**Answer the following questions and capture the flag:**

* What is the MD5 hash of the file?

56213d836485ad7afa5ef262085c4a2e

* What is the SHA256 hash of the file? (Hint: use hash calculator tool)

3e1d415ec17716efd58d98caa618648f8f3276b230f6ea193378a4e79845e317

* What file does this program drop? (Hint: use tools like regshot or procmon)

DYNAMO.EXE-1617DEFC.pf

* What registry entry did the program create? (Hint: use tools like regshot or procmon)
* What is the mutex name was created to prevent the program from having multiple instances? (Hint: use tools like procmon)

1617DEFC.pf

* To where does this program externally connect? (Hint: use tools like FakeNet-NG, Wireshark, BurpSuite)
* What is the flag? (Hint: The flag was divided in 4 parts)

Part 4->R\_X-Force

2.PcsCompu\_8c

3. RealtekU\_12