**Introduction to Computer Systems and Platform Technologies**

Study Period 3, 2021 – CPT160

Assignment 2

|  |  |
| --- | --- |
| **Student Name:** | Adam Mutimer |
| **Student Number:** | S3875753 |

Table of Contents

[Part A: System Architecture – 120 Marks 3](#_Toc88482030)

[1. For each of the 8 components labeled A, B, C, D, E, F, G, H, I and J in the above diagram: 3](#_Toc88482031)

[A. 3](#_Toc88482032)

[B. 3](#_Toc88482033)

[C. 4](#_Toc88482034)

[D. 4](#_Toc88482035)

[E. 4](#_Toc88482036)

[F. 5](#_Toc88482037)

[G. 5](#_Toc88482038)

[H. 5](#_Toc88482039)

[I. 5](#_Toc88482040)

[J. 6](#_Toc88482041)

[K. 6](#_Toc88482042)

[L. 6](#_Toc88482043)

[Pricing Question 6](#_Toc88482044)

[a) What is the best price approximately) of this motherboard, from Australian computer shops/Ebay? 6](#_Toc88482045)

[Part B: Building a Recommended Platform Machine – 78 Marks 6](#_Toc88482046)

[Part C: Recent Technology – 40 Marks 6](#_Toc88482047)

[1. What are the differences between 3D NAND and 2D NAND memory? 6](#_Toc88482048)

[2. Explain the difference between NVMe and M.2 6](#_Toc88482049)

[3. Give details of purchasing a 1TB NVMe/M.2. Details include the price and its specifications. E.g., read/write speeds. You must also describe the type of flash memory e.g., SLC or MLC, EMLC, TLC, QLC etc. 6](#_Toc88482050)

[4. Give details of purchasing a 1TB SATA/M.2. Details include the price and its specifications. E.g., read/write speeds. You must also describe the type of flash memory e.g., SLC or MLC, EMLC, TLC, QLC etc. 6](#_Toc88482051)

[Part D: Question 4 – Advanced Question (30 Marks) 7](#_Toc88482052)

[a) Explain the concept of virtual memory. Do you worry about if you are going to have enough virtual memory addresses (explain your answer)? Do you worry about if you are going to have enough physical addresses, or is there going to be any concern in terms of performance (explain your answer)? 7](#_Toc88482053)

[b) Assuming a cache miss, a data item is requested with its virtual memory address. Illustrate clearly how the corresponding page is located by using the page table directly. Explain if there are performance issues with the direct use of page table, and how the performance can be improved 7](#_Toc88482054)

[Bibliography – 26 Marks 7](#_Toc88482055)

[Part A) 7](#_Toc88482056)

# Part A: System Architecture – 120 Marks

## For each of the 8 components labeled A, B, C, D, E, F, G, H, I and J in the above diagram: [Added Missing K & L]

From Inspection of the images and vague reference to a “moderner commercial laptop motherboard” for a “Microsoft Surface Laptop” I believe this motherboard/logic board from my personal experience repairing laptops to be for a “Microsoft Surface 2” Model 1769.

This model came in a few revisions in relation to the processor (Intel i5/Intel I7), Ram and SSD Capacity so without an exact part number for this board the following answers cannot be 100% specific in all cases.

As I have both Boardview files and a schematic of this model motherboard part number: M1088058-002, I will be using that to reference any part numbers and component details.

## 

#### What is the name generally given to that component?

The name generally given to this component is CPU or APU, in this case I believe this is a APU (Accelerated Processing Unit) which combines both a CPU and a GPU.

#### What is that component designed for and given details about the component

As previously mentioned, I believe this is an APU which combines both a CPU and a GPU. In this case its designed to perform the roles of both CPU which processes information from application with various instructions and a GPU which allows it to render images on the computers display.

This Model of Surface had the following APU Options:  
Core i5-7300U – Intel HD Graphics 620  
Core i7-8650U – Intel UHD Graphics 620  
Core i7-8650U – Intel UHD Graphics 620

Both i7 Options also had models which included a Discrete graphics (GPU) of either:  
NVIDIA GTX 1050  
NVIDIA GTX 1060  
  
But as I previously mentioned this is not the case with the motherboard shown for this assessment.

## 

#### What is the name generally given to that component?

The name generally given to this item is RAM or System Memory

#### What is that component designed for and given details about the component

RAM (Random Access Memory) is a critical part of a computer system as it allows applications to store information for both reading and writing on a short-term basis, depending on the user’s workload higher capacity ram or even faster clocked ram may be required.

In the case of this motherboard, we are looking at 4 DDR3 modules, this model come in two variants’ both an 8GB and 16GB models were available.

## 

#### What is the name generally given to that component?

To the layman this would look simply like any other IC (Integrated circuit). In this case this IC is a TPM (Trusted Platform Module)

#### What is that component designed for and given details about the component

A Trusted Platform Module/TPM is a secure crypto-processor made for the sole purpose of carrying out various cryptographic operations and is used by various operating systems (when enabled and functional) to encrypted users’ data.

For example, a bit locker driver on a system with a TPM enabled cannot easily be copied to another system with or without a TPM as each TPM has a unique key and the new system would be unable to decrypt the data, however Microsoft has several recovery methods that work around this such as using a Microsoft account on the creation of the bit locker drive.

