FORENSICS V2 LAB SERIES

Lab 17: Log Capturing and Interpretation

Document Version: 2021-01-11

Contents

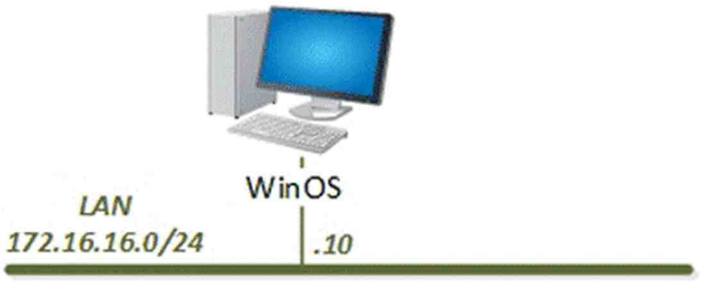
Introduction

All digital devices store logs that are mainly used to help troubleshoot and determine what activity occurred at what times. This module will cover two types of file system logs stored on a windows computer.

Objectives

- Learn what are the popular Windows logs
- Learn how to identify the USNJournal
- Learn how to identify the Event Logs
- Learn how to find simple data within these files

Lab Topology



Lab Settings

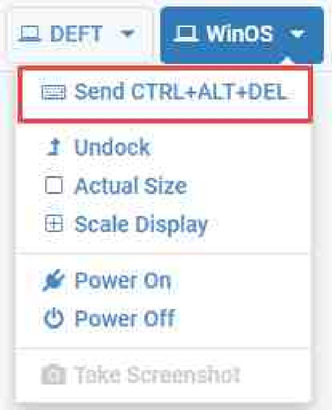
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	IP Address / 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 Identifying the USN Journal and the Windows Event Logs

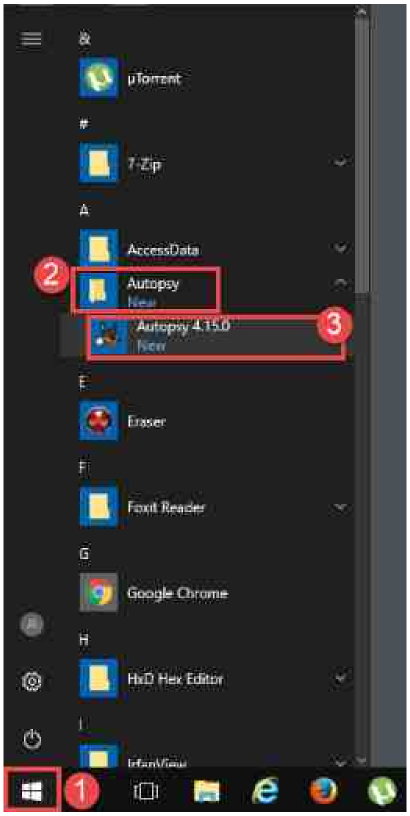
Logs are one of the best tools for troubleshooting and investigating. They provide dates and times of specific events and are extremely useful when added to timelines. In this lab, we will go over 2 of the most verbose types of logs that are stored on Windows systems, the USN Journal and the Event Logs.

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.

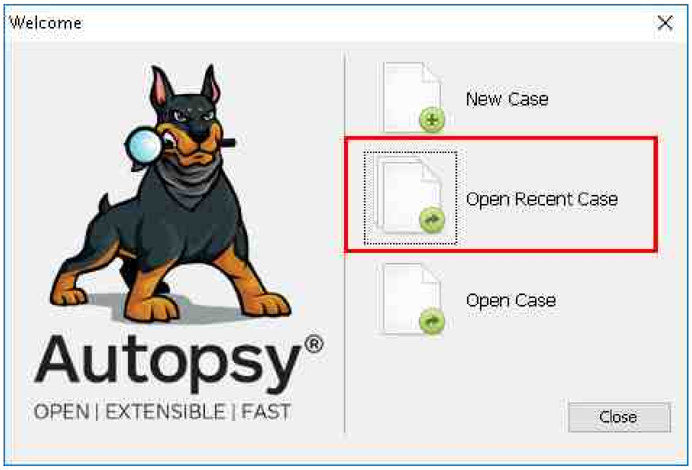


   b. Log in as `Administrator` using the password: `Train1ng$`

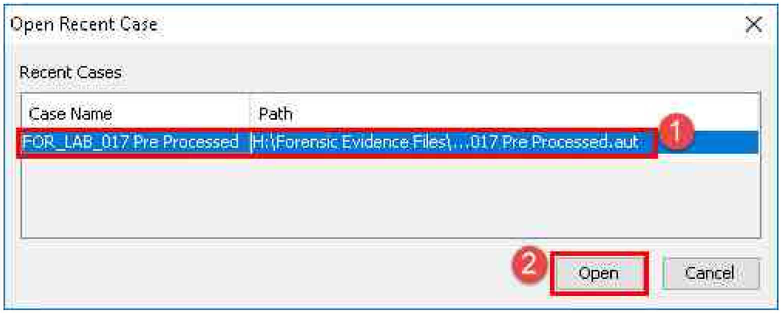
2. Once you are logged into the VM, launch the Autopsy program from the windows menu by navigating to Start Menu > Autopsy > Autopsy 4.15.0. Alternatively, you can open Autopsy from the Desktop by clicking the icon called Autopsy 4.15.0:



3. The Welcome screen will appear; click Open Recent Case as highlighted below. This will open the Open Recent Case window.

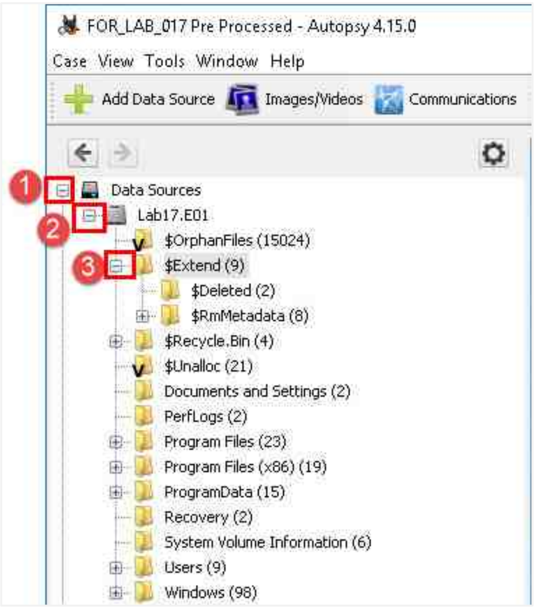


4. In the Open Recent Case window, select the case name FOR_LAB_017 Pre Processed, as highlighted in item 1 below. This case was processed with the USN Parser and ParseEvtx ingest modules. Next, click Open as highlighted in item 2 below.

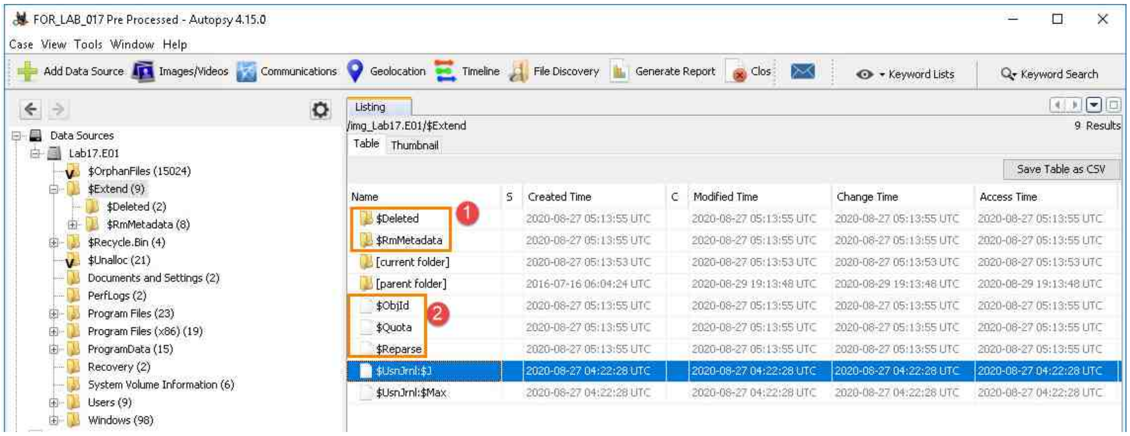


Case Name	Path
FOR_LAB_017 Pre Processed	H:\Forensic Evidence Files\...017 Pre Processed.aut

5. The pre-processed case will open, and you will be taken to the main GUI of Autopsy. Since the USN Journal and Event logs have been parsed, we will not have to manually review them. Still, we should know where to find them in the filesystem, so we know where the data is being pulled from. You should be at the Autopsy main window by now. Let us start browsing to the USN Journal first. The USN Journal is also known as the changelog, and it stores records such as creations, deletions, encryption, and more. This is a feature of NTFS Files Systems, which means it can be found on drives that do not have operating systems on it. It is always stored in the root directory of the disk in a folder hidden system file called $Extend\$USNJrnl.
6. Begin by clicking the + sign beside Data Sources to view the file structure on the drive, as seen in item 1 below. Next, expand the FEF called Lab17.E01 by clicking the + sign beside it, as seen in item 2 below. You will see the folders and files that make up the operating system. As we mentioned, the USN Journal is in the $Extend folder. Click the + sign beside it to expand it, as seen in item 3 below.



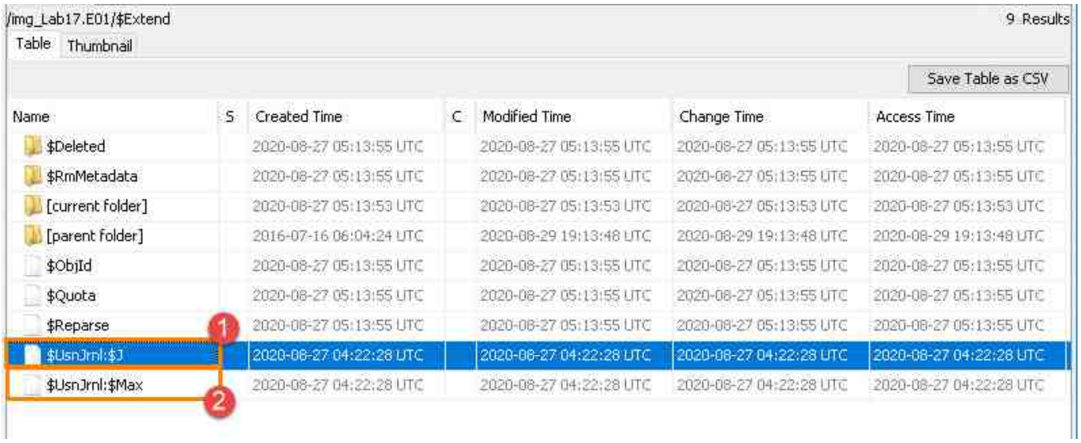
7. You will see seven files and folders that all start with $; these files are all specific to the NTFS file system and store different types of data. There are 2 files here that begin with $UsnJrnl, as seen in items 1 and 2 below. There is really only one file called $UsnJrnl with 2 files that are stored within the alternate data stream (ADS) of this file.



/img_Lab17.E01/$Extend — 9 Results

Name	S	Created Time	C	Modified Time	Change Time	Access Time
$Deleted		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$RmMetadata		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
[current folder]		2020-08-27 05:13:53 UTC		2020-08-27 05:13:53 UTC	2020-08-27 05:13:53 UTC	2020-08-27 05:13:53 UTC
[parent folder]		2016-07-16 06:04:24 UTC		2020-08-29 19:13:48 UTC	2020-08-29 19:13:48 UTC	2020-08-29 19:13:48 UTC
$ObjId		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$Quota		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$Reparse		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$UsnJrnl:$J		2020-08-27 04:22:28 UTC		2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC
$UsnJrnl:$Max		2020-08-27 04:22:28 UTC		2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC

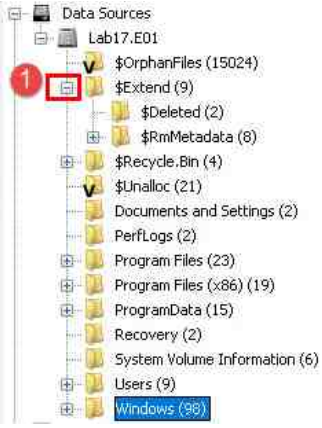
8. These are the files called $J and $Max seen after the colon. The file called $Max contains data about the maximum size of the change journal, among other things. The file called $J is the one that contains all the changes. You can tell this by looking at the size of this file and compare it to the size of the $Max file. Scroll to the right using the in items 1 and 2 below. Since the log is not stored in raw text, we need to parse the data using a tool that can interpret it. Luckily, we ran an ingest module that does just that.



