Scientific Research Publishing

Journal of Information Security, 2024, 15, 308-319
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Handwriting Analysis Based on Belief of Targeted Individual Supporting Insider Threat Detection

Jason Slaughter, Carole E. Chaski, Kellep Charles

Center for Cybersecurity Research and Analysis (CCRA), Capitol Technology University, Laurel, United States
Email: jslaughter@captechu.edu, cchaski@aliastechnology.com, kacharles@captechu.edu

How to cite this paper: Slaughter, J., Chaski, C.E. and Charles, K. (2024) Handwriting Analysis Based on Belief of Targeted Individual Supporting Insider Threat Detection. *Journal of Information Security*, **15**, 308-319.
https://doi.org/10.4236/jis.2024.153018

Received: May 6, 2024
Accepted: June 8, 2024
Published: June 11, 2024

Copyright © 2024 by author(s) and Scientific Research Publishing Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

Abstract

The Unintentional Insider Threat (UIT) concept highlights that insider threats might not always stem from malicious intent and can occur across various domains. This research examines how individuals with medical or psychological issues might unintentionally become insider threats due to their perception of being targeted. Insights from the survey "A Survey of Unintentional Medical Insider Threat Category" indicate that such perceptions can be linked to underlying health conditions. The study "Emotion Analysis Based on Belief of Targeted Individual Supporting Insider Threat Detection" reveals that anger is a common emotion among these individuals. The findings suggest that UITs are often linked to medical or psychological issues, with anger being prevalent. To mitigate these risks, it is recommended that Insider Threat programs integrate expertise from medicine, psychology, and cybersecurity. Additionally, handwriting analysis is proposed as a potential tool for detecting insider threats, reflecting the evolving nature of threat assessment methodologies.

Keywords

Insider, Threat, Detection, Targeted, Medical

1. Introduction

"This article extends the research presented in the peer-reviewed article "A Survey of Unintentional Insider Threat Category," available at (https://ijcsit.com/ijcsit-v14issue2.php) [1], and further develops themes from "Emotion Analysis Based on Belief of Targeted Individual Supporting Insider Threat Detection," accessible at (https://ijsra.net/content/emotion-analysis-based-belief-targeted-individual-supporting-insider-threat-detection) [2].

The concept of Unintentional Insider Threat underscores that such threats might not always arise from malicious intent and can occur in various domains. This form of threat often involves individuals who, due to underlying medical or psychological issues, perceive themselves as being targeted, inadvertently heightening their risk of becoming insider threats.

Insights from these studies suggest that these perceptions are frequently associated with feelings of anger. Insider Threat programs must incorporate specialized expertise from medicine, psychology, and cybersecurity to mitigate these risks effectively.

This series' concluding article proposes exploring handwriting analysis as a novel method for detecting potential insider threats, demonstrating the adaptive and interdisciplinary approach required in threat assessment across different sectors.

The background is individuals who believe they are being targeted and may become insider threats.

The focus is on individuals who may have medical problems over psychological problems or detecting actual real-world targeting occurring.

However, this study could consider either of those two cases.

To expand on the first author's background and experience, it was initially thought to be hypervigilance-causing actions and reactions in their behavior.

For instance, the first author's phone appeared to start scrolling to words on web pages that directly correlated with the first author's knowledge and history. This became of significant concern when the correlations appeared to occur across networks that should not be touching and should not have the vectors for the information to flow.

The first author initially thought a R.A.T. (Remote Access Trojan) or similar malware was present.

To date, the correlations are approaching 100 in-context words and phrases. They have run through various people's names known personally by the first author or that the first author knows of.

The correlations have covered events and locations. Many correlations focus on DoD/IC-related topics, leading the first author to believe a federal investigation or real-world targeting is occurring.

However, after further discussion and many medical tests and brain scans, it was determined to be a combination of two sleep disorders resulting in various known and documented symptoms. The life experience ultimately led the first author to perform this series of studies.

In the latest occurrence, a UTI was found to be present, and this was also found to be the case in each of the initial occurrences, which may play a part in the first author's targeted belief.

In January 2024, the first author underwent additional psychological testing with Veterans Affairs and physical testing where the UTI was discovered and treated. The correlations decreased close to immediately after treatment of the UTI. The VA medical team stated that the first author has "illusions" where there is a natural stimulus/input, but it is misinterpreted. This is different from delusions or hallucinations; they stated that it is a real-world activity occurring with possibly a misinterpretation of what author one is seeing or hearing at the time.

To date, the correlations have continued. As of this writing, the most recent occurrence was an event on the first author's front porch. He was speaking to his family about the events of Benghazi, and everyone was discussing how unhappy they were with how it was handled. The first author's brother mentioned something about the Clintons, and then the conversation moved on to something else.

The next day, the first author was at a medical appointment at the VA in the waiting room with several other people watching the TV that kept going in and out and had various visual distortions. The first author heard the following in sequence correlation, "Monitor Slaughter Clinton". It was not repeated.

Also of note were the caregivers' cell phones in the VA sitting on their desks in phone holders beside their government-furnished laptops and being used to perform patient care. The first author experienced this firsthand as the primary care provider looked up medications on their cell phone.

Additionally, note that one computer stated it was still in a video conference and was the last remaining participant, meaning there was potentially still video in the room where the first author was sitting.

The last correlations were the word black and spoken word operators.

While the UTI appears to be a contributing factor, additional analysis should occur into the correlations or the first author's perception of them.

1.1. Purpose of the Study

The study aims to expand the understanding of insider threat detection by introducing a new dimension where individuals with medical conditions are also considered potential insider threats. This approach contrasts with traditional methods that primarily focus on overt security risks, thus broadening the scope of threat analysis to include health-related vulnerabilities.

1.2. Theoretical Framework

This paper's theoretical framework analyzes personality and behavior, a recognized approach for assessing individual reactions. The authors have utilized this model to construct profiles indicative of insider threats. Additionally, they have incorporated natural language processing techniques to scrutinize personal content, thereby identifying potential insider threats.

1.3. Nature of the Study

The study will employ the ALIAS machine learning system to analyze handwriting data from individuals who perceive themselves as potential targets and, thus, may pose insider threats.

1.4. Significance of the Study

This study advances research in the field of insider threat detection by concentrating on individuals with medical conditions who perceive themselves as targets, potentially posing as insider threats. While this research does not delve into psychological incidents or actual targeting occurrences, the methodologies applied here could be adapted and refined for further exploration.

Shown in **Table 1** appears a sub-set of medical problems that may lead to unintentional insider threat scenarios. In many cases psychosis-like symptoms may occur that could lead the insider to believe events are occurring when they are not. Paranoia and anxiety may also occur increasing the distress of the employee.

