Computer Science and Creative Technologies

Coursework or Assessment Specification

Module Details

Module Code	UFCFP4-30-1
Module Title	Computer Crime and Digital Evidence
Module Leader	Jay Murphy
Module Tutors	Dr. Lindsey Gillies, Mr. Hamza Attak
Year	2021 – 2022 20SEP/1
Component/Element Number	B/CW1
Total number of assessments for this module	2, i.e. Component A and Component B The current assesses Component B
Weighting	100% of Component B, 50% of total assessment
Element Description	Report – Technical Report

Dates

Date issued to students	19/10/2021
Date to be returned to students	10/02/2022
Submission Date	13/01/2022
Submission Place	Online via Blackboard (Assignments folder)
Submission Time	14:00 GMT
Submission Notes	You must submit your individual report as a compressed (zip file) Microsoft Word (.doc or .docx) or .pdf document via Blackboard. NO paper submission is required.

Feedback

Feedback provision will be	kept confidential and will be made via the Blackboard and/or myUWE. A summary about: a) aspects that were well done, b) aspects that were weak, incorrect or missing, and, c) pointers for improvement, will be given.

Contents

Module Details 1
Dates 1
Feedback 1
Contents 2
Section 1: Overview of Assessment 3
Section 2: Task Specification 3
Section 3: Deliverables – What to submit? 6
Section 4: Marking Criteria 7
Section 5: Feedback mechanisms 7
Appendices and Additional Information 8
Marking Criteria 9

Section 1: Overview of Assessment

This assignment assesses the following module learning outcomes:

- Assess tools and techniques for investigating computer crime enabling the identification of low level information structures and hardware file formats.
- Evaluate appropriate forensic computing investigative strategies and select available tools based on their appropriateness for a given investigation.
- Understand how to use software tools to investigate the contents of electronic storage devices
- Create reports that use a language and format appropriate to their use in a court of law.

The assignment is worth ***50%*** of the overall mark for the module.

Broadly speaking, the assignment requires you to write an individual report on the Encase Demonstration Case, i.e. "Hunter XP", showing not only report writing skills but also a knowledge of the technical aspects of forensic recovery and analysis.

The assignment is described in more detail in section 2.

This is an *individual* assignment.

Working on this assignment will help you to demonstrate your ability to investigate digital evidence using various digital forensic tools, and practice your report writing skills. If you have questions about this assignment, please post them to the discussion board on Blackboard:
https://blackboard.uwe.ac.uk/uwenav/ultra/courses/_340292_1/cl/outline

Aims of this assignment

The principle aims of this assignment are to allow you to demonstrate:

- The ability to investigate digital evidence to establish *facts* and *opinions*;
- Report writing skills.

Section 2: Task Specification

Scenario:
"A forensic image of a PC was delivered to your office on 19th October 2021 (14:30 GMT). You are asked to perform a digital forensic investigation of this image and produce a document that explains your findings. You are supposed to identify users and their actions

based on the facts you found in the image, and express your opinion about any crimes committed."

You will be provided with a copy of the EnCase demo forensic image file, i.e. you will be studying the "Hunter XP" evidence file.

You should:

- Investigate the evidence for potential criminal activity.
- Keep *contemporaneous notes* of your examination.
- Write *a report presenting the facts* you have discovered.
- Create *a timeline* of the sequence of significant events in the case.
- Write a brief *summary* of your *opinion* of what occurred, based *on the facts* you discovered.

Suggested time planning

Investigating case: 24 hours
Writing report: 16 hours

For information on how your work will be assessed, see Assessment (Marking) Criteria below.

Submission

You must submit your report as a Microsoft Word (.doc or .docx) or as a PDF document via Blackboard – NO paper submission is required. Please compress your report (zip file) before uploading it on Blackboard.

Details

Your report will comprise the following four Sections (see table below).

Note that apart from Section 4 there is no specified word count (word limit).

The size of deliverables (or Sections) 1-3 will depend on your findings during your investigation.

However, credit will be given to reports that are *concise* and *avoid unnecessary verbiage*.