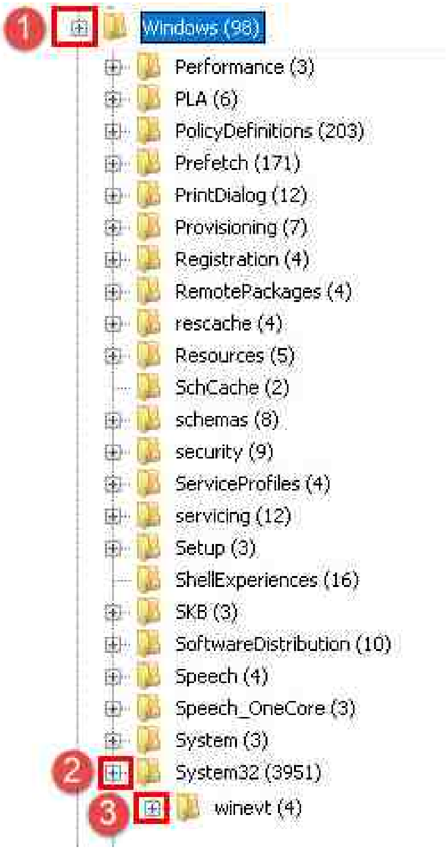
/img_Lab17.E01/$Extend — 9 Results

Name	S	Created Time	C	Modified Time	Change Time	Access Time
$Deleted		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$RmMetadata		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
[current folder]		2020-08-27 05:13:53 UTC		2020-08-27 05:13:53 UTC	2020-08-27 05:13:53 UTC	2020-08-27 05:13:53 UTC
[parent folder]		2016-07-16 06:04:24 UTC		2020-08-29 19:13:48 UTC	2020-08-29 19:13:48 UTC	2020-08-29 19:13:48 UTC
$ObjId		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$Quota		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$Reparse		2020-08-27 05:13:55 UTC		2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC	2020-08-27 05:13:55 UTC
$UsnJrnl:$J		2020-08-27 04:22:28 UTC		2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC
$UsnJrnl:$Max		2020-08-27 04:22:28 UTC		2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC	2020-08-27 04:22:28 UTC

9. Let us find the Windows Event logs now; to begin, click the - sign beside $Extend, seen in item 1 below, to contract the folder tree and make it easier to navigate.

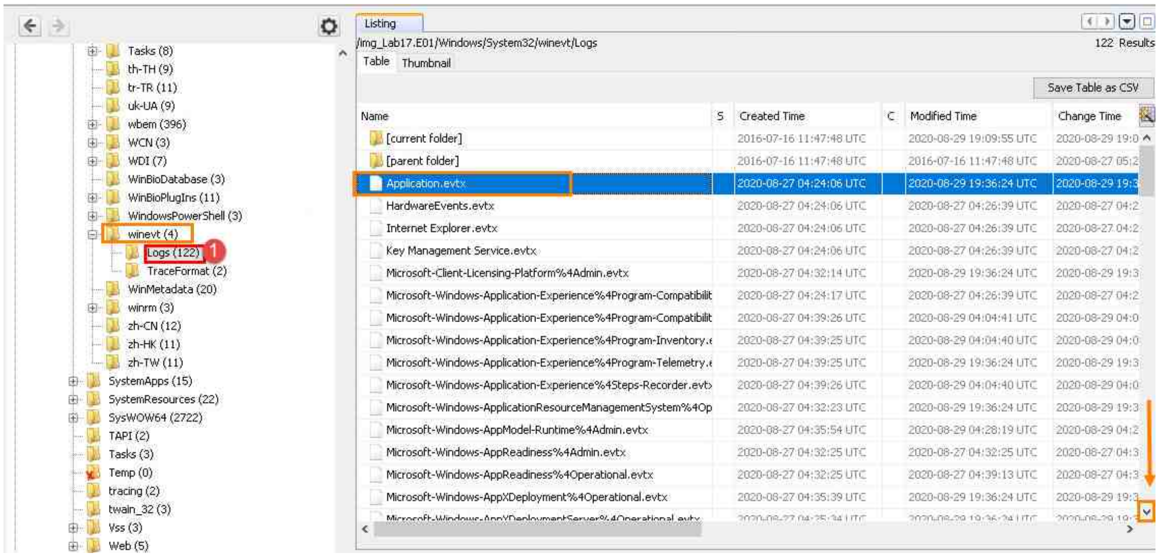


10. Next, click the + sign beside the following folders to get to the Windows event logs Windows > System32 > WinEVT, as seen in items 2, 3, and 4 below.



Autopsy displays a number in brackets to denote the number of files within a tree pane entry.

11. You will see 2 folders: Logs and TraceFormat. We are interested in the folder called Logs, so click it as seen in item 1 below. Now turn your attention to the File List pane where you will see the different event logs listed. The three main event logs we mentioned earlier are Application.evtx, System.evtx, and Security.evtx. Scroll down the File List pane to see if you can identify them all. Even though these are the popular ones, different investigations may lead you to access additional event logs. Also, note that in older versions of Microsoft Windows like XP, the path is Windows > System32 > config, and the files have the extension .evt. Now let us look at the data that we parsed earlier.



Tasks (8)
th-TH (9)
tr-TR (11)
uk-UA (9)
wbem (396)
WCN (3)
WDI (7)
WinBioDatabase (3)
WinBioPlugIns (11)
WindowsPowerShell (3)
winevt (4)
Logs (122)
TraceFormat (2)
WinMetadata (20)
winrm (3)
zh-CN (12)
zh-HK (11)
zh-TW (11)
SystemApps (15)
SystemResources (22)
SysWOW64 (2722)
TAPI (2)
Tasks (3)
Temp (0)
tracing (2)
twain_32 (3)
Vss (3)
Web (5)

/img_Lab17.E01/Windows/System32/winevt/Logs

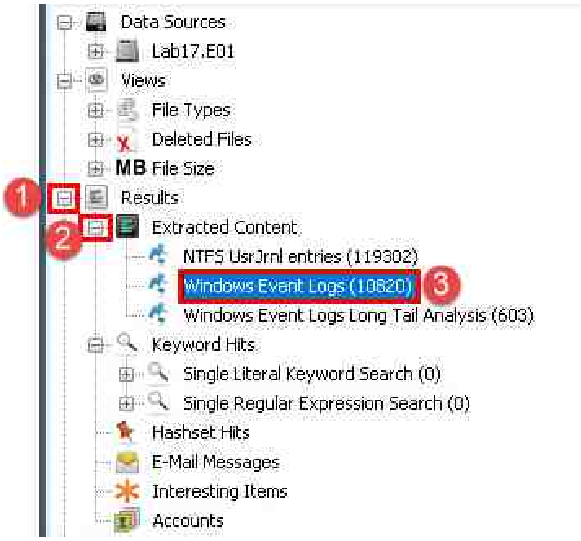
122 Results

Name	S	Created Time	C	Modified Time	Change Time
[current folder]		2016-07-16 11:47:48 UTC		2020-08-29 19:09:55 UTC	2020-08-29 19:0
[parent folder]		2016-07-16 11:47:48 UTC		2016-07-16 11:47:48 UTC	2020-08-27 05:2
Application.evtx		2020-08-27 04:24:06 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3
HardwareEvents.evtx		2020-08-27 04:24:06 UTC		2020-08-27 04:26:39 UTC	2020-08-27 04:2
Internet Explorer.evtx		2020-08-27 04:24:06 UTC		2020-08-27 04:26:39 UTC	2020-08-27 04:2
Key Management Service.evtx		2020-08-27 04:24:06 UTC		2020-08-27 04:26:39 UTC	2020-08-27 04:2
Microsoft-Client-Licensing-Platform%4Admin.evtx		2020-08-27 04:32:14 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3
Microsoft-Windows-Application-Experience%4Program-Compatibilit		2020-08-27 04:24:17 UTC		2020-08-27 04:26:39 UTC	2020-08-27 04:2
Microsoft-Windows-Application-Experience%4Program-Compatibilit		2020-08-27 04:39:26 UTC		2020-08-29 04:04:41 UTC	2020-08-29 04:0
Microsoft-Windows-Application-Experience%4Program-Inventory.e		2020-08-27 04:39:25 UTC		2020-08-29 04:04:40 UTC	2020-08-29 04:0
Microsoft-Windows-Application-Experience%4Program-Telemetry.e		2020-08-27 04:39:25 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3
Microsoft-Windows-Application-Experience%4Steps-Recorder.evtx		2020-08-27 04:39:26 UTC		2020-08-29 04:04:40 UTC	2020-08-29 04:0
Microsoft-Windows-ApplicationResourceManagementSystem%4Op		2020-08-27 04:32:23 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3
Microsoft-Windows-AppModel-Runtime%4Admin.evtx		2020-08-27 04:35:54 UTC		2020-08-29 04:28:19 UTC	2020-08-29 04:2
Microsoft-Windows-AppReadiness%4Admin.evtx		2020-08-27 04:32:25 UTC		2020-08-27 04:32:25 UTC	2020-08-27 04:3
Microsoft-Windows-AppReadiness%4Operational.evtx		2020-08-27 04:32:25 UTC		2020-08-27 04:39:13 UTC	2020-08-27 04:3
Microsoft-Windows-AppXDeployment%4Operational.evtx		2020-08-27 04:35:39 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3
Microsoft-Windows-AppXDeploymentServer%4Operational.evtx		2020-08-27 04:35:34 UTC		2020-08-29 19:36:24 UTC	2020-08-29 19:3

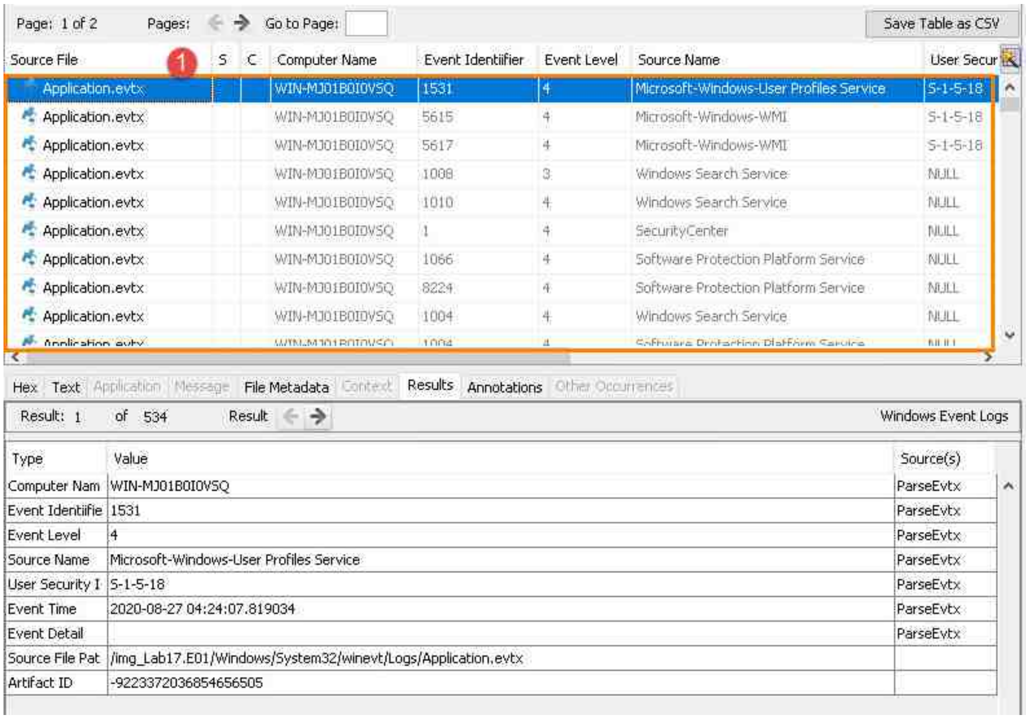
2 Reviewing Event Log Data

The event logs store detailed records of operating system events, and it can answer a lot of different questions. Details are available for events like a successful logoff or logon, an incorrect login attempt, a remote login, and networking events, to name a few. Each type of event has an Event ID that classifies the type of record. For example, Event ID 8194 is the successful creation of a system restore point. Let us use the parsed data to identify some useful events by searching for their event IDs.

1. To begin, expand the Results and Extracted Content tree items by clicking the plus sign beside them, as seen in items 1 and 2 below. You will see 2 options appear, click Windows Event Logs, as seen in item 3 below.


Data Sources
Lab17.E01
Views
File Types
Deleted Files
MB File Size
1
Results
2
Extracted Content
NTFS UsrJrnl entries (119302)
Windows Event Logs (10820)
3
Windows Event Logs Long Tail Analysis (603)
Keyword Hits
Single Literal Keyword Search (0)
Single Regular Expression Search (0)
Hashset Hits
E-Mail Messages
Interesting Items
Accounts

2. You will see the parsed event logs in the Listing pane, as seen in item 1 below. The table below the following screenshot will provide details about the data in each column.

