Static and dynamic malware analysis exercise

Questions

1) What should be the VM configuration before malware analysis?
2) What are the limitations of static and dynamic malware analysis?
3) Why do we need to emulate network connectivity?
4) Can a malware escape the VM?
5) Find more disassemblers and debuggers tools and list them

Hand-On labs

Write a detailed report a using the tools and techniques we learned to analyze the suspected files (static and dynamic)

Lab 1

Files:

1) financials-xls.exe
2) budget-report.exe

Write a report that will be divided into two parts(or more): Static and Dynamic analysis.
In each step write what you found based on the guidelines.

Guidelines:

- IoC
    - URLs, IPs, domains, packed?, files created, registry keys, process, HTML pages, HTTP requests, DNS requests, hashes
- Online resources
    - VirusTotal, hybrid-analysis
- Strings
- Sections permissions
- Suspicious DLLs, suspicious functions
- Malware persistency
    - Registry keys?
- Resources
    - Images, icons, documents
- System changes, network traffic, etc
- Based on the analysis:
    - What the malware is doing?

- What kind of malware?