FORENSICS V2 LAB SERIES

Lab 21: Chain of Custody

Document Version: 2021-01-14

Contents

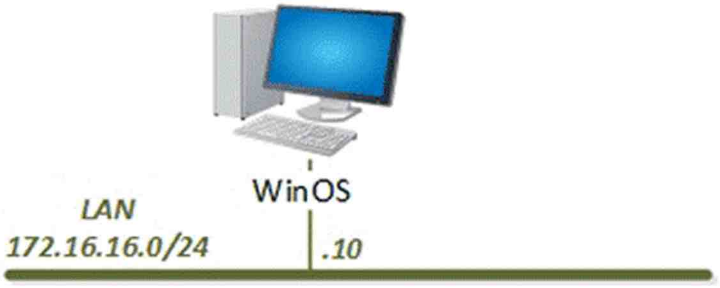
Introduction

Chain of Custody is one of Digital Forensics' most important steps. Without the proper Chain of Custody, much of the evidence brought before the courts for cases would not have been successfully admitted. This lab aims to teach the student how to properly document digital devices and ensure the proper chain of custody is followed at all times.

Objectives

- Learn what are important details to be recorded from a device
- create a log for the evidence identified

Lab Topology



Lab Settings

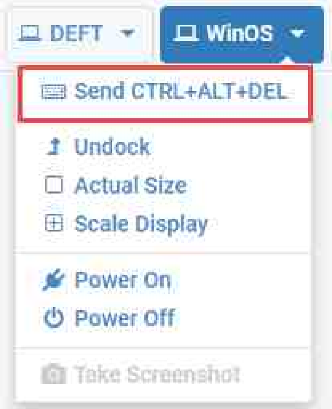
The information in the table below will be needed to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address / Subnet Mask**	**Account** (if needed)	**Password** (if needed)
Caine	172.16.16.30	caine	Train1ng$
CSI-Linux	172.16.16.40	csi	csi
DEFT	172.16.16.20	deft	Train1ng$
WinOS	172.16.16.10	Administrator	Train1ng$

1 Describing the Device for Evidence Submission

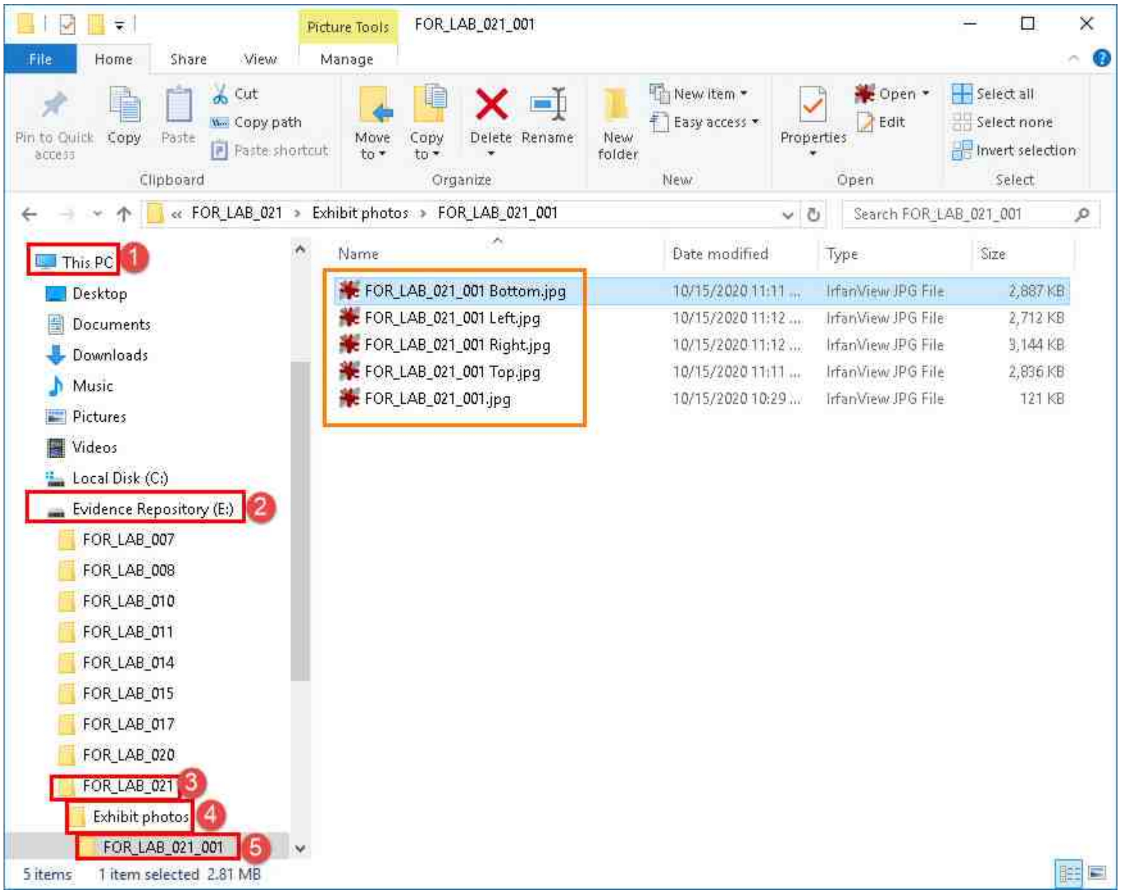
One of the most important steps of the evidence intake process is the proper documentation of items that are submitted or seized. The individual who takes control of the devices must know how to identify the serial and model numbers as well as provide an accurate description of the item. In this exercise, we will review the important details that need to be identified and recorded for the intake process.

1. To begin, launch the WinOS virtual machine to access the graphical login screen.
   a. Select Send CTRL+ALT+DEL from the dropdown menu to be prompted with the login screen.



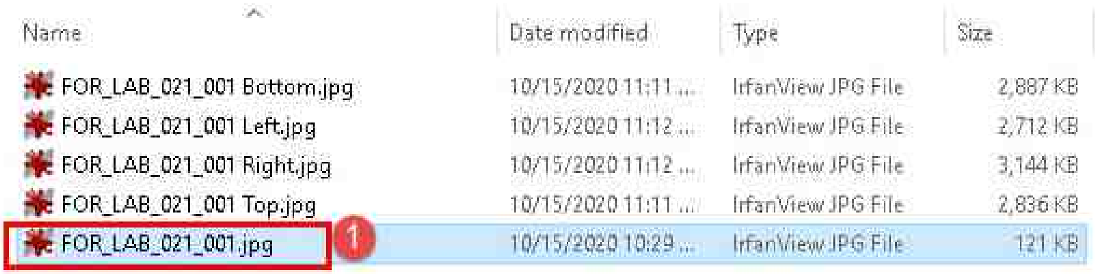
   b. Log in as `Administrator` using the password: `Train1ng$`

2. Let us look at some exhibit photos we took earlier. These devices were seized and handed over to you for intake. Let us look at how we need to describe and detail them so that they can be properly identified later. Begin by opening Windows File Explorer and navigating to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Exhibit photos > FOR_LAB_021_001 as seen in items 1, 2, 3, 4, and 5 below.



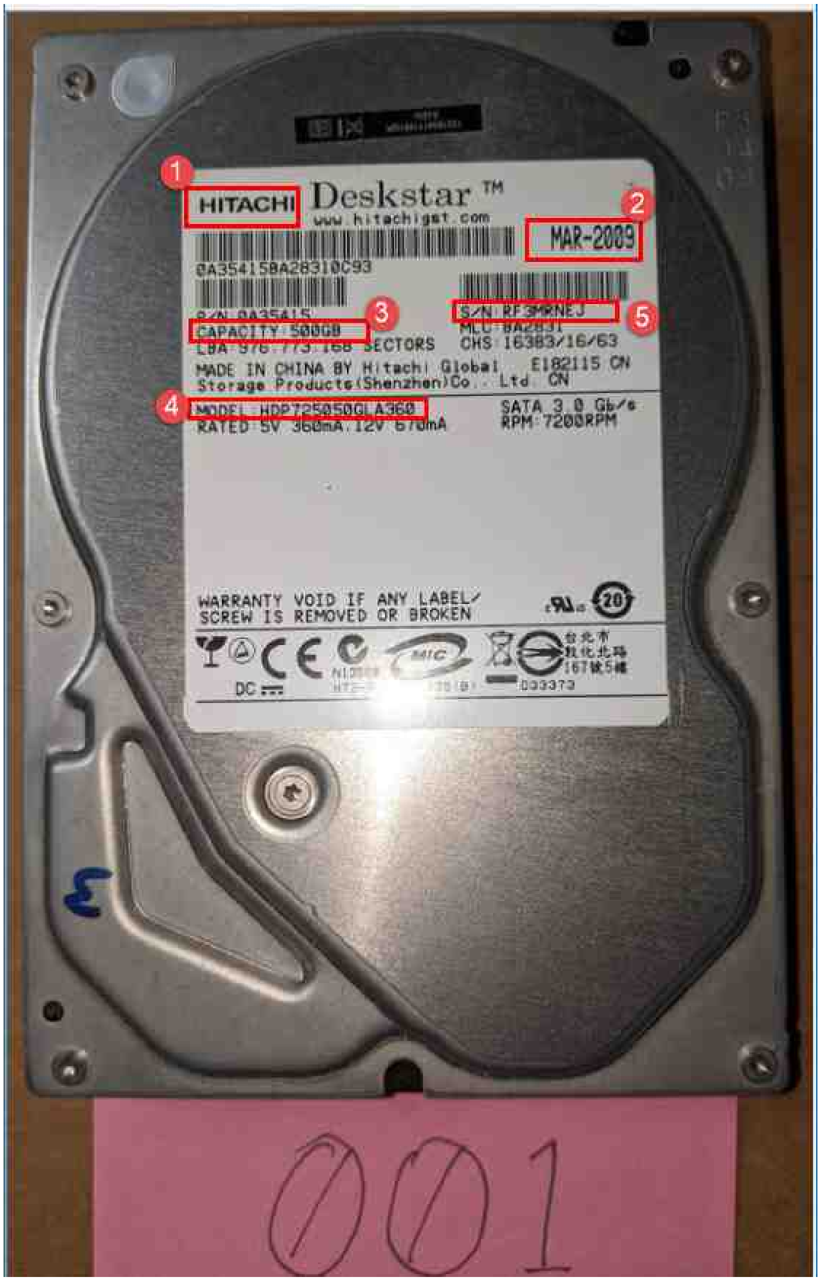
Name	Date modified	Type	Size
FOR_LAB_021_001 Bottom.jpg	10/15/2020 11:11 ...	IrfanView JPG File	2,887 KB
FOR_LAB_021_001 Left.jpg	10/15/2020 11:12 ...	IrfanView JPG File	2,712 KB
FOR_LAB_021_001 Right.jpg	10/15/2020 11:12 ...	IrfanView JPG File	3,144 KB
FOR_LAB_021_001 Top.jpg	10/15/2020 11:11 ...	IrfanView JPG File	2,836 KB
FOR_LAB_021_001.jpg	10/15/2020 10:29 ...	IrfanView JPG File	121 KB

3. In this folder, you will see several photos of a hard drive that was seized and needs to be recorded. Let us look at the one labeled FOR_LAB_021_001.jpg by double-clicking the file to open it, as seen in item 1 below.