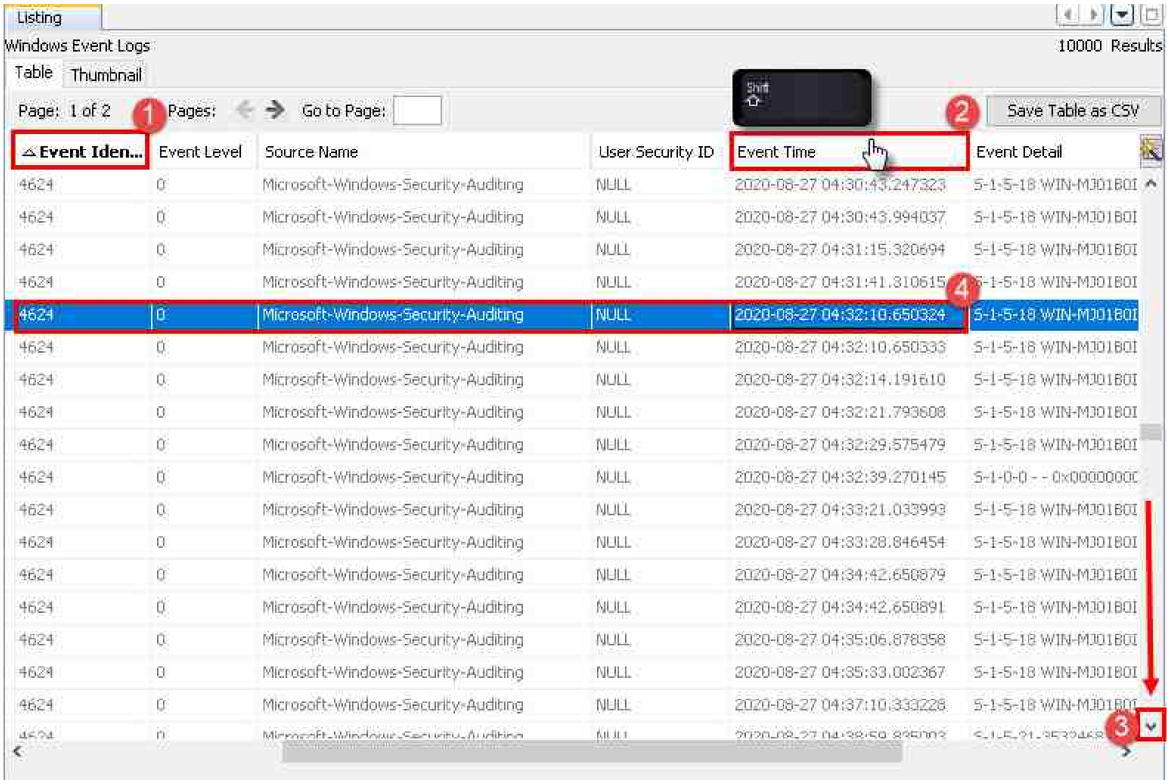


Source File	S	C	Computer Name	Event Identiifier	Event Level	Source Name	User Secur
Application.evtx			WIN-MJ01B0I0VSQ	1531	4	Microsoft-Windows-User Profiles Service	S-1-5-18
Application.evtx			WIN-MJ01B0I0VSQ	5615	4	Microsoft-Windows-WMI	S-1-5-18
Application.evtx			WIN-MJ01B0I0VSQ	5617	4	Microsoft-Windows-WMI	S-1-5-18
Application.evtx			WIN-MJ01B0I0VSQ	1008	3	Windows Search Service	NULL
Application.evtx			WIN-MJ01B0I0VSQ	1010	4	Windows Search Service	NULL
Application.evtx			WIN-MJ01B0I0VSQ	1	4	SecurityCenter	NULL
Application.evtx			WIN-MJ01B0I0VSQ	1066	4	Software Protection Platform Service	NULL
Application.evtx			WIN-MJ01B0I0VSQ	8224	4	Software Protection Platform Service	NULL
Application.evtx			WIN-MJ01B0I0VSQ	1004	4	Windows Search Service	NULL
Application.evtx			WIN-MJ01B0I0VSQ	1004	4	Software Protection Platform Service	NULL

Type	Value	Source(s)
Computer Nam	WIN-MJ01B0I0VSQ	ParseEvtx
Event Identifie	1531	ParseEvtx
Event Level	4	ParseEvtx
Source Name	Microsoft-Windows-User Profiles Service	ParseEvtx
User Security I	S-1-5-18	ParseEvtx
Event Time	2020-08-27 04:24:07.819034	ParseEvtx
Event Detail		ParseEvtx
Source File Pat	/img_Lab17.E01/Windows/System32/winevt/Logs/Application.evtx	
Artifact ID	-9223372036854656505	

Source File	This column provides data about the file that the information in each row was taken from
Computer Name	This refers to the NetBIOS name of the computer that the event is referring to
Event Identifier	This is the Event ID. It is a unique identifier for events
Event Level	Used to determine how severe and event is. There is document about the meaning of each event level
Source Name	The is the name of the Application or service that the data is retrieved from
User Security ID	This is the name of the application or service that created the event
Event Time	The time that the event was generated
Event Detail	The details of the specific event

3. Let us look at some event IDs now. The first one we will check out is the Logon event. This can provide information about which users logged on, when they logged on, and what method they used to log in. Let us sort the events by Event Identifier and then by Event Time so we can find specific events and view them in chronological order. Do this by clicking the title of the column Event Identifier, as seen in item 1 below. Now hold Shift and click the title of the column Event Time, as seen in item 2 below. This will sort by Event ID then time. You can verify that it is sorted if you see the sequential numbers 1 or 2 beside the column names. Now scroll down using the scroll bar or arrow button until you get to Event ID 4624 as seen in item 3 below. You will see a lot of these events, and most of them are system user accounts doing things in the background. Let us scroll to the one that has the timestamp 2020-08-27 04:32:10.650324 and click on it as seen in item 4 below. Note that the associated event ID is 4624, which refers to logons.



Windows Event Logs

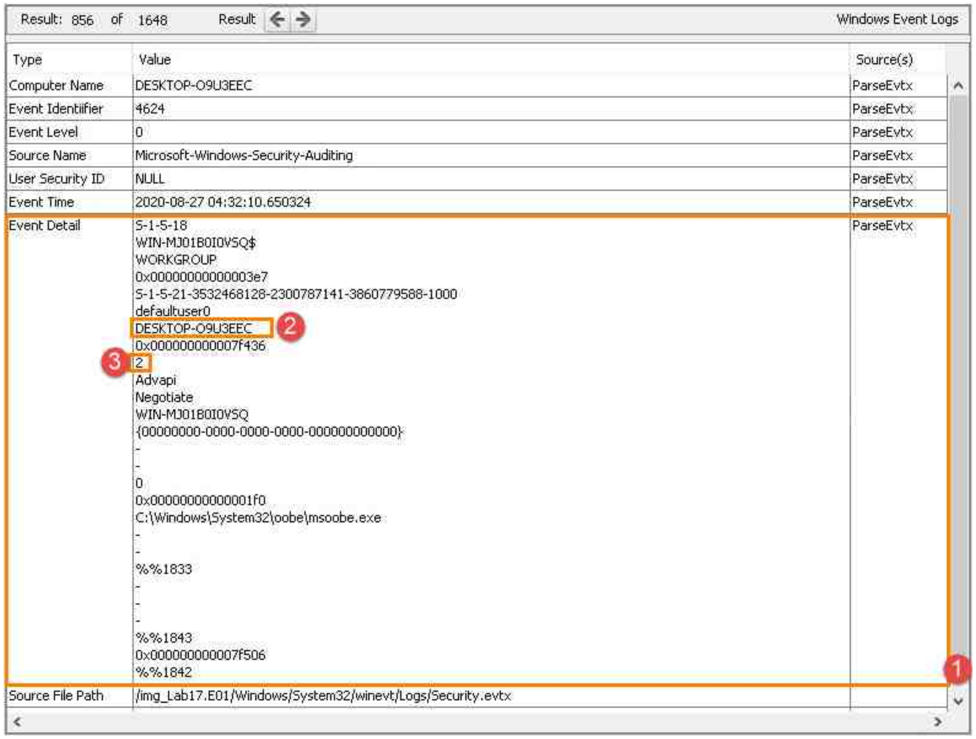
10000 Results

Page: 1 of 2 Pages: Go to Page:

△ Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Detail
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:30:43.247323	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:30:43.994037	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:31:15.320694	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:31:41.310615	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:10.650324	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:10.650333	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:14.191610	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:21.793608	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:29.575479	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:39.270145	S-1-0-0 - - 0x0000000C
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:33:21.033993	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:33:28.846454	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:34:42.650879	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:34:42.650891	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:35:06.878358	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:35:33.002367	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:37:10.333228	S-1-5-18 WIN-MJ01B0I
4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:38:59.835003	S-1-5-21-2532468

Try clicking in the Event Identifier column and typing `4624`. This is a cool feature within Autopsy that allows examiner to quickly locate specific data sets within the table.

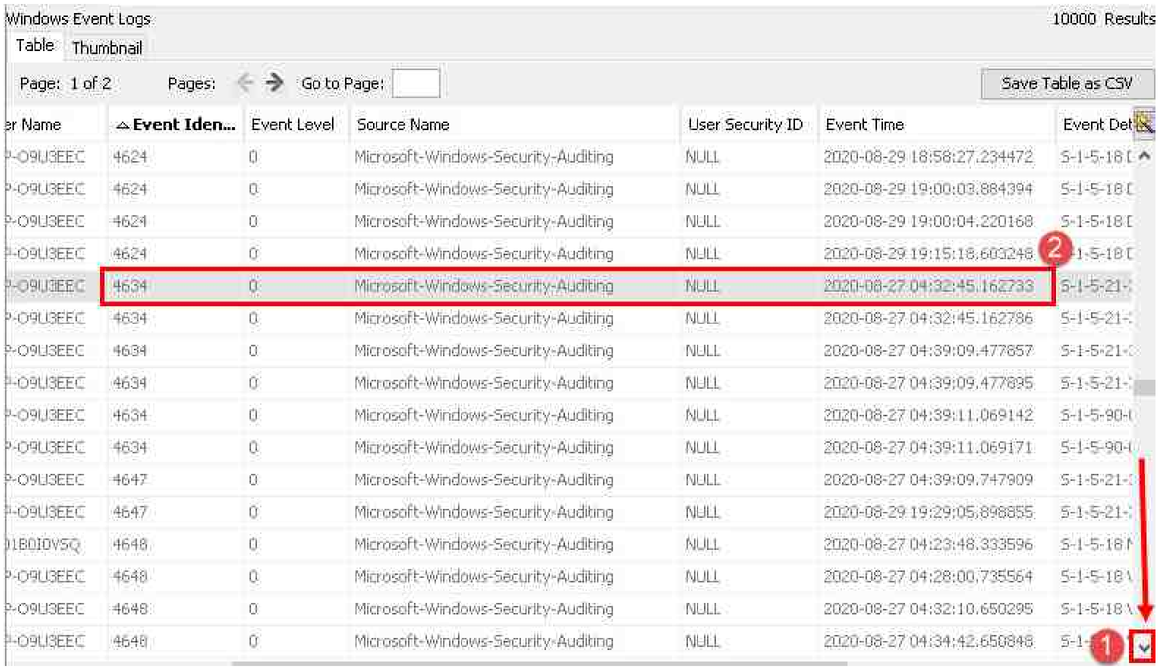
4. The details of the event will populate the View pane at the bottom-right of the window, as seen in item 1. We are interested in the Event Detail row so scroll down to it. The details list the name of the computer that was used to log in, seen in item 2 below. It also lists the username of the last user and the computer name of the destination. The value 2 seen in item 3 below is the logon type. This logon type indicates that the user logged on via a network connection.



Result: 856 of 1648 Result ← → Windows Event Logs

Type	Value	Source(s)
Computer Name	DESKTOP-O9U3EEC	ParseEvtx
Event Identiifier	4624	ParseEvtx
Event Level	0	ParseEvtx
Source Name	Microsoft-Windows-Security-Auditing	ParseEvtx
User Security ID	NULL	ParseEvtx
Event Time	2020-08-27 04:32:10.650324	ParseEvtx
Event Detail	S-1-5-18 WIN-MJ01B0I0VSQ$ WORKGROUP 0x00000000000003e7 S-1-5-21-3532468128-2300787141-3860779588-1000 defaultuser0 DESKTOP-O9U3EEC 0x000000000007f436 2 Advapi Negotiate WIN-MJ01B0I0VSQ {00000000-0000-0000-0000-000000000000} - - 0 0x00000000000001f0 C:\Windows\System32\oobe\msoobe.exe - - %%1833 - - - %%1843 0x000000000007f506 %%1842	ParseEvtx
Source File Path	/img_Lab17.E01/Windows/System32/winevt/Logs/Security.evtx	

5. Now let us see if we can find a logoff date for this logon. Use the scroll bar or arrow button to scroll to Event ID 4634, as seen in item 1 below. As you can see, there are a lot less logoffs than logons. Let us scroll to the one that has the timestamp 2020-08-27 04:32:45.162733 and click on it as seen in item 2 below. Note that the associated event ID is 4634, which refers to logoffs.