You must submit ONE individual file (zip file) that consists of the following sections by the submission date indicated below:

Submission date: Thursday 13/01/2022 (deadline 14:00 GMT)

	Tasks - Sections	***Marks***	***Submission Date and Place***
1.	**Contemporaneous Notes** Your contemporaneous notes will document the steps you took to examine the evidence; they will probably be based on the template, provided on Blackboard (Assignments folder). Factors you need to consider are: i. The notes need to be sufficiently detailed to demonstrate that you have performed a complete and coherent examination, ii. Repeatability: The notes should be sufficiently detailed to allow an independent analyst to repeat your examination with the same results. iii. Dual verification: Choose 2 key evidence items, and provide their provenance, using 2 separate tools such as EnCase and Autopsy.	*30*	
2.	**A concise written summary of the evidence file you have studied.** This section of the report will typically be around 4-5 pages long and will document the most significant evidence items e.g. picture, document, email files, which you have identified within the forensic image. This section of the report should **document facts**, not opinion, for example, the presence of a picture file, rather than a discussion of how this file possibly arrived on the disk. You should include the bulk of the evidence items within an **appendix**, including a provenance block for each item.	*40*	
3.	**A timeline of the sequence of events that occurred during this potential crime.** The timeline should be clearly laid out to show what happened when, with appropriate comments. You should concentrate upon **the significant events** in the case. You should look for evidence corroborating that the times are correct (this evidence should be mentioned in Section 2).	*15*	

4.	**A statement of your *opinion* of what occurred during this crime.** This should be around 300 words and must not exceed 500 words. You should build your opinion based on the facts given in Section 2.	*15*	
	TOTAL	***100***	**13/01/2022** **Submit on Blackboard, AS ONE .DOC or .PDF file.**

Section 3: Deliverables – What to submit?

You must submit via Blackboard one zipped individual file that consists of the following four sections (listed in detail in "Section 2: Task Specification" in this document):

- Your contemporaneous notes [on a doc(x) or pdf file; use the Template provided on Blackboard]
- Your concise written summary of the evidence file you have studied [doc(x) or pdf file]. Also include in an Appendix the provenance of the evidence items you are referring to, and/or the EnCase report created after using EnCase reporting function.
- Your timeline of significant events [can be a doc(x), ppt(x), pdf file or any file that can be read on a standard Microsoft Windows 10 computer at UWE Bristol].
- Your statement of your opinion of what occurred during this potential crime [doc(x) or pdf file].

Please take a look at the checklist on the "Appendices and Additional Information" section (Page 7) to ensure you included all requested deliverables in your submission file.

The report must be submitted by the submission date indicated below:

Submission date: Thursday 13/01/2022 by 14:00 GMT.

Follow this link to get advice about how to submit your coursework via Blackboard:
https://info.uwe.ac.uk/online/Blackboard/students/guides/assignments/default.asp

Section 4: Marking Criteria

See the assessment criteria below (Page 9) for additional information on how your work will be assessed.

Written Work

Please note that all written work should:

- *Be properly researched and referenced (if needed) using the UWE Harvard method of referencing;*
- *Have all sources critically evaluated;*
- *Have word counts applied according to UWE regulations. Further information available here:* https://www1.uwe.ac.uk/about/corporateinformation/policies.aspx
- *Be professionally formatted in .PDF or .DOC(X) format.*

General Points

- *You should not expect to get any reminders from tutors about any of these responsibilities.*
- *You should familiarise yourself with UWE Academic Regulations with regard to assessment. These are available on the UWE Home page.*
- *Non submissions are covered by UWE Academic Regulations, and will be given zero marks.*

Section 5: Feedback mechanisms

Feedback will be given on 10/02/2022 via Blackboard and/or myUWE. The feedback document will provide a summary on: a) aspects that were well done, b) aspects that were weak, incorrect or missing, and, c) pointers for improvement.

