



(U) Transnational DNI Training

(U) PINWALE





(U) Describe PINWALE

(U) What is PINWALE?





(U) PINWALE

- (C) Supports SIGINT production by providing storage and retrieval of intercept
- (TS//SI) Special partition for FBI FISA data
- (C) As a repository, it accounts for a significant portion of SIGINT production
- (C//SI) Archives documents for approx. 5 years from the data of collection
- (S//SI) Several search engines that provide retroactive, interactive, and dissemination type searches



(U) PINWALE Search Engines

- (S//SI) **LIONROAR** searches documents beyond 13 months and up to a 5-year range of the archive
- (S//SI) **LIONHEART Fusion** searches a document index of the most recent 13 months in the archive
- (S//SI) **PINWALE Dissemination** searches documents daily based on a query



Creating a Query

- For a refresher on query syntax, use the PINWALE Syntax Quick Reference Card (<http://rosato.do.nsa:9087/userweb/nexus/ref.card.030505.doc>) or the course guide for TOOL 2201
- For additional help creating queries, contact PINWALE Help Desk [REDACTED]



(U) UIS, NEXUS, AGILITY and AGILEVIEW

- **(C) NEXUS** is interface where you can conduct searches in UIS
- **(C//SI) User Interface Service (UIS)** integrates search and retrieval systems and presents data queried through NEXUS like the intended user would see (UIS Text Presenter).
- **(S//SI) AGILITY** is an alternative document viewer to the UIS Text Presenter ideal for viewing Microsoft Windows applications (MS Office, Adobe PDFs) in their native format



(U) PINWALE ID (PWID)

(S//SI) example: PWYA2006298115456 0001151730

(S//SI) PWID Dissected: PW YA 2006 298 115456 0001151730

(S//SI)

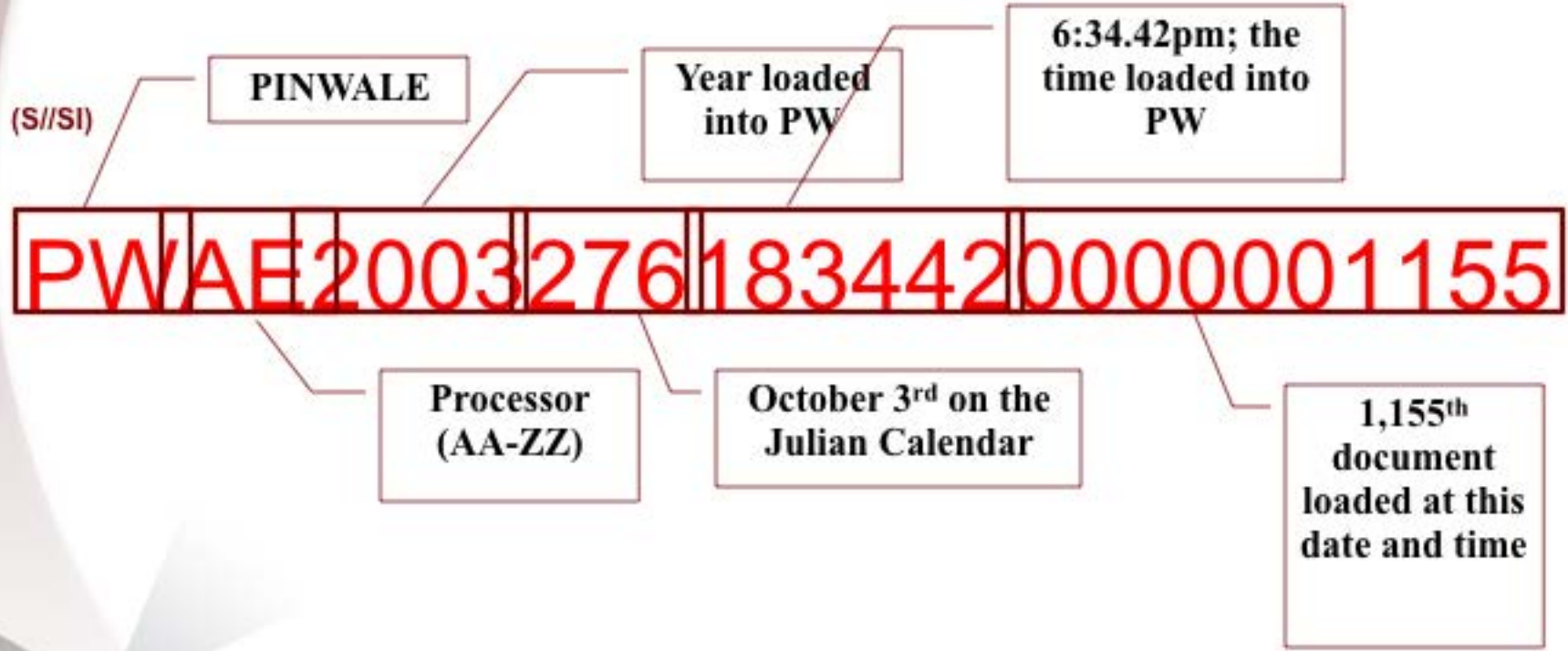
PW	PINWALE
YA	Processor ID internal to PINWALE (values AA-ZZ)
2006	Year loaded into PW
298	October 25 th on the Julian calendar
115456	Time (HHMMSS)
0001151730	10 digit document number for the documents loaded at this time.

