IBM Security

i2 Enterprise Insight Analysis (EIA)

Matt Pellegrini, i2 Threat Management Specialist

Chris Harshbarger, i2 Technical Sales Specialist at IBM

Webinar date – 15 September 2020

IBM

Who is i2 Intelligence

i2 Strategic Focus

Helping organizations generate actionable intelligence for 27+ years

Used By:

- All branches of US DoD
- 30 of the top 35 defense organizations worldwide
- 40 of the 43 coalition countries operating in Afghanistan
- 25 of the 28 NATO member countries
- All national security, intelligence and federal agencies in the USA
- 18 of the top 20 national security agencies worldwide

National Security

Counter Terrorism

Counter Intelligence

Intelligence Analysis

Border Security

Cyber Warfare

Insider Threat

Defense

Contingency Operations

Counter Insurgency

Counter Intelligence

Intelligence Analysis

Target Analysis Peacekeeping

Force Protection

Law Enforcement

Counter Terrorism

Major Investigations

Organized Crime

Public Order/Major Event Management

Volume Crime

Fusion Centers

Private Sector

Cyber Threat

Fraud investigations

Security Investigations

Risk & Compliance

Executive protection

Brand protection

Insider threat

Fusion centers

Government

Industry Oversight & Compliance

Cyber Threat

Securities Investigations

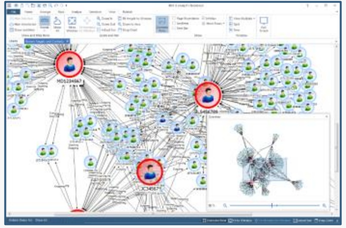
Fraud investigations

What is i2 Intelligence

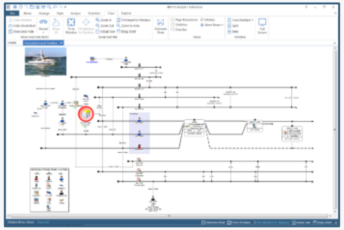
Analyst Workbench

“Front End”

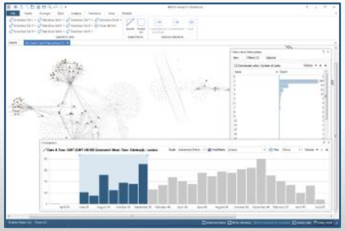
Network & Link Analysis



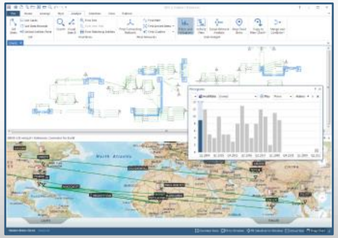
Transactional Timelines



Analytical Tools



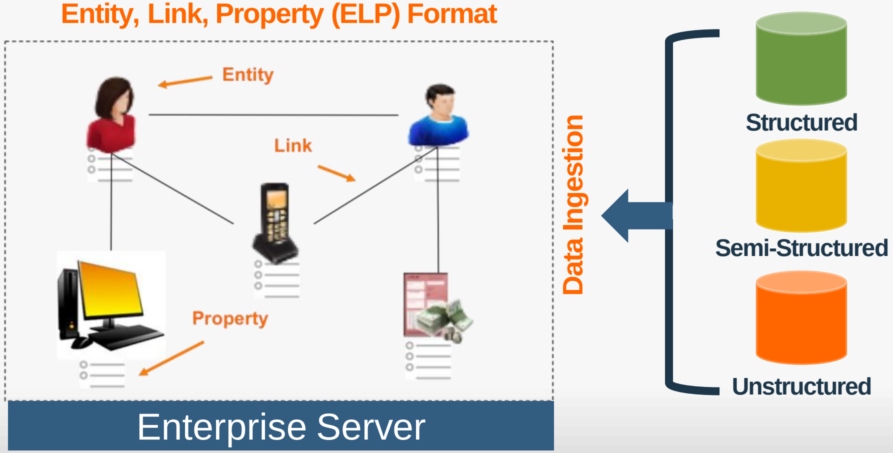
Geospatial Integration



Enterprise Server

“Back End”

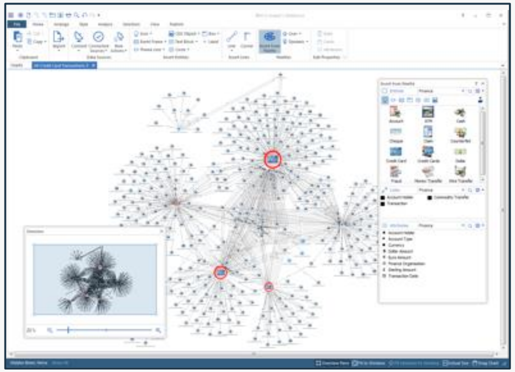
Entity, Link, Property (ELP) Format



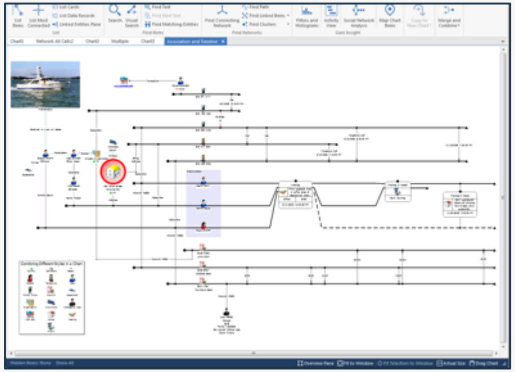
- ✓ Out-of-the-box **analytics & visualization** that help find and track adversaries in both the government and private sector
- ✓ Intuitive UI design used by 1,000’s of analysts for over 27+ years which greatly speeds up investigation with efficiency
- ✓ Create products for **decision making** or **to provide evidence** of criminal behavior or as visual aids during an investigation

- ✓ Combine all **internal & external data** sources into a **single object model** in order to understand multi-dimensional data
- ✓ Advanced searching to quickly expand on an investigation by allowing the analyst to **“pivot”** a search on any variable
- ✓ Deep server-side analytics that allow presentation of non-obvious relationships and data patterns to the analyst

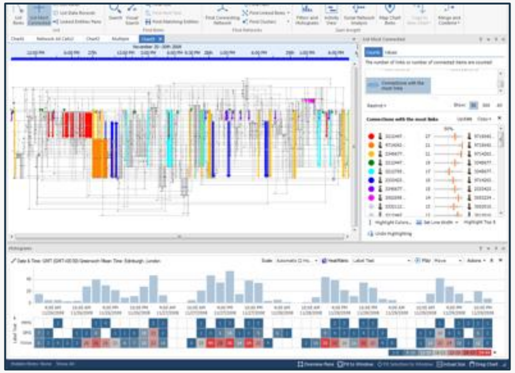
IBM i2 is a set of multi dimensional & visual analysis tools



