Network Forensics
Module 07

Network Forensics

Network forensics involves identification of suspected criminal activity and the alleged people responsible for the crime. Network forensics can be defined as sniffing, recording, acquisition, and analysis of the network traffic and event logs to investigate a network security incident.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

James, the owner of a software company, received a complaint from Jessica (one of his company's employees), that she is receiving sensitive emails from an unknown person or email ID and she suspects that another employee is sending these emails. James wanted to capture and analyze all the incoming and outgoing packets of the network in order to trace out the person who is sending the sensitive emails to Jessica.

Lab Objectives

The objective of this lab is, to make forensic investigators understand how to sniff a network and analyze packets of the target network.

The primary objectives of this lab are:

- Capturing and Analyzing the Logs of a Computer Using GFI EventsManager Tool
- Investigating System Log Data Using XpoLog Center Suite Tool
- Investigating Network Attacks Using Kiwi Log Viewer
- Investigating Network Traffic Using Wireshark

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics

Lab Environment

In this lab, you will need:

- A computer running on **Windows Server 2012** virtual machine.
- A web browser with **Internet** connection.
- Administrative privileges to run tools.

Lab Duration

Time: 70 Minutes

Overview of Network Forensics

Network forensics is the process of identifying criminal activity and the people behind the crime. Network forensics encompasses **sniffing**, **recording**, **acquisition**, and **analysis** of the network traffic and event log data to investigate a network security incident. It allows the investigator to inspect the network traffic and logs to identify and locate the attacking system.

Lab Tasks

TASK 1

Overview

Recommended labs to assist you in sniffing the network:

- Capturing and Analyzing Logs of a Computer Using **GFI Events Manager**.
- Investigating System Log Data Using **XpoLog Center Suite**.
- Investigating Network Attacks Using **Kiwi Log Viewer**.
- Investigating Network Traffic Using **Wireshark**.

Lab

1

Capturing and Analyzing the Logs of a Computer using GFI EventsManager

The GFI Events Manager automatically processes and archives logs, by collecting the information needed to know about the most important events of the computer.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

James is working as a team leader in an MNC company. Sam is an efficient, honest, and dedicated member of James's team, but recently James noticed a big drop in Sam's performance. James found out from other team members that, Sam is wasting a lot of time browsing and chatting on social networking sites. James called Sam to ask him an explanation for the drop in his performance, and Sam lied by saying that his current project is very difficult to understand and time consuming. Before taking any serious action against Sam, James wanted to capture and analyze all the logs of Sam's computer to know how he is spending his time in the office.

As an expert **forensic investigator,** to analyze the security posture of a target computer you must know how to capture and analyze the log files of a target computer.

Lab Objectives

The objective of this lab is to help the forensic investigator understand and perform log capturing of a computer using various techniques, to obtain:

- Security events
- Application events
- System events

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics

Lab Environment

To perform the lab, you will need:

- A computer running on **Windows Server 2012 virtual machine**.
- A web browser with an **Internet** connection.
- Administrative privileges to install and run tools.

Lab Duration

Time: 20 Minutes

Overview of Capturing and Analyzing log files

Every device on a network generates some kind of logs for each and every action carried out on the network. Capturing and analyzing the log files is an important task while investigating the security posture of the target network. The log files contain information about all the system, device, and user activities that took place within the network.

Lab Tasks

TASK 1

Registering on the GFI EventsManager Website

1. Log on to **Windows Server 2012** virtual machine, launch a web browser, paste the URL http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-eventsmanager/download?pid=esm in the address bar, and then press **Enter**. It will redirect you to the registration form for GFI EventsManager.
2. Fill in the necessary details in the **Registration** page and then, click **Continue** button.

GFI EventsManager assists with monitoring and managing event logs, maintaining network health and security.

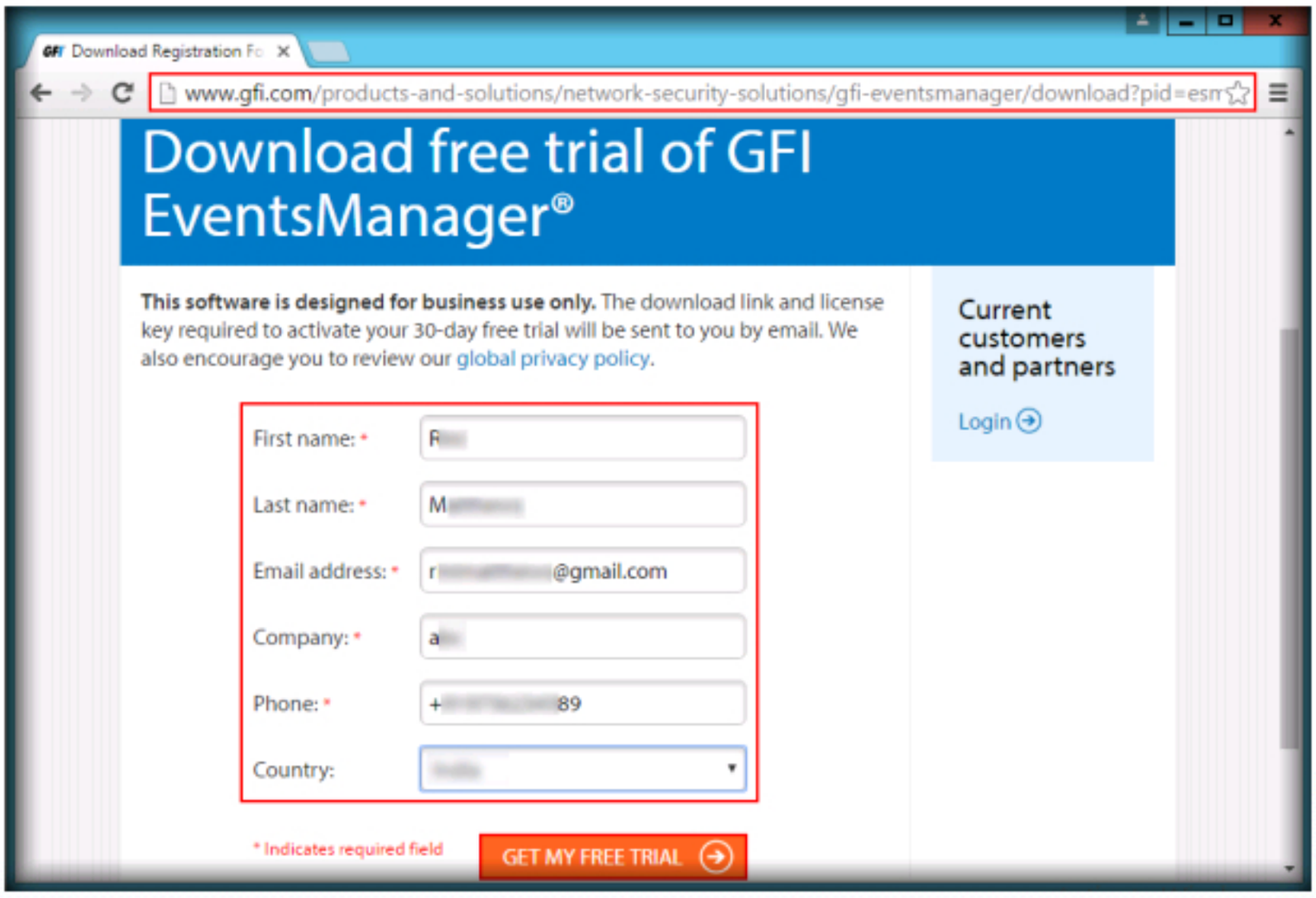

FIGURE 1.1: GFI EventsManager download registration form

3. You will be redirected to the download page, then click **Download Now**.

GFI EventsManager's powerful filtering shifts through recorded event logs allowing you to browse without deleting any records from your database.

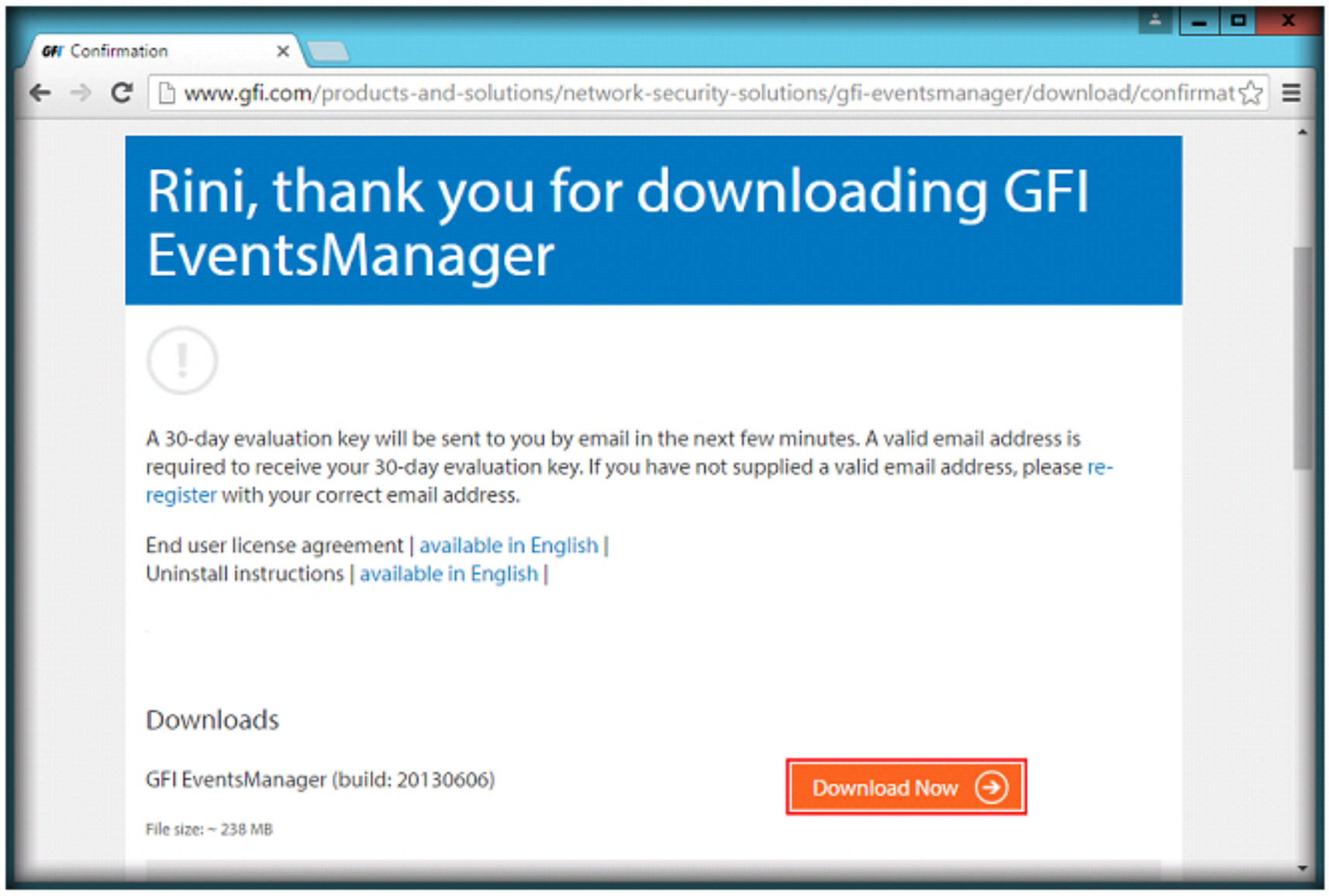

FIGURE 1.2: GFI EventsManager download registration form

4. The application begins to download. A product key will be sent to the Email ID specified at the time of registration, which is necessary for installing GFI EventsManager. So, login to your Email account and note down the product key.