(S//SI)



(U) PINWALE ID

- (U//FOUO) Deconstruct this PINWALE ID (PWID)



(S//SI)





(C//SI) PINWALE and DNI Analysis

- (S//SI//REL) Repository for all the traffic we collect and includes metadata and content, with a focus on the content
- (S//SI//REL) Helps you answer important questions:
 - What personal information is available my target?
 - Who are his contacts (buddy lists, address books)
 - What are my target's alternate accounts (e-mail accounts, chat accounts, usernames)
 - Where is my target located and where does he log on from?
 - What can I learn about my target's computer (MAC addresses, cookies)



(U) Four Most Common Searches

- (U) Search for an e-mail account
- (U) Search for an IP address
- (C) Search for a PINWALE document using a PINWALE ID (PWID)
- (C) Search for a Universally Unique ID (UUID)



(U) NEXUS Search Editor

(TS//SI)

US: Nexus Search Editor

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-1 Load-0 Save Print Validate Clear Remove

Search Information:
Name: Prt 1 Description: Prt 1 targets in SE Asia

Data Selection:

Search Engine: LIONHRT_FUSION
Search Type: Full Search
Retrieve Metadata: ON
Segd Results To: pichris
Model To Use: None

Visibility Group:
WVCENDER
KEYSTONE
KYSTYNKE
Medium Trm
SQF
STOUTHEART

Query Association:
New Edit
Remove Load

pichris/queries/Prt1

New Query Name: NewQuery

Mag Docs: 1000 Size Days: 90

From (YYYYMMDD): 20070227 To (YYYYMMDD): 20070227

Add	Visibility Group	From	To
Remove	SQF	20070227	20070227

Free Form Query:
(lagenda57) OR (chanfox 10 adj 1) OR (iwanku001) OR (kalianda33) OR (ryono asnan adj 1) OR (nenekaude) OR (topak64) OR (pilihankulah) OR (lifetsfitnah 7 adj 1) OR (fauzi nd01 adj 1))))

Latin A-I-English Keyboard (QWERTY) ISO8859_1



(U) Query an E-mail Account

- (S//SI) You can use DECODEORDAIN when querying on an e-mail account
- (C//SI) DECODEORDAIN prepares the permutations for you in the query language's native form
- (S//SI) Query PINWALE directly from DECODEORDAIN results page

[Go DECODEORDAIN](#)



