Assignment Brief and Front Sheet PGT

This front sheet for assignments is designed to contain the brief, the submission instructions, and the actual student submission for any WMG assignment. As a result the sheet is completed by several people over time, and is therefore split up into sections explaining who completes what information and when. Yellow highlighted text indicates examples or further explanation of what is requested, and the highlight and instructions should be removed as you populate ‘your’ section.

This sheet is only to be used for components of assessment worth more than 3 CATS (e.g. for a 15 credit module, weighted more than 20%; or for a 10 credit module, weighted more than 30%).

**To be completed by the student(s) prior to final submission:**

Your actual submission should be written at the end of this cover sheet file, or attached with the cover sheet at the front if drafted in a separate file, program or application.

|  |  |
| --- | --- |
| **Student ID or IDs for group work** | **e.g. 1234567** |

**To be completed (highlighted parts only) by the programme administration after approval and prior to issuing of the assessment; to be consulted by the student(s) so that you know how and when to submit:**

|  |  |
| --- | --- |
| **Date set** | October 2024 |
| **Submission date (excluding extensions)** | Monday 11th November 2024 by 12:00pm |
| **Submission guidance** | To be submitted electronically via Tabula |
| **Late submission policy** | If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.  For **Postgraduate** students only, who started their **current course before 1 August 2019**, the daily penalty is **3 marks** rather than 5. |
| **Resit policy** | If you fail this module and/or component, the University allows students to remedy failure (within certain limits). Decisions to authorise resits are made by Exam Boards. These will be issued at specific times of the year, depending on your programme of study. More information can be found from your programme office if you are concerned.  If this is **already a resit** attempt, this means you will not be eligible for an additional attempt. The University allows as standard a maximum of two attempts on any assessment (i.e. only one resit). Students can only have a third attempt under exceptional circumstances via a Mitigating Circumstances Panel decision. |

**To be completed by the module leader/tutor prior to approval and issuing of the assessment; to be consulted by the student(s) so that you understand the assignment brief, its context within the module, and any specific criteria and advice from the tutor:**

|  |  |
| --- | --- |
| **Module title & code** | WM9C1-15 Digital Forensic Investigation [MAIN SIT] |
| **Module leader** | HS Lallie |
| **Module tutor** | HS Lallie |
| **Assessment type** | Report |
| **Weighting of mark** | 80% |

