FORENSICS
LAB SERIES

Lab 12: Introduction to Digital Forensics Framework

Document Version: 2016-08-17

Copyright © 2016 Network Development Group, Inc.
www.netdevgroup.com

NETLAB Academy Edition, NETLAB Professional Edition and NETLAB+ are registered trademarks of Network Development Group, Inc.

Contents

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Introduction

This lab will introduce the features of the *Digital Forensics Framework* (*DFF*). *DFF* is an open source computer forensics platform built on top of a dedicated *Application Programming Interface*(*API*).

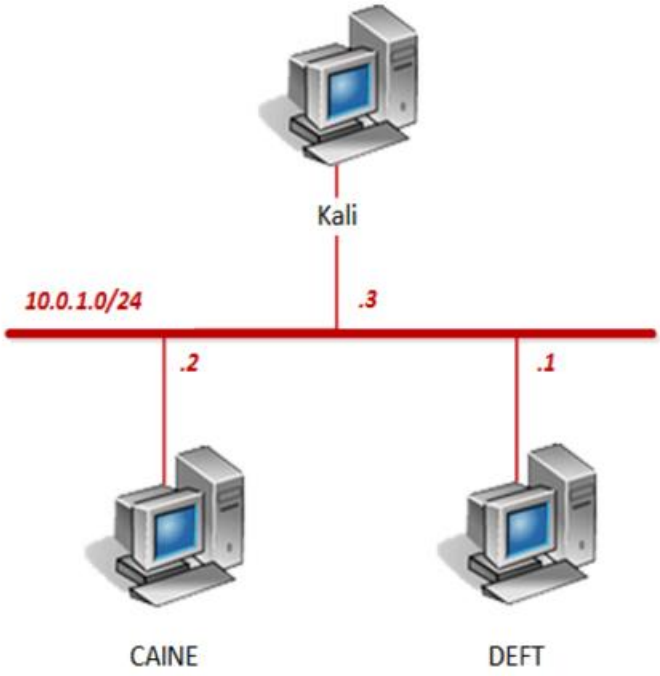
Objective

In this lab, you will be conducting forensic practices using various tools. You will be performing the following tasks:

1. Opening Partitions with DFF
2. Analyzing Partition Data with DFF

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Pod Topology



 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

Lab Settings

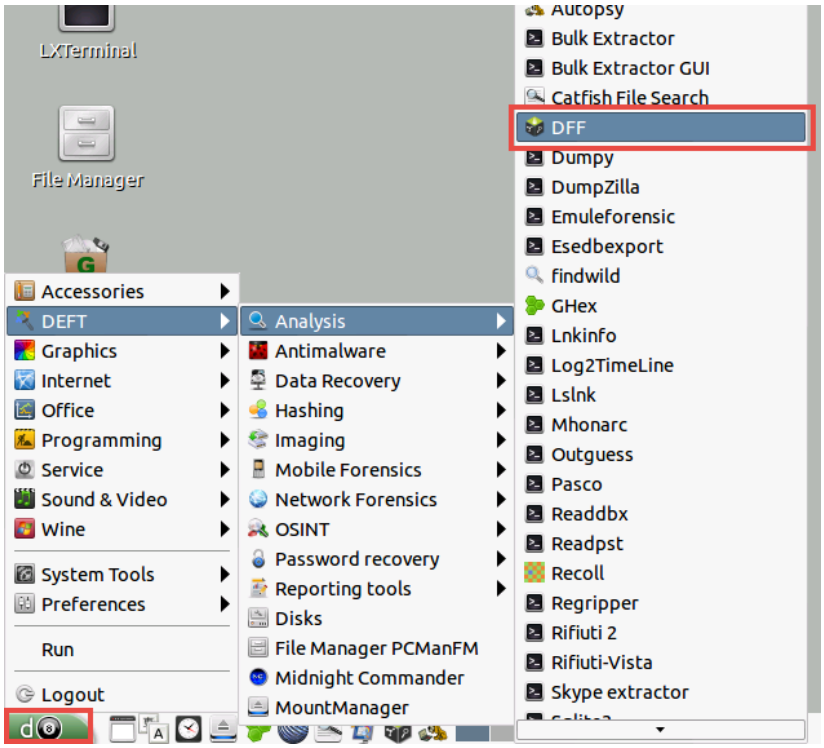
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address	Account (if needed)	Password (if needed)
DEFT	10.0.1.1	deft	password
CAINE	10.0.1.2	caine	
Kali	10.0.1.3	root	toor

