Cengage | CEN-CFORENSICS7e: Computer

Forensics 7th Edition

Ethics and Professional Responsibilities

Exercises

• Introduction

• Exercise 15-1 - Determining Hexadecimal Values for Text Strings

• Hands-On Project 15-1

• Hands-On Project 15-2

• Hands-On Project 15-3

• Hands-On Project 15-4

• Summary

Introduction

The Ethics and Professional Responsibilities module provides you with the

instructions and devices to develop your hands-on skills in the following

topics.

• Exercise 15-1 Determining Hexadecimal Values for Text Strings

• Hands-On Project 15-1

• Hands-On Project 15-2

• Hands-On Project 15-3

• Hands-On Project 15-4

Lab Diagram

During your session, you will have access to the following lab configuration.

Depending on the exercises you may or may not use all of the devices, but

they are shown here in the layout to get an overall understanding of the

topology of the lab.Connecting to Your Lab

In this module, you will be working on the following equipment to carry out

the steps defined in each exercise.

• PLABWIN10 (Windows 10 - Standalone Workstation)

Each exercise will detail which device you are required to work on to carry out

the steps.

Help and Support

For more information on using Practice Labs, please see our Help and

Support page. You can also raise a technical support ticket from this page.

Lab Assessment

Test your knowledge on the topics covered in this lab by completing the Lab

Assessment. Screenshot assessment items can be found at the end of each

exercise and review questions are located on the Summary page.

Click Next to proceed to the first exercise.

Copyright © Practice Labs 2007 - 2022. All rights reserved.Exercise 15-1 - Determining Hexadecimal Values

for Text Strings

To begin examining the forensic image, you start by determining the

hexadecimal values for the text string “Kayak4.” Follow these steps to convert

the text values into hexadecimal values and save the results to a text file so

that you can refer to them easily when performing searches for Unicode data.

Task 1 - Install HxD

If the HxD hex editor is already installed, you can skip this Task. If not,

complete the following steps to install it.

Step 1

Ensure that you have powered on the required devices in the Introduction.

Connect to PLABWIN10.

Click File Explorer on the taskbar and navigate to the Downloads folder. Run

the HxDSetup.exe install file, double-clicking is one way to accomplish this.

Step 2

Click OK in the Select Setup Language dialog box.Click Next in the Setup - HxD Hex Editor dialog box.

Step 3

Accept the License Agreement and click Next.Step 4

Click Next for the next few Setup dialog boxes, using all the default settings

until you get to the Select Additional Tasks dialog box.

In the Select Additional Tasks dialog box, check the Create a desktop

shortcut checkbox.

Step 5

Click Install in the Ready to Install dialog box.Step 6

In the Completing the HxD Hex Editor Setup Wizard dialog box, uncheck both

checkboxes and click Finish.Task 2 - Extract Disk Image

In this task, you will prepare a disk image that will be used in the computer

forensics application called ProDiscover.

To extract the disk image, do the following steps:

Step 1

On the PLABWIN10 device, File Explorer is open.

Navigate to Local Disk (C:) > Work > Data files > Mod15.

Right-click InMod15.zip and select Extract All….

Step 2

On the Select a Destination and Extract Files dialog box, click Extract.Step 3

When InMod15 is successfully extracted, you will have the InMod15New.dd

image file available in the InMod15 folder.

Close all instances of File Explorer.Task 3 - Using WinHex

In this task, you will start using WinHex and get familiar with working with

hexadecimal numbers.

Step 1

On the PLABWIN10 device, start HxD from the desktop.Step 2

Click File and select New from the menu.

Step 3Move the cursor to the Decoded text area and type a capital letter K.

In the Confirm dialog box, check the Do not ask this question again checkbox

(so we can add more characters without having to confirm each character)

On the left side, click under offset 01 and type 00. We want a null character

between each letter we are typing in the Decoded text area, but we can’t type

a null character in the Decoded text area, so we have to go back and

manually enter the hex value 00, which is a null character.

Note that you are not typing a period in the Decoded text zone. The period is

placed there automatically when you enter the hex value 00 (null character) in

the Offset area.Step 4

Continue this process of entering a character in the Decoded text zone, and

entering a null character right after it, using the Offset hex input area. The

next figure shows the desired result.Step 5

Click File and select Save As.

In the Save File As dialog box, navigate to Local Disk (C:) > Work > Data

files > Mod15 folder path.