2. Research Methodology

2.1. Population

The population for this study consists of two distinct groups. The control set will include samples of the first author's handwriting collected during basic training, providing a baseline for normal handwriting patterns under non-stressful conditions. For the test set, handwriting samples will be gathered from various events

Table 1. Table of medical problems.

Medical Condition	Description
Epilepsy [2]	A neurological disorder characterized by recurring seizures.
Encephalitis [2]	Inflammation of the brain can cause seizures and other neurological symptoms.
Meningitis [2]	Inflammation of the membranes surrounding the brain and spinal cord, which can cause seizures and other neurological symptoms
Stroke [2]	Disrupting blood flow to the brain can cause seizures and other neurological symptoms.
Traumatic Brain Injury [2]	An injury to the brain caused by an external force can cause seizures and other neurological symptoms.
Alcohol Withdrawal [2]	Abrupt cessation of alcohol consumption can cause seizures and other neurological symptoms.
Brain Tumors [2]	Abnormal growths in the brain can cause seizures and other neurological symptoms.
Sleep Disorders [2]	A broad category that encompasses several symptoms related to sleep and wakefulness. It is known to cause anxiety, paranoia, and hallucinations across all five senses when left undiagnosed and untreated.
Urinary Tract Infection (UTI)	A UTI can potentially cause psychosis-like symptoms.

where different emotional or psychological states are likely to be exhibited. This approach allows for a comprehensive comparison between standard and potentially altered handwriting behavior, aiding in identifying deviations that could indicate insider threats.

2.2. Sample

The sample consists of the first author's handwriting samples from several years and different parts of life. Specifically, handwriting was selected from a letter home from the U.S. Army Basic Training in 1999 and from handwriting in journals from 2020.

The Basic Training letter (non-diseased) was 1 page on standard notebook paper, A4 in size, and written using ink.

12 journal pages (diseased) were selected for the analysis. The pages were also written using an ink pen. The pages are standard A5 in size.

2.3. Materials/Instruments

The instrument will be ALIAS's [3] machine learning library of capabilities that will be used to analyze and determine how the research questions will be answered. ALIAS [3] includes a list of machine learning capabilities to be leveraged during the research.

Custom Python code will also be written to clean and transform the dataset into individual letters to be analyzed based on density, height, width, slant, curvature, concavity, elliptical, and circular handwriting attributes selected for the study.

Each letter was individually analyzed using custom Python scripts and machine learning to extract the averages for each handwriting attribute noted in **Figure 7**.

2.4. Data Collection and Data Analysis

The following examples show data that was collected and analyzed for this research.

The non-diseased data set shown in **Figure 1** contained 1732 letters extracted from the letter from U.S. Army Basic Training in 1999.

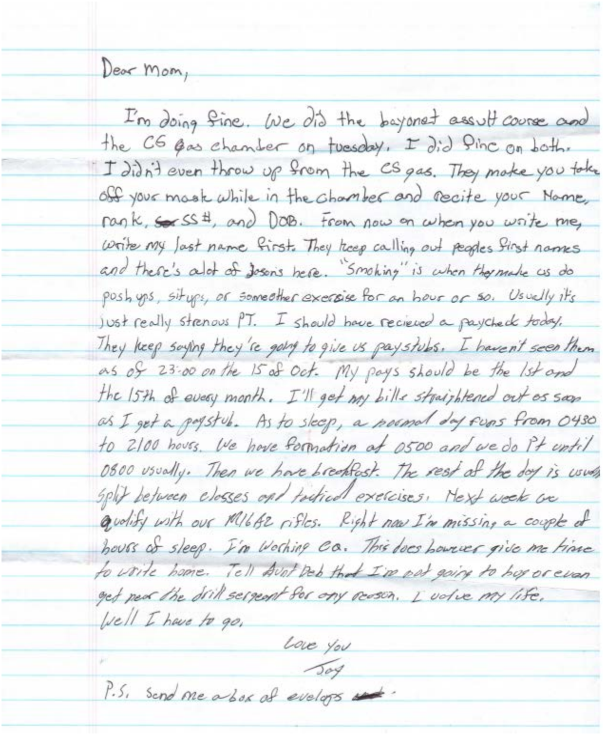
The diseased data set partially shown in **Figure 2** contained 26323 letters extracted from various handwriting performed in 2020 during the initial feelings of being targeted incident.

In **Figure 3**, logging in to the ALIAS system is completed. From here, author one navigated to the main ALIAS functionality shown in **Figure 4** [3].

From the selections in **Figure 4**, the micro text selection was chosen due to the tweets being considered micro texts by the ALIAS system [3].

In **Figure 5**, the upload tweets as JSON were selected due to the format of the tweets to be uploaded into ALIAS [3].

In **Figure 6**, a check is performed to ensure the JSON keys match what ALIAS



Dear Mom,

I'm doing fine. We did the bayonet assult course and the CS gas chamber on tuesday. I did fine on both. I didn't even throw up from the CS gas. They make you take off your mask while in the chamber and recite your Name, rank, ~~so~~ SS#, and DOB. From now on when you write me, write my last name first. They keep calling out peoples first names and there's alot of Jason's here. "Smoking" is when they make us do push ups, situps, or someother exercise for an hour or so. Usually it's just really strenous PT. I should have recieved a paycheck today. They keep saying they're going to give us paystubs. I haven't seen them as of 23:00 on the 15 of Oct. My pays should be the 1st and the 15th of every month. I'll get my bills straightened out as soon as I get a paystub. As to sleep, a normal day runs from 0430 to 2100 hours. We have formation at 0500 and we do PT until 0800 usually. Then we have breakfast. The rest of the day is usually split between classes and tactical exercises. Next week we qualify with our M16A2 rifles. Right now I'm missing a couple of hours of sleep. I'm working CQ. This does however give me time to write home. Tell Aunt Deb that I'm not going to hug or even get near the drill sergeant for any reason. I value my life.

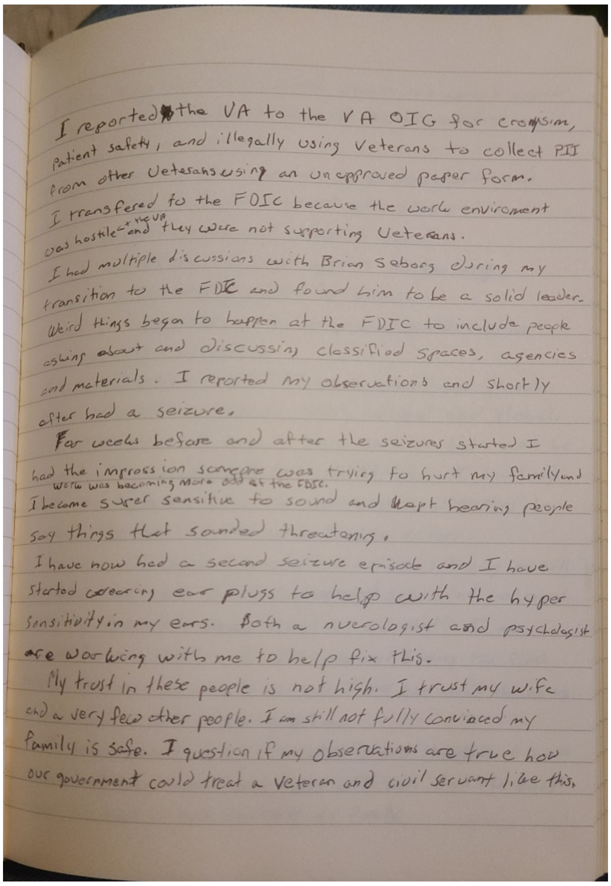
Well I have to go.