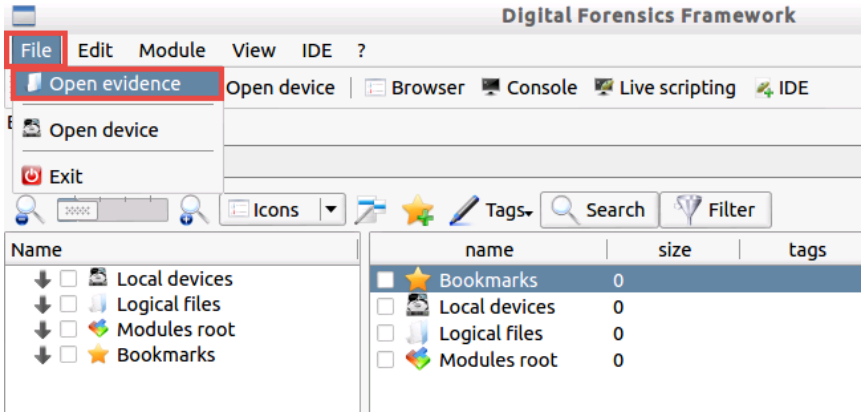
 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

1 Opening Partitions with DFF

1. Click on the **DEFT** graphic on the *topology page* to open the VM.
2. Open the *Digital Forensics Framework* application by navigating to **Menu > DEFT > Analysis > DFF**.

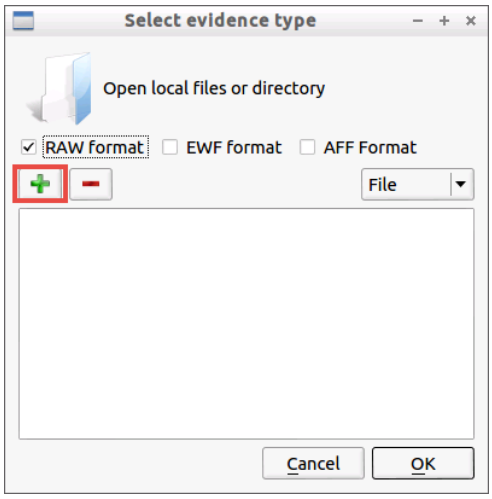


3. Once the application opens, click on **File** and select **Open Evidence**.

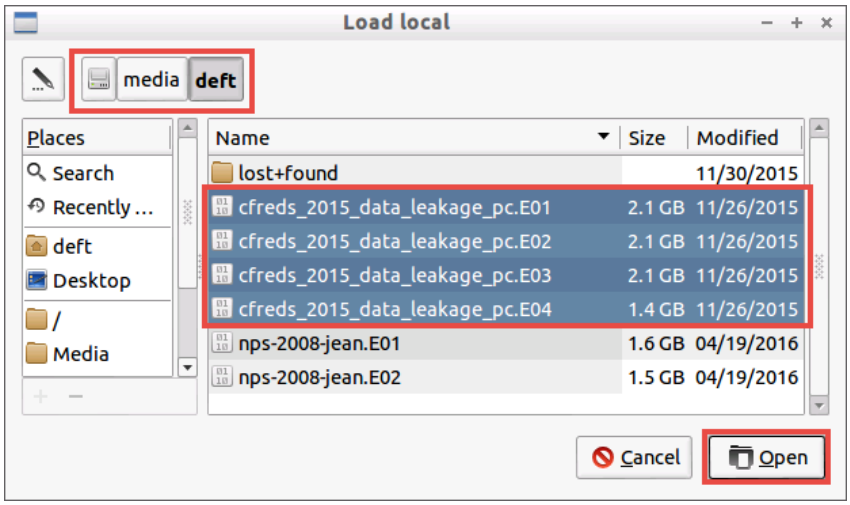


 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

4. In the *Select evidence type* dialog window, click on the **green plus** icon to open a local file.



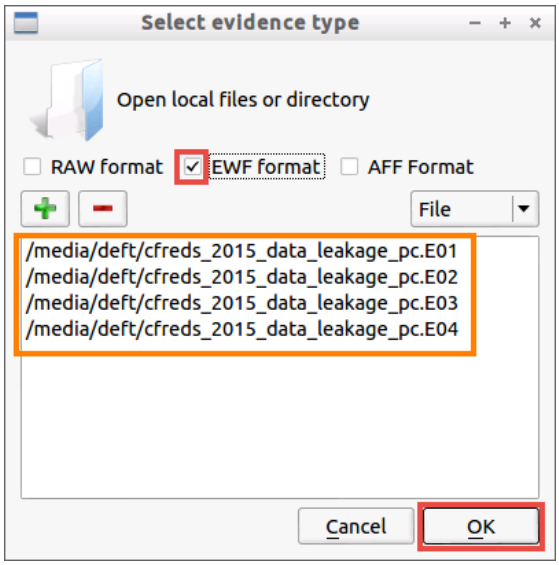
5. In the *Load local* window, navigate to the **/media/deft/** directory and select all the **cfred** files (***E01 – E04***). Click **Open**.