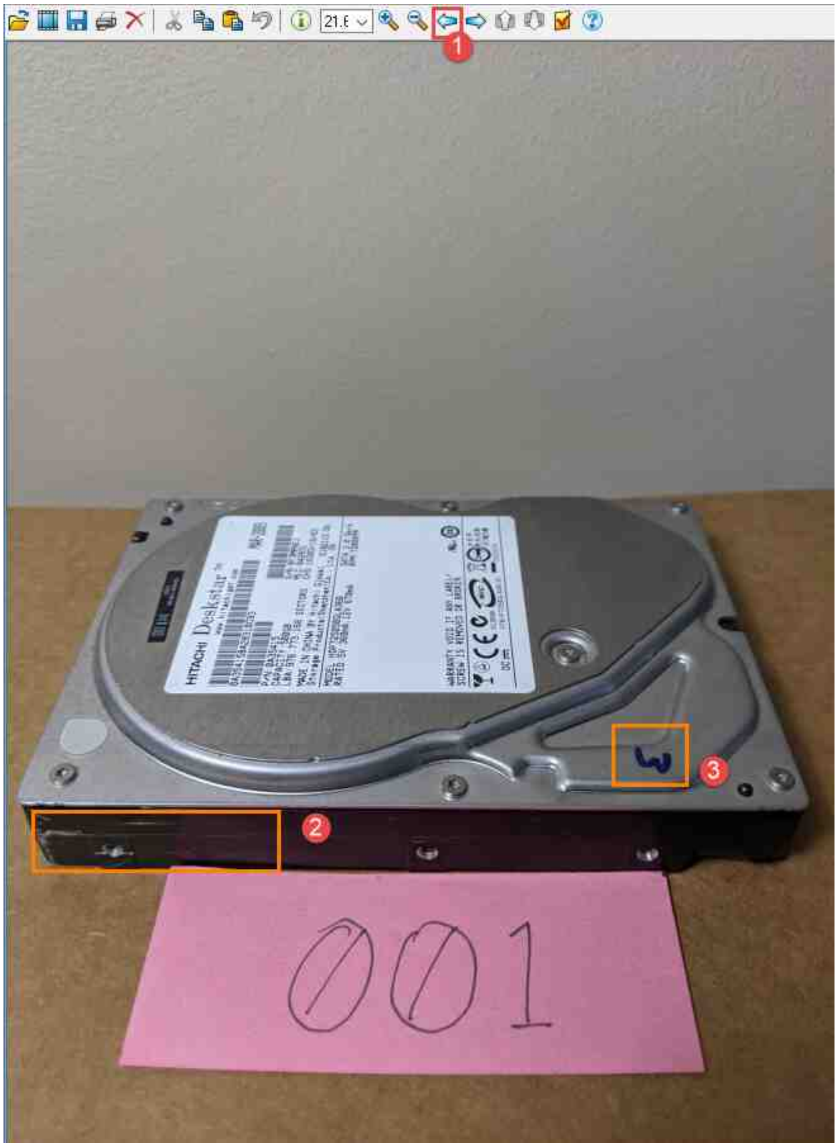


Name	Date modified	Type	Size
FOR_LAB_021_001 Bottom.jpg	10/15/2020 11:11 ...	IrfanView JPG File	2,887 KB
FOR_LAB_021_001 Left.jpg	10/15/2020 11:12 ...	IrfanView JPG File	2,712 KB
FOR_LAB_021_001 Right.jpg	10/15/2020 11:12 ...	IrfanView JPG File	3,144 KB
FOR_LAB_021_001 Top.jpg	10/15/2020 11:11 ...	IrfanView JPG File	2,836 KB
FOR_LAB_021_001.jpg	10/15/2020 10:29 ...	IrfanView JPG File	121 KB

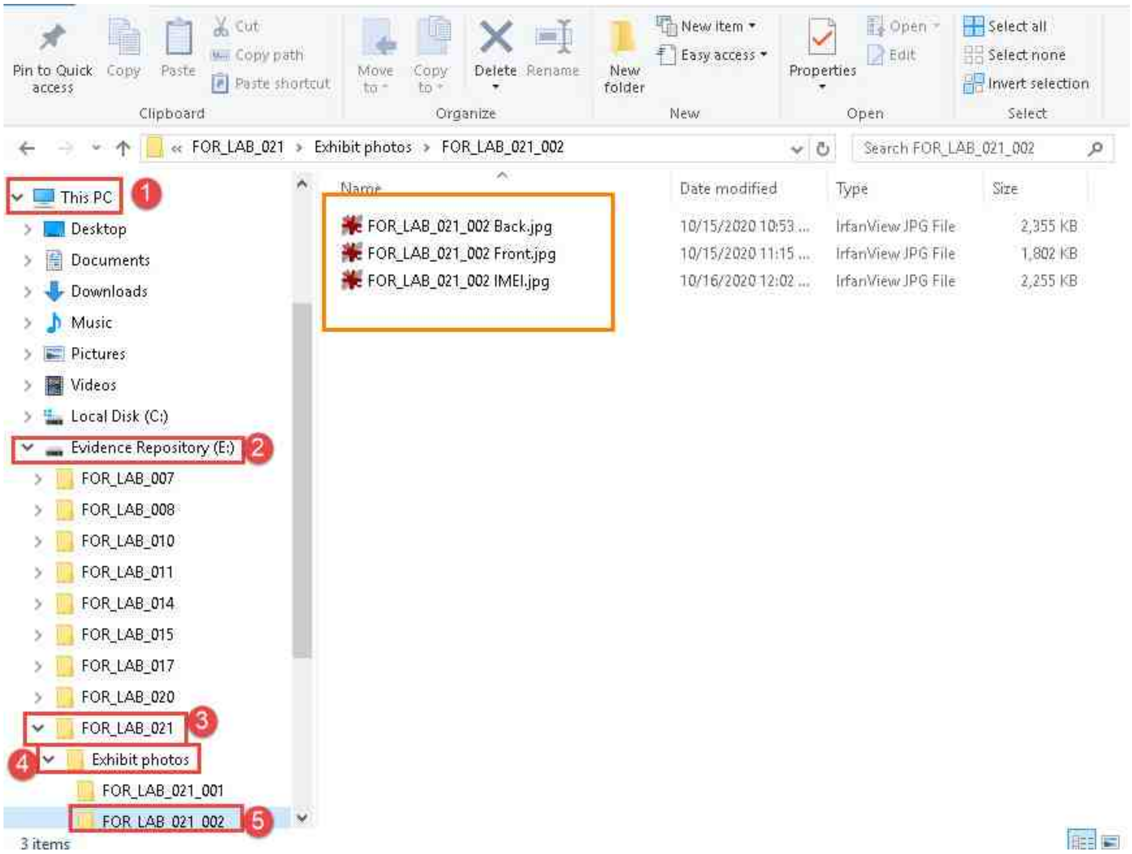
4. This is a photo of a 3.5-inch hard drive. The details of the hard drive can normally be found on the label at the front. The data highlighted as item 1 below is the Make which is Hitachi. This is the name of the company that manufactured the hard drive. The data highlighted in item 2 is the manufacture date (Mar-2009), which tells you when the hard drive was released for sale. In item 3 is the capacity of the hard drive. As you can see, this hard drive has a capacity of 500GB. The model number (HDP725050GLA360) is highlighted as item 4 and is best used for identifying the type of hard drive. The serial number (S/N) (RF3MRNEJ) is highlighted as item 5 and it uniquely identifies the drive; no two drives should have the same serial number. Because the serial number is unique, it is the best value to use for identifying the disk. The other values are also important but if a serial number exists on the device, always use it. Now that we can identify the various numbers, make note of them as we will be using them to fill our intake form.



5. Another important step in the intake process is the physical description and condition of the devices. This means the examiner should be able to state the color, form factor and any notable physical marks, especially damage done BEFORE intake. Let us look at the other photos of this hard drive to see its description. Use the left arrow seen in item 1 below to look at the photos of the hard drive from different angles. Some things you can note are the scratches on the top-left corner seen in item 2 and the number 3 written with a marker as seen in item 3. This drive does not appear to have any dents or damage, but others might, so be sure to inspect the item properly. The color description that you give can be subjective at times but helps to better identify how the device looked at the time of seizure.

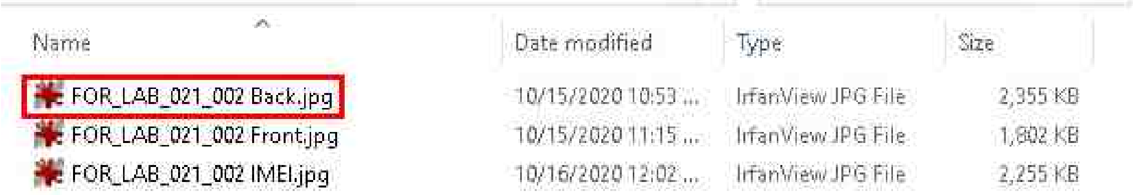


6. Before we start making note, let us look at the details on a cell phone. Go back to Windows File Explorer and navigate to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Exhibit photos > FOR_LAB_021_002 as seen in items 1, 2, 3, 4, and 5 below.



