Hunting through Log Data with Excel

***SUPPLEMENT***

GIAC GCIH Gold Certification

Author: Greg Lalla, greg.lalla@mail.com

Advisor: Christopher Walker, CISSP, GWEB, GCED, CCISO, GCUX, GCWN, GSEC

Accepted: March 25, 2017

Abstract

Gathering and analyzing data during an incident can be a long and tedious process. The vast amounts of data involved in even a single system intrusion can be overwhelming. Larger and well-funded incident response teams typically have a Security Information and Event Management (SIEM) product at their disposal to help the responder sift through this data to find artifacts relevant to the intrusion. This paper will demonstrate to the reader how to use Microsoft Excel and some of its more advanced features during an intrusion if a SIEM or similar product is not available to the incident responder.

# Pivot Tables

Pivot Tables are a great way to sort data in a way that visually allows you to pick out artifacts of interest. “A pivot table allows you to create an interactive view of your dataset. With a pivot table report, you can quickly and easily categorize your data into meaningful information, and perform a wide variety of calculations in a fraction of the time it takes by hand” (Jelen, 2006, p. 9). This categorization of data is especially true when working with Windows Event Viewer logs. Exporting the logs in XML table format provides headers that can be used to categorize the data in ways that will allow you to see trends and commonalities.

To create a Pivot Table of Event Viewer data, import an Event Viewer XML formatted export file into Excel (instructions can be found in Section 4.1.1 of the main document). Once the data is displayed in Excel in Table format, select the ‘Design Tab’ on the Ribbon bar and click on ‘Summarize with PivotTable’ (Figure 1).

