

# Perform a Strings Search using BinText

***ILABS***  
***CEH PRACTICAL***



Software programs include some strings that are commands to perform specific functions such as printing output. Strings communicate information from a program to its user. Various strings that could represent a program's malicious intent, such as reading the internal memory or cookie data, are embedded in the compiled binary code.

Searching through strings can provide information about the basic functionality of any program. During malware analysis, search for malicious strings that could determine the harmful actions that a program can perform. For instance, if the program accesses a URL, it will store that URL string.



## Aim

BinText is a text extractor that can extract text from any file. It includes the ability to find plain ASCII text, Unicode text, and Resource strings, providing useful information for each item

Here, we will use the BinText tool to extract embedded strings from executable files.



## Other String Extraction tools

- ✓ FLOSS (<https://www.fireeye.com>)
- ✓ Strings (<https://docs.microsoft.com>)
- ✓ Free EXE DLL Resource Extract (<https://www.resourceextract.com>)
- ✓ FileSeek (<https://www.fileseek.ca>)

DEMO



THANKS