In the File name box, type:

InMod15-unicode.dat

Click Save.Step 6

Close the HxD application.

Step 7

Launch the Notepad application.

The hexadecimal value for K A Y A K 4 is indicated below.

4B 00 41 00 59 00 41 00 4B 00 34 00

Please read the following information before proceeding to the next steps.

Important: If you are connected to this lab using an HTML5 client, click

the Menu drop-down found at the top center of the screen. A variety of

selections appear, including Clipboard. Click the Clipboard button. You

can use the Clipboard as a temporary placeholder for the text file that

you copy from the lab instructions. Paste the text in the Clipboard and

click Send to remote. Remember that you must clear the Clipboard

before you paste a new set of text and click Send to update the Clipboard

contents.If you are connected to this lab using a Java client, download a PDF version

of the lab instructions. Copy the hexadecimal from the PDF file and paste it

directly on the Notepad application currently open on the PLABWIN10

device.

Step 8

You can paste the string of numbers above and put it on Notepad.

You need to remove the spaces between the numbers to allow you to use

them in ProDiscover Basic.Step 9

Place the insertion point at the beginning of the string of numbers.

Click Edit and select Replace.

Step 10

On the Replace dialog box, while the insertion point is in the Find what field,

press SPACEBAR once.

Press TAB.

The insertion point jumps to Replace with field.

Click Replace All.Step 11

Notice that the spaces between the numbers were removed.

Click Cancel and then minimize the Untitled-Notepad window. You will need

this later.Task 4 - Using ProDiscover to Search for Unicode

Data

With the collected information from the previous task, now it’s time to

examine the anonymous user’s disk image.

To start using ProDiscover, perform the following steps:

Step 1

Start the ProDiscover Basic 64 application from the desktop.

On the Launch Dialog box, for the project number and filename, type:

InMod15

Click Open.Step 2

Click Action from the menu, point to Add, and click Image File.

Step 3In the Open dialog box, navigate to C:\Work\Data files\Mod15\Mod15 and

select file InMod15New.dd, and then click Open.

Step 4

Click the Action menu and select Search.Step 5

In the Search dialog box, verify that you are in the Content Search tab, and

then click the Hex option button.

Click the Search for the pattern(s) option button, if necessary, and restore

the Untitled-Notepad window.Step 6

Select the block of numbers, and then right-click on them and select Copy.

Minimize Untitled-Notepad window.Step 7

Go back to the Search dialog box.

Ensure that the Search for the pattern(s) option is selected. Right-click the

empty text box and select Paste.

Step 8

Under Select the Disk(s)/Image(s) you want to search in, click the image

file and then click OK.Step 9

Please wait while the search is in progress.

In the search results window, click pagefile.sys, and scroll down through the

contents until you have located string data matching the search criteria, and

look for K A Y A K 4Step 10

The lower pane of the search results contains a portion of what seems to be a

previously created MFT file. The FILE0 header appears to be associated with

files starting with “KAYAK4.” This finding could mean that an MFT file

occupied this space where pagefile.sys is located now. How this result might

occur varies; the cause might be a reformatted disk or a new OS installation.

Reformatting or reinstalling an OS doesn’t completely overwrite previous data

on a disk, thus revealing residual data, such as previous MFT records and their

associated files.Step 11

Next, double-click pagefile.sys.

Step 12The files are in the main ProDiscover window.

Scroll down in the file list in the main ProDiscover window, and then right-click

the pagefile.sys file and click Copy File.

Step 13

Ensure that you are using the This PC > Local Disk (C:) > Work > Data files >

Mod15 > InMod15 folder path.

Accept the indicated name in the File name text box.

Click Save.Step 14

Exit ProDiscover Basic and click Yes when prompted to save the project.

Click Save.Task 5 - Interpreting Attribute 0x80 Data Runs

The next task is a detailed examination of the pagefile.sys file in HxD. You

learn how to interpret data runs from the MFT file’s fragments found in

pagefile.sys.

Navigating through an MFT Record for this task, you need HxD and a

spreadsheet program, such as OpenOffice Calc. To examine pagefile.sys with

HxD, follow these steps:

Step 1

On the PLABWIN10 device, launch HxD from the desktop.

Click File, Open from the menu.

Step 2

Navigate to C:\Work\Data files\Mod15\InMod15 and select pagefile.sys,

and then click Open.Step 3

Notice that a new tab called pagefile.sys is opened.

