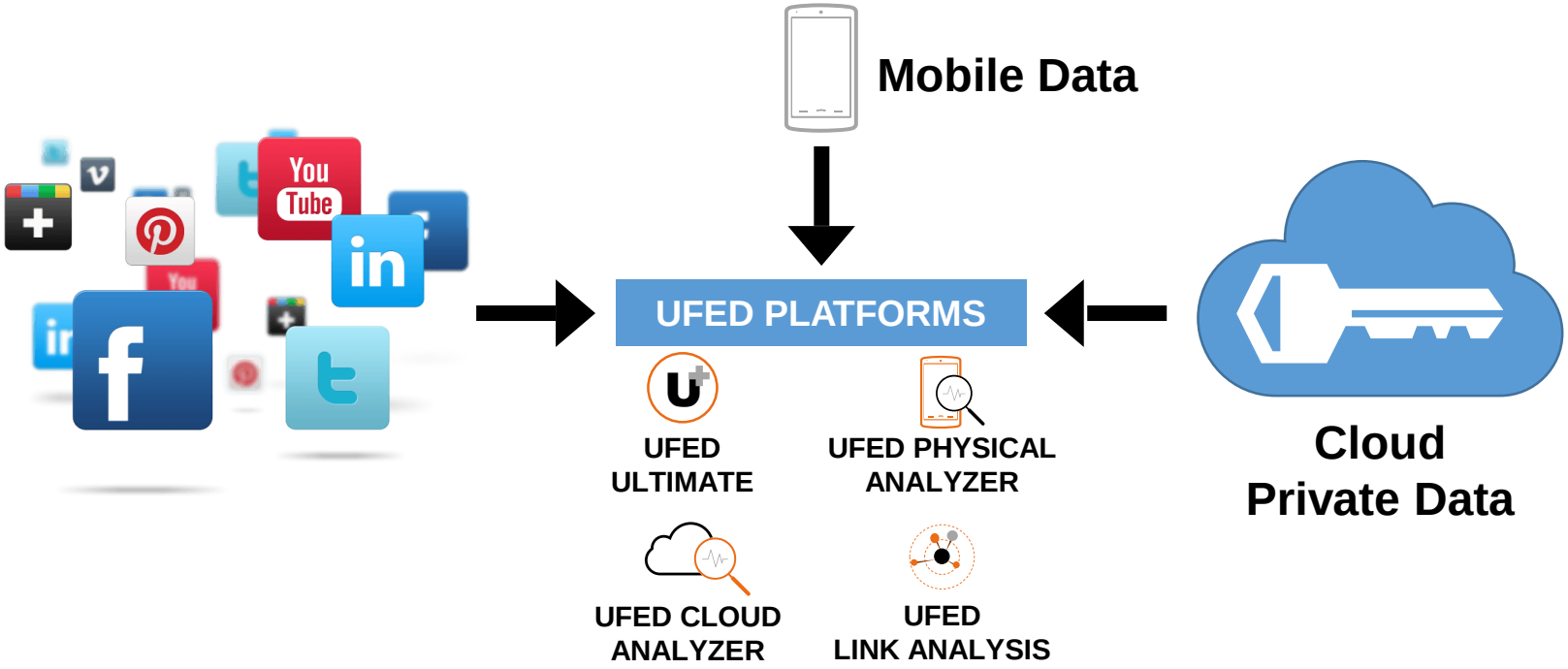
Source: 2014 Cellebrite Customer Survey

Cloud service provider – tempi di risposta?

73% dei clienti intervistati ha dichiarato che la non conformità dei fornitori di servizi con le procedure legali rappresenta un problema.

Source: 2014 Cellebrite Customer Survey

AMBIENTE FORENSE UNIFICATO



datamatic SISTEMI&SERVIZI

UFED Cloud Analyzer

Estrazione istantanea dei dati.

- Accesso al cloud con o <u>senza il consenso.</u>

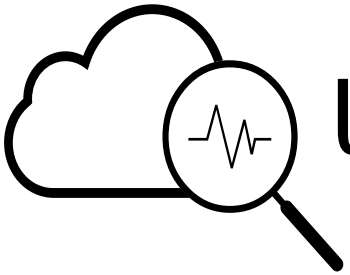
Analisi di diverse piattaforme social in tempo reale.

- Analisi istantanea “Chi? Quando? Dove?”

Report immediato.

- Esporta dati in UFED Link Analisys.

