Assignment 4: Smartphones

Digital Forensics

Dipl.-Inf.(FH) Karsten Theiner

Assignment 4: Smartphones

Beth Dutton had been invited by Heisenberg to the Vienna Inn in Vienna, VA on July 21st at 5:00 PM where she was arrested by local Police for grand theft.

Under questioning, Beth revealed that her sister, Marsha Mellos, had introduced Heisenberg to her and had stated that he was responsible for stealing cars whereas she and her sister were innocent.

Assignment 4: Smartphones

Questions (12 points):

- Are there clues or evidence for Heisenberg dealing with (stolen) cars? (2 points)
- Heisenberg used his cellphone during the arrest. Did he create any recordings of the arrest? Note: arrest took place on 2021-07-20 (1 point)
- Are there any clues for Heisenberg taking an interest in cryptocurrency? (1 point)
- Did Heisenberg use any apps for file hiding or encryption? (1 point)
- Are there any clues for Heisenberg connecting or planning to connect external drives to his Cellphone? (1 point)

Assignment 4: Smartphones

- What is the name of the vehicle Beth's phone connected to on 2021-04-06? (1 point)
- Where was Beth on 2021-06-18 around 01:00 UTC+0? What did she do? (2 points)
- In which city was Beth when she made a call to Marsha on 2021-06-29? (2 points)
- Did Beth use the app Waze on 13.07.2021-07-13? If yes, when and how often? (1 point)

Assignment 4: Smartphones

Further information:

- Cellebrite Reader runs on Windows only. Use is optional but recommended. A small tutorial video will be in the downloads folder next to the images
- You can use Cellebrite Reader to find evidence faster and use Screenshots of or reports generated by Cellebrite Reader to augment your report. However, it is **required** to manually verify your findings and to show the actual sources for your evidence (e.g. contents of databases, Plists, log-files, etc).
- Report has to be comprehensible and pleasant (target group: non-technical investigators, courts)

Recommended Tools:

- Any SQLite viewer (e.g. DB Browser for SQLite), any Plist viewer (e.g. included in iBackup Viewer)

Assignment 4: Smartphones

- Maximum points: 14
  - 12 for questions, 2 for report form
- Deadline: 2022-01-19 23:55
- Solve alone!
- Download images at:
  - Dropbox: https://www.dropbox.com/sh/df90i7c8kshkct7/AAB-68ouDs8F6_CzHUP42VjCa?dl=0
  - Key for Resilio Sync (www.resilio.com): BBC4IMA2IKZYU645FTIS2HRXZUDORYLA5
- Report has to be comprehensible and pleasant (target group: non-technical investigators, courts)
- submission:
  - report as pdf, including answers to all questions
  - if you have written code, make a ZIP file including the report

Assignment 4: Smartphones

File checksums:

Filename	SHA1
Beth iPhone X Cellebrite Reader Report.ufdr	EA5FA466B61BEB0785FB59405AA789DB1CE36C1E
Beth iPhone X Full File System.zip	D01C678EA0A9DF57DDC3329EA4F89F7DEE819014
Cellebrite Reader Tutorial.mkv	5B64FCAFD8D94BE64656D7C0D79957C944F6F376
CellebriteReader.exe	327CC80F3A477599ED2F62CB467677830405386A
Heisenberg Samsung Cellebrite Reader Report.ufdr	A76B933B785A79DA2B1B608470C87A3C2C7C0B94
Heisenberg Samsung Full File System.zip	61C9CEC020F82C14CF387F6A9288EF1049A57533