



# **DIGITAL FORENSICS**

(ACCA7031)

## **INVESTIGATIVE PROCESS**

# ENSURING INTEGRITY

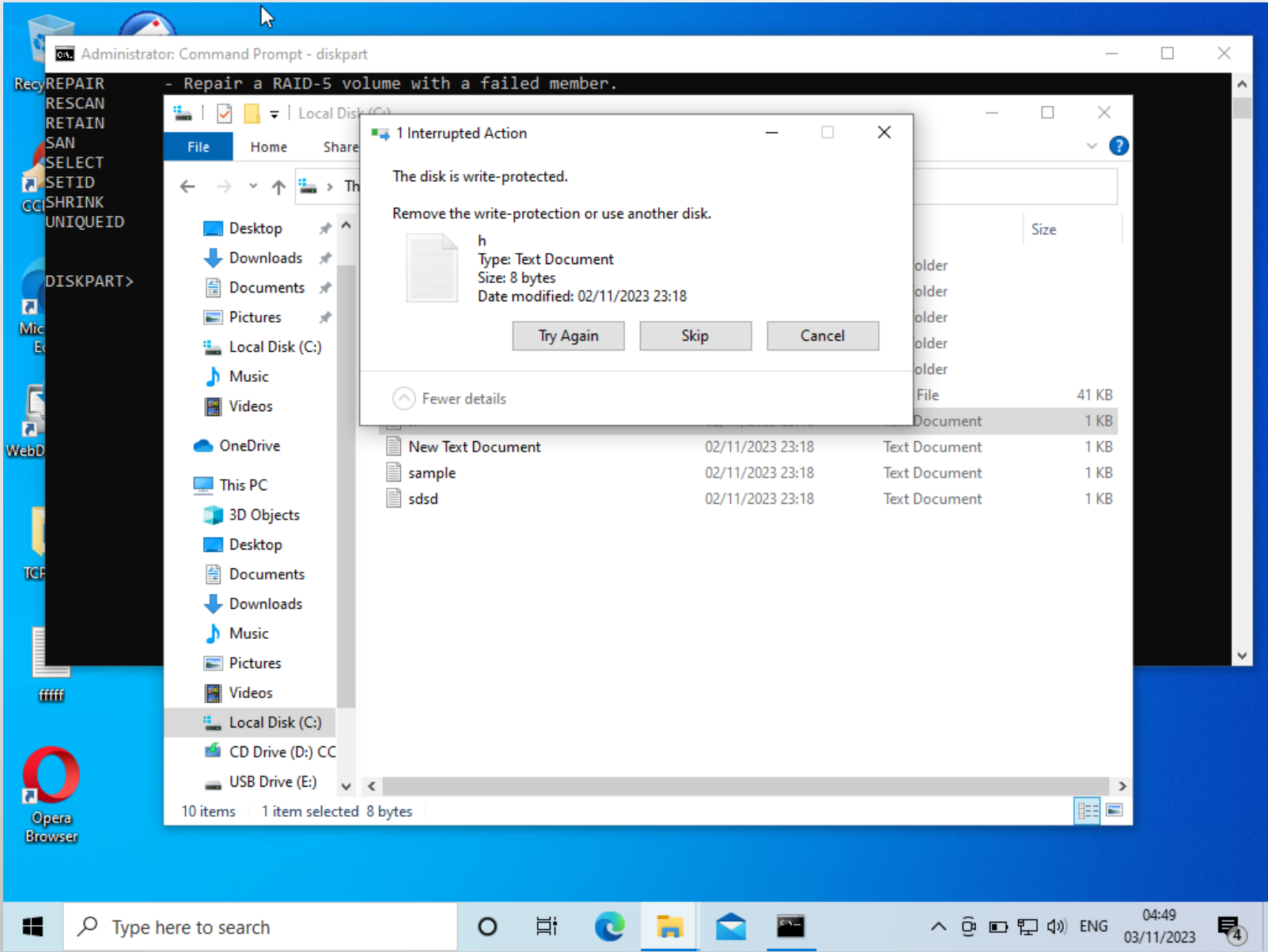
## STEPS :