(U) PINWALE

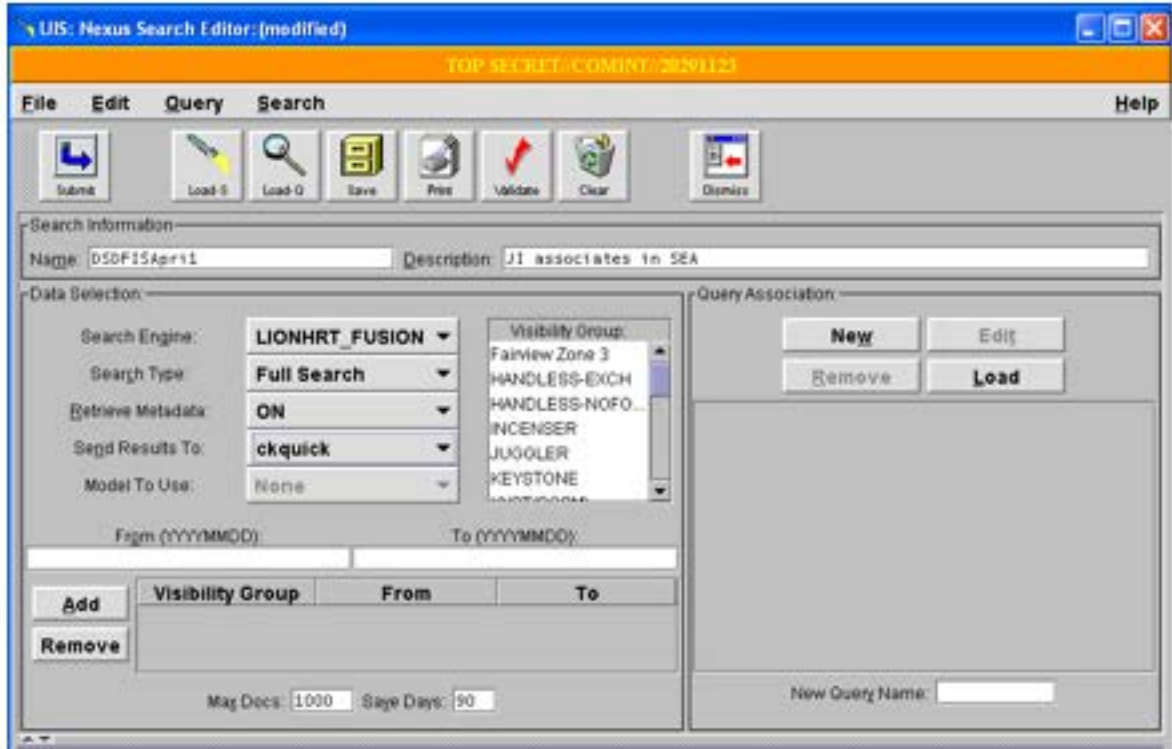
Objectives

- (U) Configure and use the UIS Metadata Viewer to process and view Pinwale search results and metadata
- (U) Create a query for viewing the FISA data



(U) Search Parameters

- (U) Search Information
 - In this area you have the Name field which is used as an identifier
 - The Description field which just provides any additional information.





(U) Search Parameters cont.

- (U) Data Selection
 - (U) Search Engine – Allows the user to select the search engine of their choice.
 - **** **Select PINWALE DISSEM**
 - (U) Search Type – Used to select whether documents are actually retrieved or just counted.
 - **** **Usually – Full Search**
 - (U) Retrieve Metadata – Can be used to disable metadata. This is not available when the selected Search Type is **Hits Only**.
 - (U) Send Results To – Sets the folder location to return the search results; defaults to your SID.
 - **** **Leave your sid for this field.**
 - (U) Visibility Group List – Allows you to select one or all of the Visibility Groups. Be sure to click on **Add** so it can be added to your search.
 - **** **Select/Highlight SQF partition**



(U) Search Parameters cont.

