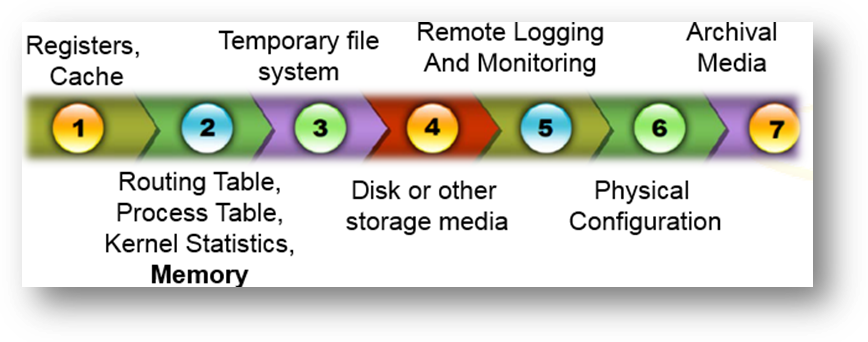
**Lab: Memory Image**

**Introduction**

Regardless of the level of information and efficiency of analysis, the system live analysis is not considered as the first option as the digital forensics investigator are advised to do not work on original evidence as there are always risk as follow:

* If the system is connected to a network, it may be remotely wiped by attacker.
* Examiner's tools and acts may overwrite data in the victim machine and cause data loss or modifications.

**Creating and backing up a forensic image helps prevent loss of data due to original drive failures.** When **collecting evidence**, the collection should proceed from the most volatile to the least volatile as shown in the figure below:



As shown in the figure above, the **physical memory or RAM** is one of the most volatile data in computer, thus memory imaging plays an important role in digital forensics investigation.

**Requirements**

* Windows Operating System
* Infected windows 10 on VM
* FTK Imager (<https://accessdata.com/product-download/ftk-imager-version-3.4.3>)
* Belkasoft Live RAM Capturer (<https://belkasoft.com/ram-capturer>?)
* Magnet RAM Capture (<https://www.magnetforensics.com/free-tool-magnet-ram-capture/>)

**Data Collection Preparation**

**USB Write Blocker**

Write protection – Ratool

**Disk Wiping Tool**

The data must be collected in a forensic sound manner. For instance, no data must be recorded in victim machine. Make sure to create the memory image in external storage such as pen drive which is forensically wiped based on method 2 which is explained in the link below:

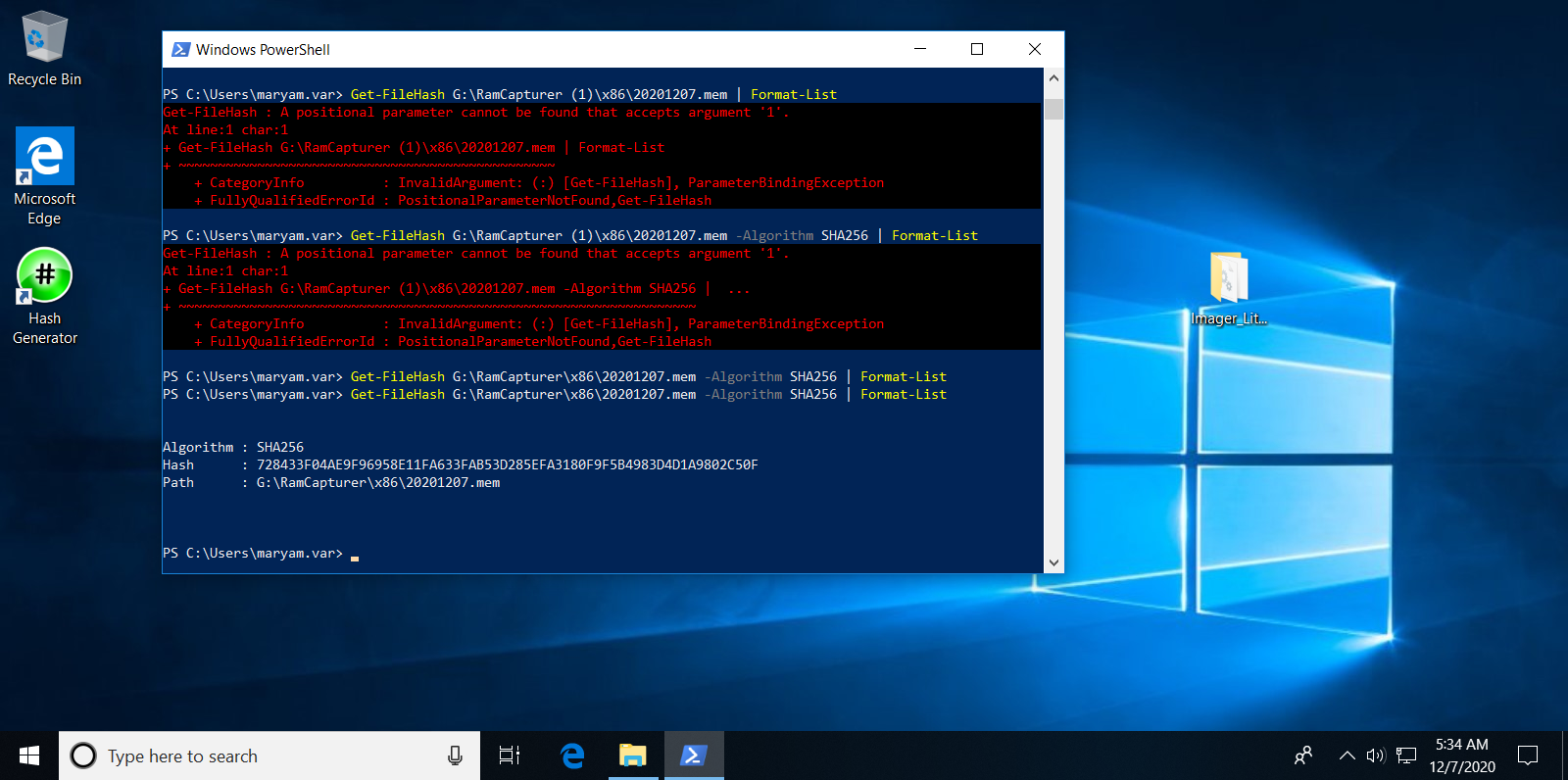
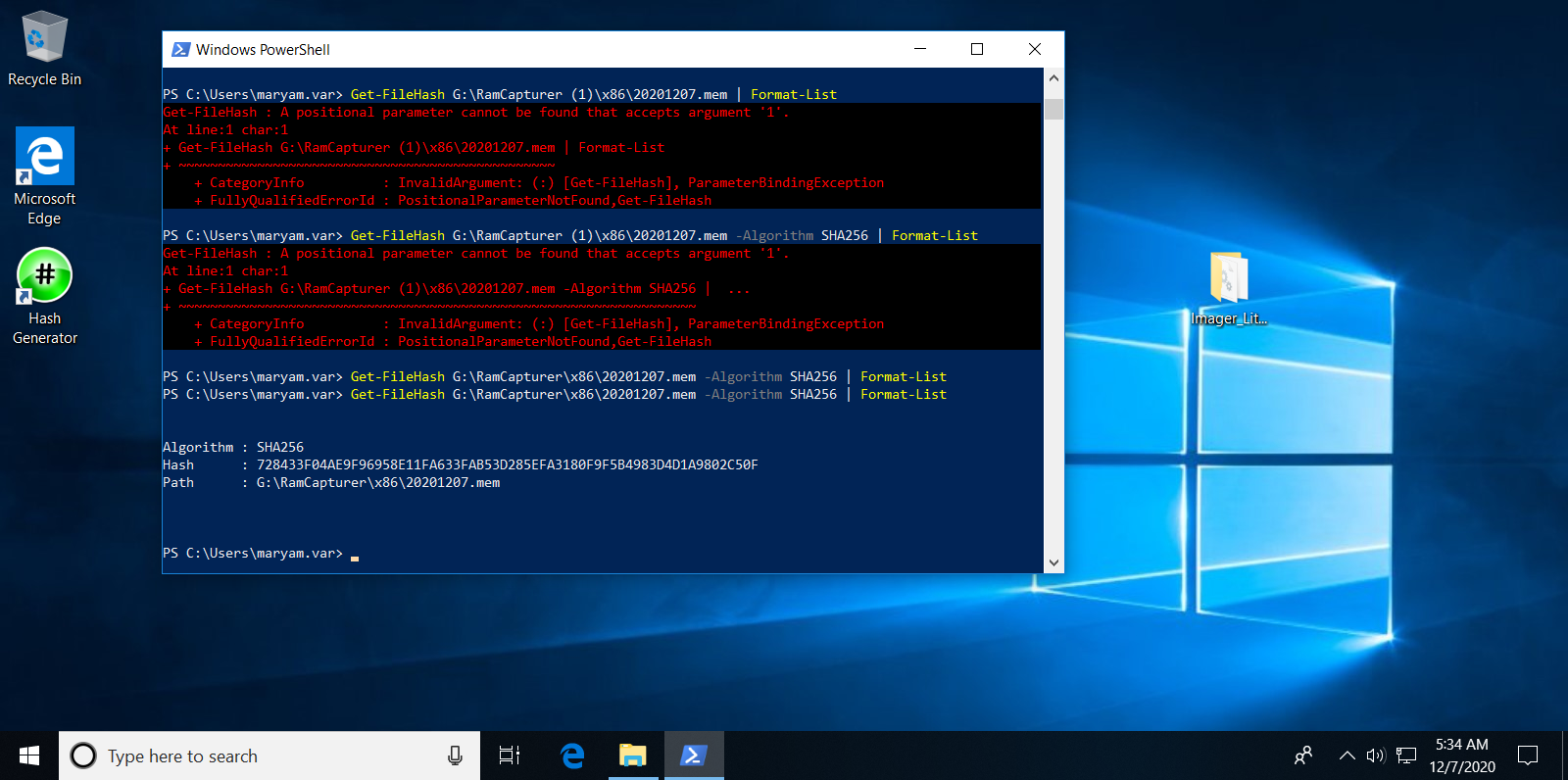
CCleaner: <https://support.piriform.com/hc/en-us/articles/204043884-Using-CCleaner-s-Drive-Wiper>