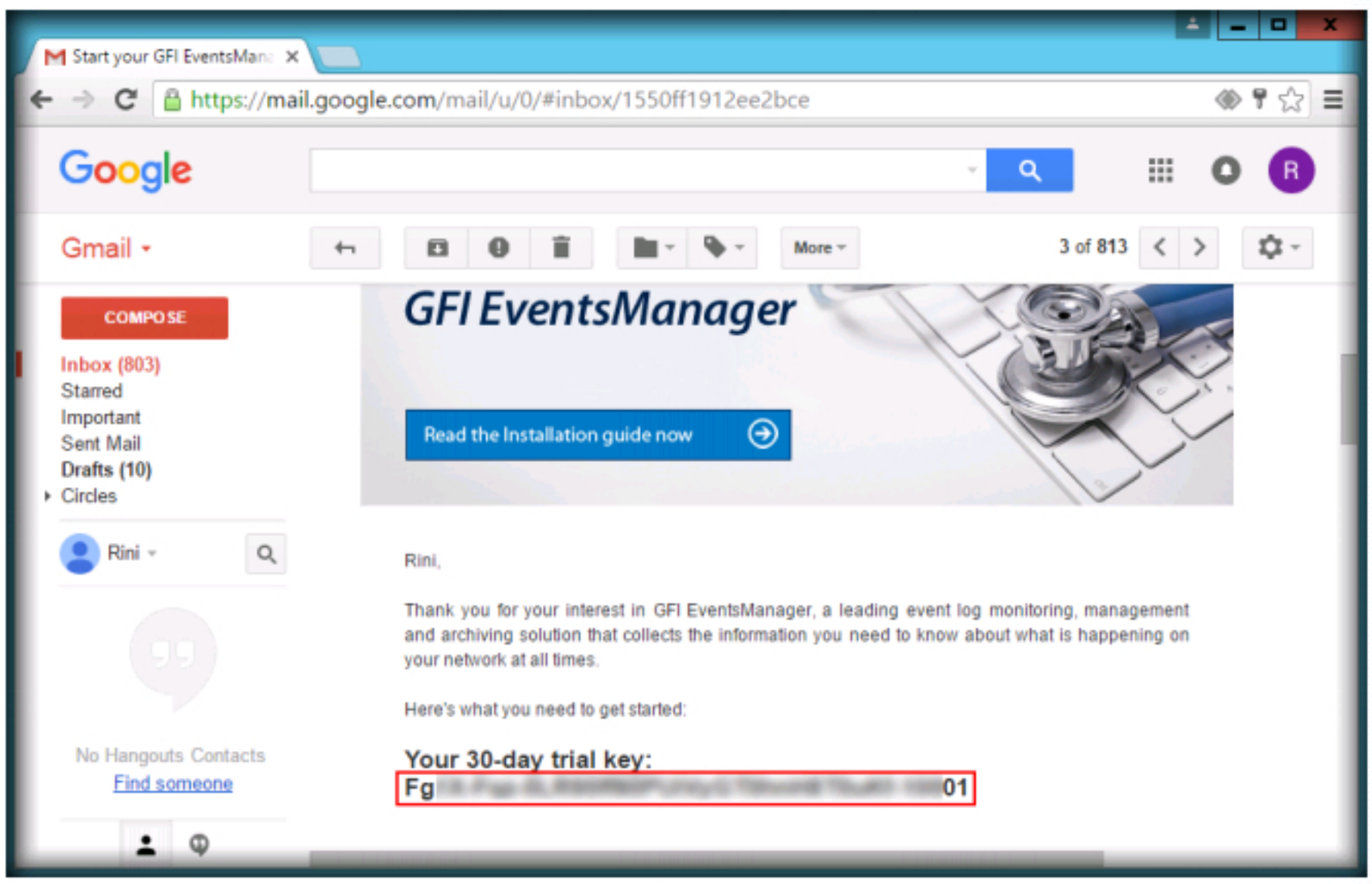

FIGURE 1.3: GFI EventsManager product key sent to the Email ID

5. On completion of download, navigate to the path where the application is saved, and double-click the installer.

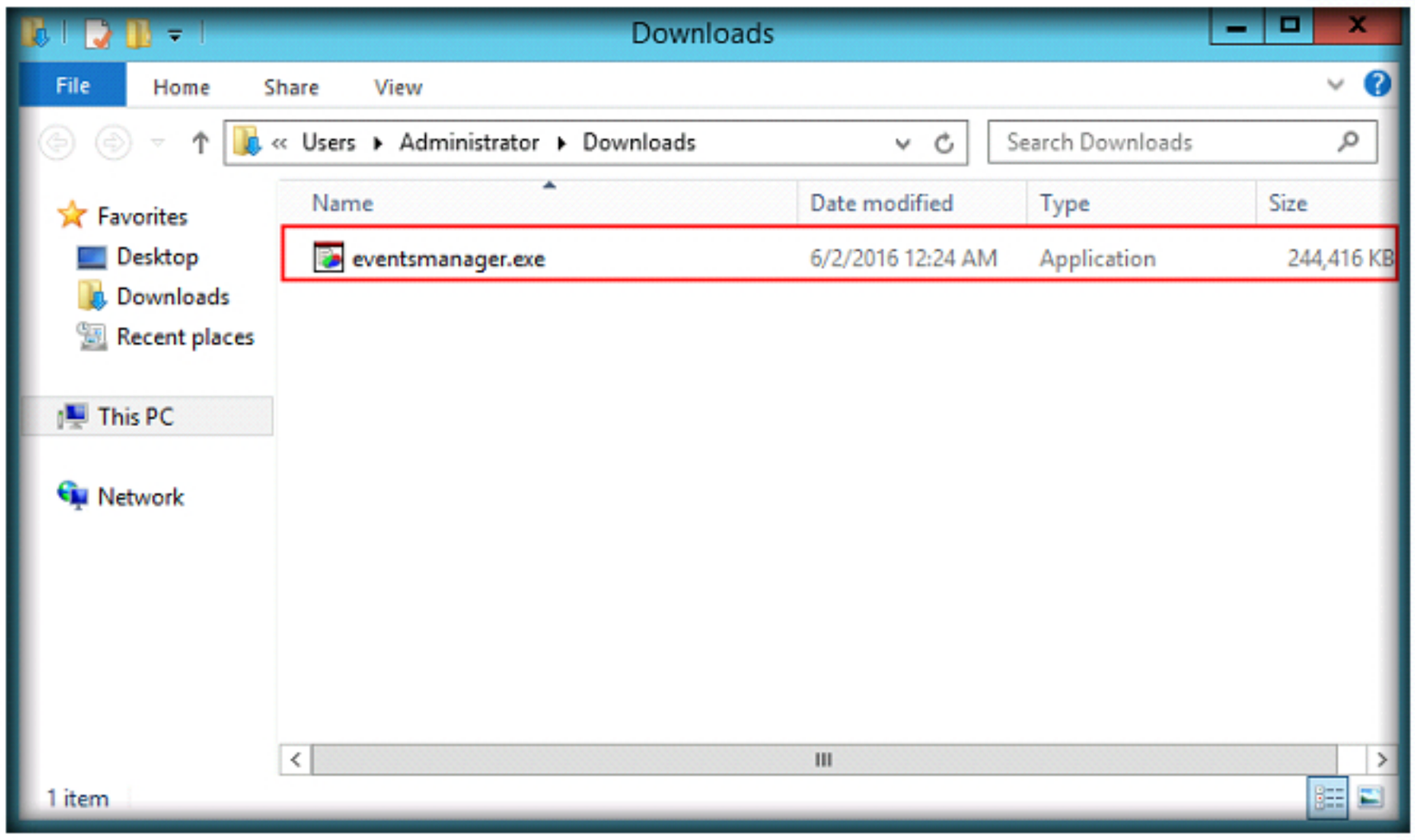

FIGURE 1.4: GFI EventsManager installer

TASK 2

Running the GFI EventsManager

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

6. GFI EventsManager wizard appears, click **Install**.

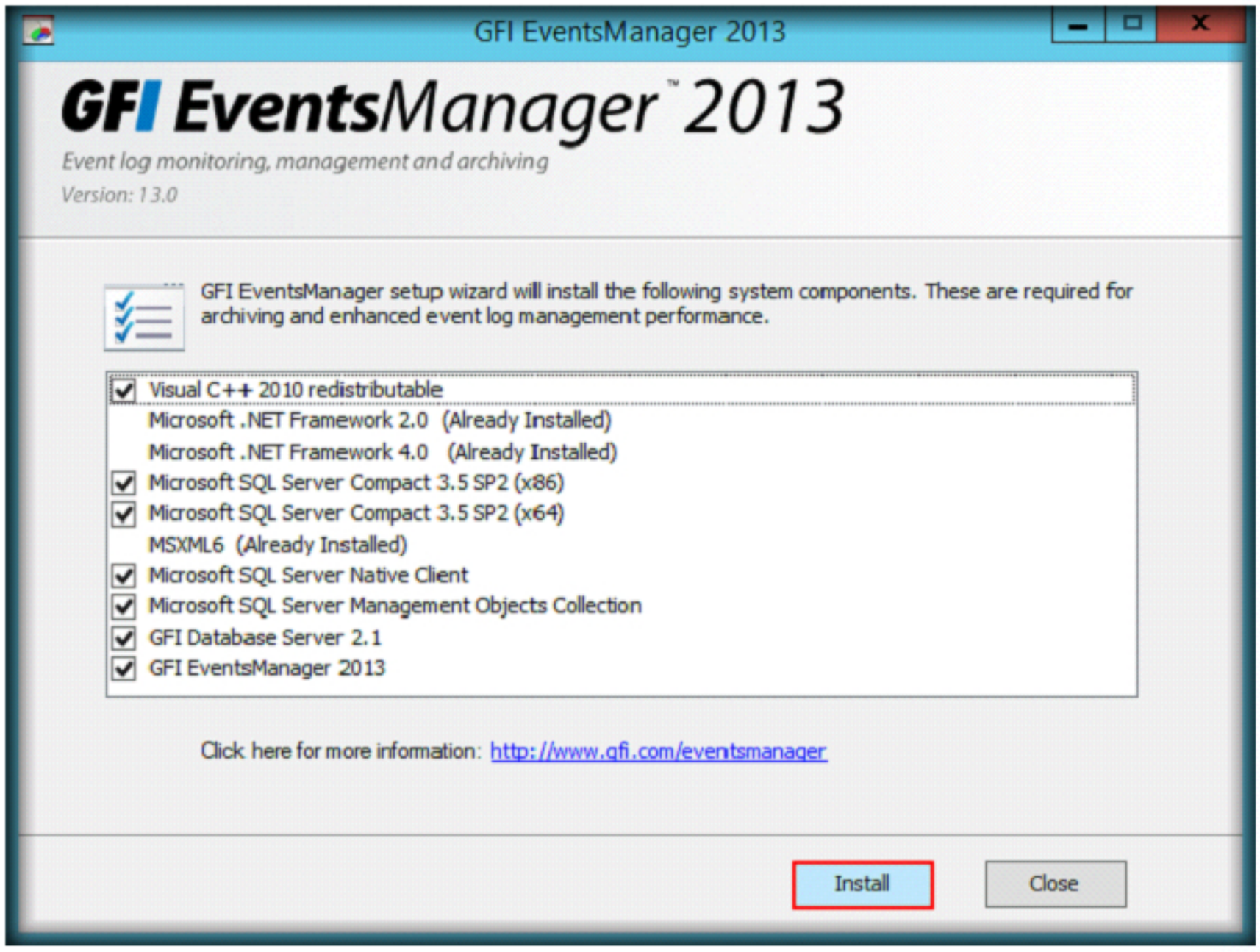

FIGURE 1.5: GFI EventsManager wizard

7. The applications that are already installed in the machine will be skipped. Installation wizard appears for those applications which have not been

installed on the machine. Follow the wizard driven installation steps to install those applications.