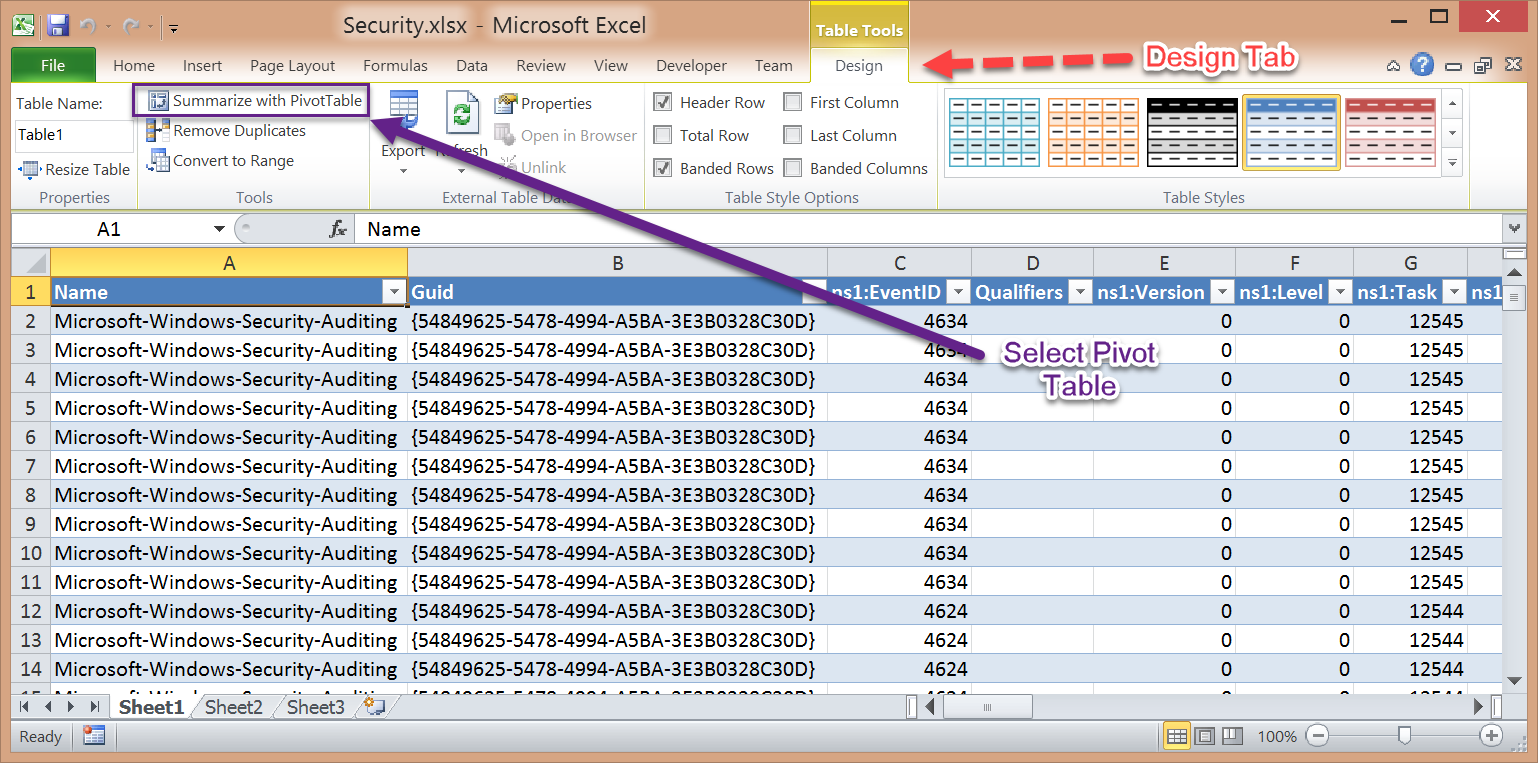


Figure . Summarize with PivotTable (Lee, 2014, digital case files)

A ‘Create PivotTable’ window will pop up asking where the new PivotTable should be created. To keep the data together, in the example below, Sheet2, Cell A1 is chosen as the location. Before clicking on ‘OK’, make sure that you are on Sheet2 as the operation will not work if the worksheet with all the data is still selected (Figure 2).