**Sdelete**

**Creating hash value**

Get-FileHash

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/get-filehash?view=powershell-7.1>



**FTK Imager**

The Forensic Toolkit Imager (FTK Imager) is a forensic imaging software package distributed by AccessData. FTK imager, available for free from Access Data, to capture a **live memory dump and the page file (pagefile.sys) which is used as virtual memory storage for Windows**.

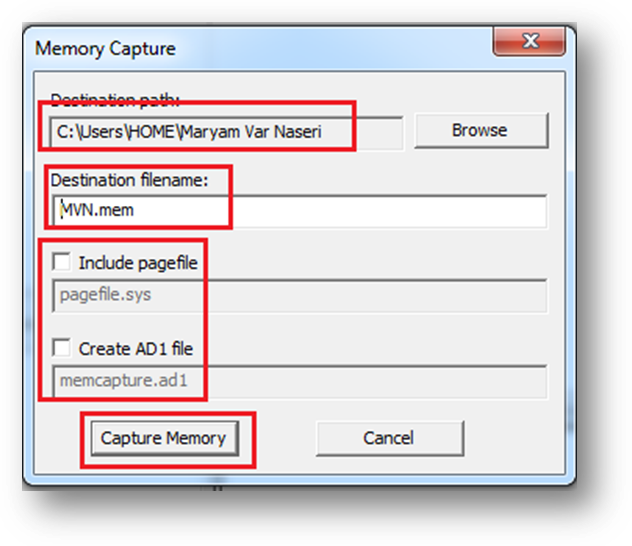
1. Download the FTK Imager form the link below