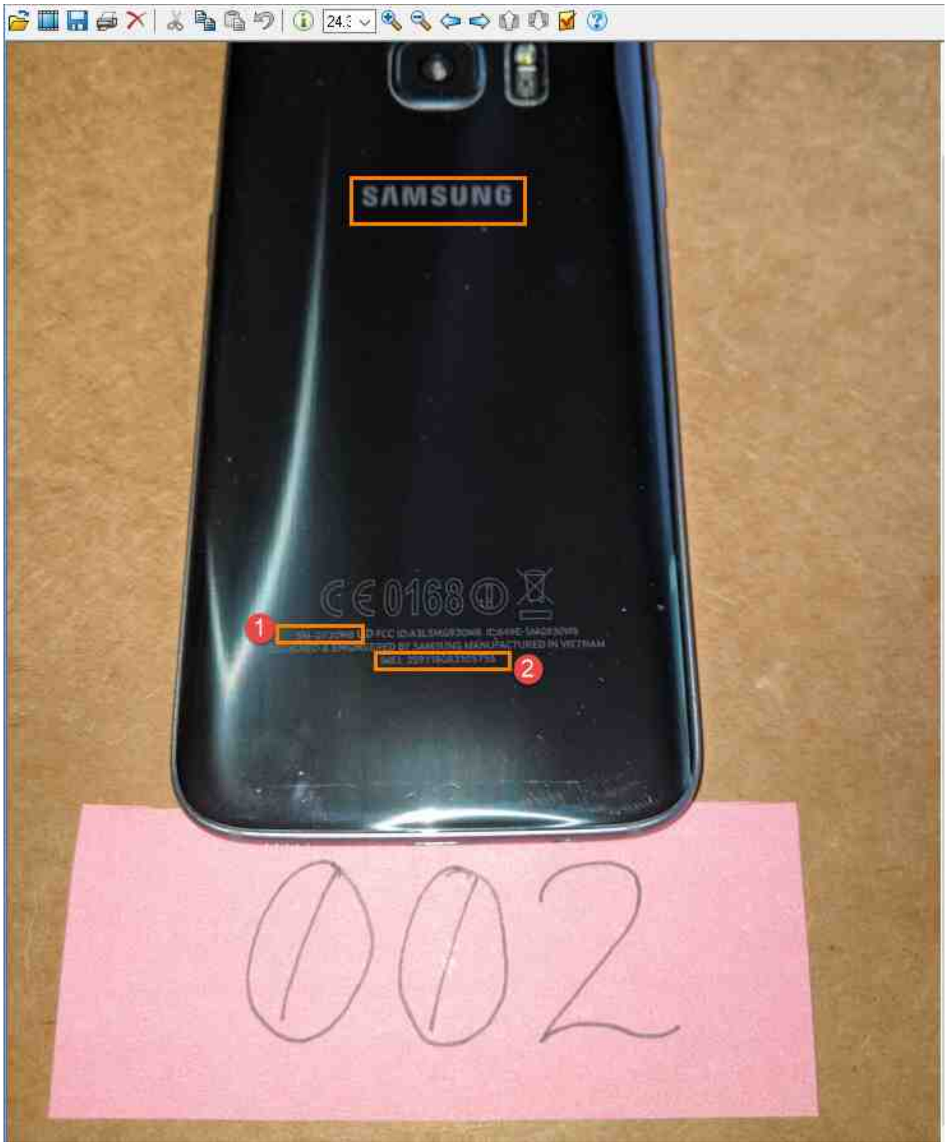
Name	Date modified	Type	Size
FOR_LAB_021_002 Back.jpg	10/15/2020 10:53 ...	IrfanView JPG File	2,355 KB
FOR_LAB_021_002 Front.jpg	10/15/2020 11:15 ...	IrfanView JPG File	1,802 KB
FOR_LAB_021_002 IMEI.jpg	10/16/2020 12:02 ...	IrfanView JPG File	2,255 KB

7. In this folder, you will see two photos of a cell phone that was also seized and needs to be recorded. Let us look at the one labeled FOR_LAB_021_002 Back.jpg by double-clicking the file to open it, as seen in item 1 below.

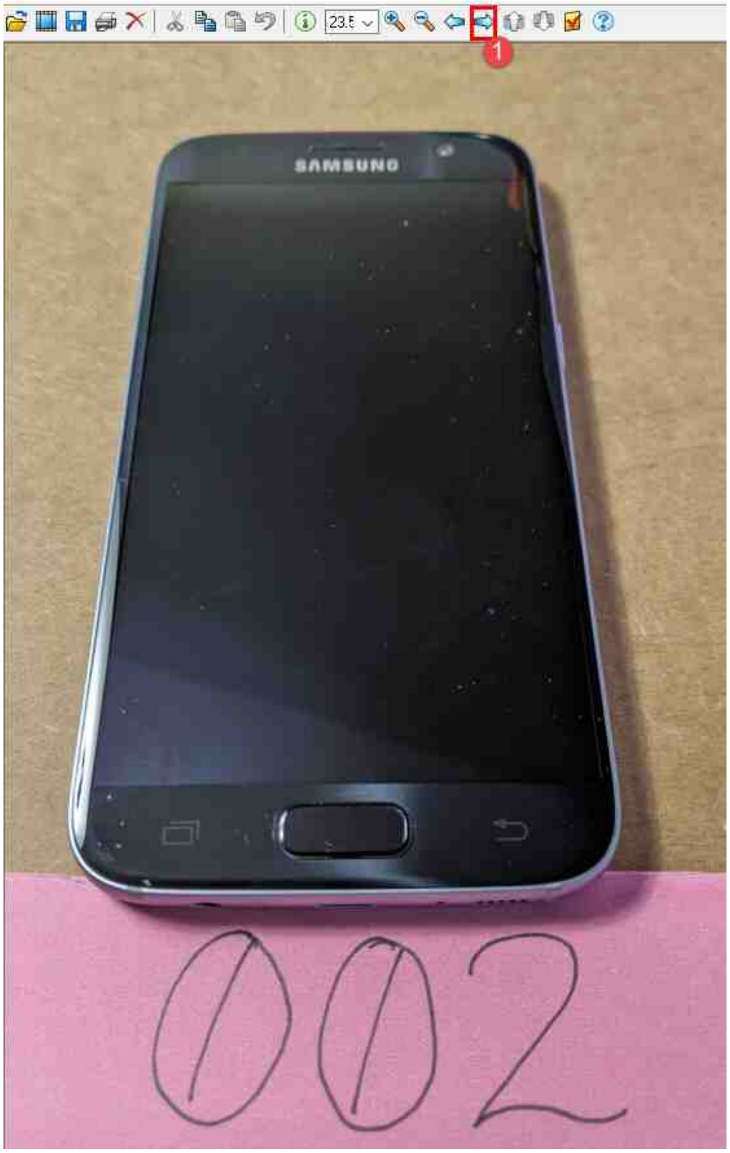


Name	Date modified	Type	Size
FOR_LAB_021_002 Back.jpg	10/15/2020 10:53 ...	IrfanView JPG File	2,355 KB
FOR_LAB_021_002 Front.jpg	10/15/2020 11:15 ...	IrfanView JPG File	1,802 KB
FOR_LAB_021_002 IMEI.jpg	10/16/2020 12:02 ...	IrfanView JPG File	2,255 KB

8. Some cell phones will have details of the devices printed within the battery-well and on the SIM Card tray. Newer smartphones are moving away from that and have since printed the device identifiers on the back, however. In the case where you do not see any details on the back or SIM tray, you may have to get the details from within the phone or using mobile forensic software to pull the information. The cellphone in the picture is a Samsung Galaxy S7, which does have the details on the back of the phone. Look at the data highlighted in item 1 to find the model number, which is SM-G930W8. Some cellphones will list the serial number on the back as well, but this one doesn't; instead, we have the value known as the International Mobile Equipment Identity (IMEI), a value that uniquely identifies a mobile device. It is different from a serial number because the serial number is not transmitted to the service provider when calls are made or SMS/MMS messages are sent, but the IMEI is. The IMEI (359118083705756) for this device can be seen in item 2 below. Like you did before, make note of these values as we will need them for the intake process.



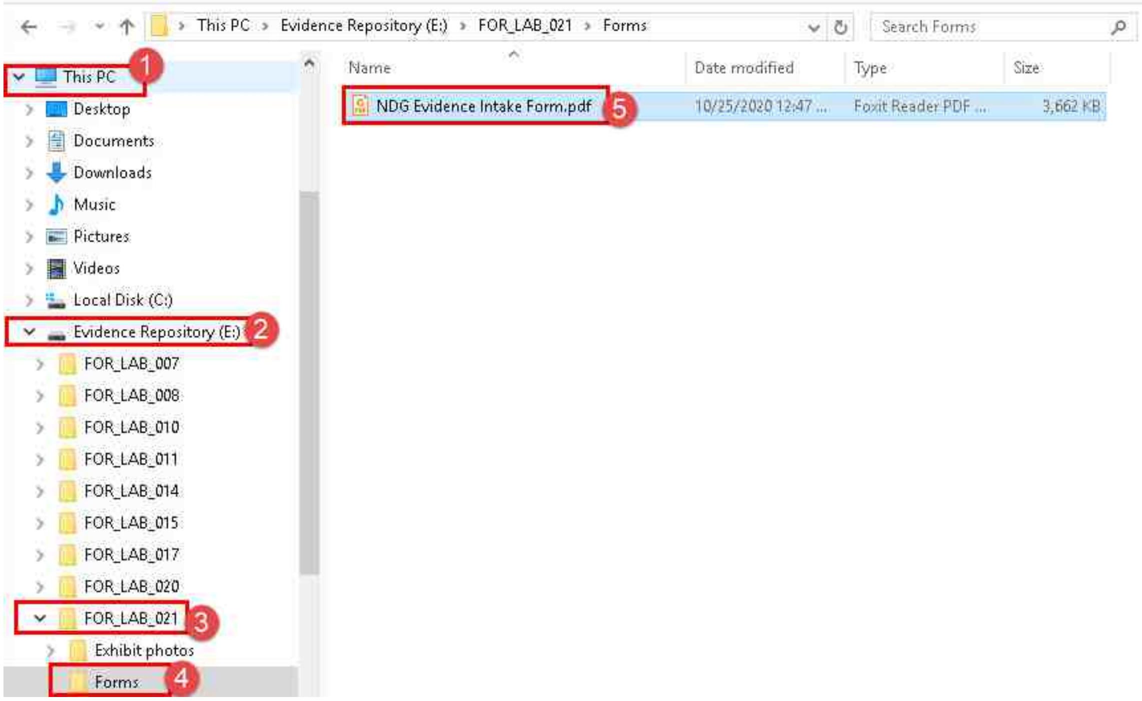
9. In the case where you must find the serial number and IMEI from within the device, simply unlock it and open the phone app. Then type `*#06*` which will bring up the following screen. You can do this on your own device to see how it works. Be sure to note your actions in case you need to explain what you did.
10. Now let us look at the description and condition of this device. Use the left or right arrow, seen in item 1 below, to look at the other photo of the phone from a different angle. As you can see, this device does not appear to have any physical damage or scratches, which should also be noted.



