# Assignment No.2

## CS-5051 Malware Analysis and Detection

**Submission Deadline: Saturday 23rd April until 4:59 pm on Google Classroom**

**Total Marks: 100**

**AIM of this assignment is to write an Analysis Report using Ghidra.**

**Description:**

In this assignment, you have to do analysis of any of four unpacked malwares using Ghidra listed below:

1. Gen:Heur.PonyStealer.4
2. Dropped:Trojan.Dropper.Agent.VOE
3. Trojan.GenericKD.3652107
4. Password-Stealer ( 003bbfec1 )
5. Gen:Variant.Ransom.Cerber.171
6. in32/Tnega.bXRKZUB
7. W32.SecretKAN.Trojan
8. Backdoor.TXLK-8101

**Questions you have to answer in your report**

Following are the list of questions you must have to answer in your report.

1. What are the different segments or sections in case of each malware?
2. What are different functions, imports and exports of each Malware?
3. What is flow of functions in case of each malware? Is there any suspicious function? Give detail (name, arguments, call mechanism) of suspicious functions?
4. What DLL's any malware includes? Are there any suspicious functionality called by these DLL's?

**Important:**

- For any help or confusion, you people can email at jawad.hassan@nu.edu.pk.
- Write an effective and detailed report in word format.
- Do not plagiarize. If found ***ZERO*** marks will be assigned.
- Late submission will also result in ***ZERO*** credit. **Best of Luck ☺**