INSIGHT

AN LEIU PUBLICATION

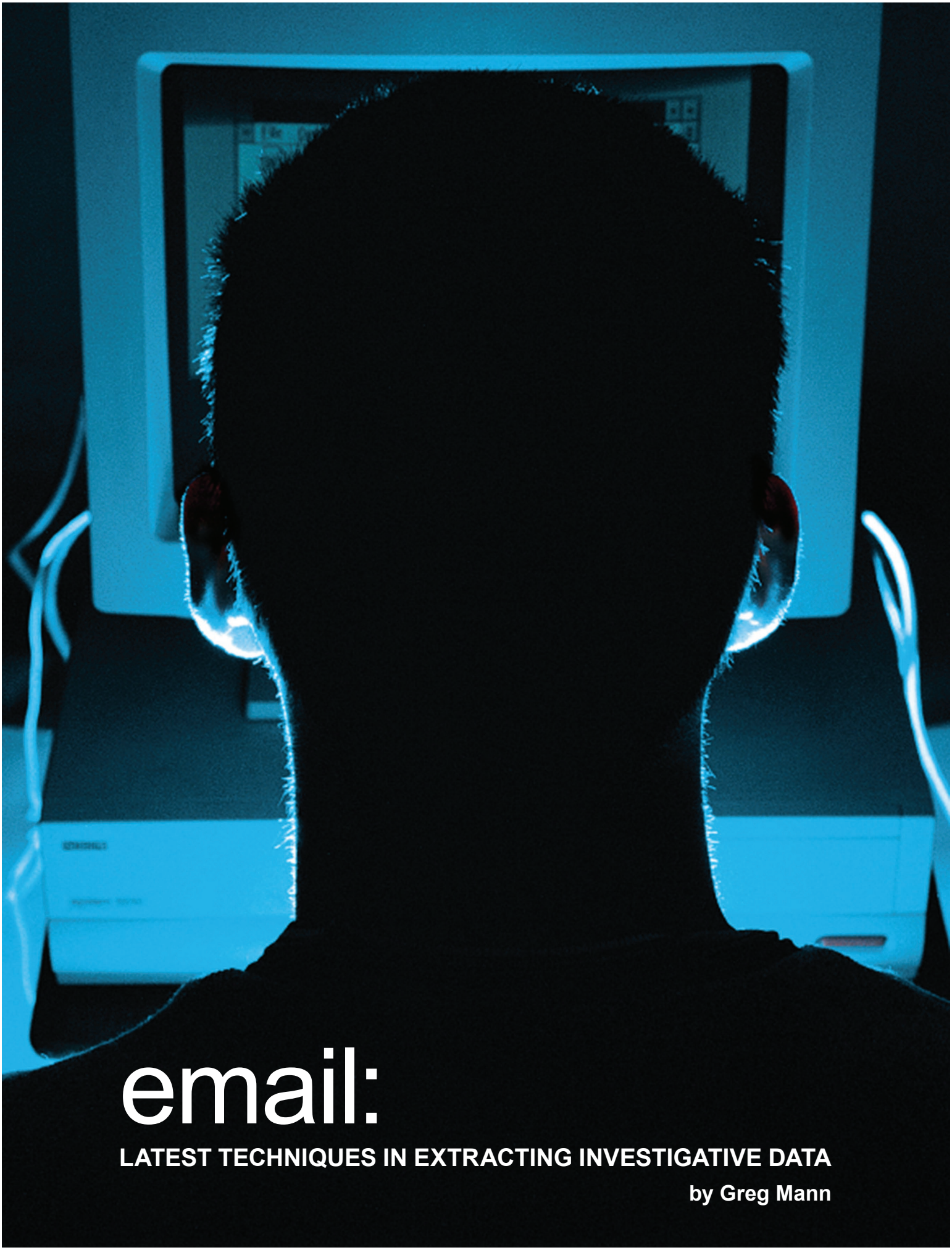
WHAT'S NEW?

You are holding a copy of LEIU's newly launched publication, INSIGHT – a new magazine format which replaces the newsletter. We hope you enjoy the new look! Please let us know your thoughts and comments on what you would like to read about in future issues. We'd like you to be part of the discussion. Our goal is to bring you relevant articles, news, updates and coverage of current intelligence-related issues you want to know about.

This issue highlights the use of specialized software to analyze email transactions, the use of spatial data to support intelligence files, a recap of the LEIU 20/20 and guidance on how to gain access to, and update the LEIU roster.

Brian Gray
Southwest Zone Chairman
Editor, Insight
intelligenceanalysis@mac.com

TABLE OF CONTENTS



email:

LATEST TECHNIQUES IN EXTRACTING INVESTIGATIVE DATA

by Greg Mann

email is one of a number of common communications and social media formats that is becoming an increasing important source of investigative data to the intelligence analyst. While many analysts have experience in acquiring and analyzing telephone call data, email is often seen as a job for forensic specialists because of the additional challenges in converting and modeling this type of data.

In this article, I will focus on a small number of techniques for the processing and analysis of email data that can be adopted by the crime or intelligence analyst. We will consider:

- The components of an email message and how they lend themselves to different analytical techniques
- How to prepare the data for analysis
- An example of analytical workflow where different tools and techniques are employed to create and test different types of hypotheses.

Email Message Components

First, it is worthwhile to examine the components that make up an email message, as these offer different opportunities for analysis. It will be apparent when reading an email message that it is composed of different components: the header, the body, and optionally, a set of attachments.

The header is largely structured data with fields such as From, To, CC, Date/Time Sent, etc. There are other important pieces of metadata hidden in the header as well (many email clients provide the option to view this data, but most users will never want to see it), but we will focus on the fields described above. The header also contains a Subject field, the contents of which will be a free text description of what the message is about.

The body of the message consists of free text. You may also see images embedded in the body of a message, but these are essentially attachment files. Attachments can include pictures, documents and other files, each of which will possess various properties that may be of interest to some investigations.

Forwarded mails and other duplications (i.e. same message in different user mailboxes) add additional complexity to any email data set.

Email Clients

Most people's experience of email is through the email client applications they use on a daily basis to compose and read their email messages. The two main types of client are the local (or fat) client such as Microsoft Outlook and web-based clients which include Yahoo Mail and Gmail. Where the actual email data is stored can vary between email clients. In the case of "web mail", the data is stored and controlled by the hosting organization, so legal steps are needed to acquire such information. Users of local clients can download copies of email from a local email server, or alternatively access their mailbox on the server.

When you acquire a set of email data, the format it is held in will depend on the client. Outlook (.pst), Apple Mail (.emix) and Lotus Notes (.nsf) all use different file formats to store email messages. This is where the first challenge to the analyst lies – getting this data into a format that can be easily analyzed as a single common set, so that it can be analysed using tools such as Excel and other analytical applications.

Email Analysis

In the context of crime analysis, we can usually assume that the analyst approaches an email data set with one or more specific questions in mind: a particular email account, a slice of time, a key word or attachment. These questions may be even more abstract in nature – are there groups of people that are working closely together, do individuals assume roles (gatekeeper, leader), are there differences between email communications and the organizational chart?

In the examples that we will work through in the second part of this article, we will start with a particular Organization in mind, identify a set of key messages, and then turn our attention to the wider picture of how these discussions evolve over time, identifying some key players along the way. We will use two pieces of software to complete the analysis

Forensic Search

We will commence our analysis by identifying a set of email messages that mention a certain company. The software application used for this first phase is Intella, a “forensic search” tool that not only allows the analyst to load a range of different email data sources ready for analysis (thus solving our first challenge of how to represent the email data), but also provides an extremely powerful search mechanism that allows an Analyst with little or no computer forensic experience to quickly identify emails of interest.

Intella can not only identify and interrogate the text content of an email, but all metadata, binary content, encrypted items and various attachment types.

Associational and Temporal Analysis

Having identified a set of mails of interest, we will then move the data into a database where it can be modelled as a set of objects and links. Email, like telephone data, has both transactional (From To) and temporal (Date/Time Sent) elements, so representing the data as a graph provides the analyst with the opportunity to apply a range of link analysis and social network analysis techniques to the dataset.

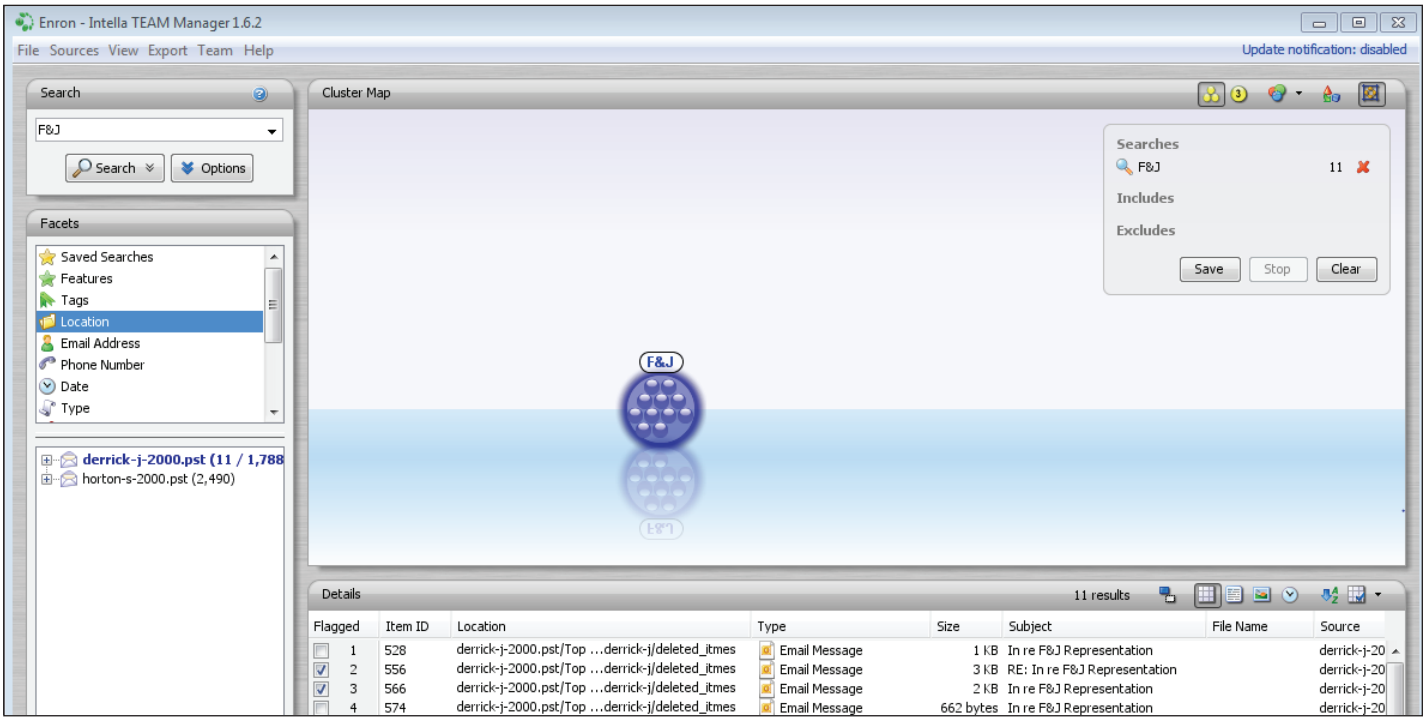
Remember that before you start your analysis, make sure to establish your investigative goals and tasks, as this will largely determine the tools and techniques you use, as well as keeping your lines of enquiry focused.