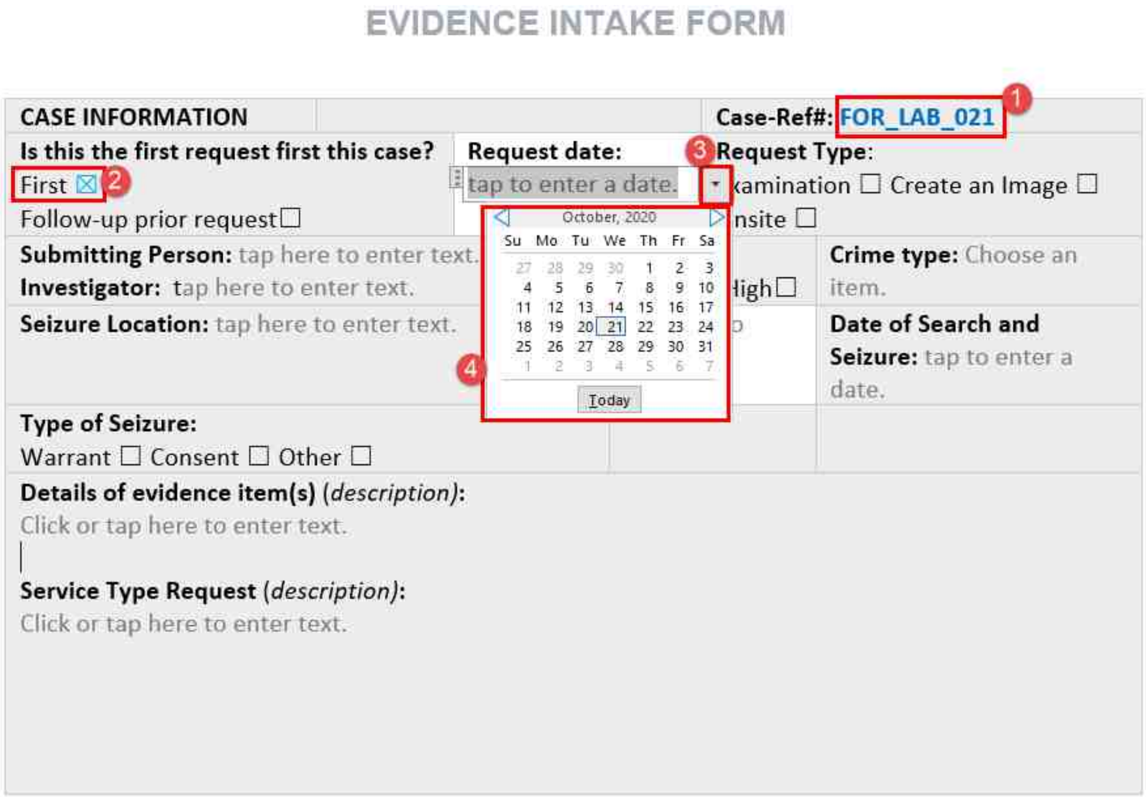
11. Now let us enter this data into the intake and Chain of Custody forms.

2 Filling Out the Intake and CoC Forms

1. Chain of custody refers to the route the evidence took from the time it was seized to the point where it is submitted to the courts. The process begins by creating an intake form that provides details about the device. This form will be signed by the person handing over the devices and the person receiving them. Let us look at what an intake form looks like and how we would fill it out. Begin by opening Windows File Explorer and navigating to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Forms as seen in items 1,2,3, and 4. Double-click the file called NDG Evidence Intake form.pdf as seen in item 5.



2. The intake form will open, allowing you to enter the details of the person who handed over the device(s). Let us fill this form out with the information we gathered from exhibits 001 in the previous exercise. First, enter the lab assigned case reference number `FOR_LAB_021` in the Case-ref# field, as seen in item 1 below. Next, click the checkbox beside First in the field called Is this the first request for this case? as seen in item 2 below. The alternate option (Follow-up prior request) would indicate to the examiner that the evidence item is related to a previous case. Next, let us enter the Request date. To do this, click the area called tap to enter a date, which will reveal an arrow as seen in item 3. Click the arrow to reveal a calendar, as seen in item 4. Use this calendar to select today's date.



EVIDENCE INTAKE FORM

CASE INFORMATION **Case-Ref#:** FOR_LAB_021

Is this the first request first this case?
First ☒
Follow-up prior request☐

Request date: tap to enter a date.

Request Type:
xamination ☐ Create an Image ☐
nsite ☐

Submitting Person: tap here to enter text.
Investigator: tap here to enter text.

ligh☐

Crime type: Choose an item.

Seizure Location: tap here to enter text.

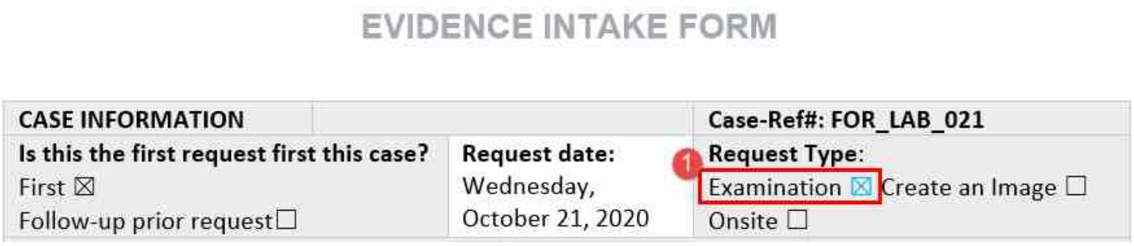
Date of Search and Seizure: tap to enter a date.

Type of Seizure:
Warrant ☐ Consent ☐ Other ☐

Details of evidence item(s) (*description*):
Click or tap here to enter text.

Service Type Request (*description*):
Click or tap here to enter text.

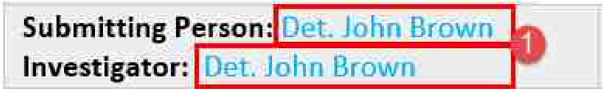
3. Next, we will select the Request Type. We will be submitting this device for forensic examination so let us click the checkbox beside Examination in the Request Type field highlighted as item 1 below. The other options refer to onsite visits and image creation only.



EVIDENCE INTAKE FORM

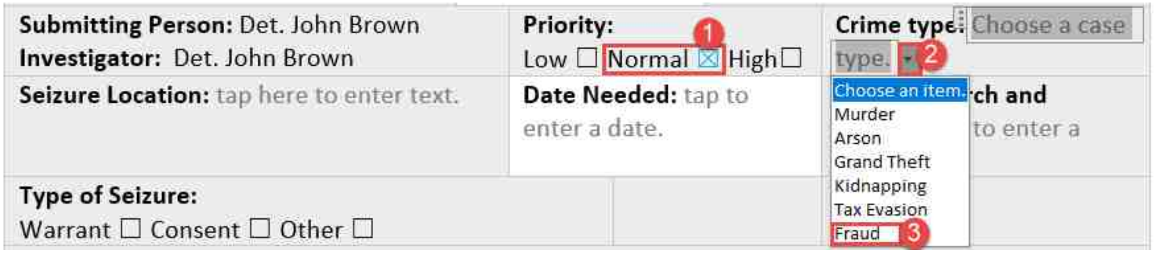
CASE INFORMATION		**Case-Ref#: FOR_LAB_021**
Is this the first request first this case? First ☒ Follow-up prior request☐	**Request date:** Wednesday, October 21, 2020	**Request Type:** Examination ☒ Create an Image ☐ Onsite ☐

4. Next, we will put the name of the submitting person. Type the name `Det. John Brown` for both Submitting Person and Investigator here as seen in item 1 below. In cases where the submitting person is different from the investigator (if applicable), you can define it here.



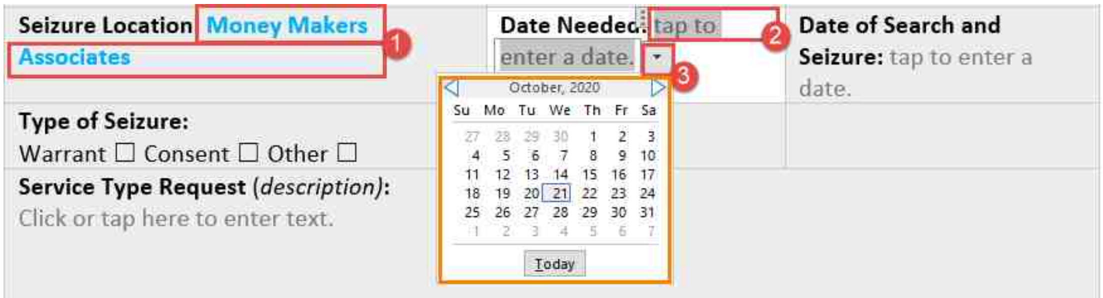
Submitting Person: Det. John Brown
Investigator: Det. John Brown

5. Now we will select the priority of the case. Click the checkbox beside Normal, as seen in item 1 below. After that, we can choose the Crime type, which will tell what type of investigation is being performed. Click the grey area marked Choose a case type in the Case Type field as seen in item 2. This will open a window where you can choose the type of matter. In this exercise, we will select Fraud, as seen items 3 below.



Submitting Person: Det. John Brown **Investigator:** Det. John Brown	**Priority:** Low ☐ Normal ☒ High☐	**Crime type:** Choose a case type.
Seizure Location: tap here to enter text.	**Date Needed:** tap to enter a date.	ch and to enter a
Type of Seizure: Warrant ☐ Consent ☐ Other ☐		

6. We will then fill out the Seizure Location. In this field, type `Money Makers Associates Ltd.` as seen in item 1 below. The next field is the Date Needed and helps the lab prioritize. Enter a date of your choice here by clicking the grey area called tap to enter a date as seen in item 2. A dropdown arrow will appear, click it, and then select a date, as seen in item 3.



Seizure Location Money Makers Associates

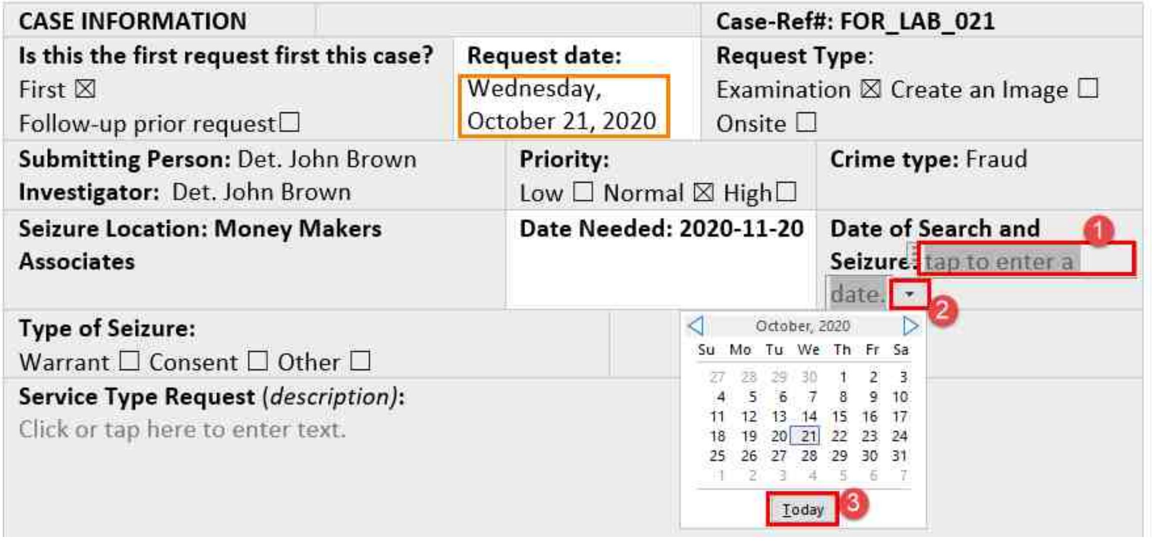
Date Needed: tap to enter a date.

Date of Search and Seizure: tap to enter a date.

Type of Seizure:
Warrant ☐ Consent ☐ Other ☐

Service Type Request (*description*):
Click or tap here to enter text.