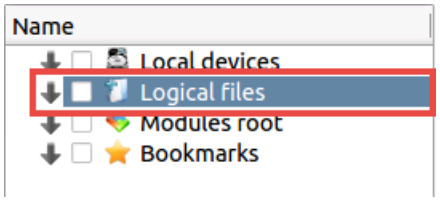
To select multiple files, select the first file, in this case **E01** and hold the **Shift** key while at the same time clicking on the last file, **E04**.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

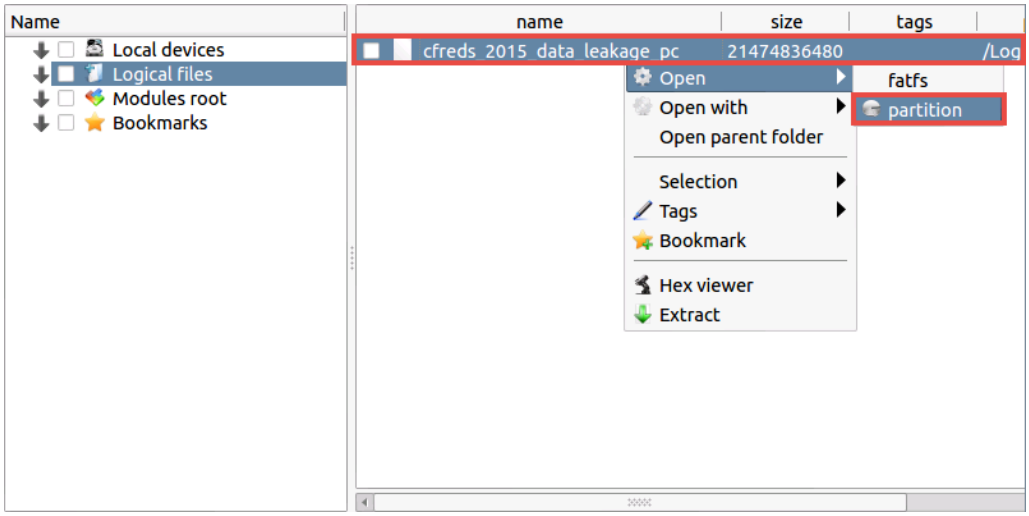
6. In the *Select evidence type* dialog window, verify that all four *cfred* files appear in the list and select **EWF format**. Click **OK**.



7. Select **Logical files** from the left pane.

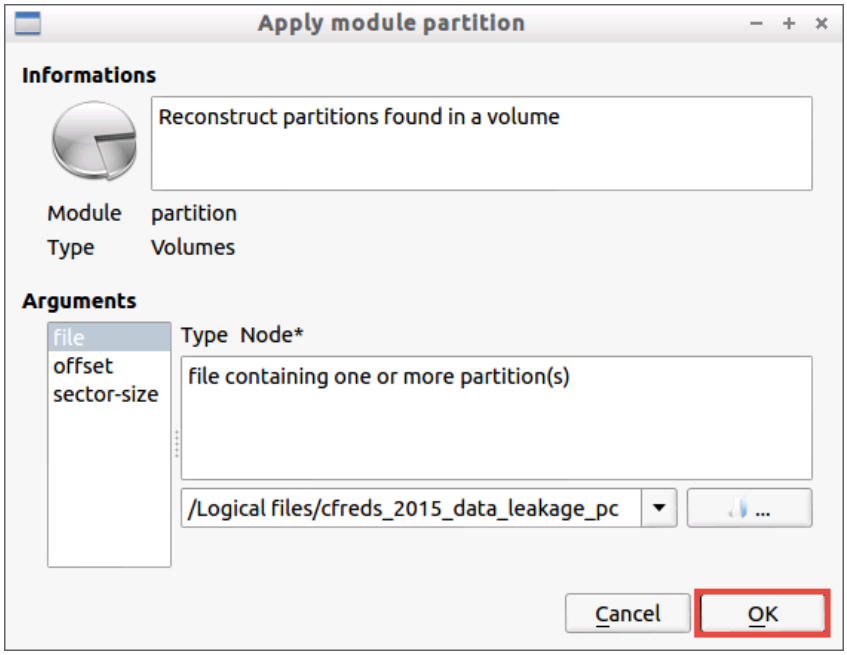


8. Notice the *cfreds_2015_data_leakage_pc* entry appears in the middle pane. Right click on the **cfreds** entry and select **Open > partition**.