8. Once all the prerequisites are installed, **GFI EventsManager Setup** wizard appears, click **Next**.

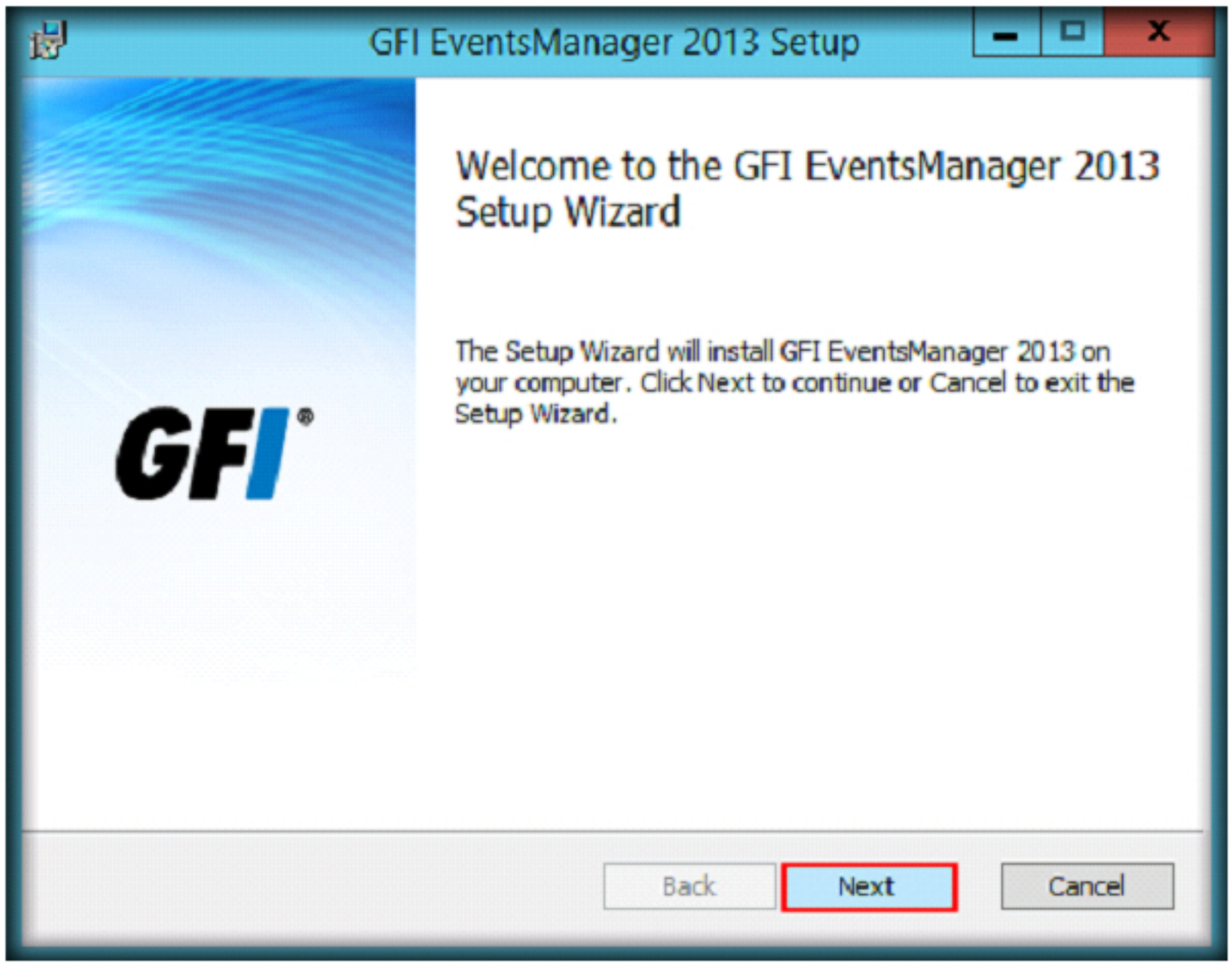

FIGURE 1.6: GFI EventsManager Setup wizard

9. In the next step of the wizard, accept the license agreement and click **Next**.

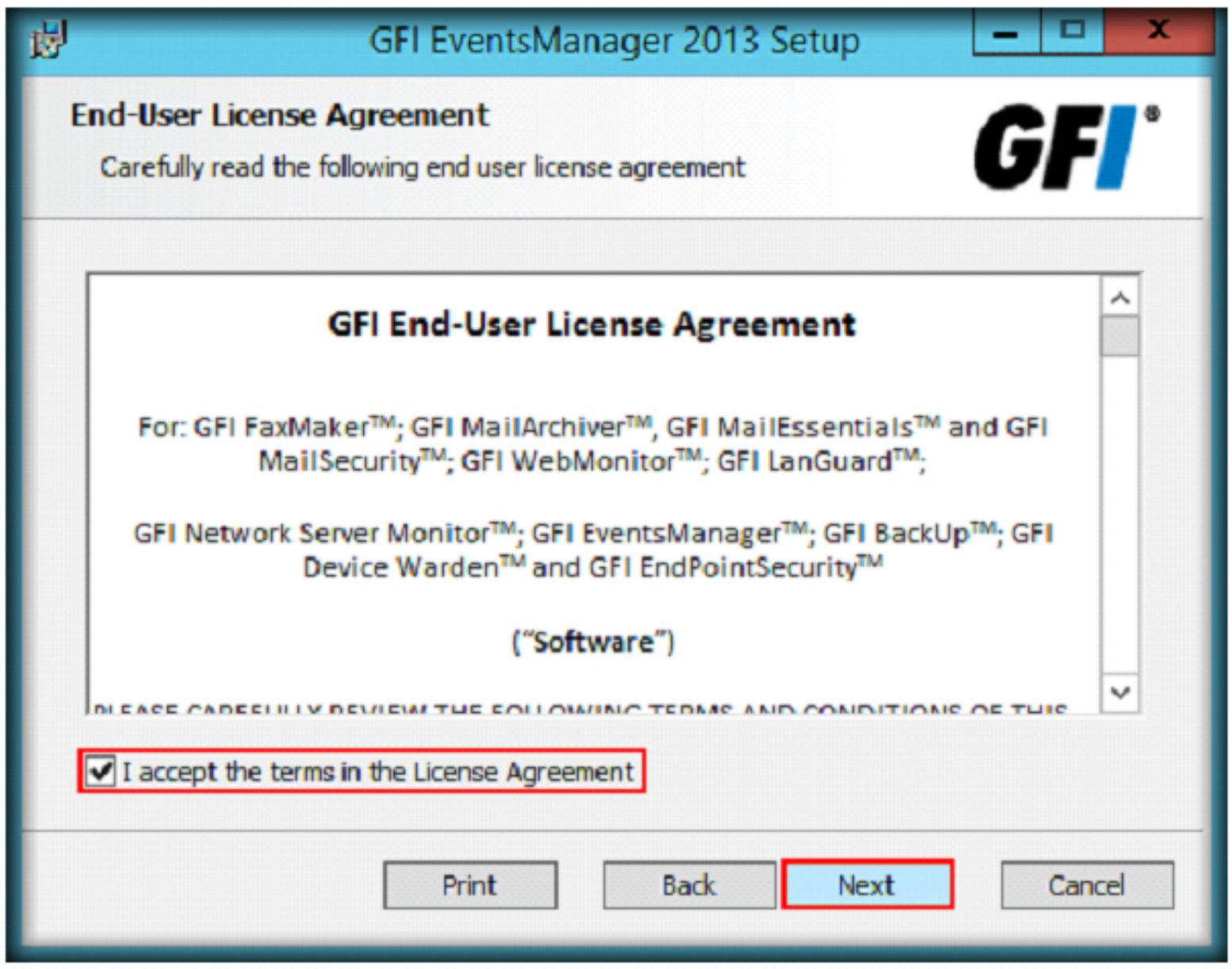

FIGURE 1.7: GFI EventsManager Setup License Agreement wizard

10. Customer Information section appears, enter the **License Key** sent to your respective Email ID and click **Next**.

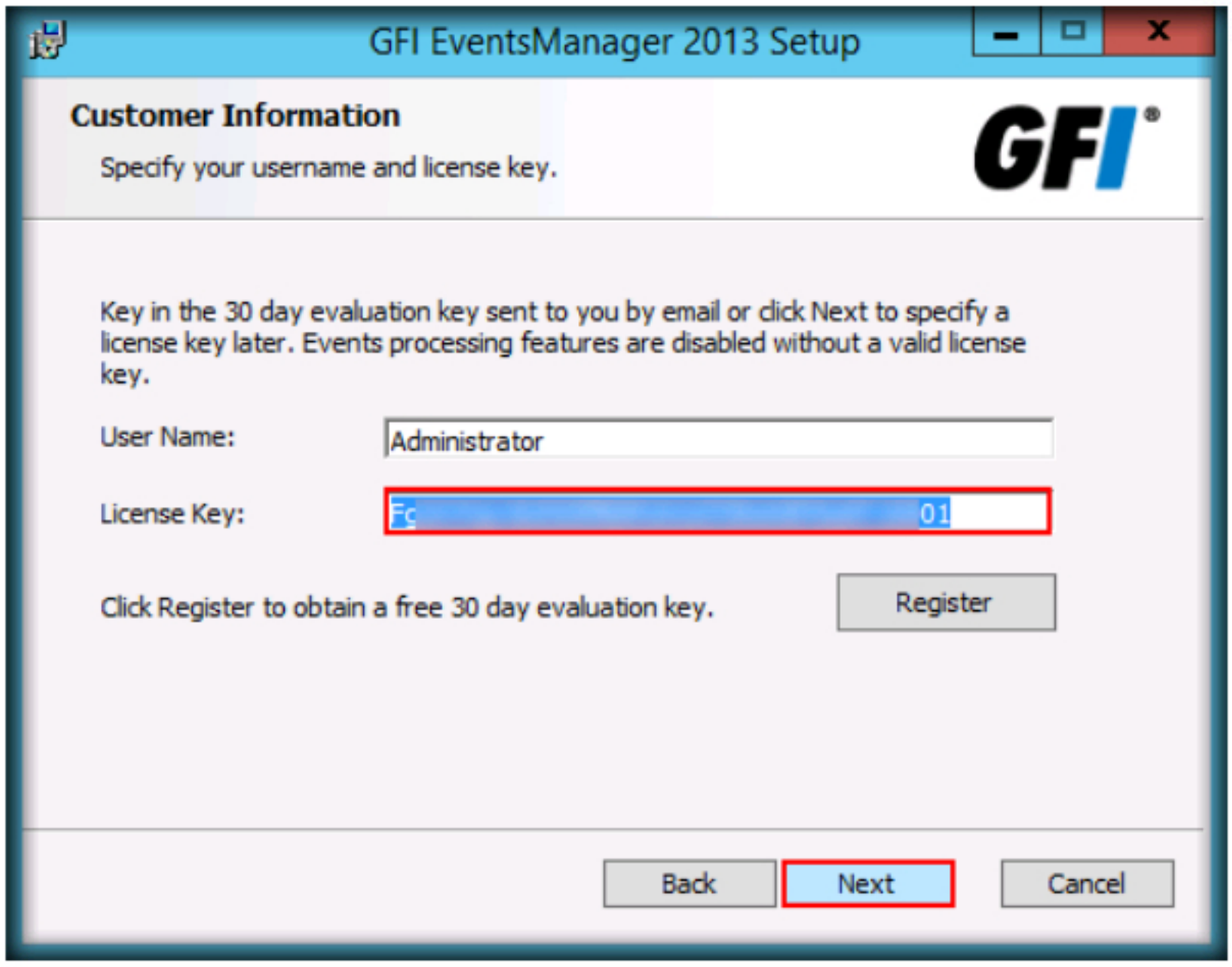

FIGURE 1.8: GFI EventsManager Customer Information section

11. Logon Information appears, enter the password of Windows Server 2012 virtual machine in **Password** field and click **Next**.