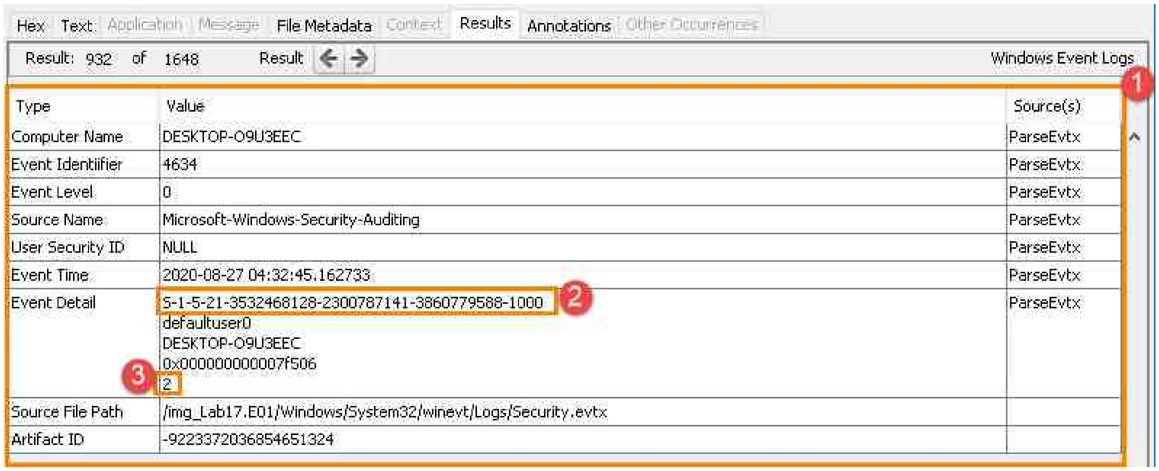


Windows Event Logs — 10000 Results

Page: 1 of 2 Pages: Go to Page:

er Name	Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Det
P-O9U3EEC	4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-29 18:58:27.234472	S-1-5-18
P-O9U3EEC	4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-29 19:00:03.884394	S-1-5-18
P-O9U3EEC	4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-29 19:00:04.220168	S-1-5-18
P-O9U3EEC	4624	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-29 19:15:18.603248	1-5-18
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:45.162733	S-1-5-21-
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:45.162786	S-1-5-21-
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:09.477857	S-1-5-21-
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:09.477895	S-1-5-21-
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:11.069142	S-1-5-90-
P-O9U3EEC	4634	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:11.069171	S-1-5-90-
P-O9U3EEC	4647	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:09.747909	S-1-5-21-
P-O9U3EEC	4647	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-29 19:29:05.898855	S-1-5-21-
1B0IOVSQ	4648	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:48.333596	S-1-5-18
P-O9U3EEC	4648	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:28:00.735564	S-1-5-18
P-O9U3EEC	4648	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:10.650295	S-1-5-18
P-O9U3EEC	4648	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:34:42.650848	S-1-

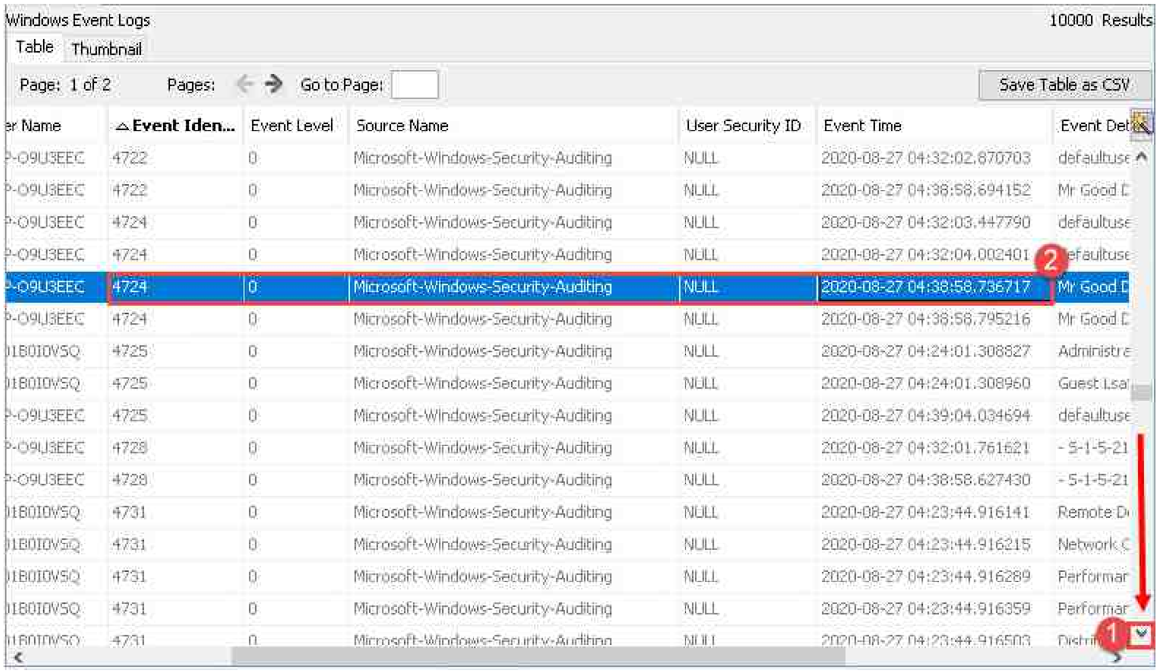
6. The details of the event will populate the View pane at the bottom-right of the window, as seen in item 1. We are interested in the Event Detail row so scroll down to it. The details list the SID, username, and the name of the computer that was used to log in, as seen in item 2 below. The value 2 seen in item 3 below is the logon type. This logon type indicates that the user logged on via a network connection. Based on the time between the 2 events, it is likely that the login and logout were automated, possibly because of the initial Windows setup.



Result: 932 of 1648 — Windows Event Logs

Type	Value	Source(s)
Computer Name	DESKTOP-O9U3EEC	ParseEvtx
Event Identiifier	4634	ParseEvtx
Event Level	0	ParseEvtx
Source Name	Microsoft-Windows-Security-Auditing	ParseEvtx
User Security ID	NULL	ParseEvtx
Event Time	2020-08-27 04:32:45.162733	ParseEvtx
Event Detail	S-1-5-21-3532468128-2300787141-3860779588-1000 defaultuser0 DESKTOP-O9U3EEC 0x000000000007f506 2	ParseEvtx
Source File Path	/img_Lab17.E01/Windows/System32/winevt/Logs/Security.evtx	
Artifact ID	-9223372036854651324	

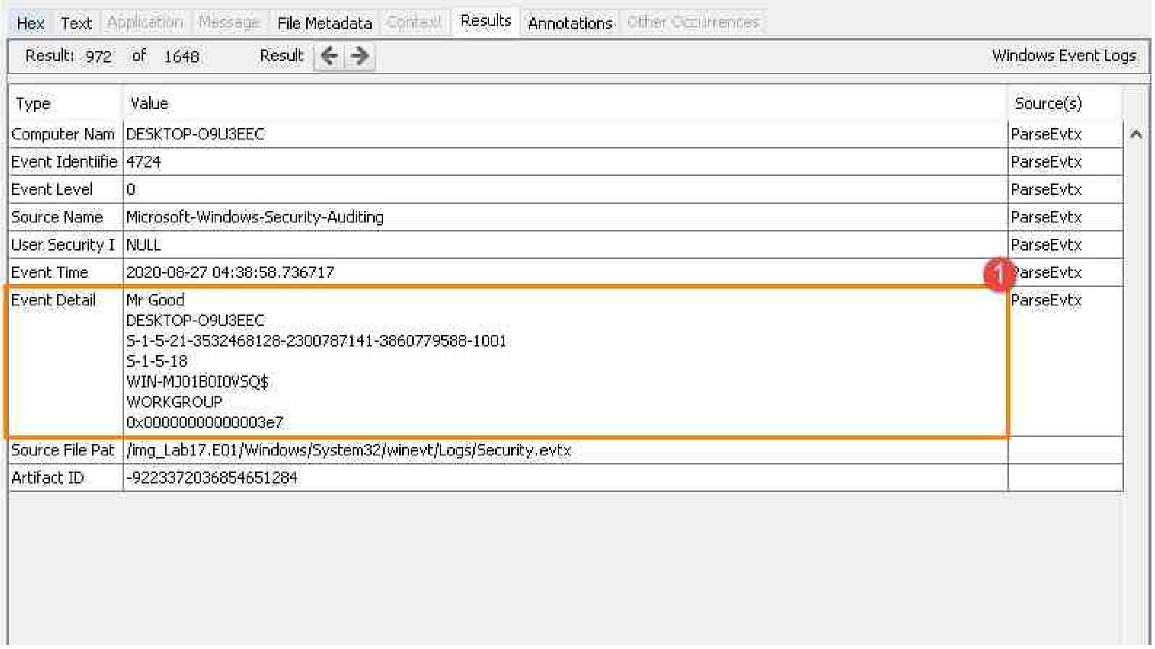
7. Next, let us look at password resets. The Event ID for password reset attempts is 4724. Let us use the scroll bar or arrow button to scroll to Event ID 4724, as seen in item 1 below. Next, select the one that has the timestamp 2020-08-27 04:38:58.736717 by clicking it, as seen in item 2 below.



Windows Event Logs 10000 Results

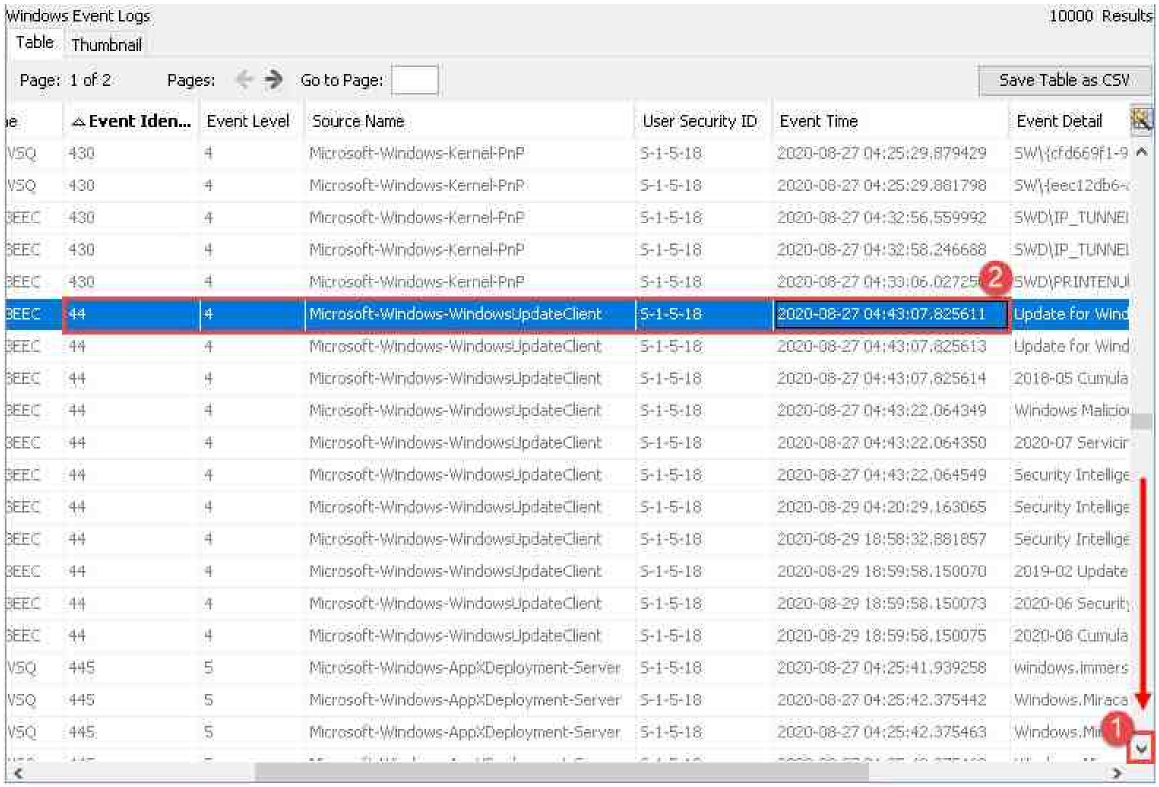
er Name	Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Det
P-O9U3EEC	4722	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:02.870703	defaultuse
P-O9U3EEC	4722	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:38:58.694152	Mr Good D
P-O9U3EEC	4724	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:03.447790	defaultuse
P-O9U3EEC	4724	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:04.002401	efaultuse
P-O9U3EEC	4724	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:38:58.736717	Mr Good D
P-O9U3EEC	4724	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:38:58.795216	Mr Good D
)1B0I0VSQ	4725	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:24:01.308827	Administra
)1B0I0VSQ	4725	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:24:01.308960	Guest Lsa
P-O9U3EEC	4725	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:39:04.034694	defaultuse
P-O9U3EEC	4728	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:32:01.761621	- S-1-5-21
P-O9U3EEC	4728	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:38:58.627430	- S-1-5-21
)1B0I0VSQ	4731	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:44.916141	Remote D
)1B0I0VSQ	4731	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:44.916215	Network C
)1B0I0VSQ	4731	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:44.916289	Performar
)1B0I0VSQ	4731	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:44.916359	Performar
)1B0I0VSQ	4731	0	Microsoft-Windows-Security-Auditing	NULL	2020-08-27 04:23:44.916503	Distri

8. The details in this event are like the logon and logoff events. As seen in item 1 below, this log provides the username of the affected user, their computer name, and the SID.