7. It is vital for examiners to know when the device was taken into custody from the device's user. The Date of Search and Seizure field can help with that. Let us fill out this field by clicking the grey area called tap to enter a date as seen in item 1. A dropdown arrow will appear, click it, and then select a date, as seen in items 2 and 3 below.



CASE INFORMATION

Case-Ref#: FOR_LAB_021

Is this the first request first this case?
First ☒
Follow-up prior request☐

Request date:
Wednesday, October 21, 2020

Request Type:
Examination ☒ Create an Image ☐
Onsite ☐

Submitting Person: Det. John Brown
Investigator: Det. John Brown

Priority:
Low ☐ Normal ☒ High☐

Crime type: Fraud

Seizure Location: Money Makers Associates

Date Needed: 2020-11-20

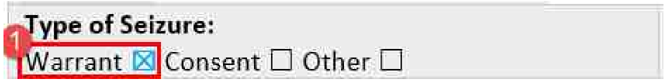
Date of Search and Seizure: tap to enter a date.

Type of Seizure:
Warrant ☐ Consent ☐ Other ☐

Service Type Request (*description*):
Click or tap here to enter text.

It is best practice to have electronic evidence submitted to the forensic laboratory on the same day of the search and seizure. It is not always the case, but this adds to the chain of custody and ensures the exhibit is protected.

8. The next field is the Type of Seizure and tells whether the device was handed over voluntarily, seized through court order, warrant, or other means. Click the checkbox beside Warrant as seen in item 1 below.

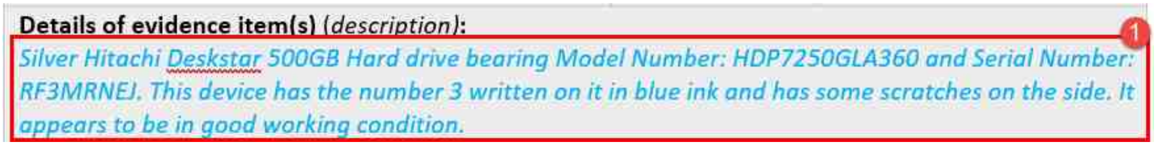


Type of Seizure:
Warrant ☒ Consent ☐ Other ☐

9. Now we get to the part of the form where you need to enter the device of the evidence item(s). This is the Details of evidence item(s) field. Click inside the box to start writing. Write the details of exhibit EID 001 as follows:

```
Silver Hitachi Deskstar 500GB Hard drive bearing Model Number: HDP7250GLA360
and Serial Number: RF3MRNEJ. This device has the number 3 written on it in
blue ink and has some scratches on the side. It appears to be in good
working condition.
```

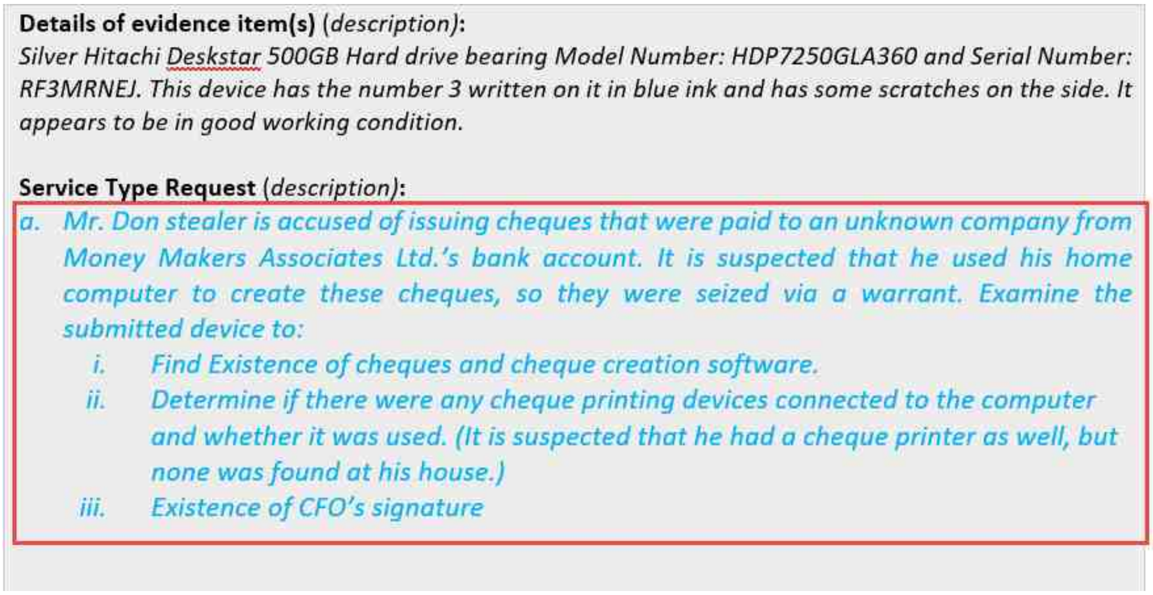
This can also be seen in item 1 below.



Details of evidence item(s) *(description)*:
Silver Hitachi Deskstar 500GB Hard drive bearing Model Number: HDP7250GLA360 and Serial Number: RF3MRNEJ. This device has the number 3 written on it in blue ink and has some scratches on the side. It appears to be in good working condition.

10. Now we will enter the purpose of the examination by entering it into the Service Type Request field. This field does not always contain enough space for filling out the purpose of the examination, and so additional reports and instructions can be attached. This field is still quite useful as the requests can often be summarized here. Let us write a quick summary for this case. Enter the following request in the Service Type Request field:

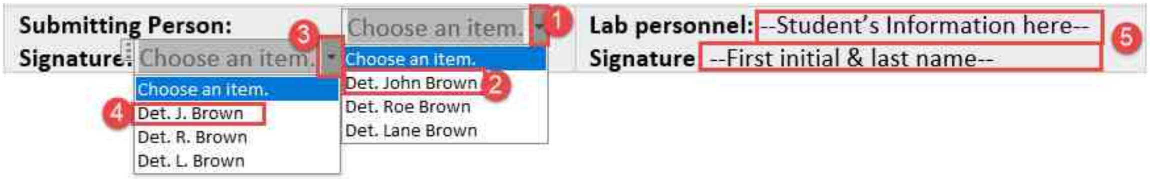
```
a.  Mr. Don stealer is accused of issuing cheques that were paid to an unknown
    company from Money Makers Associates Ltd.'s bank account. It is suspected
    that he used his home computer to create these cheques, so they were seized
    via a warrant. Examine the submitted device to:

     i.    Find Existence of cheques and cheque creation software.
    ii.    Determine if there were any cheque printing devices connected to the
           computer and whether it was used. (It is suspected that he had a
           cheque printer as well, but none was found at his house.)
   iii.    Existence of CFO's signature
```



Details of evidence item(s) (*description*):
Silver Hitachi Deskstar 500GB Hard drive bearing Model Number: HDP7250GLA360 and Serial Number: RF3MRNEJ. This device has the number 3 written on it in blue ink and has some scratches on the side. It appears to be in good working condition.

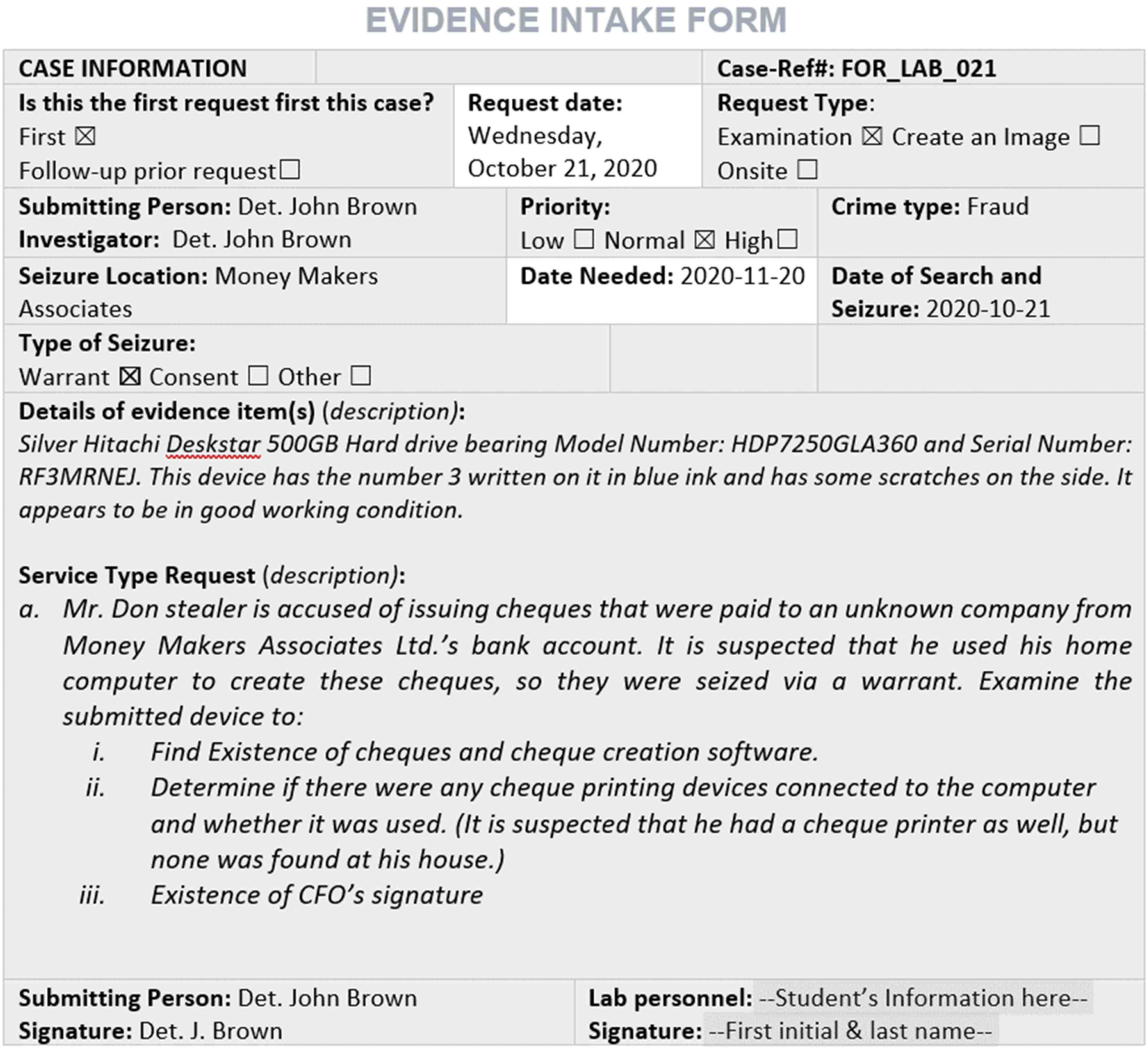
Service Type Request (*description*):
a. Mr. Don stealer is accused of issuing cheques that were paid to an unknown company from Money Makers Associates Ltd.'s bank account. It is suspected that he used his home computer to create these cheques, so they were seized via a warrant. Examine the submitted device to:
i. Find Existence of cheques and cheque creation software.
ii. Determine if there were any cheque printing devices connected to the computer and whether it was used. (It is suspected that he had a cheque printer as well, but none was found at his house.)
iii. Existence of CFO's signature

11. Finally, at the bottom of the form, we get to the names and signatures. These fields show accurately who handed over the device(s) and who received it. Select Det. John Brown in the Submitting person is first and last name field and enter Det. J Brown in the Submitting person's signature field as seen in items 1 - 4 below. Next, enter your details in the Lab personnel first and last name and Lab personnel signature fields as seen in item 5.