|  |  |  |
| --- | --- | --- |
| **Assignment brief** At the end of this document | | |
| **Word count** | The maximum word count is 3200 words.  +10% will be allowed on this word count without penalty. If you exceed this word count by more than 10% to 30%, a penalty of 10% on the original mark awarded will be applied. If you exceed this word count by more than 30%, the final mark will be capped at the pass mark.  The word count does not include tables, however, you must use tables carefully. Improper use of tables, e.g. as an opportunity to consume more words will be penalised.  The word count does not include references, or appendices. Although appendices are allowed, these will not be marked and only referred to add context, please do not place into the appendices anything which you materially rely upon in your submission. |
| **Module learning outcomes (numbered)** | Critically evaluate relevant digital forensic characteristics of selected digital electronic devices  Apply scientific techniques to investigate digital artefacts against a realistic brief  Analyse evidence uncovered through an investigation  Report on digital forensic evidence against a given legal context |
| **Learning outcomes assessed in this assessment (numbered)** | LO2, LO3, LO4 |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Criteria** | **91-100** | **81-90** | **71-80** | **61-70** | **51-60** | **41-50** | **31-40** | **0-30** |
| **Investigation (46%)** | Comprehensive, excellent and systematic investigation of artefacts/evidence; detailed investigative insight demonstrated. Advanced level of investigatory techniques applied. Publishable with no changes. | Comprehensive systematic investigation of artefacts/evidence; detailed investigative insight demonstrated. Advanced level of investigatory techniques applied. Publishable with minimal changes. | Systematic investigation of artefacts/evidence; detailed investigative insight demonstrated. Advanced level of investigatory techniques applied. Publishable with some changes. | Reasonably organised investigation of artefacts/evidence; some investigative insight demonstrated. Reasonable level of investigatory techniques applied. | Reasonably organised investigation of artefacts / evidence; some investigative insight demonstrated. Some level of investigatory techniques applied. | Often disorganised investigation of artefacts / evidence; modest investigative insight demonstrated. Modest investigatory techniques applied. | Disorganised investigation of artefacts / evidence; little investigative insight demonstrated. Few if any investigatory techniques applied. | Disorganised investigation of artefacts / evidence; little investigative insight demonstrated. Few if any investigatory techniques applied. Little or no merit in the submitted work. |
| **“Investigation” is mapped to LO2 and LO3** | | | | | | | | |
| **My Opinion (20%)** | Comprehensive, excellent and systematic projection of opinion; opinion comprehensively connected to investigation. All elements requiring an opinion presented comprehensively. Publishable with no changes. | Excellent and systematic projection of opinion; opinion strongly connected to investigation. All elements requiring an opinion presented well. Publishable with minimal changes. | Very good systematic projection of opinion; opinion strongly connected to investigation. All elements requiring an opinion presented well. Publishable with some changes. | Good systematic projection of opinion; opinion connected to investigation. All elements requiring an opinion presented well. | Acceptable projection of opinion; opinion modestly connected to investigation. Most elements requiring an opinion presented well. | Modest projection of opinion; opinion weakly connected to investigation. Some elements requiring an opinion presented reasonably well. | Weak projection of opinion; opinion weakly connected to investigation. Some elements requiring an opinion presented poorly. | Weak or no projection of opinion; opinion very weakly - if at all - connected to investigation. Some elements requiring an opinion presented poorly. Little to no merit in the submitted work. |
| **“My Opinion” is mapped to LO3 and LO4** | | | | | | | | |
| **Methodology (18%)** | Exceptionally well-written methodology. Written exceedingly well to enable successful peer review. Key methodological elements described exceedingly well. Publishable with no changes. | Very well-written methodology. Written very well to enable successful peer review. Key methodological elements described very well. Publishable with minimal changes. | Very well-written methodology. Written very well to enable successful peer review with minimal changes. Key methodological elements described very well. Publishable with some changes. | Very well-written methodology. Written well to enable peer review with a few further explanations and changes. Key methodological elements described well. | Reasonably well-written methodology. Methodology would require further explanation to enable peer review. Many, not all, methodological elements described reasonably well. | Many shortcomings in the methodology. Methodology would require significant further explanation to enable peer review. Many methodological elements missing. | Too many shortcomings in the methodology. Methodology lacks sufficient detail to enable peer review. Significant methodological elements missing. | Too many shortcomings in the methodology. Methodology so poorly written that it would not be possible to pass this to peer review. Significant methodological elements missing. Little to no merit in the submitted work. |
| **“Methodology” is mapped to LO2** | | | | | | | | |
| **Presentation (16%)** | Exceptionally well-written report showing professional skills in creativity and good design; no grammar or spelling issues; excellent use of headings, sub-headings, figures, and tables. Publishable with no changes. | Excellent report showing good skills in creativity and design; no grammar or spelling issues; and excellent use of headings, sub-headings, figures, and tables. Publishable with minimal changes. | Well-formulated structure to the report; no grammar or spelling issues; writing style is clear; and good use of headings, sub-headings, figures, and tables. Publishable with changes. | Clear structure to the report; few spelling and grammar errors. Sentences of appropriate length and punctuation; and good headings, sub-headings, figures, and tables. | Basic structure and formatting of the report; some spelling and grammar errors; and some use of headings, sub-headings, figures and tables. | Minimal and unclear structure and formatting of the report; some spelling and grammar errors; and poor use of headings, sub-headings, figures and tables. | Inadequate structure and formatting of the report; many spelling and grammar errors; some text is verbose; no or incorrect use of headings, sub-headings, figures and tables. | Unclear structure and formatting of the report; numerous spelling and grammar errors; writing style has many issues; and no use of headings, sub-headings, figures and tables. |
| **“Presentation” is mapped to LO4** | | | | | | | | |

