Digital Image Investigation Using Autopsy

Plymouth programme at NSBM Green University
Group coursework assessment brief

Investigate the lecturer-supplied forensic disk image using Autopsy. Your group must preserve evidence integrity, locate and validate image files, explain the recovery process, and submit a traceable forensic report supported by genuine evidence from your own investigation.

Assessment information	Details
Module	PUSL3133 Digital Forensics and Malware Analysis
Level	Plymouth third year
Assessment type	Group practical investigation and written report
Group size	maximum 4 students; 4 members preferred
Required tool	Autopsy; record the installed version
Evidence image	8-jpeg-search.dd, supplied by the lecturer

Evidence register template

Use one row per distinct validated file. Required fields: evidence ID; filename or assigned export name; source path or offset when available; Autopsy object ID when available; allocated/deleted/carved/unknown status and basis; size; detected format; header/signature observation; openability; relevant timestamps and time zone; SHA-256 of export; screenshot reference; examiner; interpretation and limitations. Use “not available” where justified.

Assessment purpose

This coursework develops practical digital forensic skills in evidence handling, repeatable examination, file recovery, validation and professional reporting. It assesses disk-image investigation; students must not assume that the image contains malware, a complete Windows installation, browser history or identifiable users.

Investigation scenario

In a simulated investigation, an organisation has provided a forensic image of a storage device. The investigator is asked to establish which image files can be located or recovered and whether the available artefacts support any conclusions about their status or handling. Your team acts as the forensic examination group. The scenario is fictional; all findings must come from the supplied evidence.

Investigation questions

- What file system or storage structure can Autopsy identify, and what limitations affect examination?
- Can the group locate and validate at least eight distinct image files? Which are allocated, deleted or carved, where the evidence supports that classification?
- What evidence supports each file identification and recovery claim?
- What can and cannot be concluded from available paths, metadata, timestamps and file contents?

Task 1 Evidence handling and case preparation

Obtain the image only from the lecturer-designated location. Record its filename, byte size, date received, source and SHA-256 hash. Retain an unchanged master copy and examine a working copy. Confirm matching hashes before examination and verify the image again afterwards. A match demonstrates byte-level consistency; it does not independently establish authenticity or a complete chain of custody.

Maintain an evidence handling log covering receipt, copies, transfers, examinations and exports, identifying the student responsible and the relevant date and time. Create a group case identifier such as PUSL3133-G01. Record all members as examiners in the report and document the examiner entered in Autopsy.

Task 2 Autopsy configuration and examination

Create a new Autopsy case, record the case directory, and add the working image as a disk-image data source. Select and justify the time zone; if it is unknown, state your assumption. Record the operating system, Autopsy version, ingest modules, relevant settings, execution dates and any errors or incomplete processing.

Use appropriate available modules for file type identification, hash calculation, image metadata and file carving. Justify each choice. Keyword Search can help locate relevant text or filenames; it is not itself a substitute for deleted-file recovery or carving. Where available, use the PhotoRec Carver within Autopsy for signature-based recovery. Module labels and availability may vary by installed version.

Explore the data-source structure, file listings, deleted entries and carved results. Distinguish file-system recovery from carving. Do not describe every carved file as deleted: carving alone may not establish deletion status or original filename.

Task 3 Locate and validate image evidence

Aim to identify at least eight distinct image files, reflecting the source practical. Count duplicate byte-identical copies once in the main findings register and record duplicate occurrences separately. If fewer than eight can be validated, document all attempts and limitations; do not fabricate files or findings. The quality of a supported investigation takes priority over an unsupported count.

Export relevant files to a separate evidence-output directory. For each file, record an evidence ID, available source path or offset, Autopsy object ID where available, file size, detected type, status, relevant metadata and exported SHA-256 hash. Inspect the signature or header and test whether the file opens correctly. Classify incomplete or corrupt files explicitly. Do not invent missing names, offsets or timestamps.

Task 4 Interpretation and reporting

Explain how each significant finding answers the investigation questions. Link claims to evidence IDs and labelled screenshots. Distinguish direct observations from interpretations and uncertainty. Discuss whether metadata or timestamps support a limited sequence of events; omit unsupported timeline claims. Absence of an artefact is not proof that an activity never occurred.

Tag or bookmark relevant findings in Autopsy and generate an HTML report of the selected evidence. Check that it opens and that supporting assets are present. The Autopsy report is supporting material and must accompany a student-written report; it does not replace that report.

