

**Group A**

Q1

This is an encrypted malware, and the starting bytes contain the decryption routine, which will decrypt the body of malware at run-time on the fly.

Q2

Lecture 14, slides 17-20

Q3

Lecture 16, slide 37-38

**Group B**

Q1

It could be a polymorphic or metamorphic malware. Polymorphic malware encrypts the body with a random key and differently mutates the decryption routine for each sample. Metamorphic malware does not use encryption, but directly mutates the virus body for each sample. In both cases, code mutation only changes the looks, not the functionality. Hence run time behaviour is same for all samples.

*Note: They can discuss either of the two.*

Q2

Lecture 14, slides 21-23

Q3

We could do run time detection – by monitoring the queries to see if they confirm to a normal pattern. Any query containing suspicious parameters will be rejected by database server.