Love you

Joy

P.S. Send me a box of evelops.

Figure 1. Basic training letter from 1999.



I reported the VA to the VA OIG for cronysim, patient safety, and illegally using Veterans to collect PII from other Vetesans using an unapproved paper form.

I transfered to the FDIC because the work enviroment was hostile at the VA and they were not supporting Veterans.

I had multiple discussions with Brian Seborg during my transition to the FDIC and found him to be a solid leader.

Weird things began to happen at the FDIC to include people asking about and discussing classified spaces, agencies and materials. I reported my observations and shortly after had a seizure.

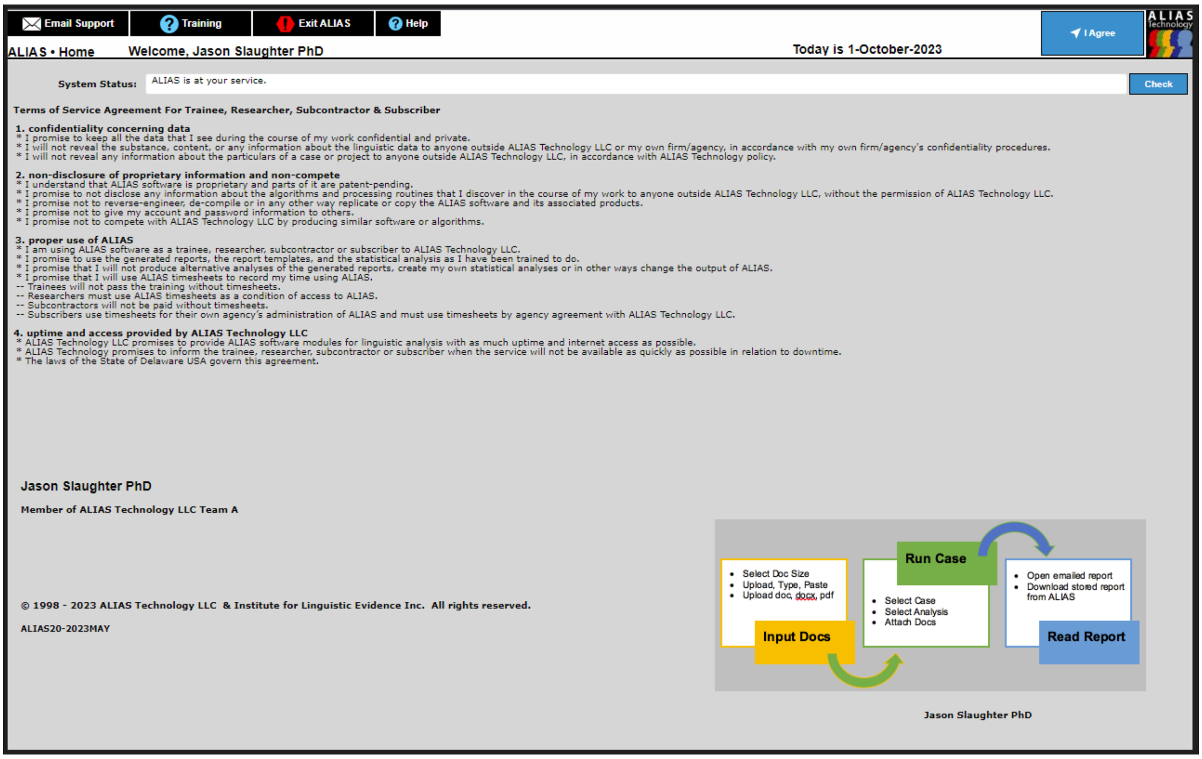
For weeks before and after the seizures started I had the impression someone was trying to hurt my family and work was becoming more odd at the FDIC.

I become super sensitive to sound and kept hearing people say things that sounded threatening.

I have now had a second seizure episode and I have started wearing ear plugs to help with the hyper sensitivity in my ears. Both a nuerologist and psychologist are working with me to help fix this.

My trust in these people is not high. I trust my wife and a very few other people. I am still not fully convinced my family is safe. I question if my observations are true how our government could treat a veteran and civil servant like this.

Figure 2. Diseased writing example 1.



Terms of Service Agreement For Trainee, Researcher, Subcontractor & Subscriber

1. confidentiality concerning data
* I promise to keep all the data that I see during the course of my work confidential and private.
* I will not reveal the substance, content, or any information about the linguistic data to anyone outside ALIAS Technology LLC or my own firm/agency, in accordance with my own firm/agency's confidentiality procedures.
* I will not reveal any information about the particulars of a case or project to anyone outside ALIAS Technology LLC, in accordance with ALIAS Technology policy.

2. non-disclosure of proprietary information and non-compete
* I understand that ALIAS software is proprietary and parts of it are patent-pending.
* I promise to not disclose any information about the algorithms and processing routines that I discover in the course of my work to anyone outside ALIAS Technology LLC, without the permission of ALIAS Technology LLC.
* I promise not to reverse-engineer, de-compile or in any other way replicate or copy the ALIAS software and its associated products.
* I promise not to give my account and password information to others.
* I promise not to compete with ALIAS Technology LLC by producing similar software or algorithms.

3. proper use of ALIAS
* I am using ALIAS software as a trainee, researcher, subcontractor or subscriber to ALIAS Technology LLC.
* I promise to use the generated reports, the report templates, and the statistical analysis as I have been trained to do.
* I promise that I will not produce alternative analyses of the generated reports, create my own statistical analyses or in other ways change the output of ALIAS.
* I promise that I will use ALIAS timesheets to record my time using ALIAS.
-- Trainees will not pass the training without timesheets.
-- Researchers must use ALIAS timesheets as a condition of access to ALIAS.
-- Subcontractors will not be paid without timesheets.
-- Subscribers use timesheets for their own agency's administration of ALIAS and must use timesheets by agency agreement with ALIAS Technology LLC.

