



**ANDERSON COUNTY GOVERNMENT
SOLE SOURCE & EXCLUSIVE RIGHTS
AND LICENSE JUSTIFICATION FORM**

SUBMIT WITH REQUISITION TO PURCHASING DEPARTMENT

DATE: 12/22/2023

CHECK ONE:

- ☒ **Sole Source** – Product or service(s) is only available from a single vendor or supplier.
- ☐ **Exclusive Rights & License** – Vendor holds exclusive patents and/or license for this product. An Exclusive Rights letter with current date must accompany this request.
- ☐ **Upgrade or renewal to an existing software system** – Provide information regarding current software system.

Requisition Number: _____ Requisition Amount: \$ 74,068.20

Vendor Name: PenLink

Vendor Address: 5944 Vandervoort Dr. Lincoln Nebraska 68516

Vendor Telephone #: _____

Requesting Department: Anderson County Sheriff's Office

Requesting Official: [Signature]

JUSTIFICATION FOR THE REQUEST

***What is the function of this product or service?
Why is it needed? What makes it unique?***

This information will be used to approve or deny the purchase. PLEASE BE SPECIFIC.

ATTACH MEMO IF ADDITIONAL SPACE IS NEEDED. Sole Source purchases that exceed the bid threshold will be noticed on vendor registry for 10 business days prior to purchase approval.

This is the only vendor with software that organizes phone data so the user can read it like a conversation instead of different zip files.

NOTE: We use the Google test to search for comparable products or services. If found, it is **NOT** considered a sole source product or service.



Quote

Company Address 5944 Vandervoort Dr.
Lincoln, Nebraska 68516
United States

Quote Number 00032460
Created Date 11/14/2023

Bill To:
Anderson County Sheriff's Department (TN)
Tennessee
United States

Ship To:
Anderson County Sheriff's Department (TN)
United States

Prepared By Shelley Sorensen
Freight Terms FOB Origin

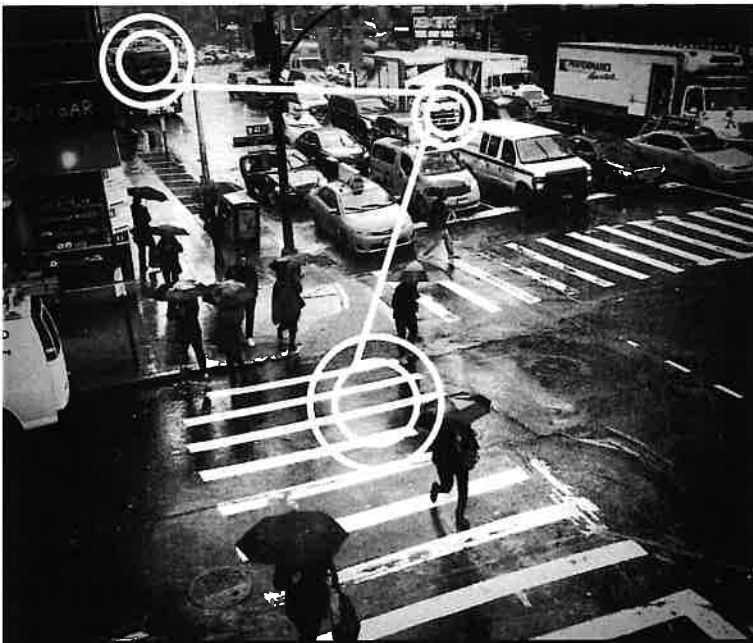
Expiration Date 12/31/2023
Payment Terms Net 30

Quantity	Product	Sales Price	Discount Each	Total Price
1.00	PLX Analysis Suite - 5 Licenses	USD 0.00		USD 0.00
5.00	PLX SOFTWARE LICENSE - PROFESSIONAL EDITION (PHONE)	USD 6,171.00	1,357.62	USD 24,066.90
5.00	PLX SOFTWARE LICENSE - SEARCH WARRANT EDITION (IP) to be combined with PROFESSIONAL or INTERCEPT EDITION (TELEPHONE)	USD 2,598.00	571.56	USD 10,132.20
5.00	ADD-ON: PEN-PROXY FOR PLX SOFTWARE LICENSE - PROFESSIONAL EDITION (TELEPHONE)	USD 626.00	137.72	USD 2,441.40
5.00	ADD-ON: CELL PHONE FORENSICS FOR PLX SOFTWARE LICENSE - PROFESSIONAL EDITION (TELEPHONE)	USD 546.00	120.12	USD 2,129.40
1.00	PLX SOFTWARE MAINTENANCE AND SUPPORT - STANDARD	USD 10,388.35		USD 10,388.35
1.00	PLX WORKGROUP SERVER II	USD 25,311.33	5,568.49	USD 19,742.84
5.00	WINDOWS SERVER DEVICE CAL	USD 36.75		USD 183.75
1.00	Third-Party Shipping	USD 509.90		USD 509.90
1.00	PenLink Academy Training Subscription	USD 4,473.46		USD 4,473.46
1.00	Annual Training Subscription - Free In-Person Seat	USD 0.00		USD 0.00
1.00	Annual Training Subscription - Free In-Person Seat	USD 0.00		USD 0.00
1.00	Annual Training Subscription - Free In-Person Seat	USD 0.00		USD 0.00
1.00	Annual Training Subscription - Free In-Person Seat	USD 0.00		USD 0.00
1.00	Annual Training Subscription - Free In-Person Seat	USD 0.00		USD 0.00

Pen-Link, Ltd is a U.S. - Based Small Business

DUNS: 195956636 / TIN: 47-0707585 / CAGE: 0K6H9

This document contains confidential and proprietary information and is the copyrighted property of Pen-Link, Ltd. Distribution of this document within the receiving agency or company is permitted, but only to such personnel as may be required to meet the goals of the project for which this document was provided. Recipients of this document may not reproduce it, in part or in whole, in any form, or convey its contents to external agencies by any means, without the express written consent of Pen-Link, Ltd. This document may not be distributed, in part or in whole, in any form, to any commercial, non-government entity.



PENLiNK

PenLink PLX Collection Systems Unique Features, Capabilities, and Services

Version 3.0 | July 10, 2019

PenLink, Ltd | 5944 VanDervoort Dr | Lincoln, NE

PenLink, Ltd
Lincoln, NE USA

(402) 421-8857
info@penlink.com
www.penlink.com

PenLink, Ltd. is a
US-Based Small Business

TIN: 47-0707585
DUNS: 195956636
CAGE: 0K6H9



Copyright © 2019, PenLink, Ltd. All rights reserved. This document contains confidential and proprietary information and is the copyrighted intellectual property of PenLink, Ltd. Distribution of this document or copies thereof within the receiving law enforcement agency is permitted only to such agency personnel as may be required to meet the goals of the project or request for which this document was provided. This document may not be distributed, nor its contents disclosed, in part or in whole, in any form or by any means, to a law enforcement agency other than the receiving agency, or to any commercial, non-governmental entity, without the express written consent of PenLink, Ltd. The PenLink logo is the copyrighted intellectual property of PenLink, Ltd. Other company logos that may appear in this document are the copyrighted property of their respective companies.

Contents

1.	Introduction	1
2.	Collection of All Communications in One System	1
2.1	Historical Communications	2
2.2	Cell Phone Forensics	3
2.3	Live Interception of All Modes of Communication	4
2.3.1	Optimized Monitoring Interfaces	5
2.3.2	Unique Minimization and Post Minimization Workflows	6
2.3.3	Compliance with All Intercept Delivery Standards	7
2.3.4	Decoding and Reconstructing Raw IP Protocols	9
2.3.5	Other IP Communication Innovations	10
2.3.6	Pen Registers and Location Pings	10
2.3.7	Other Live Collection Innovations and Unique Features	11
2.4	Real Time Alerts with Unique Proximity Alerts.....	12
2.5	Multiple Layers of Securing Evidence	12
2.6	The Power of Oracle	14
3.	Analysis of All Communications in One System	14
3.1	Unique Interactive Views and Reports	15
3.2	Saved Analysis Sessions and Automated Reporting	16
3.3	Conversation View	17
3.4	Combined View	18
3.5	Deep Search	18
3.6	Automated Deconfliction.....	18
3.7	Regular Expression (Regex) Searches	19
3.8	Gallery View with Automated Hashset Tagging	19
3.9	Presentation Manager	19
3.10	Graphical Analysis	20
4.	Compatibility with Other Systems and Agencies	21
4.1	Widespread Use of PenLink in U. S. Federal Agencies.....	21
4.2	Widespread Use of PenLink in State and Local Agencies	21
4.3	Interfaces to other Federal Agency Intelligence Systems.....	22
4.4	National Surveillance Networks and Access Points	22

4.4.1	CDC Networks	22
4.4.2	LINCOLN Access Points	23
5.	System Administration.....	23
6.	PenPoint Mobile App	24
7.	Unique Aspects of PenLink, Ltd.....	24
7.1	Strategic Positioning with Telecommunications Carriers	25
7.2	Membership in Delivery Standards Committees	25
7.3	OEM Partnerships	26
7.4	Se Habla Español.....	26
7.5	We are an American Company	27

1. Introduction

PenLink, Ltd provides state-of-the-art software and systems for the collection, storage, and analysis of telephonic and internet-based communications. PenLink's software and systems are widely recognized as industry standards, with thousands of users across hundreds of federal, state, and local law enforcement agencies throughout the United States and abroad. PenLink **PLX** is the latest in a long line of PenLink communications collection and analysis products, spanning over 30 years of excellence and innovation in serving the needs of law enforcement.