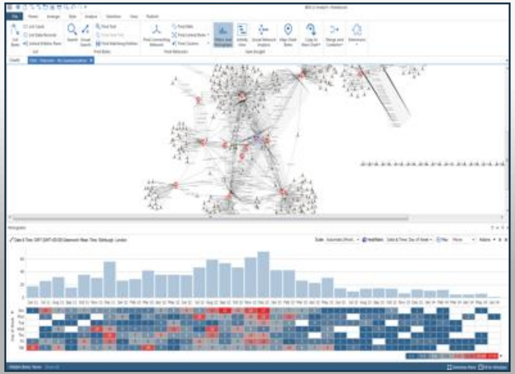
Complex network analysis



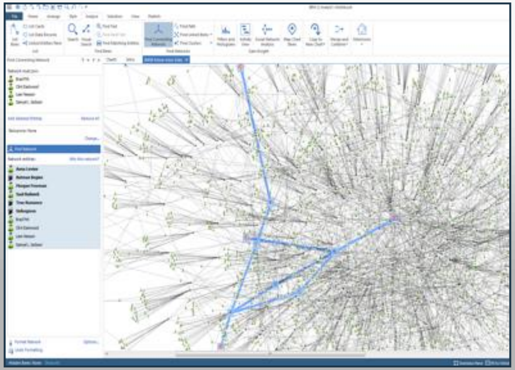
Events over time



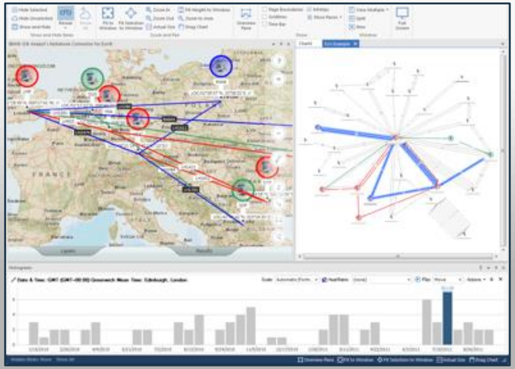
Patterns of behavior



Hotspots of activity

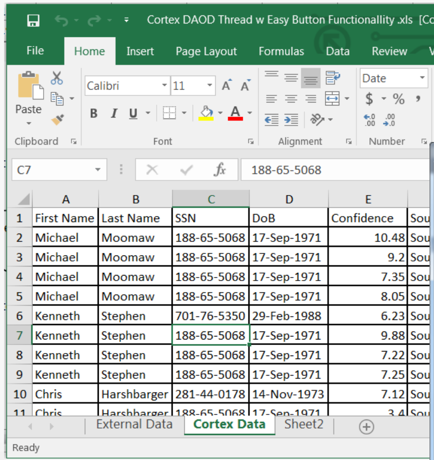


Control networks within networks



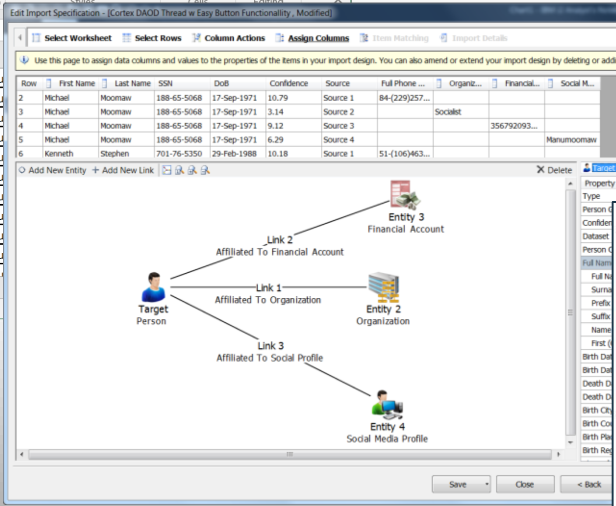
Geospatial Analysis

Analyst’s can ingest “Ad Hoc” data quickly – without an “IT Support”



	A	B	C	D	E	
1	First Name	Last Name	SSN	DoB	Confidence	Sou
2	Michael	Moomaw	188-65-5068	17-Sep-1971	10.48	Sou
3	Michael	Moomaw	188-65-5068	17-Sep-1971	9.2	Sou
4	Michael	Moomaw	188-65-5068	17-Sep-1971	7.35	Sou
5	Michael	Moomaw	188-65-5068	17-Sep-1971	8.05	Sou
6	Kenneth	Stephen	701-76-5350	29-Feb-1988	6.23	Sou
7	Kenneth	Stephen	188-65-5068	17-Sep-1971	9.88	Sou
8	Kenneth	Stephen	188-65-5068	17-Sep-1971	7.22	Sou
9	Kenneth	Stephen	188-65-5068	17-Sep-1971	7.25	Sou
10	Chris	Harshbarger	281-44-0178	14-Nov-1973	7.12	Sou
11	Chris	Harshbarger	188-65-5068	17-Sep-1971	3.4	Sou

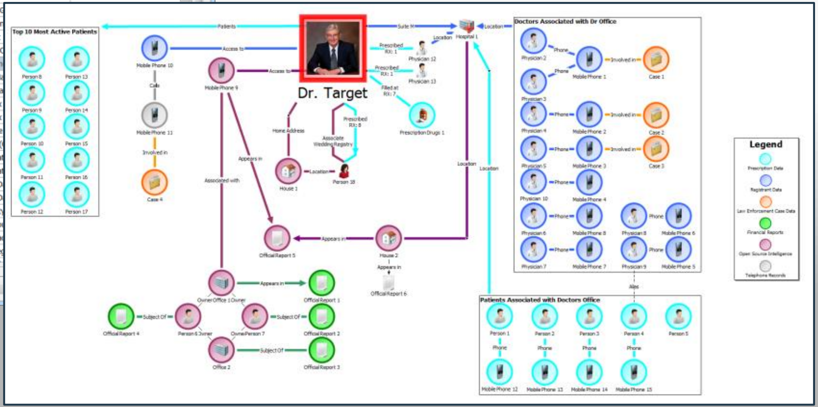
Source Data



Use this page to assign data columns and values to the properties of the items in your import design. You can also amend or extend your import design by deleting or adding further entities and links.

Row	First Name	Last Name	SSN	DoB	Confidence	Source	Full Phone ...	Organiz...	Financial...	Social M...
2	Michael	Moomaw	188-65-5068	17-Sep-1971	10.79	Source 1	84-(229)257...			
3	Michael	Moomaw	188-65-5068	17-Sep-1971	3.14	Source 2		Socialist		
4	Michael	Moomaw	188-65-5068	17-Sep-1971	9.12	Source 3			356792093...	
5	Michael	Moomaw	188-65-5068	17-Sep-1971	6.29	Source 4				Manumoomaw
6	Kenneth	Stephen	701-76-5350	29-Feb-1988	10.18	Source 1	51-(106)463...			

Import Specification


Top 10 Most Active Patients
Dr. Target
Doctors Associated with Dr Office
Patients Associated with Doctors Office
Legend

Add to Analysis

How IBM i2 works

Link Analysis’s DNA is Entity Link Property (ELP)

We all have a digital footprint that defines us

How IBM i2 works

Link Analysis’s DNA is Entity Link Property (ELP)

Name (M)	: Richardo Gomes
Name (M)	: Richard Gomez
Address (H)	: 11035 Burns Ave., Westchester, IL 60153
Address (H)	: 11035 Burns Dr, Westchester, IL 60153
CUST#	: 796
CUST#	: 857
ACCT#	: D2712151385121742
ACCT#	: V97859240062
Phone	: 064-413-9611
Phone	: 069-906-1853
Phone	: 028-891-0646
SSN	: 034-58-5720
DL	: H160-65-120A9 FL
Date Of Birth	: 1976-08-05
Activity Time	:13.26
Activity Date	:04/10/2017
Airline	:xxxx

Account 1
Arrest 1
Car 1
Car Bomb 1
Computer Log 1
Drugs 1
Female 1
House 1
IED 1
Infected Computer 1
Insurgent 1
Male 1
Meeting 1
Office 1
Place 1
Soldier 1
Telephone 1
Utility Vehicle 1

Identities & Entities have attributes (properties)