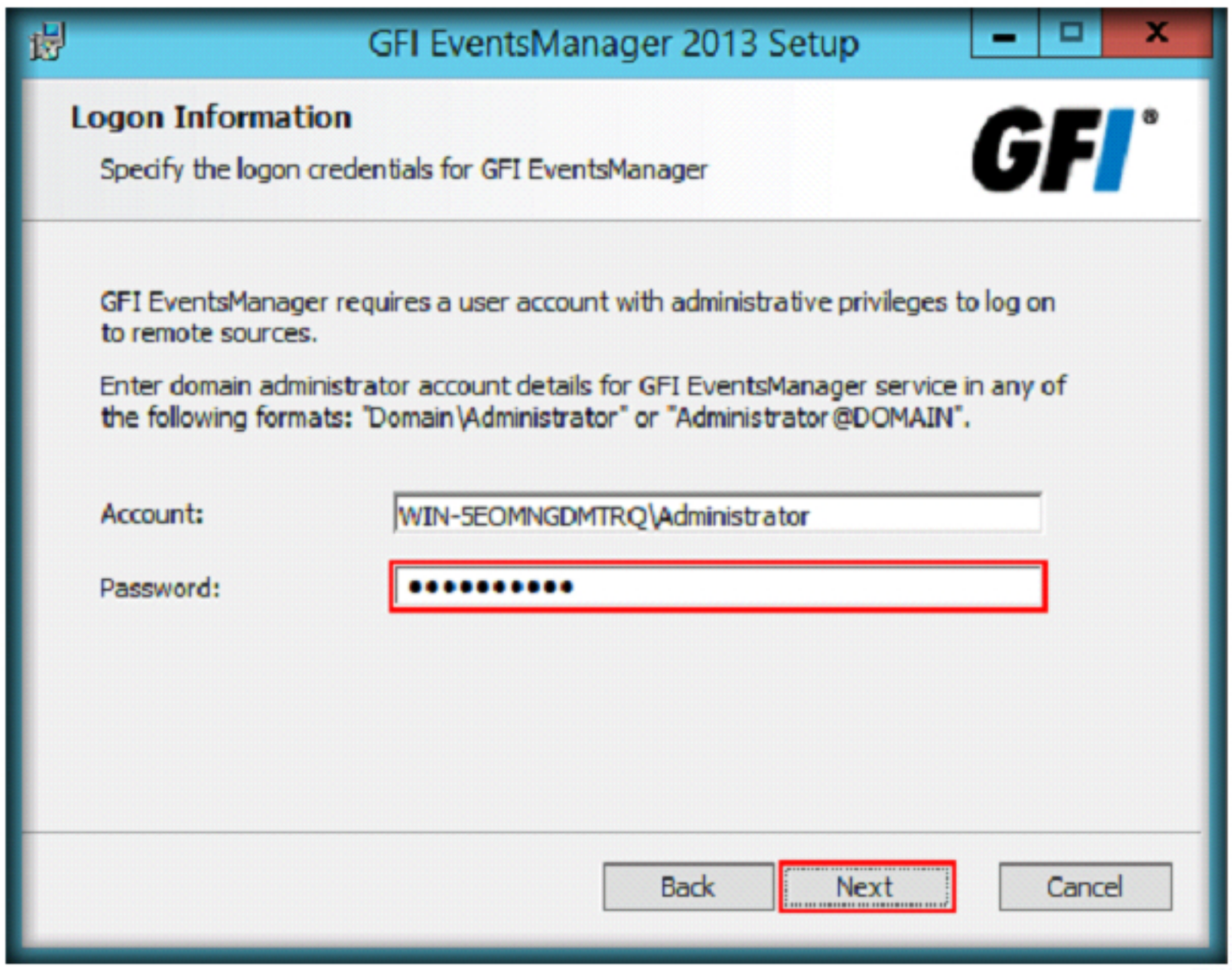

FIGURE 1.9: GFI EventsManager Logon Information

12. Follow the wizard driven installation steps to install GFI EventsManager.

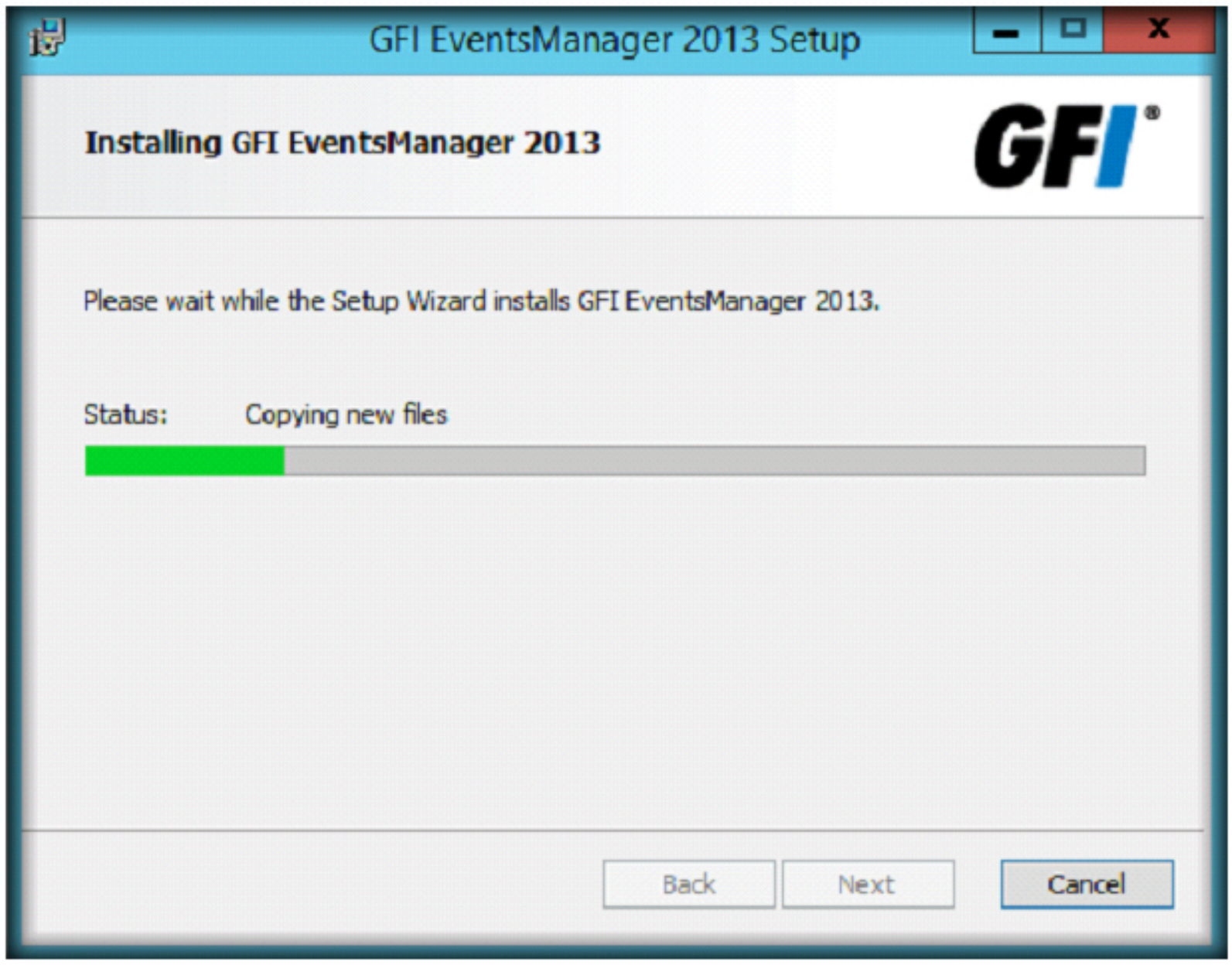

FIGURE 1.10: GFI EventsManager installation

13. On completing the installation, click **Finish**.

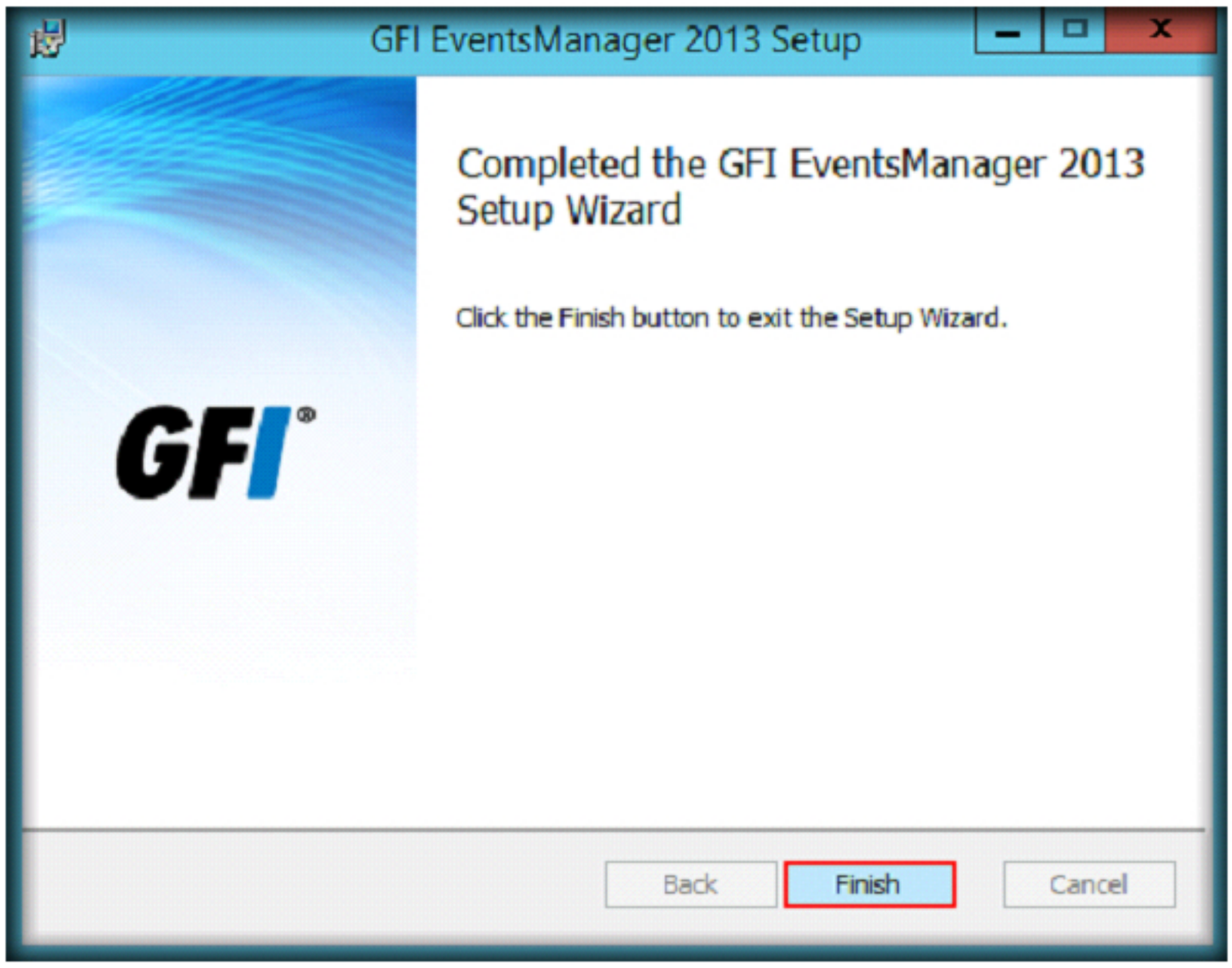

FIGURE 1.11: GFI EventsManager installation completion

14. The application begins to download and install updates as shown in the following screenshot:

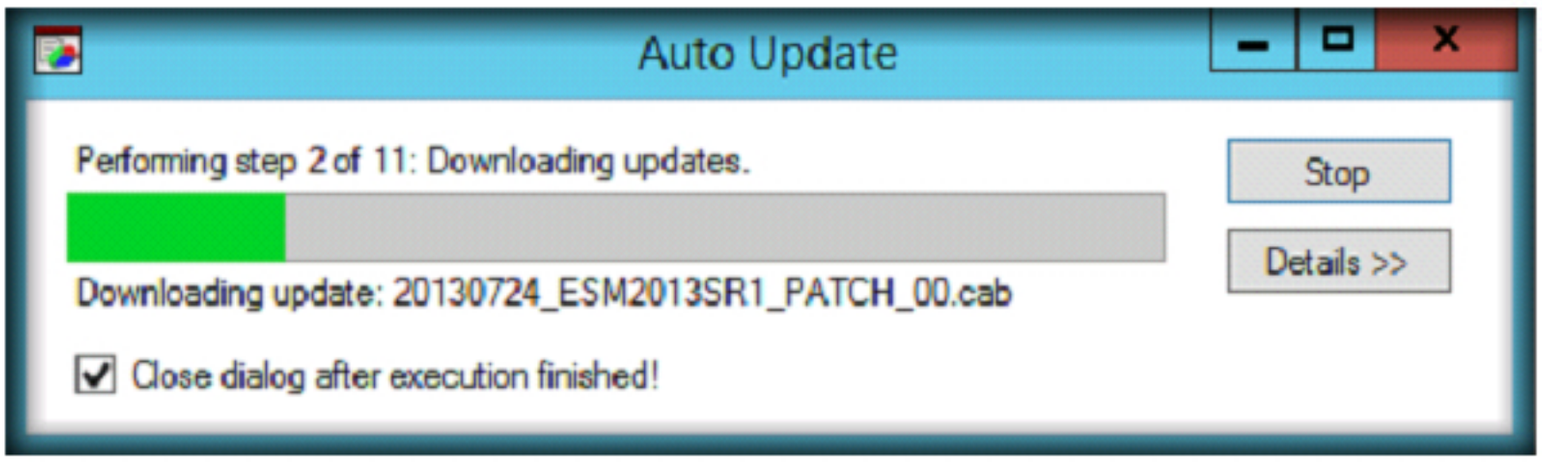

FIGURE 1.12: GFI EventsManager download

15. **Switch Database Server** dialog-box appears, click **OK** to use the Database Server on Windows Server 2012 virtual machine.

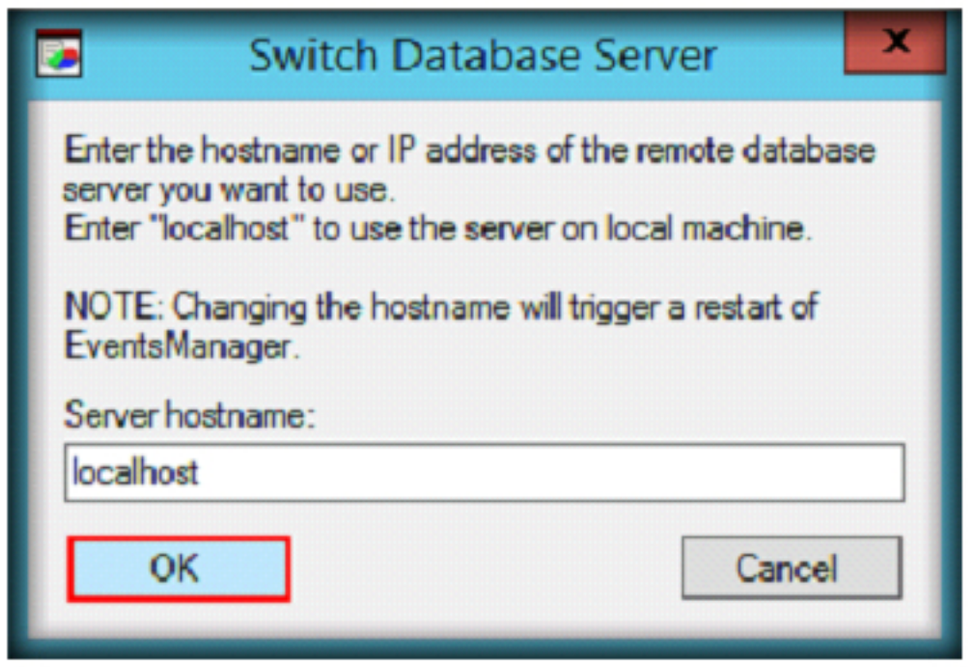

FIGURE 1.13: Switch Database Server dialog-box

TASK 3

Launching the GFI EventsManager

16. GFI EventsManager main window appears, with a pop-up displayed on it. The pop-up contains the trial period related information. Click OK to close the pop-up.

