IT2564 Cyber Forensic Technologies
AY2024 Semester 2

Practical Assignment: Data Leakage
(25 marks)

Learning Outcome

- To apply the digital forensic process and methodologies
- To use various trusted forensic tools to collect, examine and analyze evidence from a given case.
- To practice forensic investigation documentation and presentation

Important Notes

- This assignment is to be completed by one student independently.
- It is important that you attempt the forensic examination and analysis yourself. You can consult classmates or tutors for issues you encountered. However, you are **NOT** allowed to directly copy others' work. It's considered a cheating offence which will result in immediate failure of the module.

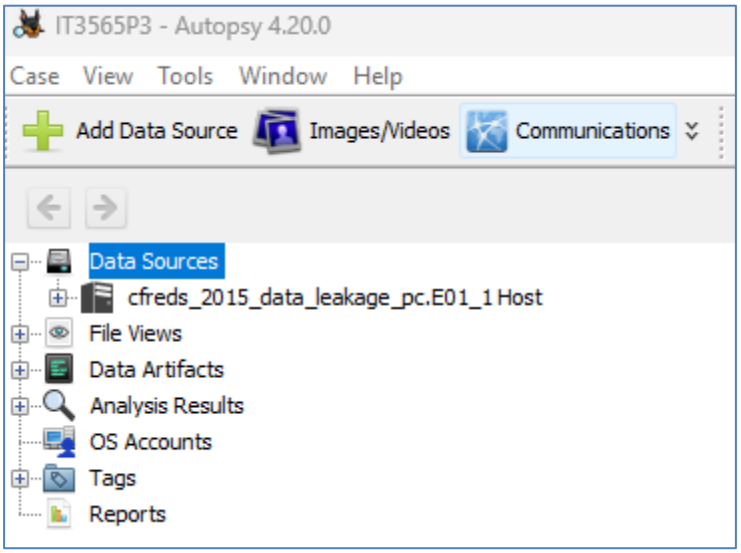
Instructions

1. Refer to the Data Leakage scenario given at
   https://cfreds-archive.nist.gov/data_leakage_case/data-leakage-case.html

2. You can find more details of the case from the file leakage-answers.docx at
   https://cfreds-archive.nist.gov/data_leakage_case/leakage-answers.docx

3. Open and log onto the student account in the IT2564 Win10_DFIR virtual machine.

4. Startup **Autopsy** forensic tool and open the recent case **IT3565P3**.



5. The case IT3565P3 was created with the PC Encase E01 Image file, and the default set of ingest modules were run on the image file.

6. Click **Case>Case Details** of the case and edit the Case Details.

7. Edit the **Examiner** details as follows

   Examiner
   - Name: Your Name (e.g. Tan Jun Wei)
   - Phone: Nil
   - Email: Your NYP email address
   - Note: IT2564 AY2024S2 Practical Assignment Done by Your Name.

8. Click Save to update the case details.

9. You are required to examine and analyze **ONLY the PC EnCase image file** in this assignment. Removable Media #1, #2 and #3 **MUST NOT** be used in this assignment.

Personal Computer (PC) – 'EnCase' Image	
Download Links	pc.E01, pc.E02, pc.E03, pc.E04 (total 7.28 GB compressed by EnCase) - hash
Imaging S/W	EnCase Imager 7.10.00.103
Image Format	E01 (Expert Witness Compression Format) converted from VMDK

10. You are required to use **Autopsy** to conduct Windows file system forensics as much as possible.

11. For those forensic tasks cannot be done by **Autopsy**, you are free to use any reputable tools to examine and analyze the evidence and add the screenshot files showing the evidence into the Autopsy case and Autopsy report.

12. Some artifact-specific tools will probably do a better job in parsing the artifact and present the information in a more user-friendly way than **Autopsy**. It's up to you to choose which tool to use in the forensic examination.