Which connect us to other Identities & Entities

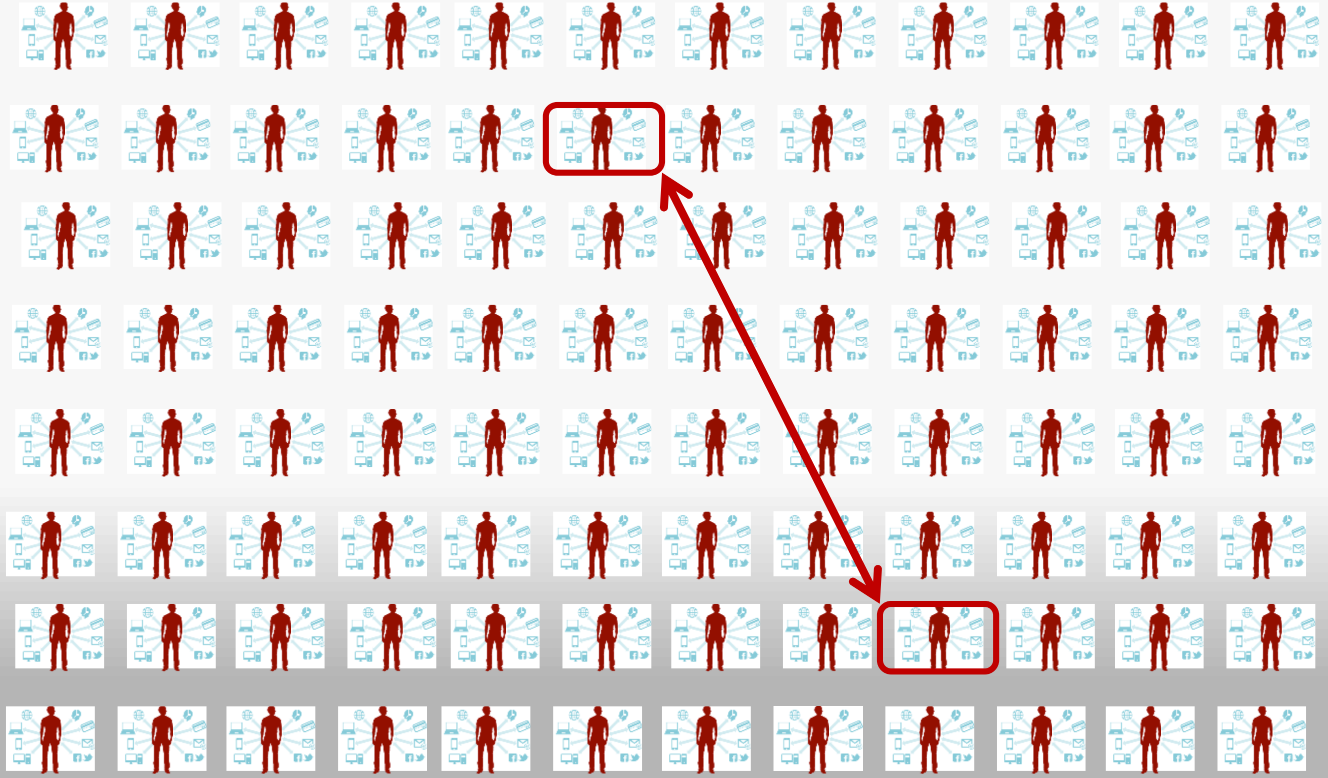
Permanent or temporary connections

How IBM i2 works

Link Analysis's DNA is Entity Link Property (ELP)

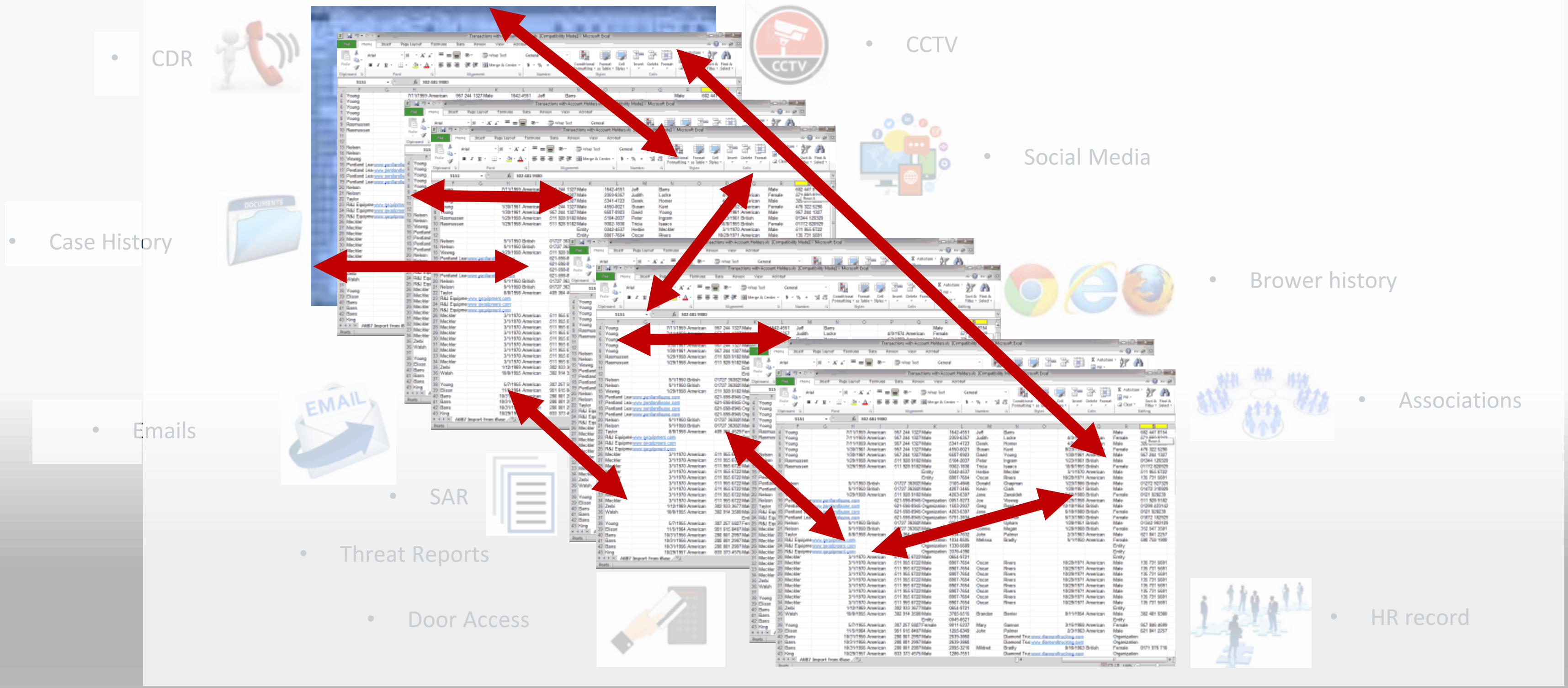
How IBM i2 works

Link Analysis's DNA is Entity Link Property (ELP)