Example

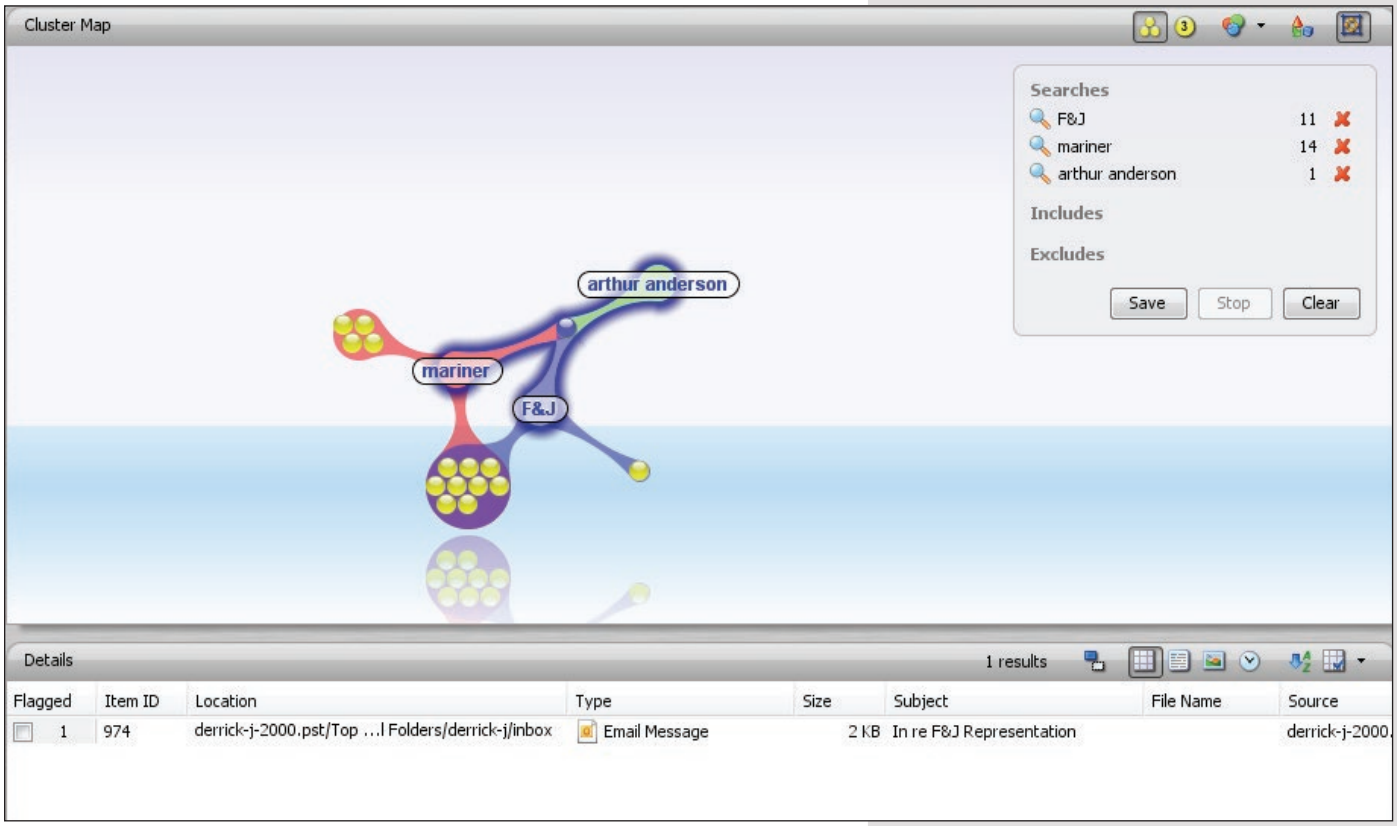
As a data source, I have used a small set of the 148 PST files belonging to the publically released Enron data set. Having acquired these PST files, the first step is to convert the native email files into a common format – this is especially important if we are dealing with a range of sources from different email clients.

Using Intella, I select the 2 PST source files – Intella loads and converts the files ready for analysis.

I have randomly selected the company “F&J” as the start of my inquiry. Entering the string “F&J” as my first search parameter, Intella returns a set of matching messages as a cluster in visualization of the search results. Clicking on this cluster displays the messages in a grid view.



By adding additional search strings, the cluster map will show how these search parameters interact – in the following picture, 3 search terms have been entered and a single mail is shown to contain all three search parameters:



The items in the grid can be opened, sorted and captured in categories for future reference.

Having identified a set of messages of interest, we will now widen the scope of our inquiry to consider:

- The social networks involved in the discussions, including highlighting the senders and receivers of messages in these conversation threads
- How the network evolves over time – who joins the conversation and who leaves it
- The nature of particular user activity just prior and after, and key email messages concerning F&J were sent

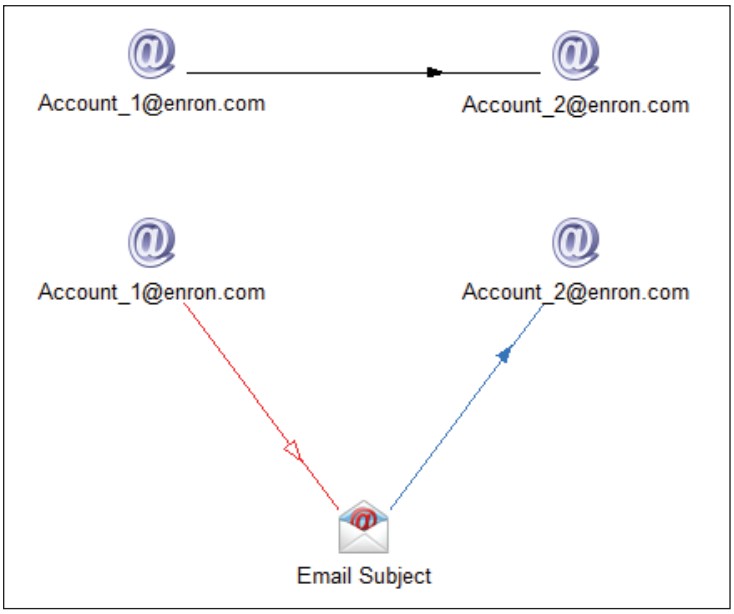
In addition to providing import functions for a wide range of email formats, Intella can also export sets of the converted email data into a structured CSV format which can be both viewed in Microsoft Excel, and loaded into link analysis and other analytical tools. For this example, we will not only export the set of messages that we were searching for, but the entire data set, as this will be needed to extend our search from our starting set of "F&J" data.

Again, there are a range of tools that could be used to perform associational and temporal visualisation, both free (NodeXL) and commercial – the application used in our example is Xanalys Link Explorer which can be used to query, visualise and analyze large data sets.

Remember that before you start your analysis, make sure to establish your investigative goals and tasks, as this will largely determine the tools and techniques you use, as well as keeping your lines of enquiry focused.

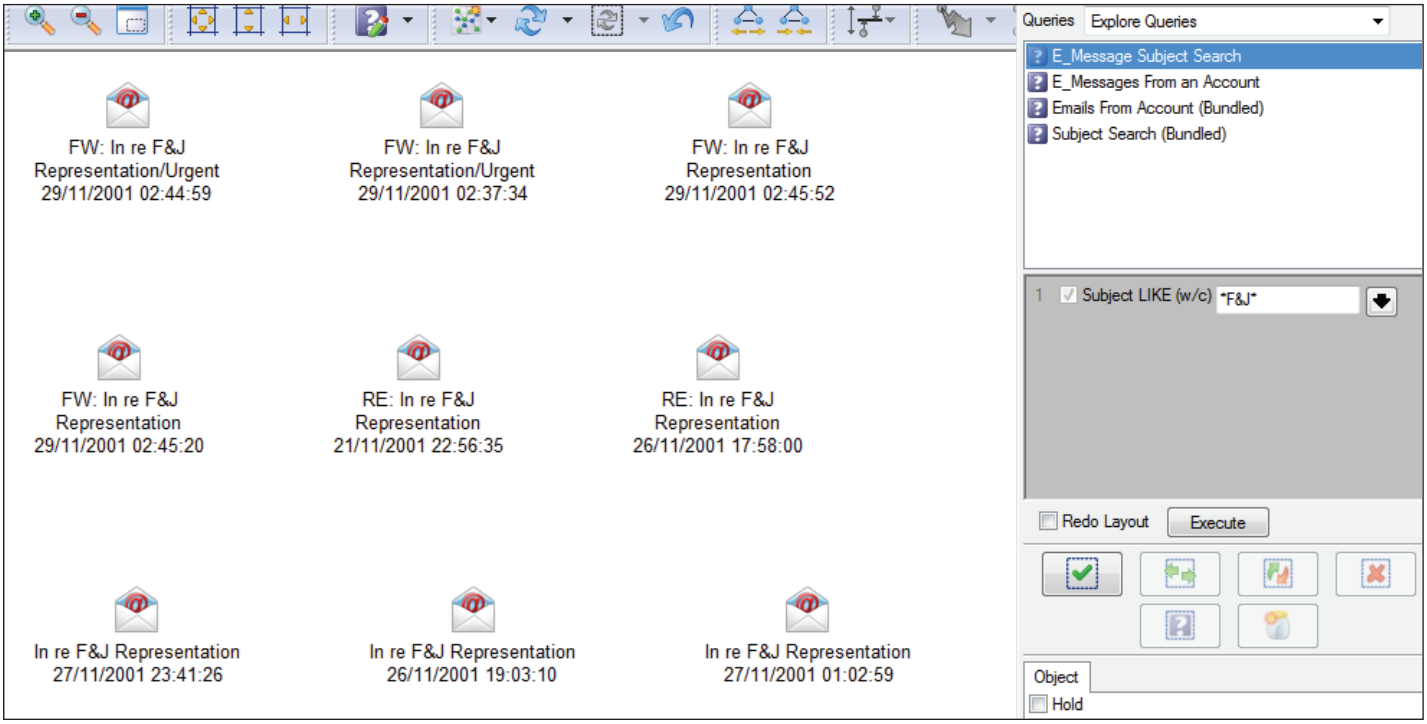
The first task in Link Explorer is to import the Intella CSV files into a database (I used MS SQL Server, but Link Explorer also comes with its own database). This import process not only transfers and loads the data, but also matches and unifies common elements within the data (e.g. if an email address is mentioned in the header of multiple messages, it is treated as a single entity linked to the many message entities).