4. uptime and access provided by ALIAS Technology LLC
* ALIAS Technology LLC promises to provide ALIAS software modules for linguistic analysis with as much uptime and internet access as possible.
* ALIAS Technology promises to inform the trainee, researcher, subcontractor or subscriber when the service will not be available as quickly as possible in relation to downtime.
* The laws of the State of Delaware USA govern this agreement.

Jason Slaughter PhD

Member of ALIAS Technology LLC Team A

© 1998 - 2023 ALIAS Technology LLC & Institute for Linguistic Evidence Inc. All rights reserved.

ALIAS20-2023MAY

Figure 3. ALIAS homepage.

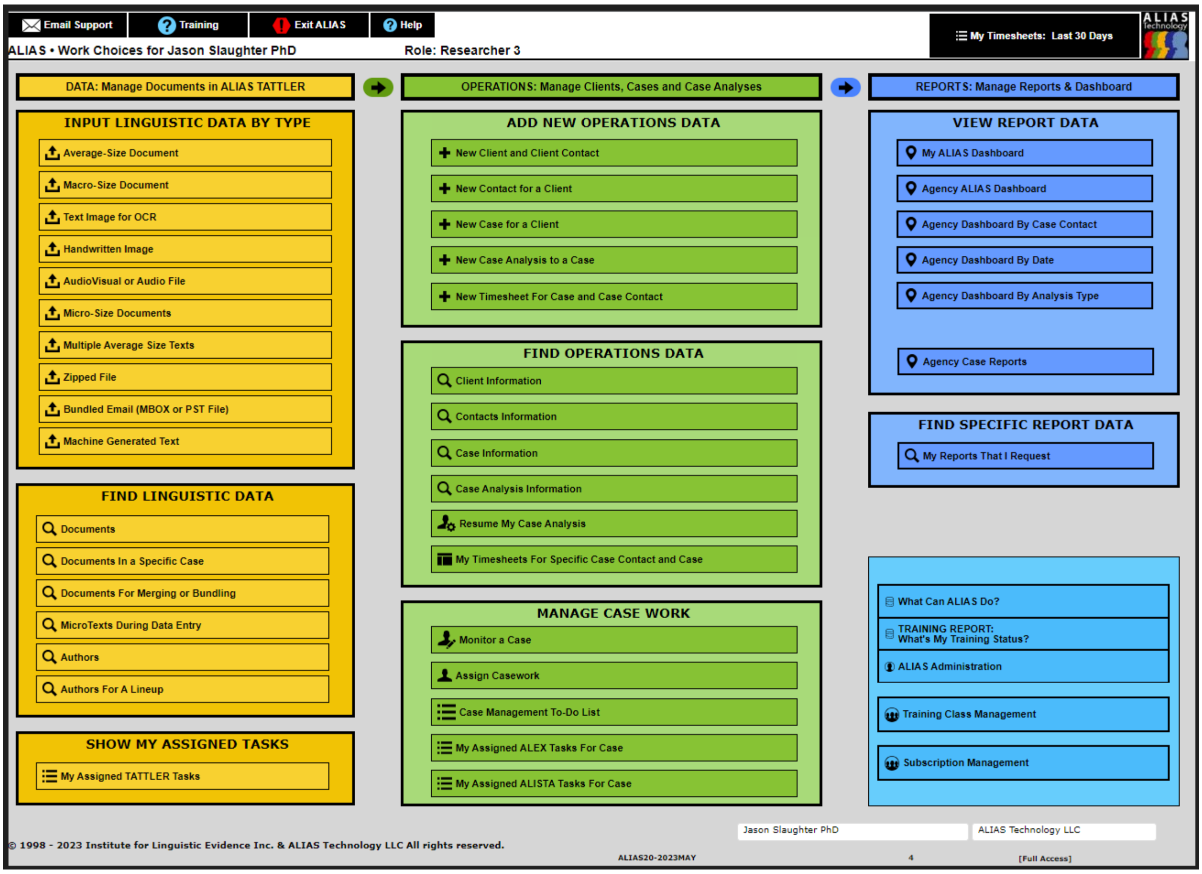
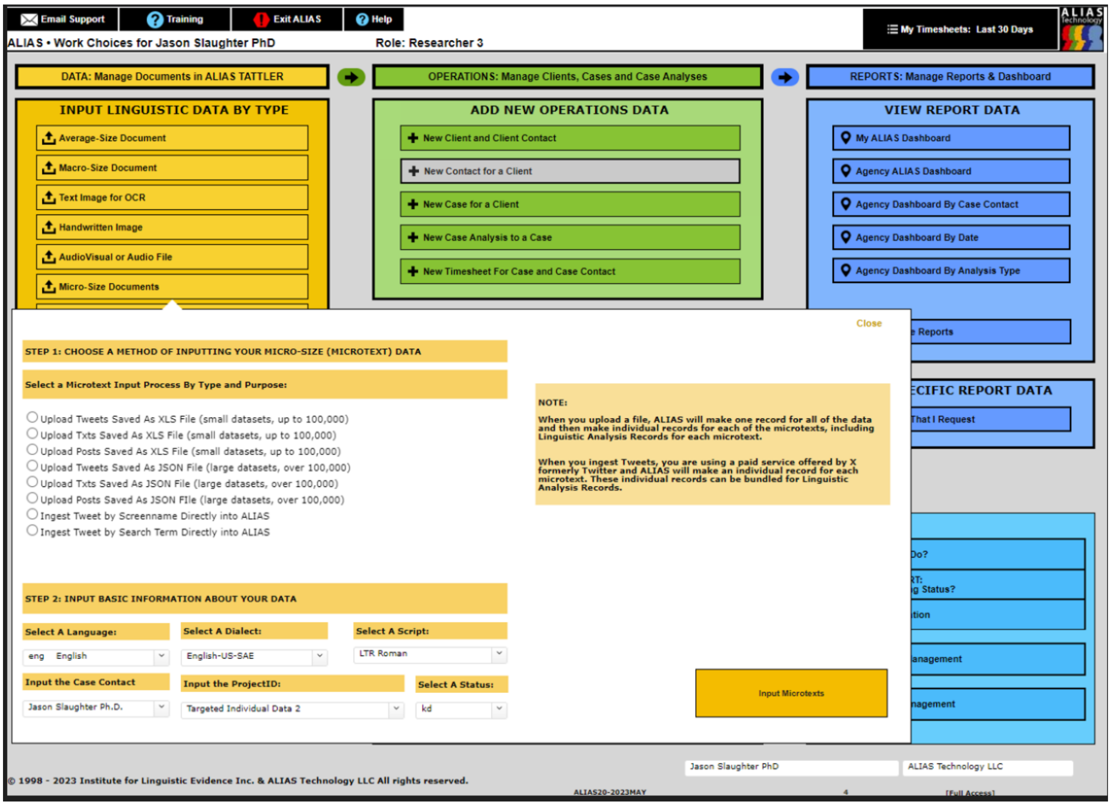