Required report structure

Section	Required content
Cover and declarations	Module, group ID, names, student IDs, word count, originality and AI declarations
Executive summary	Purpose, key supported findings and principal limitations
Scope and method	Investigation questions, evidence receipt, integrity checks, configuration and repeatable workflow
Findings	Evidence register, validated images and selected annotated screenshots
Discussion	Recovery methods, corroboration, uncertainty, errors and tool limitations
Conclusion	Answers to the investigation questions based on the recorded evidence
References	Consistent Harvard referencing for external sources and technical documentation
Appendices	Handling log, hash record, configuration details, contribution log, individual reflections and any permitted AI record

Submission package

- Submit one group report as PDF and one ZIP containing the complete Autopsy HTML report with its assets, exported evidence files, evidence register in CSV or XLSX, and handling and contribution logs.
- Name files PUSL3133_GroupID_Report.pdf and PUSL3133_GroupID_Evidence.zip. Include a short README explaining the folder structure and how to open the HTML report.
- Capture screenshots of case setup, data-source settings, ingest configuration and completion, evidence locations, validation, tags and report generation. Include captions and cross-references; screenshots must come from your own case.
- Retain the complete Autopsy case locally until marking and any review are finished. Do not upload the original disk image or full case database unless requested by the lecturer.
- Check that the ZIP opens, HTML assets load, evidence IDs match the report, and all files are readable before submitting. One nominated member submits for the group.

Group work and individual accountability

Groups must contain 4 students. Register the group and nominate a coordinator before commencing. For 4 members, suggested responsibilities are evidence handling, case configuration, file recovery, validation, and reporting coordination. For three or four members, combine responsibilities. Every member must perform practical analysis and contribute to the written report; assigning a member only formatting work is insufficient.

Maintain a contribution log recording student ID, task, date, output or evidence ID, time spent and peer verification. Include a signed contribution declaration and a 200–300 word individual reflection from each member in the appendices. Each reflection must identify a practical action, evidence contribution, difficulty encountered and what was learned.

The rubric allocates 90 marks to group work and 10 to individual contribution. Group criteria normally receive a common score; the contribution score is awarded separately to each student using the log, reflection and demonstrated understanding. The lecturer may request a short individual demonstration or viva to verify authorship and participation. Any further adjustments or misconduct decisions follow the approved module and institutional procedures.

Academic integrity and use of AI

Students must develop the report themselves. Generative AI must not draft the assessed report, produce the forensic analysis or conclusions, write individual reflections, or fabricate or alter screenshots, evidence, hashes, citations or investigation logs.

Limited AI assistance is permitted only for language editing and formatting of text already written by the students, affecting no more than 20% of the main report by word count. The main report means the executive summary through the conclusion, excluding the cover, references and appendices. Count all words in passages changed with AI assistance and calculate: affected words ÷ main-report words × 100. This is a limit on declared assistance, not permission to generate 20% of the assessed analysis.

Keep the original student-written version and the edited version. Declare the tool, date, purpose, prompts, affected passages, word count and percentage in an AI-use appendix. State “No AI assistance used” if applicable. Do not upload the evidence image, recovered files or personal data to an AI service. Ordinary spelling correction and document layout tools without generative features do not count towards this limit.

An AI-detector percentage is not a reliable measure of the proportion actually generated or edited, and a score below 20% does not establish compliance. Students must be able to explain and reproduce their submitted work. Undeclared or prohibited use is handled through the applicable academic integrity process.

Student declaration

“We confirm that the practical investigation, findings, analysis and conclusions are our own work. Every member has contributed as recorded. We have acknowledged external sources and declared any permitted AI assistance. We have not fabricated or modified evidence.” All members must provide their name, student ID, signature and date.

Marking rubric

Criterion	Marks	Evidence expected
Evidence handling and integrity	15	Complete receipt and handling records; justified preservation; matching pre and post-examination hashes; traceable responsibility.
Autopsy setup and methodology	15	Repeatable setup; justified settings and modules; documented processing, errors and time-zone assumptions.
Image discovery and recovery	25	Systematic search; supported identification of distinct files; sound recovery method; documented unsuccessful attempts and status distinctions.
Validation and interpretation	20	Signatures, opening checks and export hashes; evidence-linked analysis; corroboration; careful treatment of missing metadata and uncertainty.
Report and evidence package	15	Clear report and references; useful screenshots; complete register; functioning tagged HTML report and organised exports.
Individual contribution	10	Substantive practical and writing contribution, traceable log, specific reflection and demonstrated understanding.
Total	100	Group component 90 marks plus individual component 10 marks.

Markers assess the strength of the evidence and reasoning within each criterion. Finding eight files alone does not earn full marks, and a well-documented failed recovery can earn method marks. Unsupported assertions, unvalidated files and screenshots without explanation reduce the relevant criterion score.

Indicative performance descriptors

Band	General descriptor
70–100	Thorough, reproducible investigation; strong validation; precise evidence links; critical interpretation and clear limitations.
60–69	Sound investigation and good supporting evidence, with minor gaps in validation, traceability or critical discussion.
50–59	Competent completion of core tasks, with uneven detail, limited corroboration or descriptive interpretation.
40–49	Basic investigation demonstrated, with substantial weaknesses in documentation, validation or explanation.
Below 40	Insufficient practical evidence or major flaws in method, interpretation or submission completeness.

Submission checklist

- Group size is 4, with every member identified and contributing.
- Report answers the investigation questions and references genuine evidence.
- Hashes, configuration, evidence register and handling log are complete.
- Recovered files and HTML report are readable and included in the ZIP.
- Individual reflections, contribution declarations and AI declaration are included.