Submitting Person: Choose an item.
Signature: Choose an item.
Lab personnel: --Student's Information here--
Signature --First initial & last name--

12. Once the signatures are entered, the document becomes a link in the chain of custody for this evidence item. Typically, labs have much more detailed forms and have options that vary. The ones we provided are the basic ones that you will find in most intake forms. Most of the fields we entered can be typewritten; however, a unique signature is always recommended for the signature sections. We are now done with this form, and it should now look something like this.



EVIDENCE INTAKE FORM

CASE INFORMATION		**Case-Ref#: FOR_LAB_021**
Is this the first request first this case? First ☒ Follow-up prior request☐	**Request date:** Wednesday, October 21, 2020	**Request Type**: Examination ☒ Create an Image ☐ Onsite ☐
Submitting Person: Det. John Brown **Investigator:** Det. John Brown	**Priority:** Low ☐ Normal ☒ High☐	**Crime type:** Fraud
Seizure Location: Money Makers Associates	**Date Needed:** 2020-11-20	**Date of Search and Seizure:** 2020-10-21
Type of Seizure: Warrant ☒ Consent ☐ Other ☐		

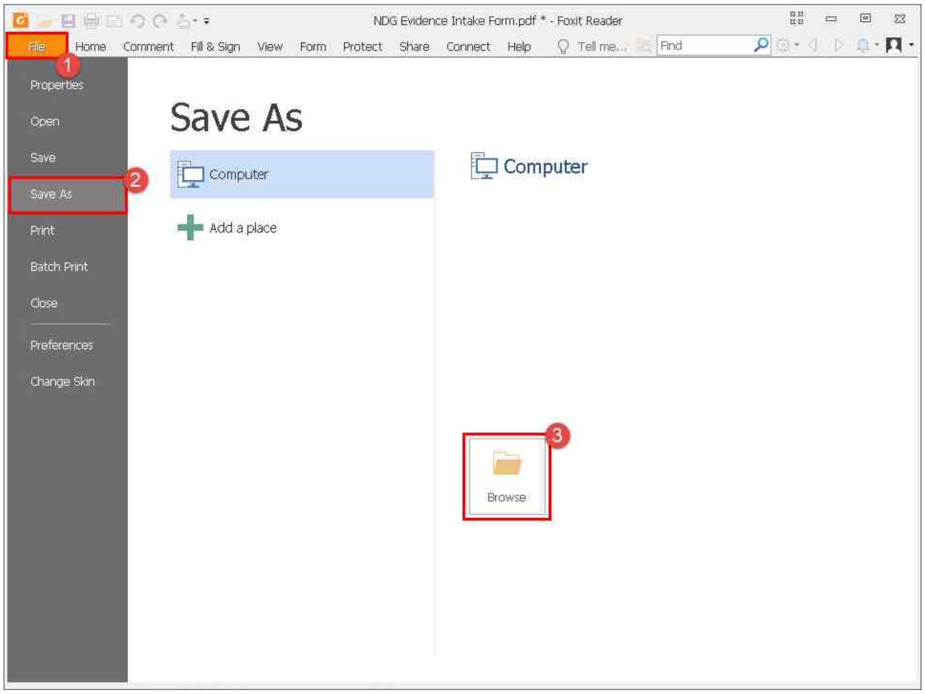
Details of evidence item(s) (*description*):
Silver Hitachi Deskstar 500GB Hard drive bearing Model Number: HDP7250GLA360 and Serial Number: RF3MRNEJ. This device has the number 3 written on it in blue ink and has some scratches on the side. It appears to be in good working condition.

Service Type Request (*description*):

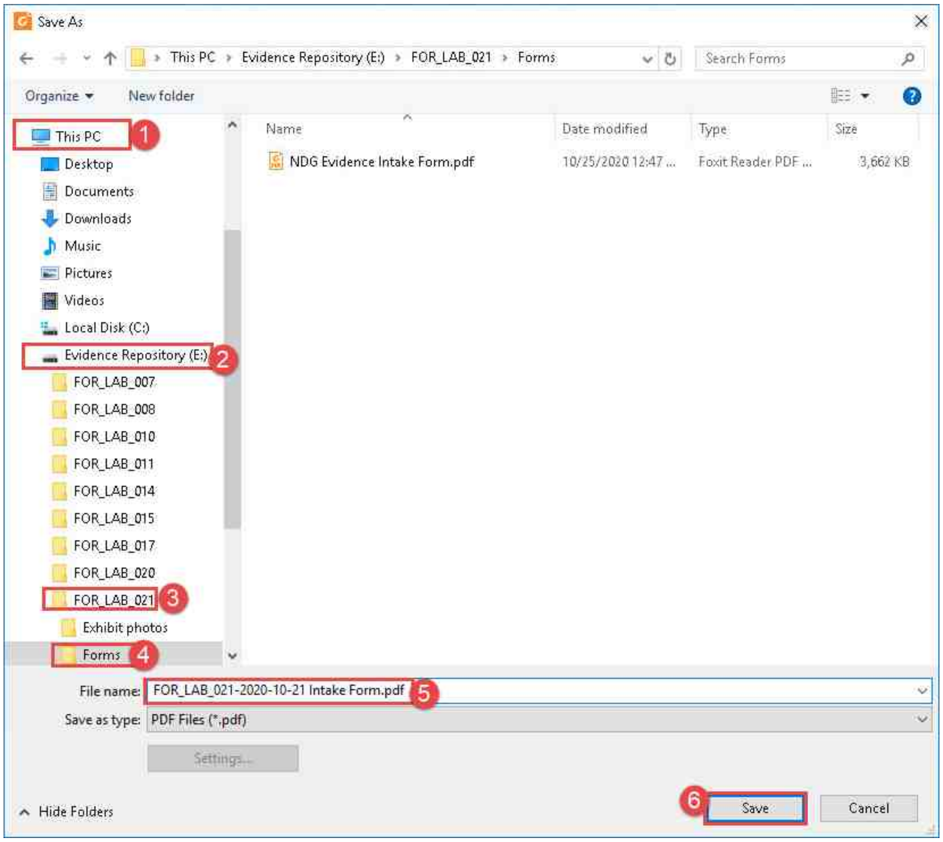
a. *Mr. Don stealer is accused of issuing cheques that were paid to an unknown company from Money Makers Associates Ltd.'s bank account. It is suspected that he used his home computer to create these cheques, so they were seized via a warrant. Examine the submitted device to:*
   i. *Find Existence of cheques and cheque creation software.*
   ii. *Determine if there were any cheque printing devices connected to the computer and whether it was used. (It is suspected that he had a cheque printer as well, but none was found at his house.)*
   iii. *Existence of CFO's signature*

Submitting Person: Det. John Brown **Signature:** Det. J. Brown	**Lab personnel:** --Student's Information here-- **Signature:** --First initial & last name--

13. Save it by navigating to File > Save As > Browse as seen in items 1, 2, and 3 below.



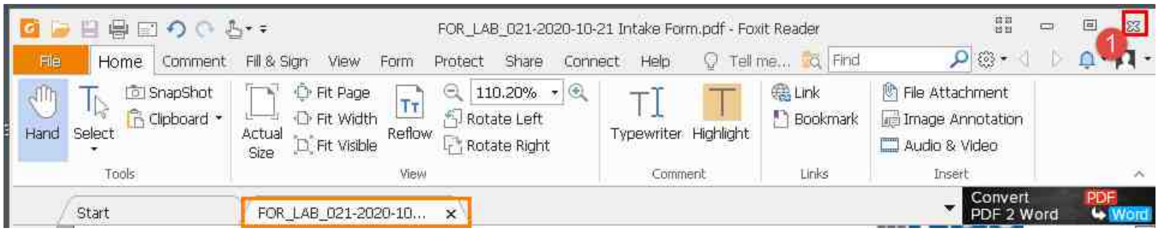
14. This will open Windows File Explorer. Navigate back to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Forms as seen in items 1,2,3, and 4. Now let us give the file a more meaningful name; this will help with recalling the contents of the form. The name format will be Case-Ref#-Request date(YYYY-MM-DD) Intake Form.pdf, for example, `FOR_LAB_021-2020-10-21 Intake Form.pdf` as seen in item 5. Once done, click Save as seen in item 6 below.



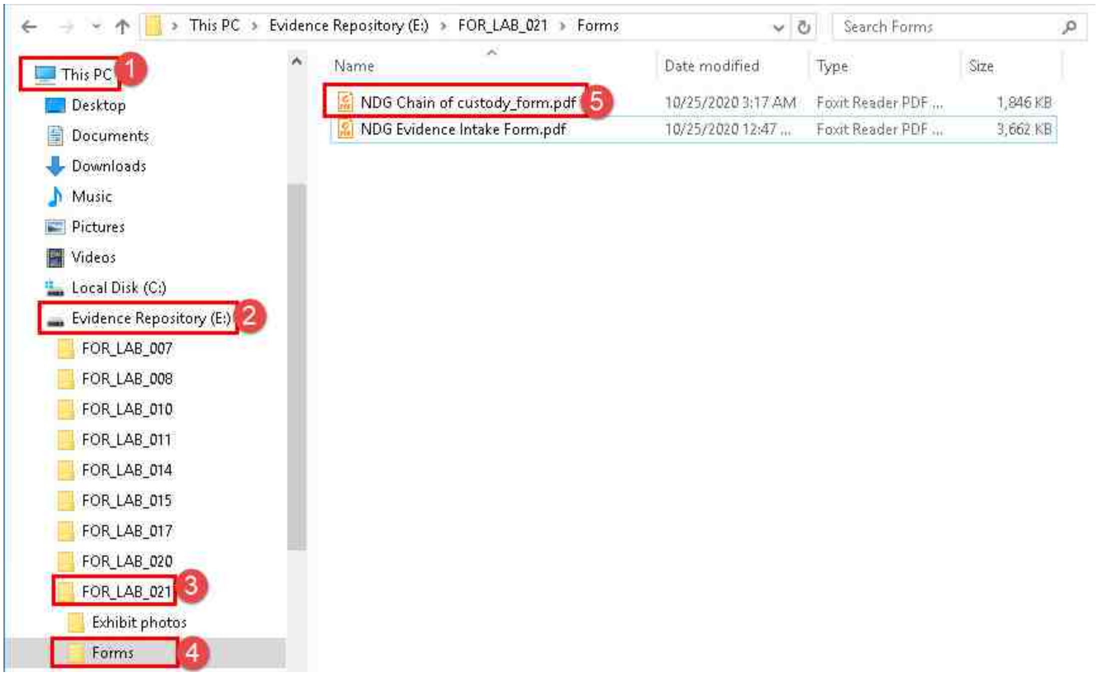
File name: FOR_LAB_021-2020-10-21 Intake Form.pdf