Appendices and Additional Information

Submission items checklist

Submit ONE zip file containing the following:

- *Your contemporaneous notes [on a doc(x) or pdf file; use the Template provided on Blackboard]*
- *Your concise written summary of the evidence file you have studied [doc(x) or pdf file]. Also include in an Appendix the provenance of the evidence items you are referring to, and/or the EnCase report created after using EnCase reporting function.*
- *Your timeline of significant events [can be a doc(x), ppt(x), pdf file or any file that can be read on a standard Microsoft Windows 10 computer at UWE Bristol].*
- *Your statement of your opinion of what occurred during this potential crime [doc(x) or pdf file].*

Change log:
v1: 30/10/2020: (Added link to discussion forum and listed deliverables in Section 3) Released on Blackboard as moderated version addressing from moderator's comments.

Marking Criteria

NON-SUBMISSIONS are covered by UWE Regulations and generally attract zero marks.

Contemporaneous Notes

[85% – 100%)	Exceptionally detailed documentation.	Exceptional neutral investigative approach, professional language.	Exceptional accuracy; all evidence items are referenced properly.	Exceptional recording of every action taken; and every output produced.	All relevant tasks were successfully done. Additional processes recorded, remarkable evidence found.
[70% – 85%)	Very detailed notes. Records are also given in the Appendix, provided by the EnCase Documentation feature.	Neutral Investigation, impartial documentation.	All references are pointing to the correct items. No inconsistencies.	All aspects of the investigation are discussed; No questions are raised for the validity of the investigation.	All relevant tasks were successfully done/documented.
[60% – 70%)	Detailed notes for all aspects of the investigation.	Impartial approach in most actions taken.	Most evidence items are referenced correctly.	Documentation for most tasks is very detailed. Minor issues in some tasks.	Additional processes were successfully done and are well documented.
[50% – 60%)	Some details are missing from the notes but most actions are documented in detail.	Some tasks are biased but the majority of the notes are impartially presented.	There might be some minor inconsistencies in the investigated evidence.	There are some tasks taken that are not presented with full details.	Elementary processes were documented. Some key tasks were not done or they were superficially discussed.
[40% – 50%)	Sufficient narrative of basic actions taken but some abstract wording exists.	Sufficient investigative approach	Sufficiently documented using some key timestamps	Sufficient documentation of basic actions taken	Sufficient processes documented for initiating a theory
[20% – 40%)	Some brief details are given for some tasks. Abstract language.	Biased documentation	Some indications of accurate recording of tasks Some tasks are not used to properly identify evidence.	Insufficient register of actions taken/results returned	Insufficient completion of tasks completed to achieve a reliable investigation.
[0% – 20%)	No submission or incomplete material	Heavily biased approach	No submission or incomplete material	No submission or incomplete material	No submission or incomplete material
	Detailed	Impartial	Accurate	Repeatable	Complete

Report

[85% – 100%)	Professionally written. Professionally edited and documented. Flawless.	Exceptional neutral investigative approach, professional language.	Exceptional accuracy; all evidence items are referenced properly.	Exceptional Report. All evidence items are properly referenced.	Provenance of all evidence items is provided. Only relevant items are identified.
[70% – 85%)	Excellent use of language. Excellent editing, formatting.	Neutral Investigation, impartial report.	All references are pointing to the correct items. No inconsistencies.	All evidence items are properly referenced. No questions raised for the validity of the documentation.	Provenance of all evidence items is provided. Some irrelevant items in the list.
[60% – 70%)	Neutral, formal language is used in the report. Most evidence are properly discussed. Well written.	Impartial approach. One or two biased references.	Most evidence items and actions are reported correctly. One or two inconsistent clauses.	Documentation for most evidence is very detailed. Very minor issues in some cases.	Provenance of most evidence items is provided.
[50% – 60%)	Sufficient report discussing formally basic Evidence. Sometimes the report does not use formal language.	Some tasks are partially biased, but the majority of the report are impartially presented.	There are some minor inconsistencies in the reported evidence.	Some evidence items are not properly referenced in the report. All key evidence is referenced.	Sufficient Provenance of basic evidence items.
[40% – 50%)	Sufficient report discussing very basic Evidence.	Sufficient report but with indications of biased discussion.	Sufficiently discussed only the basic items.	Sufficient documentation of basic evidence found. Basic pointers to evidence exist.	Sufficient Provenance of basic evidence items. Some fields are missing, e.g. no Hashes are provided.
[20% – 40%)	The report lucks of clarity, it is messy and not well documented.	Biased reporting.	Some basic evidence items are accurately reported. There are a lot of inconsistencies however.	Insufficient record of evidence found.	Insufficient Provenance of Evidence Items.
[0% – 20%)	No submission or incomplete material	Heavily biased approach	No submission or incomplete material	No submission or incomplete material	No submission of Provenance.
	Formal Language/Well written	Impartial	Accurate/ Precise	Refers to Evidence Items	Evidence Provenance given

