Create a Python program called Domain\_Analyzer+.py that analyzes email datasets for security threats. The program should:

1. Create an EmailAnalyzer class with methods to load and analyze CSV email data

2. Include domain analysis to track sender domains and calculate entropy

3. Analyze email addresses, usernames, and usage patterns

4. Extract text features using TF-IDF vectorization for clustering using 4 clusters

5. Perform K-means clustering on emails and visualize with matplotlib

6. Calculate domain age using WHOIS lookups

7. Import the VT-PY module to check domain reputation using VirusTotal API

8. Analyze email content for scam indicators (monetary terms, urgency, credentials)

9. Detect suspicious URLs and shortened links

10. Calculate a comprehensive threat score using multiple factors from the previous and below steps

11. Generate visualizations (pie charts, bar charts) of the spam or other email threat analysis

12. Create a detailed text report of all findings, including highly detailed and informative security recommendations based on the machine learning data

The program should handle various file encodings, use NLTK for text processing, and generate both visualizations and a comprehensive analysis report file providing detailed security recommendations based on the findings.

**AI/ML Features Added to the "+" Version**

The "+" version enhances the standard Domain Analyzer with several AI/ML capabilities:

1. **Text Feature Extraction & NLP**:
   * Uses TF-IDF vectorization to convert text into numerical features
   * Applies NLTK for tokenization and stopword removal
   * Analyzes content patterns through NLP techniques
2. **Unsupervised Machine Learning**:
   * Implements K-means clustering to identify patterns and group similar emails
   * Discovers natural groupings of emails without predefined categories
   * Extracts characteristic terms for each cluster
3. **Dimensionality Reduction**:
   * Uses Principal Component Analysis (PCA) for 2D visualization
   * Reduces high-dimensional text features to two dimensions for visualization
4. **Intelligent Pattern Recognition**:
   * Implements sophisticated pattern detection for scam categorization
   * Uses pre-defined pattern dictionaries for monetary terms, urgency words, etc.
   * Implements multi-category classification for scam types
5. **Advanced Threat Intelligence**:
   * Uses a weighted scoring model with multiple factors
   * Implements entropy calculation to measure domain diversity
   * Provides predictive threat levels based on multiple indicators
6. **Visualization Intelligence**:
   * Automatically generates appropriate visualizations based on data characteristics
   * Uses color-coding for threat levels and correlation displays
   * Creates intelligent cluster visualizations with domain annotations

These enhancements make Domain\_Analyzer+ significantly more powerful than the standard version by adding machine learning capabilities, pattern recognition, and advanced statistical analysis to provide deeper insights into potential email threats.