### 1. Overview

This assignment has a weighting in calculating your grade for the course. The weight for the assignment is detailed in the course handbook.

Working in your assessment team, all members will prepare and participate in a slide presentation and report that will convey research countermeasures against forensics analysis.

The expectation is that by completing this assessment, students are effectively able to:

understand the nature of countermeasures against forensic analysis.

predict potential ethical, legal and regulatory concerns from gathered evidence.

effectively communicate complex outcomes from a forensics investigation to a non-technical audience, e.g. court-room.

### 2. Background

Alva & Drexel (A&D) is a British multinational conglomerate that specialises in many different domains, including wind turbines. A&D has suspended employment for one of its software engineers while it investigates concerns that the individual has exfiltrated trade secrets for personal gains. The trade secrets include algorithms and mathematical models that pertain to the efficient management of wind turbines.

A&D representatives state the former employee has exfiltrated important trade secrets using anti-forensics techniques with the intention to: (1) release some of the information publicly, (2) sell some of the information to other entities and (3) start their own competition business.

A&D representatives base these claims on knowledge that the individual transferred more than 20,000 images between workstations and their own personal device over a number of months via removable media. A&D representatives have also intercepted unusual emails with images that have been sent to the personal email account of the employee.

The organisation believes the employee exfiltrated trade secrets outside the perimeter of the organisation via bitmap images using a combination of removable media and messaging services. The employee in question states they did not exfiltrate any data for personal gain.

The law firm Rossum & Hamilton (R&H) representing A&D are concerned they do not have sufficiently strong evidence to suggest the software engineer has or would exfiltrate data in the manner suggested by A&D representatives. R&H are unsure of the legal arguments in the specific situation regarding source code, intellectual property rights and how the employee would profit in the way suggested by the organisation.

### 3. Task

The task is to research ****countermeasures against forensics analysis and communicate that to a non-technical audience****through a report and presentation. The task must be completed in self-organising teams of no less than three members and no more than four members.

Teams are self-organising, and members must register their team via the course Moodle by the deadline stated in the Timetable chapter. Individuals not registered in a team by the deadline will be randomly allocated to a team, including those teams with less than the maximum number of team members.

The report will be used to determine the grade for the team. Team members are required to agree a single A4 page ****workload record****and include it as an appendix with the report. Furthermore, team members are required to complete their own ****personal assessment of their teammates****through allocation of 100 points. Equal contribution is assumed if an individual does not submit a personal assessment. The personal assessment of contribution is submitted separately from the final report by each team member. The ****assessment of contribution from each team member will be used to inform the individual grade for the exercise****.

The assessment is multi-route and teams can opt for one of two routes, either a non-programming or programming route to produce the report and presentation.

任务是研究针对取证分析的对策，并通过报告和演示将其传达给非技术观众。这项任务必须在不少于三人及不多于四人的自组织小组中完成。

团队是自组织的，成员必须在时间表章节中规定的截止日期前通过Moodle课程注册他们的团队。在截止日期前未注册的个人将被随机分配到一个团队，包括那些少于最大团队人数的团队。

该报告将被用来确定团队的等级。团队成员必须同意一个A4页的工作量记录，并将其作为报告的附录。此外，团队成员需要完成自己对队友的个人评估，分配100分。如果个人没有提交个人入息课税，则会被视为等额供款。每个团队成员的个人贡献评估与最终报告分开提交。对每个小组成员贡献的评估将被用来确定这项工作的个别职级。

评估是多路线的，团队可以选择两种路线之一，非编程路线或编程路线来生成报告和演示。

****4. Assessments Routes****

****Teams may follow a non-programming or programming route to produce the report and presentation, route one and route two respectively.****

### 4. Assessments Routes

#### 4.1. Route 1: Non-programming

****Teams that opt for this route are expected to produce a 6-page report.****

****The expected report for the route comprises of:****

****cover page outlining the team’s name, members, student numbers and word count.****

****recognise the problem with an overview of anti-forensics and the challenges it represents in the given context (1 page).****

****literature survey that focuses on four key areas of anti-forensics (e.g. data hiding, artefact wiping, trail obfuscation etc.) cemented in the given context (3 pages).****

****argue whether the former software engineer would have indeed exfiltrated data in such way from the organisation (1 page).****

****argue whether the case sought by the organisation is even viable, i.e. specifically the software engineer using company workstations to exfiltrate trade secrets for personal gain (hint: consider the external context and strengthen argument with relevant evidence) (1 page).****

****bibliography.****

****workload report details the contribution of members (teams may simply state all members contributed equally).****

选择这条路线的团队需要提交一份6页的报告。

该路线的预期报告包括:

