Part 1

Q1. Look at the data on the file system (Click on Data Sources and look at the hex values on the right). The file system has no files, but why are we able to find items on the disk image? Explain why the file system has no files but there are items that can be found on the disk image.

ANS เมื่อผู้ใช้สั่งลบไฟล์ ระบบปฏิบัติการจะดำเนินการเพียงแค่ ลบหรือทำลายMetadata และรายงานว่าพื้นที่ดังกล่าวเป็น พื้นที่ที่ยังไม่ได้ใช้ ซึ่งการลบข้อมูลเมตาไม่ได้หมายความว่าระบบจะ ลบเนื้อหาไฟล์ (File Content) จริงๆ ที่อยู่ในเซกเตอร์ดิสก์ ทันที ข้อมูลดิบของไฟล์ยังคงอยู่บนดิสก์ในพื้นที่ที่ถูกทำเครื่องหมายว่าเป็น "ว่าง" จนกว่าจะมีไฟล์ใหม่ถูกเขียนทับลงไป

Q2. How many objects can you find?

ANS 14

Q3. List all the objects here and report on whether or not the content is accessible

or damaged/corrupted. Also note which files were actually already deleted.

(open as logical file and read only text)

ANS

Q4. Think securely: If we want to delete files on a magnetic hard disk and not

have them be recovered by any tool, what do we need to do? And how much

time do you think you need to wipe a 1TB magnetic hard disk?

<mark>ANS</mark> การเขียนทับ อย่างน้อย7รอบ ประมาณ14ชั่งโมง หรือใช้แม่เหล็กแรงๆ ในไม่กี่วินาที
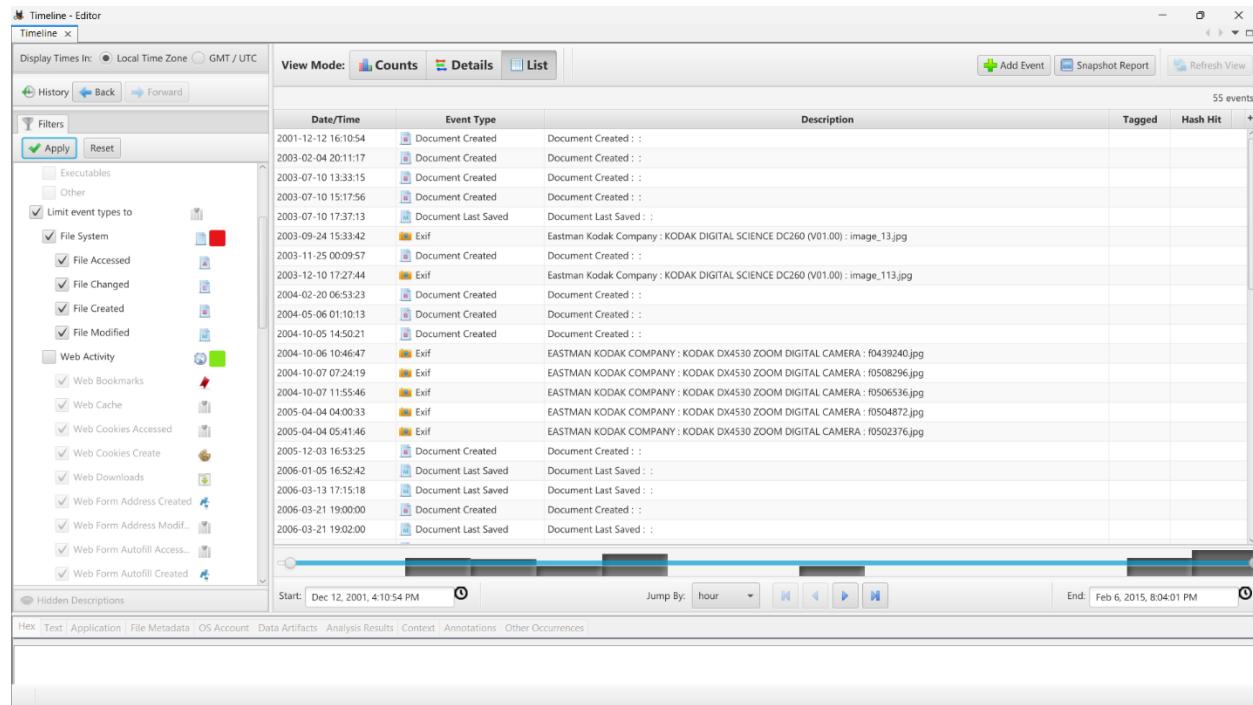
Q5. Will file carving be able to recover deleted files on an SSD? Why or why not?
<mark>ANS</mark> ไม่สามารถกู้คืนได้ หรือทำได้ยากมาก SSD ใช้คำสั่ง TRIM หรือ UNMAP ซึ่ง คอนโทรลเลอร์ SSD จะตอบสนองโดยการ
ล้างข้อมูลจริง