Email Support
Training
Exit ALIAS
Help
My Timesheets: Last 30 Days
ALIAS technology
ALIAS • Work Choices for Jason Slaughter PhD
Role: Researcher 3
DATA: Manage Documents in ALIAS TATTLER
OPERATIONS: Manage Clients, Cases and Case Analyses
REPORTS: Manage Reports & Dashboard
INPUT LINGUISTIC DATA BY TYPE
Average-Size Document
Macro-Size Document
Text Image for OCR
Handwritten Image
AudioVisual or Audio File
Micro-Size Documents
Multiple Average Size Texts
Zipped File
Bundled Email (MBOX or PST File)
Machine Generated Text
FIND LINGUISTIC DATA
Documents
Documents In a Specific Case
Documents For Merging or Bundling
MicroTexts During Data Entry
Authors
Authors For A Lineup
SHOW MY ASSIGNED TASKS
My Assigned TATTLER Tasks
ADD NEW OPERATIONS DATA
New Client and Client Contact
New Contact for a Client
New Case for a Client
New Case Analysis to a Case
New Timesheet For Case and Case Contact
FIND OPERATIONS DATA
Client Information
Contacts Information
Case Information
Case Analysis Information
Resume My Case Analysis
My Timesheets For Specific Case Contact and Case
MANAGE CASE WORK
Monitor a Case
Assign Casework
Case Management To-Do List
My Assigned ALEX Tasks For Case
My Assigned ALISTA Tasks For Case
VIEW REPORT DATA
My ALIAS Dashboard
Agency ALIAS Dashboard
Agency Dashboard By Case Contact
Agency Dashboard By Date
Agency Dashboard By Analysis Type
Agency Case Reports
FIND SPECIFIC REPORT DATA
My Reports That I Request
What Can ALIAS Do?
TRAINING REPORT: What's My Training Status?
ALIAS Administration
Training Class Management
Subscription Management
Jason Slaughter PhD
ALIAS Technology LLC
© 1998 - 2023 Institute for Linguistic Evidence Inc. & ALIAS Technology LLC All rights reserved.
ALIAS20-2023MAY
4
[Full Access]

Figure 4. ALIAS selections.



ALIAS • Work Choices for Jason Slaughter PhD

Role: Researcher 3

STEP 1: CHOOSE A METHOD OF INPUTTING YOUR MICRO-SIZE (MICROTEXT) DATA

Select a Microtext Input Process By Type and Purpose:

○ Upload Tweets Saved As XLS File (small datasets, up to 100,000)
○ Upload Txts Saved As XLS File (small datasets, up to 100,000)
○ Upload Posts Saved As XLS File (small datasets, up to 100,000)
○ Upload Tweets Saved As JSON File (large datasets, over 100,000)
○ Upload Txts Saved As JSON File (large datasets, over 100,000)
○ Upload Posts Saved As JSON FIle (large datasets, over 100,000)
○ Ingest Tweet by Screenname Directly into ALIAS
○ Ingest Tweet by Search Term Directly into ALIAS

NOTE:

When you upload a file, ALIAS will make one record for all of the data and then make individual records for each of the microtexts, including Linguistic Analysis Records for each microtext.

When you ingest Tweets, you are using a paid service offered by X formerly Twitter and ALIAS will make an individual record for each microtext. These individual records can be bundled for Linguistic Analysis Records.

STEP 2: INPUT BASIC INFORMATION ABOUT YOUR DATA

Select A Language:	Select A Dialect:	Select A Script:
eng English	English-US-SAE	LTR Roman

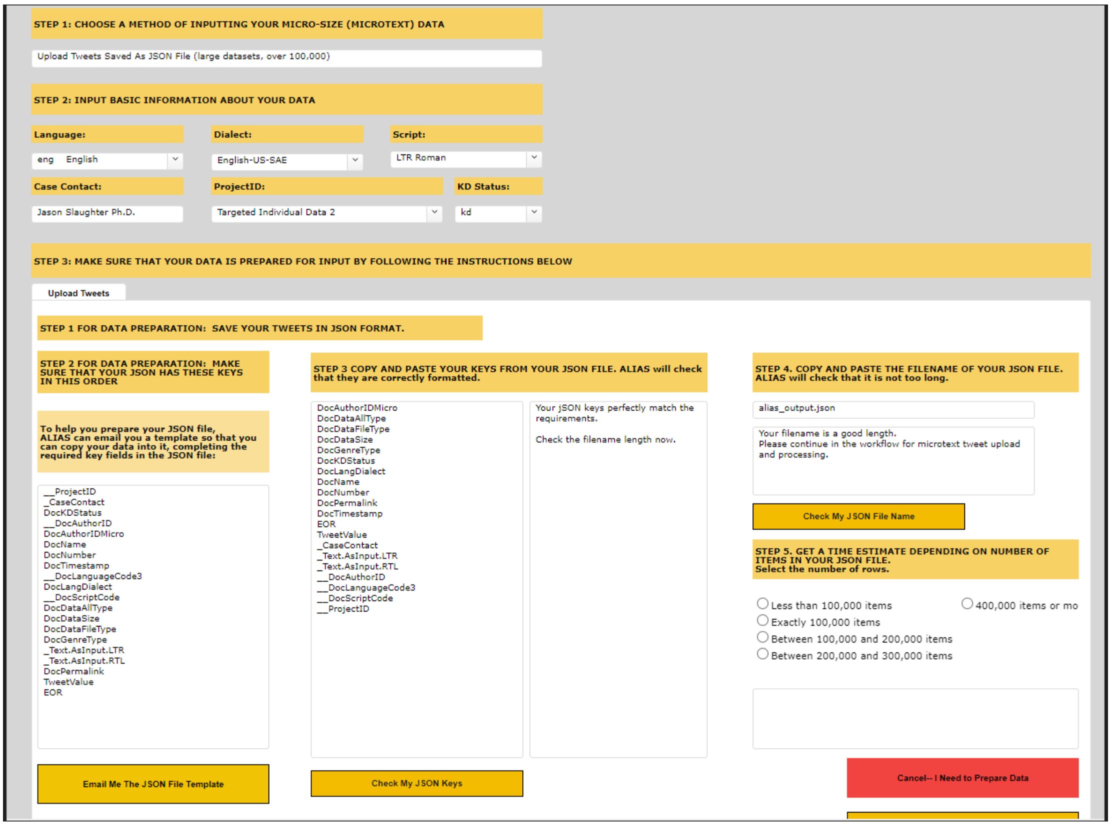
Input the Case Contact	Input the ProjectID:	Select A Status:
Jason Slaughter Ph.D.	Targeted Individual Data 2	kd

Jason Slaughter PhD

ALIAS Technology LLC

© 1998 - 2023 Institute for Linguistic Evidence Inc. & ALIAS Technology LLC All rights reserved.

