## Patents Company Case: Company Name = Project2400

In 2009, a patents company started operating on Friday, November 13th, 2009 and stopped operating on Saturday 12th December 2009. The company’s main focus was on outsourcing patent searching, but a Month is a very short time for a company to come into existence and then disappear. An insider complaint was filed against the company with a government agency and as a result the company is now under investigation. You have been hired as a digital forensics investigator to try and establish a timeline of events and to find evidence of any wrong-doing. You are provided with an image of last days of trading and the USB memory stick of one of the employees.

1. Friday, 13 November has no images, because the scenario did not officially start until the following Monday (16 November). Your data may contain drive images from Thursday, 12 November. These are for reference (e.g. prior to any employee activity).

**Task**

1. You have been given 2 files on a USB stick
2. Select the file  **Charlie-2009-12-07.E01**
3. Convert this file to a **.dd** file in FTK-Imager (this should have a .001 extension)
4. Select the file **Charlie-work-usb-2009-12-11.E01**
5. Convert this file to a **.dd** file in FTK-Imager
6. Open **Prodiscover**, add the **.dd image file.**
7. Expand **Content View** until you see the files.

You are requested to confine the search to two key phrases:

1. Click the **Search** toolbar button, click the **Content search** tab, tick the **Search for the pattern(s)** radio button. In the text box directly below type:

**project2400** on one line and

**craiglist** on a second line.

1. **Click** on the image file (highlight the file)
2. Then click **OK**. The search operation will take time. You will know that it is working be observing the bottom left of the screen (i.e. **searching in: xxxxx)**
3. In the **Search 1 tab** of the search results, click the **Filter** button, and then click **project2400.** Read the files, and then click the **Selection** button and click **Select All**. Close add comments box). When finished, click **Add to Report.**
4. Click the **Search** toolbar button**.** In the search dialog box, click the content search tab, in the **Search for Patterns text box** type
   * 1. **kitty** on one line and
     2. **kitten** on the other
5. Select the image file and click OK
6. In the **search tab 2** of the search results, click the **filter** button and then click **kitty**.
7. Click the check box next to the file that doesn’t have an extension, and then click **add to report**.
8. In the tree view, click **Report.** Then **Export** on the toolbar, In the export dialog box click **RTF Format,** browse to your **work folder.** Type **Forensic-report-Nov-21** click OK.
9. Navigate to the work folder and review the report.

You now have a report of the important artefacts on the disk. Use this report and the search results to find and document evidence and to write your assignment report. You should report only on the evidence of interest (not all files) and only on those files that have been identified in the search results.

Find any emails of interest and provide a timeline.

**Required:**

1. Documentary evidence of having followed forensic procedure.
2. Logbook – how you did the task, what you did and when you did it
3. Report – presentation of the evidence of interest and the timeline.
4. Appendix – Prodiscover report.

**You are required to:**

1. **Provide all documentation in a single uploaded document, save the document as [your name]-[A2-2021]**
2. **The format of the document should be:**
   1. **Assignment Cover Sheet**
   2. **Introduction to the case**
   3. **Forensic Procedure**
   4. **Logbook**
   5. **Report** (should contain the evidence in a way that is clear and unambiguous)

**Submission Date:**

**Sunday 28th November @ 11.59 pm.**

**Hard copy to be submitted Tuesday 30th November.**

**Additional instructions:**

1. If uploading to Blackboard, please **ensure** that you do so at least two hours before the deadline. You should realise that things can go wrong so please ensure that you have completed and submitted the assignment well before the due time.
2. Please also include **Assignment Cover Sheet.**

**Help for completion of Assignment**

**Videos**

[**https://www.officetimeline.com/make-timeline/microsoft-word**](https://www.officetimeline.com/make-timeline/microsoft-word)

<https://www.whatisfileextension.com/mab/>

<https://smallbusiness.chron.com/open-msf-file-27913.html>

<https://www.youtube.com/watch?v=nK5QpGSBR8c>

<https://www.youtube.com/watch?v=WlMKqh4xeI0>

**Template for logbook**

[**https://www.oreilly.com/library/view/implementing-digital-forensic/9780128045015/XHTML/B9780128044544150130/B9780128044544150130.xhtml**](https://www.oreilly.com/library/view/implementing-digital-forensic/9780128045015/XHTML/B9780128044544150130/B9780128044544150130.xhtml)

**Shortened Report Format:**

Executive Summary

Summary of Evidence

Email ID, date, time, summary of content in your own words, hash

Detailed Evidence

Email ID and text content of the email only

Header separately

(Note: Presentation is important)

Conclusion

Appendix: Timeline.