Click the Search menu and click Find.Step 4

In the Find dialog box, in the Search for: text box on the Text-string tab, type:

KAYAK4

Click the Case sensitive check box, if necessary.

Select Unicode for the Text encoding: option, select All for the Search

direction, and then click OK.

Step 5

When searching for specific record information, sometimes there are

duplicate files with the same name that have different data runs, meaning the

file was written to disk more than one time on separate occasions. When

performing a search, you need to examine all search results, compute their

data run values, and attempt to recover the files. If your first effort doesn’t

produce successful results, continue searching for other occurrences.

In the main window, the cursor is placed in the right pane at the start of the

first occurrence of the Unicode string KAYAK4. From this position, scroll

upward until you see FILE0.Step 6

FILE0 is found.

Step 7To position the cursor at the start of the next attribute, place the cursor in the

middle pane where FILE0 starts, and drag down 0x38 hexadecimal bytes (see

screenshot for your reference), using the Offset and Block(h) counters on the

bottom line as a guide.

Note: All numeric values in these steps are hexadecimal. If the o ff set

counter is in decimal mode, click the row of numbers to the right of the

hexadecimal section once. Each time you click here, HxD toggles between

decimal and hexadecimal modes.

Step 8

Place the cursor at the beginning of attribute 0x10 and drag down 0x60

hexadecimal bytes until you reach the next attribute, 0x30. See screenshot.

The next two sections of the file are the short and long filename attribute

0x30.

Both have lengths of 0x78 hexadecimal bytes. Repeat the previous step until

you reach attribute 0x80.Step 9

From the starting position of attribute 0x30, count 0x40 hexadecimal bytes to

the beginning of the first data run, as shown in the screenshot. Use the

Length(h) counter on the bottom line to make sure you counted 40

hexadecimal bytes.Now that you have located the data run’s starting position, the next task is to

calculate the starting and ending cluster positions of each data run fragment.

Task 6 - Configuring the Data Inspector Window in

HxD

Typically, when HxD starts, the Data Inspector window opens, where you can

view data formats into easy-to-read values, such as converting hexadecimal

values into decimal values. For the following activities, you need to know how

to configure the Data Inspector window to perform data run calculations.

Follow these steps:

Step 1

On the PLABWIN10 device, the WinHex application is open.

To find out if the Data inspector is open, click the View menu, point to Show,

and ensure that the Data inspector is checked.Step 2

Click the Tools menu and click Options.Step 3

Click the Data inspector Options tab, verify that the following check boxes

are selected: Int8, Int16, and Int24 (clearing any other check boxes that are

selected), and then click OK. You will have to scroll down to access all the

boxes that you need to uncheck.

Leave HxD open for the next activity.

Task 7 - Calculating Data Runs

Next, you determine the starting and ending cluster numbers for the MFT

record’s data run. The length of this MFT record is less than 512 bytes (0x200

hexadecimal), so the data runs don’t have an update sequence array value, as

described in Module 6.

To calculate the data runs for this example, follow these steps:

Step 1

On the PLABWIN10 device, the HxD application is open.

To determine the number of clusters for the first data run, place the cursor on

the data run position immediately to the right of the first data run position 31,

as shown in the screenshot. Because it’s only 1 byte long, the 0x08 converts to8 in decimal (as shown in the Data Inspector window), which indicates 8

clusters in the first data run.

Step 2

To determine the starting logical cluster number (LCN) position for this data

run, place the cursor to the left of the 4 in the string 45 6D 03. This address

location is 3 bytes, or 24 bits, as shown in the screenshot. Therefore, the

starting LCN position for the first data run is 224581, as shown in the Data

inspector window.Step 3

Next, move the cursor to the next data run’s cluster count position; it also has

the hexadecimal value 0x08, which converts to decimal 8. The next 2 bytes (16

bits) display the virtual cluster number (VCN) 2C FF, which converts to -212 in

decimal (see screenshot).Step 4

values.

Repeat Steps 1 to 3 to find the remaining clusters per fragment and the VCN

Refer to Module 6 for information on how NTFS manages MFT records, or

search this topic to find additional information about this concept.

Step 5

To simplify the calculations, enter the LCN and VCN values in a spreadsheet,

as shown in the following screenshot.

In the Start menu, click the OpenOffice 4.1.5 folder. Click on OpenOffice

Calc and begin entering the LCN and VCN values in the spreadsheet.

