|  |  |  |
| --- | --- | --- |
|  | **Faculty of Computing, Engineering and Science** | Final mark awarded:\_\_\_\_\_ |

**Assessment Cover Sheet and Feedback Form 2017-18**

|  |  |  |  |
| --- | --- | --- | --- |
| Module Code:  IY1D402 | Module Title:  Cyber Security Tools and Practices | | Module Lecturer:  Clare Johnson |
| Assessment Title:  Project Output 2 - Forensics | | | Assessment No.  2 |
| No. of pages submitted in total including this page:  Completed by student | | | Word Count of submission  (if applicable): Completed by student |
| Date Set:  23-Feb-2018 09:00:00 | | Submission Date:  20-Apr-2018 23:59:00 | Return Date:  21-May-2018 23:59:00 |

|  |  |
| --- | --- |
| ***Part A: Record of Submission (to be completed by Student)*** | |
| **Extenuating Circumstances**  If there are any exceptional circumstances that may have affected your ability to undertake or submit this assignment, make sure you contact the Advice Centre on your campus prior to your submission deadline. | |
| **Fit to sit policy**:  The University operates a fit to sit policy whereby you, in submitting or presenting yourself for an assessment, are declaring that you are fit to sit the assessment. You cannot subsequently claim that your performance in this assessment was affected by extenuating factors. | |
| **Plagiarism and Unfair Practice Declaration:**  By submitting this assessment, you declare that it is your own work and that the sources of information and material you have used (including the internet) have been fully identified and properly acknowledged as required[[1]](#footnote-1). Additionally, the work presented has not been submitted for any other assessment. You also understand that the Faculty reserves the right to investigate allegations of plagiarism or unfair practice which, if proven, could result in a fail in this assessment and may affect your progress. | |
| **Intellectual Property and Retention of Student Work:**  You understand that the University will retain a copy of any assessments submitted electronically for evidence and quality assurance purposes; requests for the removal of assessments will only be considered if the work contains information that is either politically and/or commercially sensitive (as determined by the University) and where requests are made by the relevant module leader or dissertation supervisor. | |
| **Details of Submission:**  Note that all work handed in after the submission date and within 5 working days will be capped at 40%[[2]](#footnote-2). No marks will be awarded if the assessment is submitted after the late submission date unless extenuating circumstances are applied for and accepted (Advice Centre to be consulted). | |
| You are required to acknowledge that you have read the above statements by writing your student number(s) in the box: | Student Number(s): |

**IT IS YOUR RESPONSIBILITY TO KEEP RECORDS OF ALL WORK SUBMITTED**

|  |
| --- |
| **Part B: Marking and Assessment**  **(to be completed by Module Lecturer)** |
| This assignment will be marked out of 100%  This assignment contributes to 50% of the total module marks.  This assignment is bonded |
| **Learning Outcomes to be assessed** (as specified in the validated module descriptor <https://icis.southwales.ac.uk/> ):  *1) To demonstrate an understanding of the practices, principles, standards, legal and ethical issues associated with information assurance. 2) To demonstrate the ability to perform forensic and security incident management.* |
| *Provisional mark only: subject to change and/or confirmation by the Assessment Board* |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Fail | Narrow Fail | 3rd Class / Pass | Lower 2nd Class / Pass | Upper 2nd Class / Merit | 1st Class / Distinction |
| ACPO Good Practice for Digital Evidence v5 [400 words maximum] 10% | * Very poor explanation of principle 1 and how it relates to a forensic investigation * Very poor explanation of principle 2 and how it relates to a forensic investigation * Very poor explanation of principle 3 and how it relates to a forensic investigation * Very poor explanation of principle 4 and how it relates to a forensic investigation | * Poor explanation of principle 1 and how it relates to a forensic investigation * Poor explanation of principle 2 and how it relates to a forensic investigation * Poor explanation of principle 3 and how it relates to a forensic investigation * Poor explanation of principle 4 and how it relates to a forensic investigation | * Satisfactory explanation of principle 1 and how it relates to a forensic investigation * Satisfactory explanation of principle 2 and how it relates to a forensic investigation * Satisfactory explanation of principle 3 and how it relates to a forensic investigation * Satisfactory explanation of principle 4 and how it relates to a forensic investigation | * Good explanation of principle 1 and how it relates to a forensic investigation * Good explanation of principle 2 and how it relates to a forensic investigation * Good explanation of principle 3 and how it relates to a forensic investigation * Good explanation of principle 4 and how it relates to a forensic investigation | * Very good explanation of principle 1 and how it relates to a forensic investigation * Very good explanation of principle 2 and how it relates to a forensic investigation * Very good explanation of principle 3 and how it relates to a forensic investigation * Very good explanation of principle 4 and how it relates to a forensic investigation | * Excellent explanation of principle 1 and how it relates to a forensic investigation * Excellent explanation of principle 2 and how it relates to a forensic investigation * Excellent explanation of principle 3 and how it relates to a forensic investigation * Excellent explanation of principle 4 and how it relates to a forensic investigation |
| Encryption / Passwords 30% | * The simple password has not been recovered * The intermediate password has not been recovered * The difficult password has not been recovered | * The simple password has been recovered with no explanation * The intermediate password has been recovered with no explanation * The difficult password has been recovered with no explanation | * The simple password has been recovered but very basic explanation was provided * The intermediate password has been recovered but very basic explanation was provided * The difficult password has been recovered but very basic explanation was provided | * The simple password was recovered with an appropriate explanation * The intermediate password was recovered with an appropriate explanation * The difficult password was recovered with an appropriate explanation | * The simple password was recovered with a good level of detail * The intermediate password was recovered with a good level of detail * The difficult password was recovered with a good level of detail | * The simple password has been recovered with excellent detail on the recovery process * The intermediate password has been recovered with excellent detail on the recovery process * The difficult password has been recovered with excellent detail on the recovery process |
| Finding forensic artefacts on the system that are pertinent to the case 30% | * The first artefact was missing or not relevant * The second artefact was missing or not relevant * The third artefact was missing or not relevant | * The first artefact is relevant but the reporting was poor * The second artefact is relevant but the reporting was poor * The third artefact is relevant but the reporting was poor | * Locating and reporting on the first relevant artefact was satisfactory * Locating and reporting on the second relevant artefact was satisfactory * Locating and reporting on the third relevant artefact was satisfactory | * Locating and reporting on the first relevant artefact was good * Locating and reporting on the second relevant artefact was good * Locating and reporting on the third relevant artefact was good | * Locating and reporting on the first relevant artefact was very good * Locating and reporting on the second relevant artefact was very good * Locating and reporting on the third relevant artefact was very good | * Locating and reporting on the first relevant artefact was excellent * Locating and reporting on the second relevant artefact was excellent * Locating and reporting on the third relevant artefact was excellent |
| Project Report 30% | * Very poor brief * Very poor work / research conducted * Very poor summary | * Poor brief * Poor work / research conducted * Poor summary | * Satisfactory brief * Satisfactory work / research conducted * Satisfactory summary | * Good brief * Good work / research conducted * Good summary | * Very good brief * Very good work / research conducted * Very good summary | * Excellent brief * Excellent work / research conducted * Excellent summary |

