**EMCS642 – Digital Forensics**

**(Mid Term Case Study – Individual Work)**

|  |  |
| --- | --- |
| **Maximum Mark Available**  | 100 |

|  |  |
| --- | --- |
| **Weighting of this coursework towards the Course mark (%)** | 20% |

|  |  |
| --- | --- |
| **Learning Outcomes Being Assessed** | Summarize how to conduct an investigation, including critiquing a case. |

|  |  |
| --- | --- |
| **Tutor this work is for**  | Dr. Maha Sabir |
| **Handout date** | 21st October 2021 |
| **Handin date** |  |
| **Expected handback date** |  |
| **Expected feedback date (if different from handback date)** | Two weeks after submission date |

|  |  |
| --- | --- |
| **Outline of Problem** | * Generate Master Boot Record (MBR) for physical drive and understand hexadecimal code using Win Hex tool.
* To understand how to analyse, review, and investigate digital evidence on image collected from suspected machine. Use the given E01 image file to obtain various information using Autopsy such as email messages investigation, number of certain documents, certain keywords, recovering deleted files, and producing HTML report.
 |
| **Detail of Questions** | **Please follow to Page # 2** |
| **What you should hand in**  | A complete report should be named as StudentID\_Name\_Report.pdf |
| **Rules** | While solving all parts, you have to:* + Answer all questions.
	+ Indicate the steps of solving the questions.
	+ Provide the screenshot of every step to get full marks.
	+ You are requested to upload:
		- **SINGLE PDF** file should be written in the given template (starting from Page#2). The report title page should mention the student's name and ID clearly.
 |
| **Guidelines/Length**  | There is no strict word limit.  |
| **Resources Required** | Autopsy, E01 image file, and Microsoft Word. |
| **Other information** | This Mid-Term case study must be an **individual work**, **not a group work**. |
| **Submission policy** | * For courses where electronic submission of assignments is required, it is the responsibility of the student to ensure that the instructor has received the assignment by the established due date and to ensure that the assignment submitted is the complete and correct version.
* Assignments should be submitted on the due date in order to receive full credit.
* Any work that has been submitted after a deadline has passed is classed as late except in cases where an extension has already been agreed.
* For **each day late**, the instructor will **reduce** the assigned grade by **1 mark**. The maximum delay will be **5 days** in total
 |
| **Plagiarism** | Your attention is drawn to the University Modular Framework Assessment Regulations regarding academic impropriety This covers cheating, attempts to cheat, plagiarism, collusion and any other attempts to gain an unfair advantage in assessments. The work you submit must conform to those regulations. |

**EMCS642 – Digital Forensics**

**(Mid Term Case Study) – Answer Template**

|  |  |
| --- | --- |
| **Student Name** |  |
| **Student ID** |  |

**PART-1 - Warm up Questions: 2 Marks**

**Task-1: Generate MBR of your machine physical drive, and fill the following table:**

**[1 Marks]**

|  |  |  |  |
| --- | --- | --- | --- |
| **Partition No.** | **File System Code** | **First Sector** | **No. of Sectors** |
| **Hex** | **Name** | **Hex** | **Decimal** | **Hex** | **Decimal** |
| 1 | 6E740000 |  | 65 79 20 4700 00 00 0000 00 00 0000 00 AC 01 |  | 6F 20 72 6500 00 00 0000 00 00 00B9 01 00 00 |  |
| 2 |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |
| **Paste Screenshot here:**Screenshot-1: Partition Table ViewScreenshot-2: Hexadecimal View |

** **

**Task-2: Create or gather Microsoft Excel (.xlsx), Microsoft Word (.docx), .gif, .jpg, .pdf, and .mp3 sample files. Record the hexadecimal codes for each file.**

**1 Marks**

|  |  |
| --- | --- |
| **File Type** | **Hexadecimal Code** |
| **Microsoft Excel (.xlsx)** |  |
| **Microsoft Word (.docx)** |  |
| **.gif**  |  |
| **.jpg** |  |
| **.pdf** |  |
| **.mp3** |  |

**PART-2 – CASE STUDY – 18 Marks**

**Important Notes:**

1. Image Link: <https://digitalcorpora.s3.amazonaws.com/corpora/scenarios/2009-m57-patents/drives-redacted/charlie-2009-12-03.E01>
2. Please use Autopsy version 4.19.1 that can be downloaded using the link <https://www.autopsy.com/download/>
3. Why Autopsy’s new version: Digital forensics tools are constantly improving in capabilities and functions. As a digital forensics’ examiner, you must learn how to use several tools so that if one tool fails, you can switch to another one.
4. Apart from Autopsy, you are free to use any tool as per the requirement, during your investigation.
5. Downloading and loading the file in Autopsy will take some time. Please remember, do not start analysis until the loading bar in Autopsy disappears (it means the file has been loaded successfully).
	1. Downloading Time: around 1hr

Wait till loading bar disappear

* 1. Loading time in Autopsy: around 50min



**Case Description:**

In this case, you will study and investigate copied image from a machine that was under the use of Mr. Charlie. The case belongs to two competitors’ companies; (i) M57.biz and (ii) Project2400 and the communication among their employees.