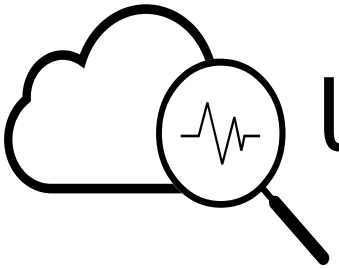
datamatic SISTEMI&SERVIZI



UFED Cloud Analyzer

Video – Demo

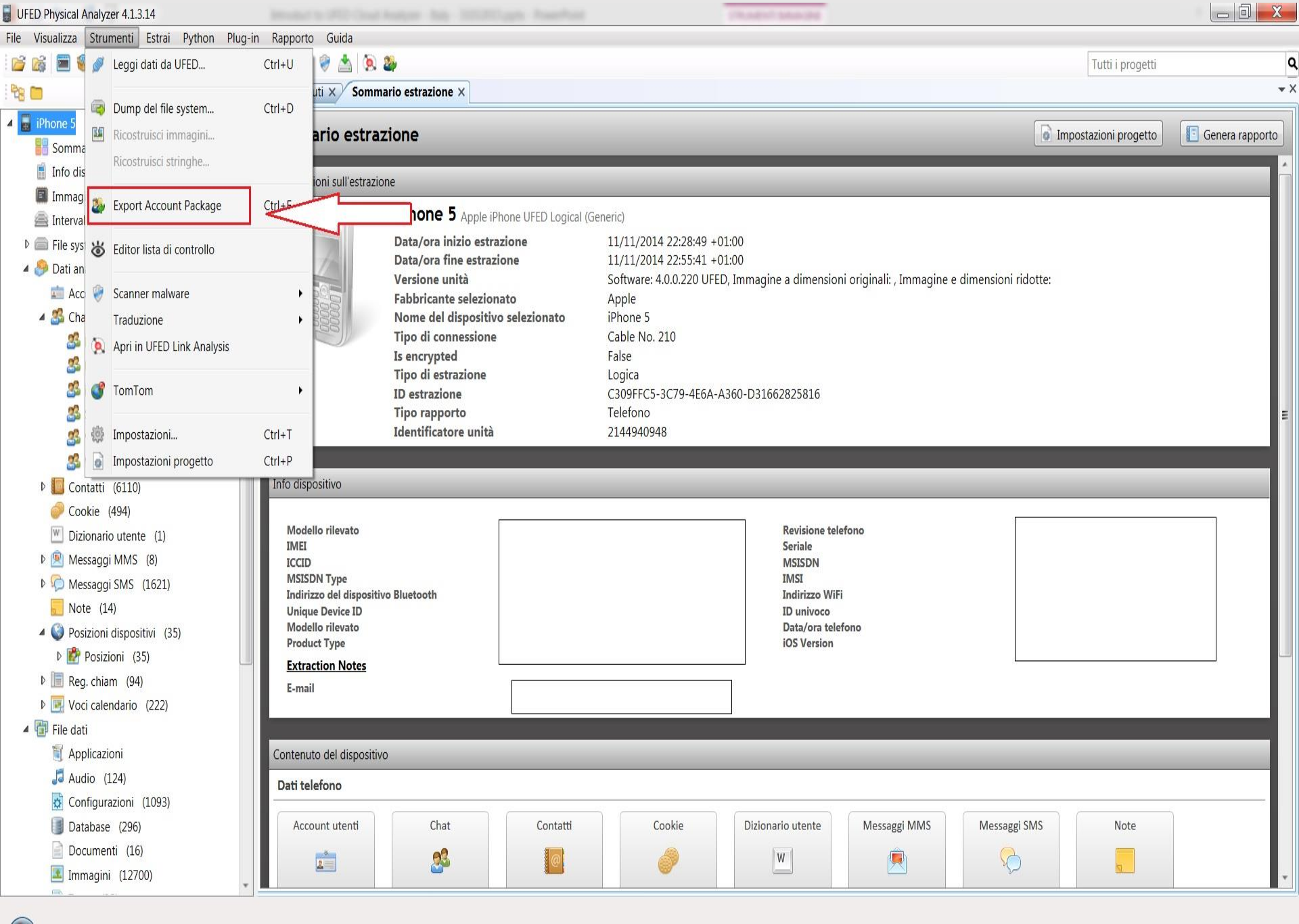
https://youtu.be/821MK_MAuBs



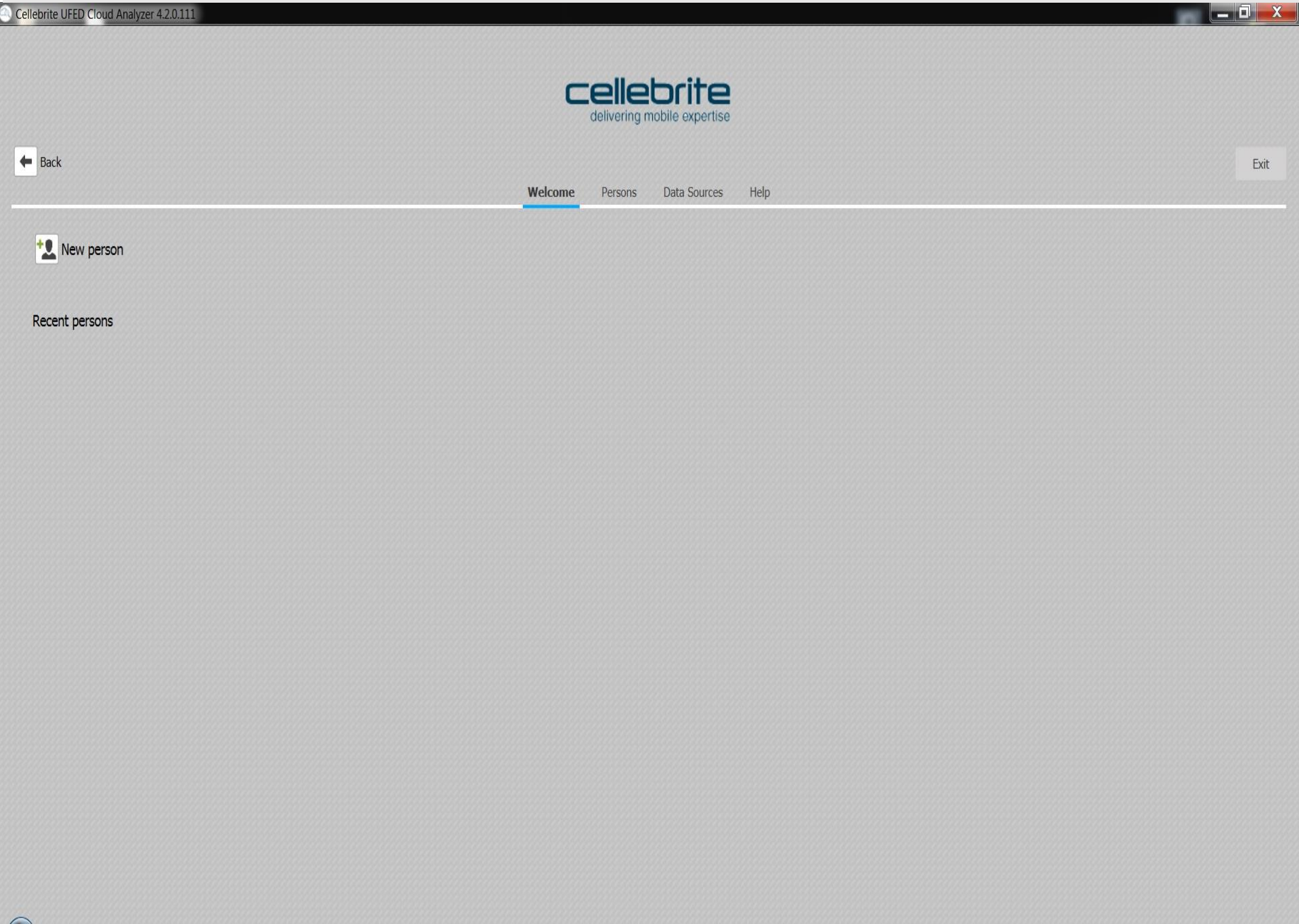
UFED Cloud Analyzer

SLIDE MODE – DEMO

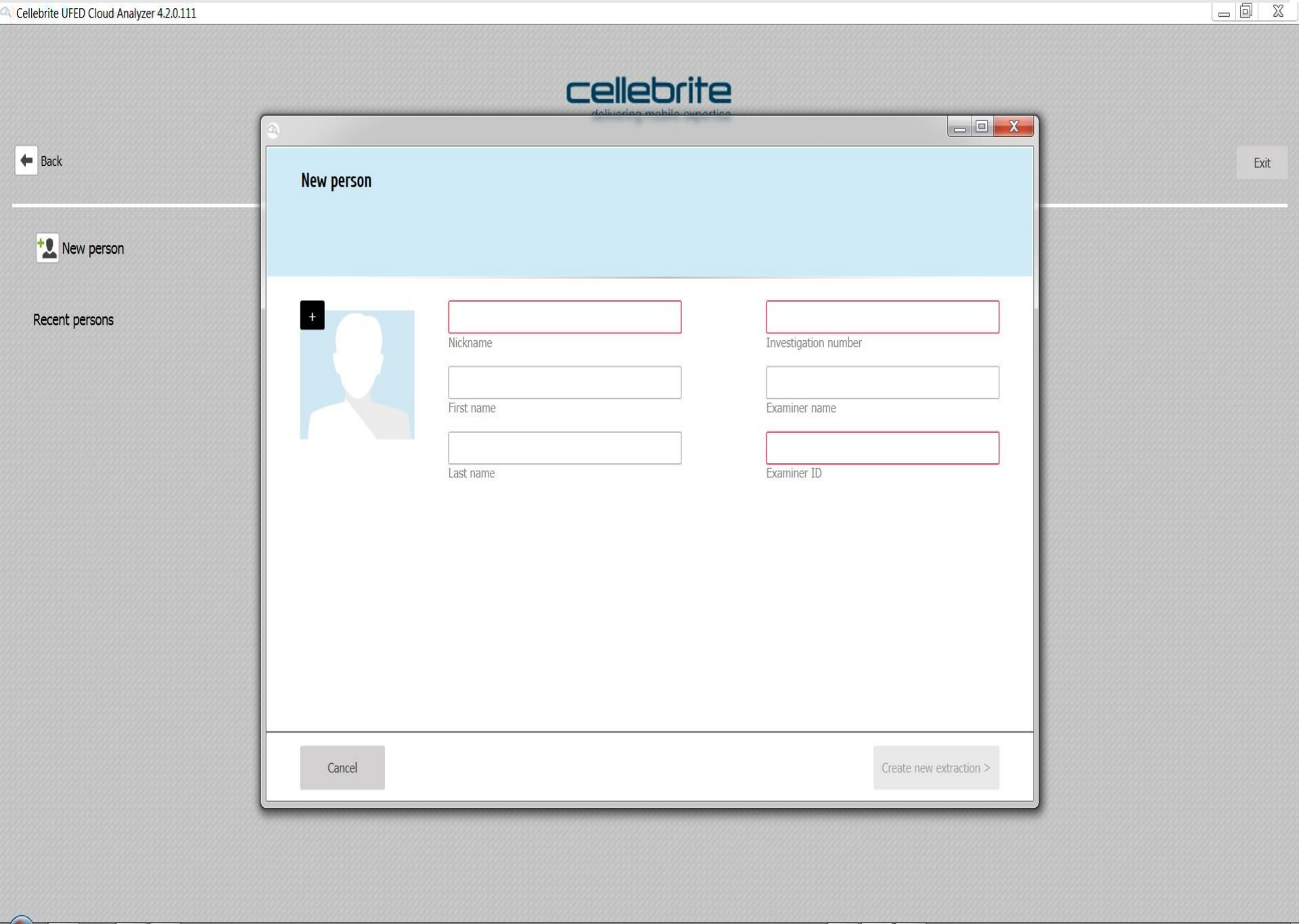
STEP 1 - EXPORT ACCOUNT PACKAGE – UFED PHYSICAL ANALYZER

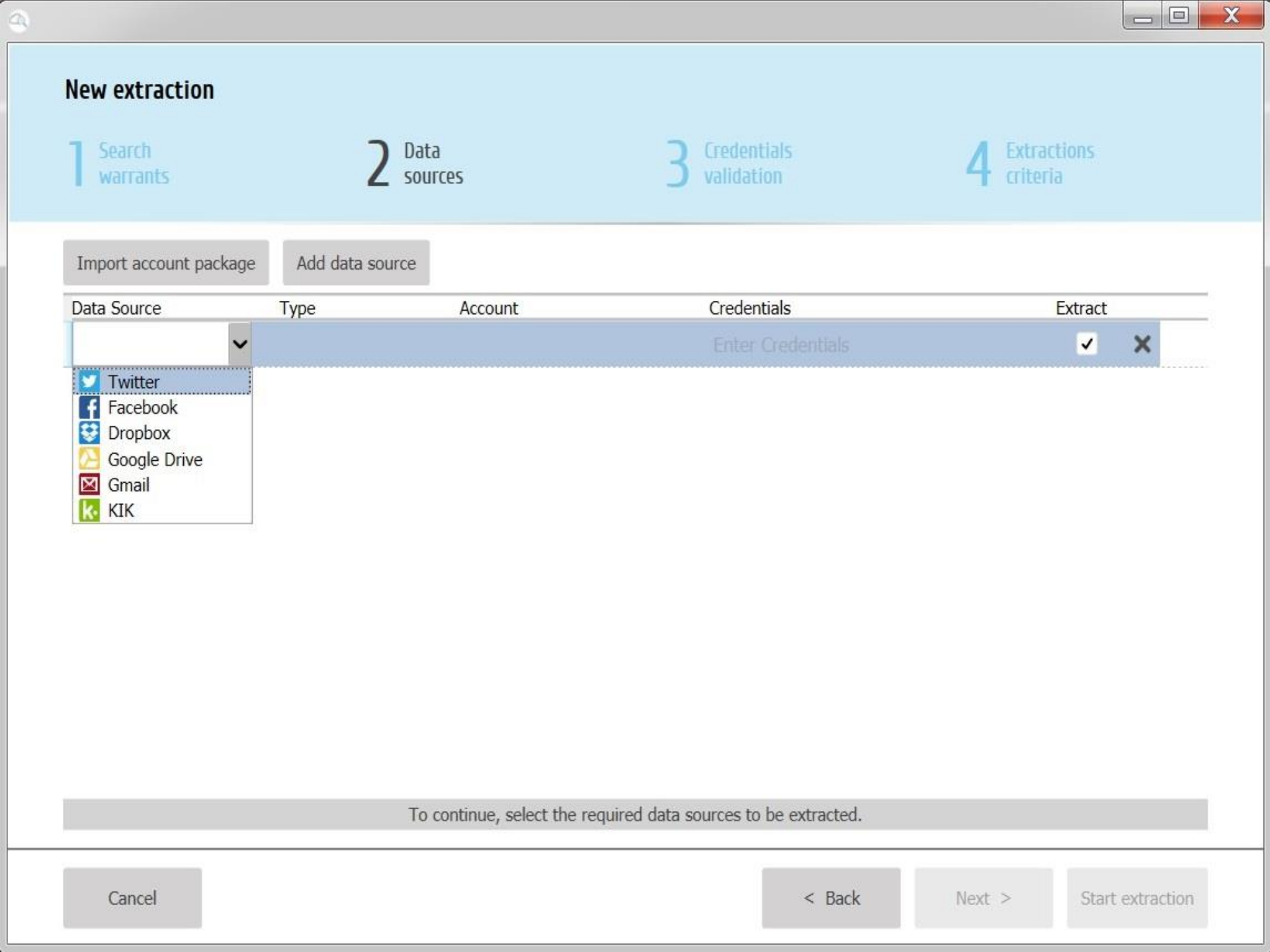