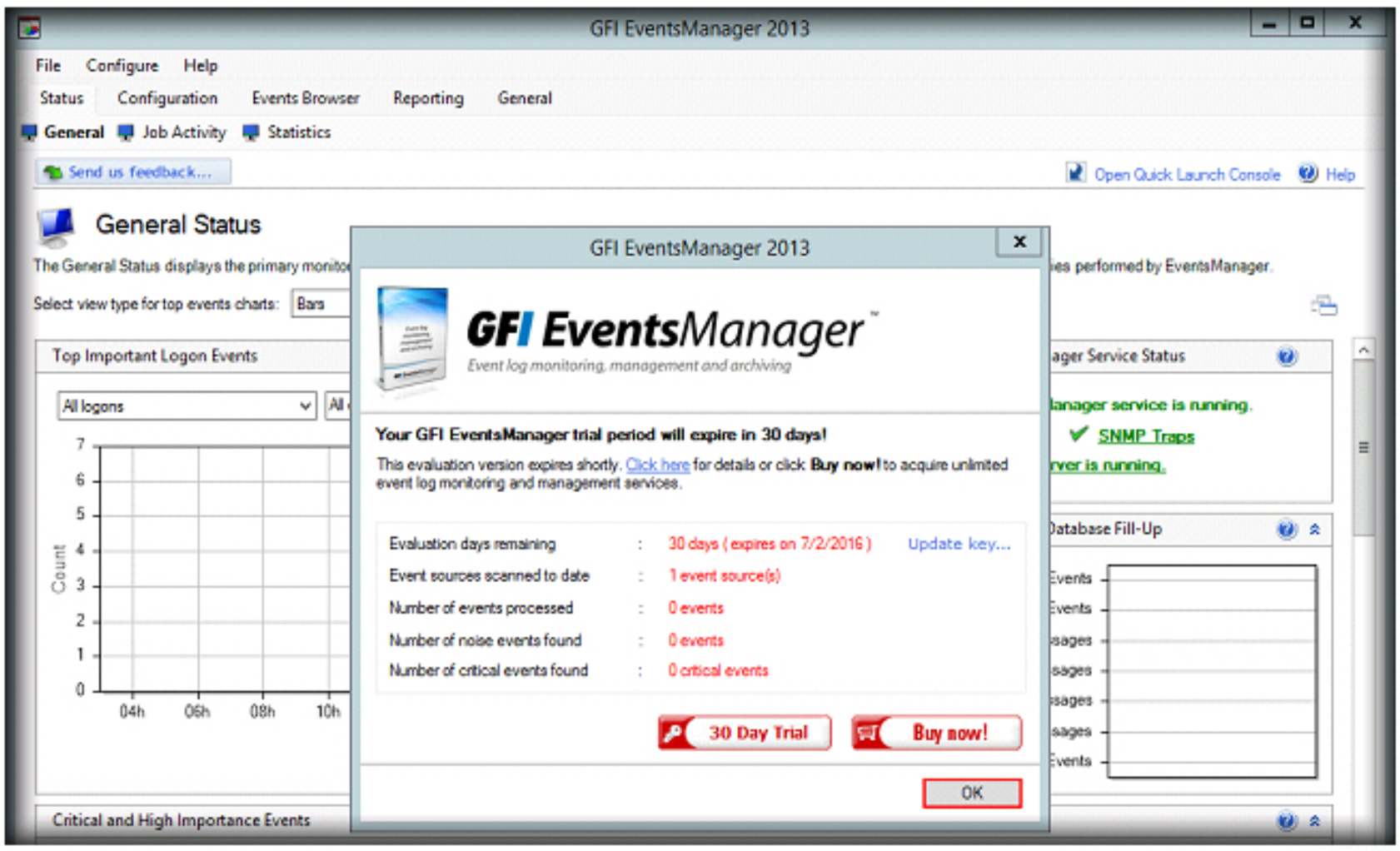

FIGURE 1.14: GFI EventsManager main window

TASK 4

Processing Events of Local Computer

17. Quick Launch Console appears on the GFI EventsManager 2013 GUI.
18. Select the **Process events - Local computer** option in the **Quick Launch Console** to collect events from the local computer. Processing starts automatically.

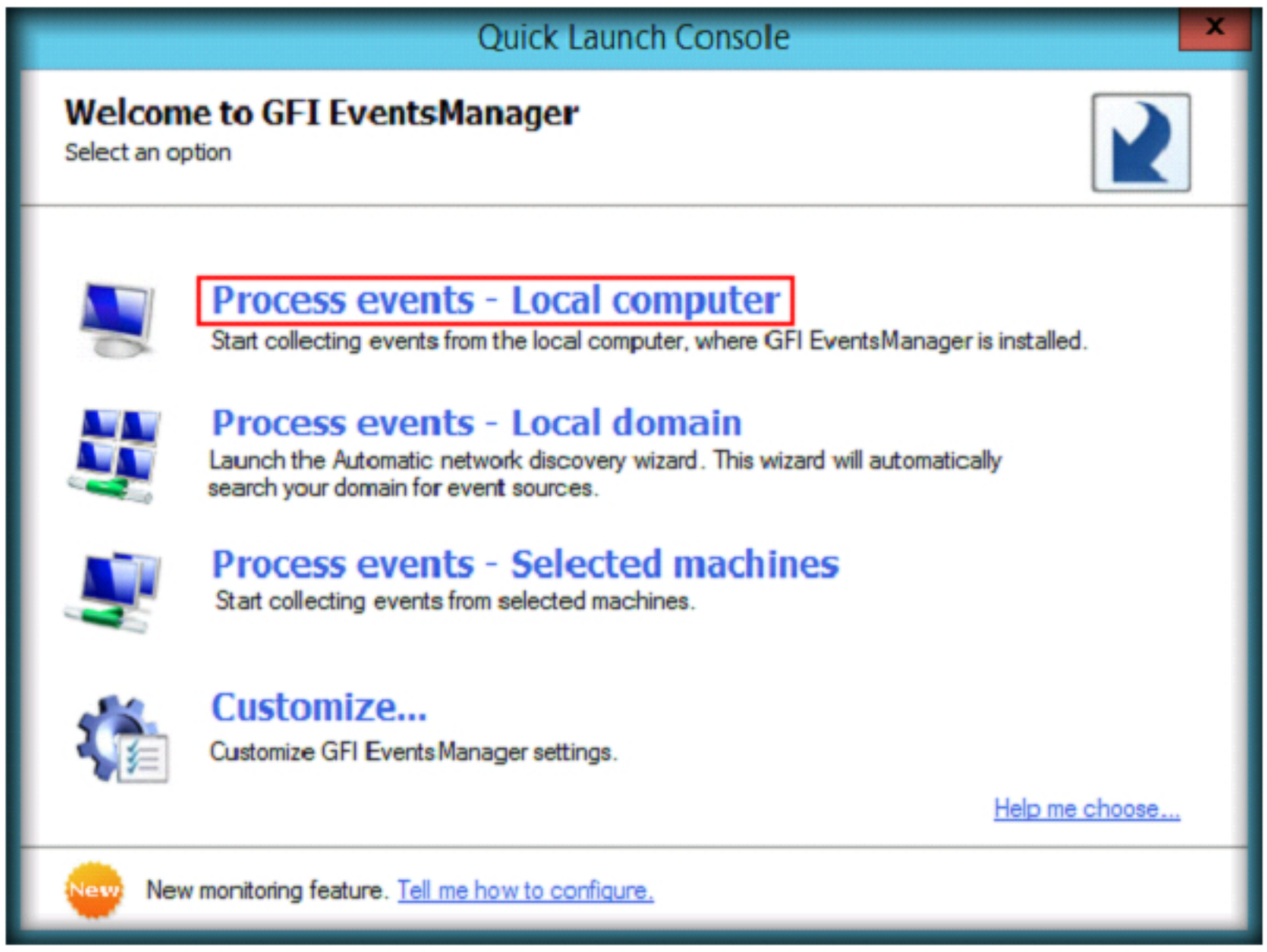

FIGURE 1.15: GFI EventsManager Process events - Local computer option

The event log analysis of GFI EventsManager includes SNMP traps, Windows event logs, W3C logs, SQL Server and Oracle audit logs, and Syslog.

19. When processing is finished, the **Quick Launch Console** displays the number of events processed, at the bottom of the dialog.

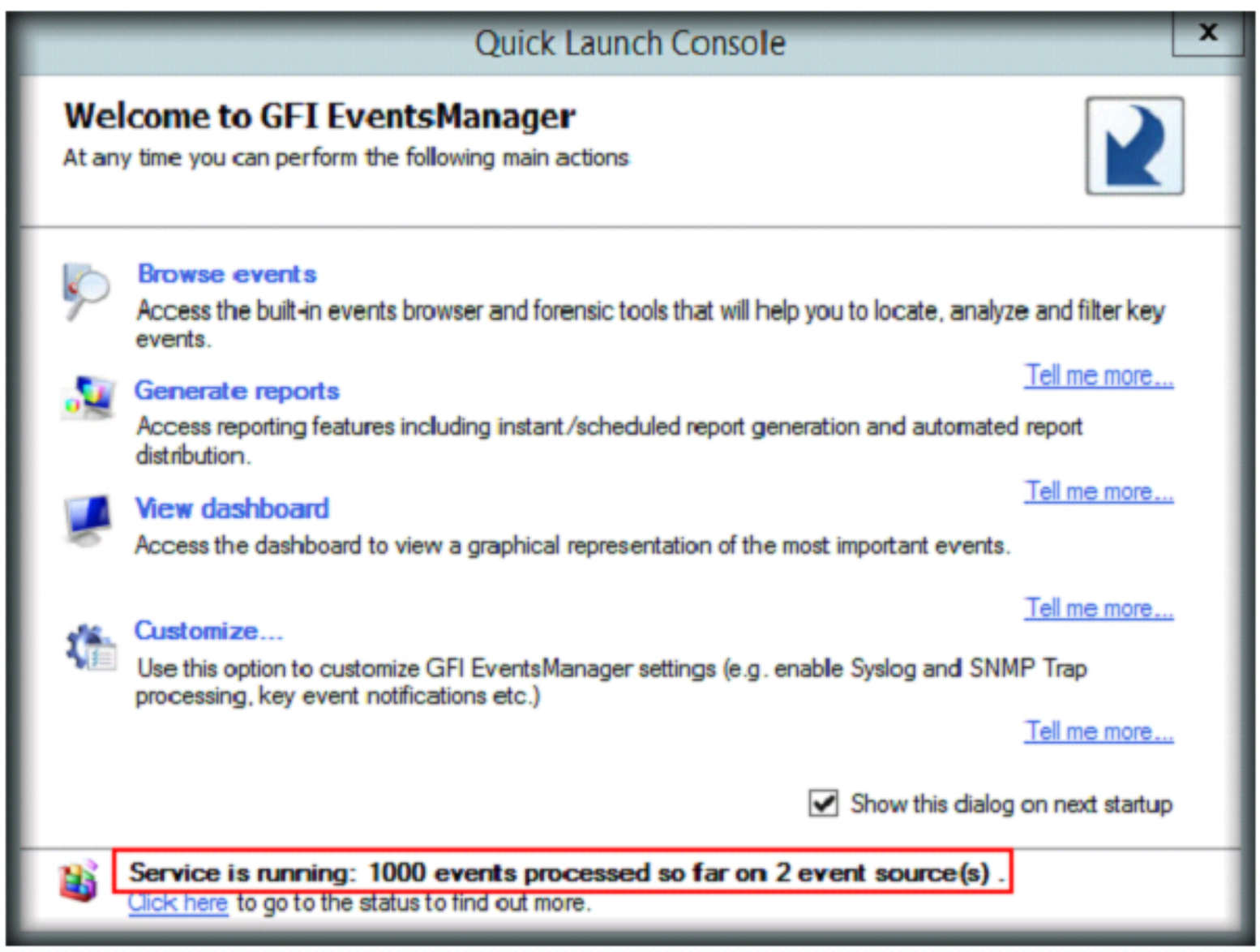

FIGURE 1.16: GFI EventsManager displaying the number of events processed

You can create processing rules and filters for Windows events by simply right-clicking on event details in the Events Browser tool.

TASK 5

Analyzing Events

The GFI EventsManager dashboard includes a number of filtering-enabled charts to provide administrators with fast and easy access to the data they seek.