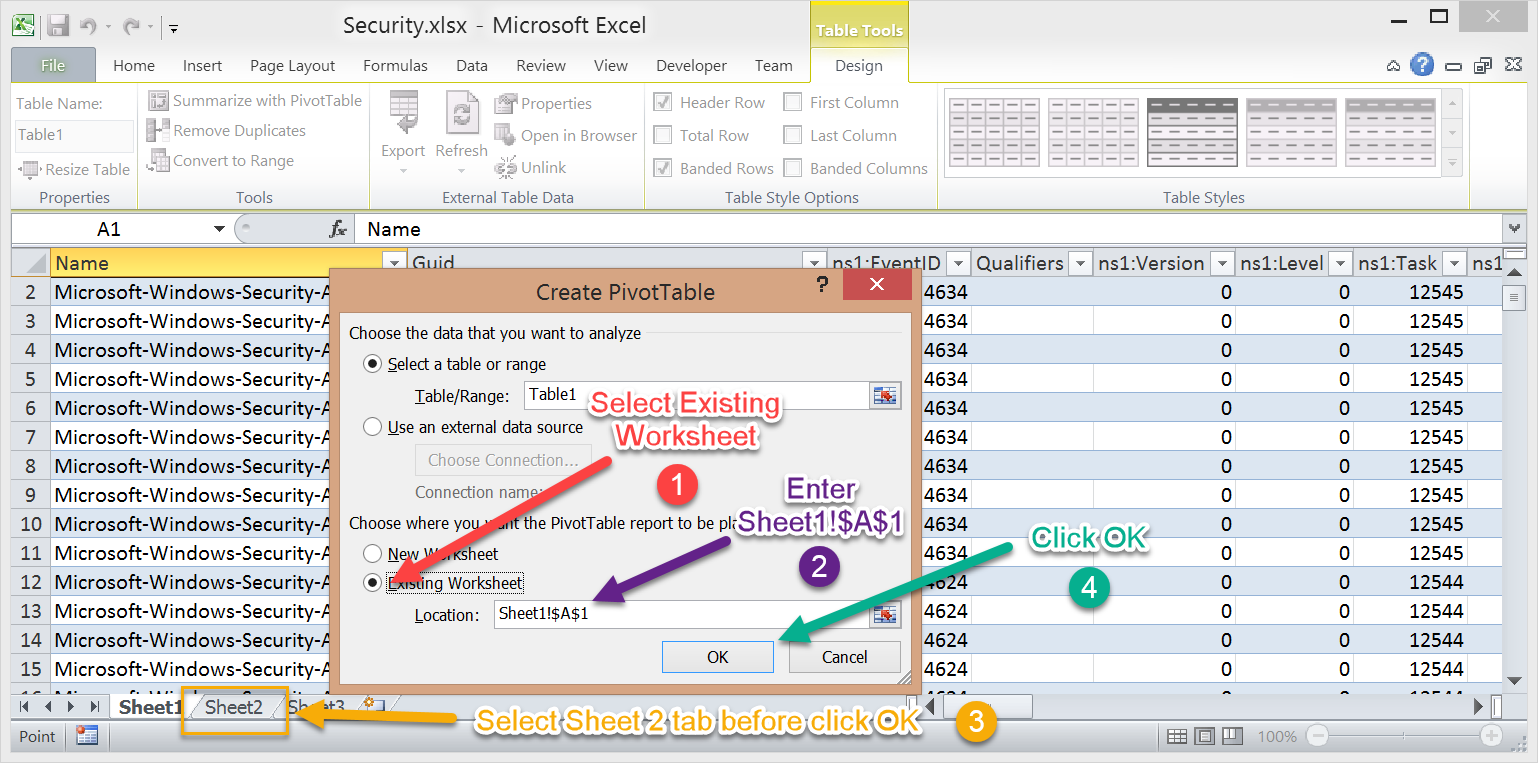


Figure . Create PivotTable. (Lee, 2014, digital case files)

When ‘OK’ has been clicked, the PivotTable design windows will be shown on Sheet 2. In the Window Pane to the right of the spreadsheet, the PivotTable outline can be created using various tools (Figure 3). When creating PivotTables from Event Viewer logs, one of the best Headers to pivot on is the Event ID field. Since one Event ID can be logged thousands of times, pivoting on that field can take those entries and condense them into a meaningful structure to display unique data points, such as IP addresses, user names, processes, etc.