Figure 5. Choose upload type.


Upload Tweets
Email Me The JSON File Template
Check My JSON Keys
Check My JSON File Name
Cancel-- I Need to Prepare Data

STEP 1: CHOOSE A METHOD OF INPUTTING YOUR MICRO-SIZE (MICROTEXT) DATA

Upload Tweets Saved As JSON File (large datasets, over 100,000)

STEP 2: INPUT BASIC INFORMATION ABOUT YOUR DATA

Language:	Dialect:	Script:
eng English	English-US-SAE	LTR Roman

Case Contact:	ProjectID:	KD Status:
Jason Slaughter Ph.D.	Targeted Individual Data 2	kd

STEP 3: MAKE SURE THAT YOUR DATA IS PREPARED FOR INPUT BY FOLLOWING THE INSTRUCTIONS BELOW

STEP 1 FOR DATA PREPARATION: SAVE YOUR TWEETS IN JSON FORMAT.

STEP 2 FOR DATA PREPARATION: MAKE SURE THAT YOUR JSON HAS THESE KEYS IN THIS ORDER

To help you prepare your JSON file, ALIAS can email you a template so that you can copy your data into it, completing the required key fields in the JSON file:

```
__ProjectID
_CaseContact
DocKDStatus
__DocAuthorID
DocAuthorIDMicro
DocName
DocNumber
DocTimestamp
__DocLanguageCode3
DocLangDialect
__DocScriptCode
DocDataAllType
DocDataSize
DocDataFileType
DocGenreType
_Text.AsInput.LTR
_Text.AsInput.RTL
DocPermalink
TweetValue
EOR
```

STEP 3 COPY AND PASTE YOUR KEYS FROM YOUR JSON FILE. ALIAS will check that they are correctly formatted.

```
DocAuthorIDMicro
DocDataAllType
DocDataFileType
DocDataSize
DocGenreType
DocKDStatus
DocLangDialect
DocName
DocNumber
DocPermalink
DocTimestamp
EOR
TweetValue
_CaseContact
_Text.AsInput.LTR
_Text.AsInput.RTL
__DocAuthorID
__DocLanguageCode3
__DocScriptCode
__ProjectID
```

Your jSON keys perfectly match the requirements.

Check the filename length now.

STEP 4. COPY AND PASTE THE FILENAME OF YOUR JSON FILE. ALIAS will check that it is not too long.

alias_output.json

Your filename is a good length.
Please continue in the workflow for microtext tweet upload and processing.

STEP 5. GET A TIME ESTIMATE DEPENDING ON NUMBER OF ITEMS IN YOUR JSON FILE.
Select the number of rows.

○ Less than 100,000 items
○ Exactly 100,000 items
○ Between 100,000 and 200,000 items
○ Between 200,000 and 300,000 items
○ 400,000 items or mo

Figure 6. Check JSON keys.

expects for the data ingest. If the keys all match during this step, the filename length check can be performed, and then the upload can continue. However, if this doesn't pass, the end user must update the JSON until it matches what ALIAS expects for the upload [3].

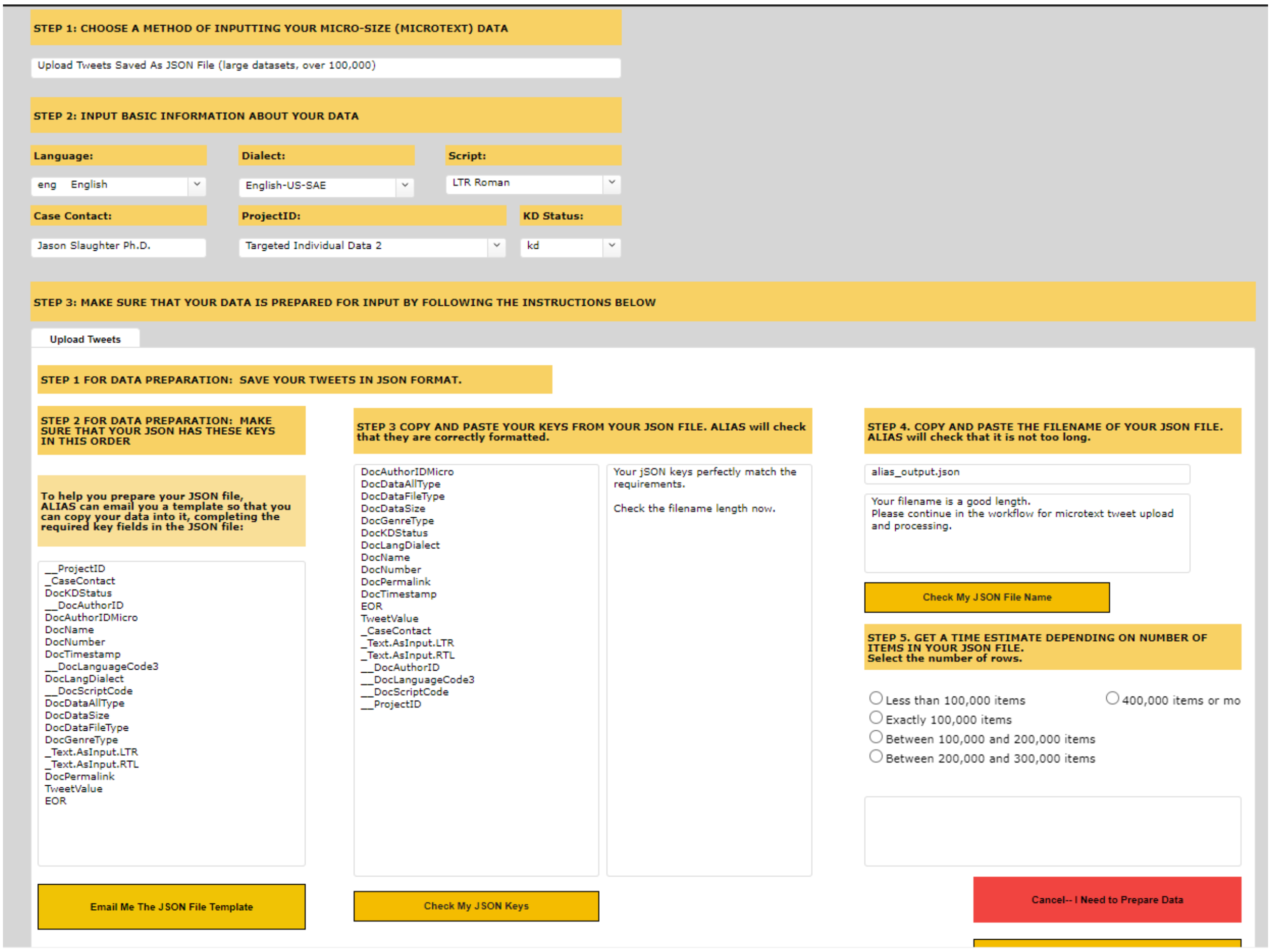
In Figure 7, the final check is performed to determine if the filename length is short enough for the system. If the file name is too long, the file must be renamed until the size is correct for ALIAS to allow the upload to continue [3].

