1. How could memory be acquired? Describe the methods and their respective pros and cons. (35)

Hardware-based

In Hardware-Based Acquisition, physical devices or specialized tools are used to directly extract data from the hardware components of a system, such as the RAM chips. These tools are not dependent on the software of the system, which includes the operating system and any installed applications.

Advantages:

- **Reliability**: Since hardware-based acquisition operates independently of the system's software, it can capture all the information stored in the system's memory without being affected by any software-level restrictions or modifications, including those caused by malware or other malicious activities. This makes the data captured through this method highly reliable.
- **Resistance to Anti-Forensic Techniques**: As this method does not interact with the system's software, it is not susceptible to anti-forensic techniques that operate at the software level. For example, some types of malware attempt to hide their presence or activities by modifying the information returned by software-based memory acquisition tools.

Disadvantages:

- **Cost and Accessibility**: Hardware-based acquisition methods require specialized equipment and expertise, which can make them expensive to use. Additionally, these methods require physical access to the system's hardware, which may not always be possible or practical. For instance, in cases where the system is located in a remote location or in a secure data center, or when dealing with cloud-based systems where the physical hardware is shared among multiple users, hardware-based acquisition may not be feasible.
- **Risk of Damage**: Since hardware-based acquisition involves physically interacting with the system's hardware, there is a risk of causing physical damage to the system.

Software-based

In this approach, forensic tools or applications running on the system are used to capture the contents of the system's memory. These tools are often able to extract the full contents of memory, which can then be analyzed offline for evidence.
Alternatively, only the memory of a specific process can be extracted, e.g. for analyzing malware.

Such tools basically work with loaded kernel modules that access OS-specific APIs. For this reason, root access to the system is required.

Advantages:

- **Ease of Deployment**: Since software-based tools don't require physical access to each machine, they are significantly easier to deploy across multiple machines. In a situation where many systems need to be analyzed (such as in a large-scale incident response scenario), software-based tools can be more efficient and scalable.

- **Remote Accessibility**: Software-based acquisition tools can be used remotely, which is a major advantage in cases where the systems to be analyzed are distributed or physically inaccessible. As long as remote access is possible and the system is running, a memory dump can be initiated.
- **Flexibility**: Software-based tools can offer greater flexibility in terms of the specific data that is captured from memory. Depending on the tool, it might be possible to target specific memory areas or processes, reducing the overall amount of data that needs to be captured and analyzed.
- **Minimal Impact on User**: If used correctly, software-based acquisition can be carried out with minimal visible impact on the user. This can be particularly important in situations where the user is not aware of the investigation.

Disadvantages:

- **Dependence on System State**: Because software-based acquisition tools run on the system, they are dependent on the state of the system to function correctly. If the system is unstable or compromised, the reliability of the memory acquisition can be impacted.
- **Potential for Altering Evidence**: Running a software-based acquisition tool on a system necessarily alters the state of the system to some degree, which can potentially alter or destroy evidence.
- **Very System Dependent**: The functionality and the results of the tools are very dependent on the used OS version, configuration of the OS, installed hardware, ..., and may vary.

VM-based

If the system to be examined is a virtual machine, there are basically 2 options for memory acquisition:

- Software-based tools within the guest VM
- Functions provided by the virtualization software used, such as pausing/suspending, snapshots or APIs.

Acquisition using the hypervisor is one of the simplest methods, which is also not very invasive, but also has disadvantages:

- **Network**: When pausing or suspending a VM, open network connections are closed, therefore these information would later be missing in the memory dump.
- **Dump Format**: Depending on the product, the memory dump is saved in different proprietary formats, which must be converted into usable formats before analysis (Volatility can still process most of them)

2. How could a memory dump provide information on open network connections, ports etc.? Why? (35)

Network related data can be analyzed because the system needs to maintain the state of these while the computer is running.

Therefore all these information are included inside a memory dump.

For example, a Linux system will keep track of:

- **Network Interface Configurations**: Information about each network interface on the system, such as the interface name (e.g., eth0, wlan0), IP address, MAC address and current status (up or down).
- **Active Network Connections**: Details about each active network connection, including the protocol (TCP, UDP), local and remote IP addresses with port numbers, and the connection state (e.g., ESTABLISHED, LISTENING, CLOSED). This can help identify who the system was communicating with at the time of the dump.
- **Listening Ports**: Information about which ports the system is listening on. This can help identify services running on the system.
- **Routing Table**: The system's IP routing table, which determines how packets are forwarded between different networks. This can help understand the network setup of the system.
- **ARP Cache**: The Address Resolution Protocol (ARP) cache, which maps IP addresses to MAC addresses. This can help identify other systems on the same local network.
- **Network-related Process Information**: Information about processes that were using the network.

3. Why is a hibernation file useful in memory forensics? (30)

A hibernation file essentially represent a snapshot of the system's RAM at the point of hibernation.
When a computer enters hibernation, the operating system saves the current state of the system – including all data in RAM – to a file on the hard drive (Windows usually) or to a swap partition (Linux usually). When the system wakes up from hibernation, it can restore this state and pick up where it left off.

Here's why that's useful in memory forensics:

- **Persistence of Data**: Unlike RAM, which is volatile and loses data when the system is powered off, a hibernation file is stored on the system's non-volatile storage and persists until the system enters hibernation again. This means that you can potentially recover valuable data from the hibernation file long after the system has been powered off or even if the system has been rebooted (as long as it hasn't entered hibernation again). Examples are open BrowserSessions, Crypto Containers, Bitlocker disks, …
- **Potentially Less Intrusive**: In software- and hardware forensics, you often have to run commands or tools on the target system to acquire data, which can alter the system state and potentially destroy evidence. However, if a hibernation file is already available, you can simply copy the file for analysis, which is less likely to alter the system state.

It's important to note that analyzing a hibernation file can be complex because the data in the file is often compressed or encrypted, so special tools or techniques are needed. For instance, Volatility provides a plugin (imagecopy) that can convert a hibernation file to a raw memory dump format that can then be analyzed with various other plugins.

But there are also some drawbacks to consider:
Before a system hibernates, the DHCP configuration (if any) is released and any active connections are terminated. As a result, networking data in hibernation files might be incomplete. Also, during this time, malware can remove itself from memory so that you're not able to detect its presence in the hibernation file.[1]

[1] The Art of Memory Forensics, Page 99