How IBM i2 works

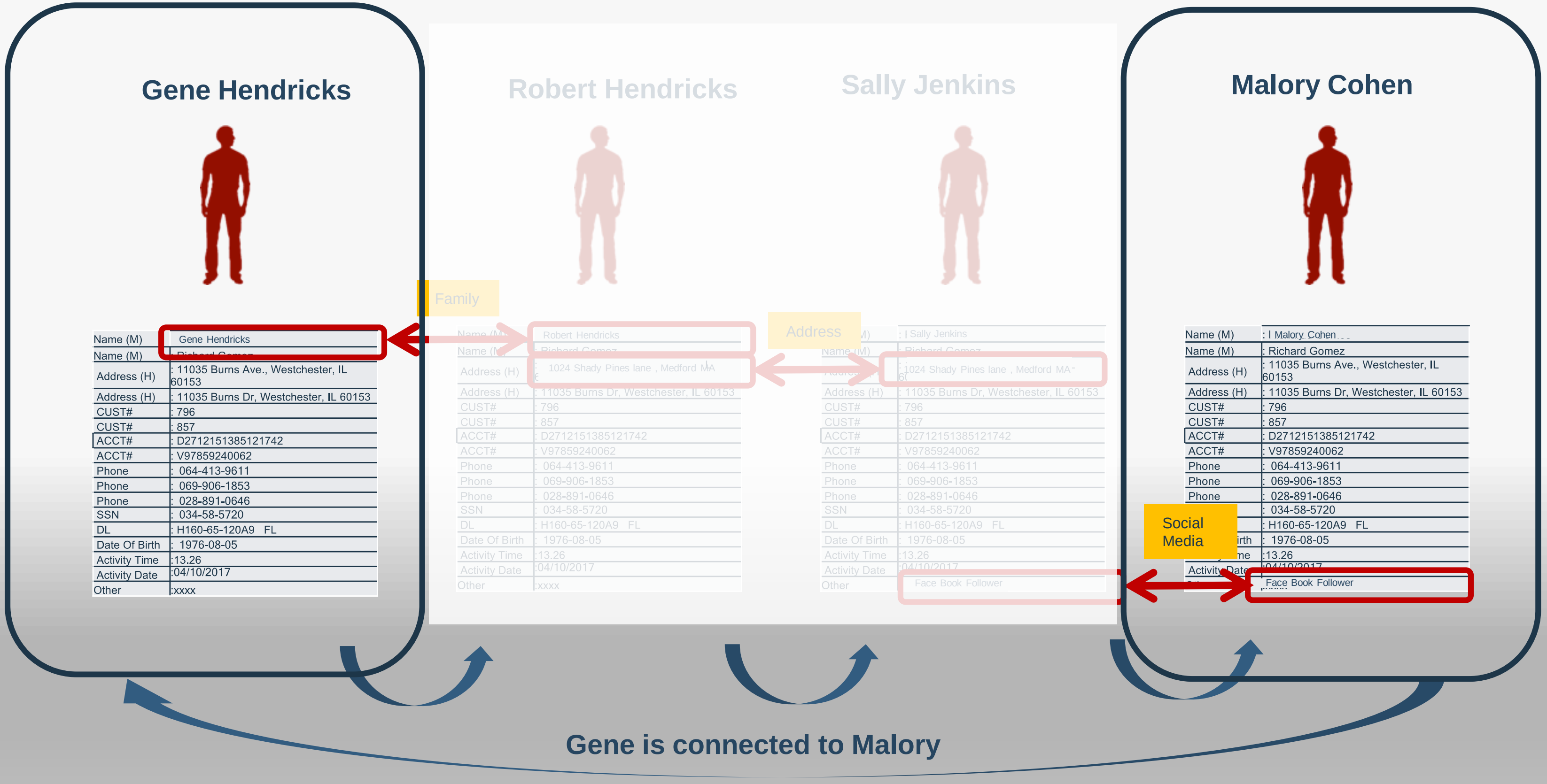
Link Analysis’s DNA is Entity Link Property (ELP)



- CDR
- CCTV
- Social Media
- Case History
- Brower history
- Emails
- Associations
- SAR
- Threat Reports
- Door Access
- HR record

How IBM i2 works

Link Analysis’s DNA is Entity Link Property (ELP)



Gene Hendricks

Name (M)	Gene Hendricks
Name (M)	: Richard Gomez
Address (H)	: 11035 Burns Ave., Westchester, IL 60153
Address (H)	: 11035 Burns Dr, Westchester, IL 60153
CUST#	: 796
CUST#	: 857
ACCT#	: D2712151385121742
ACCT#	: V97859240062
Phone	: 064-413-9611
Phone	: 069-906-1853
Phone	: 028-891-0646
SSN	: 034-58-5720
DL	: H160-65-120A9 FL
Date Of Birth	: 1976-08-05
Activity Time	:13.26
Activity Date	:04/10/2017
Other	:xxxx

Robert Hendricks

Name (M)	Robert Hendricks
Name (M)	: Richard Gomez
Address (H)	: 1024 Shady Pines lane , Medford MA
Address (H)	: 11035 Burns Dr, Westchester, IL 60153
CUST#	: 796
CUST#	: 857
ACCT#	: D2712151385121742
ACCT#	: V97859240062
Phone	: 064-413-9611
Phone	: 069-906-1853
Phone	: 028-891-0646
SSN	: 034-58-5720
DL	: H160-65-120A9 FL
Date Of Birth	: 1976-08-05
Activity Time	:13.26
Activity Date	:04/10/2017
Other	:xxxx

Sally Jenkins

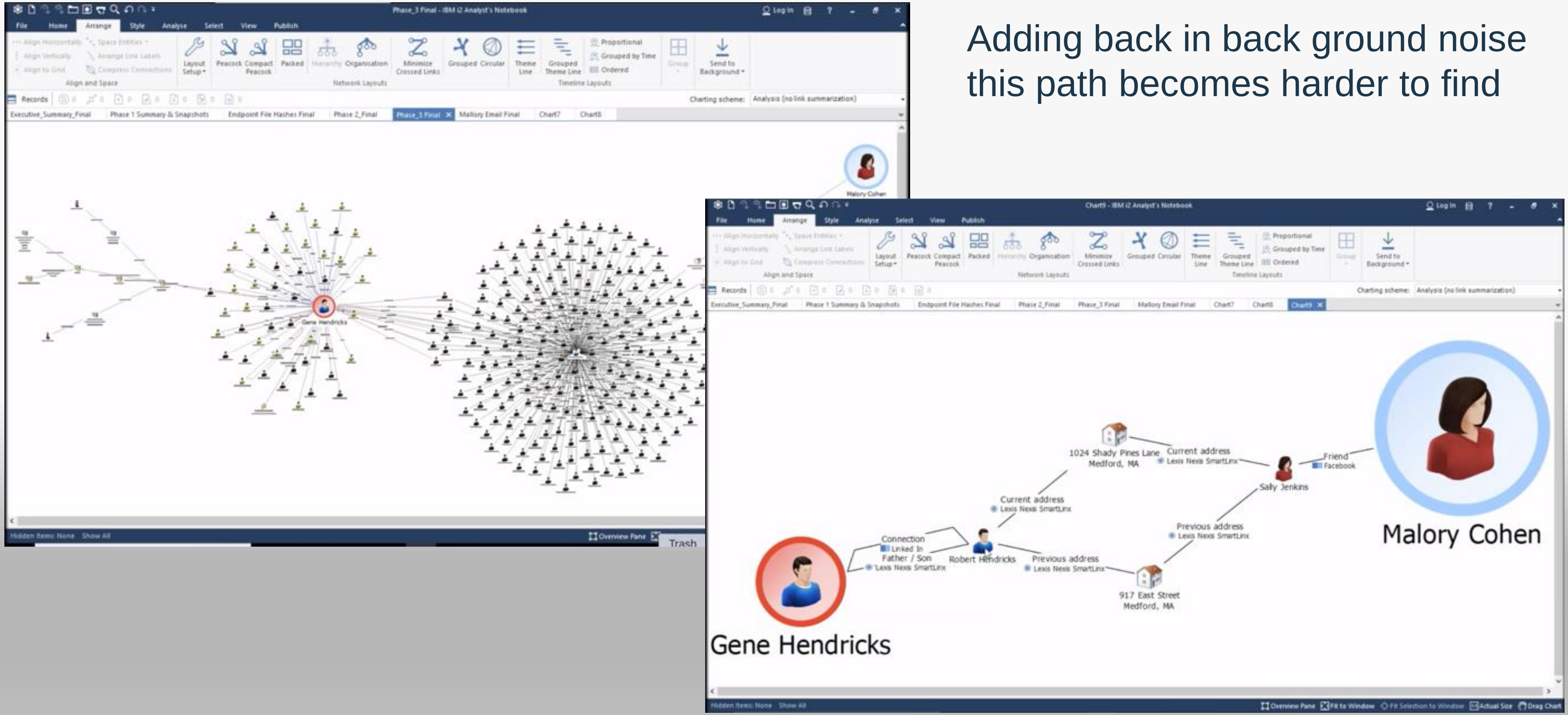
M)	: I Sally Jenkins
Name (M)	: Richard Gomez
Addres	: 1024 Shady Pines lane , Medford MA
Address (H)	: 11035 Burns Dr, Westchester, IL 60153
CUST#	: 796
CUST#	: 857
ACCT#	: D2712151385121742
ACCT#	: V97859240062
Phone	: 064-413-9611
Phone	: 069-906-1853
Phone	: 028-891-0646
SSN	: 034-58-5720
DL	: H160-65-120A9 FL
Date Of Birth	: 1976-08-05
Activity Time	:13.26
Activity Date	:04/10/2017
Other	Face Book Follower