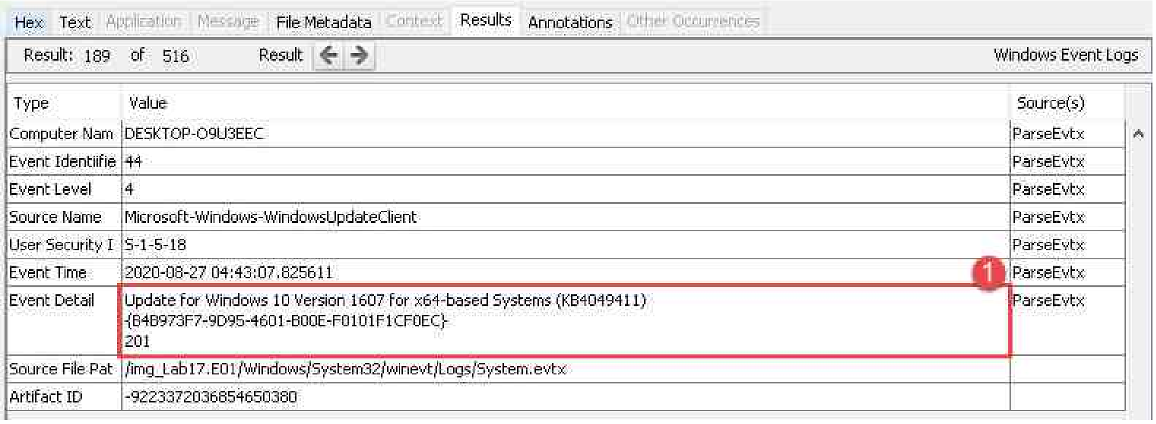
Type	Value	Source(s)
Computer Nam	DESKTOP-O9U3EEC	ParseEvtx
Event Identiifie	4724	ParseEvtx
Event Level	0	ParseEvtx
Source Name	Microsoft-Windows-Security-Auditing	ParseEvtx
User Security I	NULL	ParseEvtx
Event Time	2020-08-27 04:38:58.736717	ParseEvtx
Event Detail	Mr Good DESKTOP-O9U3EEC S-1-5-21-3532468128-2300787141-3860779588-1001 S-1-5-18 WIN-MJ01B0I0VSQ$ WORKGROUP 0x00000000000003e7	ParseEvtx
Source File Pat	/img_Lab17.E01/Windows/System32/winevt/Logs/Security.evtx	
Artifact ID	-9223372036854651284	

9. Finally, let us look at Windows updates. The Event ID for update downloads is 44. Use the scroll bar or arrow button to scroll to Event ID 44, as seen in item 1 below. Next, select the one that has the timestamp 2020-08-27 04:43:07.825611 by clicking it as seen in item 2 below.



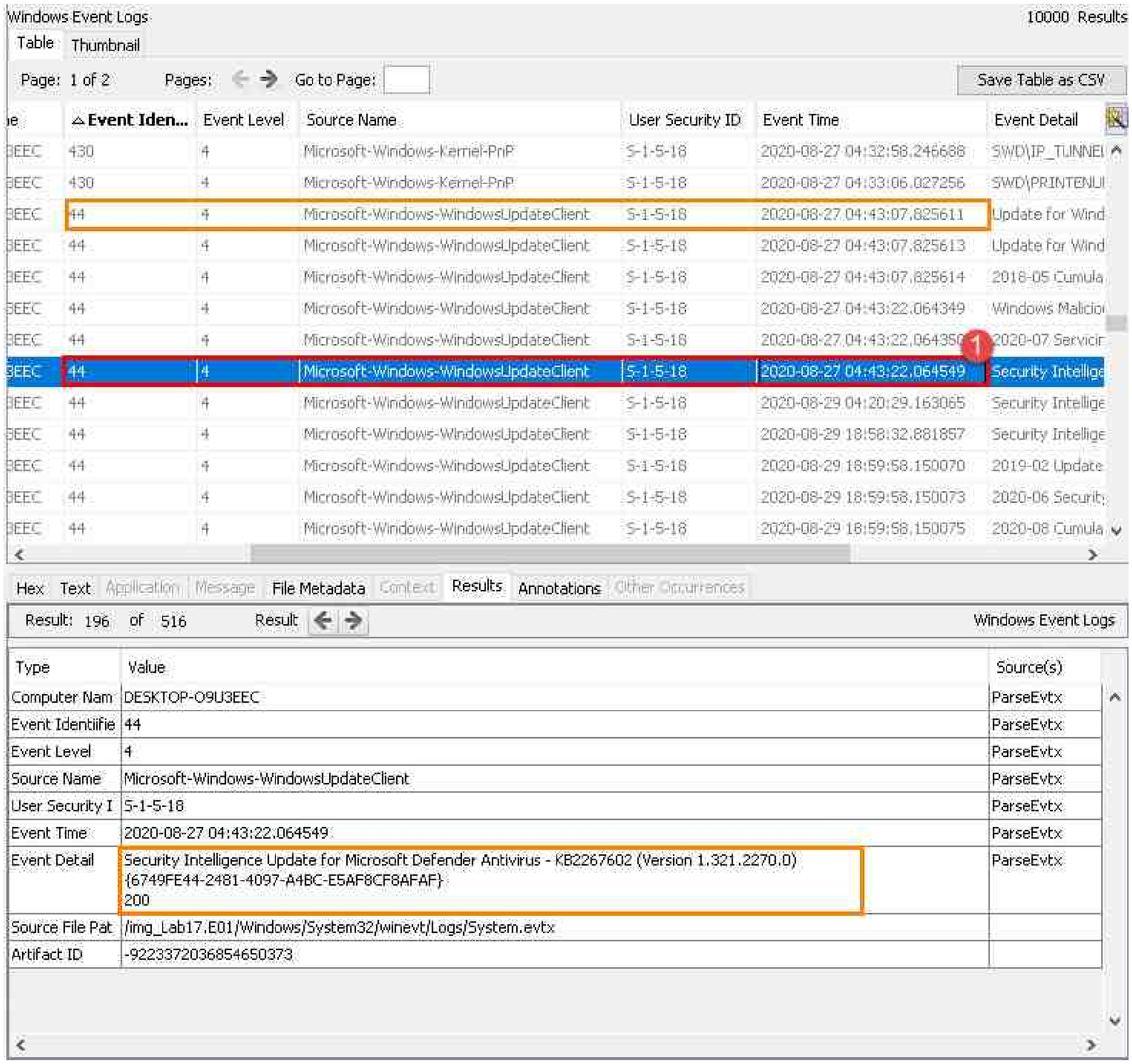
e	Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Detail
VSQ	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:25:29.879429	SW\{cfd669f1-9
VSQ	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:25:29.881798	SW\{eec12db6-
BEEC	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:32:56.559992	SWD\IP_TUNNEI
BEEC	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:32:58.246668	SWD\IP_TUNNEI
BEEC	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:33:06.02725	SWD\PRINTENU
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825611	Update for Wind
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825613	Update for Wind
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825614	2018-05 Cumula
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064349	Windows Maliciou
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064350	2020-07 Servicir
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064549	Security Intellige
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 04:20:29.163065	Security Intellige
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:58:32.881857	Security Intellige
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150070	2019-02 Update
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150073	2020-06 Security
BEEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150075	2020-08 Cumula
VSQ	445	5	Microsoft-Windows-AppXDeployment-Server	S-1-5-18	2020-08-27 04:25:41.939258	windows.immers
VSQ	445	5	Microsoft-Windows-AppXDeployment-Server	S-1-5-18	2020-08-27 04:25:42.375442	Windows.Miraca
VSQ	445	5	Microsoft-Windows-AppXDeployment-Server	S-1-5-18	2020-08-27 04:25:42.375463	Windows.Mi

10. The details in this event are significantly different from the logon and logoff events. As seen in item 1 below, this log simply provides the name of the update being downloaded for install.



Type	Value	Source(s)
Computer Nam	DESKTOP-O9U3EEC	ParseEvtx
Event Identifie	44	ParseEvtx
Event Level	4	ParseEvtx
Source Name	Microsoft-Windows-WindowsUpdateClient	ParseEvtx
User Security I	S-1-5-18	ParseEvtx
Event Time	2020-08-27 04:43:07.825611	ParseEvtx
Event Detail	Update for Windows 10 Version 1607 for x64-based Systems (KB4049411) {B4B973F7-9D95-4601-B00E-F0101F1CF0EC} 201	ParseEvtx
Source File Pat	/img_Lab17.E01/Windows/System32/winevt/Logs/System.evtx	
Artifact ID	-9223372036854650380	

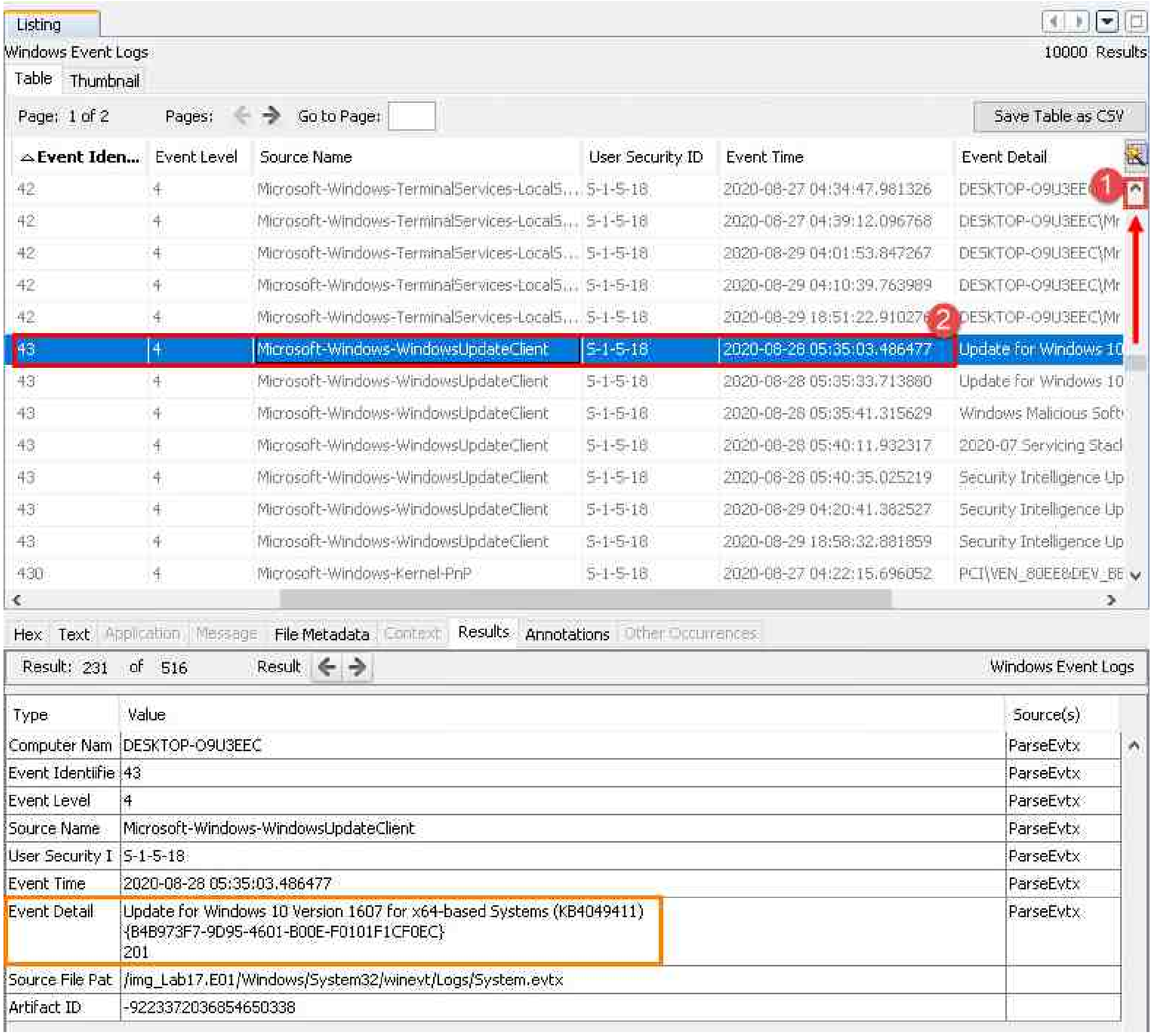
11. Let us select another update event; click the one that has the timestamp 2020-08-27 04:43:22.064549 as seen in item 1 below. As you can see in item 1, this is an update for Microsoft Defender, and it can provide information about whether the computer's antivirus was up to date at a specific date and time.