    Some tools for consideration are:

    - All-in-one forensic software
      - Autopsy (User Guide at http://sleuthkit.org/autopsy/docs/user-docs/4.19.3/)

    - Artifact-specific tools
      - Windows Registry
        - **Registry Explorer**
        - RegRipper (https://code.google.com/p/regripper/)
      - Windows Event Logs
        - Event Viewer
      - File Metadata
        - ExifTool (http://www.sno.phy.queensu.ca/~phil/exiftool/)
        - Jumplister
        - Structured Storage Viewer
        - ShellBags Explorer

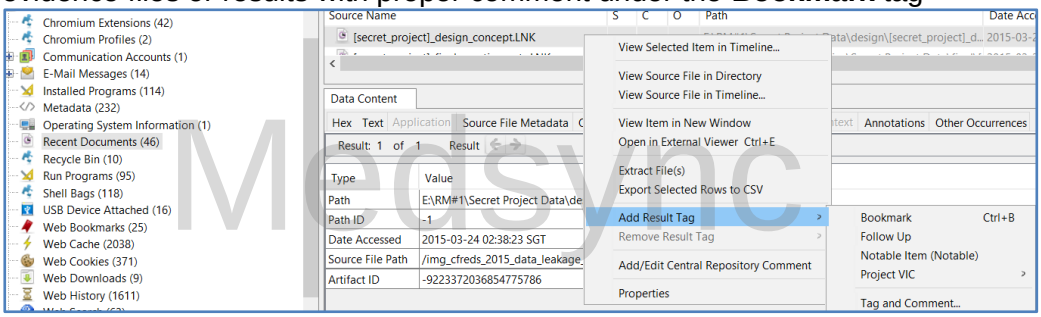
    - Evidence preview, image mounting, files exporting
      - FTK Imager

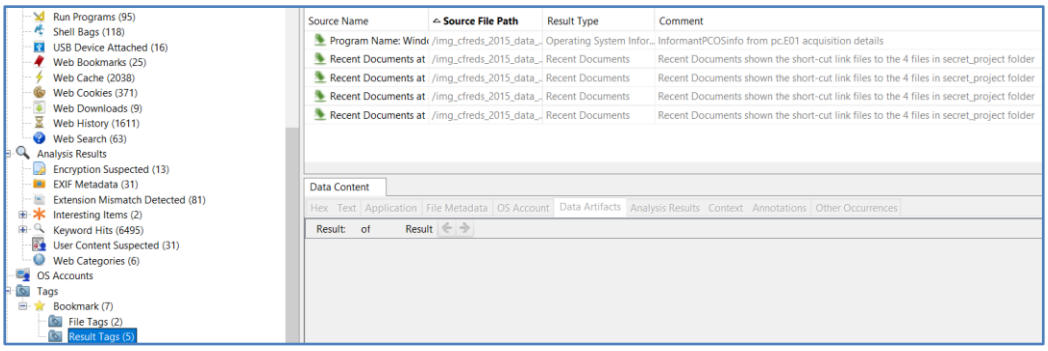
13. Case Brief

1) Iaman Informant was working as a manager of a company that developed state-of-the-art technologies and gadgets.
2) Mr Informant made a deliberate effort to hide the leakage plan. It was suspected he discussed it with Mr Conspirator using an e-mail service like a business relationship.
3) It was suspected that Mr Informant committed unauthorized access to the network file server of the company and downloaded product design documents.
4) An EnCase forensic image file was created from the local drives of the PC used by Mr Informant.
5) The PC EnCase E01 image file was added to the **Autopsy** forensic tool in the virtual machine Win10_DFIR and was processed by ingress modules.

