**[Assessment 2: Major Assignment](https://bblearn.griffith.edu.au/webapps/blackboard/content/listContent.jsp?course_id=_102851_1&content_id=_6985365_1)**

[Assessment 2: Major Assignment](https://bblearn.griffith.edu.au/webapps/blackboard/content/listContent.jsp?course_id=_102851_1&content_id=_6983583_1&mode=reset)

The objective of this assignment is to gain knowledge and understanding of digital forensics through research and practical experience. This understanding is to be demonstrated by submission of a formal technical report of an analysis of digital forensics artefacts and a Digital Forensic Investigator's report...

**In this folder you will find:**

* All **Details**relating to this assessment including supporting documents and resources.
* An Electronic **A2 Cover Sheet**
* The **A2 Submission Point**

### Details

[Details](https://bblearn.griffith.edu.au/webapps/blackboard/content/listContent.jsp?course_id=_102851_1&content_id=_6985365_1)

#### Description:

**DUE: 11:59pm, Friday 14th October 2022**

This assignment is worth 50% (marked out of 150) of the total assessment. It is **individual**work.  While you can discuss the assignment with your peers, your submission should be your own work.  You should provide evidence of your own work incorporated in your submission.

The objective of this assignment is to gain knowledge and understanding of digital forensics through research and practical experience. This understanding is to be demonstrated by submission of a formal technical report of an analysis of digital forensics artefacts and a Digital Forensics Investigator’s report for non-technical audiences.

#### Format:

Reports should be submitted as a single docx or pdf file.

The quality of the presentation of a formal technical report is as important as the quality of the technical content of the report in the profession. Your assignment will be assessed on:

1. **Task 1** should be no more than 20 pages in length.
2. **Task 2** should be no more than 5 pages in length.
3. The text of your report should be in 12-point Times New Roman or 11-point Arial font or something equivalent, and in single space.
4. Page size is A4 with 2cm in margins on all sides.

#### Referencing:

* You must cite/reference original work, author(s) etc.
* Citation and referencing should conform to **APA (American Psychological Association)** or **IEEE**(Institute of Electrical and Electronics Engineers ) format both in the body of your paper and its attached reference section.
  + [The Griffith Referencing tool](https://app.secure.griffith.edu.au/reference_tool/index-core.php) will provide you with valuable assistance in making sense of referencing rules and requirements for academic writing. Examples are provided in the most commonly used referencing styles.
  + [APA referencing guide - Murdoch](https://libguides.murdoch.edu.au/APA/home)

#### Assessment Specifications and Marking Criteria:

Please see the **Assessment Specification and Marking Criteria** item below.

[3906ICT Assessment Specifications and Marking Criteria](https://bblearn.griffith.edu.au/webapps/blackboard/content/listContent.jsp?course_id=_102851_1&content_id=_6985365_1)

#### Scenario

You work as a digital forensic investigator for the National Anti-Corruption Agency (NACA) and you have been called in to assist in a larger investigation into the actions of government intelligence operative Eason Hunter.  Russia had agreed to allow English scientists to dispose of a shipment of Russian developed bioweapons.  Eason Hunter has been accused of stealing and transporting these bioweapons from the Russian embassy in London [1]

**Task 1**

Your immediate supervisor has asked you to investigate Eason Hunter to find evidence as to where he might be and if he has committed any crimes.  The NACA with the assistance of Erika Sloane, Eason Hunter’s branch manager, has conducted searches of Hunter’s home and offices and obtained relevant digital evidence.  Your supervisor suggests you address the following questions related to each piece of evidence.

 Evidence A – A disk image of an old laptop computer found in a boat house near Hunter’s residence.

1. Who is the owner of the desktop?
2. What programs have been installed on the desktop ? What recent programs have been run?
3. Recover details of any files in the recycle bin.
4. Is there evidence that the owner of the desktop committed a crime?

Evidence B – A memory dump of Eason Hunter’s work desktop computer.

1. What applications are running on the memory dump computer?
2. What web pages has the memory dump computer visited recently?
3. What is email address of the owner of the memory dump computer?
4. What is password of the memory dump computer?

Evidence C – Network capture of the Eason Hunter’s work network.

1. Who are the people communicating in the transmission?  When does the first transmission begin and the last transmission finish?
2. What browsers and operating systems are used by the communication endpoints?
3. What was sent for Benji to collect?
4. Does the network capture reveal the relationship between Eason Hunter and the people participating in the intercepted communications?

Evidence D – A disk image of a damaged mobile phone found near last sighting of Eason Hunter.

1. What are the non-stock applications installed on the phone?
2. Who is in the contacts list? What messages and calls have been sent and received by the phone?
3. What Internet searches has the owner of the phone made?
4. Is there other evidence on the phone that might indicate the role of the owner in the bioweapon theft?
5. Conduct a timeline analysis of the pieces of evidence.
6. Provide a brief final analysis of the evidence and your conclusions.

As part of the answer for each of these questions you must include:

* A clear description of the evidence and reasoning for your answer.
* A detailed description of the process that you followed.
* A brief description of the tools that you used to obtain your conclusions. It is expected that you will include screenshots in your description.

### Evidence Details

* EvidenceA.zip (md5sum: 5f561b7e7a009286c55516f5d2914fe6)
* EvidenceB.zip (md5sum: 01d52b7b461afe4184424293b0e2b841)
* EvidenceC.zip (md5sum: 2c355382f00636d62f2d5bf1b105625c)
* EvidenceD.7z (md5sum: bfabc964a1fe1bf63ccd487567ad4f1b)

If you are using the SIFT workstation on the Griffith Cyber Range, you can download it from the following link if you are logged into the SIFT workstation. This link is only accessible if you are logged into the SIFT workstation.

http://3906ICTAssignment.griffith.internal/

If you are doing the assignment on an external system, evidence for this assessment can be downloaded at the following links:

* EvidenceA.zip (https://cloudstor.aarnet.edu.au/plus/s/DCikDL3kePt2J4y)
* EvidenceB.zip (https://cloudstor.aarnet.edu.au/plus/s/r3NuwWjpEkky35s)
* EvidenceC.zip (https://cloudstor.aarnet.edu.au/plus/s/PdjUo8wUh9k6IdV)
* EvidenceD.7z (https://cloudstor.aarnet.edu.au/plus/s/6SXxnBSQoeABt5n)

#### Task 2

An initial court hearing is to be conducted regarding the actions of Eason Hunter and your digital forensics investigation played a major role. Your supervisor has asked you to write a digital forensics white paper based on one of the forensic fields in the investigation you conducted.  The suggested topics are:

* Digital Forensics Investigation Standards and Processes
* Disk Forensics and File Carving
* Memory Forensics
* Network and Cloud Forensics
* Mobile and Embedded Systems Forensics
* Timeline Analysis

This white paper should follow the recommended report structure.

Your report on the investigation should include the following main headings:

* **Introduction**– Provide an overview of the selected field of digital forensics study.  Why is it useful? When is it used?
* **Evidence Acquisition** - Describe how evidence for this field is acquired.  What techniques are used to ensure that the digital evidence is not tampered with or altered or destroyed during the acquisition process.
* **Forensic Analysis**- Provide a detailed description of the forensic analysis that is performed in this field. What are the latest algorithms, techniques or methods used to conduct the analysis. Discuss the problems and issues that must be overcome.
* **Forensic Tools** - Provide an overview of the current tools used to conduct forensics analysis in the selected field.  Discuss the advantages and disadvantages of the available tools.
* **Conclusions** - A summary of conclusions should follow logically from previous sections in the report and should also describe the future directions of the selected field.