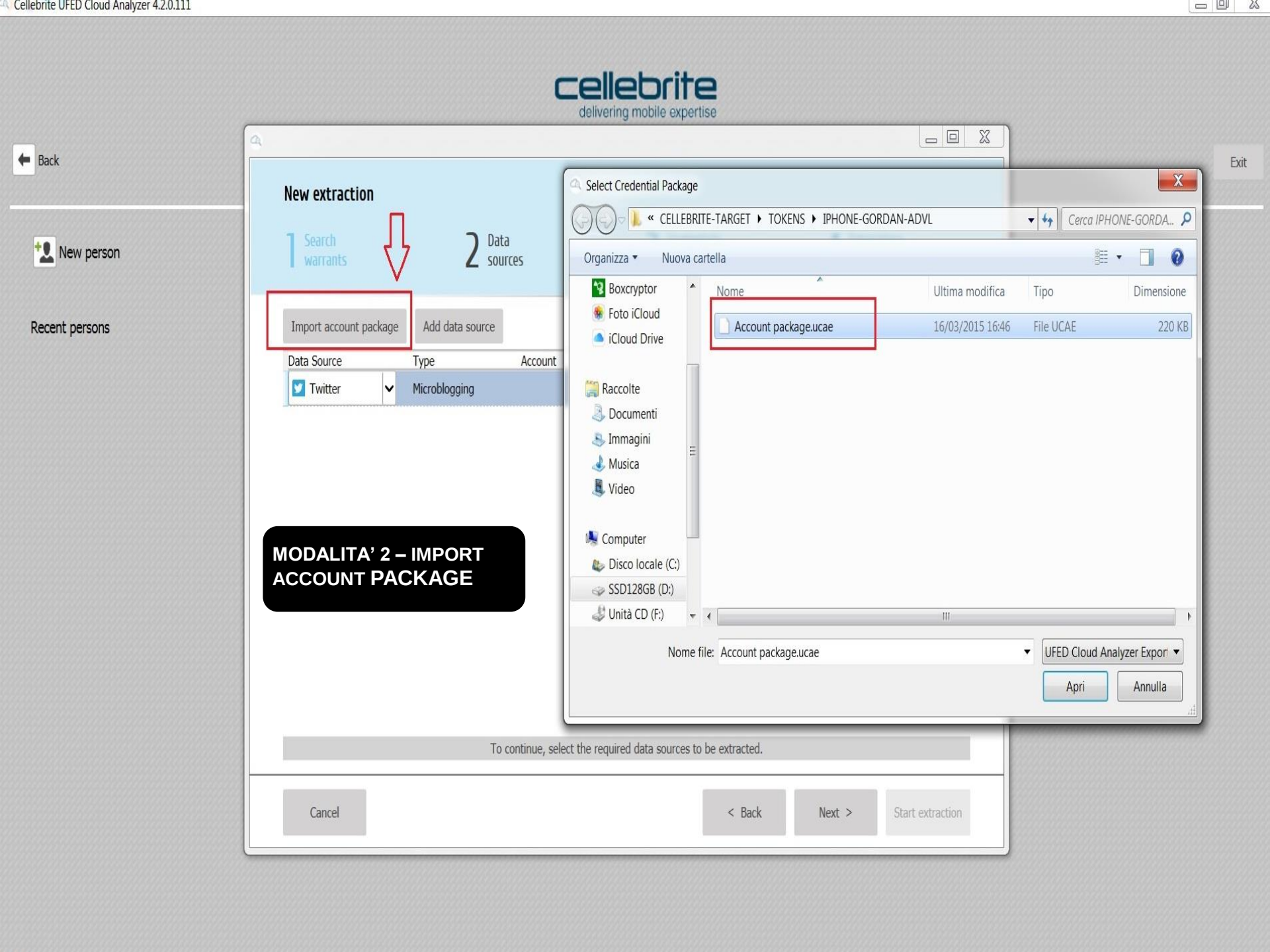
STEP 2 – CLOUD ANALYZER



STEP 3 – INSERIMENTO NUOVA IDENTITA’




New extraction
1 Search warrants
2 Data sources
3 Credentials validation
4 Extractions criteria
Import account package
Add data source
Data Source
Type
Account
Credentials
Extract
Enter Credentials
Twitter
Facebook
Dropbox
Google Drive
Gmail
KIK
To continue, select the required data sources to be extracted.
Cancel
< Back
Next >
Start extraction


Cellebrite UFED Cloud Analyzer 4.2.0.111
cellebrite
delivering mobile expertise
Back
Exit
New person
Recent persons
New extraction
1 Search warrants
2 Data sources
Import account package
Add data source
Data Source
Type
Account
Twitter
Microblogging
MODALITA' 2 – IMPORT ACCOUNT PACKAGE
Select Credential Package
« CELLEBRITE-TARGET ▸ TOKENS ▸ IPHONE-GORDAN-ADVL
Cerca IPHONE-GORDA...
Organizza
Nuova cartella
Boxcryptor
Foto iCloud
iCloud Drive
Raccolte
Documenti
Immagini
Musica
Video
Computer
Disco locale (C:)
SSD128GB (D:)
Unità CD (F:)
Nome
Ultima modifica
Tipo
Dimensione
Account package.ucae
16/03/2015 16:46
File UCAE
220 KB
Nome file: Account package.ucae
UFED Cloud Analyzer Expor
Apri
Annulla
To continue, select the required data sources to be extracted.
Cancel
< Back
Next >
Start extraction