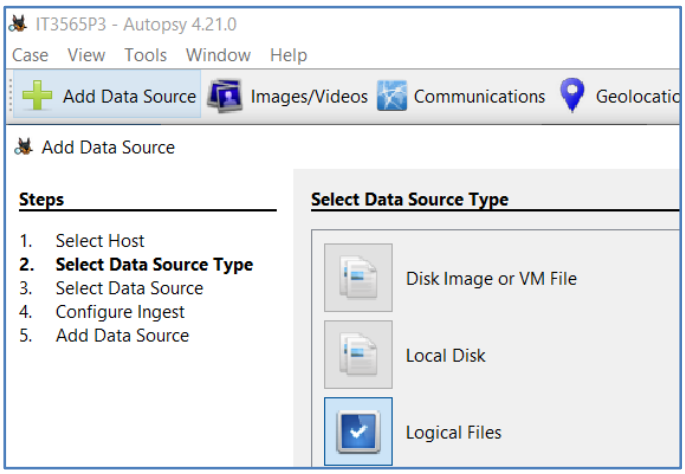
14. You are required to

1) Use **Autopsy** and other relevant forensic tools to examine and analyze the PC EnCase E01 image file and create specific tags with relevant names on evidence to answer the practical assignment questions 1 to 10.
2) Present the answer (evidence) based on date/time at the time zone of the location where the crime was committed, or UTC.
3) Locate the evidence files or results in the case, Tag and Comment the located evidence files or results with proper comment under the **Bookmark** tag

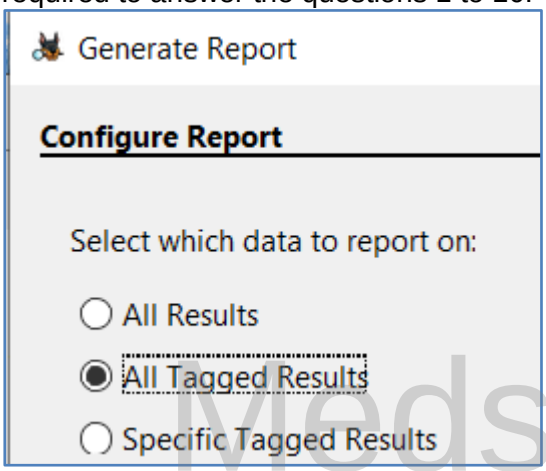




4) Whenever required, add screenshot images (jpg files) of the relevant evidence discovered by other relevant tools as data sources **Logical Files** into the **Autopsy** case.
    - Click **Add Data Source**, select **Logical Files** to add screenshots of the relevant evidence.



5) Create an **Autopsy HTML** report contains **All Tagged Results** for the evidence required to answer the questions 1 to 10.



6) Zip up the folder of the **final Autopsy HTML report** and submit it to POLITEMall.

7) Restrict the size of the zipped report to be 50MB or smaller.

8) Draft and submit **an examiner notes file** in MS Word format (docx) with the steps you took to locate the evidence files/results to POLITEMall..

15. Practical Assignment Questions, answer all 1 to 10 questions, maximum 2 marks for each question

    1) What is the MD5 hash value of the E01 drive image of Mr. Informant's PC?

    2) What is the computer name and time zone of Mr. Informant's PC?

    3) List all traces about the user logon/logoff date and time (in UTC or Mr. Informant's PC time zone).

    4) What were the files deleted and were found in 'Recycle Bin', and when did the deletion happen?

    5) List all e-mail messages sent or received by Mr. Informant related to the data leakage case.

    6) What files Mr Informant that had accessed in the company's network drives, and when?

    7) What and when were the files downloaded by Mr. Informant from the Internet onto his PC?

    8) How did Mr Informant erase evidence on his PC on the last day '2015-03-25'?

    9) When and what files in Mr. Informant's Google drive were accessed (created / modified / deleted)?

    10) What were the product design documents disclosed in this case, and how were the documents disclosed?

Submission

At the end of the examination and analysis, you are required to deliver the following 2 items.

- A 5-minute demonstration to your module tutor on how you use **Autopsy** or other relevant forensic tools to find the evidence to answer the TWO questions, **3 and 10**. (5 marks)
    - The demonstration will be carried out during Week 17-18 practical lessons.
- Submission of
    - **An Autopsy HTML report** in zip file format with tagged evidence files and results. (10 marks)
    - **An examiner notes file** in MS Word format (docx) with the steps you took to locate the evidence files/results. (10 marks)

Assessment Rubric

Demonstration (5 marks)

5 marks	• Clear demonstration on the forensic work. • The tool is used correctly. • The forensic work involves complex steps and is complete.
3-4 marks	• Relatively clear demonstration on the forensic work. • The tool is used correctly most of the time. • The forensic work involves simple steps and is somewhat complete.
1-2 marks	• Some demonstration on the forensic work. • The tool is used with misconfigurations. • The forensic work is incomplete
0 mark	• Unable to demonstrate any forensic work