Named for earlier, separate PenLink products—Pen-Link 8, LINCOLN2, and Xnet—PLX serves *all* of your historical and live communications collection and analysis needs. From traditional circuit-switched telephony like standard land line calls, cellular calls and texts, to packet-based telephony like MMS, VoIP and VoLTE, to traditional internet communications like email and web services, to social media and app-based communications like Blackberry Messenger, Facebook Messenger, WhatsApp, Instagram, Snapchat, and more, PLX helps you collect it, store it, and analyze it. All of it. While there are other companies that produce software and systems for some of these things, PenLink PLX brings all of these modes of communication into one, comprehensive platform, revealing the complete communication landscape of a single individual or an entire criminal organization, helping you to find leads, understand relationships, and collect evidence that may otherwise go unnoticed with other systems.

This document contains an overview of PLX system capabilities and PenLink services, with a focus on unique features and capabilities offered by the system, as well as unique services offered by PenLink, Ltd. For more information, please contact PenLink at (402) 421-8857 or info@penlink.com.



2. Collection of All Communications in One System

PenLink PLX is a comprehensive platform. Whether you're collecting historical communication records through subpoenas or search warrants or conducting live interception of communications, PLX can do it. Whether you're collecting transactional data only, like CDRs or pen register data, or collecting full content, like social media search warrants or live wiretaps, PLX can do it. Whether you're intercepting phone calls, text messages and MMS, or app-based communications, emails, social media activities, or other internet-based communications, PLX can do it.

PLX is a single, integrated, comprehensive platform that serves *all* of your communications collection, analysis, and intelligence needs:

- Phone **and** internet-based communications, including social media and messaging apps



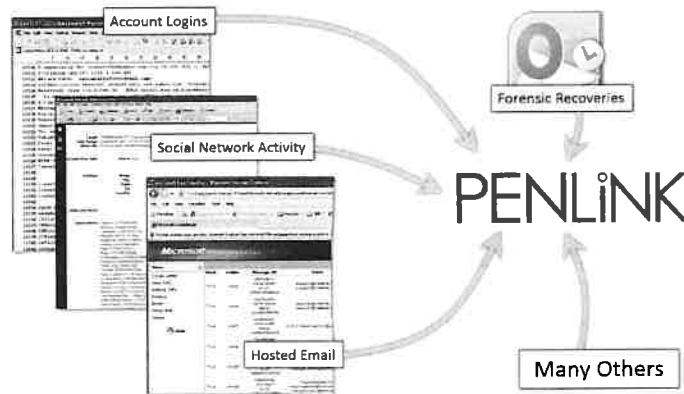
- Data **and** content; pens, pings, and wires
- Historical records **and** live interception

All of your electronic communications intelligence in one comprehensive collection and analysis platform.

2.1 Historical Communications

Investigations involving the collection of communications data and content rarely start with live interception (pen registers, wiretaps). Often times, collection and analysis of *historical* communications precedes live collection, laying the foundation upon which the need for live pen register or wiretap interception is based. Some systems available to law enforcement offer only live collection capabilities, for conducting pen registers and or wiretaps. Other systems focus on collection and analysis of historical data only. PenLink PLX stands apart from other communications collection and analysis systems and software in that it fully supports **both** live interception and collection of historical communications data and content, across the entire spectrum of electronic communications modes available to today's criminals.

Historical communications comprise any data that may be obtained by legal process served under 18 U.S.C. 2703, Required Disclosure of Customer Communications or Records, or through similar state laws. Such communications may include telephone toll records or call details records (CDRs) from telecommunications service providers, search warrant returns from online email service providers, returns from social media service providers, forensic cell phone extractions, and many other sources. Various software offerings available to law enforcement agencies focus on specific types of historical communications data. One system may focus specifically on telephone records while another might focus specifically on data from web-based email services. What sets PenLink PLX apart from these other offerings is that it can handle the full spectrum of available historical communications data, integrating all modes of communication into one platform.



Data files returned to law enforcement vary greatly from provider to provider, in type and formatting. With non-PenLink systems, such files often require significant time and effort by the end user to get the data into the system in a useable form; so much so that investigators sometimes give up trying and just use the data as best they can in its raw form. PLX offers an exclusive, one-step Autoload™ process, capable of automatically loading an extensive data sets; each directly from its native file format, without the need for complicated manual field mapping processes or time consuming exports to intermediary file formats. Simply browse to the source data file, select it, and let PLX do the rest. PLX automatically recognizes the file format, processes the records, parses the data into separate fields, with automatic formatting, and loads it into the appropriate data structures. In other words, the file is Automatically Loaded: hence, "Autoload." Data formats handled by PLX in this manner include:

- Call Detail Records (CDRs)
- Subscriber information
- Internet Protocol Detail Records (IPDRs)
- RTT Location Data for Cell Phones
- PCMD files
- Cell Tower Location Records
- Cell Tower Dumps
- Social Media and Messaging Providers (e.g., Facebook, Twitter, Instagram, WhatsApp, Snapchat, and others)
- Webmail Service Providers (e.g., Gmail, Outlook, Yahoo, Hushmail, and others!)
- Cell phone forensic extractions
- And many more

For the rare instances when you cannot Autoload a file or when you need to load data from another system, PLX offers flexible and easy-to-use interfaces for importing data from original source files.

2.2 Cell Phone Forensics

Today's cell phones bring sophisticated yet easily available communications and other capabilities to criminals and criminal organizations. When seized, however, such cell phones offer a rich variety of intelligence that can enhance and inform various operations and investigations. But for that intelligence to be actionable, you must be able to access it, extract it, store it, and analyze it.

For the greatest impact, you must be able to mingle the extracted intelligence with other communications data collected for the same case(s), to reveal possible cross-target or cross-case links. You must be able to perform these tasks quickly and easily for the intelligence to be useful in quickly evolving situations.

Forensic extraction systems, like the Cellebrite UFED or the MSAB (formerly Micro Systemation) XRY, include their own analytical software for various basic reporting functions. Such software is usually limited in scope to the data provided by the extraction system; sometimes for only one device at a time. But what about all of your other communications intelligence; how can you mix the forensic data with that? Unlike other communications collection systems, PLX can Autoload cell phone forensic data extracted through different forensic platforms, including call records, messaging records, social media activities, app usage data (e.g., WhatsApp messaging), contacts, audio recordings, videos, and photos,



along with photo-embedded EXIF data, including GPS latitudes and longitudes of where photos were taken. Once the database is populated, PLX brings to bear its powerful set of querying, reporting, graphical, and analytical functions, to run against data extracted from one device or multiple devices, along with *all* of the *other* communications intelligence you have collected—phone calls, SMS and MMS messages, social media, emails, messaging apps, etc.—to help you gain a complete understanding of the full communications landscape of your cases.

2.3 Live Interception of All Modes of Communication

PLX systems can collect data and/or content for pen register and wiretap interceptions of a wide variety of telephonic *and* internet-based communications. What sets PLX apart from competing systems in this regard is that it can collect and analyze *all* modes of electronic communication in *one platform*.



With other systems, you will be able to collect telephone-based communications with one software application, but collect internet-based communications with a different software application. Collecting different modes of communication with different systems, into separate databases, makes it exceedingly difficult to analyze all of the gathered intelligence, looking for patterns and relationships across all modes of communication. With all of the modern communication options available to criminals today—particularly those supported by social media and other internet-based services—not being able to analyze intelligence across all modes of communication would represent a serious potential weakness to a law enforcement agency, making it more likely that important patterns, relationships, leads, or evidence could be missed. PLX's live intercept collection capabilities include the ability to collect and analyze, in one platform, live intercepts involving:

- Circuit-switched telephony (e.g., traditional land line and cellular)
- Cellular GSM, UMTS, CDMA, WiMAX, LTE, GPRS, and more
- Packet-based telephony (e.g., VoIP, and cellular VoLTE)
- Google Voice and other app-based telephony over IP
- SMS (text messaging) and MMS (multimedia messaging)
- FAX transmissions
- Email
- Social Media services and apps like WhatsApp, Facebook, Facebook Messenger, Instagram, Snapchat, and others

- Blackberry Messenger (BBM)
- Web-based services, such as webmail from providers like Google (Gmail), Microsoft (Outlook, Hotmail), Yahoo, and others.
- Precision location GPS pings from cellular service providers, including Verizon, Sprint, T-Mobile, and AT&T
- And more

For internet communications, messaging services, and social media, PLX will collect all data and content regardless of whether the target used the service from his or her smart phone, tablet, or computer.

