**5.2 Section 2 - Methodology updated.**

5.2.1 Malicious Obfuscated PDF File Analysis:

To create a code snippet that can be detected by our YARA rule, we need to craft a PDF file that contains obfuscated JavaScript code and matches the conditions specified in the rule.

First, ensure we have **Node.js** installed on your system. Then, follow these steps:

**1.Create a simple example of a PDF file with obfuscated JavaScript code** that should be detected by our YARA rule and save this JavaScript code to a file, for example, `**obfuscated\_code.js**`.

A computer screen shot of a program

Description automatically generated

**2.Install `pdfkit`:**

Now, we will create a PDF file using this JavaScript code and name it `**obfuscated\_pdf\_sample.pdf**`.

To create the PDF file, we can use a tool like `**pdfkit**` in Node.js

A screenshot of a computer program

Description automatically generated

**3. Create a Node.js script (e.g., `generate\_pdf.js`) with the following code:**

A screen shot of a computer

Description automatically generated

**4. Run the script:**

A screen shot of a computer code

Description automatically generated

After running the script, a new file named `**obfuscated\_pdf\_sample.pdf**` will be created. This PDF contains obfuscated JavaScript code and should be detected by the given YARA rule when scanned it.

A screenshot of a computer

Description automatically generated

**5. Yara\_Obfuscation Rule:**

A screenshot of a computer program

Description automatically generated

A screen shot of a computer program

Description automatically generated

A screen shot of a computer code

Description automatically generated

**6. Examination of the obfuscated PDF file using our yara rule:**

A computer screen shot of a computer code

Description automatically generated