Once loaded, the user can view the data not as columns and rows in a grid, but as sets of entities and links – in fact, two different models are created:

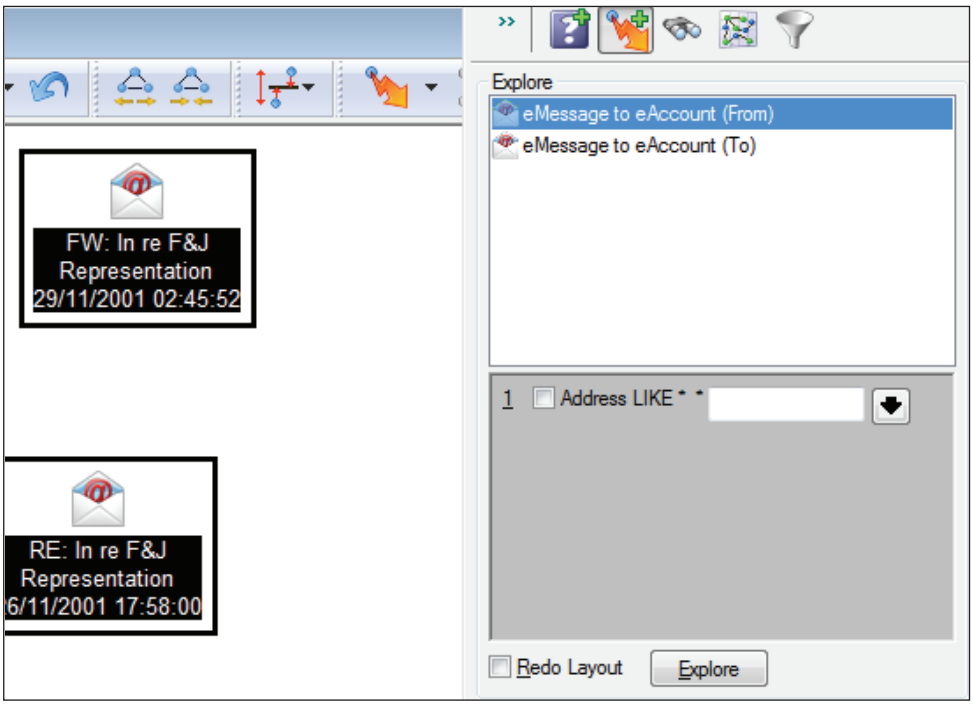


Although these two models essentially represent the same information, in the top model the message is represented by a directional link between the two email accounts, while in the second, the message is represented by an actual object. Each model has certain benefits when querying and viewing data. Clearly, the main focus is on the data stored in the "header" of the email – date/time sent, From, To, CC, etc. However, Link Explorer also supports free text search which can be applied to the Subject field, and if the body of the document is also imported into the database, to the main text content of the email.

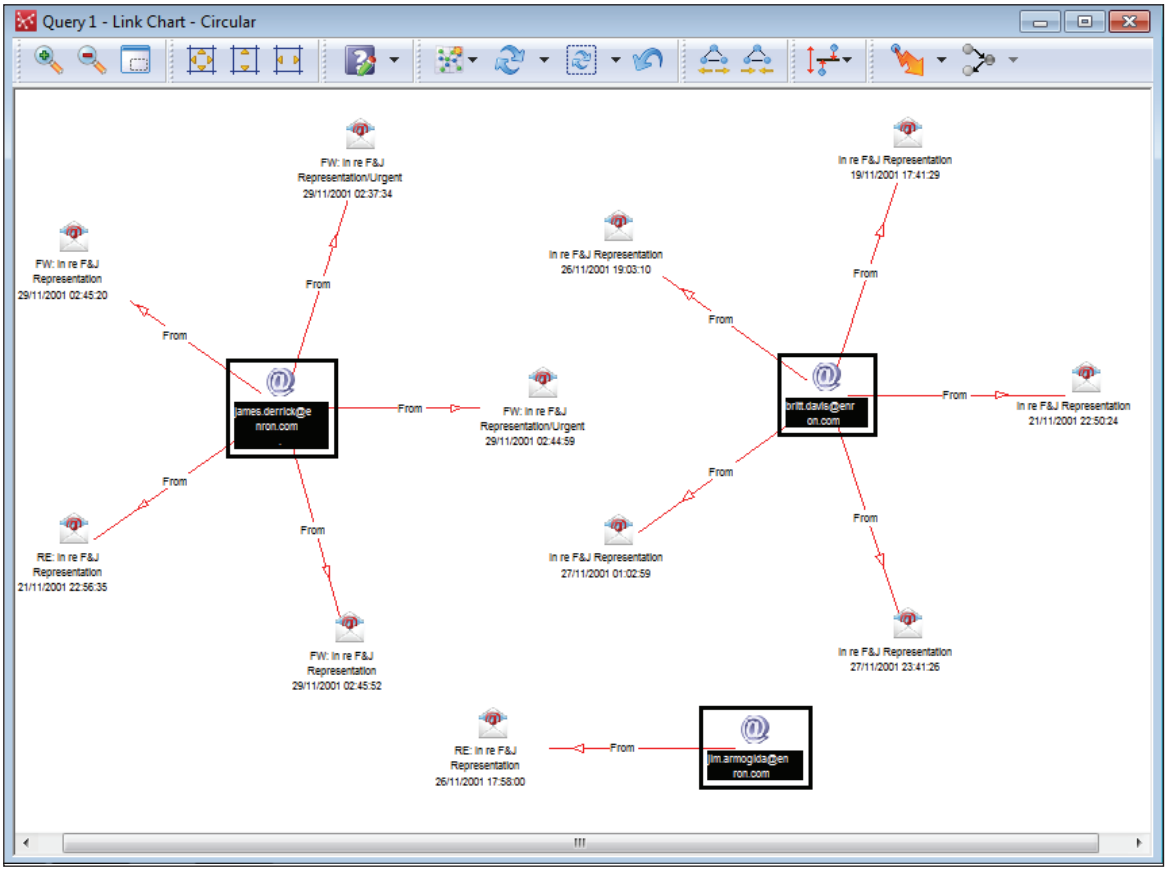
Having completed the export/import process, we recreate the "F&J" message set in Link Explorer.



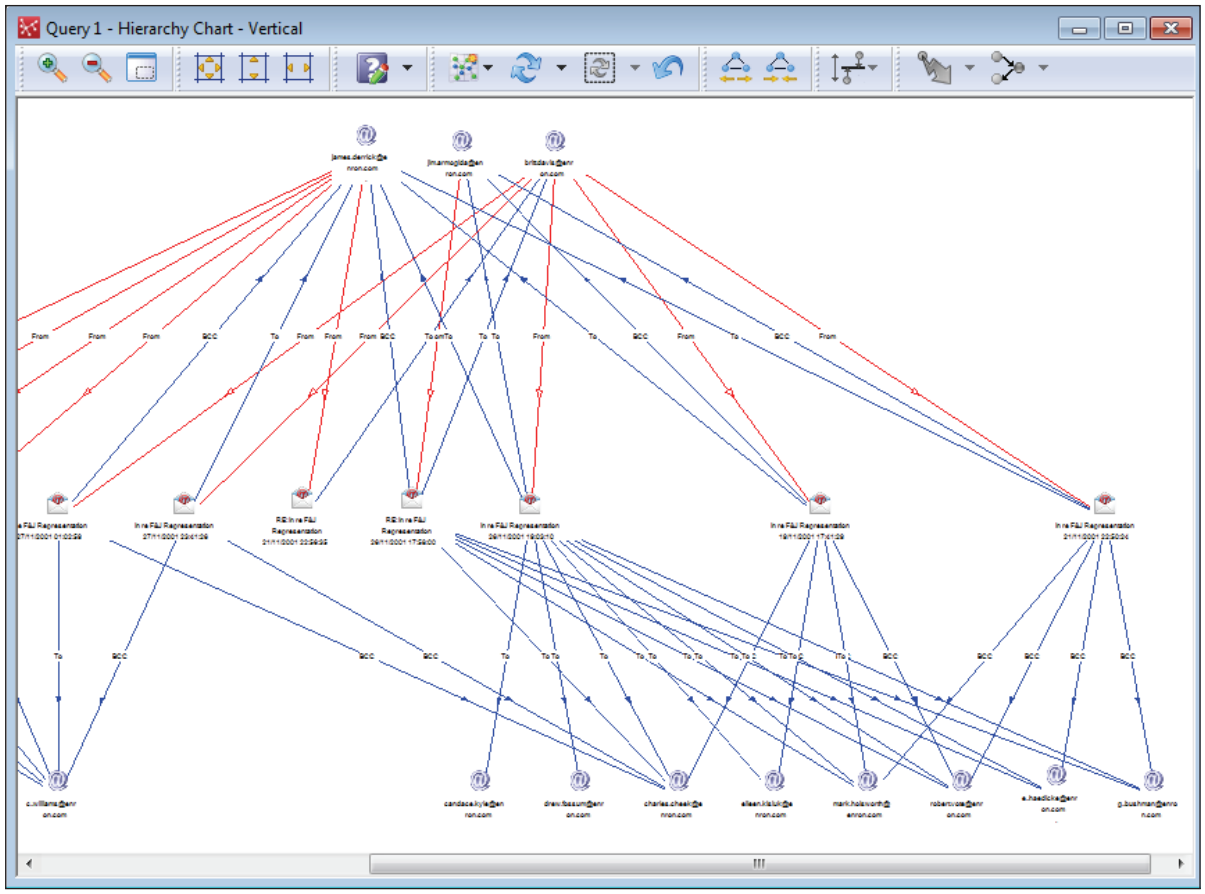
Next, we apply the Explore function on these messages, nominating to return only the senders of these messages. “Explore” is a data mining feature that returns linked objects at one or more degrees of association to our starting object(s). An associated feature that we won’t use in this example is “Find Links” which attempts to identify pathways between two objects in the database. Both of these features are extremely useful in determining associations between email accounts.



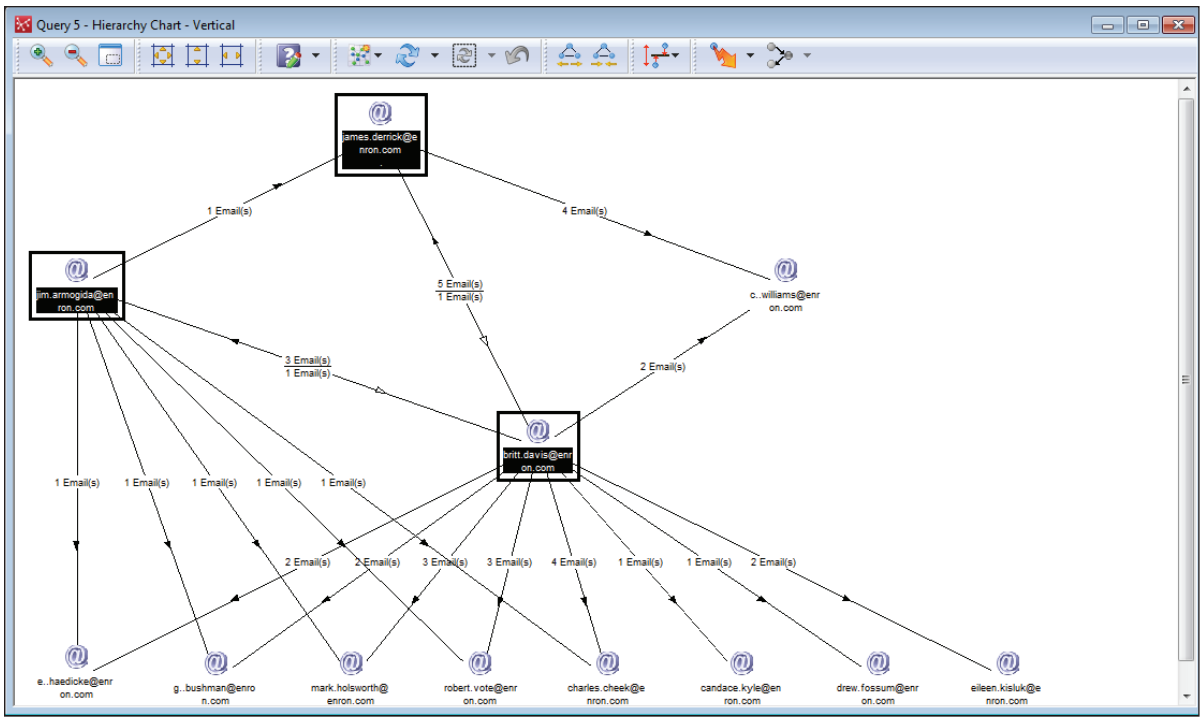
Having identified the senders of the mails, we tag, or “capture” these objects so that can be easily selected in future charts.