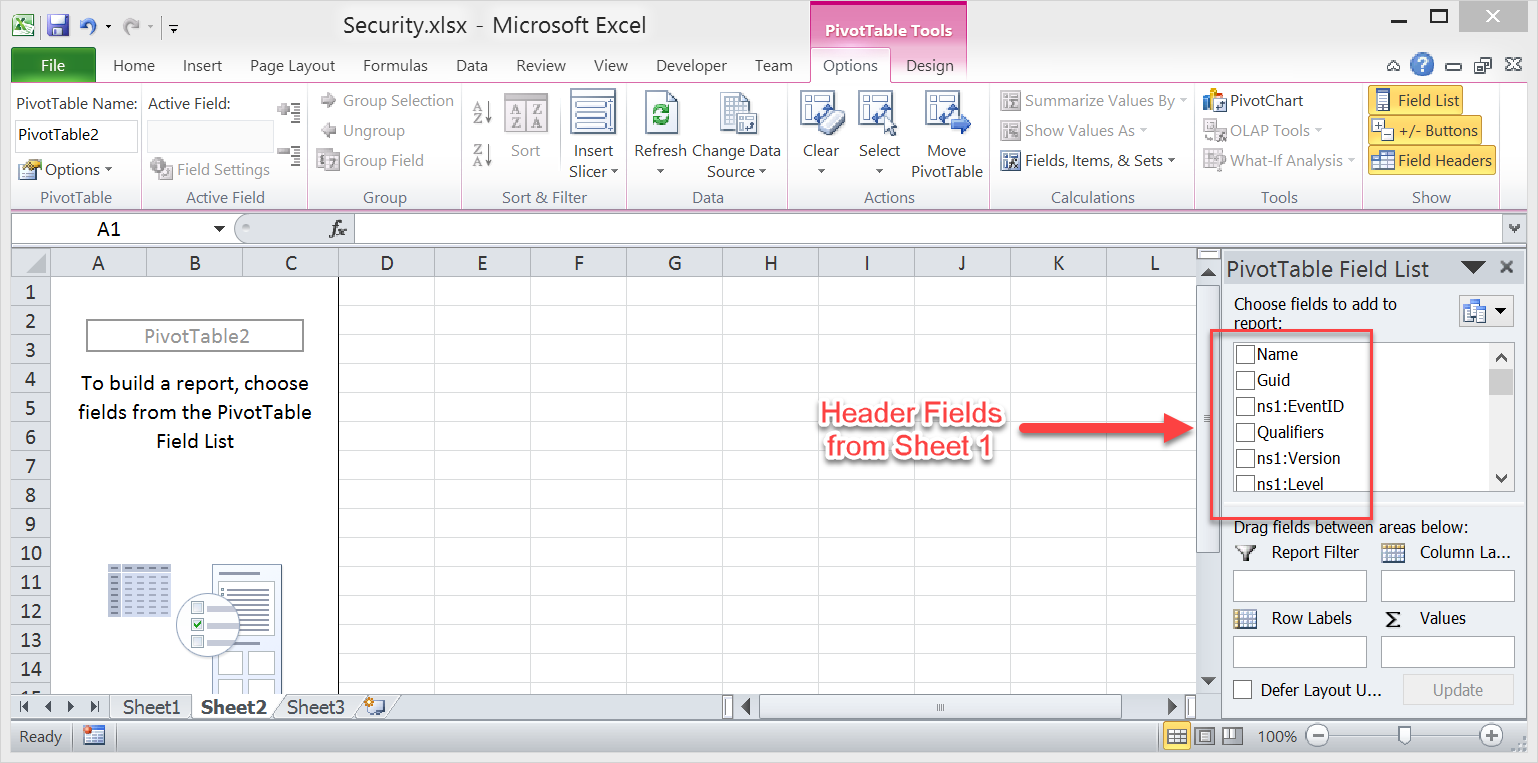


Figure . PivotTable outline. (Lee, 2014, digital case files)

In the example below, the Event Viewer Security log is going to Pivot on the Event ID (labeled ns1:EventID), then on Properties (labeled Name2), and finally on the Data (ns1:Data). This is done by choosing those Headers under the ‘Pivot Table Field List” pane (Figure 4).