1. Access Control
2. Backup and Recovery
3. Hashing and Digital Signature
4. Monitoring and Auditing
5. Data validation

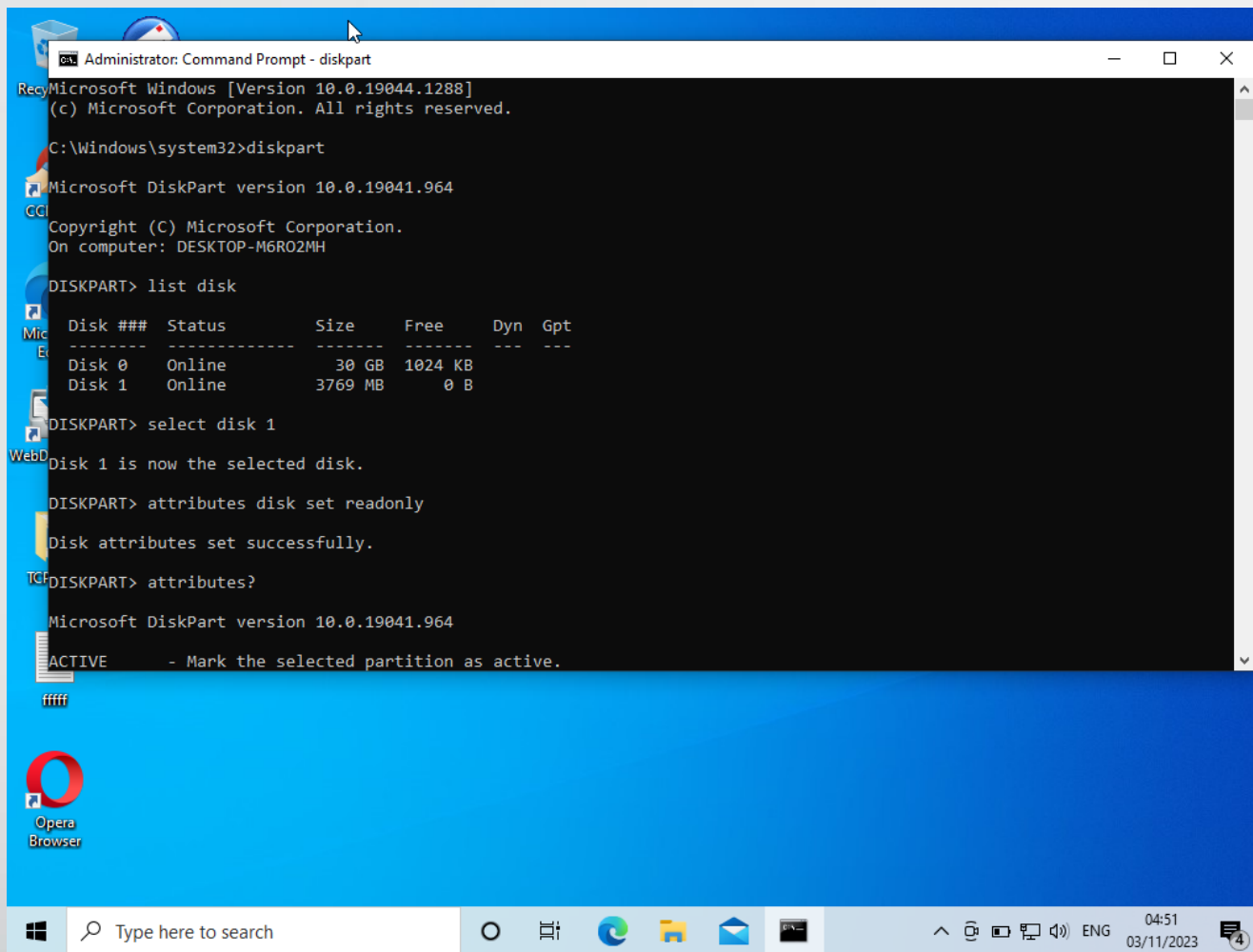
# USING WINDOWS REGISTRY

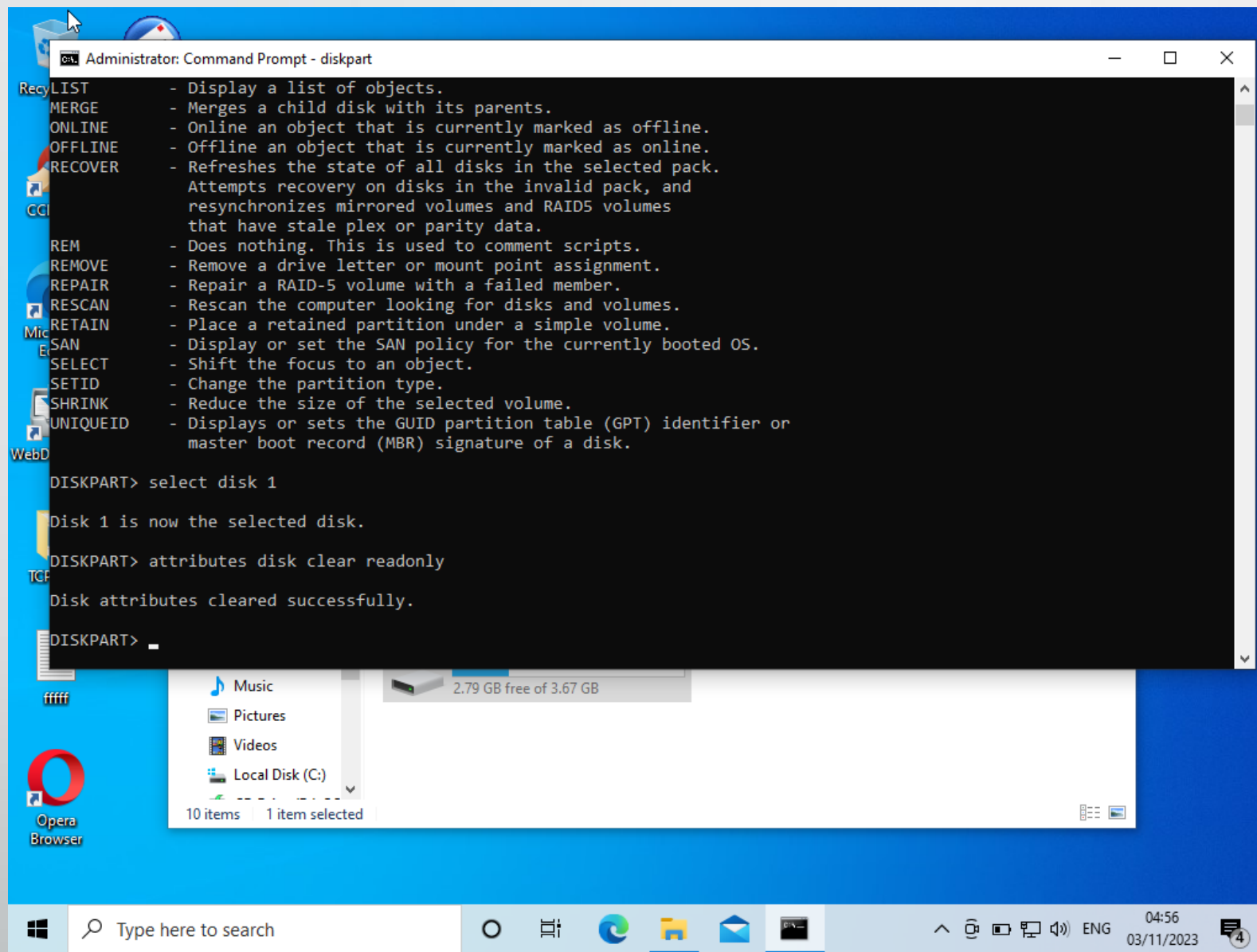
Preventing data write access to external storage devices through the Windows Registry.