When you’re finished, exit HxD. Note that columns C and E of the spreadsheet

have formulas that compute the LCN value from the VCN value in column B

and the ending LCN in column D.Task 8 - Carving Data Run Clusters Manually

Now that you have calculated the starting and ending cluster positions for the

Kayak4.jpg file, it’s time to recover the fragments in ProDiscover. Recovering

fragments of scattered data files is known as data carving.

To begin data carving, follow these steps:

Step 1

On PLABWIN10, start ProDiscover Basic 64 from the desktop.

Click Cancel in the Launch Dialog box.

Click the Open Project toolbar icon.Step 2

In the Open dialog box, navigate to This PC > Local Disk (C:) > Work > Data

files > Mod15 and click InMod15 folder.

Select the InMod15.dft project, and then click Open.Step 3

In the tree view, click to expand Cluster View and Images, if necessary, and

then click C:\Work\Data files\Mod15\InMod15New.dd.Step 4

In the spreadsheet you created in the previous activity, locate the starting

cluster position (224581) in cell C3, and then locate the clusters per fragment

(8) in cell D3.

In ProDiscover’s work area, click the Decimal check box under the Cluster

text box, type the decimal value 224581 in the text box, and then click Go.

Step 5

Notice that cluster 224581 is now highlighted in red. You may have to make

the left pane smaller so you can see it without scrolling.Step 6

Click cluster position 224581, hold the SHIFT key down, and press the right

arrow key to highlight the SEVEN additional clusters shown in the screenshot.

Note that you will be selecting clusters 224581 to 224588.

Note: When extracting fragments, it’s important to recover only the

clusters from the starting and ending cluster positions. Adding extra

clusters produces a corrupted file that the intended application, such as

Microsoft Word, Excel, or a graphics application, can’t read.Step 7

In the work area, right-click the highlighted cluster blocks and click Recover.

Step 8In the Recover Clusters dialog box, click the Recover all clusters to a single

file option button, if necessary, and then click the Recover Binary check box.

Click Browse.

Step 9

Expand This PC > Local Disk (C:) > Work > Data files > Mod15 and select the

InMod15 folder.

Click OK.Step 10

Click OK to save settings in the Recover Clusters dialog box.

Step 11Leave ProDiscover Basic running.

Step 12

Return to the spreadsheet and find the starting cluster for the second through

fourteenth data run fragments. Follow these steps for each remaining data

run fragment.

Repeat steps 4 to 11 with the following cluster positions.

• 224369 - 224376

• 220769 - 220776

• 220557 - 220564

• 220353 - 220360

• 220141 - 220148

• 219929 - 219936

• 222633 - 222636

• 220973 - 220976

• 212913 - 212916

• 212901 - 212904

• 212285 - 212288

• 212273 - 212276

• 213587Note: There may be some selected clusters on the previous lines;

therefore you are unable to see them.

Task 9 - Append the Fragments

When you have finished carving the fragmented data runs, the next step is

appending the fragments into one file. To combine all fragments, they must

be in the correct order, according to what’s listed in the data runs. If you

switch the order of any fragment, the recovered file is unreadable. Follow

these steps:

Step 1

On the PLABWIN10 device, start HxD from the desktop.

Click the Tools menu, point to File Tools, and click Concatenate.

Step 2

In the Concatenate files dialog box, click the Add button.

In the Add files window, click the InMod15Ne-00224581-00224588.txt file

(see screenshot), and then click Open.Important: The demo version of WinHex can save only files of less than

200 KB at a time. The licensed version of WinHex and X-Ways Forensics

has no limit on file sizes that can be saved.

Now, repeat this process. Continue to Add the following files in order:

• InMod15Ne-00224369-00224376.txt and then click Append.

• InMod15Ne-00220769-00220776.txt and then click Append.

• InMod15Ne-00220557-00220564.txt and then click Append.

• InMod15Ne-00220353-00220360.txt and then click Append.

• InMod15Ne-00220141-00220148.txt and then click Append.

• InMod15Ne-00219929-00219936.txt and then click Append.

• InMod15Ne-00222633-00222636.txt file and then click Append.

• InMod15Ne-00220973-00220976.txt and then click Append.

• InMod15Ne-00212913-00212916.txt and then click Append.

• InMod15Ne-00212901-00212904.txt and then click Append.

• InMod15Ne-00212285-00212288.txt and then click Append.• InMod15Ne-00212273-00212276.txt and then click Append.

• InMod15Ne-00213587.txt file and then click Append.

