1 Introduction

Velociraptor is a data acquisition tool that can be used to gather information from a machine under investigation. To minimise modification of the original evidence, it is strongly recommended to run the executable from a USB stick or a network share that can be mounted from the target machine. The output of velociraptor will be saved to the partition/folder from which velociraptor was run and the size of this output can be several hundreds of MB, hence it is important to choose a partition with enough free space.

2 Preparation (on separate machine)

1. Obtain the IBM Security X-Force version of Velociraptor from IBM Security X-Force IR consultant working with you on this case.
2. Depending on whether target machine has a physical USB port or not, either:
   - Copy received file on USB stick.
   - Copy received file on network share that can be mounted on target machine.

3 Information capture (on Windows target machine)

1. Mount the network share where Velociraptor was unzipped or connect USB stick to target machine.
2. Open in Explorer USB/Network share where Velociraptor was copied.
3. Right-click on "velociraptor-<versioning_info>.exe" and select "Run as administrator"
4. A terminal window will open where progress of the script can be followed.
5. At the end of the gathering process the terminal window will close.
6. The data gathered by Velociraptor will be found in the same folder as the Velociraptor executable, the format of the name of this file will be <hostname>_triage.zip. This file is ready to be sent to IBM Security X-Force IR.

4 Delivering files to IBM Security X-Force IR

1. Compressed archive is ready for delivery to IBM Security X-Force IR team via the agreed method of delivery.
2. Use method approved within your organization to securely erase velociraptor output after the file was delivered to IBM.