<https://accessdata.com/product-download/ftk-imager-version-3.4.3>

1. Fill the registration form
2. The download link will be send to your email address
3. Install FTK imager to your system.
4. Copy the FTK Imager folder to a forensically cleaned USB drive (Make sure the USB size must be more than the victim machine memory size).
5. Attach the USB to the victim machine and run the FTK Imager
6. Select **Capture Memory** from **file** menu.
7. Select location to store memory image and click on capture memory

Access Data

Virtual memory



**Options:**

* include the page file (virtual memory)
* Create an AD1 file which is AccessData's proprietary data type (memory image that can only analyzed by **access data tools (it gives tools to help you to analyze computer)** and may not recognized by other forensics tools.).

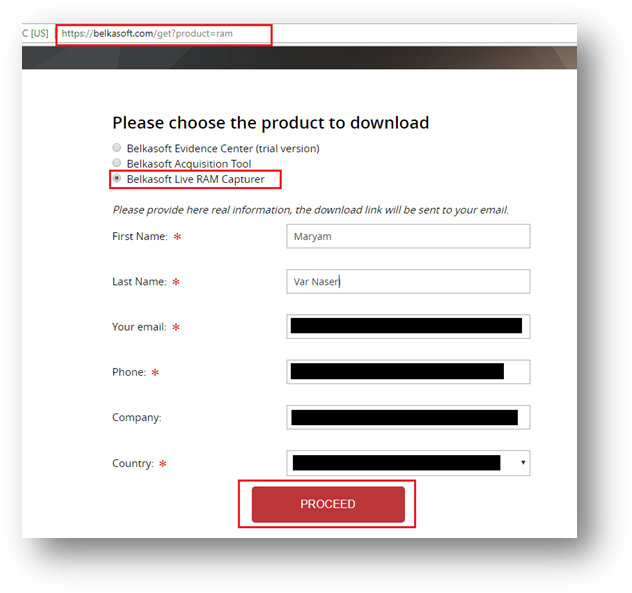
1. Wait while the FTK create memory image
2. Create hash value of the memory image.

**Belkasoft Live RAM Capturer**

Belkasoft Live RAM Capturer is a tiny **free forensic tool** that allows to reliably extract the entire contents of computer’s volatile memory – even if protected by an active **anti-debugging** or **anti-dumping** system.

1. Download the Ram Capture from the link below:

<https://belkasoft.com/ram-capturer>?



1. Depends on the type of target machine copy either 32bit or 64bit version of the belkasoft on the forensically cleaned USB
2. Connect the USB to the target machine and execute the ram capture exe file
3. Click on the capture button
4. Wait while the memory image is creating
5. Create hash value of the memory image.

**Magnet RAM Capture**

Magnet RAM Capture supports both 32 and 64 bit Windows systems including XP, Vista, 7, 8, 10, 2003, 2008, and 2012. It will acquire the full physical memory quickly and leave a small footprint on the live system being analyzed.

1. Download the Magnet Ram Capture from the link below:

<https://www.magnetforensics.com/free-tool-magnet-ram-capture/>

1. Copy the Magnet Ram Capture to the cleaned USB
2. Connect the USB to the target machine and execute the exe file
3. Click on I Accept to continue.
4. Leave the segment size to Don’t Split, select the image location and name and click start
5. Wait while the memory image is creating
6. Create hash value of the memory image.

**Answer the questions below and submit your work.**

**Question1:** Why we need to use more than one tools to create the memory images?

**Question2:** research about the aforementioned tools and provide a comparison on advantages and disadvantages.

**Question3:** what are the examples of **memory analysis tools** available on the market?

**Question4:** compare the available memory analysis tools and justify the one we should use.