Malory Cohen

Name (M)	: I Malory Cohen
Name (M)	: Richard Gomez
Address (H)	: 11035 Burns Ave., Westchester, IL 60153
Address (H)	: 11035 Burns Dr, Westchester, IL 60153
CUST#	: 796
CUST#	: 857
ACCT#	: D2712151385121742
ACCT#	: V97859240062
Phone	: 064-413-9611
Phone	: 069-906-1853
Phone	: 028-891-0646
	: 034-58-5720
	: H160-65-120A9 FL
irth	: 1976-08-05
me	:13.26
Activity Date	:04/10/2017
	Face Book Follower

How IBM i2 works

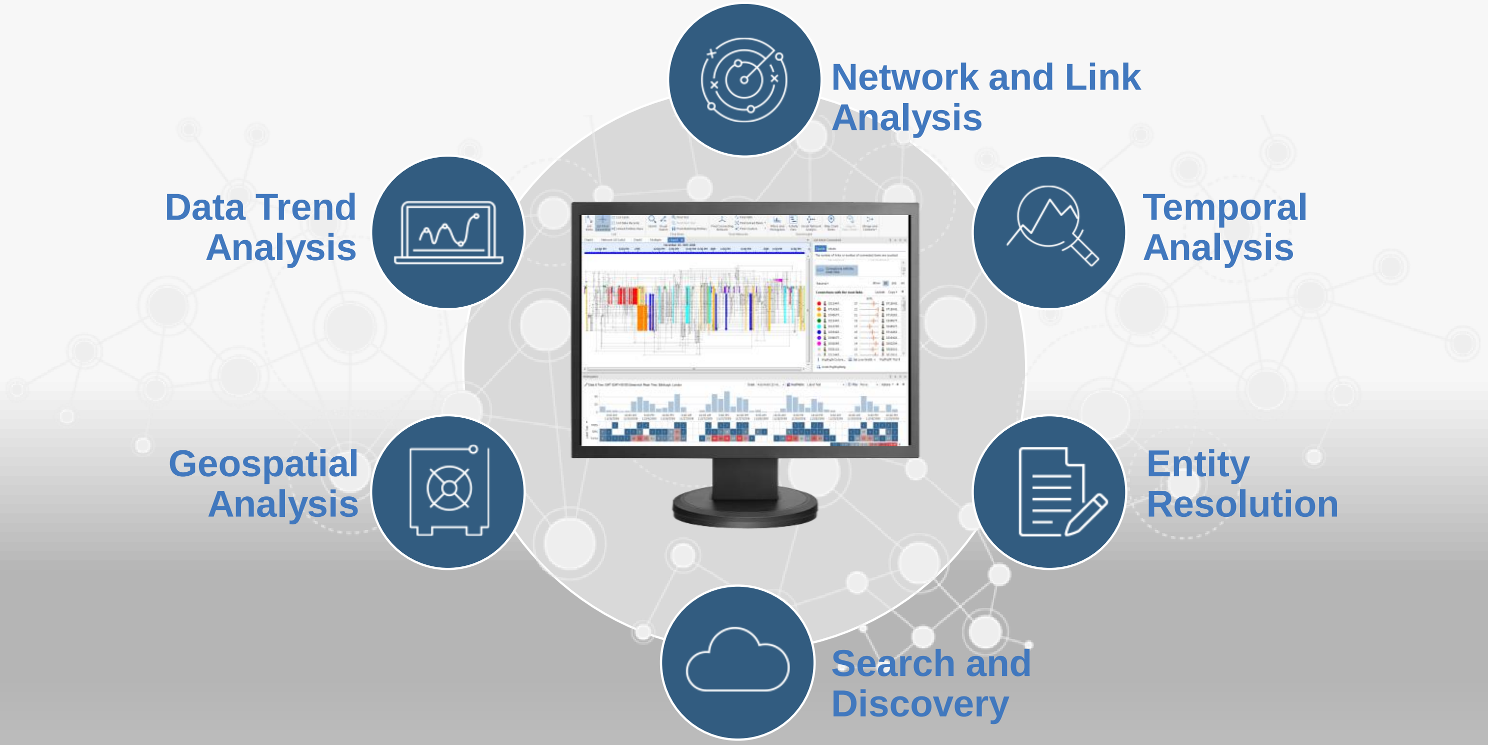
Link Analysis's DNA is Entity Link Property (ELP)



Adding back in back ground noise this path becomes harder to find

Why - IBM i2 Enterprise Insight Analysis (EIA) solution

IBM i2 focuses on the **analyst** doing **analysis** (**<u>their job</u>**) at **speed,** efficiently and effectively – where **technology enables them**, does not hinder them



Network and Link Analysis

Data Trend Analysis

Temporal Analysis

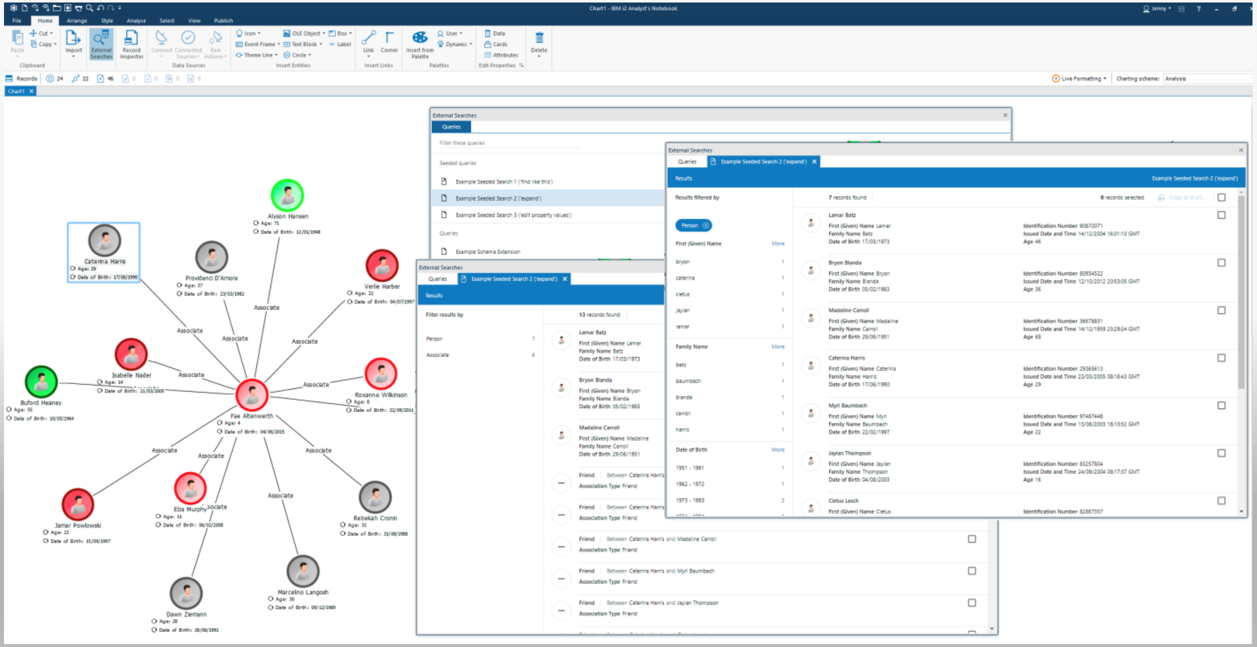
Geospatial Analysis

Entity Resolution

Search and Discovery

Exciting addition to i2 Portfolio – a new product offering!