20. From the **Quick Launch Console** wizard, click **Browse events** to see the events.

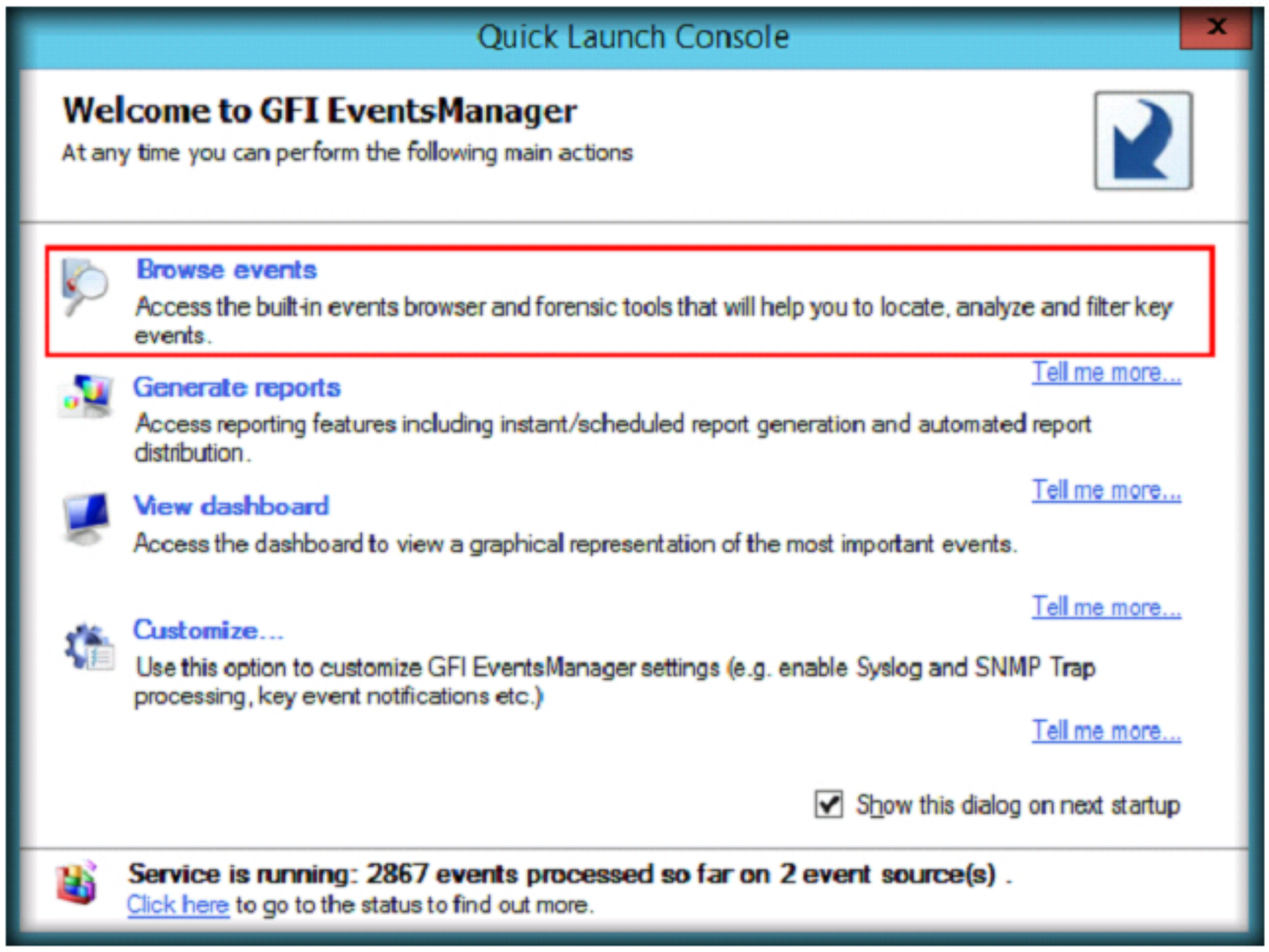

FIGURE 1.17: GFI EventsManager Quick Launch Console window

21. Close the **Quick Launch Console**.

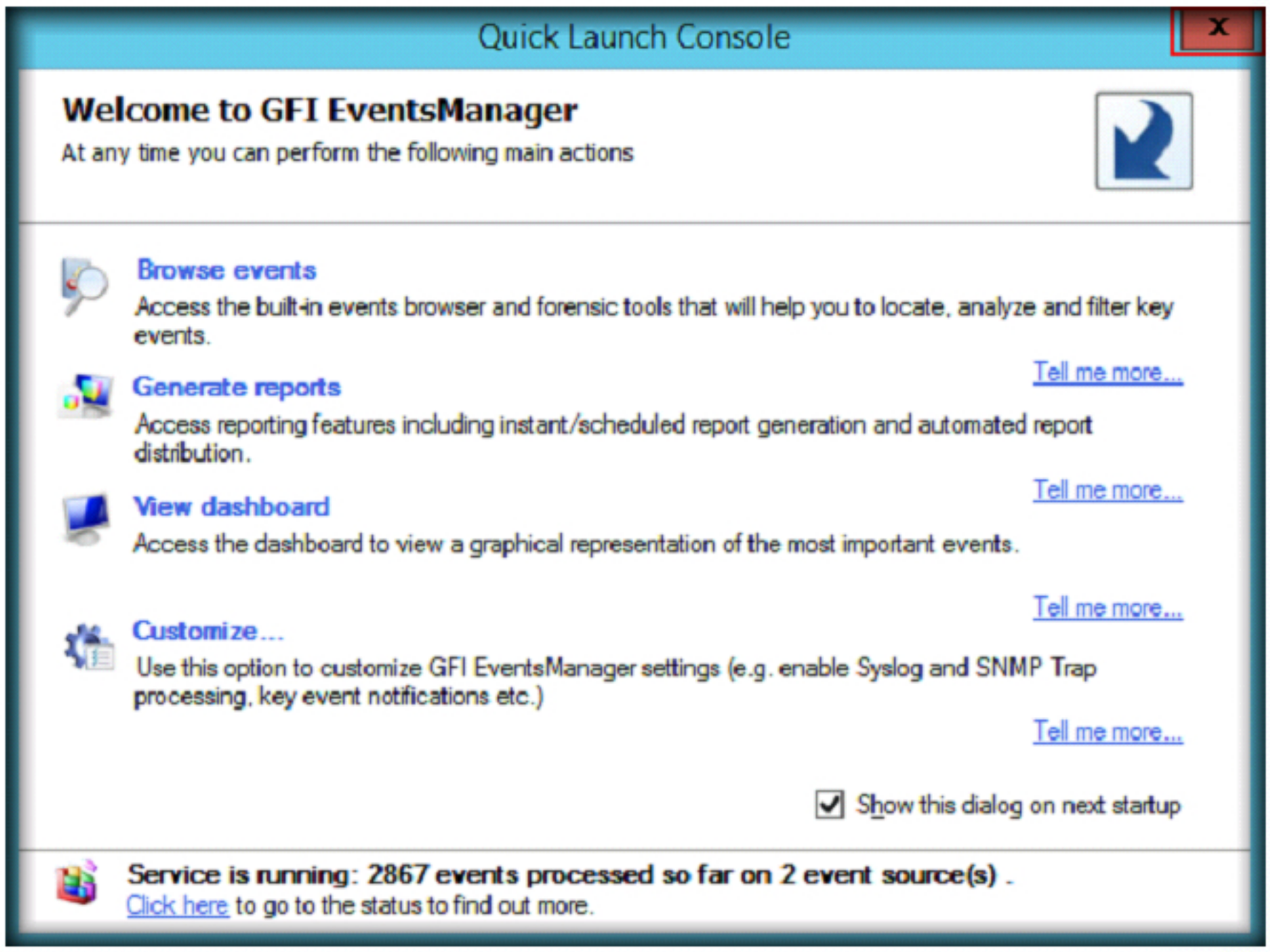

FIGURE 1.18: GFI EventsManager close Quick Launch Console window

22. GFI EventsManager displays all the events as shown in the following screenshot:

GFI EventsManager can process Oracle audit records for versions 9i, 10g, and 11g.

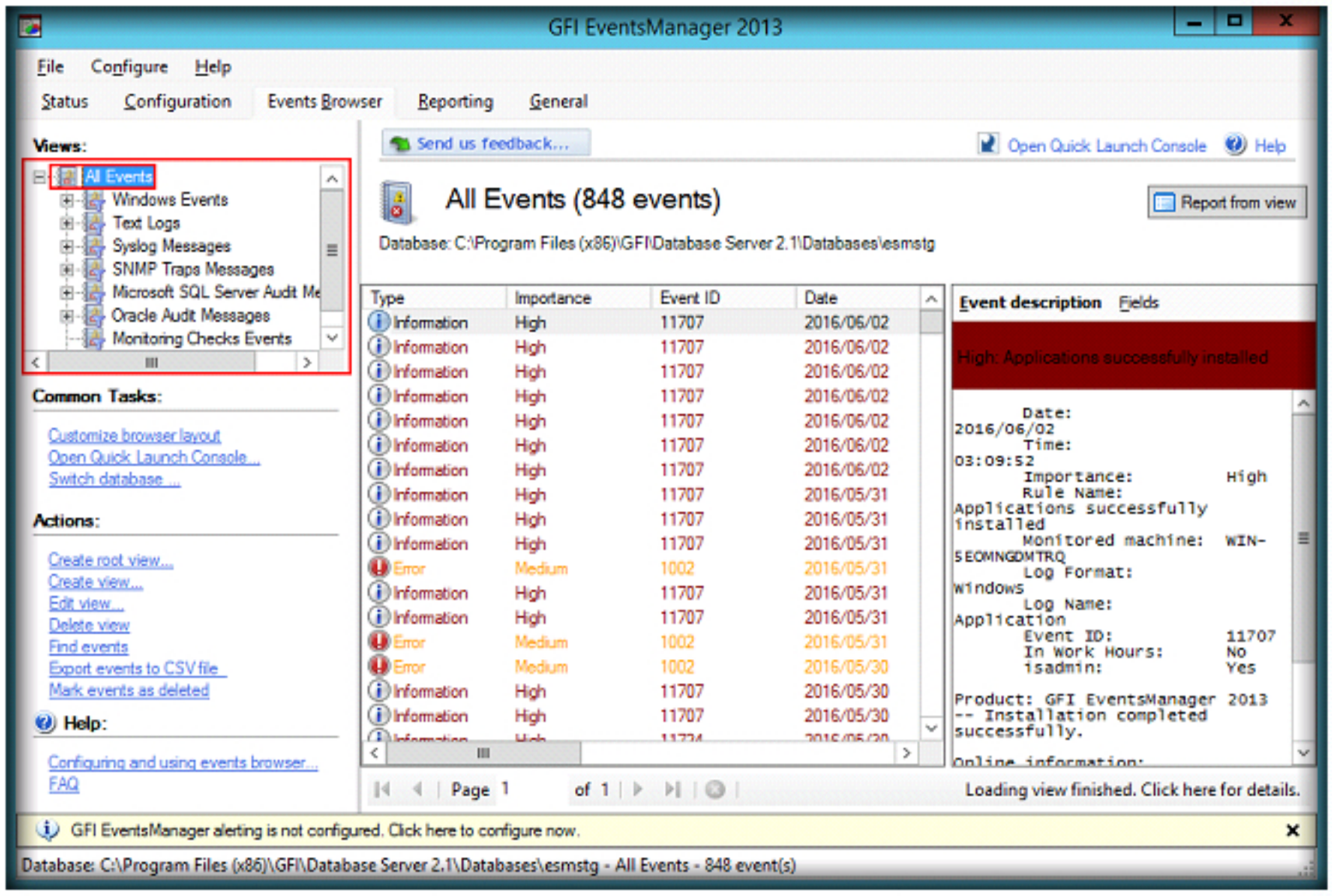

FIGURE 1.19: GFI EventsManager Events Browser

23. Expand **Windows Events** node, and click **Security Events** to view all the security events in the **log viewer**.

24. You can also see only the logs related to any subcategories under **Security Events** node, by expanding the node.

Archived data can reside on a SQL Server database or in secured and compressed files.

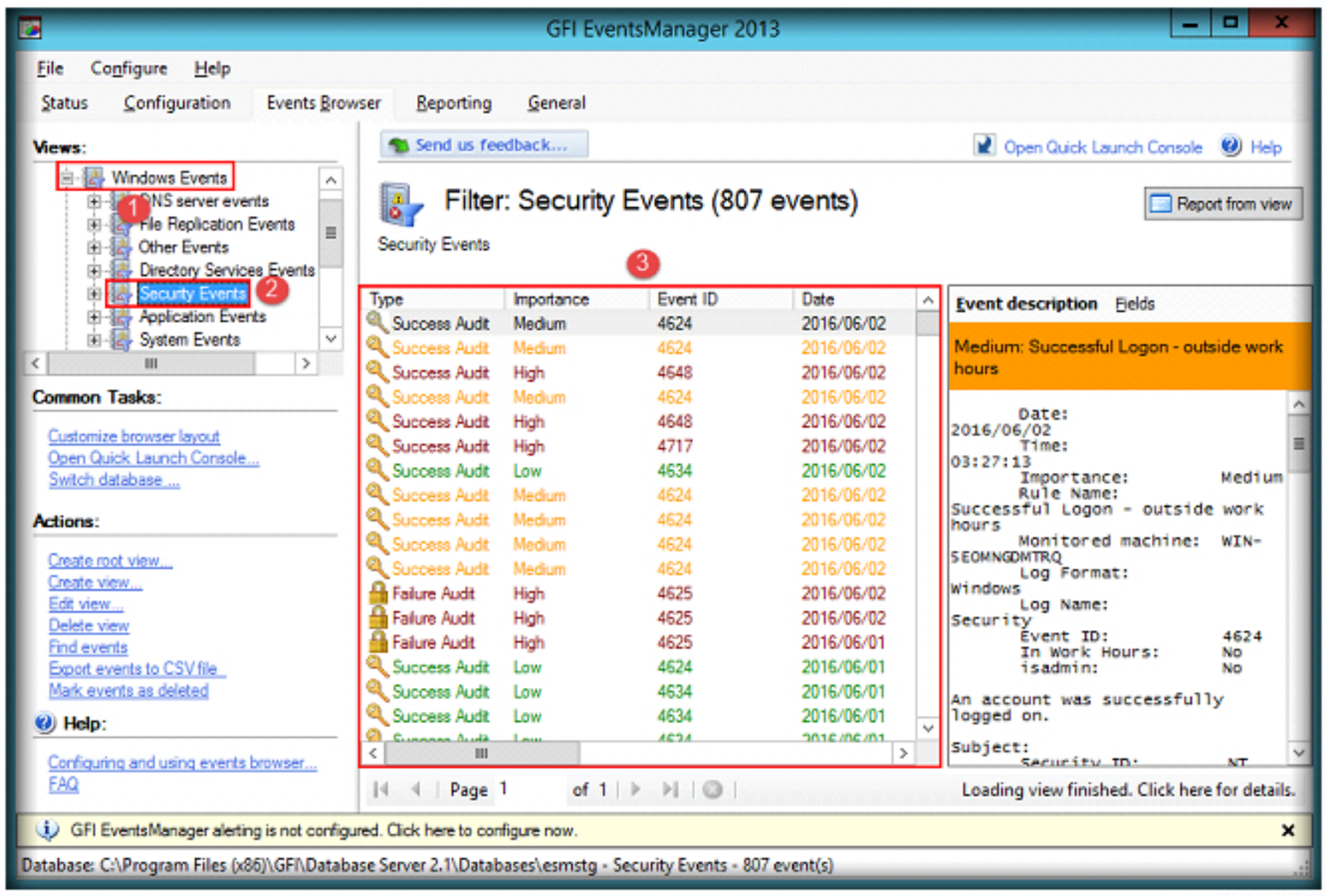

FIGURE 1.20: GFI EventsManager security events

25. Select any event among the event logs to view the details under the **Event description** section in right-pane.

GFI EventsManager has improved alert level for key events or intrusions detected on the network.