In Figure 8, the user selects the JSON file that was previously validated to be uploaded into the system. Each darker yellow "Click" button is used to upload and process the incoming data. Once the final step is complete on this page, ALIAS navigates the user to the main ALIAS functionality shown in Figure 7 [3].

Shown in Table 2 are the results of the handwriting analysis.

The research questions asked the following questions:

RQ1: What are the individuals' handwriting characteristics when they feel targeted? The conclusion is described in the Diseased column of Table 2, which also defines the measurements used for the analysis.



STEP 1: CHOOSE A METHOD OF INPUTTING YOUR MICRO-SIZE (MICROTEXT) DATA

Upload Tweets Saved As JSON File (large datasets, over 100,000)

STEP 2: INPUT BASIC INFORMATION ABOUT YOUR DATA

Language:	Dialect:	Script:
eng English	English-US-SAE	LTR Roman

Case Contact:	ProjectID:	KD Status:
Jason Slaughter Ph.D.	Targeted Individual Data 2	kd

STEP 3: MAKE SURE THAT YOUR DATA IS PREPARED FOR INPUT BY FOLLOWING THE INSTRUCTIONS BELOW

STEP 1 FOR DATA PREPARATION: SAVE YOUR TWEETS IN JSON FORMAT.

STEP 2 FOR DATA PREPARATION: MAKE SURE THAT YOUR JSON HAS THESE KEYS IN THIS ORDER

To help you prepare your JSON file, ALIAS can email you a template so that you can copy your data into it, completing the required key fields in the JSON file:

```
__ProjectID
_CaseContact
DocKDStatus
__DocAuthorID
DocAuthorIDMicro
DocName
DocNumber
DocTimestamp
__DocLanguageCode3
DocLangDialect
__DocScriptCode
DocDataAllType
DocDataSize
DocDataFileType
DocGenreType
_Text.AsInput.LTR
_Text.AsInput.RTL
DocPermalink
TweetValue
EOR
```

STEP 3 COPY AND PASTE YOUR KEYS FROM YOUR JSON FILE. ALIAS will check that they are correctly formatted.

```
DocAuthorIDMicro
DocDataAllType
DocDataFileType
DocDataSize
DocGenreType
DocKDStatus
DocLangDialect
DocName
DocNumber
DocPermalink
DocTimestamp
EOR
TweetValue
_CaseContact
_Text.AsInput.LTR
_Text.AsInput.RTL
__DocAuthorID
__DocLanguageCode3
__DocScriptCode
__ProjectID
```

Your jSON keys perfectly match the requirements.

Check the filename length now.

STEP 4. COPY AND PASTE THE FILENAME OF YOUR JSON FILE. ALIAS will check that it is not too long.

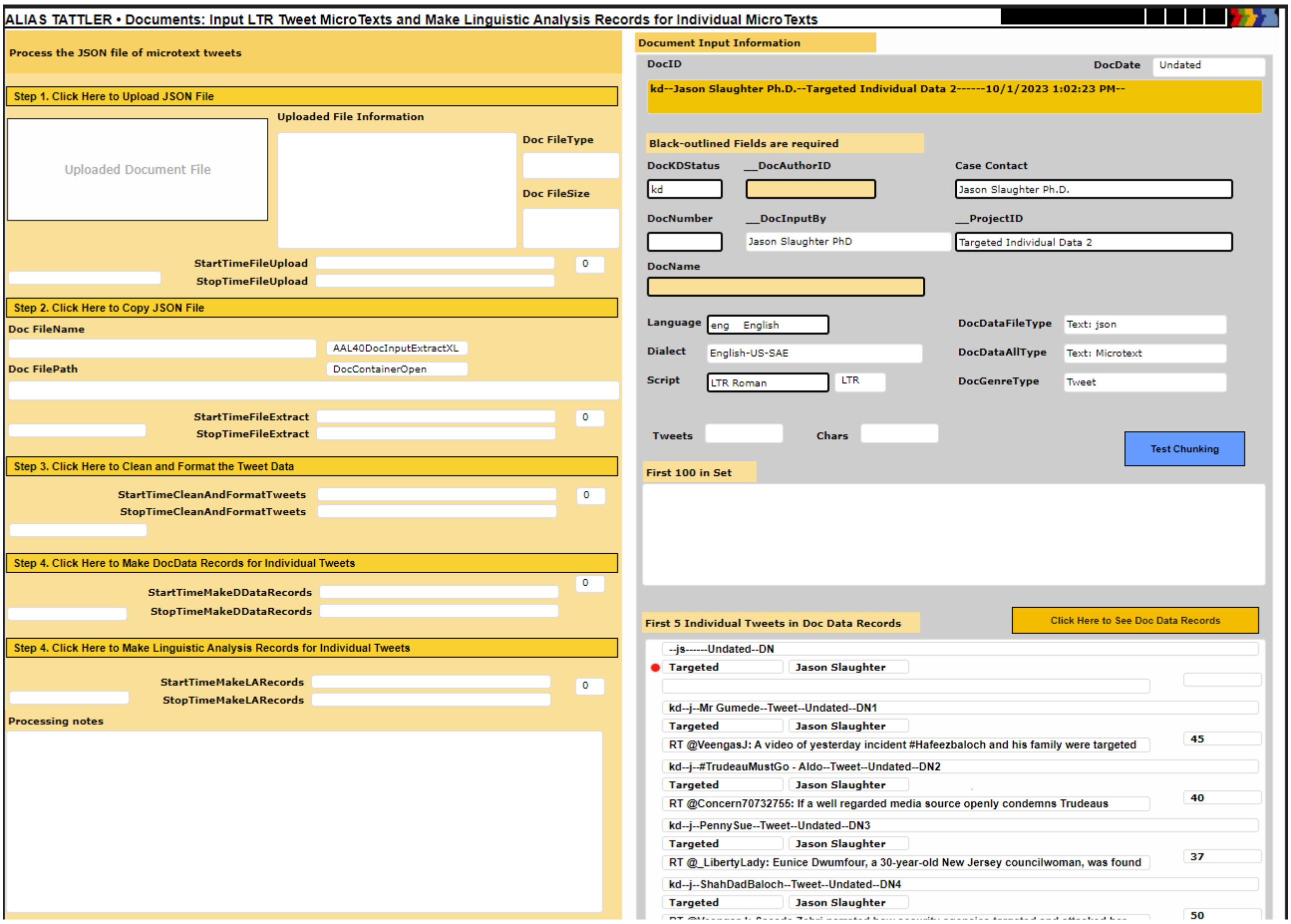
alias_output.json

Your filename is a good length.
Please continue in the workflow for microtext tweet upload and processing.