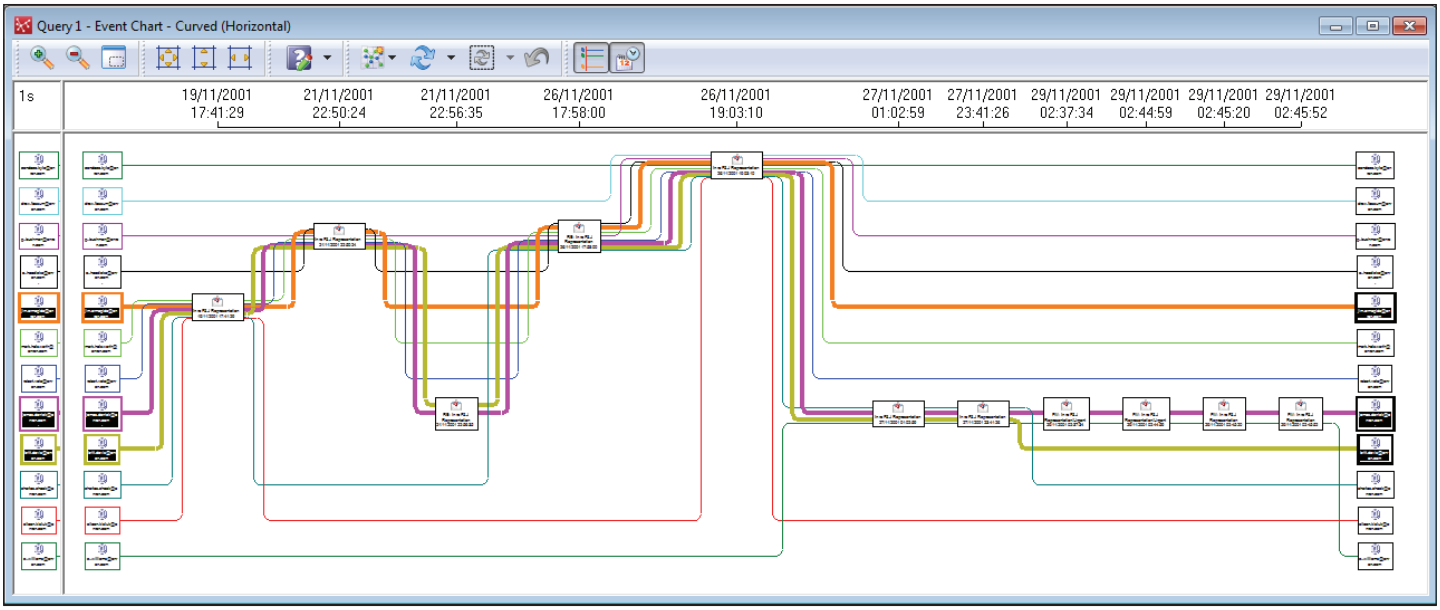
Next, Explore is used again to return the full set of email accounts associated with these messages. The resulting diagram shows us a network of accounts and messages, with the red links indicating the message had been sent from that account.



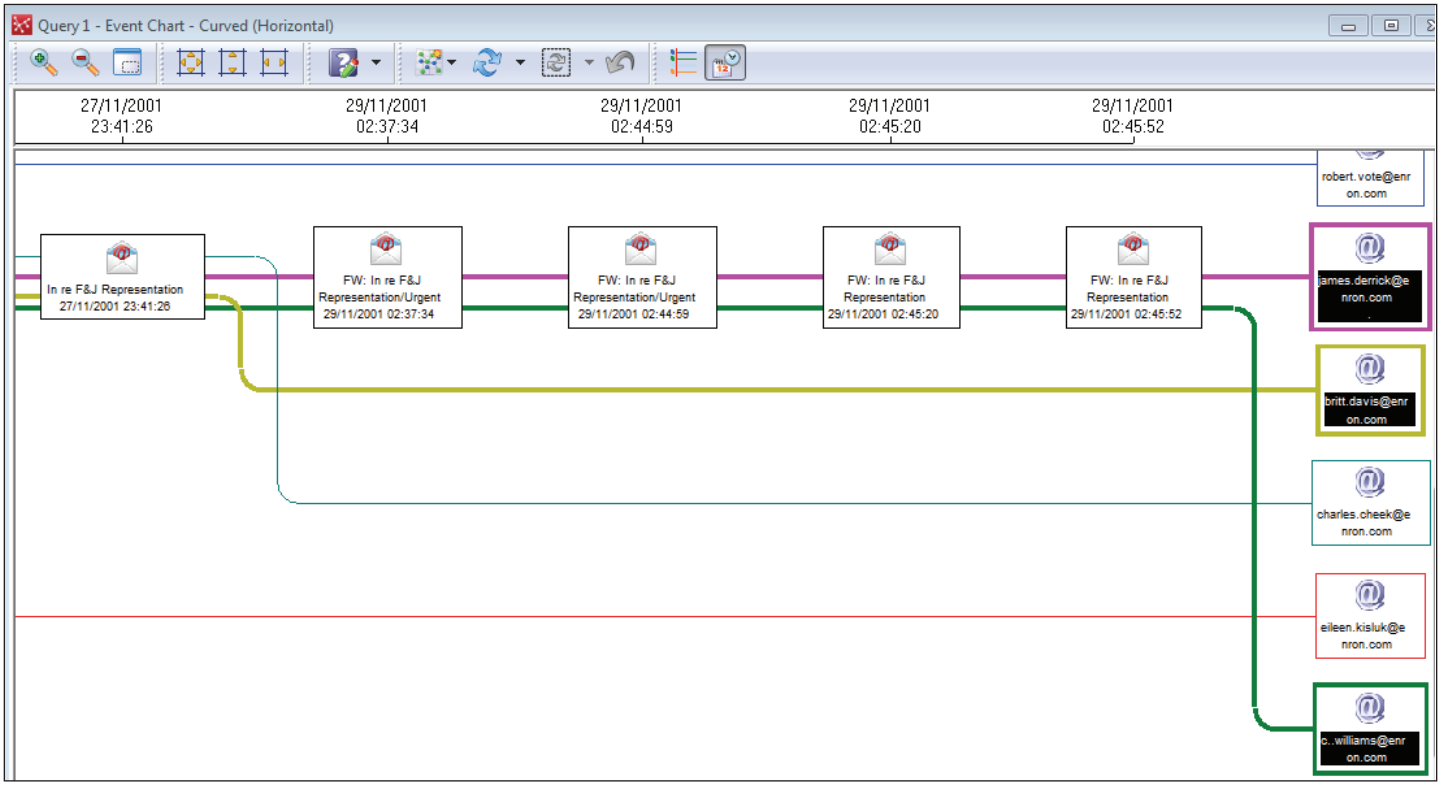
Here it is useful to view this data set using the alternative model – by removing the message entities, we obtain a clearer picture of the social network involved in these threads of conversation. The number of messages "bundled" under each link is indicated on the links.



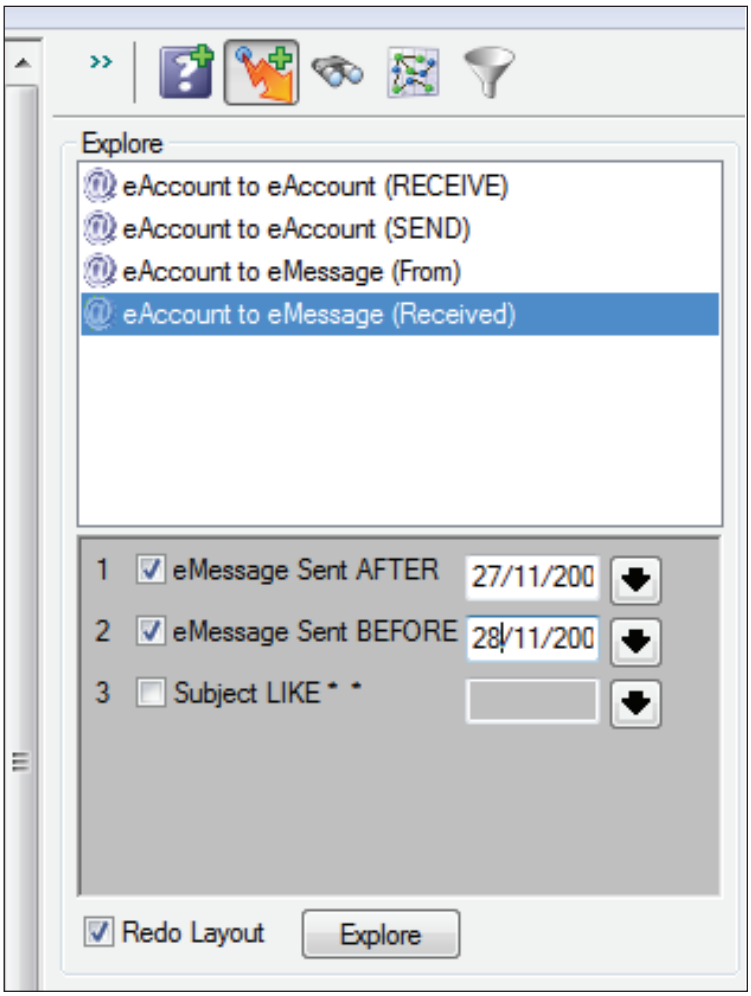
We can gain quite a different perspective of this network if we take into account the temporal aspects of the data. Having displayed the chart as a timeline, the 3 senders of the messages are selected (using the "tag" we created earlier). Note that there are definite patterns in how participants in the F&J threads join and leave the message threads.



Zooming in on the end of the thread, we see the conversation filter down to just 2 participants, once of which hasn't been involved at the earlier times. We also note the subject of the message now has the added label of "urgent".