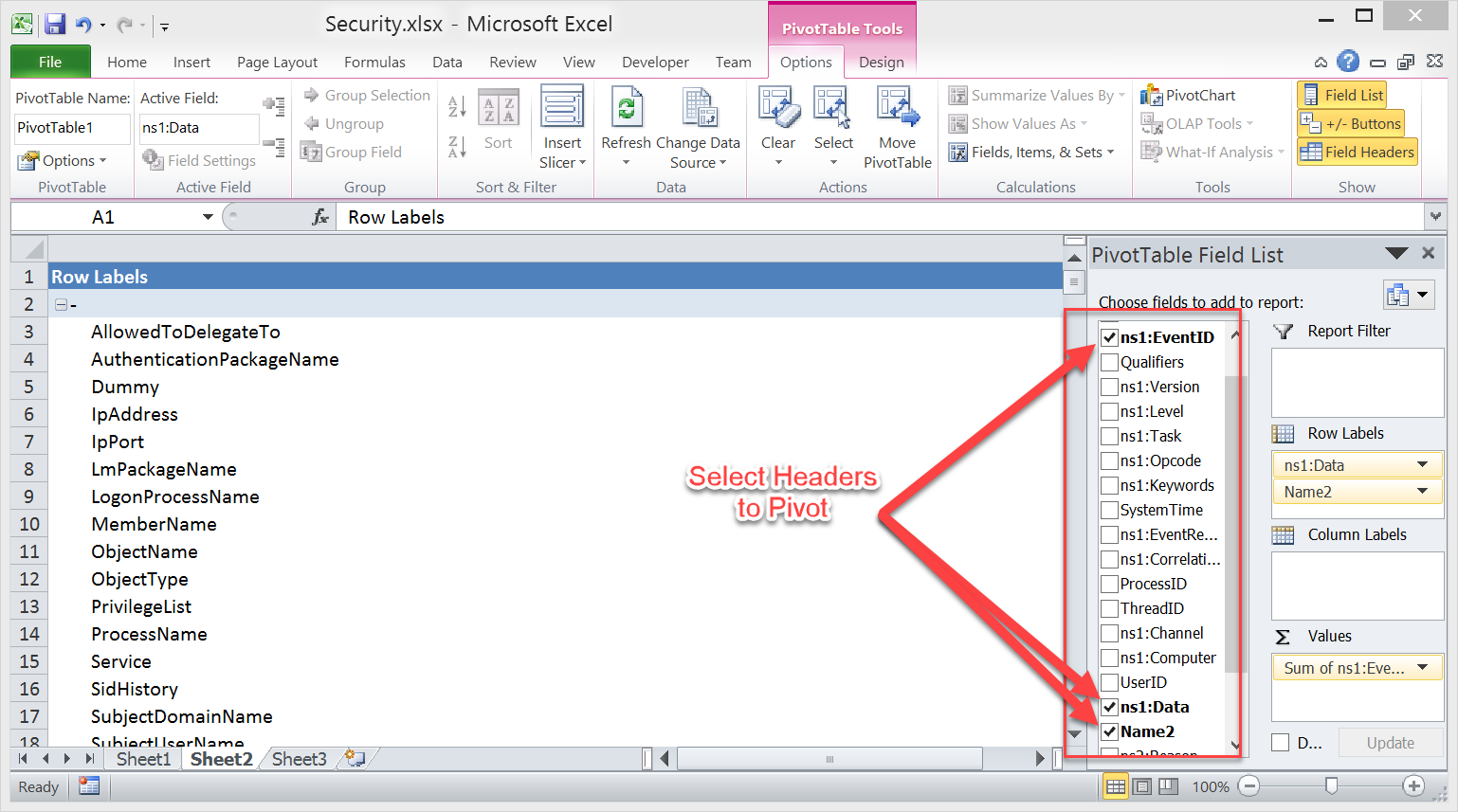


Figure . Pivot Table Field List. (Lee, 2014, digital case files)

The layout of the windows on the right-side pane can be arranged according to your preference. Below, the fields we are interested in pivoting on are all positioned in the ‘Row Labels’ window by dragging and dropping each of them in place (Figure 5).