ie	Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Detail
3EEC	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:32:58.246688	SWD\IP_TUNNEI
3EEC	430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:33:06.027256	SWD\PRINTENUI
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825611	Update for Wind
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825613	Update for Wind
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:07.825614	2018-05 Cumula
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064349	Windows Malicio
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064350	2020-07 Servicir
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-27 04:43:22.064549	Security Intellige
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 04:20:29.163065	Security Intellige
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:58:32.881857	Security Intellige
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150070	2019-02 Update
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150073	2020-06 Security
3EEC	44	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:59:58.150075	2020-08 Cumula

Type	Value	Source(s)
Computer Nam	DESKTOP-O9U3EEC	ParseEvtx
Event Identiifie	44	ParseEvtx
Event Level	4	ParseEvtx
Source Name	Microsoft-Windows-WindowsUpdateClient	ParseEvtx
User Security I	S-1-5-18	ParseEvtx
Event Time	2020-08-27 04:43:22.064549	ParseEvtx
Event Detail	Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.321.2270.0) {6749FE44-2481-4097-A4BC-E5AF8CF8AFAF} 200	ParseEvtx
Source File Pat	/img_Lab17.E01/Windows/System32/winevt/Logs/System.evtx	
Artifact ID	-9223372036854650373	

12. Let us check if these updates were installed by comparing the update download event (Event ID 44) with the update install event (Event ID 43). Let us use the scroll bar or arrow button to scroll to Event ID 43, as seen in item 1 below. Next, select the event that has the timestamp 2020-08-28 05:35:03.486477 by clicking it as seen in item 2 below. You can match each one with its download event to see if an install was attempted. There is also an event that tells whether the install was successful or it failed. This is found under event ID 19. We will not be reviewing these events in this exercise, however.



Windows Event Logs — 10000 Results

Page: 1 of 2 Pages: Go to Page:

Event Iden...	Event Level	Source Name	User Security ID	Event Time	Event Detail
42	4	Microsoft-Windows-TerminalServices-LocalS...	S-1-5-18	2020-08-27 04:34:47.981326	DESKTOP-O9U3EE
42	4	Microsoft-Windows-TerminalServices-LocalS...	S-1-5-18	2020-08-27 04:39:12.096768	DESKTOP-O9U3EEC\Mr
42	4	Microsoft-Windows-TerminalServices-LocalS...	S-1-5-18	2020-08-29 04:01:53.847267	DESKTOP-O9U3EEC\Mr
42	4	Microsoft-Windows-TerminalServices-LocalS...	S-1-5-18	2020-08-29 04:10:39.763989	DESKTOP-O9U3EEC\Mr
42	4	Microsoft-Windows-TerminalServices-LocalS...	S-1-5-18	2020-08-29 18:51:22.91027	DESKTOP-O9U3EEC\Mr
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-28 05:35:03.486477	Update for Windows 10
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-28 05:35:33.713880	Update for Windows 10
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-28 05:35:41.315629	Windows Malicious Soft
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-28 05:40:11.932317	2020-07 Servicing Stacl
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-28 05:40:35.025219	Security Intelligence Up
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 04:20:41.382527	Security Intelligence Up
43	4	Microsoft-Windows-WindowsUpdateClient	S-1-5-18	2020-08-29 18:58:32.881859	Security Intelligence Up
430	4	Microsoft-Windows-Kernel-PnP	S-1-5-18	2020-08-27 04:22:15.696052	PCI\VEN_80EE&DEV_BE

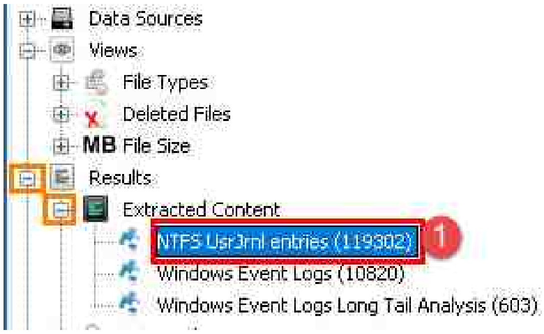
Result: 231 of 516 Result — Windows Event Logs

Type	Value	Source(s)
Computer Nam	DESKTOP-O9U3EEC	ParseEvtx
Event Identifie	43	ParseEvtx
Event Level	4	ParseEvtx
Source Name	Microsoft-Windows-WindowsUpdateClient	ParseEvtx
User Security I	S-1-5-18	ParseEvtx
Event Time	2020-08-28 05:35:03.486477	ParseEvtx
Event Detail	Update for Windows 10 Version 1607 for x64-based Systems (KB4049411) {B4B973F7-9D95-4601-B00E-F0101F1CF0EC} 201	ParseEvtx
Source File Pat	/img_Lab17.E01/Windows/System32/winevt/Logs/System.evtx	
Artifact ID	-9223372036854650338	

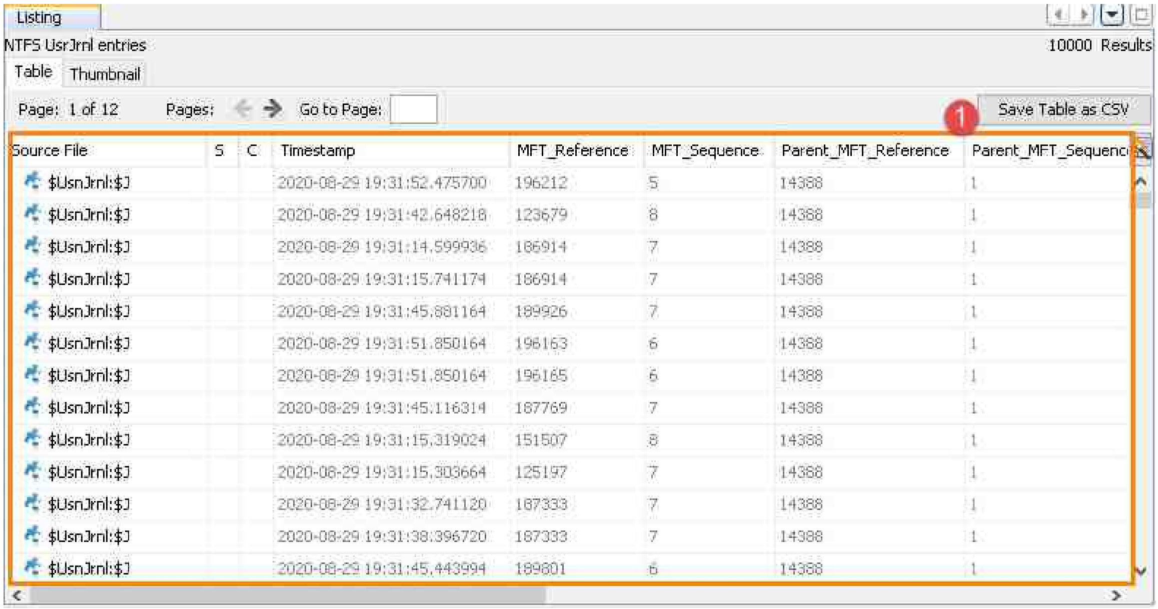
3 Reviewing USN Journal *D*ata

As we mentioned in the first section, the USN (Update Sequence Number) Journal stores records such as creations, deletions, encryption, and more. In this exercise, we will look at some of the data inside this log.

1. The Results and Extracted Content tree should already be expanded. Let us begin by clicking the NTFS UsrJrnl Entries, as seen in item 1 below.


Data Sources
Views
File Types
Deleted Files
MB File Size
Results
Extracted Content
NTFS UsrJrnl entries (119302)
1
Windows Event Logs (10820)
Windows Event Logs Long Tail Analysis (603)

2. You will see the parsed USN Journal logs in the Listing pane as seen in item 1 below. The table below the following screenshot will provide details about the data in each column.

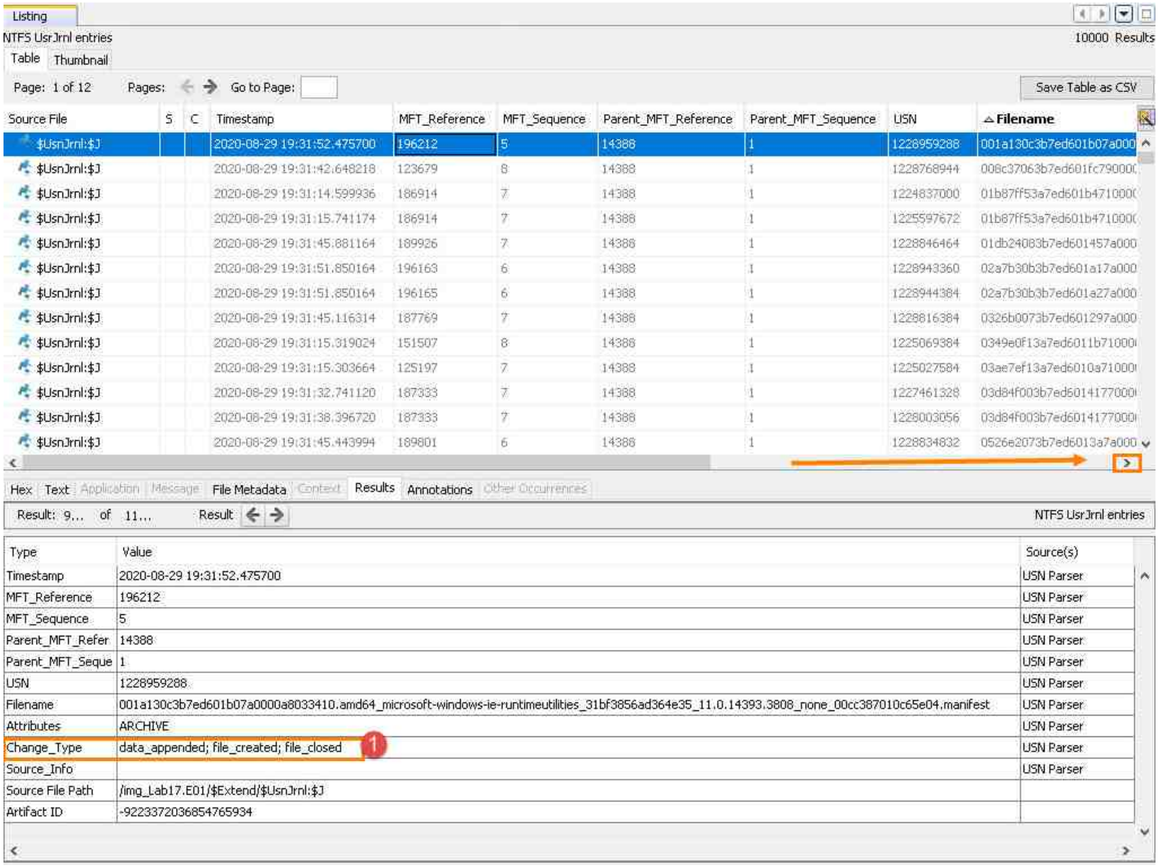


NTFS UsrJrnl entries 10000 Results

Source File	S	C	Timestamp	MFT_Reference	MFT_Sequence	Parent_MFT_Reference	Parent_MFT_Sequenc
$UsnJrnl:$J			2020-08-29 19:31:52.475700	196212	5	14388	1
$UsnJrnl:$J			2020-08-29 19:31:42.648218	123679	8	14388	1
$UsnJrnl:$J			2020-08-29 19:31:14.599936	186914	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:15.741174	186914	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:45.881164	189926	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:51.850164	196163	6	14388	1
$UsnJrnl:$J			2020-08-29 19:31:51.850164	196165	6	14388	1
$UsnJrnl:$J			2020-08-29 19:31:45.116314	187769	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:15.319024	151507	8	14388	1
$UsnJrnl:$J			2020-08-29 19:31:15.303664	125197	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:32.741120	187333	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:38.396720	187333	7	14388	1
$UsnJrnl:$J			2020-08-29 19:31:45.443994	189801	6	14388	1

Source File	This column provides data about the file that the information in each row was taken from
Timestamp	The time that the event was generated
MFT Reference	The MFT record number of the file or directory that is affected by the change
Parent_MFT_Reference	The MFT record number of the parent directory of the file or directory that is affected by the change
USN (Update Sequence Number)	The record number in the USN Journal
Filename	The name of the affected file
Attributes	Attributes of the affected file
Change_Type	Details of the change that was made

3. The logs in this journal can be very granular, so it is important that you have an idea of what you are looking for before searching it. Before we look for any specific file, look at the column called Change_Type[1] as seen in item 1. It tells you what change was made to the associated file. As you can see, there are entries like file_deleted; file_closed and file_created; file_closed. These entries indicate whether a file was deleted or created, respectively. There are several other types of change types that we will not cover in this exercise.