Part2
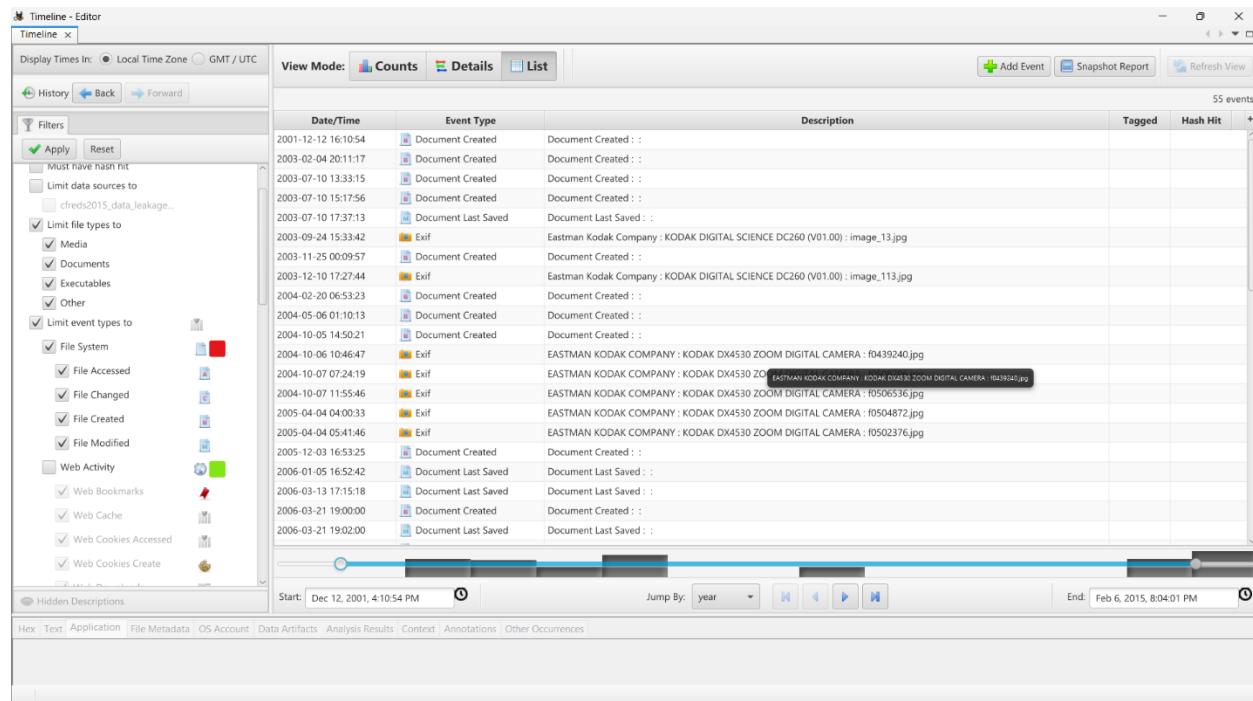
1. List all directories that were traversed in 'RM#2'.

ANS found 55 events

2. List all files that were opened in 'RM#2'.

ANS I don't know what do ya mean traversed and opend?

3. Recover deleted files from USB drive 'RM#2'. What files were you able to recover?

ANS รูปส่วยใหญ่เปิดได้ แต่mp4เปิดไม่ได้

4. What actions were performed for anti-forensics on USB drive 'RM#2'?

[Hint: this can be inferred from the results of the above question]

ANS ทั้งมีการพยายามลบหลักฐานทิ้ง และ มีการปลอมแปลงฟอร์แมตไฟล์ สังเกตว่า มีชื่อไฟล์แปลกๆที่ตั้งชื่อลงท้ายด้วย .txt แต่เนื้อหาข้างในไม่น่าใช่ จึงลองเปลี่ยน TYPE เป็น .ppt

5. Recover hidden files from the CD-R 'RM#3'. What files were you able to recover?

ANS found 15 files

6. What actions were performed for anti-forensics (data hiding) on CD-R 'RM#3'?

ANS น่าจะแค่ลบไฟล์ทำลายหลักฐานทิ้ง มั้ง