IBM i2 Connect combines seamless connection to data sources with powerful, multi-dimensional visual analysis



External Searches

Queries

Filter these queries

Seeded queries

- Example Seeded Search 1 ('find like this')
- Example Seeded Search 2 ('expand')
- Example Seeded Search 3 ('edit property values')

Queries

- Example Schema Extension

External Searches

Queries | Example Seeded Search 2 ('expand')

Results

Filter results by

Person	7
Associate	6

13 records found

Lamar Batz
First (Given) Name Lamar
Family Name Batz
Date of Birth 17/03/1973

Bryon Blanda
First (Given) Name Bryon
Family Name Blanda
Date of Birth 05/02/1983

Madaline Carroll
First (Given) Name Madaline
Family Name Carroll
Date of Birth 29/06/1951

Friend | Between Caterina Harris
Association Type Friend

Friend | Between Caterina Harris
Association Type Friend

Friend | Between Caterina Harris and Madaline Carroll
Association Type Friend □

Friend | Between Caterina Harris and Myrl Baumbach
Association Type Friend □

Friend | Between Caterina Harris and Jaylan Thompson
Association Type Friend □

External Searches

Queries | Example Seeded Search 2 ('expand')

Results | Example Seeded Search 2 ('expand')

Results filtered by

Person ⊗

First (Given) Name	More
bryon	1
caterina	1
cletus	1
jaylan	1
lamar	1

Family Name	More
batz	1
baumbach	1
blanda	1
carroll	1
harris	1

Date of Birth	More
1951 - 1961	1
1962 - 1972	1
1973 - 1983	2

7 records found | 0 records selected | Copy to chart... □

Lamar Batz □
First (Given) Name Lamar
Family Name Batz
Date of Birth 17/03/1973
Identification Number 90870071
Issued Date and Time 14/12/2004 16:01:10 GMT
Age 46

Bryon Blanda □
First (Given) Name Bryon
Family Name Blanda
Date of Birth 05/02/1983
Identification Number 80934522
Issued Date and Time 12/10/2012 20:53:05 GMT
Age 36

Madaline Carroll □
First (Given) Name Madaline
Family Name Carroll
Date of Birth 29/06/1951
Identification Number 36678831
Issued Date and Time 14/12/1959 23:29:24 GMT
Age 68

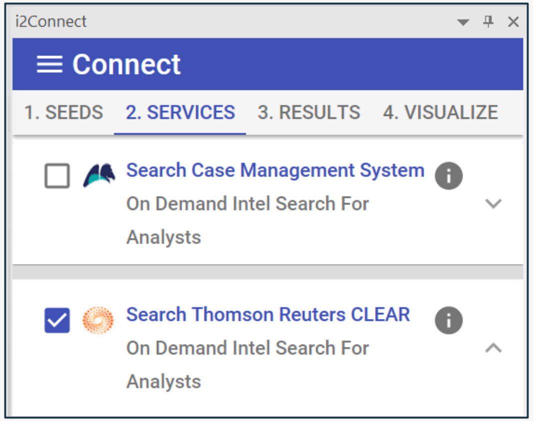
Caterina Harris □
First (Given) Name Caterina
Family Name Harris
Date of Birth 17/06/1990
Identification Number 29365613
Issued Date and Time 23/03/2005 08:18:43 GMT
Age 29

Myrl Baumbach □
First (Given) Name Myrl
Family Name Baumbach
Date of Birth 22/02/1997
Identification Number 97487448
Issued Date and Time 13/08/2003 18:10:32 GMT
Age 22

Jaylan Thompson □
First (Given) Name Jaylan
Family Name Thompson
Date of Birth 04/08/2003
Identification Number 83257804
Issued Date and Time 24/09/2004 08:17:37 GMT
Age 16

Cletus Lesch □
First (Given) Name Cletus
Identification Number 82867357

i2 Connect - On demand access to external and legacy data sources



i2Connect

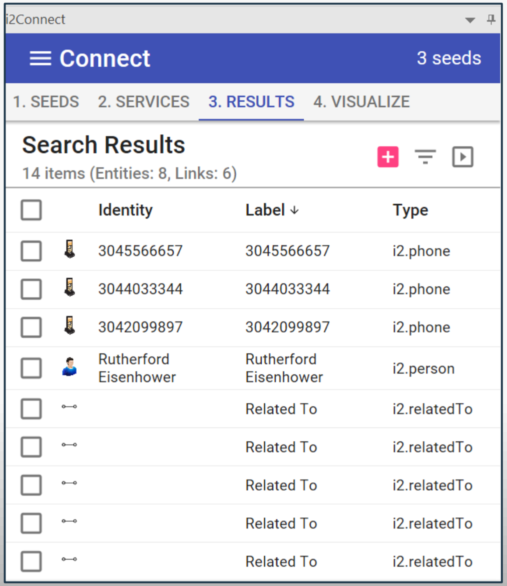
Connect

1. SEEDS · 2. SERVICES · 3. RESULTS · 4. VISUALIZE

□ Search Case Management System
On Demand Intel Search For Analysts

☑ Search Thomson Reuters CLEAR
On Demand Intel Search For Analysts

Pick an external source



i2Connect

Connect · 3 seeds

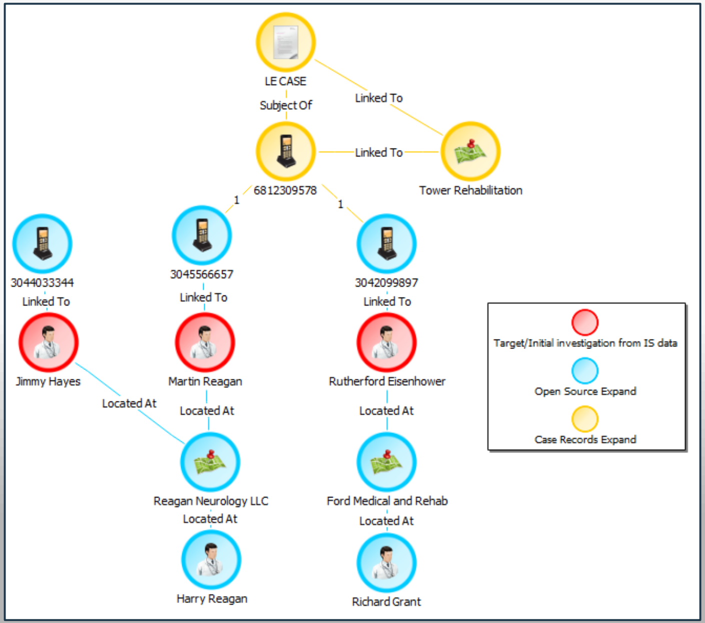
1. SEEDS · 2. SERVICES · 3. RESULTS · 4. VISUALIZE

Search Results

14 items (Entities: 8, Links: 6)

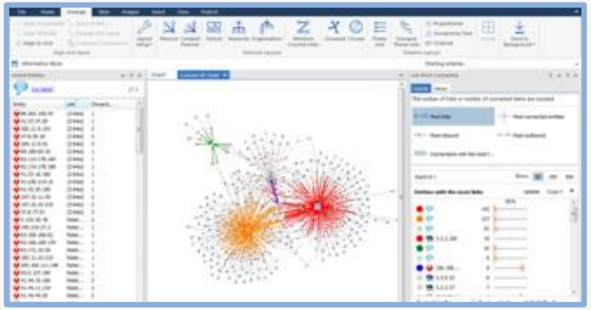
□	Identity	Label ↓	Type
□	3045566657	3045566657	i2.phone
□	3044033344	3044033344	i2.phone
□	3042099897	3042099897	i2.phone
□	Rutherford Eisenhower	Rutherford Eisenhower	i2.person
□		Related To	i2.relatedTo
□		Related To	i2.relatedTo
□		Related To	i2.relatedTo
□		Related To	i2.relatedTo
□		Related To	i2.relatedTo