NTFS UsrJrnl entries

10000 Results

Page: 1 of 12 Pages: Go to Page:

Source File	S	C	Timestamp	MFT_Reference	MFT_Sequence	Parent_MFT_Reference	Parent_MFT_Sequence	USN	Filename
$UsnJrnl:$J			2020-08-29 19:31:52.475700	196212	5	14388	1	1228959288	001a130c3b7ed601b07a000
$UsnJrnl:$J			2020-08-29 19:31:42.648218	123679	8	14388	1	1228768944	008c37063b7ed601fc79000(
$UsnJrnl:$J			2020-08-29 19:31:14.599936	186914	7	14388	1	1224837000	01b87ff53a7ed601b471000(
$UsnJrnl:$J			2020-08-29 19:31:15.741174	186914	7	14388	1	1225597672	01b87ff53a7ed601b471000(
$UsnJrnl:$J			2020-08-29 19:31:45.881164	189926	7	14388	1	1228846464	01db24083b7ed601457a000
$UsnJrnl:$J			2020-08-29 19:31:51.850164	196163	6	14388	1	1228943360	02a7b30b3b7ed601a17a000
$UsnJrnl:$J			2020-08-29 19:31:51.850164	196165	6	14388	1	1228944384	02a7b30b3b7ed601a27a000
$UsnJrnl:$J			2020-08-29 19:31:45.116314	187769	7	14388	1	1228816384	0326b0073b7ed601297a000
$UsnJrnl:$J			2020-08-29 19:31:15.319024	151507	8	14388	1	1225069384	0349e0f13a7ed6011b71000
$UsnJrnl:$J			2020-08-29 19:31:15.303664	125197	7	14388	1	1225027584	03ae7ef13a7ed6010a71000
$UsnJrnl:$J			2020-08-29 19:31:32.741120	187333	7	14388	1	1227461328	03d84f003b7ed60141770000
$UsnJrnl:$J			2020-08-29 19:31:38.396720	187333	7	14388	1	1228003056	03d84f003b7ed60141770000
$UsnJrnl:$J			2020-08-29 19:31:45.443994	189801	6	14388	1	1228834832	0526e2073b7ed6013a7a000

Result: 9... of 11... Result

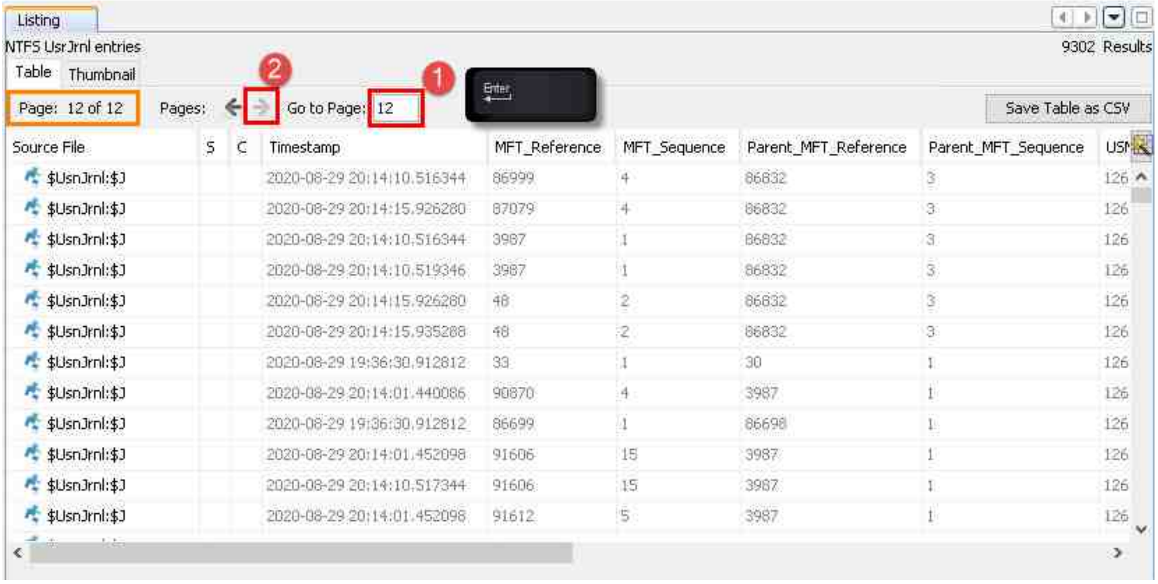
NTFS UsrJrnl entries

Type	Value	Source(s)
Timestamp	2020-08-29 19:31:52.475700	USN Parser
MFT_Reference	196212	USN Parser
MFT_Sequence	5	USN Parser
Parent_MFT_Refer	14388	USN Parser
Parent_MFT_Seque	1	USN Parser
USN	1228959288	USN Parser
Filename	001a130c3b7ed601b07a0000a8033410.amd64_microsoft-windows-ie-runtimeutilities_31bf3856ad364e35_11.0.14393.3808_none_00cc387010c65e04.manifest	USN Parser
Attributes	ARCHIVE	USN Parser
Change_Type	data_appended; file_created; file_closed	USN Parser
Source_Info		USN Parser
Source File Path	/img_Lab17.E01/$Extend/$UsnJrnl:$J	
Artifact ID	-9223372036854765934	

The data for each entry, if selected will load in the view pane. It can take a few seconds for the data to be populated, so feel free to just scroll horizontally to view each row within their respective columns.

[1] https://docs.microsoft.com/en-us/windows/win32/api/winioctl/ns-winioctl-usn_record_v2?redirectedfrom=MSDN

4. Let us look at an event that occurred that was recorded in the USN Journal. Begin by changing to page 12 of the USN Journal entries by clicking and typing `12` in the Go to Page field and pressing Enter as seen in item 1 or by clicking the right arrow beside pages, as seen in item 2 below. This will take you to the end of the journal.



NTFS UsrJrnl entries

9302 Results

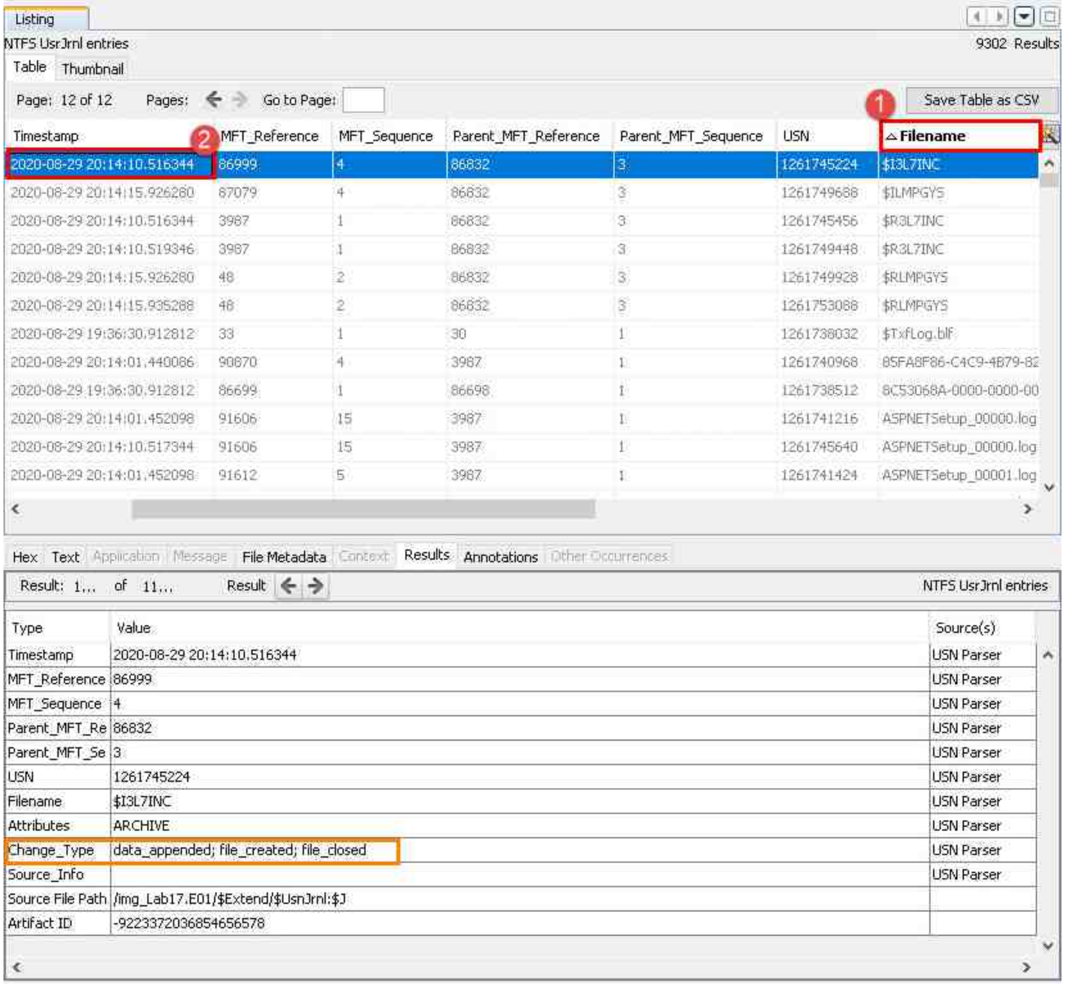
Page: 12 of 12

Go to Page: 12

Source File	S	C	Timestamp	MFT_Reference	MFT_Sequence	Parent_MFT_Reference	Parent_MFT_Sequence	USN
$UsnJrnl:$J			2020-08-29 20:14:10.516344	86999	4	86832	3	126
$UsnJrnl:$J			2020-08-29 20:14:15.926280	87079	4	86832	3	126
$UsnJrnl:$J			2020-08-29 20:14:10.516344	3987	1	86832	3	126
$UsnJrnl:$J			2020-08-29 20:14:10.519346	3987	1	86832	3	126
$UsnJrnl:$J			2020-08-29 20:14:15.926280	48	2	86832	3	126
$UsnJrnl:$J			2020-08-29 20:14:15.935288	48	2	86832	3	126
$UsnJrnl:$J			2020-08-29 19:36:30.912812	33	1	30	1	126
$UsnJrnl:$J			2020-08-29 20:14:01.440086	90870	4	3987	1	126
$UsnJrnl:$J			2020-08-29 19:36:30.912812	86699	1	86698	1	126
$UsnJrnl:$J			2020-08-29 20:14:01.452098	91606	15	3987	1	126
$UsnJrnl:$J			2020-08-29 20:14:10.517344	91606	15	3987	1	126
$UsnJrnl:$J			2020-08-29 20:14:01.452098	91612	5	3987	1	126

We are only going to this location because we know that the files of interest are located there. In practice, use different search and sorting techniques to identify files of interest.

5. Now that we are at the last page, click the column called Filename to sort the column alphabetically, as seen in item 1. Ensure that the files are sorted from a – z, which means the arrow beside Filename should be pointing up. Scroll down until you get to the timestamp 2020-08-29 20:14:01.516344, as seen in item 2 below. This is a file that has a name that resembles a file found in the Recycle.Bin folder. As you can see from the Change_Type for this file is data_appended; file_created; file_closed. This means the file called $I3L7INC was created at that specific time, and data was appended to it before it was closed.