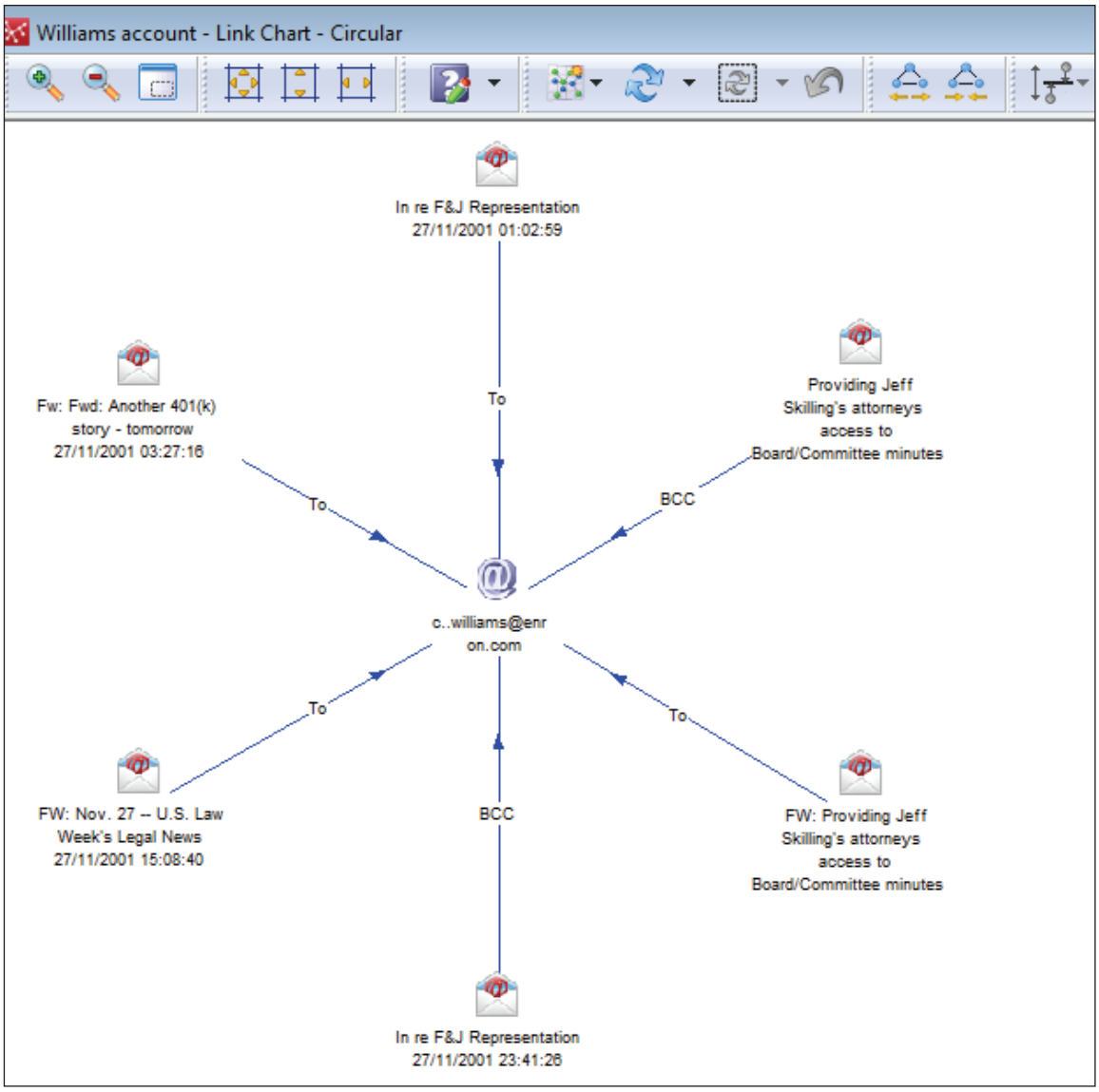


Can we learn more about this person and what their role in the organization is? Selecting the icon representing the account, we create a new chart containing just that entity. Applying the Explore again, this time however we focus on returning only the messages they send/receive around the time of those "urgent" messages – we do this by constraining our Explore operation with a start and end date.



For the analyst, while it is important to gain a practical knowledge of these techniques, it is just as important to understand the different components of email data, and which of these should be focused on to reveal the information relevant to their investigation.

Our final chart reveals a set of messages, some of which concern the Company President. Double-clicking on the icon will open a copy of the message that can be reviewed.



In this article, we have introduced a number of simple analytical techniques, some which are commonly used on other communication data such as telephone call analysis, that allow us to query and visualize a corpus of email data. For the analyst, while it is important to gain a practical knowledge of these techniques, it is just as important to understand the different components of email data, and which of these should be focused on to reveal the information relevant to their investigation.

Greg Mann is Managing Director for Xanalys Limited. Xanalys creates award-winning software that addresses the complex demands of investigation management and analysis.

ROSTER UPDATE ON THE LEIU SECURE PORTAL

More and more we are communicating non-sensitive information via agency e-mail. For this reason, it is extremely important that we keep our contact information up-to-date. The LEIU roster, where you can obtain member contact information, is kept and maintained on a secure website at the California Department of Justice/CCA. The website is the LEIU Secure Portal (although the URL now says CAL JRIES—it will soon change). The roster is the backbone for our member contact (not only from us to you—but between members). Utilizing the LEIU Secure Portal, you can edit your information in the roster. We automatically give permission for the representative and the alternate representative (the first two names on the roster) to make roster edits, as long as they have LEIU Secure Portal access. If you want to designate someone else in your agency to have this capability, please advise LEIU Executive Director Bob Morehouse at bob.morehouse@doj.ca.gov and we will add those permissions to that person after they have obtained access. The LEIU Secure Portal will also allow you access to the LEIU Gaming Index and the LEIU Intelligence Database. The LEIU Intelligence Database requires a security card to be filed, after which we will issue a digital token. Please contact Executive Director Bob Morehouse at the e-mail above to obtain a security card (if you already have a digital token no need to contact us). Access to the LEIU Gaming Index does not require a security card. Additionally, we use the LEIU Secure Portal to post many other items including Executive Board meeting minutes, the Constitution & Bylaws, and a Representative Responsibilities document. We also post many criminal intelligence-related documents and publications for your review and education. There is also a section on the LEIU site for the LEIU National Gambling Intelligence Sharing Group (NGISG). Given all the above, it is critical that you and your personnel sign up for access to the site.

Only LEIU members have access to the LEIU Secure Portal. To apply for access to the LEIU Secure Portal, please enter: **https://clix-reg.doj.ca.gov/LEIURegistration/default.aspx** into your browser. After gaining access, please confirm all of the information for your agency is correct (people, addresses, phones, etc.).

LEIU MEMBERS & CORPORATE PARTNERS

Who is eligible to be an LEIU member?

A municipal, county, state, or federal law enforcement agency having a criminal intelligence function which meet all other criteria of a Member Agency as established by the Executive Board. Exceptions must be approved by the Executive Board. An individual federal agency member may be appointed by the General Chairperson to represent federal agencies on the Executive Board. Only municipal county and state agency members are eligible to hold other Association offices.

What is an Associate Membership?

Associates - Associate status is available to individuals in the below listed categories. Any person who meets the specified criteria can apply to become an associate. Exceptions must be approved by the Executive Board.
Applicants in category 1 must provide a documented supervisory recommendation from their employing agency to apply for membership. Category 2 applicants must provide an endorsement from their former agency to apply. Associates do not have voting rights and cannot hold elected Association office. Associates do not have access to information contained in the LEIU confidential database and must identify their Associate standing when communicating with employees of a member agency.

- Individuals assigned to National Intelligence functions – This category includes individual law enforcement and non-law enforcement federal employees assigned to national security details whose employing agency is not a member agency.
- Retired LEIU Representatives – Retired, former law enforcement personnel who have served as an LEIU primary representative or who represented a LEIU member agency at two (2) or more National or Bi-Zone training seminars.

Who are Corporate Partners?

As in 1956, when law enforcement agencies from around the world first came together to fight the far reaching effects of organized crime, partnerships prove to be the instrument by which progress is made. Today we offer corporations an opportunity to join these partnerships as we proceed into the 21st century.

Who do I contact for more information about LEIU?

If you want more information about LEIU or a membership application, please contact your zone chairman (on the following page, locate your region and corresponding chairman). You can also access general information on our website: **www.leiu.org**

LEIU ZONE MAP AND CONTACT INFORMATION

General Chairman
Van Godsey, Assistant Director
Division of Drug & Crime Control, MSHP
(573) 526-6122
email: van.godsey@mshp.dps.mo.gov

Vice General Chairman
Robert Fowler, Lieutenant
Garden Grove Police Department
(714) 741-5867
email: robertf@garden-grove.org

Past General Chairman
Richard "Dick" Wright, Captain (Ret)
Simi Valley Police Department
(805) 929-1394
email: zwrights229@aol.com

Secretary / Treasurer
Steve Sanbar, Captain
Los Angeles Police Department
(213) 486-7220
email: 24822@lapd.lacity.org

Assistant To Secretary / Treasurer
Angela Perez
Los Angeles Police Department
(213) 486-7253
email: G9409@lapd.lacity.org

Executive Director
Bob Morehouse
CA DOJ, Bureau of Investigation
(916) 227-7880
email: bob.morehouse@doj.ca.gov

Federal Agency Representative
James McDermond, Asst. Director
ATF - Office of Strategic Intelligence
(202) 648-7991
email: James.McDermond@atf.gov

CCA - Coordinator
Kent Shaw, Chief
CA DOJ, Bureau of Investigation
(916) 319-8299
email: kent.shaw@doj.ca.gov

Recording Secretary CCA
Michele Panages
CA DOJ, Bureau of Investigation
(916) 227-7881
(800) 824-3860
email: michele.panages@doj.ca.gov

Legal Advisor
Keith Gardiner Burt, DDA (Ret)
San Diego County District Attorney's Office
(858) 737-7170
email: kgburt@cox.net

Eastern Zone Chairman
Angelo Woodhouse, First Sergeant
Virginia State Police
(804) 553-3541
email: angelo.woodhouse@vsp.virginia.gov

Eastern Zone Vice Chairman - Vacant

Northwestern Zone Chairman
Ron Leavell, Captain
Seattle (WA) Police Department
(206) 684-5549
email: ron.leavell@seattle.gov

Northwestern Zone Vice Chairman
Rick Herrington, Special Agent Supervisor
Washington State Gambling Commission
(360) 486-3590
email: rickh@wsgc.wa.gov

Central Zone Chairman
Lowell Due, Sergeant
Tulsa (OK) Police Department
(918) 669-6858
email: Ldue@ci.tulsa.ok.us

Central Zone Vice Chairman
Aaron Kustermann, Chief of Intelligence
Illinois State Police
(217) 785-4586
email: aaron_kustermann@isp.state.il.us

Southwestern Zone Chairman
Brian Gray, Manager
Riverside County Sheriff's Department
(951) 955-9296
email: bgray@riversidesheriff.org

Southwestern Zone Vice Chairman
Tony Lee, Captain
Beverly Hills (CA) Police Department
(310) 285-2109
email: tlee@beverlyhills.org

GST IntelNexus™

System Overview

GST IntelNexus™, developed by GeoSpatial Technologies, Inc. (GST), is an advanced intelligence database management system designed specifically for law enforecement agencies to collect, organize, maintain, and analyze sensitive information about individuals, organizations and their activities.

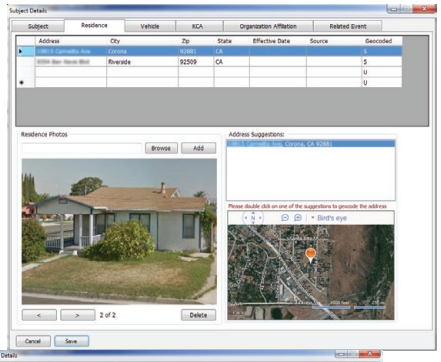
The system enables authorized users to create programs and reports pertaining to subjects, events, and organizations. Authorized users may easily and effectively search and retrieve specific sets of information from the database to create new reports or edit exisiting ones.