View Results



Add to analysis

Adding value by using i2 Connect



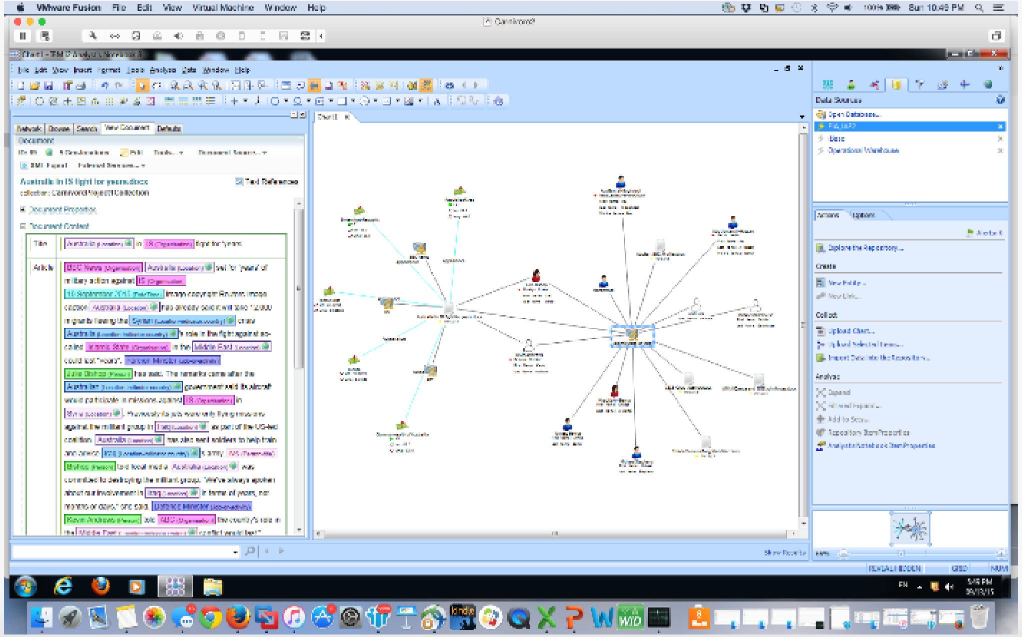
- **Improve data insights, easily connect to data**
- Harness the power of **multiple, disparate data sources** to help detect vulnerabilities and disrupt threats, both cyber and physical

- **Reduce cost and complexity of investigation**
- With minimal technical investment, use or create **data connectors to allow rapid access** to any data source or API for analysis

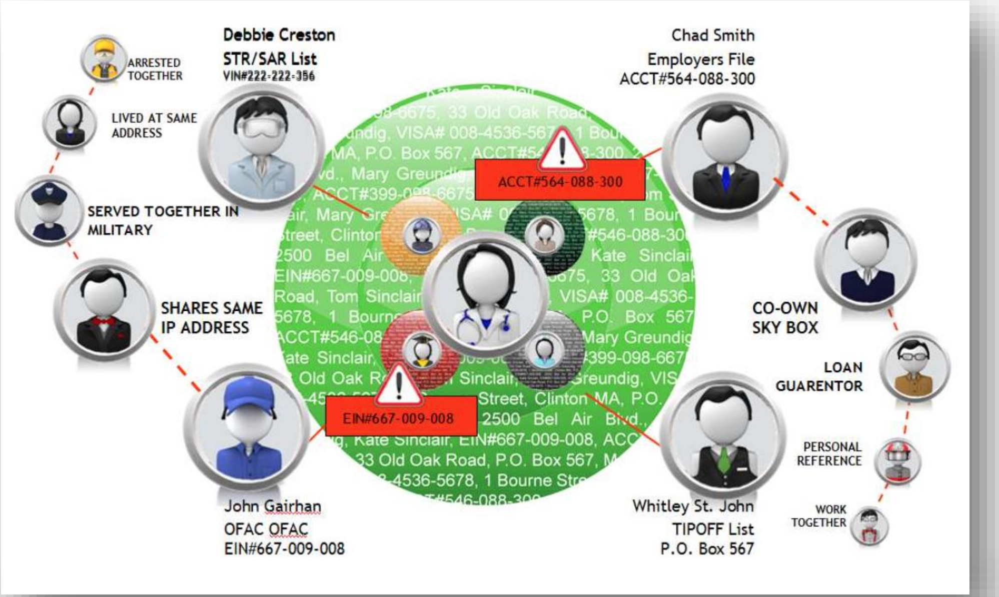
- **Save time: get actionable insights quicker**
- Reduce time required to derive rich, actionable intelligence from complex data sets **using powerful advanced analytics**

Unstructured Text Analytics

- Sources of Unstructured Text:
  - Suspicious Activity Reports
  - Intelligence Reports
  - Interrogation Reports
  - Open Source – Websites
  - Messaging and Social media
- Extract entities (people, places, events) and the relationships between them.
- Resolve the names (President Trump, Donald Trump, Mr. Trump, etc.)
- Provide links to the source text for validation



Entity Resolution



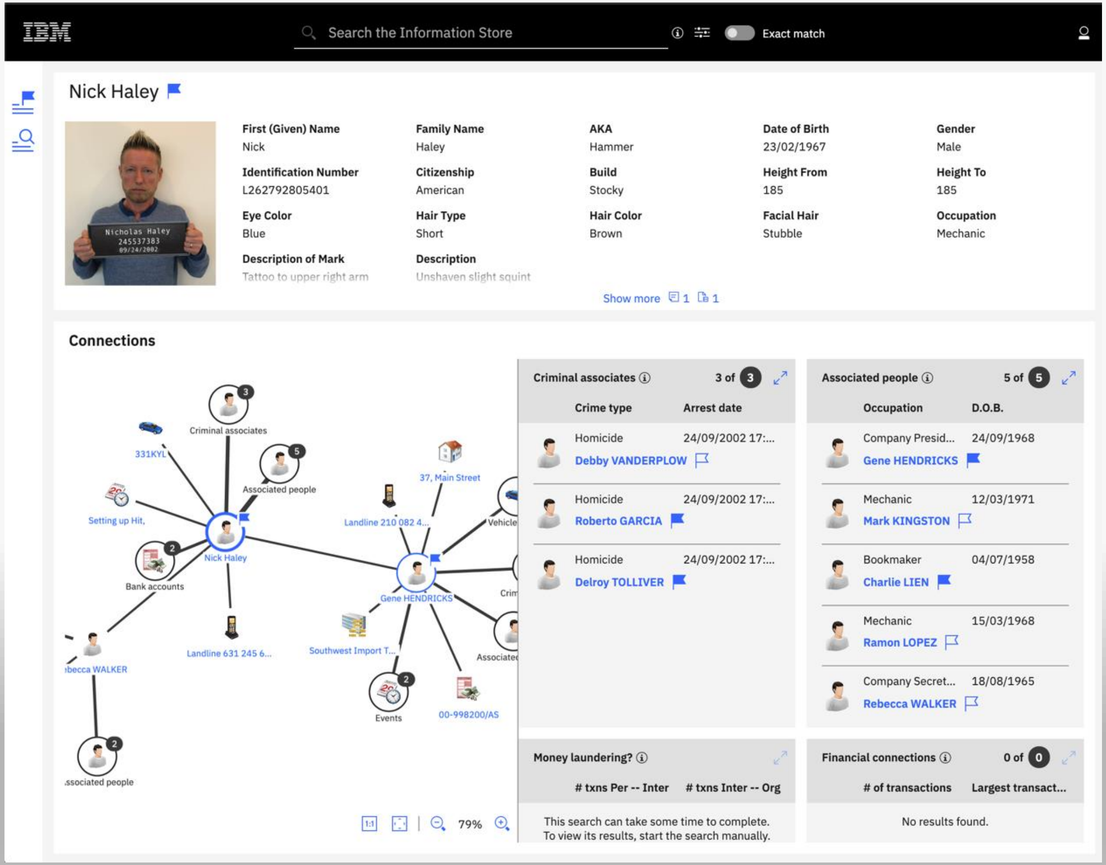
Robust Analytics Built Right In

Deep algorithms that become better over time in detecting non-obvious events

- **Entity Resolution** allows you to **merge like objects** and find out “Who is Who” and “Who knows who” – alerting you in real-time
- **Recommendation Engine discover key patterns**, events, and relationships that are nearly impossible to detect through manual analysis
- **Social Network Analysis (SNA) ranks relationships between objects** using multiple network analysis algorithms including K-Core, Eigenvector, Between-ness, Degree, etc.

