(U) Transnational DNI Training

(U) PINWALE
(U) Describe PINWALE

(U) What is 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 the 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.
(S//SI) example: PWYA2006298115456 0001151730

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

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

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

- PINWALE
- Year loaded into PW
- 6:34.42pm; the time loaded into PW
- Processor (AA-ZZ)
- October 3rd on the Julian Calendar
- 1,155th document loaded at this date and time

PWAE20032761834420000001155
(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 on 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)
(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) Query an E-mail Account

[Image showing a web interface for querying an email account]
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.

The image shows a screen capture of a software interface for searching a database. The interface includes options for selecting search engines, data selection, and query association. Specific parameters include:

- **Search Engine**: PINWALE_DISSEM
- **Search Type**: Full Search
- **Retrieve Metadata**: On
- **Send Results To**: quick
- **Model To Use**: None
- **From (YYYY/MM/DD)**:
- **To (YYYY/MM/DD)**:
- **Visibility Group**:
  - PINWALE_DISSEM
  - PINWALE_DISSEM
  - PINWALE_DISSEM
- **Save Days**: 90

The interface also includes buttons for submitting, loading, and saving queries.
(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.
(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.
(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_DISSEEM (PSL) forms are SmartForm, SmartForm II, Zoned Search, String – Smart Form, Set Ops, and Freeform

Select “Smartform”
(U) Selecting a Query Form
(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.
(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.
(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.
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) 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) 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 seconds 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.
(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)
(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
  - E-mail: DL UIS_HELP

- (U//FOUO) PINWALE Help?
  - Contact
  - E-mail: DL NEXHELP
(U) Exercise

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