- ❖ Access Windows Registry
- ❖ Navigate to USB Write Protection Key:  
`HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies
- ❖ Create or Modify DWORD Value:
- ❖ Restart Your System
- ❖ Test Write Protection



## Write to Protection Error

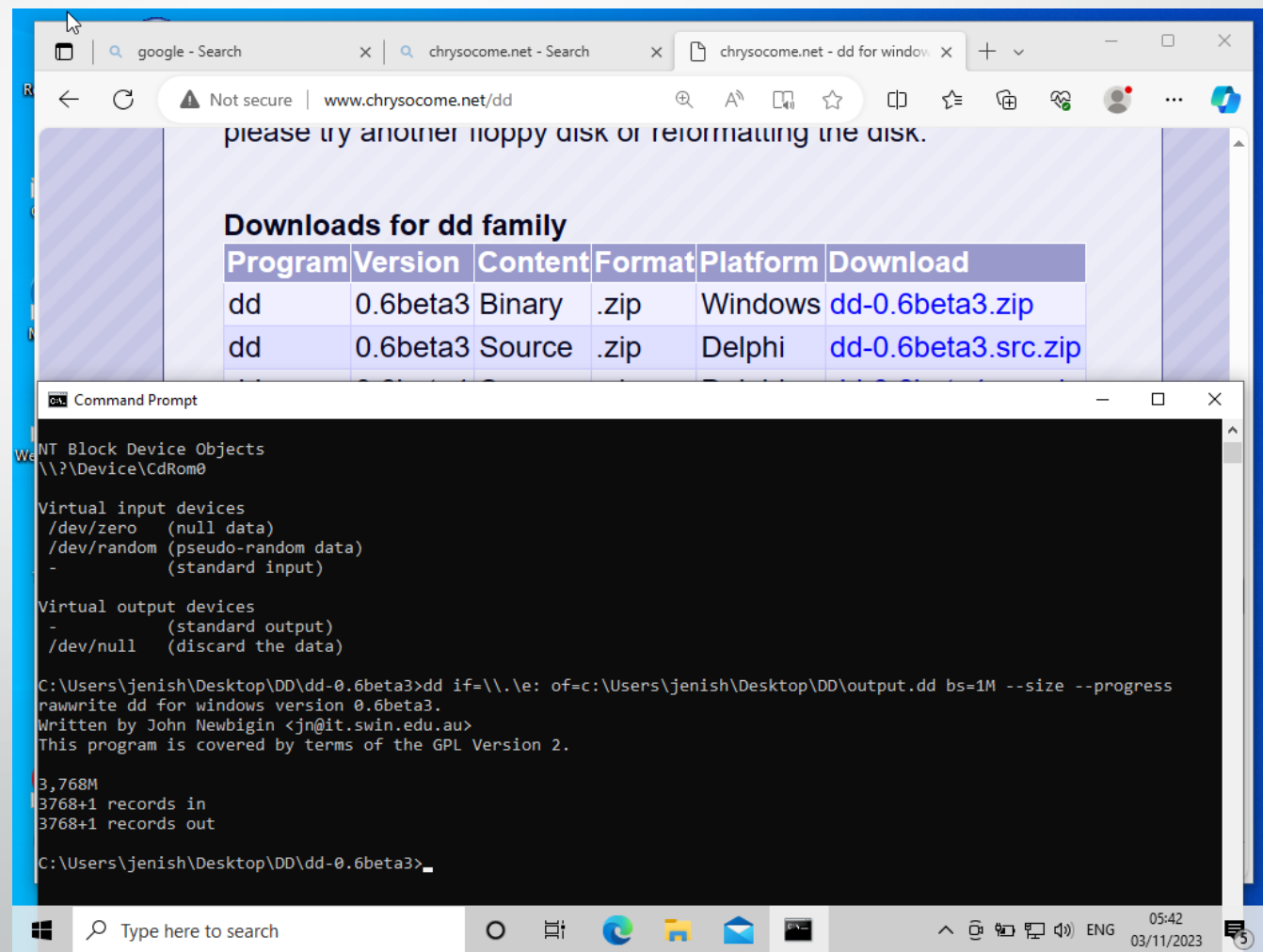
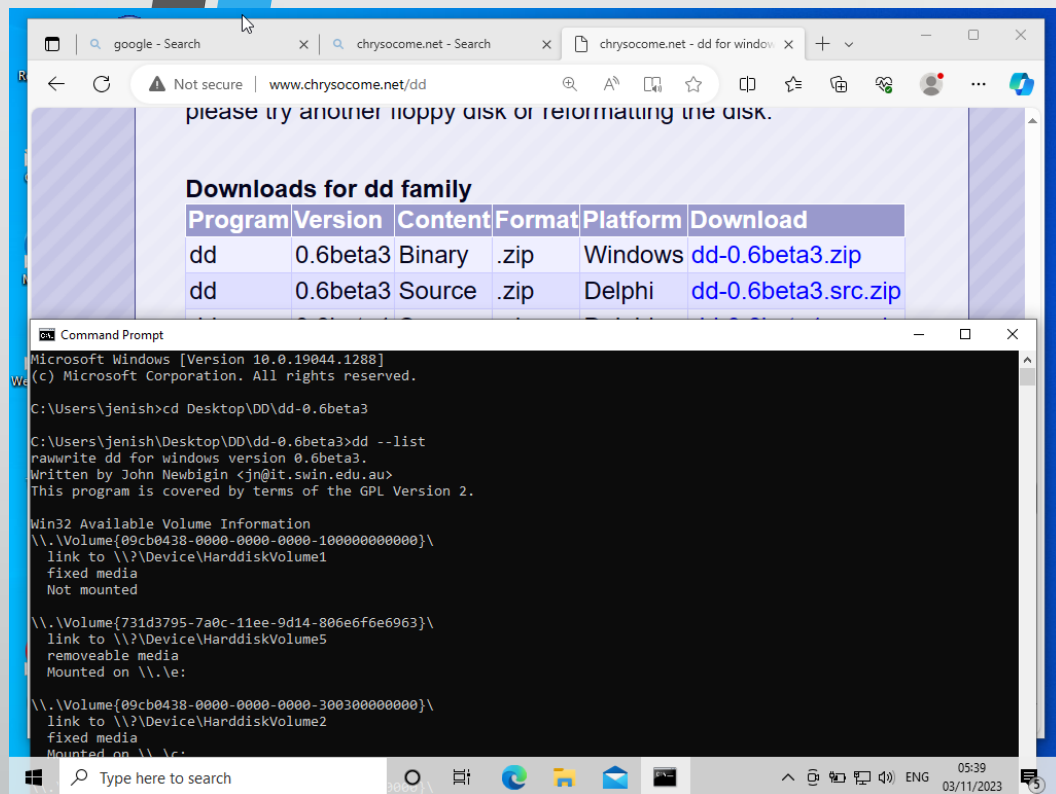