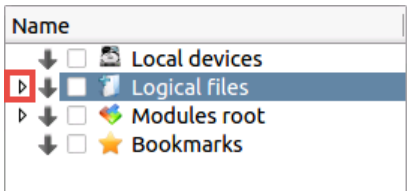


 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

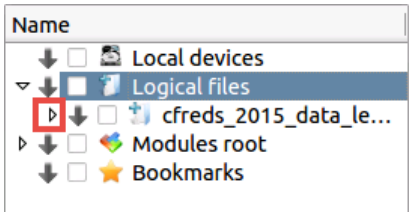
9. On the *Apply module partition* dialog window, click **OK**.



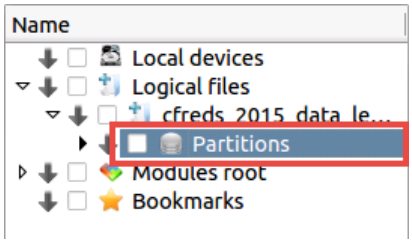
10. In the left pane, click on the **arrow** next to *Logical files* to expand the list.



11. Expand the list for the *cfreds_2015_data_leakage_pc* entry by clicking on the **arrow**.

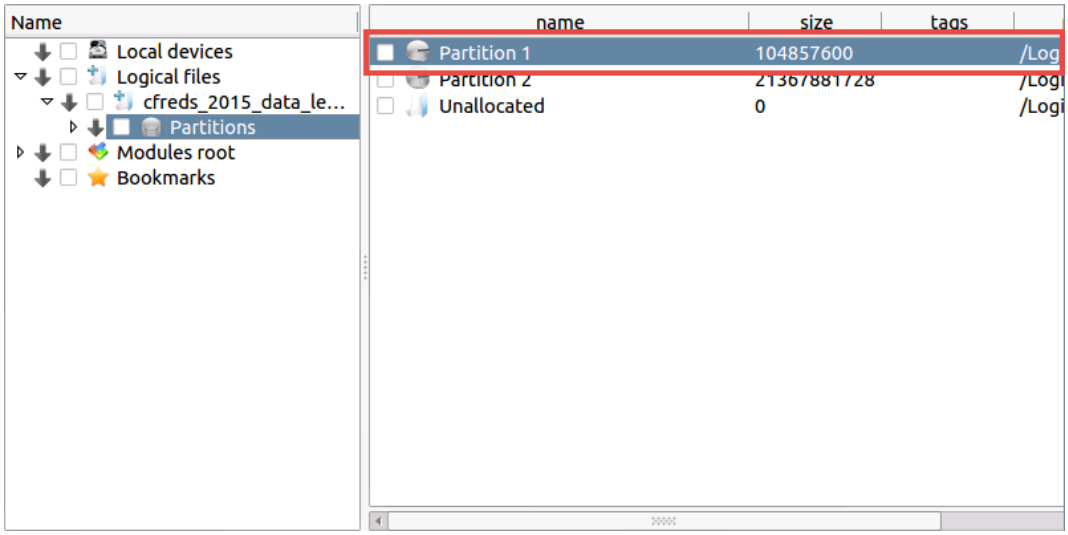


12. Select the **Partitions** entry.

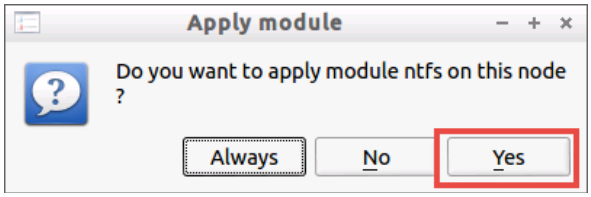


 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

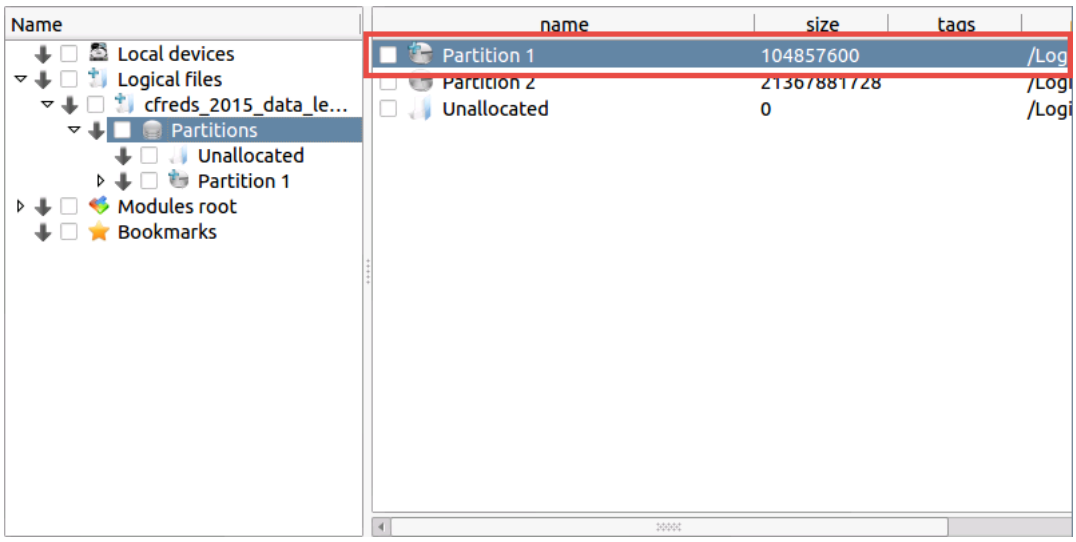
13. In the middle pane, notice two partitions appear. Double-click on **Partition 1**.