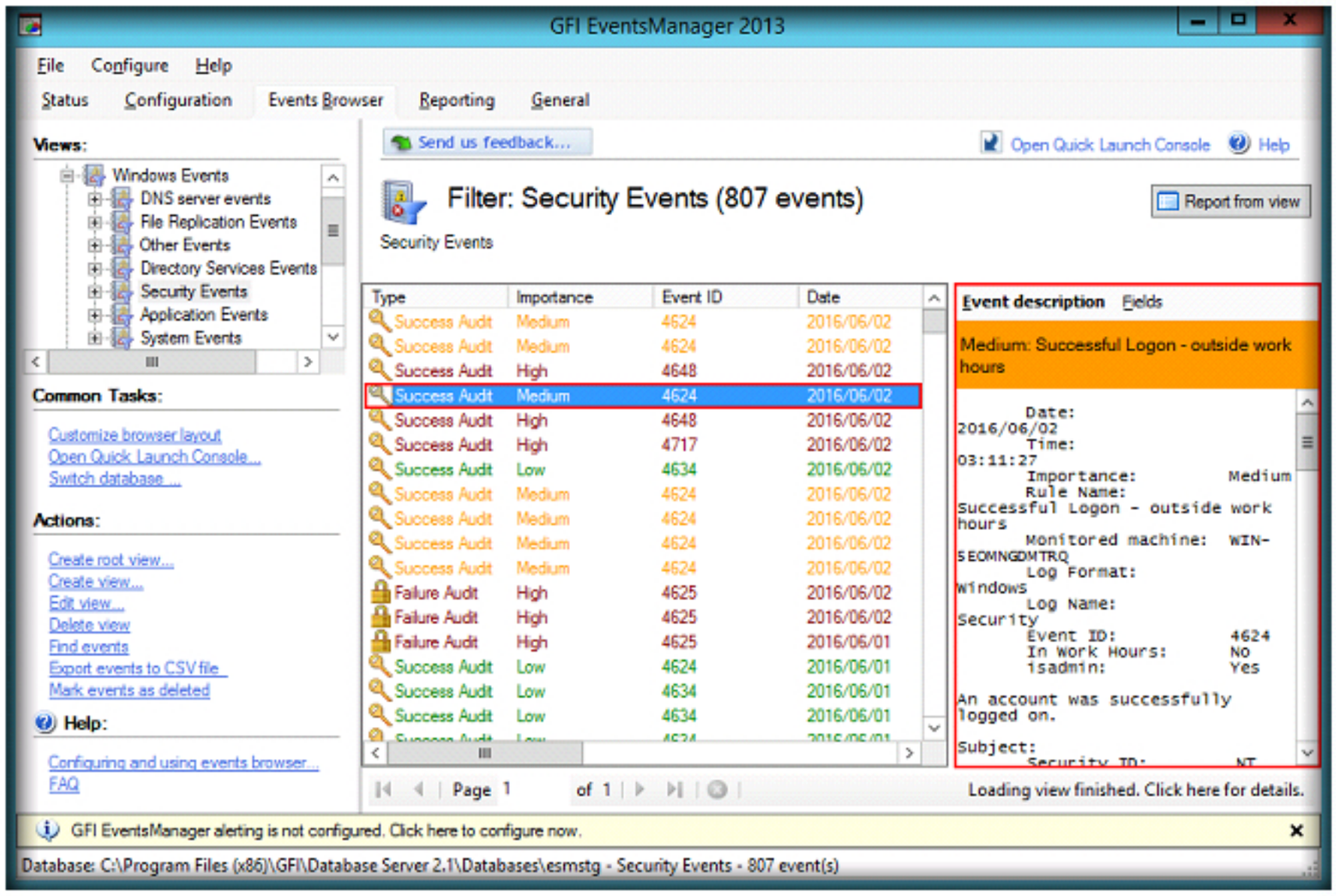

FIGURE 1.21: GFI EventsManager Events Browser

26. Expand the **Application Events** node, and click **Application Events** to see all the application events in the **log viewer** pane.

GFI EventsManager is a log processing solution that provides network-wide control and management of Windows event logs, W3C logs, SQL Server and Oracle audit logs, and Syslog events generated by your network sources.

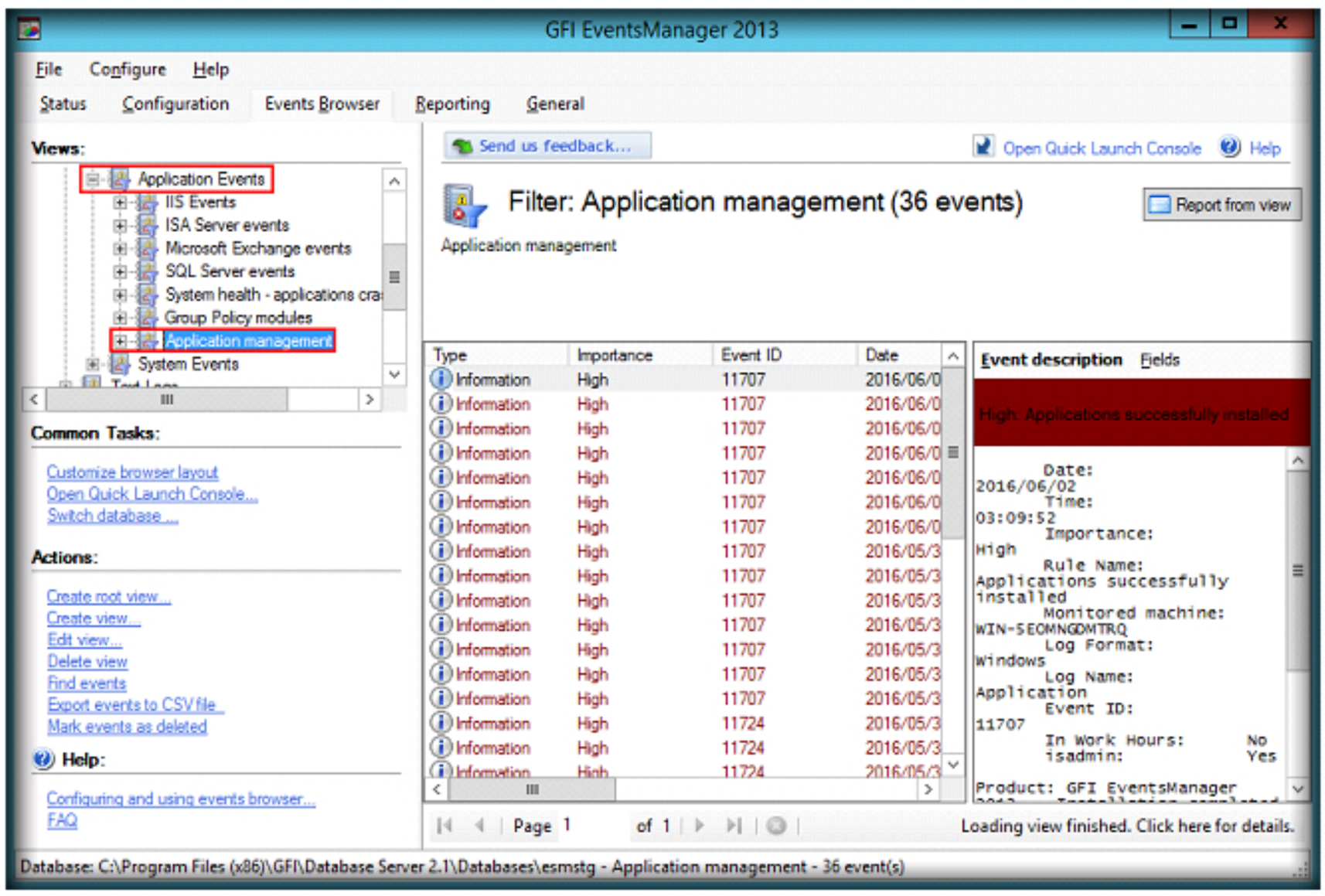

FIGURE 1.22: GFI EventsManager application events

27. Select the **System Events** node to view all the event logs pertaining to **System Events**. You may expand this node to view the sub nodes associated with it.

GFI EventsManager supports Simple Network Management Protocol, the language spoken by low-level devices such as routers, sensors, firewalls, etc.

GFI EventsManager allows you to trigger actions such as sending alerts to one or more people by email, network messages, SMS notifications sent through an email-to-SMS gateway or service, and includes SNMPv2 traps.

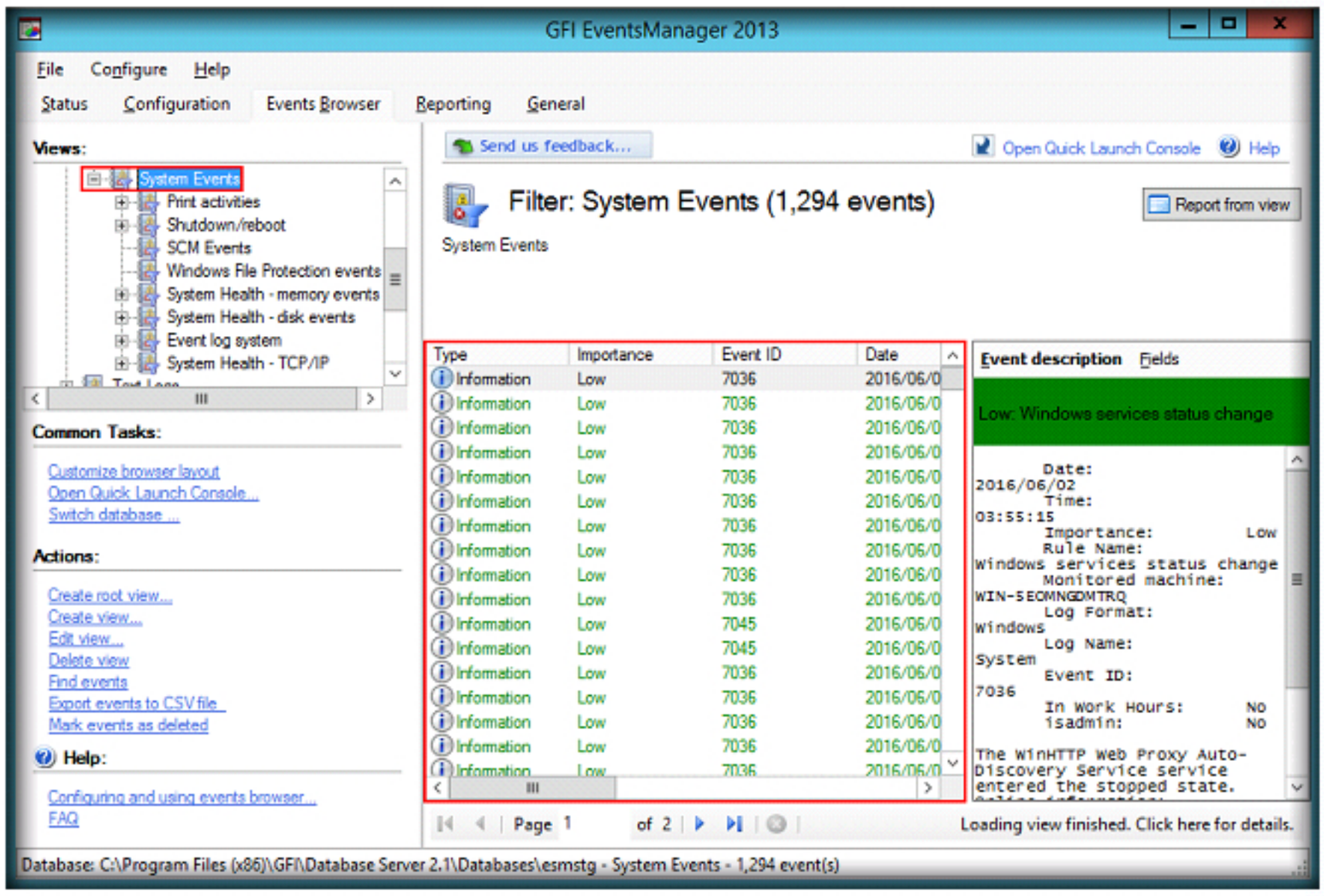

FIGURE 1.23: GFI EventsManager all events

28. You may select an event from the **log viewer** pane, and from the **Actions** pane. Select any action to perform on selected events.