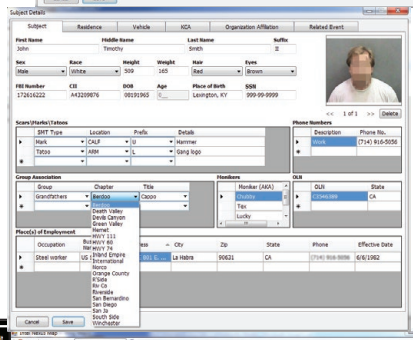
A built-in security mechanism requires the approval of system administrators for any new or edited reports to be accepted into the database. The system administrator may audit detailed end-user activities in retrieving information from the database at any time. When a report file nears it's required purging date, e-mail notifications are automatically generated to alert the designated personnel.

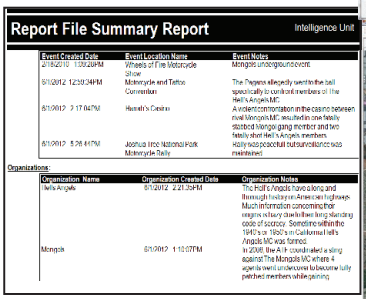
Files of any type can be attached to reports and stored securely in the database for quick retrieval. Location mapping is supported with an add-on module utilizing either Microsoft© Bing Maps with national map coverage, or an agency's own GIS data with detailed local information. The mapping module enables the user to validate any address and plot its location on the map. The spatial searching feautres enable the user to validate any address and find all the subjects, events, and organizations within a specified distance. IntelNexus™ databases can also be linked to GST CrimeMap to utilize it's powerful functionality in crime analysis.

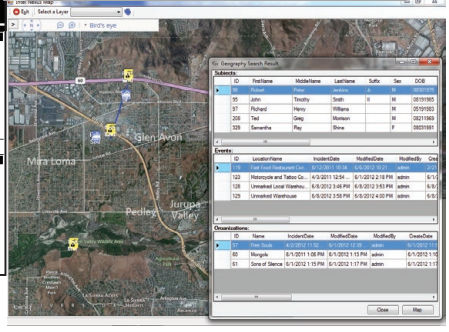
Key Features

- **Quick Summary and Detailed Reports** - Search for specific information fast and effectively
- **User-editable Fields** - Administrators may add new options to critical information tables
- **Well-Defined User Roles** - General and administrative access privileges strictly enforced
- **Secured Database** - Sensitive intelligence information kept confidential and secured
- **Extensive Database Searching Tools** - Conduct investigations extensively and thoroughly
- **Report Status Assignment** - Automatically assign permanent or temporary report status per CFR 28 regulations
- **Automatic Notification of Pending Purges** - Administrators may purge or extend a pending report
- **File Attachment** - Pictures of subjects, vehicles, buildings, events, can be incorporated
- **Subject-to-Subject Associating** - Identify individuals associated with any subject quickly
- **Audit Report** - Administrators may audit user activities to maintain accountability and ensure data confidentiality
- **Linkage to GST CrimeMap** - Utilize it's full-range of crime mapping and analysis tools
- **Location Mapping Add-on Module** - Geocode and validate addresses on Microsoft© national maps or local GIS maps
- **Spatial Search** - Identitfy subjects, organizations, and events within a distance from any location









System Requirements

Server:

- OS: Windows© Server 2008 or newer
- Database: Microsoft© SQL Server 2008 R2/SQL Server 2012 (unlimited size), or Microsoft© SQL Express 2008/SQL Express 2012 (10 GB database size limitation)
- Database Disk Space: 120 GB or more recommended

Workstation:

- OS: Windows© Vista / Windows 7
- Public Internet access (only required if using Microsoft© BING Maps for Location mapping)
- SMTP Server access for e-mail notifications
- Other: Network accessible storage

© 2012 GeoSpatial Technologies, Inc. All rights reserved.

GST®
GeoSpatial Technologies, Inc.
3130 S. Harbor Blvd. Ste 430 Santa Ana, CA 92704
Tel: (714) 434- 9936 | Fax: (714) 434-9937
Email: info@geospatialtech.com
Url: www.geospatialtech.com

20/20

THE 20/20 DEBUTS IN BEVERLY HILLS, CA

Some people may know it as the place movie stars live, or think of it when they see reruns of Pretty Woman, or the crazy antics of a fictitious Detroit cop named Axel Foley.

But last October law enforcement administrators, detectives, officers and analysts made their way through Los Angeles morning traffic, and on to their destination – Beverly Hills. And it was at the famous Beverly Wilshire Hotel where the Southwest Zone of the LEIU hosted the inaugural LEIU 20/20. If you missed it, don't worry, you will get another chance this year. Speaker selection will begin in April and the event will take place later in the year.

What exactly is the LEIU 20/20?

A paradigm shift in training – where hindsight, insight, and foresight work collectively together – to rise to the challenges of the changing world of crime. The 20/20 provides a platform where 20 speakers, speaking no more than 20 minutes each, are free to challenge the old ways of doing things and embark on a path that leads to inspiration and new ideas.

A variety of topics from many noteworthy speakers

Our speakers were selected based on expertise, ability to enthusiastically communicate their ideas, passion for their topic, and the their topic's appropriateness for a varied law enforcement audience:

Dick Wright (LEIU past General Chairman) opened the event with an enlightening presentation on the historical aspects of LEIU and the role LEIU plays in the lives of intelligence officers across the United States. With this role in mind, Southwest Zone Chairman, Brian Gray laid out the thinking and motivation for hosting the 20/20, his thoughts on the need for a paradigm shift and the importance of a different kind of law enforcement training model.

Stephan Margolis (LAPD Lieutenant) shifted our focus to how we make decisions and he offered practical advice on changing the decision-making culture we work in.

Following this presentation Robert Bjork Ph.D (UCLA Professor) shared his research on how our memory works, how we learn and on the implications for lasting training.

Chris Njunge (Ph.D Student from Claremont Graduate University) spoke to the hearts and minds of everyone who has ever felt unappreciated at work, and talked about being the 'glue' that holds teams together.

Renee Mitchell (Sacramento PD, Sergeant) of Evidence Based Policing fame talked about getting law enforcement to change its SOP's and long held beliefs when faced with evidence contrary to how we normally operate.

Brian Heidt (Xpect Software) used his vast and varied experience as an Intelligence Manager and Analyst to talk about the challenges we all face working in the intelligence field. Heidt also shared some best practices and tips for both novices and veterans alike.


20/20

Award winning speaker, Sue Bauer Ed.D comically related speaking to building a cheeseburger, her presentation on how to deliver a successful presentation was both informative and creative.

Randy Throne J.D. (RSO Chief Deputy (Ret)) dared to ask the question: How do you know what you know? Or more importantly: How do you know what you do not know? His talk on information filtering and building better data collection techniques offered ideas for improvement.

Ken Osborn, author of Stop the Lies, engaged the audience with a talk on how to spot deception by observing subtle, verbal, vocal and kinesics subconscious behaviors, while Paula Sassi discussed detecting lies and predicting behavior through the use of handwriting analysis.

Michael Downing (LAPD Deputy Chief) discussed the evolution of an ever-changing terrorism threat. We now see terrorist groups converging with other criminal groups. The federal government and all levels of law enforcement face challenges of dealing with a threat that is now more complex and an intelligence signal that is weaker than it once was. He stated the best opponent for a decentralized adversary is a decentralized organization – State and Local Law Enforcement.

Crystal English spoke of the innovative research that is taking place in the GIS community. Crystal's talk focused on the use of spatial clustering, remote sensing, and open source programming languages to enhance the tools we currently have to fight crime spatially.

Sonya Grayson (Medical Liaison Analyst, LAPD) left no one in their chairs, as she actively involved the audience members throughout her presentation. Sonya demonstrated that breaking out of your comfort zones could lead to great discoveries. She challenged everyone to move from the sharing of ideas to the risk taking of implementation.

Brian Hospodar (Detective LAPD) gave one of the best talks on ethics in law enforcement I have ever heard. His sometimes touching, sometimes funny but always-serious approach to this difficult topic had everyone listening. He inspired us to develop a level of self-awareness to our actions and thoughts and spoke to the importance of personal integrity.

Joanna Mendelson (Director of Special Projects, ADL) gave an informative presentation on the ideology and symbology associated with white supremacy groups and other domestic terrorist groups.

Glenn McGovern (Senior Criminal Investigator, Santa Clara District Attorneys Office) spoke about the dangers law enforcement personnel face during "non-duty" hours. His research over the past 10 years indicates that attempts on justice community personnel are increasing. McGovern spoke to the motivation of the offenders and showed the audience many of these attacks occur at our homes.

Vaughan Miller (Asst. Fire Chief, Ventura County FD) spoke about advances in geographic information systems to allow first responders to gain situational awareness, assess risks and support decision makers. As impressive as these new advancements are, he also touched on the internal resistance that occurs before new technology and change is accepted.

Usha Sutliff (Program Manager, National Consortium for Advanced Policing) spoke to the need for more law enforcement collaboration in dealing with transnational threats. Sutliff illustrated the current needs for collection plans, intelligence gathering, intelligence analysis, intelligence led policing practices, and developed human sources. Her discussion touched on the great disparity between what we need and what we currently have.

Wendy Harn (Asst. Director, LASD) spoke passionately about innovation in law enforcement analysis. Based on years of experience, she noted the importance of listening, observing, discussing, inspiring, creating, processing, adapting and acting.

The LEIU 20/20 is a law enforcement event like no other.

When a collective group of professionals come together to share their experiences, passions and even untested but promising theories, a new form of learning takes place.

We hope to see you at the next LEIU 20/20 event being held in Fall 2013, Beverly Hills California.

Do you have what it takes?

If you have a gift for speaking in short form presentation style, an idea you want to share – and the guts to put yourself out there – we want to hear from you. To keep costs down, speakers volunteer for this event and must agree to follow the 20/20 rules. Interested speakers should contact Brian Gray at: **intelligenceanalysis@mac.com** or by phone (714) 595-5750.

Thank You, Vendors and Sponsors!

LEIU 20/20 VENDORS

GST - GeoSpatial Technologies
John Lim, CEO
3130 S Harbor Blvd
Santa Ana, CA 92704
Tel: (714) 434-9936
email: jlim@geospatialtech.com

PEN-LINK, LTD.
John Spomer
5936 VanDervoort Drive
Lincoln, NE 68516-2503
Tel: (402) 421-8857
Fax: (402) 421-9287
email: Jspomer@penlink.com

Xpect Software
Brian Heidt, Subject Matter Expert
Tel: (856) 924-5203
Cell: (609) 678-7388
email: bheidt@xpect-software.com

LEIU 20/20 SPONSOR

American Military University
Dennis Porter
Sr. Law Enforcement Education Coordinator,
Western Region
10110 Battleview Parkway, Suite 114, Manassas, VA 20109
Tel: (562) 252-6195
Fax: (703) 396-6433
email: dporter@apus.edu

EMBRACING AND INTEGRATING LOCATION-BASED
INTELLIGENCE TECHNOLOGIES

by Hong Chou, Ph.D and Christopher Mason, M.A.