UIS: Nexus Search Editor:(modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-S Load-Q Save Print Validate Clear Demiss

Search Information

Name: DSDFI5Apr11 Description: JI associates in SEA

Data Selection:

Search Engine: PINWALE_DISSEM

Search Type: Full Search

Retrieve Metadata: ON

Send Results To: ckquick

Model To Use: None

Visibility Group:

- PSC-Text
- SGRNSPC-YNKE
- SQF
- SQX
- STOUTHEART
- SUGAR-HALFLEX

From (YYYYMMDD): To (YYYYMMDD):

Add	Remove	Visibility Group	From	To

Save Days: 90

Query Association:

New Edit

Remove Load

New Query Name: _____



(U) Search Parameters cont.

- (U) Date Range – Enter the date range in the **From** and **To** fields. It is important to remember to leave the fields blank for the **PINWALE_DISSEM** as it is a continuous running search.
- (U) Visibility Group Table – By clicking the **Add** you are able to insert the visibility groups and the date range into the Visibility Group table. Please note that if there is no data for any day within the date range you will get an informational window popping up and saying “Data is not available for the entire date range specified”.
 - (U) Max Docs/Max Hits – **Max Docs** limits the number of documents that will be returned by the queries associated with a **Full Search**. **Max Hits** limits the number of hits that will be returned by the queries associated with a **Hits Only** query. Keep in mind that the system limits are 20,000 Max docs and 1000000 Max hits.
 - (U) Save Days – Determines the length of time that the results from a search will remain in the folder manager.



(U) Search Parameters cont.

UIS: Nexus Search Editor: (modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-S Load-O Save Print Validate Clear Demiss

Search Information
Name: D5DF1SApr11 Description: JI associates in SEA

Data Selection:
Search Engine: PINWALE_DISSEM
Search Type: Full Search
Retrieve Metadata: ON
Send Results To: ckquick
Model To Use: None

Visibility Group:
PSC-Text
SGRNSPC-YNKE
SQF
SQX
STOUTHEART
SUGAR-HALFLEX

Query Association:
New Edit
Remove Load

From (YYYYMMDD): To (YYYYMMDD):

Add	Visibility Group	From	To
Remove	SQF	-	-

Save Days: 30

New Query Name:



(U) Creating A Query

- (U) Query Association Area – This area contains a list of queries associated with the search as well as functions to edit the queries. Remember if you do not wish to submit a query you had previously opened in the editor, you must remove it from the association list, **before** hitting the *submit* button.
- (U) New Query Name – This is probably the easiest function in PINWALE. Type the query name then either press the **Return** or **Enter** keyboard buttons or click the **New** button. Try and use something related to what you are going after.
- (U) Query Buttons
 - **New** – Creates a new query and is given the name in the New Query Name Field
 - **Edit** – Opens a selected query from the Query Association List, or brings the selected query window to the front if multiple queries are open
 - **Remove** – Simply removes the selected queries from the Query Association List. Keep in mind that the queries are not deleted from the **Saved Queries** folder.
 - **Load** – Opens the Load Query dialog box, allowing you the user to add a personal or shared Saved Query.



(U) Creating A Query cont.

UIS: Nexus Search Editor: (modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-S Load-O Save Print Validate Clear Dimiss

Search Information
Name: OSDP15Apr11 Description: JI associates in SEA

Data Selection:

Search Engine: PINWALE_DISSEM
Search Type: Full Search
Retrieve Metadata: ON
Segd Results To: ckquick
Model To Use: None

Visibility Group:
PSC-Text
SORNSPC-YNKE
SQF
SQX
STOUTHEART
SUGAR-HALFLEX

From (YYYYMMDD): To (YYYYMMDD):

Add	Visibility Group	From	To
Remove	SQF	-	-

Save Days: 30

Query Association:
New Edit
Remove Load
FISA_pri1
New Query Name: _____

FISA_pri1

File SE-Type Options Forms
TOP SECRET//COMINT//20291123
Description: _____
Free Form Query



(U) Selecting a Query Form

- (U) Query Forms – Vary in complexity from the Smart Form, which performs syntax formatting to the Freeform which requires you to format the entire query in the native query language.
- a. Valid LIONHEART_FUSION (RW) forms are SmartForm, SmartForm II, Fielded Search, and Freeform
 - b. Valid LIONROAR/PINWALE_DISSEM (PSL) forms are SmartForm, SmartForm II, Zoned Search, String – Smart Form, Set Ops, and Freeform
Select **“Smartform”**