Both companies are famous for providing innovative and creative ideas to attract companies, inventors, as well as investors. Research and development were the main domain areas for both companies. These companies are always trying to launch new ideas to improve their revenues, and number of customers by generating quality work.

Mr. Charlie was an employee of M57.biz. The company was recently established and is working hard to give strong competition to other companies in the market. The company has a number of employees working under the supervision of the CEO. During the period of November 16, 2009, and December 9, 2009, the company was discussing new research ideas and was planning to publish two research patents. Mainly, Email was the communication channel in order to discuss the formal project ideas and assigned tasks to the team members. In addition, there were some other informal discussion topics that were part of their communication.

On the other side, the company Project2400 was a big competitor of Mr. Charlie’s company. With hard work and dedication, this company also established a reliable name in the market as a research and development industry.

The investigation was initiated after finding out that Mr. Charlie was allegedly involved in selling the ideas to one of the employees belonging to the competitor company. Surely, behind all of these illegal activities, Mr. Charlie’s main concern was to earn unlawful financial benefits (that is still not confirmed). According to the ch

arges applied on Mr. Charlie and during the preliminary investigation conducted internally, the company found him “guilty”. On the other side, Mr. Charlie was continuously denying the charges and recorded the following statements during initial investigations:

* 1. During a specific period of time (when some suspicious events happened), I was having some problems accessing my account.
	2. Several times, he called for technical support and even asked for remote assistance, then finally the problem was solved by getting help from the technical support team.
	3. In addition, he mentioned that he was planning for Christmas vacation with his friend “Alix” and I was busy with other activities.
	4. In addition, he further added in denying the charges on him that “I never been in contact with any person nor sent emails to the competitor company for selling my company’s ideas/files”.
	5. Finally, he said, “We were very happy that we received two new business contracts, one from Nitroba.com and the second from another company and all of us were working hard for those projects”.

The above are some important details about the case you are investigating. Now, the case has been delegated to you to proceed further based on the preliminary analysis. You are required to search for the evidences that can help to prove Mr. Charlie as “Innocent” or “Guilty”. Therefore, you have been given an image of Mr. Charlie’s machine acquired on 4th December 2009. You are guided to proceed as follows (but not limited to):

* Investigate email messages.
* Dig deep the documents specially related to Mr. Charlie machine.
* Search for the files sent and received by Mr. Charlie
* Investigate Mr. Charlie’s machine’s system files, desktop files, web searches, downloaded files and so on.
* Explore, use and show us your investigation by using “Communication” and “Timeline” investigation tools available in Autopsy (as shown in below picture) that can extract some hidden and useful information/graphs/bar.
* 

Following are the tasks you should provide answer for each with proper justification, screenshots, and explanation (if required):

**Task-1: Get Name, email and phone number of M57.biz company’s CEO. [1 Mark]**

|  |  |
| --- | --- |
| Name | Pat McGoo |
| Email Address | pat@m57.biz |
| Phone No. | 831-555-1234 |

**Task-2: Get whatever details you find about Nitroba Company’s CEO. [1 Mark]**

**Task-3: Discuss about the first meeting of both CEOs M57.biz and Nitroba CEO. When and where? [1 Mark]**

**Task-4: What was the main work assigned to Mr. Charlie from his boss regarding the Nitroba project. [1 Mark]**

**Task5: Search and investigate Three main evidences that can prove Mr. Charlie guilty.**

**[6 Marks]**

**Task6: According to Mr. Charlie statement, he said: [2 Mark]**

“We were very happy that we received two new business contracts, one from Nitroba.com and second from another company and all of us were working hard for those projects”.

The question is, according to the answer of Task-4. Investigate evidence that he was really working for his company’s tasks or not? Add screenshots to prove your answers

**Task7: One of the main reasons behind the illegal act performed by Mr. Charlie that his boss's behavior with the employee was not good. Do you agree? Support your answer with evidence. [1 Mark]**

**Task8: Mr. Charlie’s opinion about his boss was very good. Do you agree? Support your answer with evidence. [1 Mark]**

**Task-9: As he mentioned about his friend “Alix” and preparation for Christmas vacation. Is he lying? Does this event occur before suspicious activity or later? [1 Mark]**

**Task10: Show us some interesting facts using “Communication” and “Timeline” tools in Autopsy as shown in following picture:**



**Task 10.1. Using Communication tool, find out who has strong or weak relationships with the help of Email IDs. [1 Mark]**

**Task 10.2. Using a Timeline tool, create a timeline for an event that can help to collect strong evidence during investigation. [1 Mark]**

**Task11: Generate HTML Report and put the screenshot below. [1 Mark]**