Spring 2022

Reference Document: Goal 17 Each1 Teach1 Merritt College Digital Forensics Internship 2022

This document is Calvin Hsieh's Grading Report of Demetric Jones's Forensic Examiner's Report and Evidence Document.

Demetric's Documents are copied for grading purposes.
Copy of Demetric's Forensic Examiner's Report (This document).
Copy of Demetric's Evidence Document.

Solution Document and Case Document by Batkhuu Batsaikhan.

==========

Batkhuu's Grading Rubric:

.....
.....

Counterfeit LV: Case Description, Grading Rubric (By Batkhuu Batsaikhan)

Victim reported receiving fake products from online shopping, specifically getting it from craigslist and Alameda County sheriff's office caught the suspect and retrieved a laptop and 8 fake Louis Vuitton bags for evidence.

Case file: suspect_device1

Grading
100- 90 A
89 - 80 B
79 - 70 C

EXAMINATION

EXAMINER'S NAME: Demetric Jones 03/26/2022

_____

EXAMINER'S SIGNATURE 03/26/2022

TITLE: Intern Examiner

_____

TECHNICAL REVIEWER'S SIGNATURE DATE

FILE NAME: xxxxxxx

_____

ADMINISTRATIVE REVIEWER'S SIGNATURE DATE

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

69 - 50 D
49 - 0 F

Visited websites/ website history

- 6 or more artifacts – 15 points 6 found: 15 points.

Downloaded files

- 4 or more artifacts – 15 points 4 found: 15 points

Documents

- 4 artifacts – 15 points 4 found: 15 points

Pictures

- 3 artifacts – 15 points 3 found: 15 points

Recycle bin

- 1 artifacts –10 points 1 found: 10 points.

Deleted and removed from recycle bin

- 2 or more – 10 points
  - **Found screenshot, but it was not categorized as carved. Not sure whether the deleted password protected folder was found. However, other deleted items were found: 10 points.**

Installed/run programs – 10 points

Solution did not provide a list of installed and run programs, but many (installed / run) programs were found: 10 points.

Email addresses -10 points

Only one of the two protonmail addresses is identified in the FE Report. victimemail@proton.com was not identified: 5 points?

Extra points

USB attached – 10 points 5 found: 10 points

Hidden Partition -10 points 9 found: 10 points

Forensic Examiner's initials _____
Technical Reviewer's Initials_____
Administrative Reviewer's Initials_____

LAB NUMBER: xxxx DATE: [03/26/2022]
AGENCY: San Francisco Police Department

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

Password protected file – 10 points

The report seems to have identified drive H as containing password protected files, but it did not identify the password protected zip file: 5 points?

Total Score: 120/100.

==========

Demetric's Forensic Examiner's Report:

.....
.....

DIGITAL & MULTIMEDIA EVIDENCE EXAMINATION REPORT

SUBMITTING AGENCY:	San Francisco Police Department
LABORATORY NUMBER:	xxxxxx
EXAMINATION REQUESTED BY:	Sergeant xxxx
VICTIM OR SUSPECT:	UNKNOWN
CASE NUMBER:	xx-xxxx
LABORATORY CLASSIFICATION:	Digital & Multimedia Evidence
DATE OF REPORT:	[03/26/2022]
OFFENSE:	Counterfeiting

EVIDENCE SUBMITTED:

One unpackaged evidence item (Item 1), relative to the above case, was received into the Laboratory from Sergeant Lee by Sheriff's Technician Jones on [03/24/2022]. The item was found as follows:

_____

Forensic Examiner's initials _____
Technical Reviewer's Initials_____
Administrative Reviewer's Initials_____

LAB NUMBER: xxxx DATE: [03/26/2022]
AGENCY: San Francisco Police Department

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

Item #1:
.VDI Image Batkhuu Batsaikhan (Counterfeit LV Case v2)-15GB

Counterfeit LV Case Description Grading Rubric.docx

Forensic System/Software/Tools – Acquisition (.VDI):

System: HP Laptop, powered on [03/26/2022], no errors during boot
Write Block Device used: N/A
Acquisition software used: Oracle VM VirtualBox, VBoxmanager.exe (convert to RAW file)

Forensic System/Software/Tools – Analysis (IMG): Autopsy 4.19.3

System: HP Laptop, powered on [03/26/2022], no errors during boot
Analysis software used: Autopsy 4.19.3

REQUEST:

On [03/26/2022], Sergeant Lee of the San Francisco PD submitted a request for the forensic examination of a hard drive reportedly removed from a suspect's computer. Sergeant Lee requested an examination of the hard drive for any images, videos, emails, chat logs, active/deleted/altered files, or any other files that would assist with her investigation.

Sergeant Lee prepared a search warrant that was signed by a judge of the Alameda County Superior Courts authorizing the examination of the digital media. The search warrant was reviewed prior to processing this case.

On [03/26/2022] I examined the submitted hard drive. It appeared to be in working condition. I documented my examination of the hard drive with photographs(evidence doc). In order for the drive to be read the .vdi must first be converted to a raw format. To do the conversions I ran VBoxmanage.exe in the command prompt along with image location paths. Once finished, I then loaded the .img into Autopsy to begin processing the image to extract and analyze the data as well as recover deleted files.

