Objectives of Malware Analysis of Documents

Why malicious document?

What to look for?

- URLs to download second payload
- Commands, eg, Powershell, Javascript, wscript, etc
- Filenames – what it is downloaded and where
- Embedded file signatures, eg, PE header with MZ magic bytes

Virtual Machines