NTFS UsrJrnl entries

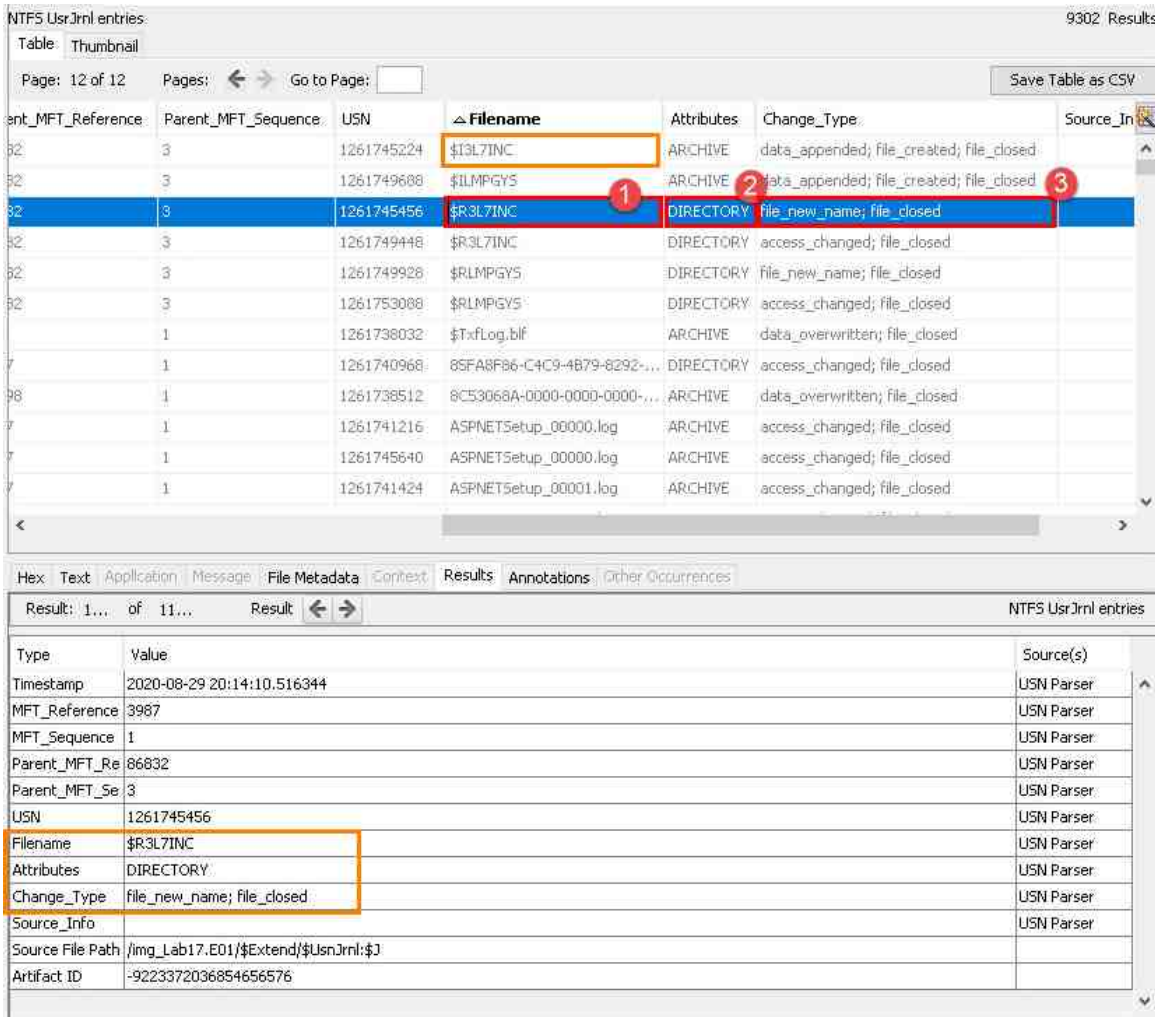
9302 Results

Timestamp	MFT_Reference	MFT_Sequence	Parent_MFT_Reference	Parent_MFT_Sequence	USN	△ Filename
2020-08-29 20:14:10.516344	86999	4	86832	3	1261745224	$I3L7INC
2020-08-29 20:14:15.926280	87079	4	86832	3	1261749688	$ILMPGYS
2020-08-29 20:14:10.516344	3987	1	86832	3	1261745456	$R3L7INC
2020-08-29 20:14:10.519346	3987	1	86832	3	1261749448	$R3L7INC
2020-08-29 20:14:15.926280	48	2	86832	3	1261749928	$RLMPGYS
2020-08-29 20:14:15.935288	48	2	86832	3	1261753088	$RLMPGYS
2020-08-29 19:36:30.912812	33	1	30	1	1261738032	$TxfLog.blf
2020-08-29 20:14:01.440086	90870	4	3987	1	1261740968	85FA8F86-C4C9-4B79-82
2020-08-29 19:36:30.912812	86699	1	86698	1	1261738512	8C53068A-0000-0000-00
2020-08-29 20:14:01.452098	91606	15	3987	1	1261741216	ASPNETSetup_00000.log
2020-08-29 20:14:10.517344	91606	15	3987	1	1261745640	ASPNETSetup_00000.log
2020-08-29 20:14:01.452098	91612	5	3987	1	1261741424	ASPNETSetup_00001.log

NTFS UsrJrnl entries

Type	Value	Source(s)
Timestamp	2020-08-29 20:14:10.516344	USN Parser
MFT_Reference	86999	USN Parser
MFT_Sequence	4	USN Parser
Parent_MFT_Re	86832	USN Parser
Parent_MFT_Se	3	USN Parser
USN	1261745224	USN Parser
Filename	$I3L7INC	USN Parser
Attributes	ARCHIVE	USN Parser
Change_Type	data_appended; file_created; file_closed	USN Parser
Source_Info		USN Parser
Source File Path	/img_Lab17.E01/$Extend/$UsnJrnl:$J	
Artifact ID	-9223372036854656578	

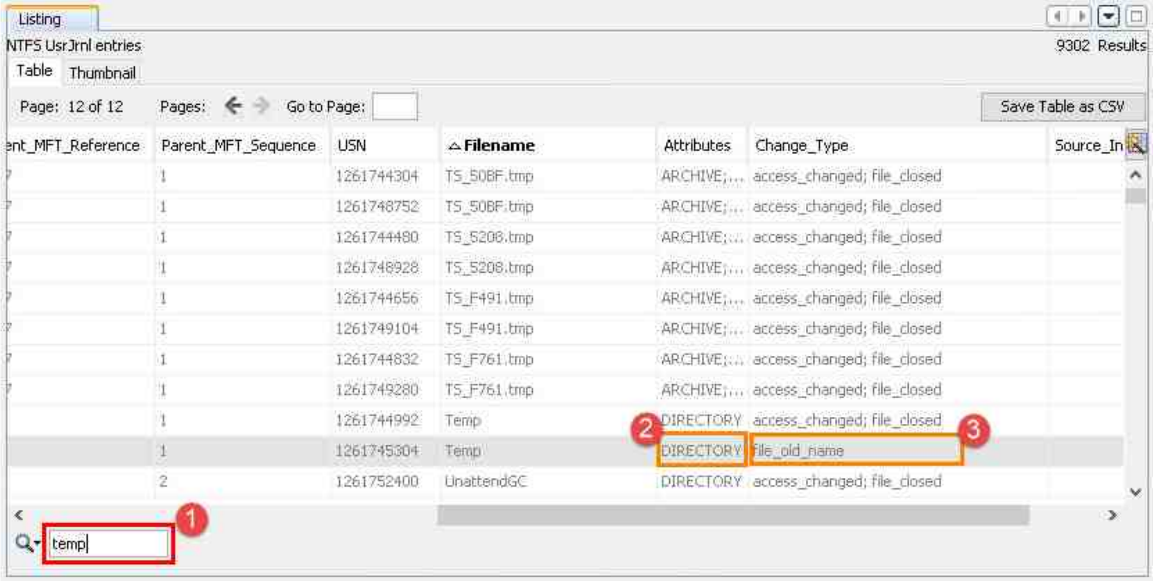
6. Let us look at the next file $R3L7INC, as seen in item 1 below. This file also has a naming convention that resembles a recycled file. The Attributes column in item 2 indicates that this item is a directory as well. Now look at the Change_Type column as seen in item 3, where it states file_new_name; file_closed. This entry corresponds with the previous one and indicates that the folder called Temp was deleted, and the name was changed to $R3L7INC. As with files in the Recycle.Bin folder, an index for the recycle bin entry called $I3L7INC was also created right before the rename. This process gives you some insight into the behavior of the USN Journal and how to track activity inside it.



ent_MFT_Reference	Parent_MFT_Sequence	USN	Filename	Attributes	Change_Type	Source_In
32	3	1261745224	$I3L7INC	ARCHIVE	data_appended; file_created; file_closed	
32	3	1261749688	$ILMPGYS	ARCHIVE	data_appended; file_created; file_closed	
32	3	1261745456	$R3L7INC	DIRECTORY	file_new_name; file_closed	
32	3	1261749448	$R3L7INC	DIRECTORY	access_changed; file_closed	
32	3	1261749928	$RLMPGYS	DIRECTORY	file_new_name; file_closed	
32	3	1261753088	$RLMPGYS	DIRECTORY	access_changed; file_closed	
	1	1261738032	$TxfLog.blf	ARCHIVE	data_overwritten; file_closed	
7	1	1261740968	85FA8F86-C4C9-4B79-8292-...	DIRECTORY	access_changed; file_closed	
98	1	1261738512	8C53068A-0000-0000-0000-...	ARCHIVE	data_overwritten; file_closed	
7	1	1261741216	ASPNETSetup_00000.log	ARCHIVE	access_changed; file_closed	
7	1	1261745640	ASPNETSetup_00000.log	ARCHIVE	access_changed; file_closed	
7	1	1261741424	ASPNETSetup_00001.log	ARCHIVE	access_changed; file_closed	

Type	Value	Source(s)
Timestamp	2020-08-29 20:14:10.516344	USN Parser
MFT_Reference	3987	USN Parser
MFT_Sequence	1	USN Parser
Parent_MFT_Re	86832	USN Parser
Parent_MFT_Se	3	USN Parser
USN	1261745456	USN Parser
Filename	$R3L7INC	USN Parser
Attributes	DIRECTORY	USN Parser
Change_Type	file_new_name; file_closed	USN Parser
Source_Info		USN Parser
Source File Path	/img_Lab17.E01/$Extend/$UsnJrnl:$J	
Artifact ID	-9223372036854656576	

7. Next, search for the filename `Temp` as seen in item 1. There should be two files with the name Temp, the one we are interested in has the Attributes column indicating that it is a directory, as seen in item 2, and the Change_Type is file_old_name, as seen in item 3. This means that this item was renamed.



Listing

NTFS UsrJrnl entries — 9302 Results

Table | Thumbnail

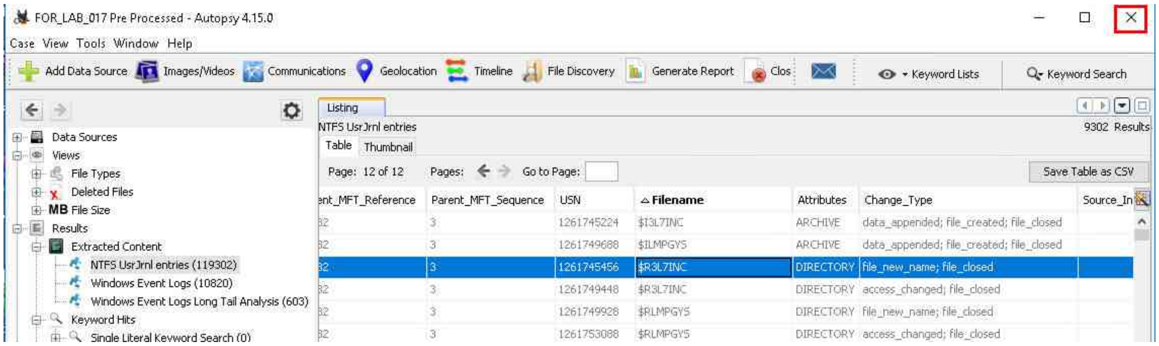
Page: 12 of 12 Pages: Go to Page: — Save Table as CSV

ent_MFT_Reference	Parent_MFT_Sequence	USN	Filename	Attributes	Change_Type	Source_In
	1	1261744304	TS_50BF.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261748752	TS_50BF.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261744480	TS_5208.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261748928	TS_5208.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261744656	TS_F491.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261749104	TS_F491.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261744832	TS_F761.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261749280	TS_F761.tmp	ARCHIVE;...	access_changed; file_closed	
	1	1261744992	Temp	DIRECTORY	access_changed; file_closed	
	1	1261745304	Temp	DIRECTORY	file_old_name	
	2	1261752400	UnattendGC	DIRECTORY	access_changed; file_closed	

temp

Remember, this can be achieved easily by clicking within the column Filename and typing `temp` as seen in item 1.

8. Now on your own, scroll down to look for another delete folder and note its old name, new name, and the times of the changes.
9. Once done, close all the open windows and log out of the workstation. You are now at the end of this lab.



FOR_LAB_017 Pre Processed - Autopsy 4.15.0

Listing

NTFS UsrJrnl entries — 9302 Results

Table | Thumbnail

Page: 12 of 12 Pages: Go to Page: — Save Table as CSV

ent_MFT_Reference	Parent_MFT_Sequence	USN	Filename	Attributes	Change_Type	Source_In
32	3	1261745224	$I3L7INC	ARCHIVE	data_appended; file_created; file_closed	
32	3	1261749688	$ILMPGYS	ARCHIVE	data_appended; file_created; file_closed	
32	3	1261745456	$R3L7INC	DIRECTORY	file_new_name; file_closed	
32	3	1261749448	$R3L7INC	DIRECTORY	access_changed; file_closed	
32	3	1261749928	$RLMPGYS	DIRECTORY	file_new_name; file_closed	
32	3	1261753088	$RLMPGYS	DIRECTORY	access_changed; file_closed	