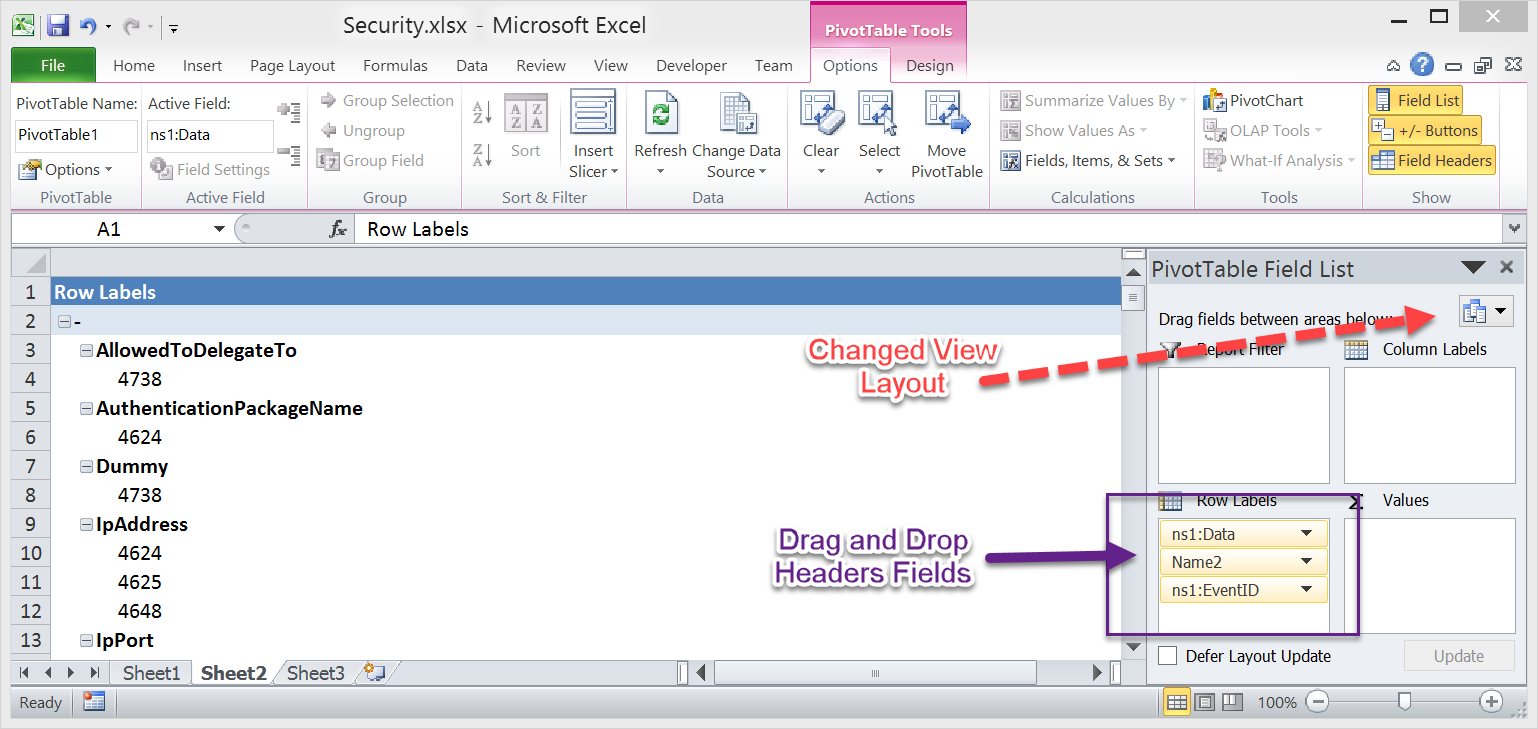


Figure . Change View Layout. (Lee, 2014, digital case files)

The order of the Header fields matter. Each of them can be moved either by dragging and dropping or by click the down arrow to the right of the item and selecting one of its options (Figure 6).