封面概述团队的名字，成员，学生人数和字数。

通过对反取证的概述以及它在给定上下文中所代表的挑战来识别问题(1页)。

文献调查，集中在反取证的四个关键领域(如数据隐藏，人工制品擦拭，痕迹混淆等)巩固在给定的上下文中(3页)。

争论前软件工程师是否确实会以这种方式从组织中窃取数据(1页)。

论证该组织所寻求的案件是否可行，即具体来说，软件工程师利用公司工作站窃取商业机密以谋取个人利益(提示:考虑外部环境，并用相关证据加强论证)(1页)。

参考书目。

工作量报告详细说明了成员的贡献(团队可以简单地说明所有成员的贡献相同)。

#### 4.2. Route 2: Programming

****Teams that opt for this route are expected to produce an application, documentation and a presentation.****

****Teams that opt for route two are expected to construct a lightweight application in Java, a report as well as an accompanying presentation. The lightweight application in Java would demonstrate an individual could exfiltrate data through bitmap images. R&H want to argue the ‘lightweight application’ would demonstrate an A&D software engineer could construct the application and discard it within a single session on a workstation without requiring third-party libraries or frameworks.****

****The documentation for the route should comprise:****

****cover page outlining the team’s name, members and student numbers.****

****detailed test cases demonstrating the capability and limitations of the application (e.g. 3 expected cases and 2 extreme cases).****

****setup and operation instructions (e.g. the version, build numbers etc, particularly laborious setups will result in penalties).****

****complete and commented source code.****

****workload report detailing the contribution of members (teams may simply state all members contributed equally).****

选择这条路线的团队需要制作应用程序、文档和演示文稿。

选择路径二的团队被期望用Java构建一个轻量级的应用程序、一个报告以及一个附带的演示。Java中的轻量级应用程序将演示个人可以通过位图图像窃取数据。R&H认为，“轻量级应用程序”将证明A&D软件工程师可以在工作站上的单个会话中构建应用程序并丢弃它，而不需要第三方库或框架。

路线的文件应包括:

封面概述团队的名称，成员和学生编号。

详细的测试用例展示了应用程序的能力和局限性(例如3个预期用例和2个极端用例)。

设置和操作说明(例如版本，版本号等，特别费力的设置将导致处罚)。

完成并注释源代码。

工作量报告详细说明了成员的贡献(团队可以简单地说明所有成员的贡献相同)。

****bibliography.****

****appendix containing sufficiently commented and structured source code that demonstrates intellectual input, recognition of the problem and coverage of key steps.****

****The expected presentation for the route comprises of:****

****cover slide introducing team, including name, student numbers and length.****

****recognition of the problem with an overview of anti-forensics and associated challenges with specific focus on stenography.****

****coverage of key steps in the process through explanation and demonstration of the lightweight Java application****

****describe bitmap images and argue the motivation for engineer to opt for the format as a vessel.****

****articulate the importance of the header within the file and how to embed the size of the payload within the vessel as well as how this supports recovery of the payload and varying payload sizes.****

****describe how the payload will be converted into bits in Java and how these bits are embedded within the vessel.****

****demonstrate test cases, specifically the entire process of embedding a payload within a vessel and then recovering it from it as well as recovering a payload from another bitmap vessel.****

