

Activity: Digital Forensic Investigation Report

Objective:

To analyze digital evidence from a simulated cyber incident and prepare a formal *Digital Forensic Report* demonstrating technical, analytical, and reporting skills.

Scenario:

A company's HR department reported that sensitive employee data may have been exfiltrated from an internal workstation. The IT security team discovered suspicious USB activity and unauthorized file transfers during non-working hours.

As a digital forensic investigator, you have been provided with:

- A disk image of the suspect's system (Suspect_PC.E01)
- A log file containing recent USB connection details
- Extracted browser history and email archives
- Metadata from key documents found on the system

Your task is to examine the provided evidence and reconstruct the sequence of events to determine whether data theft occurred, by whom, and how.

Tasks / Questions:

1. Case Introduction & Objectives (10 marks)
 - Briefly summarize the incident and define the scope of your investigation.
 - Mention the potential digital evidence sources you plan to examine.
2. Evidence Handling (10 marks)
 - Describe the evidence acquisition and verification process.
 - Explain how you would maintain *chain of custody* and ensure *data integrity*.
3. Forensic Analysis (30 marks)
 - Examine the provided evidence (USB logs, metadata, emails, etc.).
 - Identify and explain key findings such as file transfers, device usage, deleted files, or hidden data.
 - Include relevant screenshots, recovered timestamps, or hash values.
4. Timeline Reconstruction (15 marks)
 - Reconstruct the sequence of events leading to the data breach.
 - Indicate which user actions correspond to the suspected activity.
5. Interpretation & Conclusion (15 marks)
 - Summarize your findings.
 - Provide a logical conclusion on whether data exfiltration occurred, and if so, who was responsible.
6. Recommendations (10 marks)
 - Suggest security and policy measures to prevent similar incidents in the future.
7. Report Format & Professionalism (10 marks)
 - Ensure the report follows a formal *Digital Forensic Report* structure:
 - Title Page
 - Executive Summary
 - Investigation Details
 - Findings
 - Conclusion & Recommendations
 - References / Appendices

Deliverable:

Submit a Digital Forensic Report (PDF) with proper formatting, screenshots, and evidence-based analysis (approx. 8–10 pages).

Appendix

Digital Forensic Investigation Scenario

Case Title:

Investigation into Unauthorized Transfer of Confidential HR Data

Background:

On 28 October 2025, the HR Manager at ABC Pvt. Ltd. reported that confidential employee salary information might have been copied from an internal computer.

The IT Security team identified unusual USB and email activity on the workstation assigned to Rahul Verma (HR Executive).

You, as the digital forensic investigator, are asked to analyze the collected evidence and determine if data theft occurred.

EVIDENCE SET

You can give students these files as simulated “evidence folders.”

Each artifact below includes sample content you can directly copy into .csv, .txt, or .docx files.

USB Connection Log — USB_Activity_Log.csv

Date & Time	Device Name	Serial Number	Action	Drive Letter	File Transfer
2025-10-28 09:12	KingstonDataTraveler	1A2B3C4D5E6F	Connected	F:\	-
2025-10-28 09:14	KingstonDataTraveler	1A2B3C4D5E6F	File Copied	F:\	HR_Salary_Data.xlsx
2025-10-28 09:15	KingstonDataTraveler	1A2B3C4D5E6F	File Copied	F:\	employee_data_backup.zip
2025-10-28 09:25	KingstonDataTraveler	1A2B3C4D5E6F	File Deleted	F:\	employee_data_backup.zip
2025-10-28 09:27	KingstonDataTraveler	1A2B3C4D5E6F	Disconnected	F:\	-

Date & Time	Device Name	Serial Number	Action	Drive Letter	File Transfer
2025-10-28 09:45	SanDiskCruzer	9D7A5B8E4C1	Connected	G:\	-
2025-10-28 09:46	SanDiskCruzer	9D7A5B8E4C1	File Copied	G:\	meeting_notes.docx
2025-10-28 09:49	SanDiskCruzer	9D7A5B8E4C1	Disconnected	G:\	-

⌚ Clue: Only the Kingston device contains evidence of sensitive HR file transfers.