Save as type: PDF Files (*.pdf)

15. Once done, in the top-right corner to close this file, as seen in item 1.

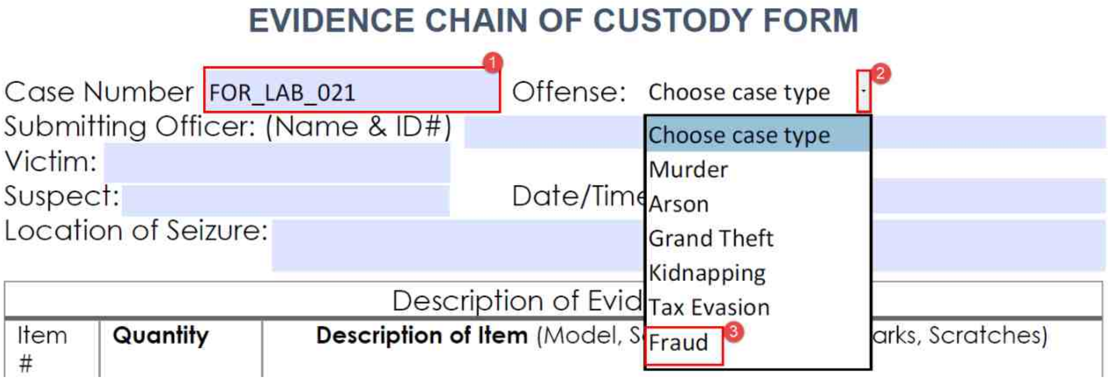


16. Next, we will fill out the chain of custody form for each device that was seized. Begin by opening Windows File Explorer and navigating to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Forms as seen in items 1,2,3, and 4. Once there, double-click the file called NDG Evidence Intake form.pdf as seen in item 5.



Name	Date modified	Type	Size
NDG Chain of custody_form.pdf	10/25/2020 3:17 AM	Foxit Reader PDF ...	1,846 KB
NDG Evidence Intake Form.pdf	10/25/2020 12:47 ...	Foxit Reader PDF ...	3,662 KB

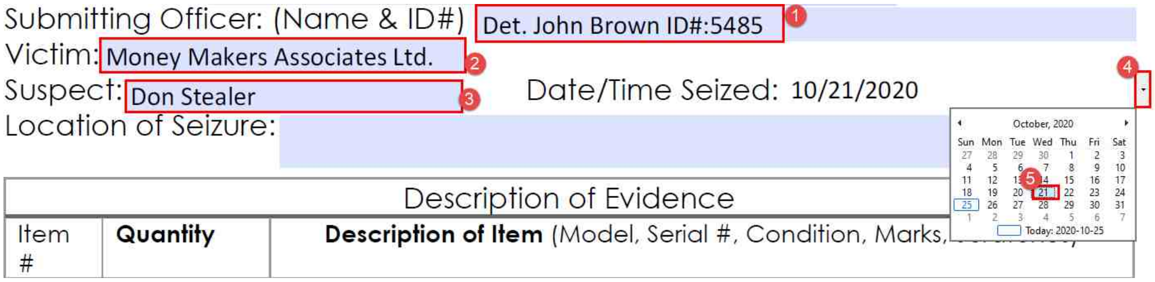
17. The chain of custody form will open, allowing you to enter the details of each person who handles the device after the intake form was filled out. Let us fill this form out with the information we gathered from exhibits 001 in the previous exercise. First, provide details of the case, such as the assigned case number. Enter `FOR_LAB_021` in the Case Number field, as seen in item 1 below. Next, choose a case type. This will tell what type of investigation is being performed. Click the grey area marked Choose a case type as seen in item 2. This will open a window where you can choose the type of matter. In this exercise, we will select Fraud as seen in item 3 below.



EVIDENCE CHAIN OF CUSTODY FORM

Case Number: FOR_LAB_021
Offense: Choose case type

18. Next, we will put the name of the submitting person. Type the Name and ID # `Det. John Brown ID# 5485` here, as seen in item 1 below. In the Victim field, type `Money Makers Associates Ltd.` and enter `Don Stealer` as the Suspect, as seen in items 2 and 3, respectively. Next, enter the current date and time in the Date Seized field by clicking the click to enter a date area, as seen in item 4. This will open a calendar that will allow you to find the current date and time as seen in item 5 below.



Submitting Officer: (Name & ID#) Det. John Brown ID#:5485

Victim: Money Makers Associates Ltd.

Suspect: Don Stealer

Date/Time Seized: 10/21/2020

Location of Seizure:

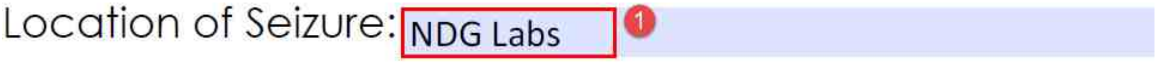
Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks,

October, 2020

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

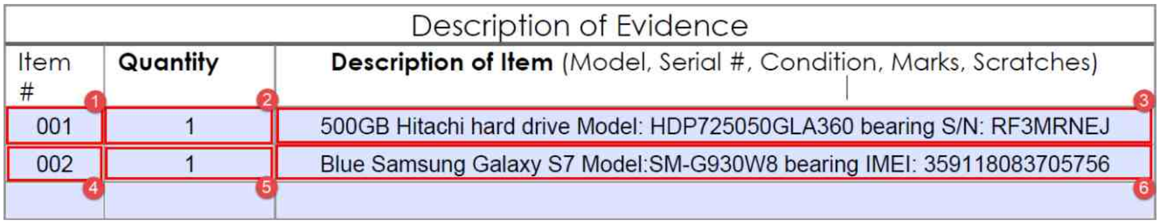
Today: 2020-10-25

19. Next, we will enter the Location of Seizure. Enter `NDG Labs` in this field, as seen in item 1.



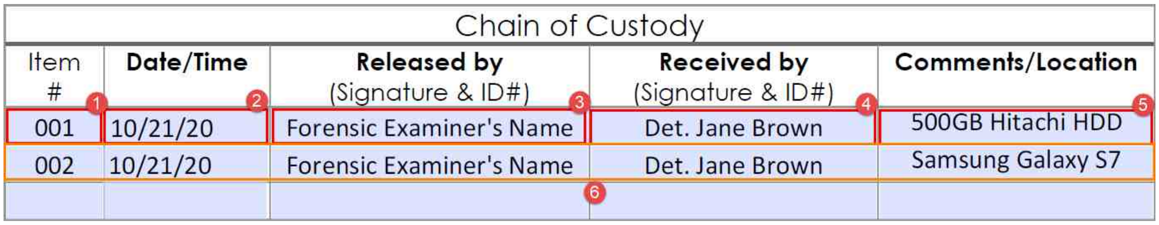
Location of Seizure: NDG Labs

20. Now we will enter the details of the device(s) being entered in this form. This will be done in the Description of Evidence table. The first column contains the evidence ID (eg. 001). Enter `001` in the first row in this column, as seen in item 1. The quantity column refers to the number of items being accounted for. Since evidence 001 is just 1 hard drive, we will put 1 in the quantity as seen in item 2. Next is the description of EID 001. Enter the description you noted for EID 001, `500GB Hitachi hard drive Model: HDP725050GLA360 bearing S/N: RF3MRNEJ` as seen in item 3. Repeat the process for EID 002 `Blue Samsung Galaxy S7 Model:SM-G930W8 bearing IMEI: 359118083705756` as seen in items 4, 5, and 6 below.



Description of Evidence		
Item #	**Quantity**	**Description of Item** (Model, Serial #, Condition, Marks, Scratches)
001	1	500GB Hitachi hard drive Model: HDP725050GLA360 bearing S/N: RF3MRNEJ
002	1	Blue Samsung Galaxy S7 Model:SM-G930W8 bearing IMEI: 359118083705756

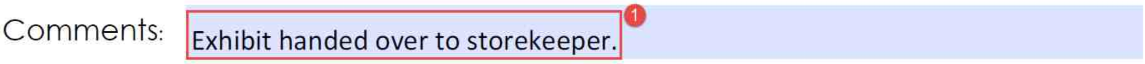
21. Once you are done entering EID 001 and 002, let us move to the table called Chain of Custody. In this form, we will simulate handing over the device to the exhibit storekeeper. Let us begin by entering `EID 001` in the item # column as seen in item 1 below. Next, we will enter the current date and time to indicate the time of the custody change, as seen in item 2. Next, enter your name in the Released by field seen in item 3. (A signature should be entered in this field as well to verify that the person handling the evidence matches the signature.) In the Received by field, enter `Det. Jane Brown` as seen in item 4. In the Comments/Location field, enter the names of each exhibit, as seen in item 5. Repeat the process for EID 002 as seen in item 6 below.



Chain of Custody

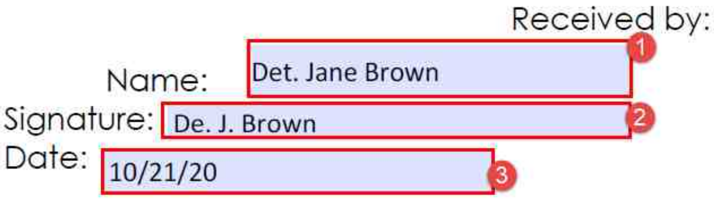
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
001	10/21/20	Forensic Examiner's Name	Det. Jane Brown	500GB Hitachi HDD
002	10/21/20	Forensic Examiner's Name	Det. Jane Brown	Samsung Galaxy S7

22. Next, enter some comments to provide a summary of the purpose for the change. Enter `Exhibit handed over to storekeeper` in the Comments field, as seen in item 1 below.



Comments: Exhibit handed over to storekeeper.

23. Finally, at the bottom of the form, we get to the name and signature. These fields show who received the device(s). Enter `Det. Jane Brown` in the Name field, enter `Det. J Brown` in the Signature field, and the Date as seen in items 1, 2, and 3 below.