PAPER MAPS AND PUSH PINS. These were the humble beginnings of spatial analysis within the intelligence community. Intelligence officers are challenged with location-related questions all the time – e.g. Where is the geographical influence of organized crime groups? Where do the members of organized crime groups reside? Where does the presence of organized crime effect the community? And we cannot forget the tactical need for maps and aerial imagery and their impact on planning and decision-making…

Within the past decade, law enforcement agencies have embraced location-based technology at an increasing rate. This is partially due to the commercialization of Geographic Information Systems (GIS) and on-board navigation devices. Today, sophisticated mapping programs are not only available but affordable. The large volumes of geographic information available in most parts of the county are a further benefit to the intelligence community (to include schools, parks, banks, and other theme based information). The major challenge is two-fold: how can we incorporate the latest location-based technologies into the intelligence function, and how can we use location-based information to educate new intelligence officers/analyst of spatially significant areas within the area of responsibility. This can be done in several ways, two of which include the development of spatially enhanced intelligence files and implementation of location-based technology in real time.

Development of spatially enhanced intelligence files

One difficulty the intelligence community faces is sifting through the enormous volumes of information available. The intelligence community has a need to work accurately, efficiently, and timely. This can be accomplished by creating an automated system to run information in the intelligence files (names of people, residences, vehicles, places of employment, etc.) against open source databases and records data. Access to this timely information can quickly support and enhance human intelligence. Although human

intelligence is only about 10% of the information we analyze, it is a crucial part of the intelligence files. On the other hand, open source information makes up 90% of the intelligence files. Many open source databases now have built in batch lookups and alerts to notify the user of changes in requested information. Creating similar batch lookups and alerts on records data and combining the information with open source information can spatially show where subjects in the intelligence files were recently FI'd, changes in residence, where events of significance took place in the past, and so forth. In addition, many law enforcement agencies are utilizing Automated License Plate Readers (ALPRs) to track dates, times, and locations of vehicles in the problem areas of the community. This information can also be collated into spatial analysis to enhance the intelligence files. Layering records data, open source data, and intelligence using spatial analysis software reveals a larger picture of the patterns for criminal organizations and their members.

Implementation of Location-Based Technology in Real Time

Intelligence is an incredibly unique field in law enforcement. Similar to other specialized units, it takes years to develop a working knowledge and expertise not only in the intelligence guidelines but in understanding certain organizations, their thought processes, their belief systems, the areas of operation, the type of criminal activity they conduct, other members or groups they associate with, and the list goes on. This can easily take a minimum of 3 to 5 years to develop. Unfortunately, the intelligence community faces is turnover at the same rate as any other unit. Officers get promoted or transferred and now someone new has to start from scratch to develop the expertise to do the job. Articulating the years of experience in writing, and ultimately displaying the information spatially can be invaluable in tackling the issue of turnover.

Patrol has started to embrace the use of location-based technology to improve the location data in the records system. What if undercover vehicles for intelligence units utilized these technological advances in location-based technology? Developing a location-based alert system in undercover vehicles can inform intelligence officers on a variety of spatially relevant information – when an officer moves into a geographical area where members of organized crime groups reside or conduct business, where members of the organized crime groups were FI'd, where significant events have taken place (homicides, shootings, narcotics busts, etc.), where members reside in relation to crime problems, geographical areas of influence for organized crime groups and how those areas have changed over time, and so on. This information is valuable for both seasoned officers and new comers into the intelligence unit. Using this spatially relevant information, intelligence officers would be able to take a more proactive approach in dealing with organized crime and is a positive step toward actionable intelligence.

Technology for a Safer World

There have been tremendous advancements of GPS, GIS, and wireless communications in the past decade. The technological capabilities that were once only dreams in the imagination of the intelligence community are now a reality. The intelligence community once faced the dilemma of having too little information. Now, due to technological advancements, the intelligence community is swimming in an ocean of information. Rather than depending on stagnant paper maps to show unmoving locations, officers and analyst now have access to digital maps that are dynamic and changing as information changes. Location-based technology can offer the intelligence community a wide range of powerful tools, from the analysis of spatial linkage in criminal investigations to the real-time situational awareness during field operations.

Many key members of LEIU have been forerunners in the development and promotion of technology through the proud history of LEIU. They have played a vital role in leading the intelligence community to build and utilize all the best available technology for a safer world!

Hong Chou, Chief Technology Officer
GeoSpatial Technologies, Inc.
3130 S. Harbor Blvd. Suite 430, Santa Ana, CA 92704

Christopher Mason
Crime & Intelligence Analyst Consultant
Riverside County Sheriff's Department (7 years)

A FINAL NOTE

Brian Gray
Southwest Zone Chairman, LEIU

This morning I walked in to my office sat down and was looking at the many career-related books on my shelf. Some I have read and some waiting to be read. Some I bought myself and some were gifts from peers and mentors. Each with its own story to tell, each with a point the author wanted you to think about, remember or put into practice.

About 3 years ago, I was assigned to attend a 6-month course on leadership. More than likely, it was similar to ones you may have attended, perhaps a bit longer. To be honest, I didn't want to go. I was 'too busy' to add one more thing to my plate, but I decided to try to make the best of it.

Like many classes of this type you receive copies of articles, academic publications, instructor insight and many books. Yes, even a copy of that Steven Covey Book "7 Habits of Highly Successful People". In fact, it's one of the books on my shelf and that's where this story begins. After spotting this book and reading its title, I opened my email to the Seth Godin blog posting below:

"There's a million habits out there, some good, some bad, all learned. Every habit (your market, your family, your organization has) was formed because people got rewarded for it, at least in the short run.

The thing is, every habit is changeable with effort." – Seth Godin

The more I researched, the more I learned about habits. In fact, did you know there is an app for that? I queried "Habit" in my apps program and it brought up 400 apps, but a free one called "LIFT" seems to be one of the most popular. After downloading this app, I discovered that the ten most popular habits people are trying to form are:

1. Exercise (59,711 participants)
2. Drink More Water (53,814 participants)
3. Read (27,000 participants)
4. Floss (26,204 participants)
5. Pushup(s) (24,038 participants)
6. Sleep by Midnight (21,511 participants)
7. Run (20,027 participants)
8. Meditate (19,642 participants)
9. Take Multivitamin (19,210 participants)
10. Go To Gym (18,865 participants)

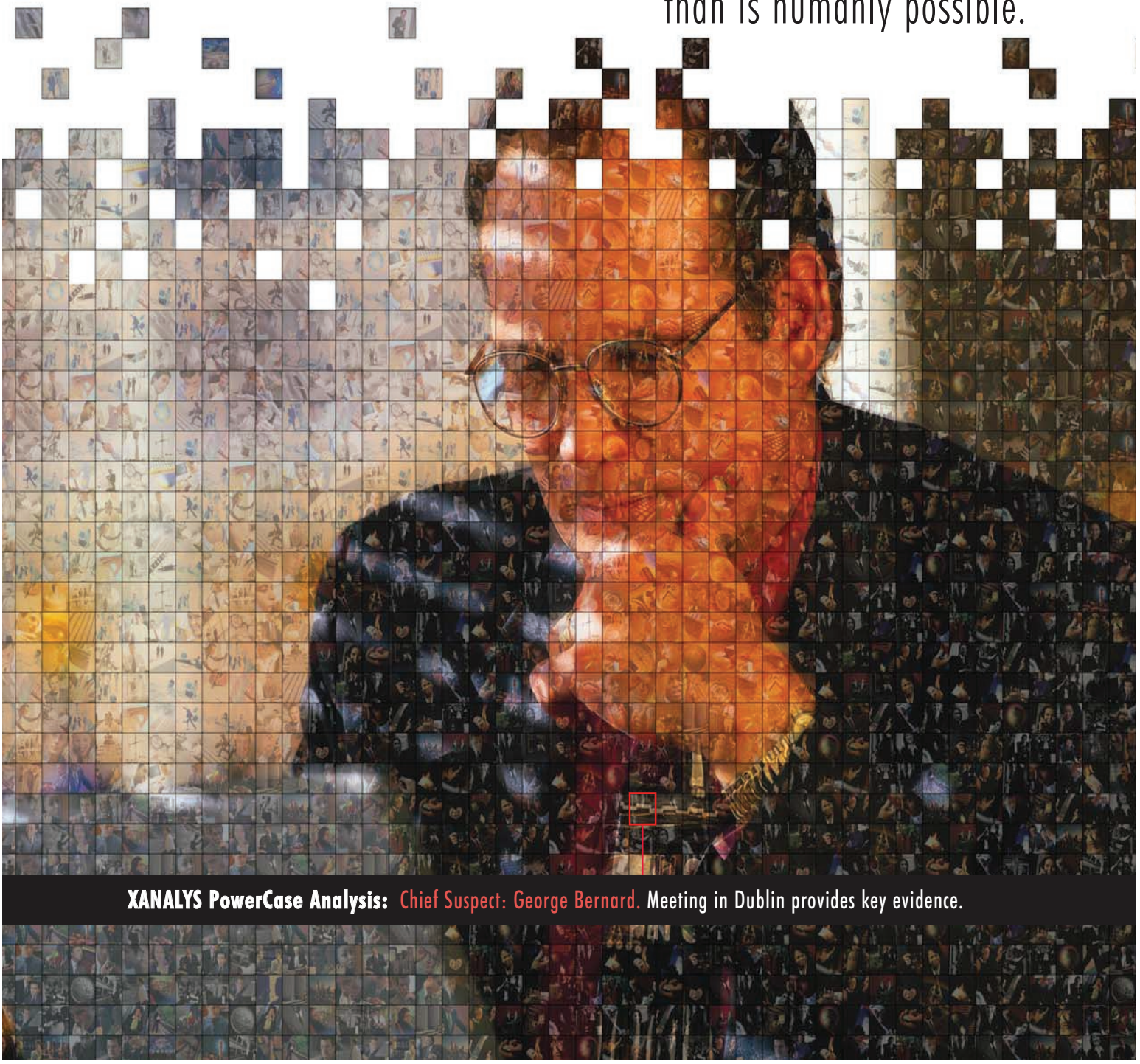
But the list didn't stop there; people were using this app to remind them to take walks, write in journals, make their beds, quit smoking, eat salads, eat fruit, brush their teeth and even tell their loved ones they love them. Good habits can be learned and this got me thinking. What habits do we as intelligence professionals want to form and what habits do we need to break? Perhaps we might make a list like this:

1. The habit of doing it right, instead of doing it over
2. The habit of quality work, over quantity of work
3. The habit of following the intelligence cycle
4. The habit of going above and beyond
5. The habit of opening ourselves to new experiences
6. The habit of not underestimating or overestimating
7. The habit of good communication
8. The habit of ending complacency
9. The habit of risk taking
10. The habit of sharing

What might your list look like? Assess your personal habits (to either add to or delete from your work life) and with a little reflection, your own list can go a long way to personal growth in your career.

XANALYS PowerCase –

There actually is a way to do more than is humanly possible.



Xanalys®

Let nothing escape you.

XANALYS PowerCase –

Ensuring effective investigative management.

War. Terrorism. Epidemics. Murder. Fraud. Corruption. As incident after incident tears at our society and public fears noisily escalate, the clamor for better investigative results is increasing exponentially. And not just for after the fact results, but also for preventive results. Public confidence is reinforced by investigations having clear and uncompromising outcomes.