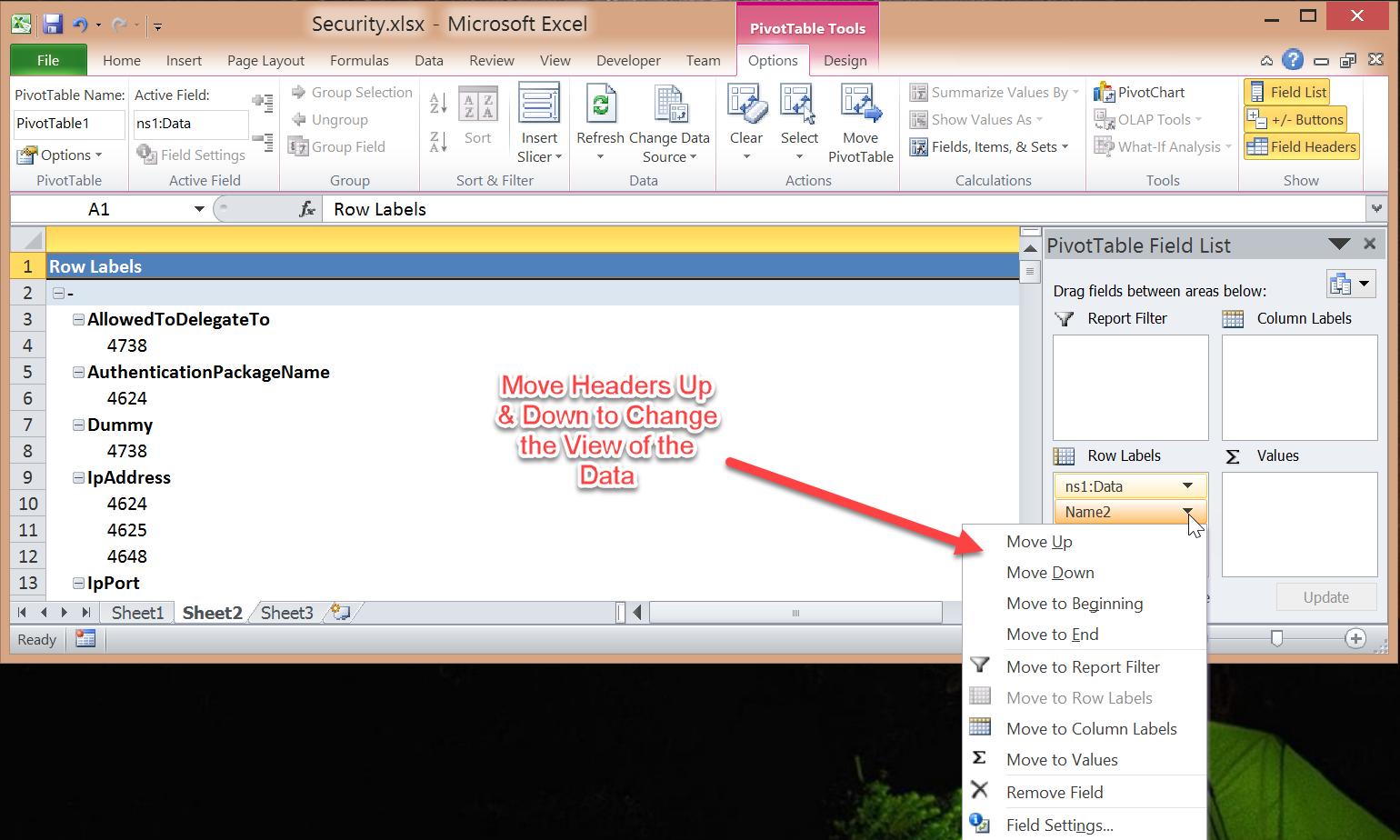


Figure . Header Field Order. (Lee, 2014, digital case files)

In Figure 7, the Event ID field is the prime pivot point and is placed first on the list. The next point is the Property Names field, followed by the Data field. This combination displays the data in a hierarchical structure in which we can easily see the types of data found for each of the Event IDs.