(U) Selecting a Query Form

UIS: Nexus Search Editor: (modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-S Load-Q Save Print Validate Clear Demote

Search Information
Name: DSDP15Apr11 Description: JI associates in SEA

Data Selection:

Search Engine: PINWALE_DISSEM
Search Type: Full Search
Retrieve Metadata: ON
Segd Results To: ckquick
Model To Use: None

Visibility Group:
PSC-Test
BORN-SPC-YN/KE
SOE
SOX
STOUTHEART
SUGAR-HALFLEX

Query Association:
New Edit
Remove Load
FISA_pri1
New Query Name: _____

From (YYYYMMDD): To (YYYYMMDD):

Add	Remove	Visibility Group	From	To
		SOE	-	-

Save Days: 30

FISA_pri1

File SE-Type Options Forms

Free Form Query
Smart Form
SmartForm II
Set Ops
String - SmartForm
Zoned Search
Fielded Search
DC Field Form

Free Form Query SmartFo

CRET//COMINT//20291123



(U) Entering Query Terms

(U) As you type the terms into a form the native rendition of the term will be displayed above the field for information and feedback purposes.

(U) When using forms associated with RW, if you type something incorrect, the feedback will turn **red**, alerting you to the fact that the term needs to be fixed in some way.

- Enter FISA target case notations in the fields/blanks.



(U) Entering Query Terms cont.

LIIS: Nexus Search Editor: (modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Load-S Load-Q Save Print Validates Clear Dismiss

Search Information
Name: DSOF15Apr11 Description: JI associates in SEA

Data Selection:
Search Engine: PINWALE_DISSEM
Search Type: Full Search
Retrieve Metadata: ON
Segd Results To: ckquick
Model To Use: None

Visibility Group:
PSC-Text
SORNSPC-YNKE
SQF
SOX
STOUTHEART
SUGAR-HALFLEX

Query Association:
New Edit
Remove Load
FISA_pri

From (YYYYMMDD): To (YYYYMMDD):
Add Remove
Save Days: 30

Visibility Group	From	To
SQF	-	-

New Query Name: _____

FISA_pri

File SE-Type Options Forms

TOP SECRET//COMINT//20291123

Description: JI associates in SEA on special collection

Free Form Query Smart Form

Proximity: 1 DOCUMENT

cs=150059_1 ("SQF056212") or cs=150059_1 ("SQF065558") or cs=150059_1 ("SQF065168")
 (SQF056212 or SQF065558 or SQF065168 or
 or or) and



(U) Validate Queries

- (U) The Validate button runs all queries through a basic syntax check.
- (U) Pop-up window activated to show **IS Valid** or **Has Errors**
- (U) Best way to validate a query is to use the **Validate** command on the query form's **Options** menu.



(U) Validate Queries cont.

UIS: Nexus Search Editor: (modified)

TOP SECRET//COMINT//20291123

File Edit Query Search Help

Submit Lead-S Lead-Q Save Print Validate Clear Diagnostics

Search Information
Name: DSDP15Apr13 Description: JI associates in SEA

Data Selection
Search Engine: PINWALE_DISSEM
Search Type: Full Search
Retrieve Metadata: ON
Segd Results To: ckquick
Model To Use: []
From (YYYYMMDD): []

Visibility Group:
PBC-Text
SORNSPC-YNAKE
SQF
SQX
STOUTHEART
SUGAR HALEY

Query Association
New Edit
Remove Load
FISA_pn1

Add Remove Visibility Group
SQF

FISA_pn1
File SE-Type Options

Description: JI associates in SEA
Free Form Query Smart Form

Proximity: 1 DOCUMENT

ca=150059_1 ('S0F06212') or ca=150059_1 ('S0F06558') or ca=150059_1 ('S0F065168')
(S0F06212 or S0F06558 or S0F065168) and

Query Validation Summary

Query Validation Summary
FISA_pn1 / {is Valid } (Cost=96)
(Total Cost=96)

OK



(U) Saving your Work

- (U) Easiest way to save your search and queries at the same time is to click the **Save** button on the toolbar. There are other ways but this is the most efficient.