2.3.1 Optimized Monitoring Interfaces

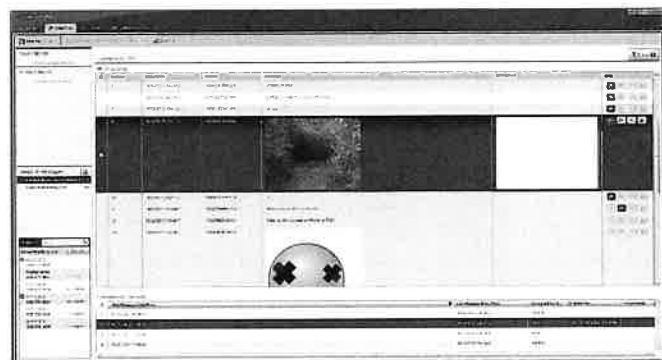
PLX supports U. S. Title III wiretaps, with all required minimization controls and reporting procedures, as well as consensual or FISA/Title 50 wires, for all modes of electronic communications, including (but not limited to) telephonic, internet, and social media communications. Where other systems have one standard monitoring interface, the PLX system offers live monitoring interfaces that are optimized for the mode of communication being intercepted, promoting more efficient workflows and maximizing the effectiveness of monitor personnel. For live monitoring of wires, the PLX Monitor View responds dynamically to the monitor's choice of target, optimizing its display for the type of communications involved.

The PLX Monitor View offers several innovations that are unique to the PLX platform as a group, to make the monitor's work easier and more efficient, including:

- User-programmable hotkey functions (e.g., Play, Play/Pause (toggle), Pause, Stop, Fast Forward, Rewind, Instant Replay, Skip Forward, Increase Speed, Decrease Speed, and more).
- Foot pedal playback, rewind, and fast-forward control
- Playback speed control with automatic pitch correction
- Voice enhancements and noise filters



Monitoring Intercepted Phone Calls



Monitoring Intercepted Social Media Messages

- Audio tagging (momentary and spans) with synopsis hyperlinks
- User-defined report grid layouts
- Rich text synopsis and transcript entry
- Transcribing with Word or WordPerfect, with automatic cover page creation and custom agency macro support
- Automatic saving
- Automatic transfer to a new live session, and subsequent return to previous work
- An integrated voice sample library
- User-defined text replacements (e.g., for creating shortcuts for repetitive text entry)
- And many more features

Professional contract monitors from various services companies, who have used many different intercept platforms, have uniformly praised PenLink PLX for its intuitive monitoring interfaces that allow tagging pertinent audio segments, mapping live call data, viewing messaging conversations inline, viewing live decoded multimedia, and categorizing, transcribing, translating and synopsisizing intercepted communications—all duties of a monitor—without having to navigate away from the monitor view.

2.3.2 Unique Minimization and Post Minimization Workflows

For intercepted phone calls, minimization can be performed manually, in real time, by the system operator who is monitoring the live call (the Monitor). Manual minimization is achieved by the Monitor clicking a button in the Monitoring interface. The button is a toggle, so that clicking the same button subsequent to minimization for an ongoing call restores the audio for continued monitoring and recording. Recording and minimization are synchronized in lock step so that it is not possible for the system to record audio that is not played live, or play live audio that is not being recorded.



For some intercepted communications, real-time minimization is not possible because the content must be reconstructed *after* the communication is received by the system. These include SMS or MMS messaging, FAX transmissions, app-based messaging (e.g., Facebook Messenger, Blackberry Messenger, etc.), email, and other packet-based communications. Such situations call for a robust method of allowing content to be minimized after the fact (commonly called “post minimization”) so that only authorized minimization personnel see non pertinent content, which is kept apart from and inaccessible to non-authorized minimization personnel. For intercepts where content cannot be monitored or minimized in true real time due to the nature of the communications themselves, PLX offers appropriate security roles and unique and customizable workflow procedures to support post-collection minimization while maintaining the integrity of the collected evidence.



2.3.3 Compliance with All Intercept Delivery Standards

Lawfully Authorized Electronic Surveillance (LAES) activities rely heavily on delivery “standards” for the delivery of intercept metadata and content from the service provider to the LEA’s collection system. For a collection system to be effective, therefore, it must comply with any and all delivery standards used by the service providers that operate where the collection system is to be deployed. Such is the case with PenLink PLX collection systems. To our knowledge, PenLink systems are the only systems available that comply with *all* published U.S. and international intercept delivery standards, as well as various non-published, proprietary delivery protocols. PLX systems comply with:

- All standards used for CALEA-based interception in the United States.
- All standards developed by the European Telecommunications Standards Institute (ETSI) to support LAES.
- All standards used to support interception of communications using technologies developed under the 3rd Generation Partnership Project (3GPP).



- All standards developed by the Alliance for Telecommunications Industry Solutions (ATIS) to support LAES. (ATIS is not only an ANSI-accredited standards body, but is also the North American Organizational Partner in the 3GPP.)

PenLink is a **voting member** of ATIS and participates in developing and approving delivery standards used for CALEA-based intercept delivery in the United States. The PLX system is compliant with all

delivery standards used in the United States—including all versions of J-STD-025, T1.678, 102 232, and T1.IAS, as well as many others—to deliver content and metadata for CALEA-based intercept collection, as well as standards widely used outside of the United States. The most widely used standards that PenLink systems support are listed in the following table.

Table 1: Common Intercept Delivery Standards Supported by a PenLink PLX System

Standard	Name and Application
J-STD-025-A J-STD-025-B J-STD-025-B-1 J-STD-025-B-2	Lawfully Authorized Electronic Surveillance (LAES) - For Circuit-switched telecommunications and intercepted IP packet data in wireline and wireless networks
[formerly and now informally T1.678:] ATIS-1000678.2006 ATIS-1000678.a.2007 (supplement A) ATIS-1000678.b.2010 (supplement B) ATIS-1000678.v3.2015 ATIS-1000678.v2.2006(S2018)	Lawfully Authorized Electronic Surveillance for Voiceover Packet Technologies in Wireline Telecommunications Networks - For Voice services over IP; Voice services over MPLS; Voice Services over ATM; VoIP and VoLTE communications.
[formerly and now informally T1.IAS:] ATIS-1000013.2007 ATIS-1000013.a.2009 (supplement A)	Lawfully Authorized Electronic Surveillance (LAES) for Internet Access and Services - For IP communication intercepts (U.S.); e.g., Internet intercepts
ATIS-0700005 ATIS-0700005.a	Lawfully Authorized Electronic Surveillance (LAES) for 3GPP IMS-based VoIP and other Multimedia Services - Reporting interface of Lawfully Authorized Electronic Surveillance for 3GPP IMS-based VoIP, VoLTE, and other multimedia services.
PKT-SP-ESP1.5-I01-050128	PacketCable Electronic Surveillance Specification 1.5 - VoIP in Cable Networks
TIA-1066	Lawfully Authorized Electronic Surveillance - VoIP in Cable Networks
ETSI TS 133.108 3GPP TS 33.108 T1P1 T1.724	Universal Mobile Telecommunications System (UMTS); 3G security; Handover interface for Lawful Interception (LI) - Packet Data in a UMTS network. VoIP and VoLTE communications.
ETSI TS 102 232	Lawful Interception (LI); Handover specifications for IP delivery - IP intercepts both inside and outside of the U.S.
ETSI ES 201 671	Telecommunications security; Lawful Interception (LI); Handover interface for the lawful interception of telecom traffic - intercepts of circuit switched communications
eGISH	Enhanced General Intercept System Handover specification - Delivery of metadata and content during live interception. Used extensively throughout South America and the Caribbean.

2.3.4 Decoding and Reconstructing Raw IP Protocols

It's one thing for a system to be able to collect internet-based communications that are mediated into a published delivery standard, such as those discussed above, but quite another thing for a system to also be able to collect, decode, reassemble, and analyze raw IP packet-based internet communications. Not all systems can do this, but PLX can.

A PLX system is capable of receiving and decoding live data feeds from network probes deployed on a carrier's network or at targeted facilities. For internet-based communications, the system can decode all common, registered and well known IP Application Layer protocols—too numerous to list here—to identify the protocol used for an intercepted communication (e.g., by deep packet inspection, use of standard port numbers, and other identifying characteristics) and to display details of intercepted IP sessions in various analytical reports.



The system performs deep packet inspection on all packet-based content collected and can reassemble and reconstruct intercepted content for a variety of protocols, displaying the content in various monitoring interfaces and analytical reports, including but not limited to those protocols shown in the following table:

Table 2: Protocol Reassembly and Reconstruction Index

BitTorrent	HTTPS	MSN Messenger	TFTP
DNS	ICQ / AOL IM	NNTP	VoIP
eDonkey	IMAP	PGP	Web
FastTrack	IRC	POP3	XMPP
FTP	MIME	SIP	Yahoo Messenger
Gnutella	MMS	SMTP	
HTTP	MSIM	Telnet	

Some of these protocols are used as the underlying communication transport layers by most of today's popular communication apps, like WhatsApp, Skype, SnapChat, Instagram, Voxel, and more. The PLX system also uses a unique reconstruction plugin subsystem whereby reconstruction plugins can be added to the system as the need to reconstruct any particular protocol arises.

2.3.5 Other IP Communication Innovations

PLX systems support a variety of other unique innovations for processing and analyzing captured IP communications, including:

DNS Resolution. The system includes a DNS Resolution service that can perform reverse DNS lookups to identify the domain name for any captured, non-private IP address.

IP2Location Support. The system has the optional ability to integrate data from IP2Location (www.ip2location.com) into the central PLX database. With this information and the corresponding functionality it unlocks, PLX can—with no external network connectivity required—identify the Internet Service Provider (ISP) or Company Name, Domain Name, Country, State or Region, City, Latitude and Longitude, and where applicable (for mobile devices), the Mobile Country Code (MCC), Mobile Network Code (MNC), and Carrier Brand of origin for any captured non-private IP address.