Times have changed, and everyone is watching. There is no more margin for error, and we cannot count on luck. Quite simply, the way we initiate and conduct an investigation will determine the outcome of that investigation. Organizations such as the following are feeling the pressure like never before:

- Law Enforcement
- Financial Services
- Homeland Security
- Insurance Industry
- Intelligence Agencies
- Healthcare
- Public Health
- Public Inquiries
- Investigative Consultancies
- Humanitarian and Peacekeeping Agencies
- Environmental Agencies

All these interests share an essential common requirement: a coherent investigative system that inherently drives activities toward success.

THE INVESTIGATIVE MANAGEMENT SOLUTION

Existing investigative systems suffer from decentralized, largely paper-based memo-and-memory processes that rapidly overload and break down. As a result, investigators grope through incomplete information and must rely on intuition and subjectivity. Without a standardized investigative methodology and a centralized information repository, manual systems have outlived their usefulness.

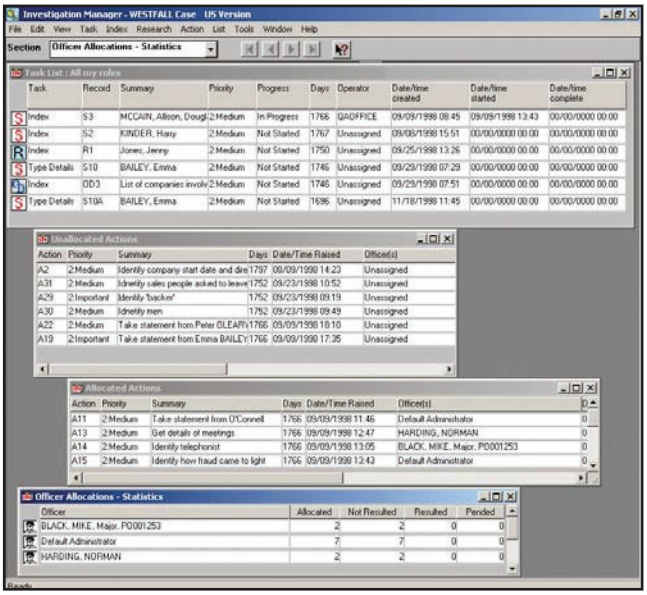
In spite of all good intentions, today's investigation managers are a vulnerable target. While the subjects of their investigations grow ever more difficult and complex, they struggle with restrictive budgets and resources. At the same time, the public and press respond to perceived carelessness, delays, failures and excuses with increasingly strident cries for better, faster, more certain results. Investigation managers need a helping and reliable hand.

XANALYS PowerCase pulls all this together and more by helping drive the investigation to a successful outcome through the end-to-end support of the complete investigative management process.

COLLABORATION

XANALYS PowerCase provides a collaborative environment for effective teamwork that reduces costly investigation times and increases efficiencies — a boon in these days of resource and budgetary restrictions.

XANALYS PowerCase supports unlimited numbers of investigators in multiple locations and enables investigative teams to smoothly work together in the collection and management of information, including evidence, assumptions and actions.



XANALYS PowerCase supports a collaborative environment where actions allocated to team members can be reviewed, prioritized and monitored.

SEARCHING

XANALYS PowerCase can search and find key information on the current case or across multiple cases (including archived cases) that could turn up the essential fragment that resolves a case. This puts an end to dependencies on memory, misplaced memos, or recalling cases from the past.

Investigation teams working on separate cases have little opportunity to compare notes and ideas.

INDEXING

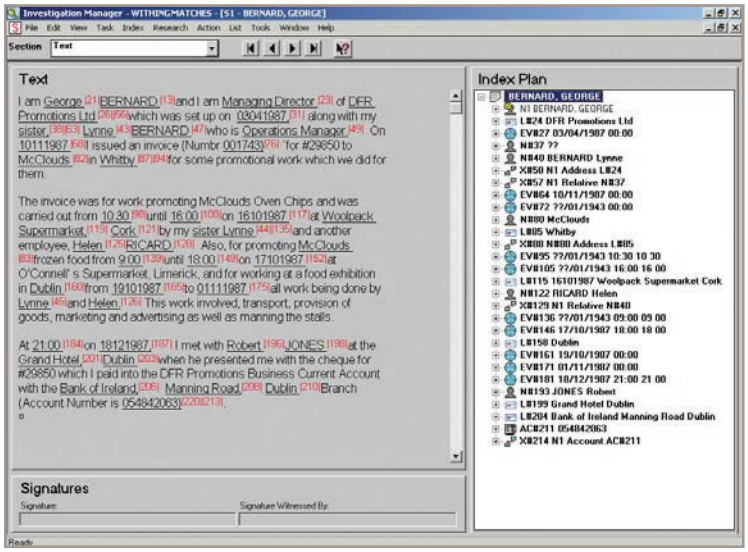
XANALYS PowerCase supports both manual and automatic indexing of documents. Indexing is the process of identifying relevant information in raw documents, such as notes, memos and investigation reports, so it can be organized for integration with the structured database.

Because manual indexing is labor intensive, XANALYS PowerCase provides XANALYS Indexer to automatically translate unstructured data into meaningful structured information. XANALYS Indexer uses Xanalys' patented natural-language processing capability to analyze documents, mark up text, and extract meaningful entities and attributes. With a structured database, research and analysis can proceed with speed and accuracy.

DOCUMENTATION AND REPORTING

In the political and professional pressure-cooker that is today's investigative setting, careers can hang in the balance of investigation outcomes. Regardless of the type of investigation — criminal, scientific, political, business or financial — the accuracy and completeness of case documentation significantly affects everyone involved.

Investigation managers need the latest information on a daily or even hourly basis. XANALYS PowerCase puts up-to-date, accurate information concerning all investigative activities, the status of actions and deployment of resources at the fingertips of the investigation team and management at any time.



XANALYS Indexer automatically translates unstructured data into meaningful structured information called an Index Plan.

XANALYS PowerCase

At a Glance

- Up-to-the-minute information is always available.
- Laser-precise search, research and analysis.
- Every action of the investigation team is tracked and integrated.
- Managers are assured that team members know what to do and when to do it.
- Collaboration is maximized and duplication is minimized.
- Information sources and data acquisition details are faithfully recorded.
- Bulletproof documentation of complete investigation.

XANALYS investigative software solutions:

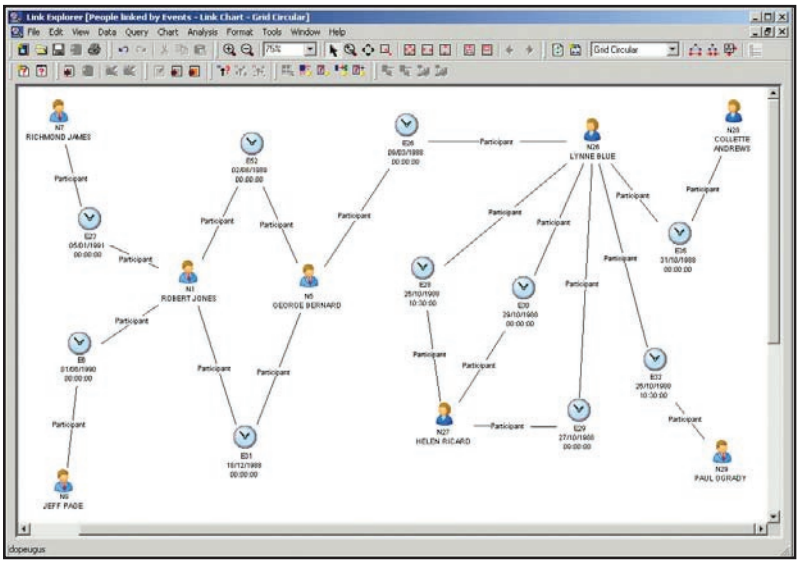
- XANALYS PowerCase®
- XANALYS Link Explorer
- XANALYS Indexer

Everything has been documented in XANALYS PowerCase, linked back to its origins — who, what, where, when and why, and available for electronic access or printing for the court or senior management. Such thoroughness is difficult, if not impossible, to be undermined by the closest scrutiny of the most ardent critic of the evidence.

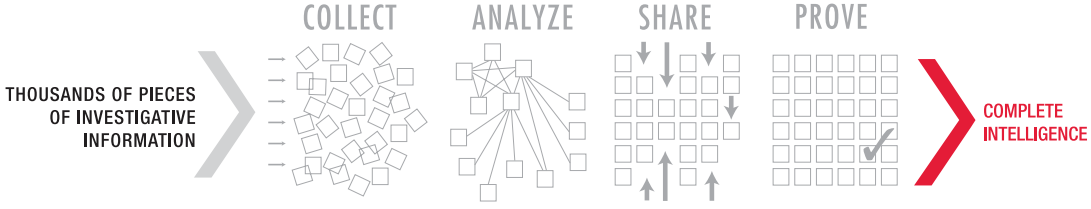
WORKFLOW AND ACTION MANAGEMENT

Because investigations never stand still, rapid and accurate action management generates a distinct tactical advantage for investigation managers by being able to put the right people in the right place at the right time. Priorities and workload balancing is comprehensively supported, enabling investigations to move forward more efficiently and effectively. Actions allocated to team members can be reviewed, prioritized and monitored by managers.

XANALYS PowerCase's internal workflow controls the flow of documents through every stage of information processing. It determines what tasks need doing and to which task lists they belong based on the status of actions and documents. And XANALYS PowerCase automatically alerts users when documents and actions require their attention.



XANALYS PowerCase integrates seamlessly with XANALYS Link Explorer, which provides powerful link analysis capabilities that can rapidly reveal the links between people and events.



An innovative investigative approach:

Xanalys provides a dependable suite of software solutions that enable you to rapidly collect, manage, analyze and share actionable, proven investigative intelligence. Every bit of data capable of helping your team to accurately and efficiently solve its case is quickly refined and distilled into crystal-clear intelligence. You miss nothing. No case will ever be compromised.

Xanalys®
Let nothing escape you.

www.xanalys.com

Xanalys Limited
Market Court
20-24 Church Street
Altrincham, Cheshire
WA14 4DW
United Kingdom
Ph: +44 (0) 161 941 7792
Fx: +44 (0) 161 332 8285

© 2004. Xanalys Limited. All rights reserved. Xanalys, the Xanalys logo, PowerCase, Watson, and Quenza are registered trademarks of Xanalys Limited. PowerDetecter and Triggering are trademarks of Xanalys Limited. All other trademarks or registered trademarks are the property of their respective owners. All references to persons herein are fictitious, and any resemblance to actual persons, living or dead, is purely coincidental.

0804-PB-XIM01

GET PLUGGED INTO LEIU!

The LEIU annual conference provides certificated training and the opportunity for intelligence professionals to network with other members and their associates. LEIU also provides its members with evaluation and technical assistance in the formation and organization of their agency's intelligence function. In addition, LEIU provides timely publications and appropriate advocacy for professional criminal intelligence standards on the national level. LEIU is an agency-based membership.

If your agency is not a member and would like to join or receive information on joining, please contact the LEIU Central Coordinating Agency at leiu@doj.ca.gov or call LEIU at 916-227-7881.
Let LEIU be "Your Voice at the National Level!"

LAW ENFORCEMENT INTELLIGENCE UNITS
LEIU
founded 1956

www.leiu.org