|  |  |
| --- | --- |
| **Academic guidance resources** | In class |

|  |
| --- |
| **Where to get help:**   1. Talk to your module tutor if you don’t understand the question or are unsure as to exactly what is required. 2. Study, Professional and Analytical Skills (SPA) Moodle site – we have a lot of resources on this website with workbooks, links and other helpful tools.  <https://moodle.warwick.ac.uk/> 3. There are also numerous online courses provided by the University library to help in academic referencing, writing, avoiding plagiarism and a number of other useful resources. <https://warwick.ac.uk/services/library/students/your-library-online/> 4. If you have a problem with your wellbeing, it is important that you contact your personal tutor or wellbeing support services <https://warwick.ac.uk/services/wss> |

# Assessment brief

At 06:10 on the 15th September 2024 a warrant was executed by West Midshires Police (“WM Police”) at the home address of Andran Gratis Mercil (“The Suspect”).

The arrest took place following an assault on John Doe, also known as ‘BirminghamDrop’ and further intelligence linking The Suspect to the distribution of Class A (red), Class B (blue), and Class C (green) Jelly Beans the distribution of which were made illegal in 2007.

## The law

Subject to sufficient evidence being produced, WM Police believe they may be able to refer the case to the CPS under section 20, Offences against the person act 1861 and the Misuse of Drugs Act 2007 wherein Class A drugs attract the highest custodial sentence, and Class C drugs attract the lowest custodial sentence.

## Exhibits

Two items were recovered during the arrest: a laptop and a lens-damaged dashcam. Both items have been imaged and are supplied to you by West Midshires Police as:

A laptop computer was seized during the arrest. The computer was imaged and is supplied to you by WM Police as:

**Radovan-Marc-Andran.img**

MD5 checksum: **ee502c20fb1468c55449b5b84ff53a44**

SHA1 checksum: **c3aa79dddaf6177bb59726a4a9c4e2531b2ae068**

**Dashcam.E01** (comprising 7 files)

MD5 checksum: **7dc6816622a33143ebda7f0342dc4970**

SHA1 checksum: **11c9a4ebca348f01119123e438eeb565b11c7d86**

Additionally, case files have been created and supplied by the case technician with all relevant ingest modules activated.

## Interview

During initial interview, the Suspect stated that he:

* Does not know the victim
* Has never met or spoken with the Victim
* Was in Leicester on the day of the assault
* Has not been involved with the possession and / or supply of drugs

## Task

Your senior officer has updated your task and asks you to examine the two new exhibits and:

1. Determine whether there is any evidence to connect the Suspect with the Victim.
2. Determine whether the Suspect was in the vicinity of the assault.
3. Consider each of the statements made by the suspect in interview and identify any evidence to corroborate or refute these statements.
4. Determine and identify other suspects.
5. Report any other relevant issues.

The findings must be presented as an expert witness report, a template is provided in Appendix 3. You must not stray from the template.

**Important notes**

1. The case was created by HS Lallie between February-September 2024.
2. Two pre-ingested cases have been provided to you.
3. You do not have permission to convert any DFIs provided to you into virtual machines and/or operating those virtual machines. If you do, this will result in a reduction of marks.
4. The Windows exhibit was created in a virtual machine. Any artefacts relating to the virtual machine can be ignored.

If there are any other oddities that you believe may be related to the case simulation, please report them to [HL@warwick.ac.uk](mailto:HL@warwick.ac.uk).

# Special instructions

Do not include the Assignment Guidance and Front Sheet in the submission.

**Spelling/grammar.** Ensure that you spell check the submission, use a grammar checker and ensure that you proofread your work prior to submission. Spell/grammar checkers must be set to UK English, do not use ‘Americanised’ spellings.

**References.** References are to be included at the end of the report using the Harvard referencing system. You may also include a bibliography. Each reference must be connected to a citation within the main body of the report.

Do not attempt to hide text within JPEGs, this will be construed as an attempt to mislead the assessor.

**Coherence**. A poorly worded report will hide excellent content. The narrative should be easy to read, and arguments should be presented coherently and convincingly.