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

I performed a keyword search using the following terms (not case-sensitive)

- Suspect
- LV
- Bag
- .txt
- .png
- Receipt
- PDF

Major Evidence Found

Device Overview

1. System
    a. System name: DESKTOP-MQL10PA
    b. Processor: AMD64
2. Software
    a. OS: Windows 10 Home
        i. Installation Date / Time: 2022-03-19 17:40:13 PDT
        ii. Language: English
    b. Owner: Suspect
3. Partitions
    a. Partition number (allocation: Sector location)
        i. Vol 1: Unallocated
        ii. Vol 2: NTFS / eXFAT
        iii. Vol 3: NTFS / eXFAT - Main Drive C:/
        iv. Vol 4: Unallocated
        v. Vol 7: NTFS / eXFAT
        vi. Vol 8: Unknown Type
        vii. Vol 9: Unallocated
    a. Hidden Partitions (allocation: Sector location)
        viii. Vol 7: NTFS / eXFAT - Drive H:/
        ix. Vol 8: Unknown Type - possible error when creating partitions
4. Accounts
    a. Suspect
    b. Admin

c. Guest

5. Devices Attached
   a. USB 1: Root Hub
   b. USB 2: Root Hub 3.0
   c. USB 3: Gembird MicroSD Card Reader/Writer
   d. USB 4: VirtualBox USB Tablet
   e. USB 5: VirtualBox USB Tablet

Internet-Related

6. Internet Activities
   a. Web Search Terms
      i. Chrome
      ii. Firefox
      iii. Louis Vuitton
      iv. WinRaR
      v. Craigslist
      vi. Adobe
      vii. Proton mail
   b. Web Site Visited
      i. Craigslist.org
      ii. google.com
      iii. Get.adobe.com
      iv. Mozilla.org
      v. Protonmail.com
      vi. Us.louisvuitton.com
      vii. Louisvuittonreplica.to
      viii. Pdffiller.com
      ix. Tech-latest.com
      x. win-rar.com
   c. Web Sites Bookmarked
      i. None
   d. Online Accounts
      i. suspectemail@protonmail.com
      ii. Acct 2
   e. Online Map Locations and Directions
      i. None
   f. Downloaded Files
      i. Tracking information.png
      ii. Conversation craigslist.jpg (Evidence Document identify it as recycle bin item)

iii. LV_neverfull_gm.jfif

g. Downloaded Programs
   i. ChromeSetup.exe
   ii. Firefox Installer.exe
   iii. Winrar.exe
   iv. Adobereader.exe

7. Emails
   a. Email Accounts
      i. Suspect used web email with protonmail
   b. Suspicious Email Addresses
      i. Email addr 1
      ii. Email addr 2
      iii. etc.
   c. Email Subject Lines or Messages Found
      i. None
   d. Email Attachment Downloads
      i. Conversation_craigslist.jpg (using Protonmail)
      ii. Tracking information.png (using protonmail)
   e. Local Email Clients
      i. None found
   f. Email Backups
      i. None found

Data Files and Programs

8. Files
   a. Plain Text Files
      i. Make money from fake LV.txt
   b. Documents of other formats
      i. Suspect receipt.pdf
      ii. Victim receipt.pdf
      iii. Receipt 8 bag.pdf (not visible)
   c. Images
      i. LV bag.jfif
      ii. Louis Vuitton Site .png
      iii. Louis Vuitton Craigslist post .png (carved?)
      iv. Louis Vuitton Replica Site .png
      v. Tracking Information.png
   d. Videos / Audios / etc.
      i. None

e. Opened Files
    i. None
f. Hidden Files (in visible folders, or in hidden partitions)
    i. Password Protected Folder in H:/
g. Files with mismatched extension
    i. None
h. Encrypted Files
    i. None
i. Deleted Files
    i. Conversation Craigslist.jpg
j. Recovered / Carved files
    i. Suspect Reciept.pdf
    ii. Victim Reciept.pdf

9. Password
    a. Password found
        i. LV in .txt document
    b. Password guessed
        i. None
    c. Password cracked
        i. None
    d. Password files
        i. File name Password_Protected H:/ (assuming suspect tried to add a password to protect file)

10. Programs
    a. Installed Programs
        i. Firefox Browser
        ii. Chrome Browser
        iii. WinRar
        iv. McAfee
    b. Executed Programs
        i. Firefox
        ii. Chrome
        iii. WinRar
        iv. McAfee
        v. Adobe
    c. Log files
        i. None
    d. Uninstalled Programs
        i. None

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

Peripherals and Networks

11. Phone backup data
    a. None found
12. Network Traffic Files (PCAP):
    a. None found

Reconstructed Timeline of Major Events

Time / Date	Event	Artifact Created	Artifact Location	Evidence Category

CASE #: xx-xxxx
CRIME: xxxxxx
VICTIM OR SUSPECT: UNKNOWN

AUTHENTICATION:

During the acquisition process, the forensic software creates a hash value of the media being imaged. These hash values were compared to those generated after imaging and processing of the image file. I verified that the hash values were the same. This indicated that the image file is identical to the original and was not altered during processing.

EVIDENCE DISPOSITION:

Upon completion of the data extraction, the original evidence (Item 1) and the report CD-R (Item 2) prepared for release to the submitting agency.

DISC CONTENTS (as applicable):

N/A