****communicate a rational argument and demonstrate intellectual input on the process and the case itself.****

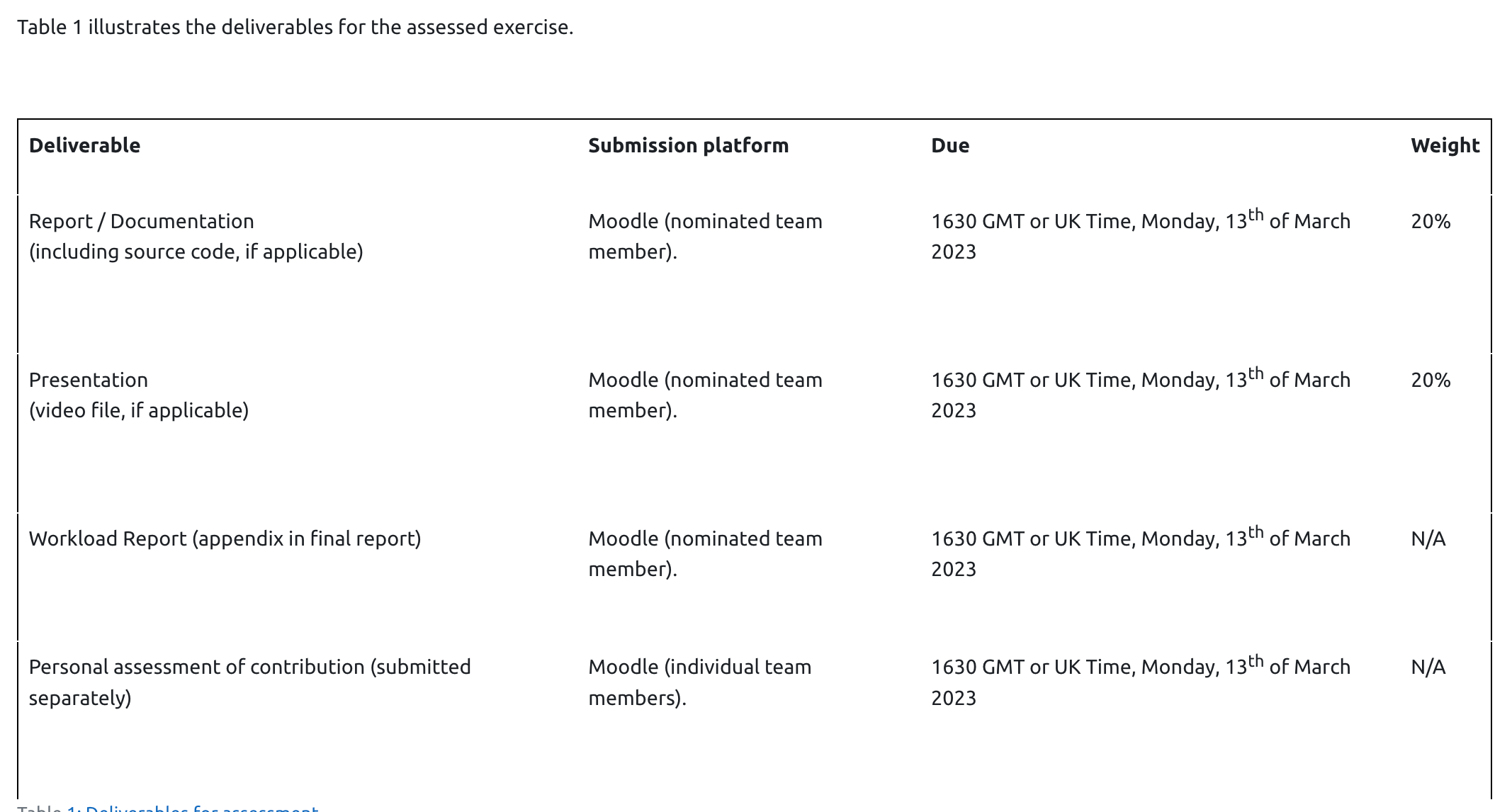
****argue whether the former software engineer would have indeed exfiltrated data in such way from within the corporation.****

****argue whether the case sought by the organisation is even viable, i.e. specifically the software engineer using company workstations to exfiltrate trade secrets for personal gain (hint: consider the external context and strengthen argument with relevant evidence)****

### 5. Deliverables

Table 1 illustrates the deliverables for the assessed exercise.

|  |  |  |  |
| --- | --- | --- | --- |
| ****Deliverable**** | ****Submission platform**** | ****Due**** | ****Weight**** |
| Report / Documentation (including source code, if applicable) | Moodle (nominated team member). | 1630 GMT or UK Time, Monday, 13th of March 2023 | 20% |
| Presentation (video file, if applicable) | Moodle (nominated team member). | 1630 GMT or UK Time, Monday, 13th of March 2023 | 20% |
| Workload Report (appendix in final report) | Moodle (nominated team member). | 1630 GMT or UK Time, Monday, 13th of March 2023 | N/A |
| Personal assessment of contribution (submitted separately) | Moodle (individual team members). | 1630 GMT or UK Time, Monday, 13th of March 2023 | N/A |



#### 5.1. Submission

A nominated team member should upload presentation, report and relevant supplementary material. Team members are expected to submit their personal assessment of peers separately via Moodle. The team grade is determined from the report and presentation. The individual grade is determined through consideration of the individual assessments of contribution from team members.

##### Submission format for report

The ****report****should be formatted in the following way:

team name and comprising members on cover-page.

PDF format.

12-point font, 1-inch margins.

filename including the matric numbers of comprising members, separated by underscore, e.g. 0122456\_0126657\_0123488.pdf

##### Submission format for presentation

The ****presentation**** video should be formatted in the following way:

team name and comprising members outlined at start of video.

video should be MP4 format.

teams must ensure the video is accessible and can be ****downloaded****.

presentation video should be 10 minutes in length (plus or minus 1 minute).

