Basic Static Analysis

**\*\*\*The samples used in this lab are actual malware. Do not analyze on a system unfit for analysis\*\*\***

Using some of the skills we covered in the first week of class (strings, sandboxes, hashing, file, etc.), answer the following questions using the malware samples provided. For each prompt, provide a screenshot showing how you came to your conclusion. Add an explanation if you think it is necessary.

Remember to defang URLs or domains. For example, the DSU website would be hxxps[://]dsu[.]edu instead of dsu.edu or https://dsu.edu. Then, it is not clickable.

**Follow the lecture video instructions to acquire the files.**

## Sample: fileone.bin

1. What is the MD5 hash of fileone.bin?
2. What type of file is fileone.bin?
3. What malware family is this file associated with?

## Sample: e5b6a70fec4fd42919225607b0eb1ec5.bin

**Note:** this file behaves differently for different users/machines/times. The prompts below reference this run in particular: <https://app.any.run/tasks/3c19d0b9-c035-4e11-92f4-f36aa83b7b3e/>

1. Is this file packed? With which packer?
2. A Microsoft Cabinet file is created – what type of information is in this file? (note: /F is the argument for directives, not the file itself)
3. What malware family is this file associated with?

## Sample: 349d13ca99ab03869548d75b99e5a1d0.bin

1. What type of file is this?
2. What process is launched to retrieve the second stage?
3. What malware family is this file associated with?

## Sample: 13d8f19c8847ad9fb7df3929214e4931.bin

1. What domain does this malware attempt to interact with? (Do not navigate to the domain)