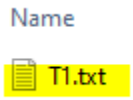
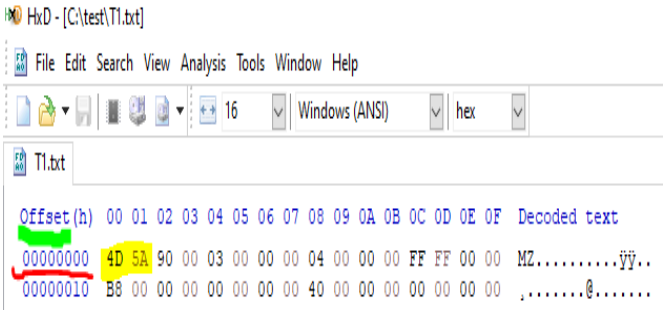
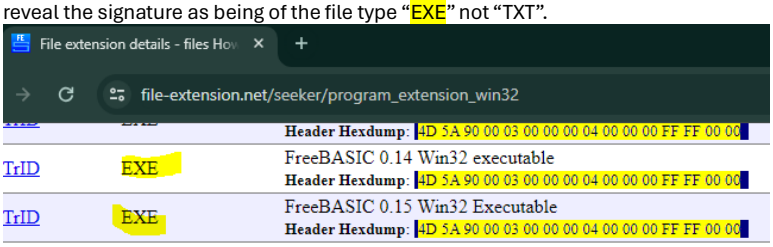
Title:	File Signature Verification Steps
Purpose:	Verify file type
Reason:	Threat actors hide the true file type to avoid detection
Author:	Darrell Clark
Date:	5-19-24

Step 1.	Load the file being examined into a hex editor.  Example file	 Hex editor used in this example
Step 2.	Compare the file extension T1.txt to the file signature header displayed in the hex editor. The file signature displayed in the hex editor shows the real file format “4D 5A” which is the signature for an “.exe” file extension. The “.exe” was changed to “.txt” to hide the true file format. The file needs to be quarantined and investigated further.	
Notes	The file signature header is revealed in the first line of hex digits below the “Offset” line. If you do not recognize the hex digit signature do a google search using the hex digits in line 00000000 and compare the results with the written file extension (in this example it is T1.txt)if they do not match quarantine the file and investigate further.	For example, a google search using the file signature hex digits from line 00000000 4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 reveal the signature as being of the file type “EXE” not “TXT”. 
Notes	The file signature is also referred to as the files “magic number”.	An example of a threat actor hiding the file extension is with a phishing attack using the “Right-to-Left Override” technique. More information on this technique can be found at: Masquerading: Right-to-Left Override, Sub-technique T1036.002 - Enterprise | MITRE ATT&CK®