(U) Search & Results

Submit Search

- (U) This function can not be accomplished until your queries have been validated and optionally saved.
- (U//FOUO) The submitted search then goes through four phases
 - Queued
 - Submitted
 - Running
 - Getting results to complete

Checking the Hits

- (U) Once the search is complete the Hit Count and items column next to the query folders will be populated with the results.
- (U) If you don't see results then refresh the Folder manager



(U) Customizing Metadata Viewer Fields

- (U) Currently there are 700 fields that you as an analyst/linguist can select from to assist you in search of your target. Keep in mind that you can take and setup as many MDV layouts as you desire to suit the needs of the target that you are doing your research/analysis on.



(U) Loading Results

- (U) The Metadata Viewer or as it is commonly called the (MDV) is where the results set their metadata.
- (U) Results are stored in an ORACLE database and are linked to a container folder in the UIS Folder Manager.
- (U) To load the results from metadata for a Query, simply select the query folder and double click. Note: You may load multiple results into the MDV simply by CTRL-selecting multiple query folders before applying the load function.
- (U) Keep in mind that when loading documents it can take as short as a few second or longer depending on the actual number of results and the search engine that was being used.



(U) Sorting Metadata

- (U) By using the MDV sorting can be as simple as the ordering of a column of data in ascending or descending order, or as complex as sorting a partial or full set of results using multiple fields.
- (U) Sorting can be useful for such tasks as analyzing events in chronological order and or finding anomalies in target communication profiles.

UIS: Metadata Viewer (fisa)

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20291123

Table Viewers Print Present Edit Sort Find Filter Colors Fields Prioritize Services Help

Reload Present Prev Next Print Show PD Delete Undelete Show GC Dismiss

#	DTG	Case Notation	SIGINT A...	Visib.
1	20070226:05:38:00:000	XX.SQF075193	US-984J	SQF
2	20070227:13:37:00:000	XX.SQF075193	US-984J	SQF
3	20070227:13:37:00:000	XX.SQF075193	US-984J	SQF
4	20070227:14:13:00:000	XX.SQF075193	US-984J	SQF
5	20070227:14:13:00:000	XX.SQF075193	US-984J	SQF
6	20070227:14:13:00:000	XX.SQF075193	US-984J	SQF
7	20070227:14:13:00:000	XX.SQF075193	US-984J	SQF
8	20070227:14:15:00:000	XX.SQF075193	US-984J	SQF
9	20070227:23:58:00:000	XX.SQF075193	US-984J	SQF
10	20070228:05:53:00:000	XX.SQF075193	US-984J	SQF
11	20070228:22:53:00:000	XX.SQF075193	US-984J	SQF
12	20070228:22:55:00:000	YY.SQF075193	US-984J	SQF



(U) PINWALE Resources

- (U) PINWALE Tip of the Week (E-mail)
- (U) Tip of the Week also announces dates and times for upcoming:
 - PINWALE Query Walk-in Service
 - PINWALE Users Group Meeting
 - PINWALE Training Sessions
- (U) NCS Training dates and times also found in the tip of the week
- (U) You need to request to be on this mailing list. (DL NEXHELP)



(U) Protocol Help

- (S//SI) Problems with interpreting or identifying your traffic?
 - You can see your target's e-mail, but don't recognize the traffic
 - (C//SI) Send your questions to DL CTSAMPLES with **only** the PINWALE ID



(U) Help?

- (U//FOUO) UIS Help?
 - Contact [REDACTED]
 - E-mail: DL UIS_HELP

- (U//FOUO) PINWALE Help?
 - Contact [REDACTED]
 - E-mail: DL NEXHELP



(U) QUESTIONS?





(U) Exercise

- (U) Create PINWALE_DISSEM query
- (U) Load Query Results
- (U) Customize MDV