Web Shrinker Support. The system has the optional ability to interface with the Web Shrinker service API from DNSFilter, Inc.

(www.webshrinker.com), to categorize IP Addresses and Domains in analytical reports, enabling the system operator to more efficiently access IP communications that fall into various categories and subcategories of internet-based communication types (e.g., Web Search, Adult Content, Content Server, Email, Chat, Messaging, Streaming Media, Social Networking, Hotels, Air Travel, File Sharing, and many more). This capability requires a Web Shrinker account. Web Shrinker is a third-party service, the costs and licensing details of which are separate from PenLink technologies

ID	Domain Name	Category	Country	IP
1	Domain Name: Facebook.com	70.0%	US	11.07.2018 11:07:2018
2	Domain Name: Bing.com	24.0%	US	11.07.2018 11:07:2018
3	Domain Name: Twitter.com	40.0%	US	11.07.2018 11:07:2018
4	Domain Name: Skype.com	18.0%	US	11.07.2018 11:07:2018
5	Domain Name: LinkedIn.com	14.0%	US	11.07.2018 11:07:2018
6	Domain Name: Instagram.com	12.0%	US	11.07.2018 11:07:2018
7	Domain Name: Yahoo.com	11.0%	US	11.07.2018 11:07:2018
8	Domain Name: Google.com	10.0%	US	11.07.2018 11:07:2018
9	Domain Name: Netflix.com	9.0%	US	11.07.2018 11:07:2018
10	Domain Name: Skype.com	8.0%	US	11.07.2018 11:07:2018

2.3.6 Pen Registers and Location Pings

As with wiretap monitoring interfaces, PLX's other live collection interfaces are optimized for the type of data being collected. Where other systems use the same interface for live wiretap, pen register, and location ping collection, for example, PLX has a specialized live collection interface that is optimized for collection of pen register and location ping data.

The PLX Pen Register View shows collected pen register and location ping data in a convenient grid format, where you can arrange the grid to show any fields in any order, sort by any field or combination of fields, and filter on the fly by any field or set of fields. It's essentially the same as having basic reporting capability built directly into the live collection view. You can even save your own customized views for later use.

A color-coding system in the collection grid makes it easy to tell multiple targets apart with a quick glance. You can easily open any record or set of records from the grid to drill into the details. Flexible mapping support built into the Pen View makes it easy to map one record or a group of records—showing cell sector use, tower frequencies, ping locations, subscriber locations, and more—without leaving the live collection interface. The PLX client can do all of these things while running remotely—from an off-site or in a mobile platform—making PLX an ideal solution to support cell tracking teams.



2.3.7 Other Live Collection Innovations and Unique Features

Some other PLX innovations that improve the capabilities of Collection and Analysis include:

Integrated Voice Samples. Searching for and opening multiple records simultaneously is a common practice among monitors to compare voices while trying to identify a speaker. PLX's integrated Voice Sample Library streamlines the task by being immediately available, with a single button click, during live or playback mode. A monitor can make even more efficient use of time by playing a selected sample to one ear (using headphones) while listening to the live session with the other, to compare voices.

“Collection Box” Function. The PLX system is equipped with a function that can automatically output live collected metadata to file formats that are able to be consumed by Department of Justice units for incorporation into other national databases.

Pass to Collection Box Function. A PLX system is capable of passing live data and content through to another collection system (PenLink or otherwise) over secure network connections. Some law enforcement agencies cannot afford their own network delivery connections from carriers or do not have the technical expertise to maintain them. This capability allows agencies that can and do maintain direct network delivery connections from service providers to assist downstream agencies with live collection for their own pen register and wiretap operations.

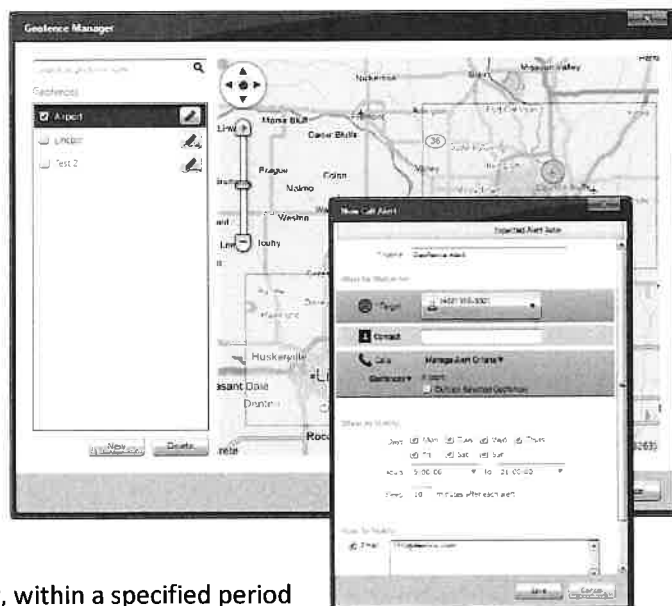
2.4 Real Time Alerts with Unique Proximity Alerts

The PLX System lets you create real time alerts to be sent to recipients in the field, automatically and in near real time. You can configure a wide variety of alert triggers based on events associated with live collection of calls or location pings. Triggers include conditions involving some combination of Target, Contact ID, Call Type (e.g., Voice, Text, MMS, Data, etc.), Direction (Outgoing, Incoming), Location (cell sectors, or user-defined geofences), Call Status (e.g., Serving System message, Call End), and others.

PLX offers a unique alert feature called **Proximity Alerts** that allow you to define an alert trigger based on the distance (defined by you) of one Target from another, within a specified period of time (also defined by you); e.g., trigger an alert when Target A is within 2 miles of Target B, within a 10-minute time frame.

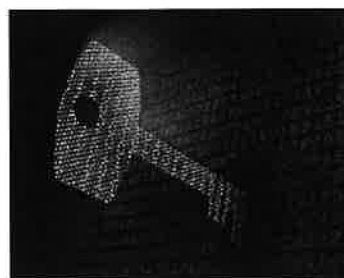
You can limit alerts to be active during certain days of the week and/or a specified time range within each day. You can also configure any alert to “sleep” for a period of time after being triggered, to avoid flooding field operatives with repetitive information.

Alert messages contain details about the call or ping that triggered the alert, including target, phone numbers, date, time, locations, and other information. You may set up multiple separate alerts for different recipients or send the same alert to a group of recipients. Alerts can be delivered “in app” (i.e., within the PLX network) or externally, to field agents or other operatives. External alerts are typically delivered to remote users via outbound email (SMTP), but may also be delivered via an email gateway for SMS (text message) delivery.



2.5 Multiple Layers of Securing Evidence

While some collection systems apply only the basic steps to securing evidence, PLX systems apply multiple layers of security to protect the integrity of your evidence and shield it against claims of tampering made by defense attorneys in criminal court. A PLX Collection Server collects and digitally records—in industry standard formats—all data and evidence delivered through live delivery channels. As live collection takes place, the Notification Service writes evidence files to the designated evidence, working copy, and backup storage paths, securing evidentiary files in several ways.



Digital Signatures. Each evidence file is digitally signed by the system using a secret, private-key certificate issued by an industry-standard certificate authority based in the United States. Each evidence file written to any volume is accompanied by a digital signature file, written to the same location as the evidence file, at the same time. Digital signatures comply with the current Federal Processing Standards Publication (FIPS PUB) 180 series Secure Hash Standard, and are verifiable by an impartial third party.

Cryptographic Hashing. The system uses the 256-bit digest variant (SHA-256) of the SHA-2 cryptographic hash algorithm developed by the NSA as part of the evidence writing subsystem, to facilitate authentication analyses (often desired by prosecutors) to determine if tampering has occurred, and to ensure that evidence written to files is written to storage media correctly. For every evidence file collected, the system calculates a unidirectional cryptographic hash value for that evidence file, using the 256-bit digest variant of the SHA-2 algorithm, and stores the hash value and the evidence file in the database, using the same base filename, containing matching dates and times, for each. Subsequently, the evidence file (e.g., .WAV file) and its corresponding hash file (.SHA2) are written to the SAN. In this manner, every evidence file written to a SAN is accompanied by a corresponding SHA-2 hash file (as well as a corresponding .SIG digital signature file).

Database Hash Storage. When a hash value is calculated for an evidence file, the hash is stored in the central database, along with the corresponding evidence. This provides secure, unalterable storage for hash values should they be needed at a later date to further support an examination of external files for evidence of tampering.

Physical Read/Write Security on Evidence SANs. The root directories to which evidence files and corresponding digital signature and hash files are written and, as a result, all subdirectories thereof, are secured against unauthorized write access by granting write permission only to the Service Account used by the Notification Service (the service that actually writes the files). As a practical matter, this approach means that once a file is written to these paths, it cannot be altered or deleted.

Use of Write-Once BD-R Discs. When evidence (original or backup) is burned to an optical disc, all original evidence files and their corresponding hash files are written to the disc. The Rimage Disc Publisher that is included with some PLX Systems is able to write to many types of optical media. But when burning disks for evidence to seal, for discovery, for working or backup purposes, or for any other purpose involving the removal of files from the system, it is best to burn to Read Only media, such BD-R. Files written to such media may only be written once. This is a property of the media itself, not of the equipment used to write to it or read from it. Once a file is written to such media, it is not possible to delete, edit, or overwrite it.