Timeline

[85% – 100%)	Exceptionally detailed documentation. Professionally described.	Exceptional accuracy. All events are relevant and accurately described (maybe using multiple resources).	Exceptional timeline of events. Complete, readable, absolutely relevant events are listed, tells the whole story.	Exceptional visualisations, professionally edited.
[70% – 85%)	Excellent record of relevant events. No abstract actions are recorded.	All major events are listed. Always refers to Evidence items.	All relevant events/actions are listed correctly. Timeline makes logical sense. No inconsistencies.	Excellent visualisations. Clear timeline. Avoids listing unrelated events.
[60% – 70%)	Accurate description of all aspects of the investigation.	All major events are listed. Always refers to Evidence items (one or two discrepancies only).	Most relevant evidence items are listed correctly. Timeline makes logical sense. Maybe one or two minor inconsistencies exist.	Well documented timeline. Good visuals. Useful representation of events.
[50% – 60%)	Some details are missing but most facts are documented in detail.	All major events are listed. Sometimes refers to Evidence items.	All basic events are listed. The timeline is readable and the sequence of basic actions makes sense.	Good demonstration of visual representation of main events.
[40% – 50%)	Sufficient details for basic events but still some abstract events occur.	Most major events are listed. Sometimes refers to Evidence items.	Timeline is reasonably helpful. An intention to put 3-4 major events in a sequence.	Sufficient but superficial visualisation of basic events
[20% – 40%)	Some brief details are given for some events. Abstract in most of the cases.	No references to Evidence items, but the major events are listed.	Timeline is not helpful. An intention to put 3-4 major events in a sequence, but the outcome is not readable.	Insufficient record of events
[0% – 20%)	No submission or incomplete material	No submission or incomplete material	No submission or incomplete material	No submission or incomplete material
	Accurate (time stamped)	Refers to Evidence Items	Readable/Complete	Aesthetically pleasing/Useful

Opinion

[85% – 100%)	Exceptional, professionally given opinion, independent, justified opinion, clearly expressed, well structured.	Exceptional neutral investigative approach, professional language.	Exceptional, professional discussion of relevant legislation.	Exceptional discussion of similar cases.
[70% – 85%)	Independent, justified opinion, clearly expressed, well structured.	Neutral Investigation, impartial documentation.	Excellent referencing and discussion of relevant legislation.	Excellent referencing and discussion of similar cases.
[60% – 70%)	Independent opinion, justified, clearly expressed (might be difficult to follow in places).	Impartial approach in most actions taken.	Very good discussion and reference of relevant legislation.	Convincedly references and discusses a similar case.
[50% – 60%)	Independent opinion, mostly justified, but not clearly expressed.	Some tasks are biased but the majority of the notes are impartially presented.	Sufficiently references relevant legislation.	Sufficiently references a similar case.
[40% – 50%)	Sufficiently given opinion, maybe not well justified, and not clearly expressed.	Sufficient investigative approach overall, difficult to follow the argument.	Adequately talks about relevant legislation. References are missing.	Adequately discusses a similar case. References are missing.
[20% – 40%)	Abstract language; opinion not justified.	Biased documentation	Maybe states same kind of legislation.	An attempt to discuss similar cases.
[0% – 20%)	No submission or incomplete material	Heavily biased approach	No submission or incomplete material	No submission or incomplete material
	Justified/Based on facts (Evidence Items)	Analytical	Refers to Legislation (U.K. or local)	Provides Examples of similar Cases.

End of coursework specification.