New extraction

1 Search warrants
2 Data sources
3 Credentials validation
4 Extractions criteria

Import account package | Add data source

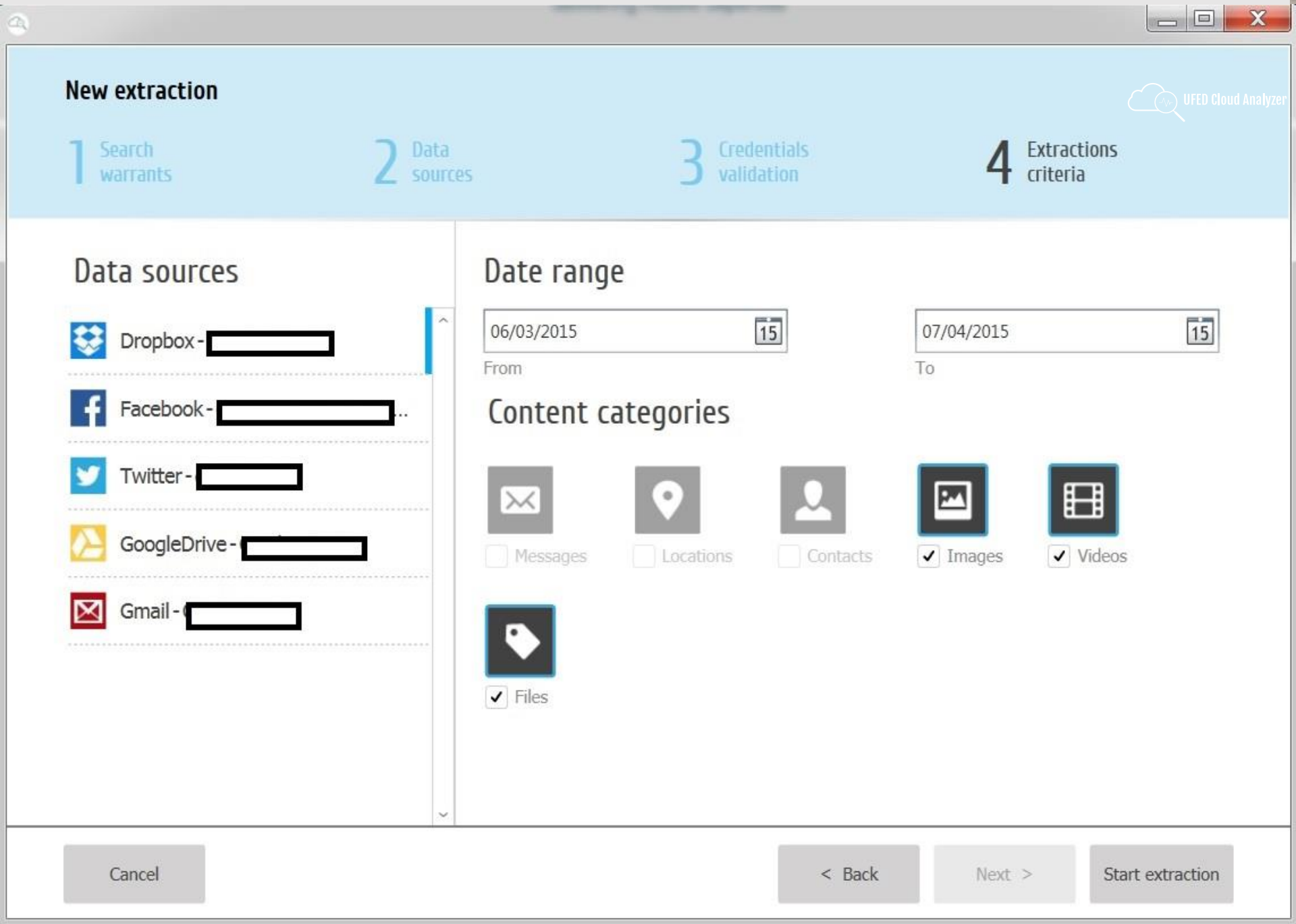
Data Source	Type	Account	Credentials	Extract
Dropbox	Storage service		Available	
Facebook	Social network		Available	
Twitter	Microblogging		Available	