Evidence Verification. The system also incorporates a unique Evidence Verification Tool that, for any Target, will (a) verify that all files that are supposed to be present in the evidence path, working copy path, or externally produced volume (e.g., BD-R) are, in fact, present, and (b) identify any file that is not expected to be in the evidence or working copy path or on an externally produced volume.



2.6 The Power of Oracle

To our knowledge, PLX is the only intercept collection system available that is based on Oracle, bringing the capabilities of one of the world's most powerful database systems to bear. There is no limit to the number of cases, targets, and records the system can handle, and the upper limit for physical storage is imposed not by the software, but by what your physical hosts (e.g., SANs) can store.



To make things even better, the PLX Oracle database is an embedded instance of Oracle. What does this mean? Some agencies are reluctant to take on what they think of as challenges associated with managing an instance of Oracle as opposed to, say, the simpler database systems used by PenLink's competitors. But because PLX's database is an embedded instance of Oracle 12c Enterprise, there is very little database management and maintenance required; all of the database management and administration functions are automated by automated internal jobs and processes. Hence, you get the power of Oracle, without the management and administration overhead required even for a Microsoft SQL Server or MySQL installation.

Because the PLX database is an Oracle database, PLX systems also offer various native Oracle options to support high availability and disaster recovery.

Built-in Backups. PLX incorporates a native Oracle backup system capable of running in both an online and offline state and providing incremental and/or full backups on an administratively defined schedule. You can, for example, schedule the system to take daily incremental backups while spacing full backups over a longer timeframe, resulting in minimal impact to system performance.

Warm Failover Functionality. Oracle Data Guard is a native data protection and data availability solution for Oracle databases and provides the management, monitoring, and automation software to create and maintain one or more synchronized standby databases that protect data from failures, disasters, errors, and corruptions; supporting both synchronous and asynchronous configurations. Further, there are no restrictions on where the databases (primary and standby(s)) reside, provided they can communicate with each other over a network, making Oracle Data Guard an excellent, native Oracle option not only for High Data Availability but also for offsite Disaster Recovery. The PLX Database includes an Enterprise License of Oracle, which enables the use of Oracle Data Guard, at the customer's option, for no additional cost.

3. Analysis of All Communications in One System

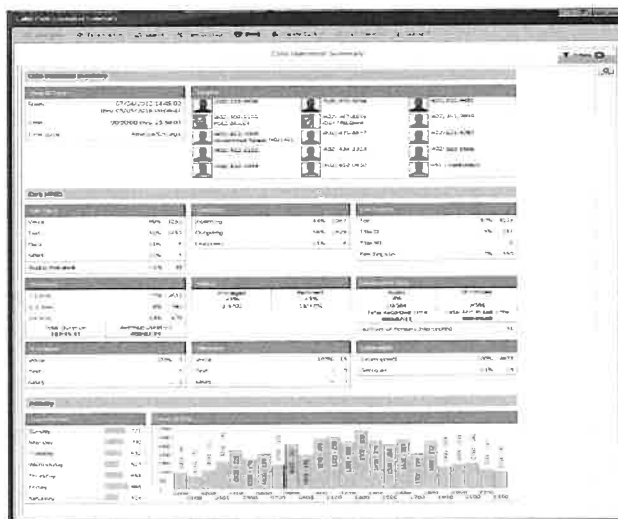
Once collected into PLX, all data and content reside in a single, unified database, easing the analytical tasks of mixing communications channels to gain a greater understanding of the full communications spectrum of the individuals or organization under investigation. PLX incorporates a powerful yet easy-to-use suite of reporting and analysis tools to help you drill down into the volumes of data you collect, helping you to gain insights and to reveal connections, trends, and relationships that might otherwise go undetected. You can run analyses on calls, emails, messages (e.g., WhatsApp, Facebook, Instagram, BBM, etc), account logins, locations, IP sessions, internet content, and subscribers, querying the database using any available field, alone or in combination with any other available field(s), and group (e.g., for statistical tabulation), filter, display, and sort the resulting record sets based on any available

field or combination of fields. PenLink PLX offers several unique and innovative analytical functions not found in other systems, some of which are discussed in the following sections.

3.1 Unique Interactive Views and Reports

PLX's analytical Interactive View lets the intelligence analyst change quick filters, advanced filters, frequency groupings, field order, sort order, commonality filter, second-level filter, or other properties of the view any number of times within a record set without having to re-query the database. PLX also has a set of predefined reports that are designed to help conduct particular analyses quickly and easily. Some of these reports are, to our knowledge, unique in the industry.

Common Contact IDs across Targets automatically identifies Contact IDs (phone numbers, email addresses, Facebook ID, etc.) that have been in communication with multiple Targets, which can help identify additional potential Targets in a criminal organization.



Common Contact IDs across Cases automatically identifies Contact IDs that appear under more than one Case, helping to identify cross-case conspiracies.

Common Received Targets across Labels can automatically identify any commonality across any property of a record that you choose. It is useful, for example, in automatically searching through cell tower dump records (sometimes millions per case) to automatically identify common Contact IDs that were in the vicinity of multiple crime scenes (e.g. robberies, assaults, bombings, serial shootings, etc.), around the times the crimes took place.

Target to Target Frequency automatically identifies instances of Targets communicating with one another and shows which such communications are most active, helping to determine the relative importance of Targets in a criminal organization.

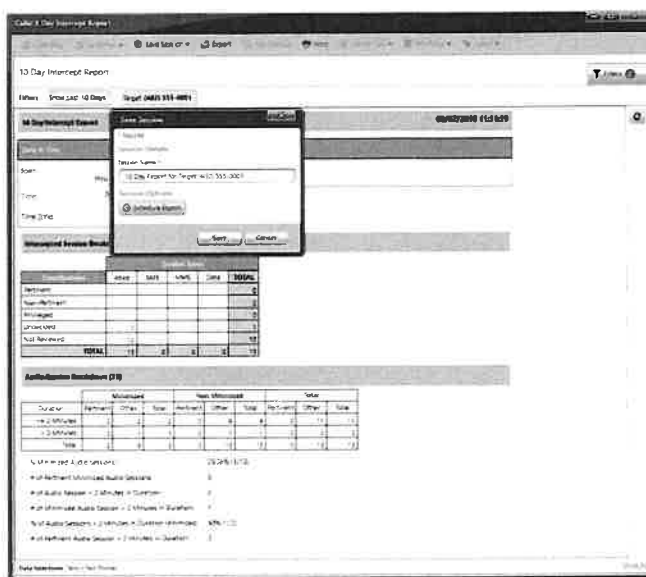
Summary Differences automatically shows Contact IDs that appear during one user-specified date/time range but not another, which can be useful, for example, in determining what the new Target device or account is after a suspect "drops" (stops using) his phone or online account and switches to another.

The **Subpoena Report** automatically determines which Contact IDs do not have any associated subscriber data within the system and can assist in preparing subpoenas for subscriber records. The report can also submit batches of Contact IDs to various third-party data providers—like Clear, Lexis Nexis, TransUnion, Whooster, iconectiv, and others—for subscriber lookup, current provider, and porting history, and load the returned results into the database for automatic association with the corresponding Contact IDs.

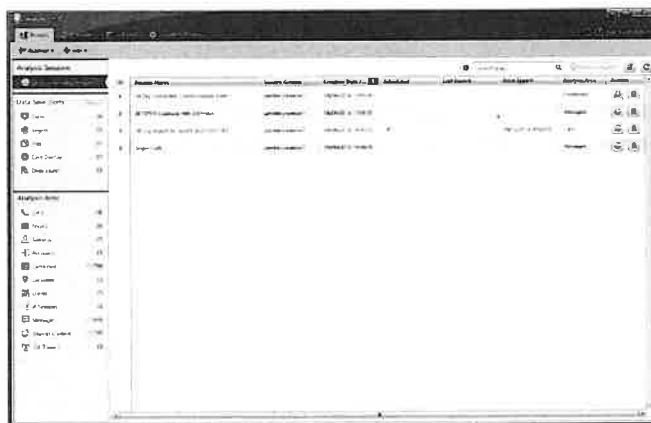
And there are many more. When you have a new Interactive View or Report that you particularly like, you can save the customizations under a new name, for future use with the same case or with other cases. You can keep the new View or Report private or share it with other users who may find it useful.

3.2 Saved Analysis Sessions and Automated Reporting

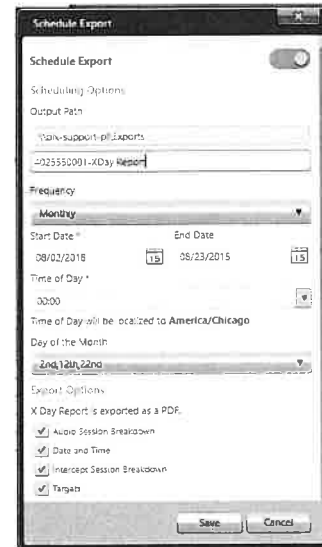
PLX includes the unique ability to automate various analyses, including user-defined custom reports, by saving Analysis Sessions for future use and, optionally, scheduling them to be generated and output automatically. An analysis session is essentially an interactive grid analysis or a report that is saved by the user and includes any case(s), target(s), or original file(s) selection, along with any advanced filters or quick filters that were used to generate the data set displayed by the interactive grid or report. This functionality allows a user to save custom analysis sessions for future retrieval and use, without having to select case(s), target(s), monitor ID, workflow status, etc. each time, and is particularly useful when used with “sliding” date and time filters (e.g., Last x Hours, Last x Days, Last x Weeks, or Last x Months). The example shown here is an “X Day Intercept Report”—with filters set to generate the report for Target (402) 555-0001, over a date range of the Last 10 Days—being saved as an Analysis Session named “10 Day Report for Target (402) 555-0001.” When a user opens this saved Analysis Session at a later date, it will automatically re-generate the report for the same Target, over the most recent 10 days.



