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)

- Obtain the IBM X-Force version of Velociraptor from X-Force IR consultant working with you on this case.
- Depending whether target machine has a physical USB port or not, either:
  - Ccopy 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)

- Mount the network share where Velociraptor was unzipped or connect USB stick to target machine.
- Open in Explorer USB/Network share where Velociraptor was copied.
- Right-click on "velociraptor-<versioning_info>.exe" and select "Run as administrator"
- A terminal window will open where progress of the script can be followed.
- At the end of the gathering process the terminal window will close.
- 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 X-Force IR.
- Use method approved within your organization to securely erase velociraptor output after the file was uploaded to Box and/or Aspera.

4 Delivering files to IBM X-Force IR

- Compressed archive is ready for delivery to IBM X-Force IR team via the agreed method of delivery.