# Assessment Task

A subject of a police investigation is Mr. Bad Guy. He has been arrested as a **suspect in hacking** with his accomplice Peter Dish. The police were able to recover a 16GB red USB memory stick. They were unable to gather any other digital evidence. Mr. Guy is denying the USB memory stick is his even though it was found in his pocket. Currently, there is no substantial proof in the case. The police have enlisted you as a forensic expert to link the USB memory stick to both Mr. Bad Guy and suspected involvement in the case.

This case will most likely need to go to court so the evidence needs to be handled in an appropriate manner meeting the ACPO guidelines and appropriate laws. The police are not interested in any other criminal activity so only report on things relevant to the case. You should only include the three most significant/relevant artefacts that you discover related to hacking. You should explain your motivation for the artefacts selected along with how they were concealed.

**Submission**

You will need to compile:

1. A case report documenting any processes taken to retrieve the relevant data. The evidence needs to be verified and all appropriate data should be included. [2000 words maximum]
2. A project report detailing the work you have carried out on the project(s) that you have been allocated. [2000 words maximum]

# Report Structure – REQUIRED

There is a *4000-word limit* for this report. As it is a technical report, you may wish to investigate templates further online.

Please structure your report in the following way:

**Title Page**

This should include your student number, the case name, the date of the investigation etc.

**Contents Page**

A detailed table of contents should be included in the report indicating pages.

**ACPO**

Explain the ACPO principles in your own words.

**Evidence Listing and Reporting**

Use the template below to list the three most relevant evidential items recovered along with the techniques used to recover them.

**Passwords Recovered**

Use the passwords recovered and the process required. *[simple, intermediate and difficult]*

**Projects**

Report on the project(s) you have been working on including details of the brief(s), work / research conducted and summary.

**References**

Include any references used throughout your report

**Appendix**

Include any outputs from your project work

**NOTE:** E01 files can get corrupted. Every day you work on the coursework you should start by verifying the evidence.

**HINT:** Remember to use the graphical, overview and index search tabs to aid your investigation. You should not need to analyse every single file on the PC. You need to document the effectiveness of any hiding techniques you discover.

**Case Number:** {enrolment number}\_IY1D402\_CW2

E.g. 12345678\_IY1D402\_CW2

# General Forensic Report Guidance

This is a general guide and is not a comprehensive guide of writing a forensic report.

* Evidence numbers should be in bold. Evidence numbers are typically made up of your initials and an incremental number. E.g. Artefact 1 detected by Ross Davies would become **RD01**
* Any technical terms should be explained at the first use and then referred to in a glossary of terms. Each instance should once again be in bold. E.g., the word **Hash Value** would be in bold.

Each artefact should be included in your report. You can use the example artefact table as a starting point add any information you thing is relevant to the investigation.

Example artefact template:

|  |  |  |  |
| --- | --- | --- | --- |
| Filename (including ext.) |  | Hash (MD5) |  |
| Date Created |  | Is deleted? |  |
| Date Modified |  | File path |  |
| Date Accessed |  | Size (L/P) |  |
| FTK Number |  | Evidence Number |  |
| Evidence Description (media/text) |  | | |
| Technique used |  | | |
| Reason for selection |  | | |

The evidence should be verified using a program such as FTK. The hash values need to be included in your report. You should separate the characters out. Remain consistent on capitalisation. It is preferable to use capital letters. You may use the following template.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| MD5 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sha1 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

**Note:** For the purposes of this assignment, you are required to explain your reasons for including any evidence. You also need to explain the effectiveness of the hiding techniques and the forensic tools that can be used to discover the content. However, in a standard investigation you are not allowed to comment on the nature of the evidence. Cite any sources of information.

1. University Academic Misconduct Regulations [↑](#footnote-ref-1)
2. Information on exclusions to this rule is available from the Advice Centre at each Campus [↑](#footnote-ref-2)