Automated Scheduled Output from Saved Analysis Sessions. Just as with any manually run analytical View or Report, a saved Analysis Session can access any and all data stored in the system, subject to the permissions of the user who save the Analysis Session. If the user has the additional permission to automate Analysis Sessions, he or she may also schedule saved Analysis Sessions to run automatically, with the results automatically exported, at future, repeating intervals, supporting the automatic movement of intercept data out of the system for use by external processes or review by other personnel. Scheduling can be activated, and the schedule defined, when the Analysis Session is initially saved or *after*, by selecting the session from the Saved/Scheduled Sessions list (shown below). When scheduling an Analysis Session to run automatically, the user can:



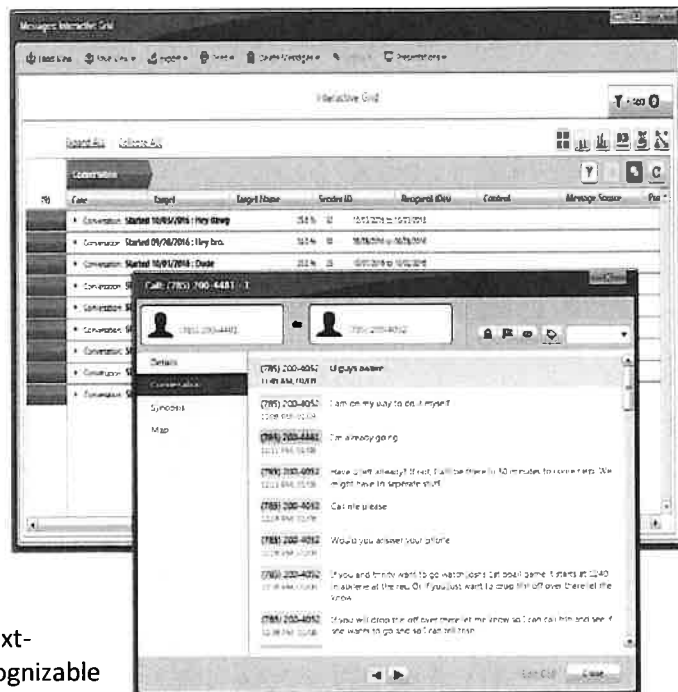
- Enable the Schedule Export option (turn it on).
- Specify an optional subfolder under the primary Output Path (which is administratively configured) to hold the scheduled output.
- Specify the frequency of the output schedule (Daily, Weekly, or Monthly). The remaining scheduling options in the dialog will vary according to the Frequency selection. The example here shows the scheduling options for the Monthly selection.
- Set other scheduling option pertinent to the Frequency setting, including Time of Day (localized), Day of Week (for Weekly frequency; Monday, Tuesday, etc.), and Day of Month (for Monthly frequency; 1st, 2nd, 3rd, etc.).
- Set other output options that can vary according to the expected type of report result, such as those shown in the example here for X Day Intercept Report output.



Once enabled, each Scheduled Export will run on its defined schedule and output to the designated Output Path and (if set) sub folder. Output will be contained in a .zip file with a base file name starting with the date and time that the export took place and ending with the name of the saved Analysis Session.

3.3 Conversation View

Message-based communications—texts, emails, BBM, social media messaging, etc.—are intercepted one message at a time, but the *real* value of messaging content is in understanding any given message in the context of the larger thread or conversation to which it belongs. The PLX Conversation View lets you open any single message and, with one click, view that message in the context of its full conversation, including *all* messages in the same thread, both before and after the selected message, including any captured multimedia. Rather than spending valuable time querying, sorting, and filtering records, you can **instantly** extract a full conversation from all of the other collected messages in any data set, and view it in a text-message-like listing that is immediately recognizable to anyone who has ever text messaged.



Conversation views can also be exported to easily readable PDF files for printing or viewing by other personnel, or for use as exhibits for prosecution.

3.4 Combined View

Based on its unified database, and because it contains all collected data and content, from all modes of electronic communication, PLX offers a Combined View as part of its analytical tools. This view merges the collected records from multiple modes of communication into one integrated view, allowing you to access the entire set of communications for any target or set of targets—regardless of whether they were phone calls, social media messages, emails, etc.—and providing tools like Timeline Analysis and a Conversation View. Simply put, the Combined View puts all of your case’s communications, regardless of type, in one analytical interface.

3.5 Deep Search

Have you ever wanted to query across **all** cases and targets to see if a Contact ID (e.g., phone number, email, BBM PIN) exists in the database? The PLX Deep Search function does exactly that. Input the search value into one field, click a button, and PLX searches millions of records through the entire enterprise-wide database and, within seconds, returns a listing of all cases containing that contact ID. What if you want to look for more than one contact at a time? Use the **Batch Deep Search** function!

3.6 Automated Deconfliction

PLX provides automatic deconfliction for contact IDs (e.g., phone numbers, email addresses, BlackBerry Messenger IDs, etc.) that are loaded into the system by any user. The analysis is performed by the system automatically for each new data set loaded (historical or live), with alerts automatically emailed to case agents for cases that contain the same contact IDs. As your data grows you can see where investigations overlap with one another without any extra work. For the contact IDs of interest, the Case Overlap analysis also identifies whether the contact ID came from subscriber or call records, indicates if the number was a target or not, gives the date ranges for the cross-case involvements, and shows the owners of the involved cases (e.g., case agents’ names) to facilitate communications among multiple case agents. This is an especially valuable tool for deconfliction across multiple agencies (e.g., task forces or otherwise) that may have personnel (perhaps even undercover) working on overlapping investigations.

3.7 Regular Expression (Regex) Searches

PLX reports allow you to run queries of text-based content (e.g., text messages, social media content, instant messenger messages) using regular expressions. Regular expressions are a powerful way to formulate queries to look for matches to defined patterns in your data. For example, the following regex

```
\(?:[2-9][0-9]{2}\)?[-.]+[2-9][0-9]{2}[-.]+[0-9]{4}
```

will match phone numbers in the North American Numbering Plan, with or without parentheses around the area code and using a space, dash, or dot as a delimiter, or no delimiter at all. A phone number appearing in social media (or other) messaging content as 4024218857, 402-421-8857, 402 421 8857, 402.421.8857, (402) 421-8857, (402)421-8857, 402 421-8857, and various other combinations would all match the regex query. Such a search in PLX would locate phone numbers inside of tens of thousands of messaging records in just a few seconds, providing possible leads that might otherwise take days to find.

3.8 Gallery View with Automated Hashset Tagging

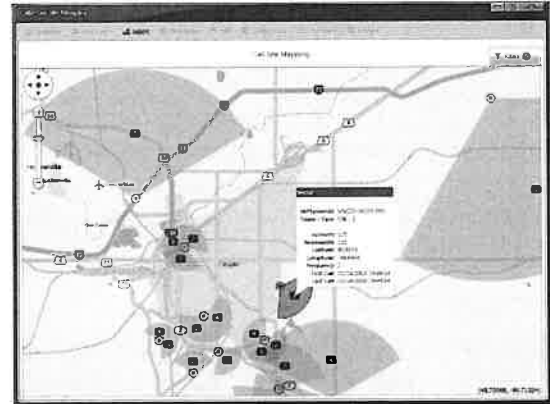
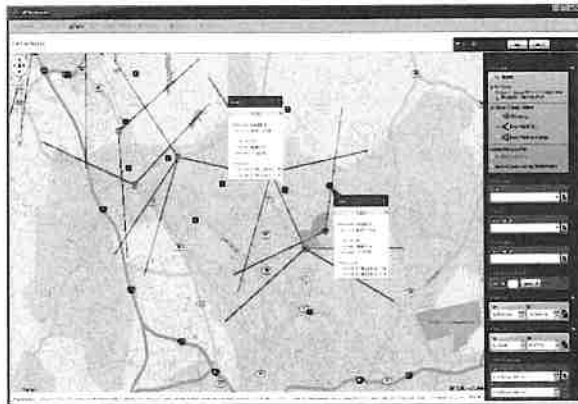
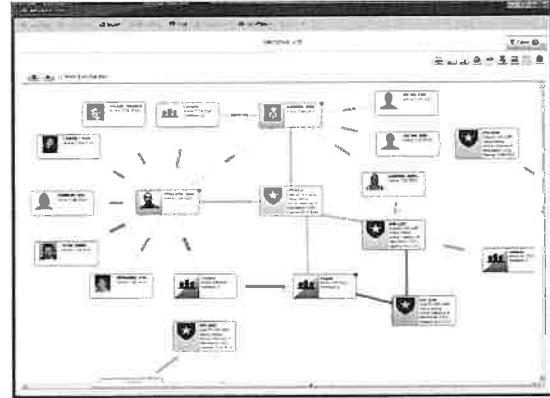
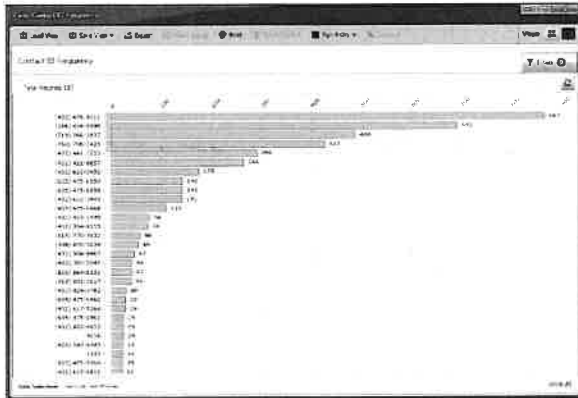
PLX offers a unique Gallery View function for multimedia collected through social media and messaging service search warrants and live intercepts. This function presents a thumbnail gallery of images, for example, contained within a set of collected messages that match the database query. The system can apply hashsets—such as those available from the National Center for Missing and Exploited Children (NCMEC) through Project Vic—to automatically identify and tag multimedia images containing known illegal content, such as child pornography. This feature is a tremendous time saver for monitors and analysts that must go through hundreds, sometimes thousands, of images to identify those pertinent to a case. In addition, PLX users can flag new images as containing illegal content, to generate new hashsets that can be exported from the system and shared with other users and agencies.