14. In the *Apply module* dialog window, click **Yes** to apply one of the built-in modules in DFF to translate the data.



15. In the middle pane, double-click on **Partition 1** once more.

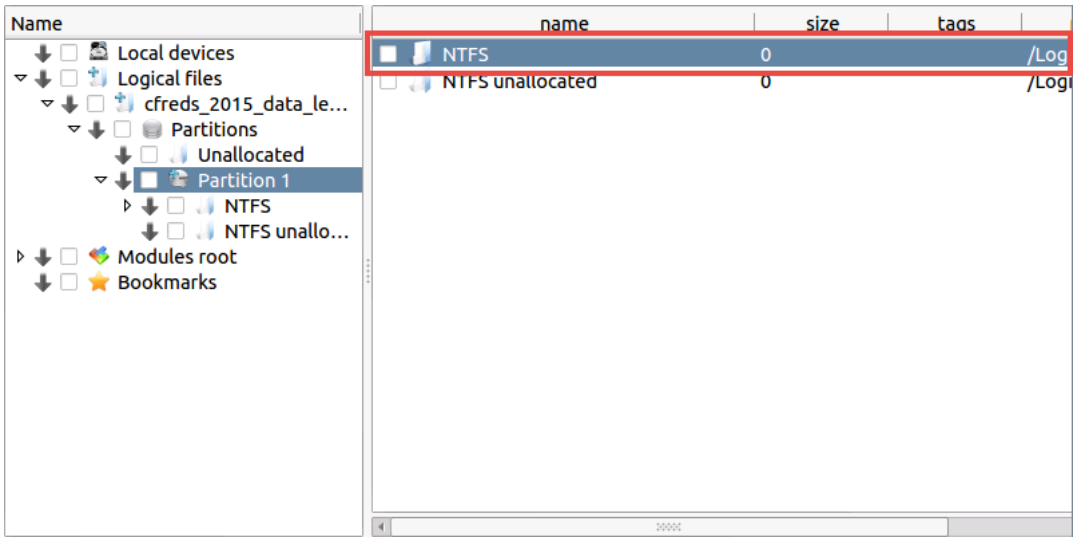


16. Leave the *DFF* application open to continue on with the next task.

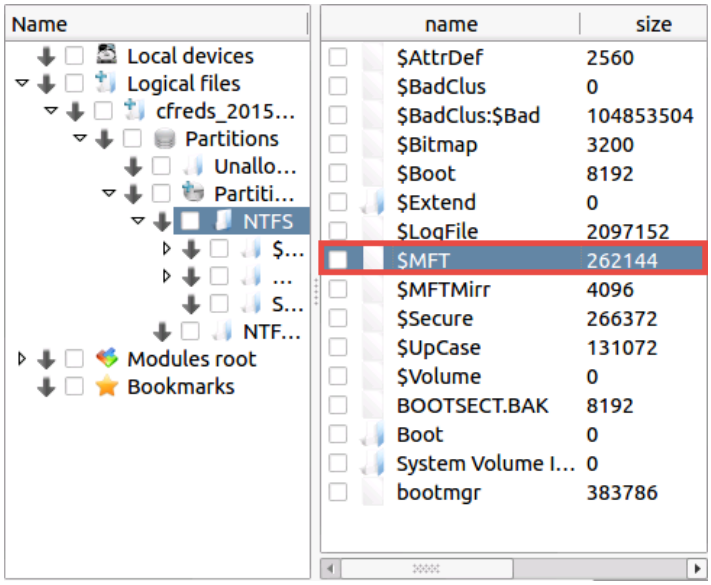
 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

