Test #N - NAME *[Please Duplicate Before Filling Out]*

In Short: Describe the goal of the test in 1-3 sentences.

Why: Describe why this test will be helpful in identifying CIB in 1-3 sentences.

How: List the steps for how this test could be built.

1.
2.
3.

References: List or link to any studies that refer to or explore concepts related to the above methodology.

-
-
-

Related concepts: Are there any additional uses this test could help identify?

-
-
-

EXAMPLE 1: Test #1 - Copypasta

In Short: This test scans for identical strings of repeated text. The test provides the content of repeated text strings, the number of times the text strings are repeated, and the usernames/unique post numbers corresponding to the repeated text.

Why: Many networks of bots or human users will simply copy and paste identical text to save time and brainpower when conducting information campaigns.

How:

1. Parse text via ngrams analysis, looking for the smallest length (by word count) of any text appearing more than once. It may be advisable to set a minimum size for ngrams. For example, ngrams of length three (three words) may be the minimum length scanned for.
2. Continue identifying ngrams by increasing length (i.e. if ngrams of length three were the starting length analysis, now scan for ngrams of length four).
3. Continue until the longest ngram appearing more than once is found (i.e. there are no longer ngrams than that in the dataset).
4. Spawn data into this template spreadsheet, with each page belonging to a ngram length (start with shortest).

References:

- Copypasta explanation

EXAMPLE 2: Test #6 - Levenshtein Distance

In Short: Use Levenshtein Distance, a method of identifying how different two strings of information are, to test for bad actors trying to pass themselves off as credible sources. Levenshtein Distance refers to the minimum number of single character changes required to turn one word into another.

Why: Misinformation that looks like it comes from a credible source is more likely to trick users and spread.

How:

1. Extract the relevant text (usernames, article links, etc.)
2. Compare that text to known experts or publications (Surgeon General, New York Times, etc.)
3. Text that meets a similarity threshold is flagged as suspicious.

References:

- This algorithm has been used to detect email scammers trying to appear as a common contact or legitimate service by changing one character in an email domain. http://www.jcomputers.us/vol9/jcp0902-26.pdf
- This 2019 paper also used it and the derived Damerau Levenshtein Distance to detect “hoax” news. https://iopscience.iop.org/article/10.1088/1742-6596/1524/1/012035/pdf
- One challenge with this method is that a large percentage of impersonated misinformation comes in the form of photoshopped images of articles, so this method would not help with detecting that.

Related Concepts:

- Social media impersonation; Phishing