If you add any of the files in the wrong order, you can change a file position in

the list by selecting it and using the green up and down arrow buttons.

Step 3

Click the browse (…) button beside the Output file name: text box and

navigate to the C:\Work\Data files\Mod15 folder.

In the File name text box, type:

Kayak4.jpg

Ensure that you are in the C:\Work\Data files\Mod15 folder path.

Click Save, and then click OK.Step 4

There is no message box telling you that the concatenation has been

completed; HxD just displays an empty interface.Step 5

Open File Explorer, navigate to C:\Work\Data files\Mod15 folder, and

double-click Kayak4.jpg to view the recovered file.

Step 6

The kayak4.jpg file opens successfully.

Screenshot Click the button to take a screenshot of PLABWIN10

1 of 10

Note: If it fails to open or only a partial image is displayed, review your

steps to make sure you collected the correct clusters and have appended

them in the correct order.

Close Windows Photo Viewer and File Explorer windows.

Similarly, exit the HxD application.The previous exercise is extensive as you collected evidence from a disk

image and concatenated the text files to recover a .jpg file. Well done.

Leave the devices you have powered on in their current state and

proceed to the next exercise.Hands-On Project 15-1

For this project, Sasha wants you to recover a spreadsheet file starting with

the name “Baidar” in InMod15New.dd.

You will use the PLABWIN10 device.

Please note that the above disk image is found in C:\Work\Data

files\Mod15\InMod15. The disk image file should be there, or you may need

to extract it from the zip file as described in Exercise 15-1.

She also needs to know the following:

• When the file was created and last modified

• How many versions of this file are on the drive

• How many versions of this file can be recovered

To find this information, you need HxD and ProDiscover to examine the

pagefile.sys file in InMod15New.dd. As described in the in-chapter activity,

use HxD to find the date and time values, find the cluster addresses from

each data run, concatenate data run fragments, and use ProDiscover to

extract clusters.

Screenshot Click the button to take a screenshot of PLABWIN10

2 of 10

When you have finished this project, write a one-page report describing your

findings and any irregularities in date and time values.

Leave the devices you have powered on in their current state and

proceed to the next exercise.Hands-On Project 15-2

Sasha has new information that the InMod15New.dd image might contain

additional evidence for you to recover. All she knows is that the file might be

named “tourguide.” She has no idea what type of file it is and wants you to

determine its file extension and whether the file can be recovered.

Using ProDiscover Basic 64, conduct a search for the “tourguide\*” keyword

(see screenshot). Examine the file’s contents and perform any steps needed to

extract it from the image file and make it readable. Save the file in your work

folder and give a copy to your instructor.

Screenshot Click the button to take a screenshot of PLABWIN10

3 of 10

Leave the devices you have powered on in their current state and

proceed to the next exercise.Hands-On Project 15-3

After reviewing the files you recovered, Sasha needs to know the creation

date for the Kayak4.jpg file. Using the information in Module 6 for reference

on how to interpret date and time values, locate the created date value for

this file, and use HxD to extract this information from the pagefile.sys file you

used in the in-chapter activity. After determining this information, please

write a short report listing the file’s creation date and turn it into your

instructor.

When using the Data Inspector window for date and time values, place the

cursor at the beginning of the date field. For example, if the date and time

string is EC 09 3A 73 02 C6 C9 01, place the cursor on the EC value.

Screenshot Click the button to take a screenshot of PLABWIN10

4 of 10

Leave the devices you have powered on in their current state and

proceed to the next exercise.Hands-On Project 15-4

Sasha wants you to retrieve a PDF file with a message addressed to Jim Shu

from the InMod15New.dd image.

Using ProDiscover, reopen the in-chapter case file InMod15.dft (you need to

re-create this project if you had previously shut down the PLABWIN10

device) and do a search on the term “\*.pdf.” When you have found this PDF

file, make a note of the path to it. Navigate to this path and examine the file’s

contents. Save the file in your work folder and give a copy to your instructor.

Screenshot Click the button to take a screenshot of PLABWIN10

5 of 10

Lab Assessment

Did you complete all the lab steps? Don't forget to complete the review

questions on the next page.Summary

• Ethics are rules you internalize and use to measure your performance

(internal standards) or standards that you’re compelled to adhere to by

external forces, such as licensing bodies (codes of professional conduct or

responsibility). Laws governing codes of professional conduct or

responsibility typically define the lowest level of action or performance

required to avoid liability.