2 Analyzing Partition Data with DFF

1. In the middle pane, double-click on **NTFS**.

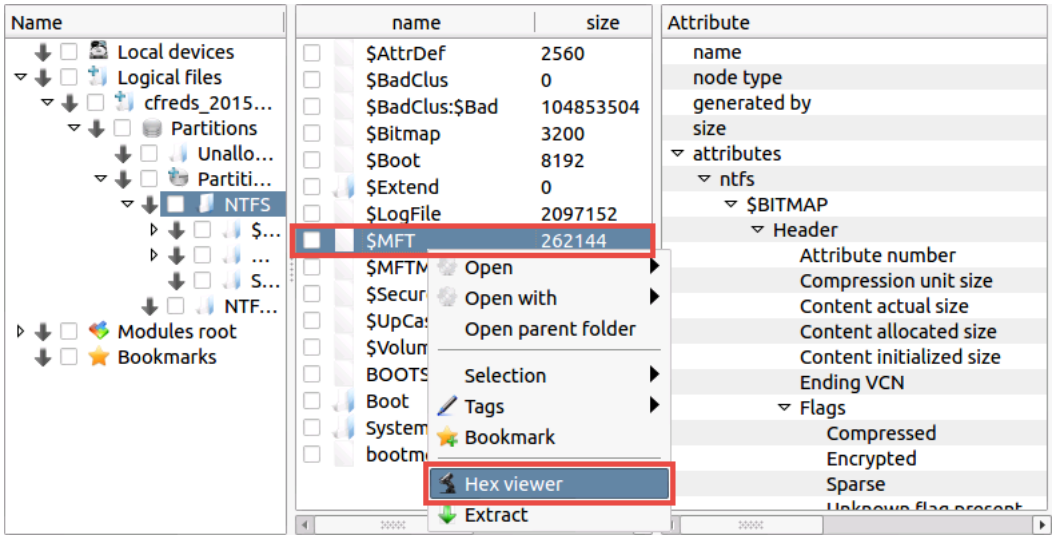


2. Notice the data available from the partition. In the middle pane, select the **$MFT** file.



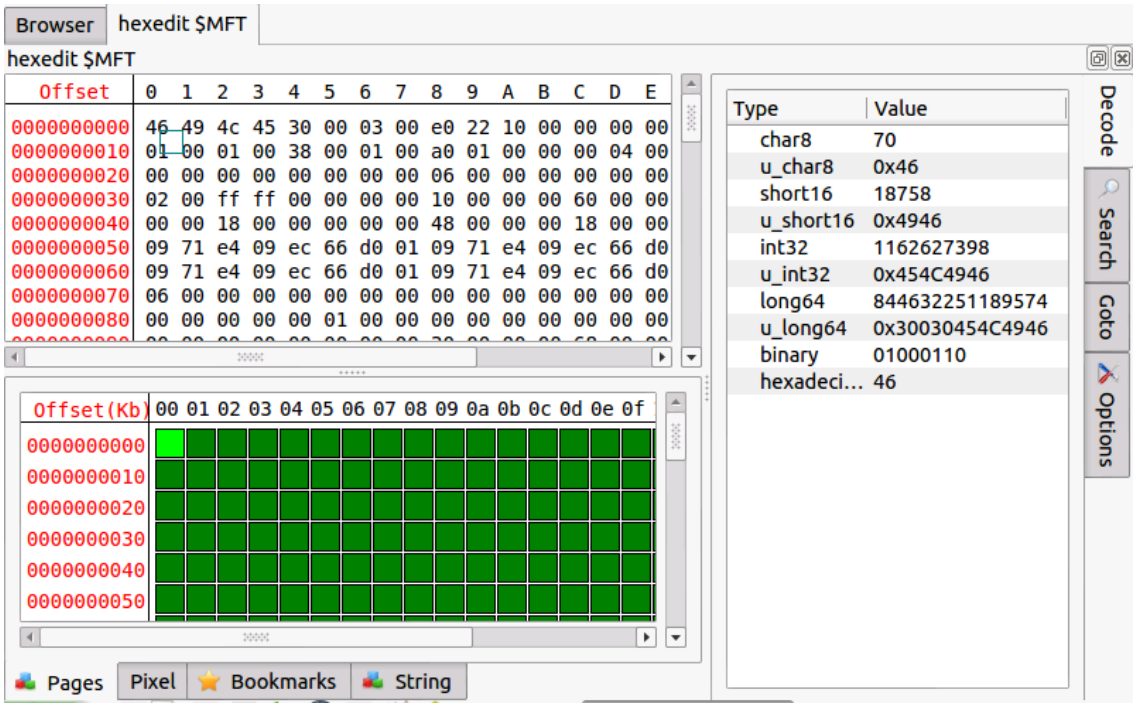
 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

3. Once selected, notice to the right, an *Attribute* pane is made available. The contents of the file and the values for each field can be seen here. Right click on the **$MFT** file and select **Hex viewer**.