## 

#### What is the name generally given to that component?

These are more integrated circuits; however, these 4 chips are part of the touch screen circuitry for touch and gesture detection and are part of the I/O of this system (Input/Output)

#### What is that component designed for and given details about the component

These components are designed to detect a user touching the touchscreen and converting that user input into binary singles that system will understand.

In this case we have 3x BGA82 surface mount IC’s and a single BGA64 surface mount IC which connect to each other and the 80pin “Sense connector” ribbon cable above on the left of the selected area and the 50 pin “Drive connector” ribbon cable above on the right on the selected area

## 

#### What is the name generally given to that component?

This is generally referred to as an IC. In this case it is a PMIC (power management integrated circuit)

#### What is that component designed for and given details about the component

A PMIC (power management integrated circuit) is designed regulated and manage power output to an upstream circuit or IC. In this case the two PMICs in question are manufactured by Texas Instruments with manufacture part number TPS62085RLTR and cost about $3 when purchased singly.

This PMIC is designed to take a voltage of 2.5v – 6v and output 0.8 – 6v with a max output draw of 3 Amps, This PMIC is part of the SSD power circuit.

## 

#### What is the name generally given to that component?

Electronically Erasable Programmable read-only memory OR EEPROM for short.

#### What is that component designed for and given details about the component

This component is designed to store information or be used as memory by a microcontroller and functions similar to other forms of computer memory however it doesn’t require power source to retain data, these are commonly used to store firmware/software such as a BIOS (basic input/output system).

In the case of this motherboard as its part of the onboard WIFI controller circuitry it most likely contains firmware used by the Wireless + Bluetooth controller.

This particular EEPROM is made by Atmel with a part number of AT24C16D-MAHM-T and is designed to store information for 100 years with a total of 16K of storage space and uses the I2C interface. This chip costs $0.43 if buying a single chip.

## 

#### What is the name generally given to that component?

This is generally referred to as a flash rom or IC Flash

#### What is that component designed for and given details about the component

This component is designed to be used as storage. This particular component on this motherboard is manufactured by WindBond Electronics with a manufacturer part number: W25Q128JVPIQ.

This IC Flash uses NOR Memory 16MB X 8 supporting a total storage capacity of 128MBs and supports the following interface types SPI - Quad I/O (Serial Peripheral Interface – Quad Input/Output), QPI (Intel QuickPath Interconnect), DTR (Dual Transfer Rate). This IC Flash costs $2.77 when purchased individually.

This IC Flash is part of the UEFI (Unified Extensible Firmware Interface) circuitry and is used to store the UEFI bios firmware.

## 

#### What is the name generally given to that component?

#### What is that component designed for and given details about the component

## 

#### What is the name generally given to that component?

#### What is that component designed for and given details about the component

## 

#### What is the name generally given to that component?

#### What is that component designed for and given details about the component

## 

#### What is the name generally given to that component?

#### What is that component designed for and given details about the component

## 

#### What is the name generally given to that component?

#### What is that component designed for and given details about the component

## Pricing Question

### What is the best price approximately) of this motherboard, from Australian computer shops/eBay?

# Part B: Building a Recommended Platform Machine – 78 Marks

# Part C: Recent Technology – 40 Marks

## What are the differences between 3D NAND and 2D NAND memory?

## Explain the difference between NVMe and M.2

## Give details of purchasing a 1TB NVMe/M.2. Details include the price and its specifications. E.g., read/write speeds. You must also describe the type of flash memory e.g., SLC or MLC, EMLC, TLC, QLC etc.

## Give details of purchasing a 1TB SATA/M.2. Details include the price and its specifications. E.g., read/write speeds. You must also describe the type of flash memory e.g., SLC or MLC, EMLC, TLC, QLC etc.

# Part D: Question 4 – Advanced Question (30 Marks)

## Explain the concept of virtual memory. Do you worry about if you are going to have enough virtual memory addresses (explain your answer)? Do you worry about if you are going to have enough physical addresses, or is there going to be any concern in terms of performance (explain your answer)?

## Assuming a cache miss, a data item is requested with its virtual memory address. Illustrate clearly how the corresponding page is located by using the page table directly. Explain if there are performance issues with the direct use of page table, and how the performance can be improved

# Bibliography – 26 Marks

## Part A)

**Mainboard Schematic and Boardview for M1088058-002 - $12.50 USD**  
*Accessed: 16/11/2021*  
<https://www.laptopschematic.com/microsoft-surface-1769-m1088058-schematic-boardview/>

**TPM/Trusted Platform Module**  
*Accessed: 16/11/2021*  
<https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview>

**Texas Instruments - TPS62085RLTR***Accessed: 16/11/2021*  
<https://www.digikey.com.au/en/products/detail/texas-instruments/TPS62085RLTR/5178707>

**Atmel - AT24C16D-MAHM-T***Accessed: 16/11/2021*<https://au.mouser.com/ProductDetail/Microchip/AT24C16D-MAHM-T?qs=sGAEpiMZZMvjAcTDbo5QTldnfDcTY8mplHurMrN7TM0%3D>

**WindBond Electronics - W25Q128JVPIQ**  
*Accessed: 16/11/2021*  
<https://www.digikey.com.au/en/products/detail/winbond-electronics/W25Q128JVPIQ/6819668>