[2] Browser History Extract — Browser_History.csv

Visit Date & Time	URL	Title	Activity Type
2025-10-28 09:30	https://mail.proton.me/login	ProtonMail Login	Email
2025-10-28 09:31	https://mail.proton.me/inbox	ProtonMail Inbox	Email
2025-10-28 09:33	https://mail.proton.me/compose	Compose New Message	Email
2025-10-28 09:34	https://drive.google.com	Google Drive	Cloud Access
2025-10-28 09:35	https://wetransfer.com/upload	File Upload	File Sharing
2025-10-28 09:35	https://www.google.com/search?q=how+to+send+large+files+securely	Google Search	Search

Visit Date & Time	URL	Title	Activity Type
09:37			
2025-10-28 09:38	https://www.google.com/search?q=delete+file+activity+windows	Google Search	Search

⌚ Clue: The browsing timeline overlaps with the USB and email activity period.

[3] Email Log — Email_Archive.txt

Date: Tue, 28 Oct 2025 09:35:21 +0400

From: rahul.verma@abcpltd.com

To: rahulpersonal@gmail.com

Subject: Project Files

Attachments: employee_data_backup.zip (2.3 MB)

Message-ID: <E21EFD4A@abcpltd.com>

Hi Rahul,

Please review these files urgently from your home system.

Make sure to keep them secure.

Thanks,

Rahul

⌚ Clue: The email attachment matches the same file found in USB logs.

[4] File Metadata Report — File_Metadata_Report.csv

File Name	Author	Created Date	Modified Date	Last Accessed	Comments
HR_Salary_Data.xlsx	Rahul Verma	2025-10-27 16:05	2025-10-28 09:14	2025-10-28 09:16	"Salary data for export – confidential"
employee_data_backup.zip	Rahul Verma	2025-10-28 09:13	2025-10-28 09:15	2025-10-28 09:25	"Backup of HR files"
meeting_notes.docx	Priya Sharma	2025-10-20 11:20	2025-10-21 09:30	2025-10-28 09:46	—

⌚ Clue: employee_data_backup.zip was created right before email and USB activities.

[5] System Event Log — System_Events.txt

[2025-10-28 09:12] USB device detected: KingstonDataTraveler SN:1A2B3C4D5E6F

[2025-10-28 09:14] File HR_Salary_Data.xlsx opened by user rahul.verma

[2025-10-28 09:15] File employee_data_backup.zip created
[2025-10-28 09:16] Outlook process started by user rahul.verma
[2025-10-28 09:35] Email sent with attachment employee_data_backup.zip
[2025-10-28 09:37] Recycle Bin emptied by user rahul.verma

Clue: The event log confirms sequential file copy, compression, and email transmission.

6 Optional Disk Image Summary — Suspect_PC.E01 (description only for activity)

Students won't need a real E01 file — you can simulate this by providing:

- A folder called /Suspect_PC_Drive/ containing subfolders:
 - Documents/HR_Salary_Data.xlsx
 - Downloads/usb_sync_setup.exe
 - Temp/employee_data_backup.zip (deleted)
 - RecycleBin/ (empty)
 - Instruct students to "treat it as an image mount" and analyze file properties and timeline.
-

Student Tasks

1. Analyze all the above evidence to determine:
 - Whether data theft occurred
 - Which files were involved
 - How and when the data was transferred
 2. Reconstruct a timeline of events using timestamps from all files.
 3. Prepare a Digital Forensic Report that includes:
 - Introduction & Scope
 - Evidence Handling
 - Analysis & Findings (with table/graphs/screenshots)
 - Timeline Reconstruction
 - Conclusion & Recommendations
-

Expected Outcome / Learning Goals

Students will learn to:

- Correlate USB, email, and browser data.
 - Interpret metadata and event logs.
 - Apply forensic reasoning to reconstruct user activity.
 - Write a formal digital forensic report in professional format.
-