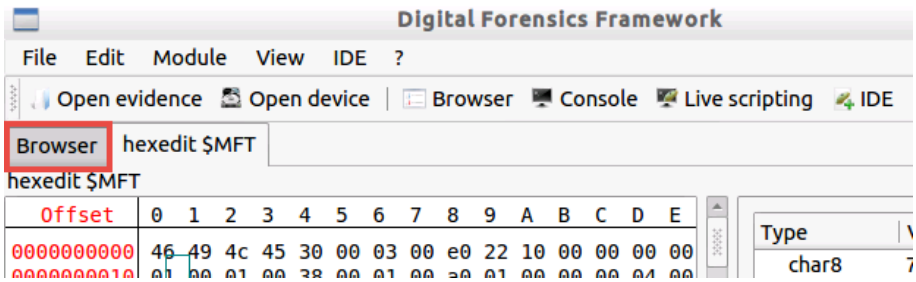
If the *Attribute* pane is not visible, maximize the *DFF* application window and adjust the pane sizes by moving the dividers between the different panes.

4. Notice a new *hexedit $MFT* tab appears. Briefly analyze the hex information for the *$MFT* file.

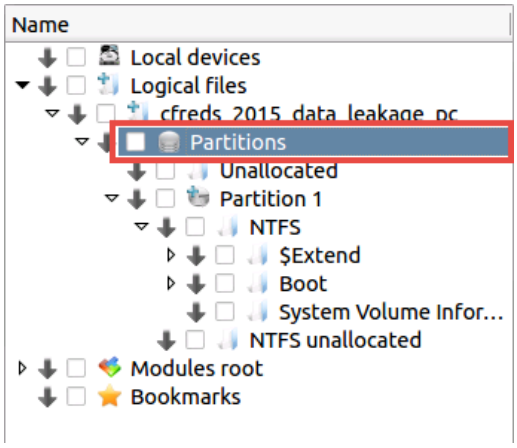


 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

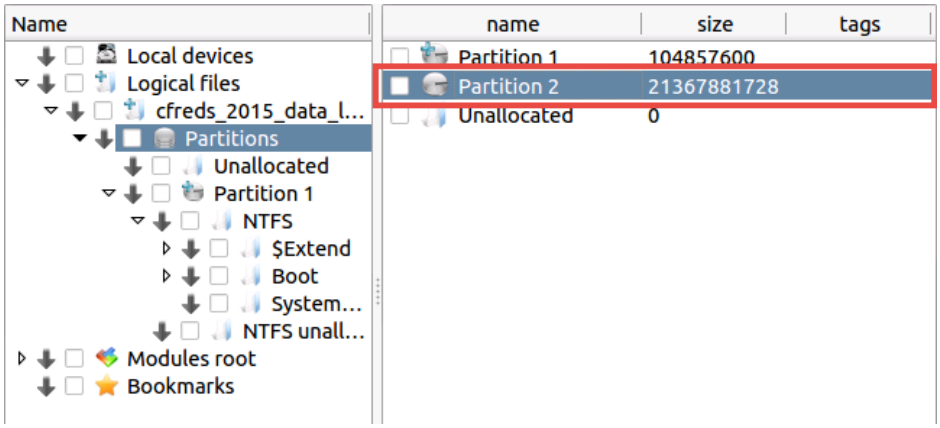
5. Navigate to the previous tab by clicking on the **Browser** tab.



6. In the left pane, click on **Partitions**.



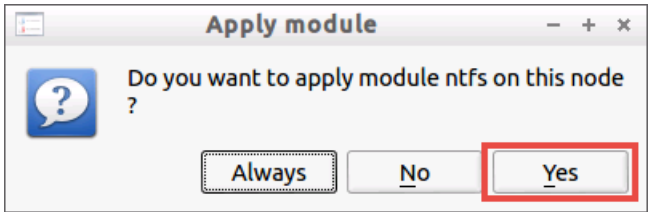
7. In the middle pane, double-click on **Partition 2**.