CONTENUTI DISPONIBILI ANALIZZATI DA ACCOUNT PACKAGE

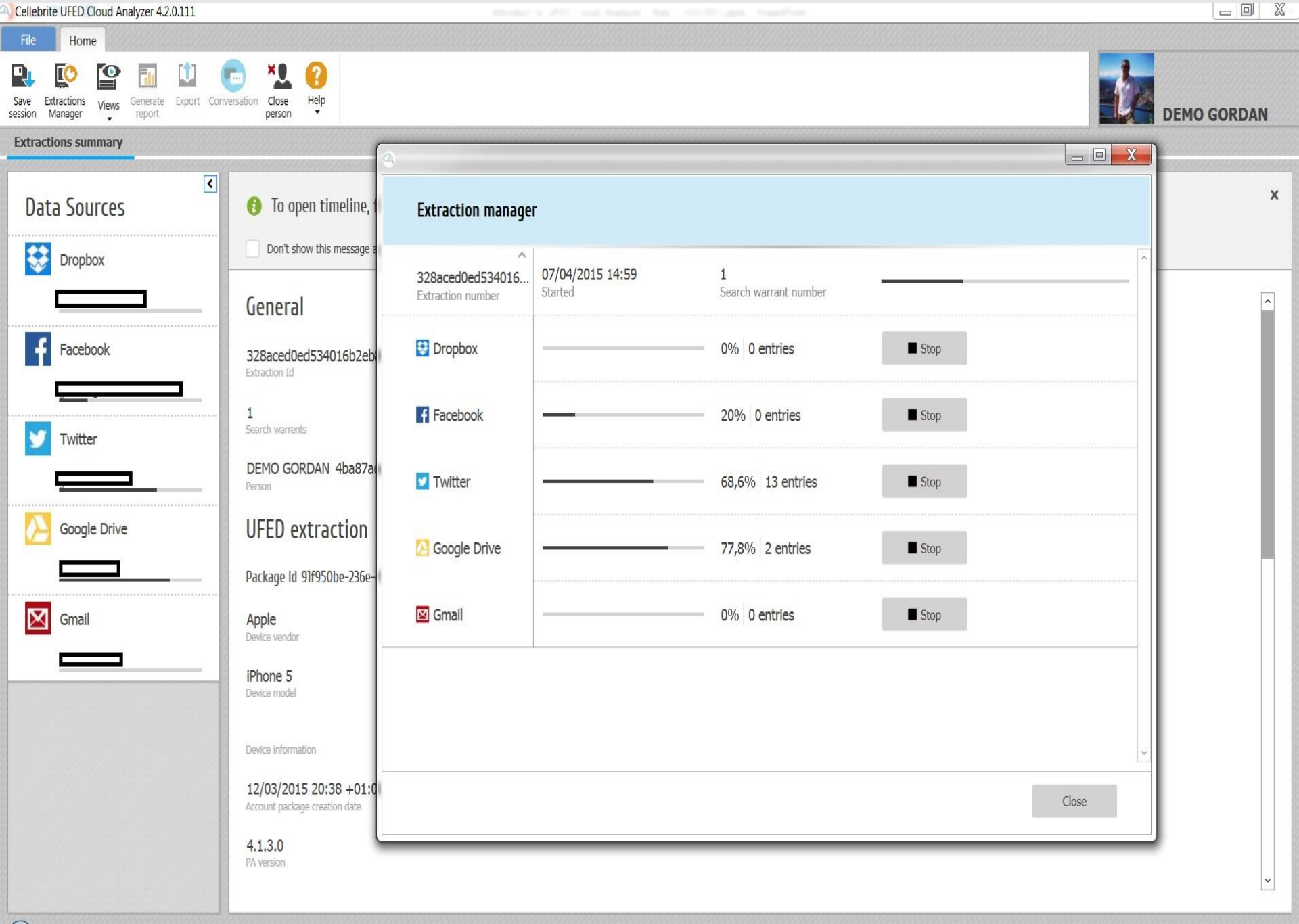
To continue, select the required data sources to be extracted.

Cancel | < Back | Next > | Start extraction

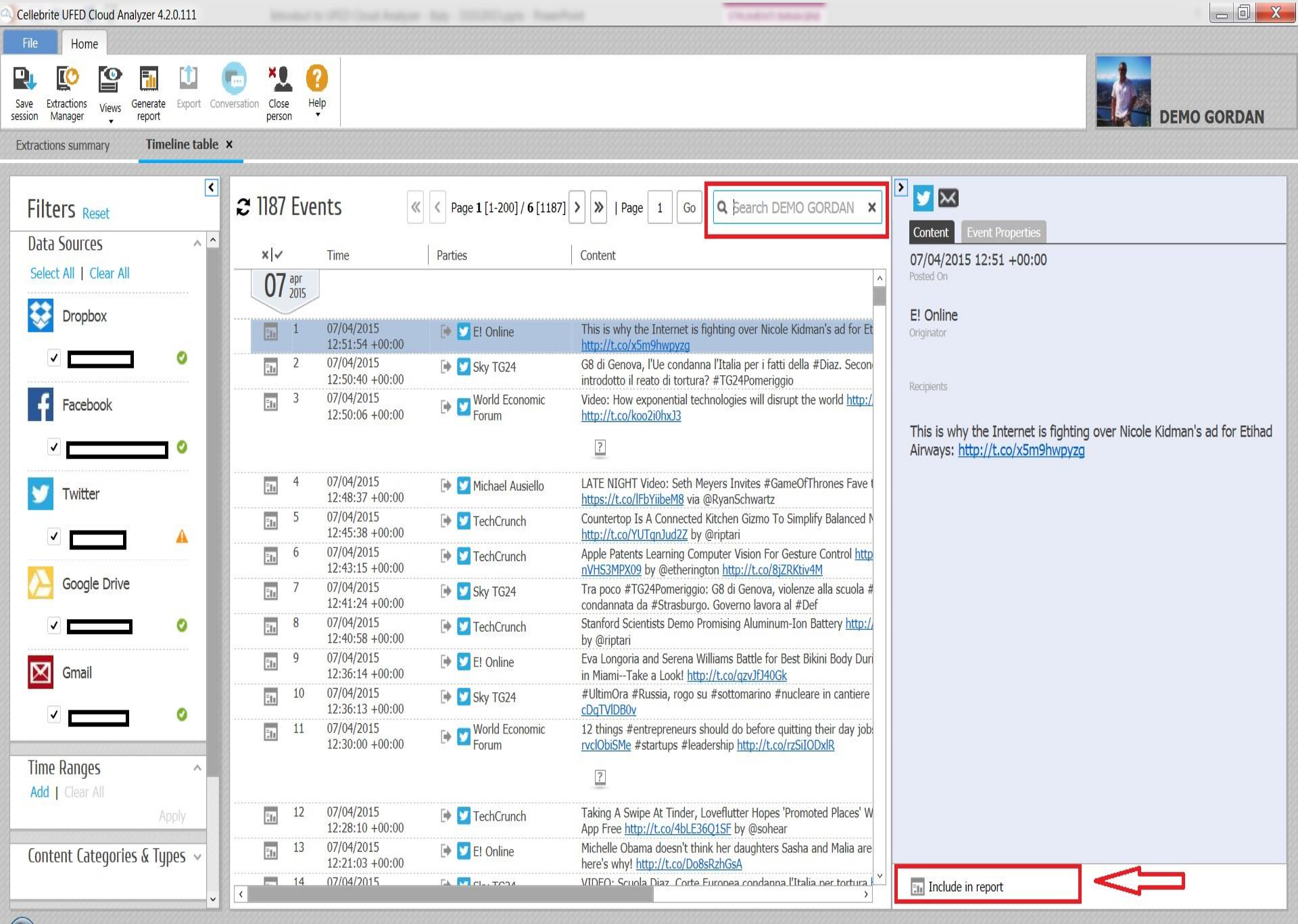
STEP 4 – INSERIMENTO TIMELINE DA ANALIZZARE