**Presentation.** At this stage in your studies, there is no excuse for poor presentation. You will not receive marks for presentation; however, your submission will be penalised for poor presentation.

**Formatting**. All figures and tables must be properly labelled and captioned. All pages must be numbered. Formatting must be consistently applied throughout the submission. Submissions that stray from this guidance may be penalised.

Appendices 1. Format for the coursework report

WMG Title page

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**Title of the action:** normally `Rex' in the case of a criminal case v Normally we use the parties surname. Example: Rex vs Smith.

**Court reference number:** The court reference number is a unique reference to the case. In the case of coursework, please make up a number.

**Final report of:** Student number, not name.

**Dated:** This is the date you submitted the report.

**Specialist field:** What is your specialist field - insert `digital forensics'.

**On behalf of the Claimant/Defendant** Who are you acting on behalf of - the claimant or defendant? Delete the one that does not apply.

**On the instructions of:** Who instructed you? In this case it was not a solicitor firm, a private entity or a corporate entity, it was WM police

**Subject matter:** Brief statement of case, e.g. `Assault on John Doe, 12-1-22’.

Here is an example of a completed front page.

**Title of the action:** Rex vs Doe

**Court reference number:** D1245f

**Final report of** 1243562 for **Barwickshire Crown Court**

**Dated:** 21-5-23

**Specialist field:** digital forensics

**On behalf of:** the Claimant

**On the instructions of:** WM police

**Subject matter:** Assault on John Doe, 12-1-22

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**Table of Contents**

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**1. Introduction**

Explain the purpose of the report. What has happened, what have you been asked to do? What are the objectives? Who is the suspect? Anything else?

**2. Investigation**

**2.1 Investigation Findings**

This is a substantive section in your report. This is where you explain what you found, but not necessarily how you found it, that comes in appendix 1. Organise this section into subsections.

Begin the section with an overview of the system you investigate. Set the scene, explain the system you investigated, the users, dates, file systems etc. Now you have set the scene, move onto the investigation.

An example of how you could develop the narrative in this section is as follows: “I analysed the emails sent between The Suspect and The Victim [A1.3] and found 23 emails which...” where [A1.3] is appendices 1, section 3 which is the methodology section, and which explains how you analysed the emails. Here is another example: “I found three items of malware on the system [A1.7]. The malware I found was...” where [A1.7] is appendices 1, section 7 which is the methodology section, and which explains how you analysed the malware. You do not explain methodology in the main body.

A small sample of evidence can be included here, fuller samples must go into an appropriate appendix.

Specific results of analysis such as shellbag, prefetch, jumplists etc must go here. Detailed overviews into the methodology.

**3. My opinion**

This section provides your opinion on the questions you were asked to answer. Take each question in turn and answer it.

You can also provide opinion on questions that you were not asked but which you believe are relevant.

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**Appendices**

**A1. Methodology**

**A1.1 Background**

State any background information relating to the DFI(s) that you investigated. This is a good point at which to provide basic forensic hygiene information.

Keep this section brief. Overall it should not exceed two pages. Do not use two pages if you do not need to.

**A1.2 Statement of methodology**

Use this section to explain HOW you found the evidence that you refer to in the Investigation section. Your investigation must be repeatable, but do not write this like a tutorial manual.

Explain the investigative environment, what did you do first?

So, if you analysed the emails, maybe you analysed them directly through the Autopsy tool, or maybe you felt an easier way of doing this would be through exporting the email into CSV, and analysing them through there. Maybe you used a third-party tool.

Keep this section brief. Overall, it should not exceed three pages. Do not use the full three pages if you feel you do not have to. A lot of this section can probably be completed during your tutorials, hint, pay attention in the tutorials…

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**A2. Chronology**

Juries (and markers of your coursework) like chronologies

\_\_\_\_\_\_\_\_ This is followed by a new page \_\_\_\_\_\_\_\_

**A3. Glossary of technical terms and tools**

\_\_\_\_\_\_\_\_ This is followed by new page(s) \_\_\_\_\_\_\_\_

**A4…. Other**

Include fuller samples of evidence, e.g. images, maps, tables of images etc.