Autopsy HTML Report and **Examiner notes** – (answers to the 10 questions: maximum 2 marks per question)

2 marks	Deep understanding of the forensic artifact and show full details (tagged files and results with relevant comments and detailed examiner notes on the steps) on findings/evidence related to the answer to the question.
1.5 marks	Good understanding of the forensic artifact and show good details on findings/evidence
1 mark	Some understanding on the forensic artifact and show some screenshot/explanation of findings related to the answer to the question.
0.5 mark	Demonstrate little understanding of the relevant forensic artifact and steps to obtain the findings/evidence
0 mark	Does not show any understanding of the relevant forensic artifact and steps to obtain the findings/evidence.

Sample Answers

When and where (the computer name) Mr Informant last logon to? (2 marks)

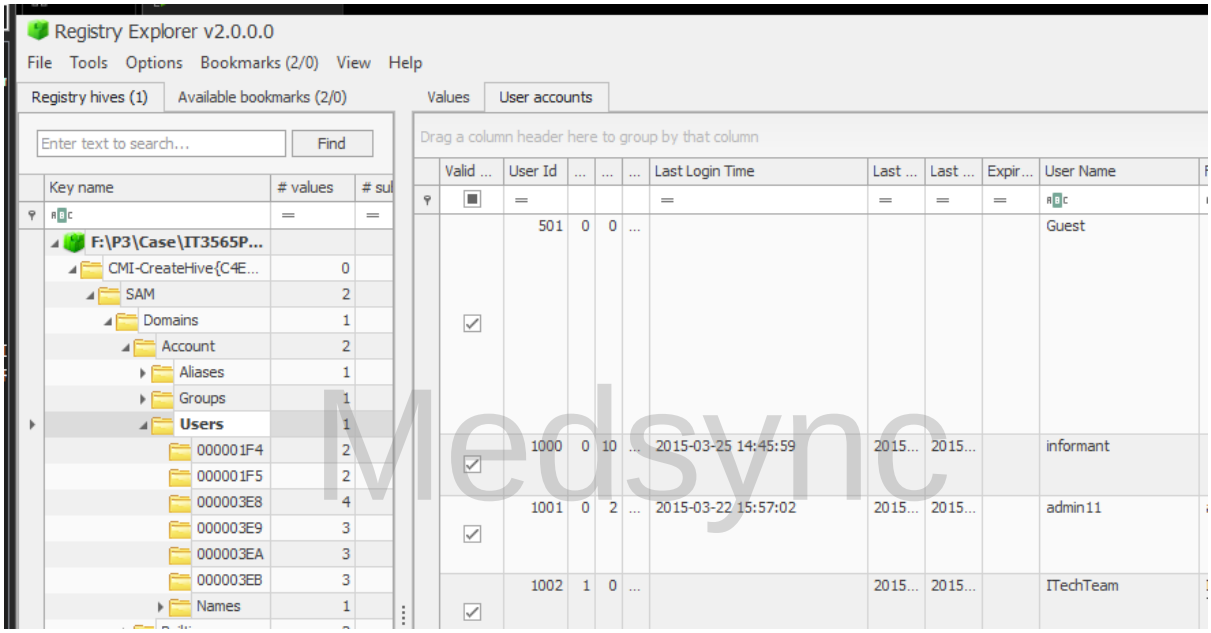
Sample Examiner Notes

Using SAM and SYSTEM file with Registry Explorer

The link to the tool is https://www.sans.org/tools/registry-explorer/

I need the SAM and SYSTEM file both stored in **%SYSTEM_ROOT%/System32/Config/**

The SAM Hive stores account information for users, like informant, and contains the property Last Logon Time



In the second row I can see that the Last Login Time for informant is 2015-03-25 14:45:59 (UTC 00:00) which is **2015-03-25 22:45:59 SGT** (UTC +8)

I can get the computer name from the SYSTEM FILE under the key ControlSet001/Control/ComputerName using Registry Explorer