• Digital forensics examiners don’t have the same formal, detailed codes of

conduct that professions such as medicine and the law have, so relying on

an internal code of ethics may be more critical. Additional sources include

codes of professional associations you belong to, certifying bodies that

have granted you a certification, and your employer’s rules of

professional conduct. Most examiners rely on a combination of these

standards to construct their professional ethical codes.

• You owe your client a full understanding of the facts relevant to your

opinion, and you can ask them to establish that there is evidence

supporting the facts your opinion will be based on.

• Be aware of attempts to disqualify you as an expert. Opposing counsel

might attempt to disqualify you based on any deviations from opinions

you have given in previous cases, so be prepared to explain the reason for

any changes in your position. Some attorneys might contact you solely for

the purpose of discrediting or disqualifying you (conflicting out). Always

note calls from attorneys and the nature of the communication and

require that any attorney contacting you complete a client questionnaire

and send you an investigation retainer.

• Courts use many factors in determining whether to disqualify an expert,

such as whether an expert was formally retained and compensated,

whether an expert was informed that discussions were confidential, and

so on.

• Be aware of and avoid obvious ethical errors, such as altering data or

presenting false data, ignoring contradictory data, performing work

beyond your expertise or competence, allowing the attorney who hired

you to influence your opinion improperly, and reaching a conclusion

before completing your research.

• No single source offers a definitive code of ethics for expert witnesses, so

you must draw on standards from other organizations to form your own

ethical standards. Many professional organizations, such as the ABA and

the APA, have rules to guide their members in areas such as interaction

with patients/clients, objectivity, role in society, fees, solicitation,independence, and contractual relationships.

• The International Society of Forensic Computer Examiners (ISFCE) Code

of Ethics and Professional Responsibility provides guidelines for its

members, and the International Association of Computer Investigative

Specialists (IACIS) has a well-defined, simple guide describing the

expected behavior of forensics examiners.

• The inherent conflict between the needs of the justice system and your

obligations for professional conduct can create ethical difficulties. With

an adversarial legal system, pressures from hiring attorneys, and a

tendency to identify with the side you’re working for, maintaining

impartiality can be difficult. Digital forensics examiners should consider

their personal values, review the codes of conduct that apply to other

professions, and develop a personal code of conduct that will protect

them from ethical errors.

• The attorney who has retained you, opposing counsel, and the court owe

ethical responsibilities to you when you serve as an expert witness. For

example, your attorney owes you a fair statement of the case or situation,

adequate time to review the evidence and prepare your report, and a

reasonable opportunity to examine data, conduct testing, and investigate

the matter before rendering an opinion.

• As a forensics examiner, you will interact and work with attorneys, so be

aware of the basic rules of professional conduct they must follow. The

American Bar Association is not a licensing body, but its Model Code of

Professional Responsibility and its successor, the Model Rules of

Professional Conduct, are the basis of state licensing bodies’ codes.

• The tools you use to recover, control, and track evidence are subject to

review by opposing parties. If the court deems them unreliable, the

evidence you recovered with those tools might not be admitted or be

admitted with a limiting instruction. If you create tools for your own use,

you must still validate them and submit them for review.

• Digital forensics examiners should develop and use an intake form. The

intake form serves several purposes, including ascertaining the nature of

the examination, ensuring sufficient information is collected about a case,

documenting the skills, resources, and information necessary to conduct

an examination and support the case, and identifying any possible

conflicts of interest for the examiner.

• Digital forensics examiners may be asked to peer review a report to verify

the findings or to identify strengths and weaknesses in another

examiner’s work. A peer review report should be objective and shouldinclude evidence that supports or disputes the other examiner’s findings.

Lab Assessment

Test your knowledge on the topics covered in this lab by completing the

review questions below.

6 of 10

Question What is the action of extracting data fragments of a scattered data file

for the purpose of reassembling them in order to recover the file called?

Question Which of the following organizations has a guide for the expected

behavior of forensics examiners?

7 of 10

8 of 10

Question In this lab, you need to recover a file using a forensic technique – if done

correctly, what is the image?9 of 10

Question Which of the following are codes of conduct that attorneys must follow?

Question All of the following would be considered ethical errors, EXCEPT:

10 of 10

Summary

Please ensure you have completed all items before submitting your

report, submitting will log you out.

Screenshot 

Screenshot 

Screenshot 

Screenshot Screenshot 

Question 

Question 

Question 

Question 

Question 