Teams should upload the report, link to presentation, any appendices and source code (if applicable) as a single compressed archive (e.g. zip file) via Moodle submission link.

### 6. Timetable

Table 2 illustrates the timetable of milestones for the task. The reminder of this assessed exercise specification comprises some guidance, remarks as well as expected deliverables.

|  |  |  |
| --- | --- | --- |
| ****Week**** | ****Milestone**** | ****Date**** |
| 1 | Assessment specification announced in class. | Tuesday, 10th of January 2023. |
| 2 | Teams confirmed on Moodle. | Friday, 20th of January 2023. |
| 8 | Assessment week (class does not meet). | Tuesday, 28th of February 2023 |
| 10 | Report, presentation and supplementary submission. | Monday, 1630 GMT or UK Time, 13th of March 2023. |
| 10 | Individual assessment of team members contributions. | Monday, 1630 GMT or UK Time, 13th of March 2023. |

### 7. Feedback

The final individual grade will be published via Moodle. General comments and feedback on the team research exercise will be provided to the entire class via Moodle. Team members may book an appointment to clarify feedback on individual performance after the release of performance.

### 8. Marking Scheme

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ****Grade**** | ****Problem Recognition****    (weight 10%) | ****Content Coverage****      (weight 30%) | ****Intellectual Input****      (weight 15%) | ****Rationality of Argument****    (weight 15%) | ****Use of Visual Aids****      (weight 10%) | ****Clarity of Speech****      (weight 10%) | ****Written Quality****      (weight 5%) | ****Team Performance****      (weight 5%) |
| ****A****  (A1 – A5)  excellent | excellent understanding of problem, excellent understanding of key concerns. | thorough consideration of key steps in code or areas in research, ample relevant sources. | excellent demonstration of critical and independent thought | highly structured, logical argument, selective use of sources to support arguments. | excellent use of visual aids, effective staging of content, excellent complement to delivery | excellent pace, excellent articulation and confident communication. | very well structured, highly literate, excellent comments in source code. | excellent demonstration of team collaboration, well integrated and coherent artefacts produced. |
| ****B****  (B1 – B3)  very good | very good understanding of problem, very good understanding of key concerns. | very good consideration of key steps in code or areas in research, considerable relevant sources. | very good demonstration of critical and independent thought | well structured, logical argument, very good use of sources to support arguments. | very good use of visual aids, very good staging of content, excellent complement to delivery | very good pace,  very good articulation and confident communication. | well structured, literate | very good demonstration of team collaboration, generally well-integrated and coherent artefacts produced. |
| ****C****  (C1 – C3)  good | good understanding of problem, good understanding of key concerns. | good consideration of key steps in code or areas in research, fair number of relevant sources. | good demonstration of critical and independent thought | moderately well structured, logical argument, good use of sources to support arguments. | good use of visual aids, good staging of content, excellent complement to delivery | good pace, good articulation and confident communication. | moderately well structured, occasionally ungrammatical | good demonstration of team collaboration, integrated and coherent artefacts produced. |
| ****D****  (D1 – D3)  satisfactory | adequate understanding of problem, adequate understanding of key concerns. | adequate consideration of key steps in code or areas in research, some relevant sources. | adequate demonstration of critical and independent thought | adequately structured, logical argument, adequate use of sources to support arguments. | adequate use of visual aids, adequate staging of content, excellent complement to delivery | adequately paced and articulation, often not confident communication | adequately structured, fairly often ungrammatical | adequate demonstration of team collaboration, integrated, but at times incoherent artefacts produced. |
| ****E****  (E1 – E3)  weak | weak understanding of problem and concerns. | weak consideration of key steps in code or areas in research, little relevant sources. | weak demonstration of critical and independent thought | poorly structured, flawed argument, few sources used to support arguments. | weak use of visual aids, weak staging of content, excellent complement to delivery | poorly paced and articulated, lacks overall confidence in communication | poorly structured, frequently ungrammatical | weak demonstration of team collaboration, generally poorly integrated and incoherent artefacts produced. |
| ****F-G****  (F1 – G2)  poor | poor understanding of problem and concerns. | no clear consideration of key steps in code or areas in research, almost no relevant sources. | poor demonstration of critical and independent thought | very poorly structured, logical argument, little to no use of sources to support arguments. | poor use of visual aids, poor staging of content, excellent complement to delivery | very poorly paced and articulated, no confidence in communication. | very poorly structured, ungrammatical | poor demonstration of team collaboration, poorly integrated and incoherent artefact produced. |