3.9 Presentation Manager

PLX includes a unique Presentation Manager function that lets you select records of reconstructed content (e.g., social media messaging) and output them to an autonomous presentation for viewing outside of the PLX system. The output is based on industry-standard html hypertext with linked multimedia included in subfolders of the directory containing the index file. With this approach, the entire presentation is viewable using any standard web browser. The entire output of a presentation may be packaged as a single industry-standard .zip file so that is easily transportable or transferable to other personnel outside of the PLX system. The ability to generate and manage presentations is useful for preparing case summaries (e.g., for a supervisor or investigative team) or creating courtroom presentations to support prosecutions.

3.10 Graphical Analysis

While some systems may offer graphical analysis functions as add-on features or through third-party products, PLX comes equipped with wide variety of integrated graphical analysis features, including Frequency Charts, Link Charts, and Maps.



PLX's mapping functions lets you plot things like cell sector use, cell tower frequencies, location pings, IP addresses (e.g., from app-based messaging, account logins, etc.), case event locations, custom "places" (as user-added pushpins; e.g., crime scenes, stash houses, etc.), and subscriber addresses; from historical data or live intercepts. Mapping functions are available from the live Collection interface and from the Analysis interface. The system includes its own built-in, world-wide GIS layers (so you don't have to rely on internet connectivity), and can also map to external platforms like Map Point, Google Earth, ESRI ArcGIS Earth, and other .kml/.kmz mapping systems.

4. Compatibility with Other Systems and Agencies

For some agencies, particularly those working in multi-agency task forces, a high level of compatibility with communications collection and analysis systems used by other law enforcement agencies can be an important factor in determining what system to purchase. PenLink systems are widely used, by hundreds of agencies at all levels of law enforcement, and also incorporate various customized interfaces for many federal agencies. PenLink systems therefore offer an exceptionally high degree of compatibility and interoperability across multiple local, state, and federal law enforcement agencies.

4.1 Widespread Use of PenLink in U. S. Federal Agencies

Many U. S. federal law enforcement agencies use PenLink systems, including (but not limited to) the Drug Enforcement Administration (DEA), Federal Bureau of Investigation (FBI), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), Marshals Service (USMS), Secret Service (USSS), ICE Homeland Security Investigations (HSI) and Customs and Border Protection (CBP), United States Postal Inspection Service (USPIS). Some agencies, such as DEA and HSI, use PenLink systems for live intercept collection in various domestic divisions as well as internationally, while others—including USMS, USSS, and ATF—use PenLink systems for live collection on a national scale. For many of these agencies (we do not feel at liberty to name them), PenLink PLX systems also serve a nationwide user base as a primary communications intelligence warehouse and analysis system, whereby all of the historical communications data and all of the data collected from live intercepts (even if collected by a competing vendor's system) ultimately ends up in a PLX system for storage, analysis, and various other uses in support of national security.

4.2 Widespread Use of PenLink in State and Local Agencies

PenLink systems are also widely used by state and local investigative agencies and task forces. Below, we provide a small sampling of these.

- **Multi-Agency Task Forces.** Pen-Link Systems have been used by a variety of large, multi-agency task forces for many years, such as the Los Angeles HIDTA, LA CLEAR, the Central Valley HIDTA, the North Central HIDTA, the Middle Tennessee Drug Task Force, and the Inland Regional Narcotics Enforcement Team (IRNET). PenLink software is also used by various RISS network agencies.
- **State-Wide Collection Systems.** Several state agencies in the U. S.—including the Florida Department of Law Enforcement (FDLE), Pennsylvania State Police (PSP), California Department of Justice (CAL DOJ), Oregon DOJ, Ohio Bureau of Criminal Investigation (BCI), Tennessee Bureau of Investigation (TBI) and, of course, the Nebraska State Patrol, just to name just a few—use Pen-Link Collection Systems to support lawfully authorized communications intercept operations throughout their states.
- **County Agencies.** Many Sheriff's Departments throughout the United States use Pen-Link Collection Systems. Gwinnett County (GA), for example, has used Pen-Link Collection Systems in their intercept program for 15 years. The Orange County (CA) Sheriff's Department switched to

Pen-Link from a different vendor's system nearly six years ago. The San Bernardino Sheriff's Department (SBSD) has the largest State and Local Law Enforcement CALEA Intercept Collection System (a Pen-Link system) on the west coast and has been a PenLink customer since 2002. They support many other agencies, both in-state and across the country, who do Title III, Pen Register, and GPS Location Ping collection through the Sheriff's office and IRNET.

- **City Agencies.** Police Departments and other city agencies of all sizes throughout the United States use PenLink systems, including (but not limited to) Chicago PD, Houston PD, New York Department of Investigation (DOI), Los Angeles Police Department, Las Vegas Metro PD, Jacksonville (FL) Sheriff (a joint city/county agency), and our own local Omaha Police Department and Lincoln Police Department.

There are many other such agencies and task forces that use PenLink technologies; names are available upon request.

4.3 Interfaces to other Federal Agency Intelligence Systems

PenLink systems incorporate various customized interfaces to several other intelligence systems operated by different U. S. federal agencies. We are not at liberty to divulge details in this document about such systems, but can say that these customized interfaces are specifically designed to support the exchange of data between PenLink systems and these various other systems operated by U. S. federal law enforcement agencies with which state and local task force officers are likely to work, facilitating compatibility and interoperability across multiple agencies.

4.4 National Surveillance Networks and Access Points

PenLink systems offer unique features and capabilities that support the formation of secure national networks for real-time distribution of electronic surveillance data, both within and agency and between cooperating agencies.

4.4.1 CDC Networks

The LINCOLN Collection Service components of PenLink systems (LINCOLN stands for Local Intercept Network Collection)—which are the functional components responsible for directly receiving real-time intercept data delivered by service providers over network connections from those providers—are able to communicate in real time with one another over secure wide area network (WAN) connections. Various U. S. federal law enforcement agencies—including DEA, HSI, and ATF—use this capability to form National CDC (Call Data Channel) Networks for the distribution of live CDC messaging (e.g., passing of mediated data) over secure national networks. Data is received over secure network channels from service providers, into an aggregation point maintained by the agency, then transferred automatically to the agency's private, secure National CDC Network for real-time delivery to divisions and systems throughout the United States, including to non-PenLink collection systems. It is PenLink technologies that make such National CDC Networks possible, even when they include non-PenLink systems.

4.4.2 LINCOLN Access Points

The PenLink technology that supports the creation of National CDC Networks also allows agencies—federal and otherwise—to offer LINCOLN Access Points (LAPs for short) that support delivery of real-time electronic surveillance data and content over VPN network connections, to agencies who do not have their own surveillance network connections to service providers. LAPs support sharing not only of data channels, but also content channels, such as digital PRI/T1 channels for the reception of live audio content. In this manner, larger agencies are able to leverage their network connections and IT resources to support lawfully authorized electronic surveillance (pen registers and/or wiretaps) by smaller agencies and task forces who have PLX software but may not otherwise have the IT resources to use this valuable investigative technique. To our knowledge, this capability is unique to PenLink technologies.

One of the largest and most active LAP providers in the United States happens to be right in our hometown of Lincoln, NE: the Nebraska State Patrol (NSP). This LAP serves state and local law enforcement agencies throughout the United States, as well as some federal agencies. In 2018, this LAP supported over 1,000 communications intercepts (pen registers or wiretaps) and has supported over 375 so far in 2019. An agency supported by a LAP might receive *all* of its lawfully authorized electronic surveillance data and content through the LAP or, at their discretion, just *some* of it. One of the advantages of having access to a LAP—which we could help any of our customers do through the NSP—is that it provides quick access to smaller carriers who may become subject to a surveillance order. In other words, some of the agencies supported by a LAP maintain their own network delivery connections to the large service providers, but when they need to do surveillance on a target who subscribes to a smaller service, like nTelos, or connect to Bandwidth Inc. (an API platform provider) to intercept incoming Google Voice calls, then they might do so through a LAP connection like the NSP's, which already has network connections to these providers.

