Jere Mike C. Hipos

BSIT 4-1

PROBLEM 1: A client's computer is experiencing frequent blue screen of death.

1.**Initial Diagnosis:** The first step is to gather information. I'd begin by asking the user about recent changes to the computer, such as new software installations or hardware upgrades. Then, I would boot the computer into Safe Mode to see if the problem persists. I'd also check the Windows Event Viewer for specific error codes or log entries related to the blue screens, as this can often pinpoint the exact cause. Potential hardware components that might be causing the issue include a faulty RAM module, an overheating CPU or GPU, a failing hard drive or SSD, or a malfunctioning power supply unit (PSU).

2.**Troubleshooting Process:** My troubleshooting process would start with **diagnostic tests**. I'd run a memory diagnostic tool to check the RAM, a hard drive diagnostic tool to check for bad sectors, and a temperature monitoring program to check for overheating components. If these tests don't reveal a problem, I'd proceed to a **physical inspection** of the hardware. I'd open the computer case to check for loose cables, improperly seated RAM sticks or expansion cards, and excessive dust buildup on fans and heat sinks. I'd also check the CPU fan to ensure it's spinning properly and that the thermal paste is still effective.

3.**Communicating with a Non-Technical Client:** To explain my findings to a non-technical client, I would avoid jargon and use simple analogies. For example, instead of saying, "The RAM is faulty," I might say, "The computer's short-term memory is having trouble, which is causing it to forget what it's doing." I would describe the problem and the proposed solution in a clear, concise way, focusing on the impact on them and the next steps. I would also provide an estimated timeline for the repair and the associated costs.

PROBLEM 2. A user Is complaining about slow computer performance.

1. Detailing Steps to Identify the Root Cause

To identify why a computer is slow, I'd first check for **malware** and viruses by running a full system scan with up-to-date antivirus software. Next, I would examine the **startup programs**. Many applications automatically launch when the computer boots, which can significantly slow down the startup process and overall performance. I'd use the Task Manager (in Windows) to review and disable unnecessary programs. Finally, I would check the **hardware limitations**. A computer's performance is often limited by its hardware, especially the amount of **RAM**, the

type of **storage drive** (HDD vs. SSD), and the **CPU's** speed. I'd check the resource monitor to see if any of these components are consistently maxed out, which would indicate a bottleneck.

2. Optimizing the System's Performance

Once I've identified the root causes, I'd take specific steps to optimize the system. If I found malware, I'd remove it. For excessive startup programs, I would disable all non-essential ones. If the hardware is the bottleneck, I would recommend upgrades. For instance, upgrading from a traditional Hard Disk Drive (HDD) to a Solid-State Drive (SSD) provides a massive speed increase for boot times and application loading. Increasing the amount of **RAM** can also significantly improve performance, especially for users who multitask or use memory-intensive applications. I'd also recommend freeing up disk space by deleting unnecessary files and using a disk cleanup tool.

3. Importance of Regular Maintenance and Software Updates

Regular system maintenance and software updates are crucial for preventing future performance issues. **Software updates** often include performance improvements, bug fixes, and critical security patches that protect the system from new threats. Failing to update software can leave the computer vulnerable to malware that could slow it down. **Regular maintenance**, such as running scheduled disk cleanup, defragmenting the hard drive (if it's an HDD), and regularly scanning for viruses, helps to keep the system running smoothly. These habits help to prevent the build-up of temporary files and fragmentation that can slow down performance over time.

Problem 3: A small office network is experiencing intermittent internet connectivity problems.

When a small office network has intermittent connectivity issues, a systematic troubleshooting methodology is essential to isolate the problem. The first step is to check the most common culprits. I would start by physically inspecting all **network cables** to ensure they are securely plugged in and aren't damaged. A loose or faulty cable is a frequent cause of connection drops. Next, I'd check the **router's status lights**. The lights on a router provide valuable information; for example, a blinking or solid "Internet" light usually indicates a good connection, while an orange or red light often signals a problem. I'd then check the **modem's status lights** for similar signals.

To further test the network connectivity, I would use a variety of tools and techniques. A simple but effective method is to use the **ping command** from a computer connected to the network. Pinging a reliable external site like Google's DNS server (ping 8.8.8.8) can determine if the problem is with the local network or the internet service provider (ISP). If the ping fails, the

issue is likely external. If it succeeds but websites are still slow, the problem might be related to DNS. I'd also use **ipconfig** (on Windows) or **ipconfig** (on macOS/Linux) to verify the computer has a valid IP address and to check the default gateway. Another useful tool is **tracerouting** (or tracer on Windows), which can help identify where along the path from your computer to a destination server the connection is failing, pointing to a potential bottleneck or point of failure.

PROBLEM 4. A client has accidentally deleted important files.

1. Data Recovery Methods and the Importance of Backups

The method for recovering accidentally deleted files depends on three main factors: the type of file, the storage device it was on, and the time since deletion.

Type of File: Smaller, unfragmented files are generally easier to recover because they are stored in a single, continuous block on the disk. Larger files, which are often broken up and scattered across the disk, are more difficult to piece back together.

Storage Device: The type of storage is critical. With traditional Hard Disk Drives (HDDs), deleting a file doesn't actually remove the data; it just marks the space as available. This makes recovery possible with specialized software. However, with Solid-State Drives (SSDs), a command called TRIM often erases the data shortly after deletion to maintain performance, making file recovery nearly impossible.

Time Since Deletion: The most crucial factor is how long ago the file was deleted. The longer you wait, the higher the chance that the space the file occupied will be overwritten by new data, making the original data unrecoverable. For this reason, the first and most important step is to stop using the device immediately to prevent any new data from being written.

To recover the files, I would first use file recovery software like Test Disk to scan the drive. If this fails, the next option is to contact a professional data recovery service, although this can be expensive. This is why regular data backups are so important. An effective strategy should follow the 3-2-1 rule: 3 copies of your data, stored on 2 different media types (e.g., an external hard drive and cloud storage), with 1 copy kept off-site.

2. Communicating the Risks of Data Loss and the Benefits of Backups

When talking to a client about the risks of data loss, I would avoid technical jargon and use a relatable analogy. I might compare their data to something valuable and physical, like important documents, photos, or a personal diary. I would then explain that data can be lost due to many things besides accidental deletion, such as a hardware failure, a malware attack, or even physical damage from a fire or flood. This helps the client understand that their data is not inherently safe just because it's digital.

I would then explain the benefits of a comprehensive backup plan. A backup plan provides peace of mind and is a form of insurance against these events. It ensures that even if something goes wrong, they can restore their data and get back to work with minimal downtime. The key benefit is **business continuity**: a good backup plan ensures that a single event won't cripple their operations or lead to the loss of irreplaceable personal memories or critical business information.