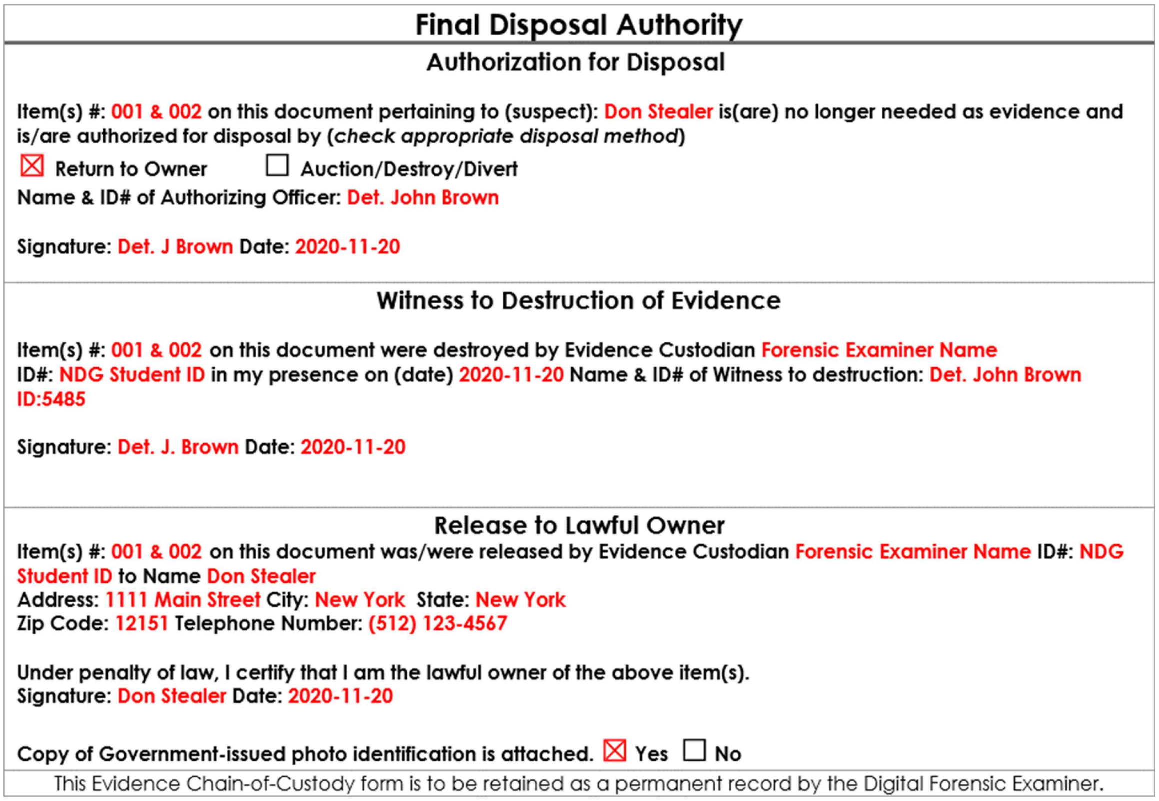
Received by:

Name: Det. Jane Brown

Signature: De. J. Brown

Date: 10/21/20

24. This form also has a Final Disposal Authority section, which provides details on how you disposed of the exhibit. We will not be filling out this form, but it is worth reviewing to see what options are available for disposal and the types of information necessary to perform the disposal.



Final Disposal Authority

Authorization for Disposal

Item(s) #: 001 & 002 on this document pertaining to (suspect): Don Stealer is(are) no longer needed as evidence and is/are authorized for disposal by (*check appropriate disposal method*)

☒ Return to Owner ☐ Auction/Destroy/Divert

Name & ID# of Authorizing Officer: Det. John Brown

Signature: Det. J Brown Date: 2020-11-20

Witness to Destruction of Evidence

Item(s) #: 001 & 002 on this document were destroyed by Evidence Custodian Forensic Examiner Name ID#: NDG Student ID in my presence on (date) 2020-11-20 Name & ID# of Witness to destruction: Det. John Brown ID:5485

Signature: Det. J. Brown Date: 2020-11-20

Release to Lawful Owner

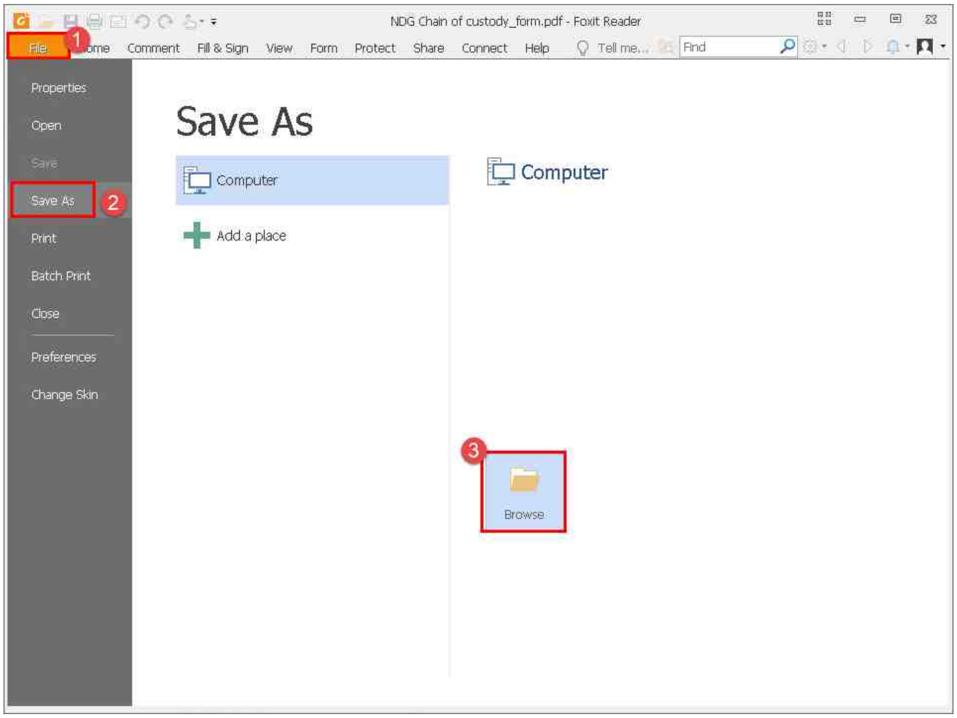
Item(s) #: 001 & 002 on this document was/were released by Evidence Custodian Forensic Examiner Name ID#: NDG Student ID to Name Don Stealer
Address: 1111 Main Street City: New York State: New York
Zip Code: 12151 Telephone Number: (512) 123-4567

Under penalty of law, I certify that I am the lawful owner of the above item(s).
Signature: Don Stealer Date: 2020-11-20

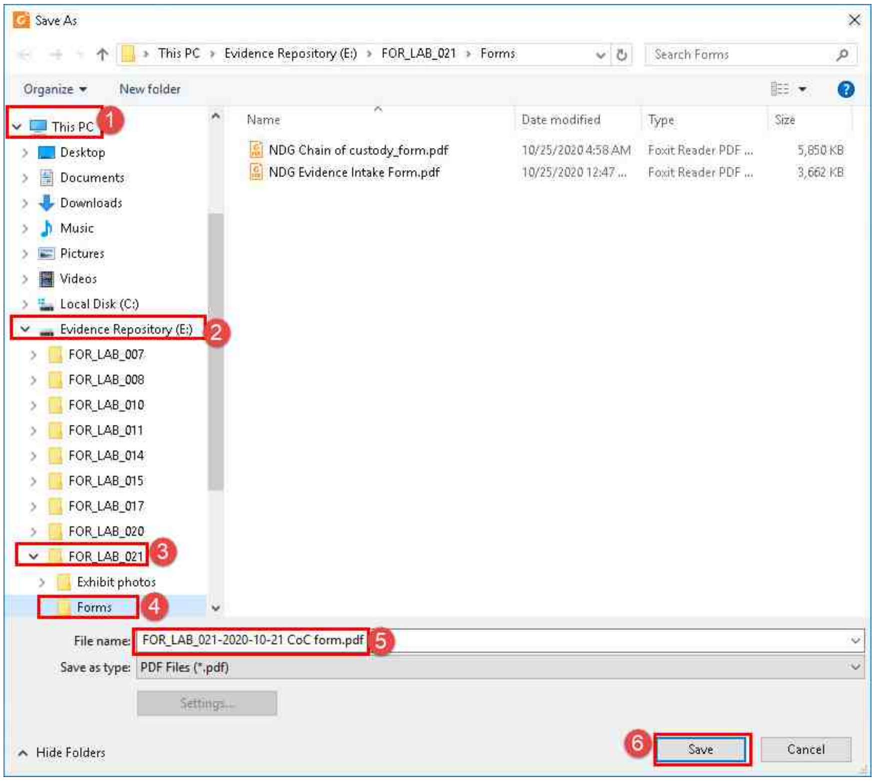
Copy of Government-issued photo identification is attached. ☒ Yes ☐ No

This Evidence Chain-of-Custody form is to be retained as a permanent record by the Digital Forensic Examiner.

25. We are now done with this form. Save it by navigating to File > Save As > Browse as seen in items 1, 2, and 3 below.



26. This will open Windows File Explorer. Navigate back to ThisPC > Evidence Repository (E:) > FOR_LAB_021 > Forms as seen in items 1,2,3, and 4. Now let us give the file a more meaningful name; this will help with recalling the contents of the form. The name format will be Case-Ref#-Request date(YYYY-MM-DD) CoC form.pdf, for example, `FOR_LAB_021-2020-10-21 CoC Form.pdf` as seen in item 5. Once done, click Save, as seen in item 6 below.

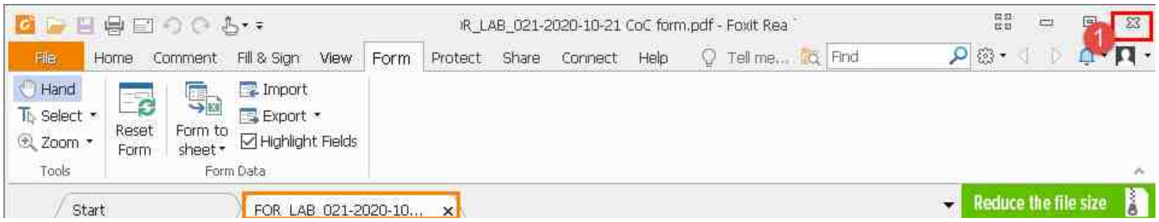


Name	Date modified	Type	Size
NDG Chain of custody_form.pdf	10/25/2020 4:58 AM	Foxit Reader PDF ...	5,850 KB
NDG Evidence Intake Form.pdf	10/25/2020 12:47 ...	Foxit Reader PDF ...	3,662 KB

File name: FOR_LAB_021-2020-10-21 CoC form.pdf (5)

Save as type: PDF Files (*.pdf)

27. Once done, click the X in the top-right corner to close this file, as seen in item 1.


R_LAB_021-2020-10-21 CoC form.pdf - Foxit Rea
1
File
Home
Comment
Fill & Sign
View
Form
Protect
Share
Connect
Help
Tell me...
Find
Hand
Select
Zoom
Tools
Reset Form
Form to sheet
Import
Export
Highlight Fields
Form Data
Start
FOR_LAB_021-2020-10...
Reduce the file size