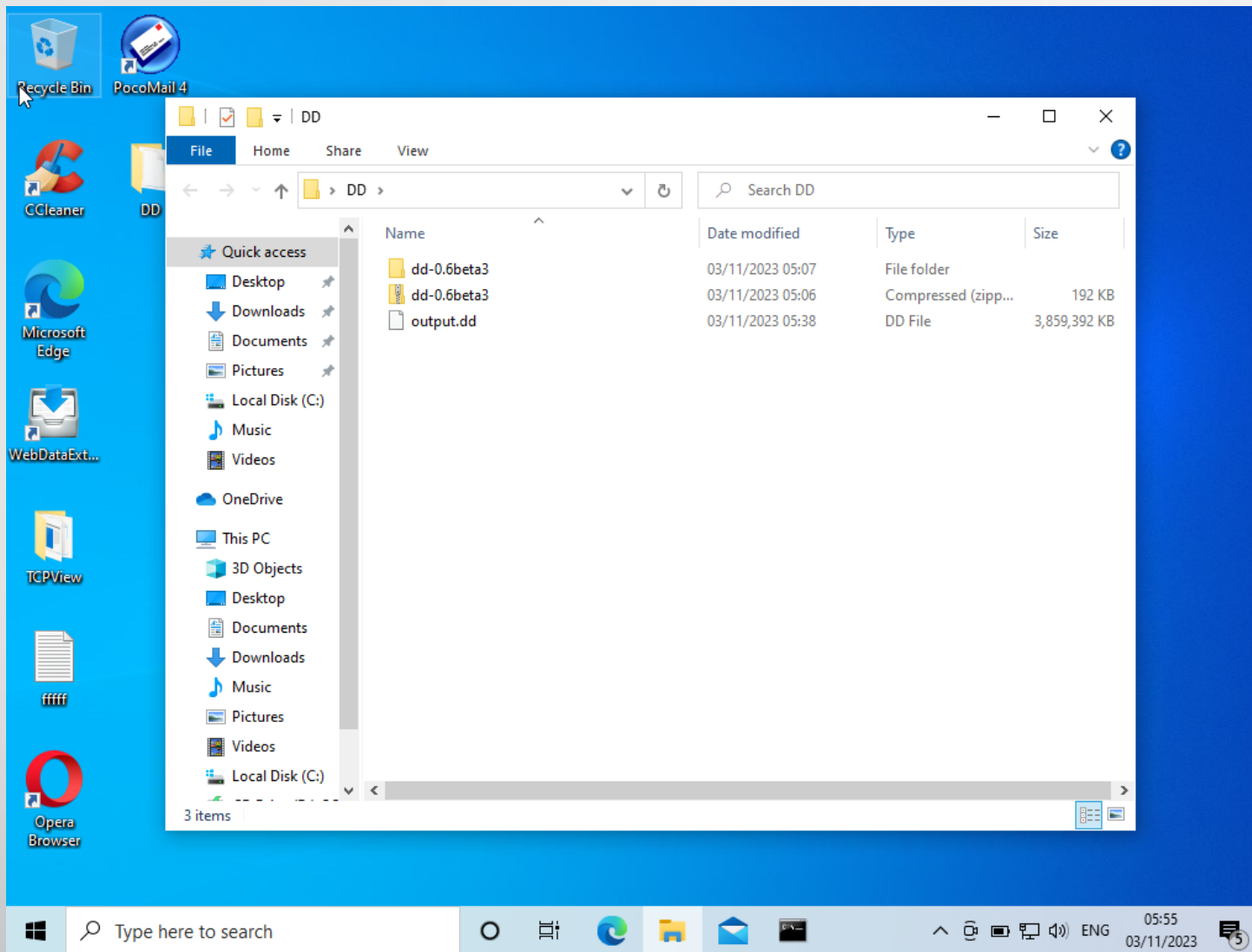


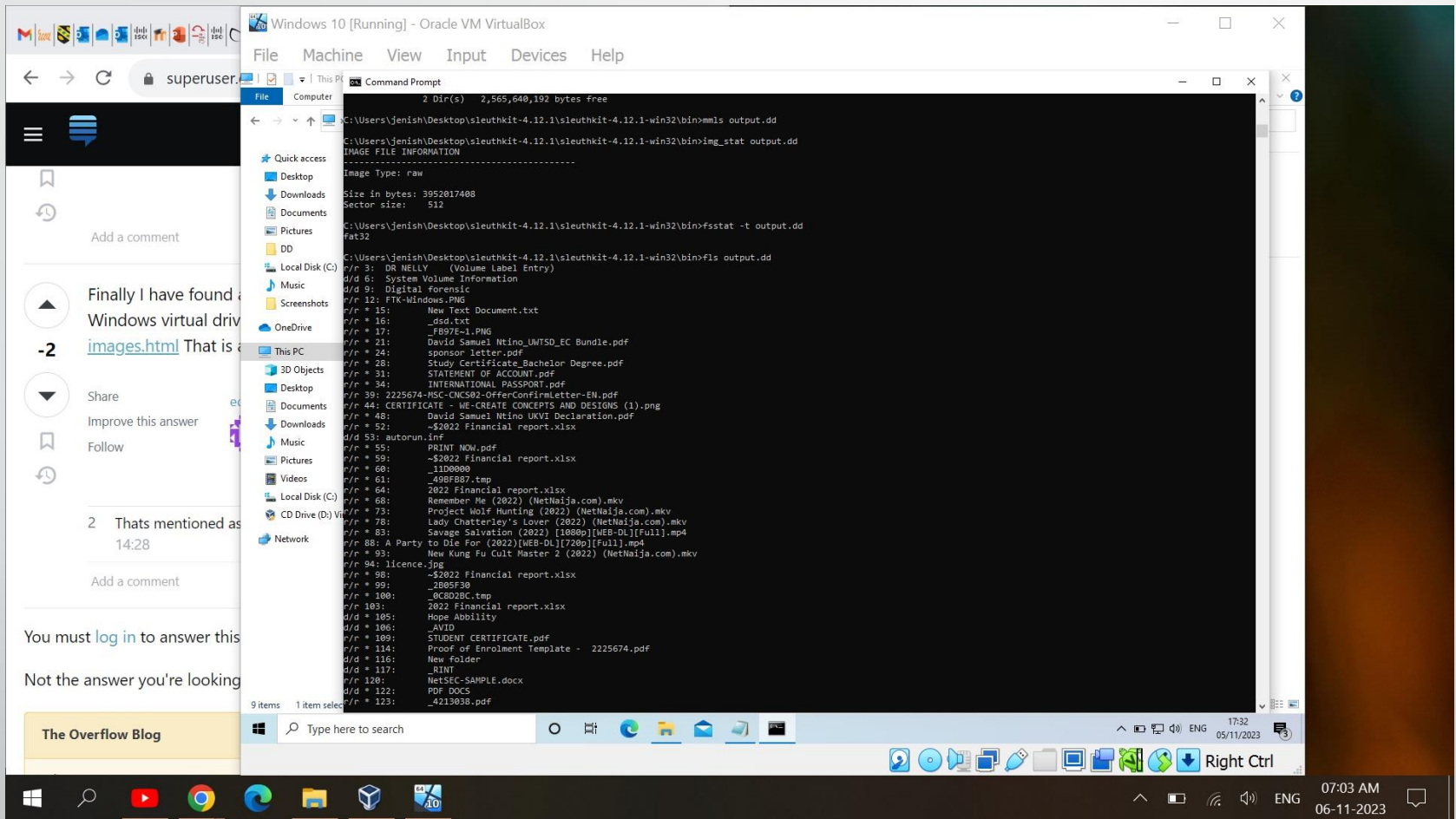
## Write Protection Remove

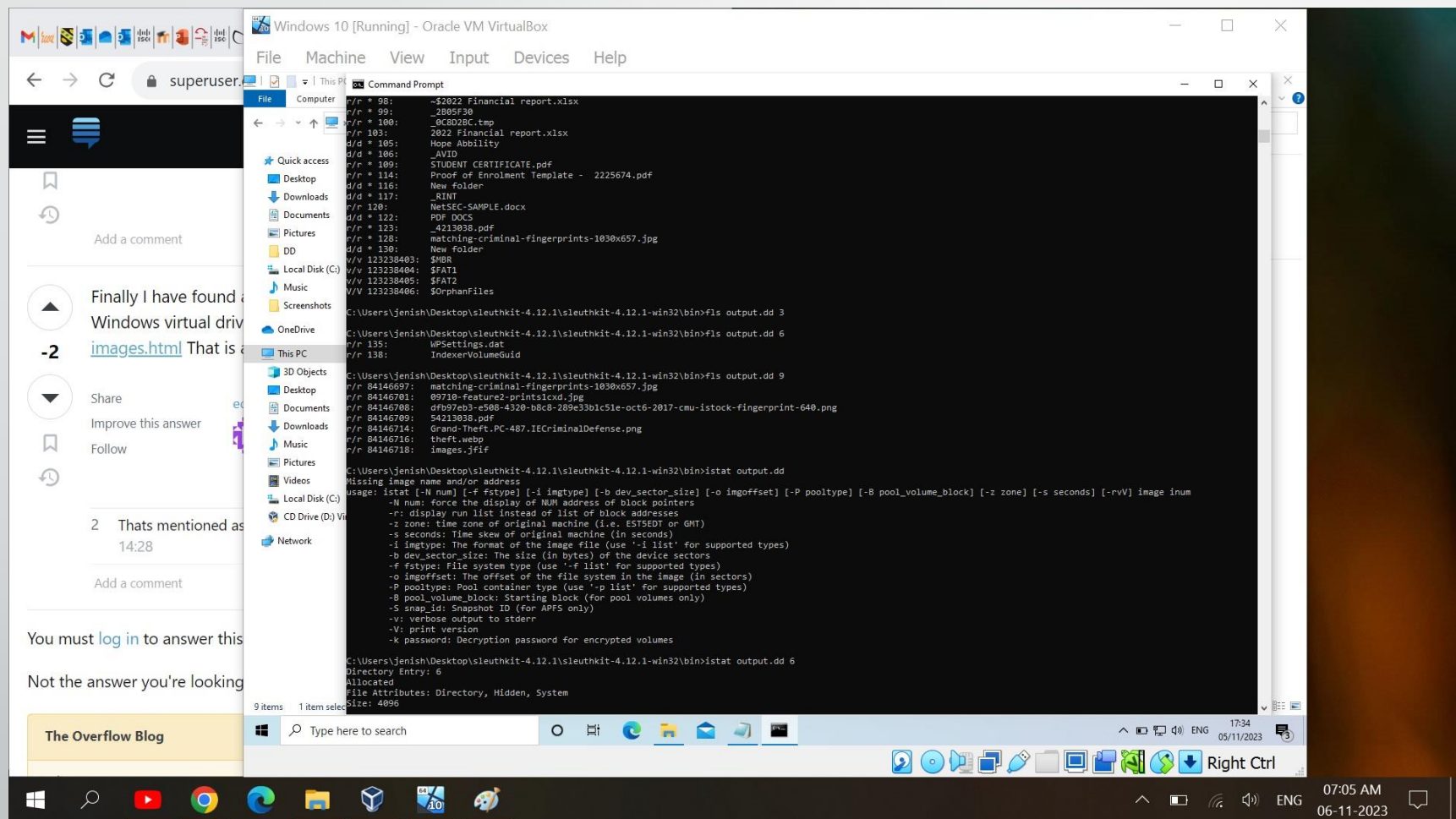


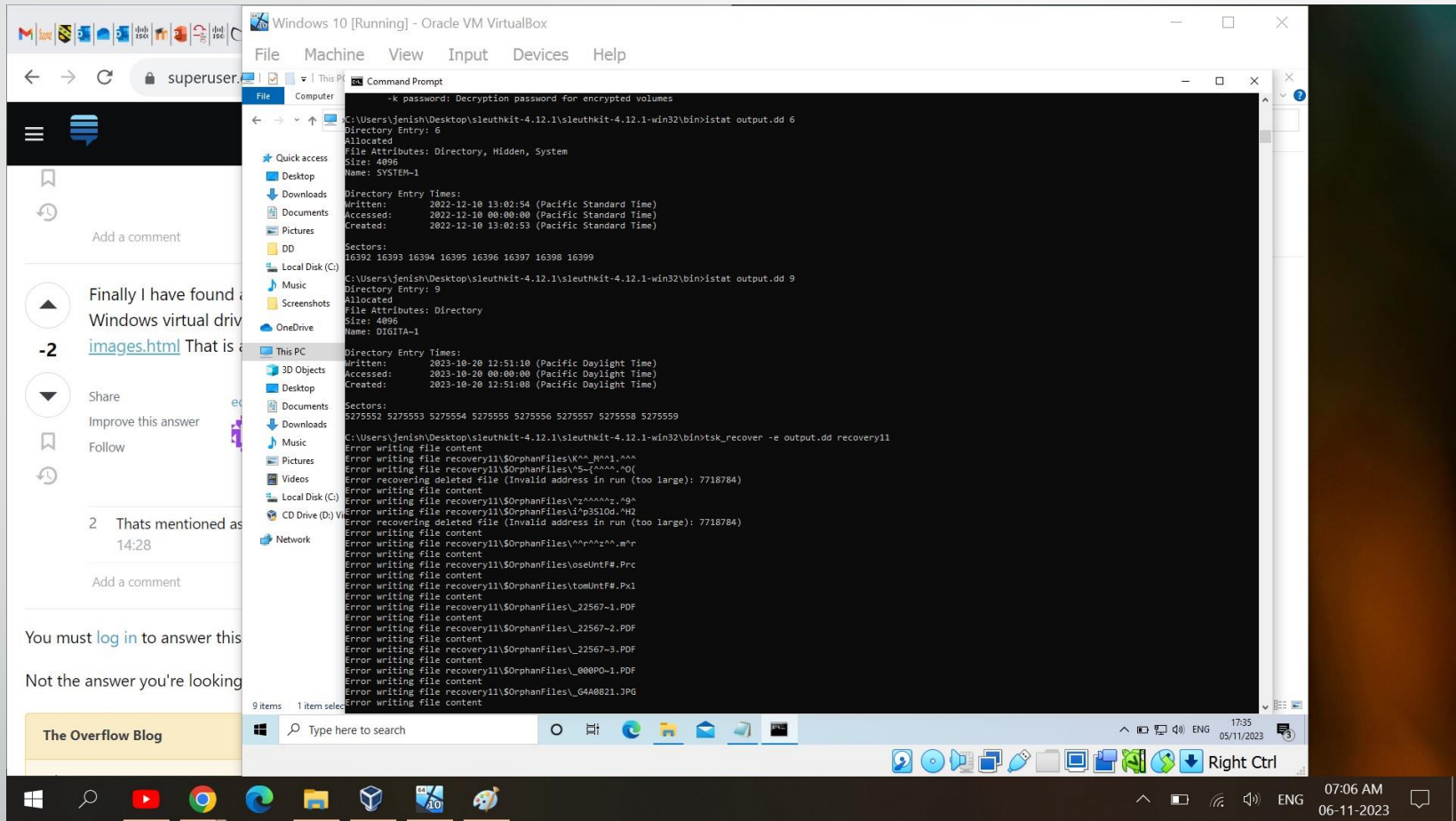
# Image Acquisition

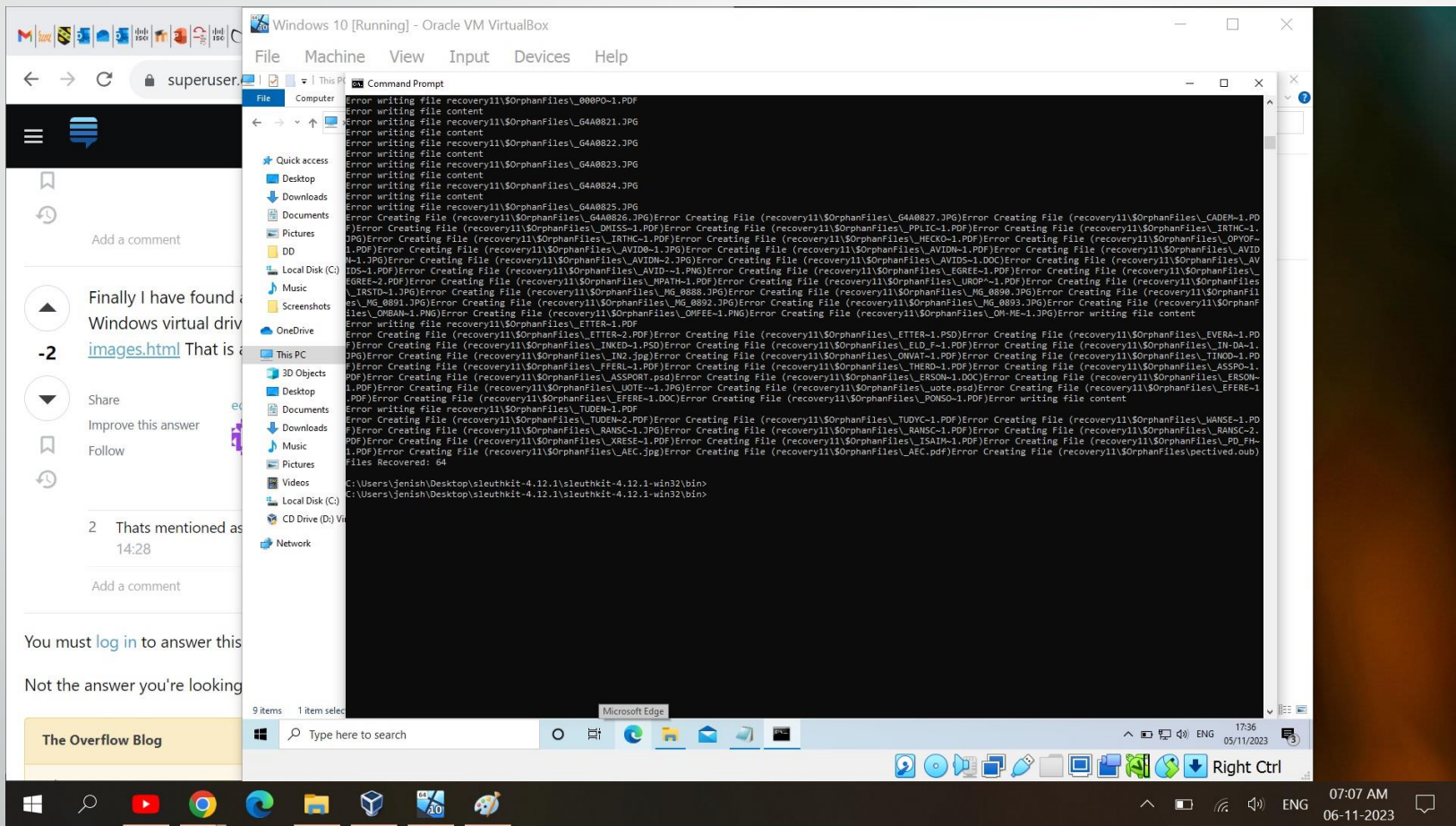












### CONSENT TO SEARCH ELECTRONIC MEDIA

I, \_\_\_\_\_, hereby authorize \_\_\_\_\_, who has identified himself / herself as a law enforcement officer, and any other person(s), including but not limited to a computer forensic examiner, he / she may designate to assist him / her, to remove, take possession of and / or conduct a complete search of the following: computer systems, electronic data storage devices, computer data storage diskettes, CD-ROMs, or any other electronic equipment capable of storing, retrieving, processing and / or accessing data.

The aforementioned equipment will be subject to data duplication / imaging and a forensic analysis for any data pertinent to the incident / criminal investigation.

I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind and with full knowledge of my constitutional right to refuse to give my consent for the removal and / or search of the aforementioned equipment / data, which I hereby waive. I am also aware that if I wish to exercise this right of refusal at any time during the seizure and or search of the equipment / data, it will be respected.