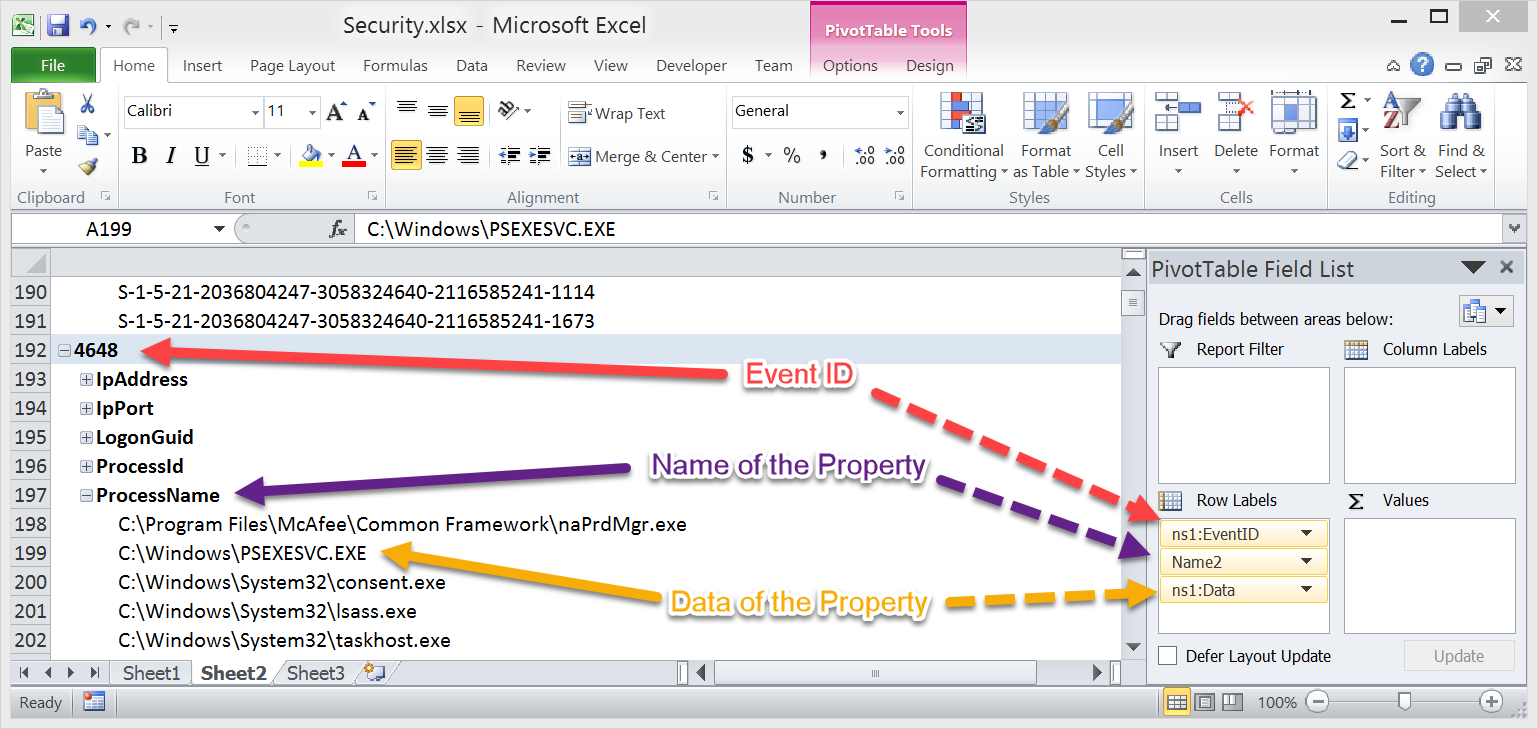


Figure . Event ID is the prime pivot point. (Lee, 2014, digital case files)

That is just one of the many ways to view PivotTable data. Experimenting with different headers, in different orders, can provide other opportunities to bring out the data that may be relevant to an intrusion. As an example, for the Application Event Viewer logs, the following Header arrangement has been found to be beneficial:

*ns2:EventID*

*UserID*

*ns2:Data*

References

Jelen, B., & Alexander, M. (2006). *Pivot Table Data Crunching*. Indianapolis, IN: Que Publishing

Lee, R. (2014). *SANS Forensic 508 Advanced Computer Forensic Analysis and Incident Response, Stark Research Labs Intrusion: Exercise Workbook*.