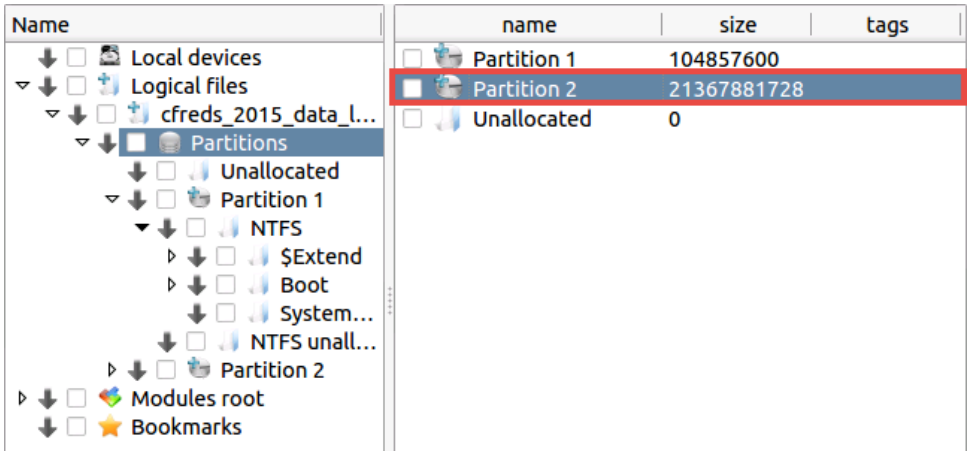
If opening *Partition 2* results in an error, try once more to open it. Wait for a minute for the program to open the partition.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

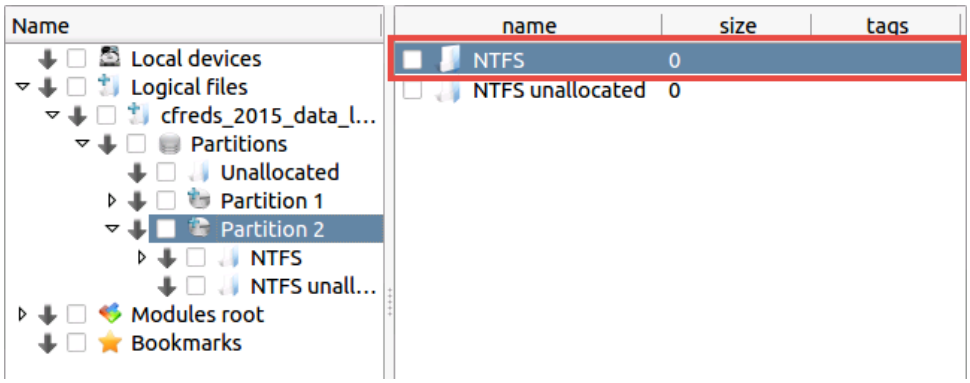
8. When prompted to apply the module, click **Yes** to continue.



9. In the middle pane, double-click on **Partition 2** once more.

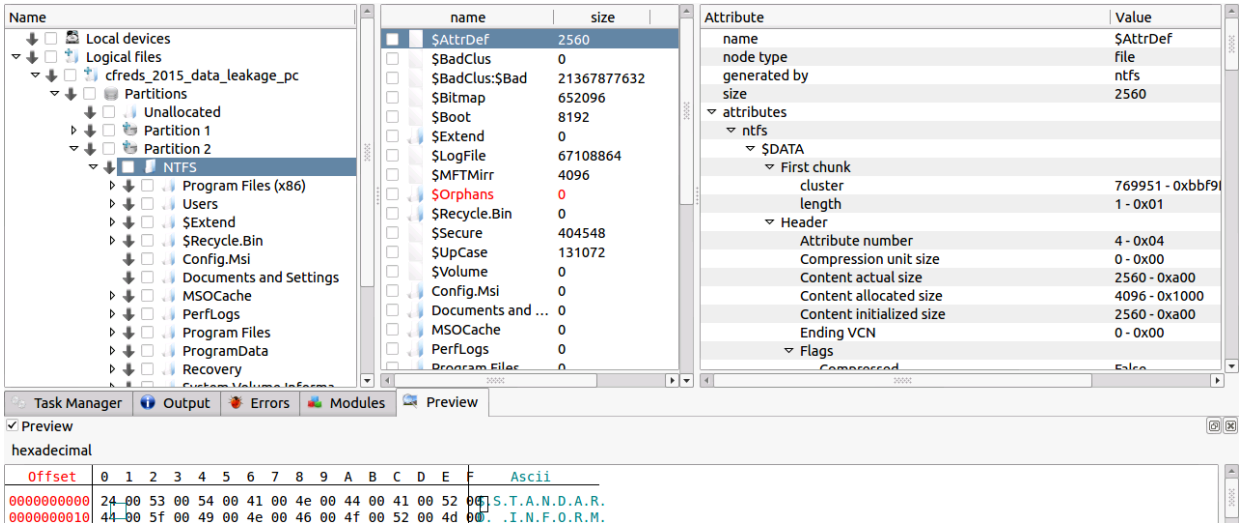


10. In the middle pane, double-click on **NTFS**.



 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com

11. Notice all the available files that can be forensically examined. Using DFF, a forensic examination can be accomplished, just like using a commercial tool.



12. Close all **PC Viewers** and end the reservation to complete the lab.

 Copyright © 2016 Network Development Group, Inc. www.netdevgroup.com