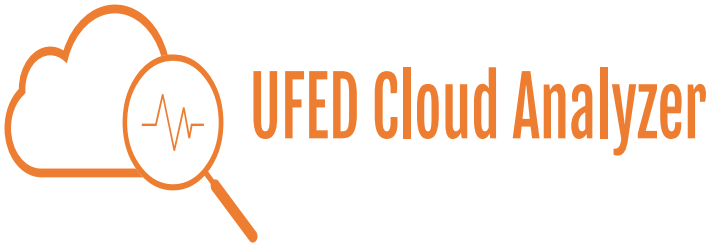


STEP 5 – EXTRACTION MANAGER



STEP 6 – FINE


Cellebrite UFED Cloud Analyzer 4.2.0.111
File
Home
Save session
Extractions Manager
Views
Generate report
Export
Conversation
Close person
Help
DEMO GORDAN
Extractions summary
Timeline table
Filters
Reset
Data Sources
Select All | Clear All
Dropbox
Facebook
Twitter
Google Drive
Gmail
Time Ranges
Add | Clear All
Apply
Content Categories & Types
1187 Events
Page 1 [1-200] / 6 [1187]
Page 1
Go
Search DEMO GORDAN
Time
Parties
Content
07 apr 2015
1 07/04/2015 12:51:54 +00:00 E! Online This is why the Internet is fighting over Nicole Kidman's ad for Et http://t.co/x5m9hwpyzg
2 07/04/2015 12:50:40 +00:00 Sky TG24 G8 di Genova, l'Ue condanna l'Italia per i fatti della #Diaz. Secon introdotto il reato di tortura? #TG24Pomeriggio
3 07/04/2015 12:50:06 +00:00 World Economic Forum Video: How exponential technologies will disrupt the world http:/ http://t.co/koo2i0hxJ3
4 07/04/2015 12:48:37 +00:00 Michael Ausiello LATE NIGHT Video: Seth Meyers Invites #GameOfThrones Fave t https://t.co/IFbYiibeM8 via @RyanSchwartz
5 07/04/2015 12:45:38 +00:00 TechCrunch Countertop Is A Connected Kitchen Gizmo To Simplify Balanced N http://t.co/YUTqnJud2Z by @riptari
6 07/04/2015 12:43:15 +00:00 TechCrunch Apple Patents Learning Computer Vision For Gesture Control http nVHS3MPX09 by @etherington http://t.co/8jZRKtiv4M
7 07/04/2015 12:41:24 +00:00 Sky TG24 Tra poco #TG24Pomeriggio: G8 di Genova, violenze alla scuola # condannata da #Strasburgo. Governo lavora al #Def
8 07/04/2015 12:40:58 +00:00 TechCrunch Stanford Scientists Demo Promising Aluminum-Ion Battery http:/ by @riptari
9 07/04/2015 12:36:14 +00:00 E! Online Eva Longoria and Serena Williams Battle for Best Bikini Body Duri in Miami--Take a Look! http://t.co/qzvJf140Gk
10 07/04/2015 12:36:13 +00:00 Sky TG24 #UltimOra #Russia, rogo su #sottomarino #nucleare in cantiere cDqTVlDB0v
11 07/04/2015 12:30:00 +00:00 World Economic Forum 12 things #entrepreneurs should do before quitting their day jobs rvclObiSMe #startups #leadership http://t.co/rzSiIODxlR
12 07/04/2015 12:28:10 +00:00 TechCrunch Taking A Swipe At Tinder, Loveflutter Hopes 'Promoted Places' W App Free http://t.co/4bLE36Q1SF by @sohear
13 07/04/2015 12:21:03 +00:00 E! Online Michelle Obama doesn't think her daughters Sasha and Malia are here's why! http://t.co/Do8sRzhGsA
Content
Event Properties
07/04/2015 12:51 +00:00
Posted On
E! Online
Originator
Recipients
This is why the Internet is fighting over Nicole Kidman's ad for Etihad Airways: http://t.co/x5m9hwpyzg
Include in report



LIVE DEMO

Info: cloudanalyzer@datamaticdss.it