This consent to search is given by me this \_\_\_\_\_ day of, \_\_\_\_\_

20\_\_\_\_\_, at \_\_\_\_\_ am / pm.

Location items taken from: \_\_\_\_\_

Consenter Signature: \_\_\_\_\_ Signature

Witness Signature: \_\_\_\_\_ Signature

Witness Signature: \_\_\_\_\_ Signature

Property Record Number: \_\_\_\_\_

Anywhere Police Department  
**EVIDENCE CHAIN OF CUSTODY TRACKING FORM**

Case Number: \_\_\_\_\_ Offense: \_\_\_\_\_  
Submitting Officer: (Name/ID#) \_\_\_\_\_  
Victim: \_\_\_\_\_  
Suspect: \_\_\_\_\_  
Date/Time Seized: \_\_\_\_\_ Location of Seizure: \_\_\_\_\_

| Description of Evidence |          |                                                                    |
|-------------------------|----------|--------------------------------------------------------------------|
| Item #                  | Quantity | Description of Item (Model, Serial #, Condition, Marks, Scratches) |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |
|                         |          |                                                                    |

| Chain of Custody |           |                               |                               |                   |
|------------------|-----------|-------------------------------|-------------------------------|-------------------|
| Item #           | Date/Time | Released by (Signature & ID#) | Received by (Signature & ID#) | Comments/Location |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |

APD\_Form\_#PE003\_v.1 (12/2012)

Page 1 of 2 pages (See front)

**EVIDENCE CHAIN-OF-CUSTODY TRACKING FORM**  
(Continued)

| Chain of Custody |           |                               |                               |                   |
|------------------|-----------|-------------------------------|-------------------------------|-------------------|
| Item #           | Date/Time | Released by (Signature & ID#) | Received by (Signature & ID#) | Comments/Location |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |
|                  |           |                               |                               |                   |

| Final Disposal Authority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authorization for Disposal</b><br>Item(s) #: _____ on this document pertaining to (suspect): _____<br>is/are no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)<br><input type="checkbox"/> Return to Owner <input type="checkbox"/> Auction/Destroy/Discard<br>Name & ID# of Authorizing Officer: _____ Signature: _____ Date: _____                                                                                                                                                                                                                             |
| <b>Witness to Destruction of Evidence</b><br>Item(s) #: _____ on this document were destroyed by Evidence Custodian<br>_____ ID# _____<br>In my presence on (date) _____<br>Name & ID# of Witness to destruction: _____ Signature: _____ Date: _____                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Release to Lawful Owner</b><br>Item(s) #: _____ on this document was/were released by Evidence Custodian<br>_____ ID# _____ to _____<br>Name: _____<br>Address: _____ City: _____ State: _____ Zip Code: _____<br>Telephone Number: (____) _____<br>Under penalty of law, I certify that I am the lawful owner of the above item(s).<br>Signature: _____ Date: _____<br>Copy of Government-issued photo identification is attached. <input type="checkbox"/> Yes <input type="checkbox"/> No<br><b>This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.</b> |

APD\_Form\_#PE003\_v.1 (12/2012)

Page 2 of 2 pages (See front)

## EVIDENCE CHECKLIST

ECT Claim No.: \_\_\_\_\_

Name of Party/Representative: \_\_\_\_\_

| <u>S/N</u>                  | <u>Name of item</u>                                                                                                                                                                                                                                                              | <u>Yes(Y)/<br/>Not<br/>submitting<br/>(NS)</u> | <u>Date<br/>uploaded/<br/>submitted</u> |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|-----------------------------------------|
| <i>Documentary evidence</i> |                                                                                                                                                                                                                                                                                  |                                                |                                         |
| 1.                          | All documentary evidence that I/we wish to rely on has been uploaded to CJTS.<br><i>Note: Examples of documentary evidence are employment contract, letters, emails, electronic messages (SMS, <del>Whatsapp</del> messages, etc.), video/audio transcripts and photographs.</i> |                                                |                                         |
| 2.                          | I/we have prepared the originals of the uploaded documents to be exhibited at the hearing, if necessary.                                                                                                                                                                         |                                                |                                         |
| <i>Other evidence</i>       |                                                                                                                                                                                                                                                                                  |                                                |                                         |
| 3.                          | I/we have submitted copies of electronic evidence (e.g. video, audio recordings) that will be relied on to the Registry and the opposing party.                                                                                                                                  |                                                |                                         |
| 4.                          | I/we have prepared all physical evidence that will be relied on (e.g. samples) to be exhibited at the hearing, if necessary.                                                                                                                                                     |                                                |                                         |
| <i>Witness evidence</i>     |                                                                                                                                                                                                                                                                                  |                                                |                                         |
| 5.                          | I want to rely on the evidence of the following witnesses at the hearing.<br><i>Note: List <u>all</u> witnesses, including yourself, if you are also giving evidence. <u>Continue on</u> additional sheets if necessary.</i>                                                     |                                                |                                         |
|                             | a.                                                                                                                                                                                                                                                                               |                                                |                                         |
|                             | b.                                                                                                                                                                                                                                                                               |                                                |                                         |
|                             | c.                                                                                                                                                                                                                                                                               |                                                |                                         |

### Explanatory notes on witnesses and witness statements

#### Declaration

I/we have read and understood the above and confirm that, aside from what is listed above, I/we have **no** other evidence I/we want the Tribunal Magistrate to consider.

I/we understand that, if we have further evidence other than those listed above, I/we may not be allowed to tender the evidence if there is no satisfactory reason for not including the evidence in this list, and in that event, they will not be considered by the Tribunal Magistrate.

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Date: \_\_\_\_\_



**THANK YOU**



***Any Questions ?***