STEP 5. GET A TIME ESTIMATE DEPENDING ON NUMBER OF ITEMS IN YOUR JSON FILE.
Select the number of rows.

○ Less than 100,000 items
○ Exactly 100,000 items
○ Between 100,000 and 200,000 items
○ Between 200,000 and 300,000 items
○ 400,000 items or mo

Figure 7. Check filename length.



ALIAS TATTLER • Documents: Input LTR Tweet MicroTexts and Make Linguistic Analysis Records for Individual MicroTexts

Process the JSON file of microtext tweets

Step 1. Click Here to Upload JSON File

Uploaded Document File

Uploaded File Information

Doc FileType

Doc FileSize

StartTimeFileUpload 0

StopTimeFileUpload

Step 2. Click Here to Copy JSON File

Doc FileName AAL40DocInputExtractXL

Doc FilePath DocContainerOpen

StartTimeFileExtract 0

StopTimeFileExtract

Step 3. Click Here to Clean and Format the Tweet Data

StartTimeCleanAndFormatTweets 0

StopTimeCleanAndFormatTweets

Step 4. Click Here to Make DocData Records for Individual Tweets

StartTimeMakeDDataRecords 0

StopTimeMakeDDataRecords

Step 4. Click Here to Make Linguistic Analysis Records for Individual Tweets

StartTimeMakeLARecords 0

StopTimeMakeLARecords

Processing notes

Document Input Information

DocID

DocDate Undated

kd--Jason Slaughter Ph.D.--Targeted Individual Data 2------10/1/2023 1:02:23 PM--

Black-outlined Fields are required

DocKDStatus kd

__DocAuthorID

Case Contact Jason Slaughter Ph.D.

DocNumber

__DocInputBy Jason Slaughter PhD

__ProjectID Targeted Individual Data 2

DocName

Language eng English

Dialect English-US-SAE

Script LTR Roman LTR

DocDataFileType Text: json

DocDataAllType Text: Microtext

DocGenreType Tweet

Tweets

Chars

Test Chunking

First 100 in Set

First 5 Individual Tweets in Doc Data Records

Click Here to See Doc Data Records

--js------Undated--DN

● Targeted Jason Slaughter

kd--j--Mr Gumede--Tweet--Undated--DN1

Targeted Jason Slaughter

RT @VeengasJ: A video of yesterday incident #Hafeezbaloch and his family were targeted 45

kd--j--#TrudeauMustGo - Aldo--Tweet--Undated--DN2

Targeted Jason Slaughter

RT @Concern70732755: If a well regarded media source openly condemns Trudeaus 40

kd--j--PennySue--Tweet--Undated--DN3

Targeted Jason Slaughter

RT @_LibertyLady: Eunice Dwumfour, a 30-year-old New Jersey councilwoman, was found 37

kd--j--ShahDadBaloch--Tweet--Undated--DN4

Targeted Jason Slaughter

50

Figure 8. Before JSON upload.

Table 2. Handwriting analysis results.

Measurements	Non-Diseased	Diseased
Density	1	1
Height	49.3445	49.4417
Width	49.3329	49.4375
Slant	31.1875	16.6935
Curvature	193.355	193.758
Concavity	0	0
Elliptical	0.999793	0.999815
Circular	1.2312e−10	1.2318e−10

RQ2: What are the individuals' handwriting characteristics when they do not feel targeted? The non-diseased column of Table 2 describes this.

RQ3: Are there any significant differences between the results from RQ1 and RQ2? Differences are noted in the handwriting between the Diseased and Non-Diseased columns of Table 2. Slant offers the most significant deviation in the handwriting analysis performed.

3. Assumptions

The assumption is that all three RQs will be answered given the data samples available.

4. Limitations

The study faces potential limitations primarily related to the effectiveness of the coding and the machine-learning algorithms used for analyzing handwriting samples. The accuracy of the results is contingent upon the sophistication and calibration of these technological tools. Another significant constraint could be the disparity in the sample sizes between handwriting collected in 1999 and those from 2020. This temporal variation might introduce biases or affect the generalizability of the findings, as handwriting styles and the conditions under which they were collected may have evolved. These factors combined could influence the robustness and applicability of the study's outcomes in real-world settings.

5. Ethical Assurances

The data collection process for this study was meticulously designed to avoid gathering any personally identifying information about the participants, ensuring that privacy and confidentiality were maintained throughout. As such, this article does not contain or generate any publicly identifiable information (PII) about the respondents, except the names listed in the acknowledgments section. This approach reinforces the commitment to ethical research practices by safeguarding participant anonymity and minimizing the risk of privacy breaches.

6. Conclusions

This article delves into the complex relationship between individuals who perceive themselves as targeted and their subsequent potential to become unintentional insider threats. It builds upon a foundation of previous research that has identified both medical and psychological issues as contributing factors that may lead individuals to feel targeted. Such perceptions can significantly alter behavior in ways that are pertinent to the detection of insider threats.

The study underscores the critical need for insider threat programs to integrate medical and psychological expertise. By incorporating insights from these fields, the article highlights how certain conditions, such as urinary tract infections (UTIs) and sleep disorders, may skew an individual's perceptions, making them feel threatened.

Furthermore, the research aims to broaden the scope of current insider threat detection methods by including medical conditions as a critical variable. It proposes using handwriting analysis as a novel diagnostic tool to identify subtle behavioral shifts that might indicate an insider threat. This innovative approach seeks to enhance detection capabilities and foster a more holistic understanding of the factors influencing insider threats, thus contributing to more effective and nuanced security measures.

The study underscores the potential of integrating medical diagnostics into security protocols, providing a novel approach to understanding and mitigating insider threats.

Overall, the study advocates for a broader, interdisciplinary approach to insider threat detection, integrating medical, psychological, and cybersecurity measures to understand better and mitigate risks posed by individuals who feel unjustly targeted.

Declaration

The author's affiliation with The MITRE Corporation is provided for identification purposes only and is not intended to convey or imply MITRE's concurrence with or support for the positions, opinions, or viewpoints expressed by the author.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Slaughter, J. and Charles, K. (2023) A Survey of Unintentional Medical Insider Threat Category. *International Journal of Computer Science and Information Technologies*, **14**, 20-24.

[2] Slaughter, J., Chaski, C.E. and Charles, K. (2024) Emotion Analysis Based on Belief of Targeted Individual Supporting Insider Threat Detection. *International Journal of Science and Research Archive*, **11**, 226-237. https://ijsra.net/content/emotion-analysis-based-belief-targeted-individual-supporting-insider-threat-detection

[3] Chaski, C. (1997) ALIAS Technologies. ALIAS Technologies. https://aliastechnology.com/