i2 EIA Investigate Add On - 360 Views

- Major refresh this release
- Expand the i2 user community
- Minimal training required
- Fast target investigation via a web browser
- Answer common questions quickly and easily



IBM Search the Information Store Exact match

Nick Haley

First (Given) Name	**Family Name**	**AKA**	**Date of Birth**	**Gender**
Nick	Haley	Hammer	23/02/1967	Male
Identification Number	**Citizenship**	**Build**	**Height From**	**Height To**
L262792805401	American	Stocky	185	185
Eye Color	**Hair Type**	**Hair Color**	**Facial Hair**	**Occupation**
Blue	Short	Brown	Stubble	Mechanic
Description of Mark	**Description**			
Tattoo to upper right arm	Unshaven slight squint			

Show more 1 1

Connections

Criminal associates ⓘ 3 of 3

	Crime type	Arrest date
	Homicide Debby VANDERPLOW	24/09/2002 17:...
	Homicide Roberto GARCIA	24/09/2002 17:...
	Homicide Delroy TOLLIVER	24/09/2002 17:...

Associated people ⓘ 5 of 5

	Occupation	D.O.B.
	Company Presid... Gene HENDRICKS	24/09/1968
	Mechanic Mark KINGSTON	12/03/1971
	Bookmaker Charlie LIEN	04/07/1958
	Mechanic Ramon LOPEZ	15/03/1968
	Company Secret... Rebecca WALKER	18/08/1965

Money laundering? ⓘ

# txns Per -- Inter	# txns Inter -- Org

This search can take some time to complete.
To view its results, start the search manually.

Financial connections ⓘ 0 of 0

# of transactions	Largest transact...

No results found.

i2 Functionality – ***Operational Support***

Geo-Spatial Analysis

Save time and effort, reuse valuable work
Improved visualization for greater analytical capabilities

Mapping Schemes

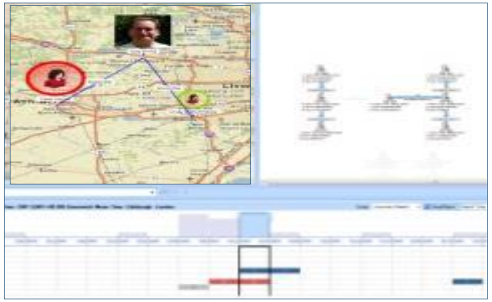
- Save drawings you have created
- Maintain snapshots of geo-spatial query results
- Easily recreate your map views and associate them with charts so they can be shared with other users.

Improved Chart Map Interactions

- Use a Histogram, Heat Matrix or Filter to select chart items on the map.
- Drawings or other shapes can be use to interactively select mapped chart items
- Display Icon frames and images

Drawing Tools & Layers

- Shapes drawn on the map can be edited to update their geometry.
- Individual shapes can be named and renamed.
- Reorder the display of buffer zones, drawings and chart items for improved map clarity



IBM i2 Offers Individual, Workgroup and Enterprise solutions

IBM i2 Analyst's Notebook

Powerful visual analysis tool for individual analyst (chart centric)

IBM i2 iBase with IBM i2 Analyst's Notebook

Workgroup oriented with repository for sharing and searching

IBM i2 Enterprise Insight Analysis

Enterprise wide intelligence analysis and sharing

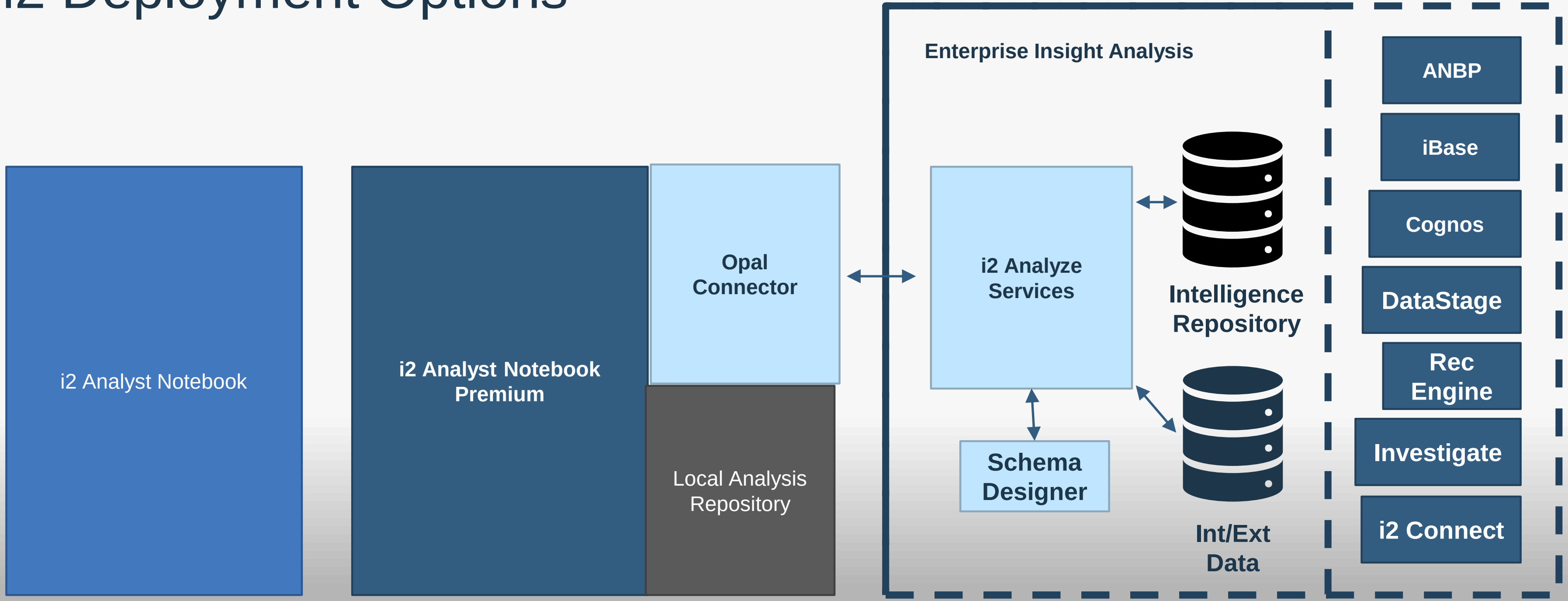
With IBM i2 Analyst's Notebook Premium includes a local repository (chart and data centric) for individual analyst

Helps an organization address:

- Overwhelming data
- An evolving user base
- Enterprise level needs

with scale, extensibility and core system improvements

i2 Deployment Options



i2 Analyst Notebook

i2 Analyst Notebook Premium

Opal Connector

Local Analysis Repository

Enterprise Insight Analysis

i2 Analyze Services

Schema Designer

Basic

Intermediate

Advanced

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®