5. System Administration

There are several unique innovations in a PLX system that are designed specifically to improve the ease and efficiency of system administration, including:

Admin Anywhere. Because most of the major system functions are Windows Service based (e.g., Collection Service, Streaming Service, etc.), PLX administrative tasks can be performed at any time, from any workstation, by any system administrator, over any connection to the system's network, without the need for remote desktop applications (e.g., RDP, NetOp, etc.), simply by running the PLX client.

Dynamic dialogs. Dynamic dialogs are a modern and more efficient alternative to the "Wizard" approach to configuring complex settings. As an administrator enters information and sets options, the dialog responds by changing its input fields and controls to adjust contextually to the input already provided, highlighting the next required settings and eliminating those that no longer apply. According to one system administrator who is already using PLX in the T2S2 fleet, "This new kind of dialog makes administration a one-man job."

Intercept Summary Report. The PLX system includes an Intercept Summary report function that will output a summary, for any user-provided date range, of all intercepts—pen and wire—conducted with the system over the specified date range. The output is suitable for annual statistical reporting of

intercept activities required of all Department of Justice agencies each year and helps save significant time in preparing such reports.

System Management Report. The PLX system offers a function that will output a summary of intercept monitoring activities (e.g., calls monitored, calls listened to, calls synopsis) by hour of day and day of week, by any user or set of users within the system over a user-defined date range. This output is especially useful in reporting on and allocating human resources for monitoring duties.

6. PenPoint Mobile App

To our knowledge, PenLink is the only intercept collection system vendor that offers a mobile app as part of its suite of software. PenPoint is a mobile app for iOS and Android devices, allowing agents or other operatives in the field to receive location-based electronic surveillance intelligence in near real time, and perform queries and various analyses for data already gathered by the PLX system, all from the mobile convenience of a smart phone or tablet.



PenPoint is a valuable tool to field agents, providing them with convenient, real-time access to call detail information and maps of target locations, in an easy-to-use, intuitive mobile user interface. With numerous filtering and display options, intuitive navigation between mapped data points, and live push notifications on the arrival of new data points, PenPoint effectively transforms a phone or tablet into a mobile record retrieval and location tracking device to view Call Details, map precision location pings and cell sector usage, include satellite imagery, view heat maps of activity, browse location histories, and analyze location frequencies.

7. Unique Aspects of PenLink, Ltd

PenLink has been in business—the same business—since 1986. During these 30+ years, while some of our competitors have delved into other arenas of business (e.g., call centers, encrypted radio systems, video processing), we have maintained a tightly focused area of expertise; we do one thing, and we do it well. We develop state-of-the-art systems and software used by Law Enforcement and Intelligence Agencies for communications interception and analysis, including historical and live telecommunications

and internet-based communications. We have committed our extensive experience and expertise to continuing to support the missions of Law Enforcement and Intelligence Agencies with the technologies and services they need to protect and serve our society.

During our more than three decades of serving the communications collection and analysis needs of Law Enforcement, we have developed various unique aspects to our company that we feel sets us apart from our competitors in ways that directly benefit our customers.

7.1 Strategic Positioning with Telecommunications Carriers

As part of our normal business practice, we maintain parallel strategic initiatives to address interception and collection from the delivery side as well. We are proactive with telecommunication service providers and their switch vendor solutions, providing systems and services that carriers incorporate into their CALEA test labs. Our technology has regularly been selected by service providers and switch manufactures as a solution to test their latest CALEA delivery features, prior to implementing them in their networks.



We have sold and delivered over 60 Test Systems to both switch manufacturers and telecommunication service providers affected by CALEA. Testing CALEA delivery with a collection system that is widely used by law enforcement validates a carrier's CALEA mediation and delivery solutions to ensure that they will work with law enforcement collection systems and standards and meet the requirements of CALEA. We have developed such a good reputation among these groups that they often seek our advice on the development of their delivery systems and invite us to participate in interoperability "plug tests" and First Office Application (FOA) demonstrations of delivery solutions for law enforcement, both domestically and internationally. The service providers and switch manufacturers using their own PenLink Systems to test their delivery and network solutions include (but are not limited to) AT&T Mobility, AT&T Network Security, AT&T Labs, AT&T Production, AT&T Government Solutions, Charter Communications, Comcast Cable Communications, Qwest, Sprint Systems Labs, Sprint Systems Production, Sprint Fraud Management, Verizon Security Assistance Team, Verizon Wireless, Verizon VZT Outside Plant, T-Mobile, Subsentio ("Trusted Third-Party" provider), Motorola, Siemens, and many others.

7.2 Membership in Delivery Standards Committees

Much of the work that goes into developing and maintaining a CALEA-compliant collection system involves making sure that it can correctly collect what CALEA-compliant delivery systems output. CALEA delivery systems used by service providers normally implement one or more "standards" of communication that define how the data will be packaged for delivery from the carrier. These Delivery Standards are developed and published by various Standards Committees that make recommendations to the telecommunications industry and to the FCC. Most of the companies that manufacture switches, routing equipment, and other communications gear for intercept delivery using these standards have representatives on these Standards Committees. Some



collection system vendors do not have members on these committees, but we do. Two of our employees are current members of various committees or subcommittees, including the Packet Technologies and Systems Committee (PTSC), Lawfully Authorized Electronic Surveillance (LAES) subcommittee, of the Alliance for Telecommunications Industry Standards (ATIS). PenLink is a voting member of ATIS, representing our and our customers' interests in the acceptance (or not) of new or changing ATIS recommendations affecting delivery standards and other areas of interest to the telecommunications industry. Having our own personnel on such committees means that, among other things, we help to develop and approve CALEA-compliant delivery standards in the U. S. In so doing, we also gain valuable insights into those standards, which help us to gain a unique perspective when designing functionality to collect CALEA-compliant surveillance information; a perspective that some of our competitors do not have.

7.3 OEM Partnerships

While some companies merely purchase and resell computer hardware, or have the customer purchase their own hardware for a system from a separate supplier, PenLink provides turnkey systems, including all hardware and software. We do not, however, simply purchase then resell hardware. PenLink is an Original Equipment Manufacturer (OEM) partner with Dell and an Authorized Reseller of Dell equipment and that of many other major technology manufacturers. These partnerships and business relationships provide value to our customers by ensuring direct product supply chains, delivery priority, and top tier equipment support directly from the manufacturer.

We provide Dell hardware platforms as part of a turnkey solution for PenLink systems. As an OEM Partner of Dell, we are also in a key position to provide real-world experience and expertise when it comes to solutions hosted on Dell platforms. In addition to maintaining a product testbed hosted entirely on Dell platforms, including the same baseline hardware models provided to our customers (such as Dell OptiPlex, Dell PowerEdge, Dell VRTX, Dell PowerConnect, and Dell EqualLogic and Compellent), we also run all company production operations on these same Dell platforms. This allows our support and engineering staffs to accrue extensive hands-on, real-world configuration, support, and service experience with Dell equipment.

7.4 Se Habla Español

Many of our collection system customers conduct wiretap collection cases in which the targets and their associates speak in foreign languages. For this reason, such customers often employ linguists or native speakers to monitor and/or transcribe the intercepted conversations. By far, the most common foreign language encountered by our customers during their wiretap collections is Spanish; both spoken (e.g., phone intercepts) and written (e.g., social media intercepts). For this reason, linguists employed as wiretap monitors are often native Spanish speakers. Some of these PenLink users are more comfortable speaking or corresponding with PenLink personnel in Spanish when they require technical support or training, or simply have questions about the system. Several PenLink employees—including support technicians, trainers, and engineers—are fluent in Spanish, both spoken and written, with native expertise in multiple dialects. The PenLink PLX User Interface can even be switched from English to Spanish!

7.5 We are an American Company

PenLink, Ltd. is a U.S.-based small business. We maintain three office in the United States: our corporate headquarters in Lincoln, NE, our DC Area Office in the Washington, DC area, and our Innovation Office in Boulder, CO. Our main competitors in the arena of communications intercept collection systems are foreign companies. While these companies have subsidiaries that operate in the United States, they are headquartered in other countries (e.g., Canada and Israel).



Given the sensitive nature of the work conducted with our systems by U.S. law enforcement agencies, we feel that it is important to point out that we are a wholly-owned U. S. company. PenLink, Ltd was founded in and remains based in Lincoln, Nebraska. We are not a U. S. subsidiary of a foreign-owned company; we have no foreign ownership or foreign controlling interest. Our company is owned by its employees, all of whom are United States Citizens.

We feel that it is important to mention these things for a few reasons. First, as proud Americans, we take our commitment to supporting the missions of U.S. Law Enforcement and Intelligence Agencies very seriously. This commitment is reflected in our dedication to quality in both our technology and in the support and services we provide to our users. Your successes are our successes. Second, we believe strongly that U. S. funds are best kept in the U. S. economy whenever possible, particularly in the difficult economic times we now face as a nation. And finally, a PenLink system offers zero exposure to foreign entities through the vendor. Nobody from a foreign company, nobody with interests in a foreign company, nobody with possible ties to foreign intelligence or security services will ever come close to accessing your system through PenLink, Ltd or its technologies.