GFI EventsManager offers a compelling view of the security status of your network and delivers better compliance reports by integrating key information provided by GFI LanGuard and GFI EndPointSecurity. This information refers to vulnerabilities, unauthorized applications, removable device usage, and more.

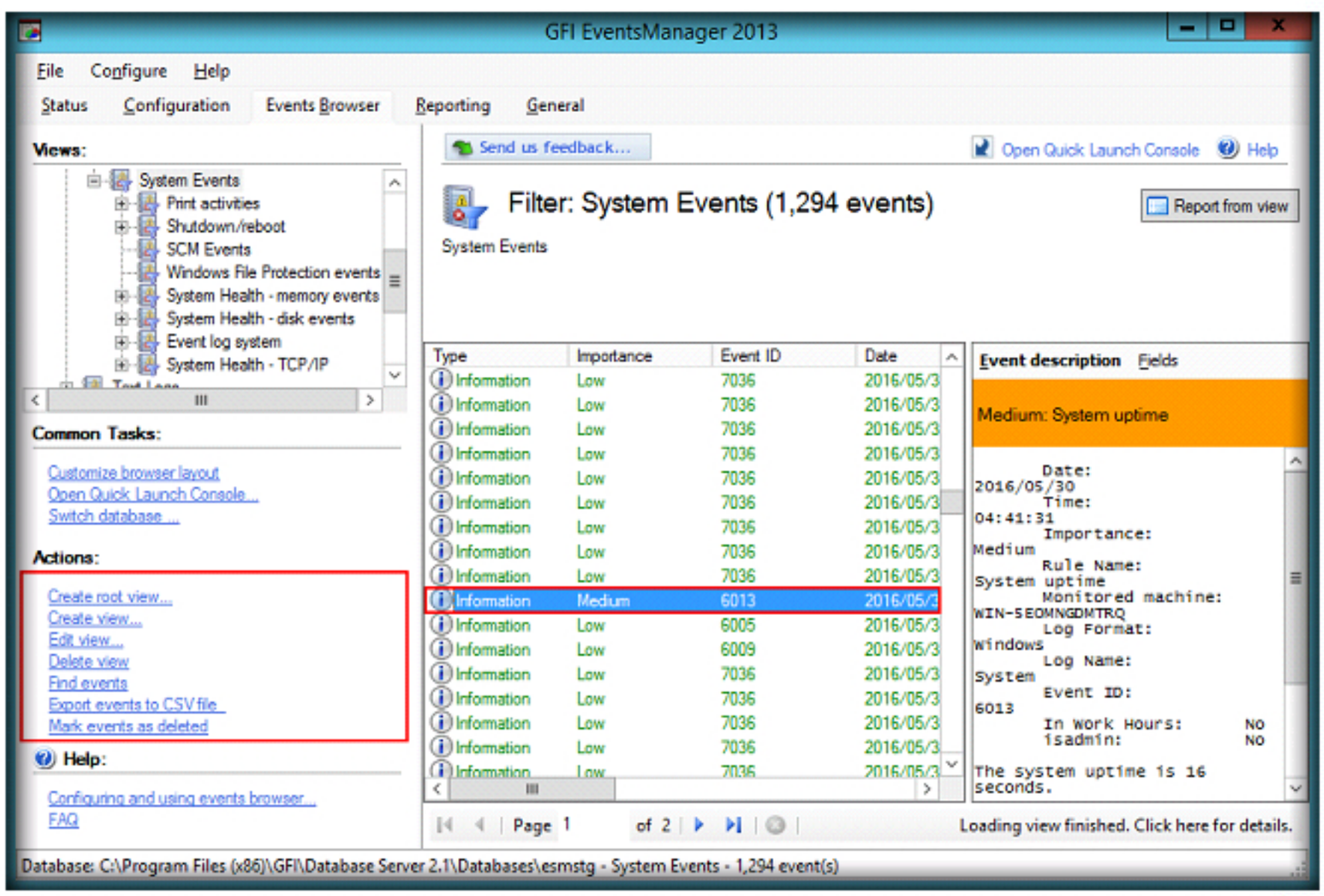

FIGURE 1.24: GFI EventsManager actions

TASK 6

Monitoring Status

GFI EventsManager collects and archives logs generated by most of your network systems, servers, and applications.

29. To create a report for all the events, click **All Events** node and then, click **Report from View**.

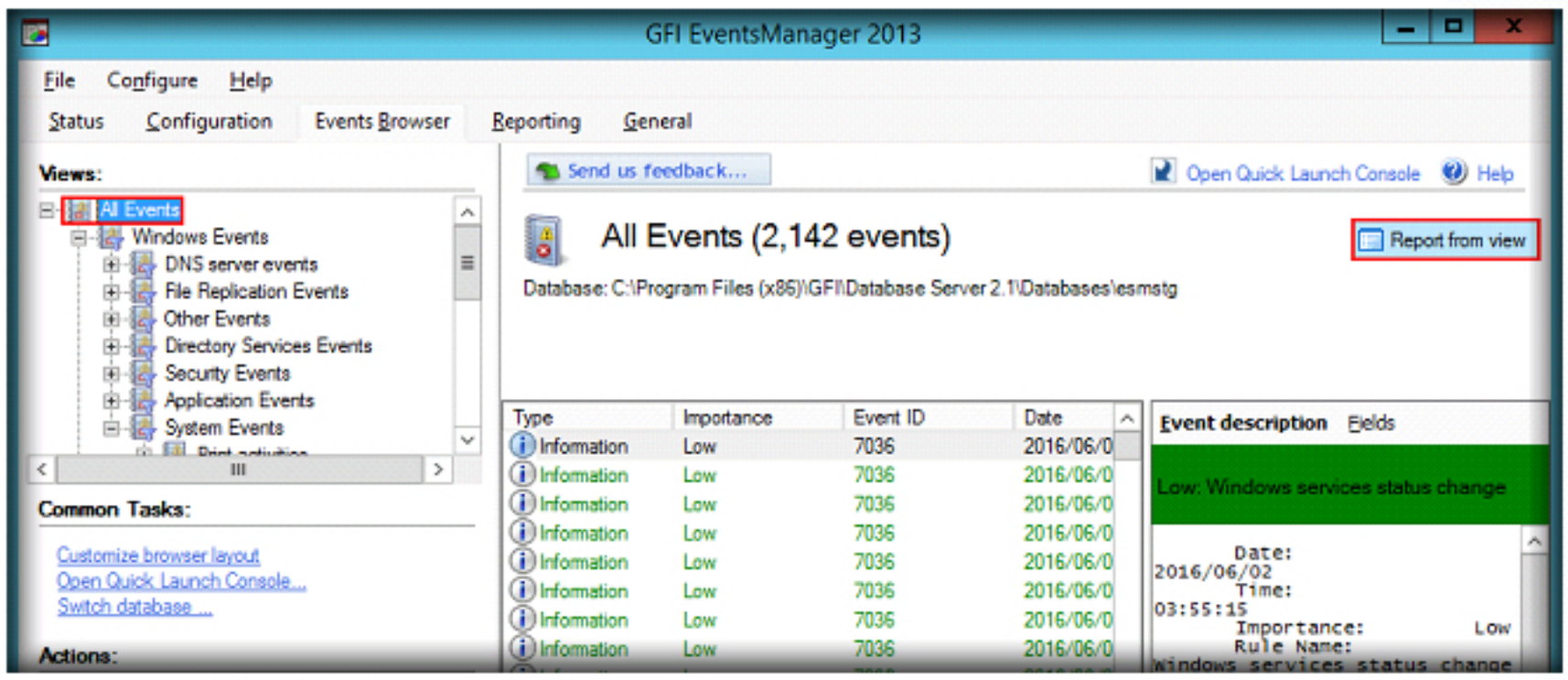

FIGURE 1.25: GFI EventsManager exporting view to HTML

30. **Create Report** window appears, select **Options** tab, assign a location to save the file, click **Apply** and click **OK**.

Note: In this lab, a folder named **Report for Events** is created on **Desktop**, and this location is given as **Target path** to save the file.

When you click Apply, if a **GFI EventsManager 2013** dialog-box appears stating that "No conditions have been defined", click **Yes** to continue.

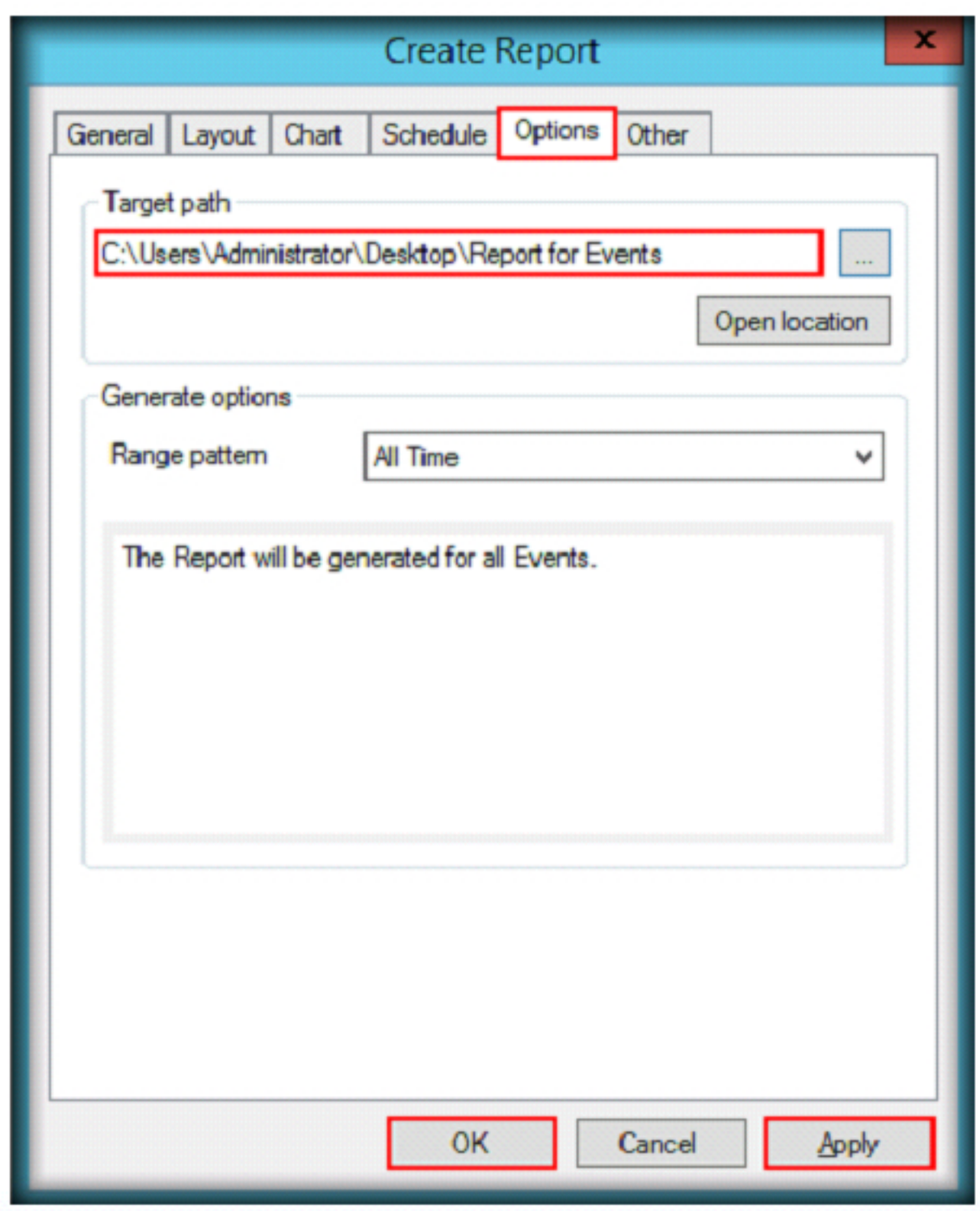

FIGURE 1.26: GFI EventsManager Create Report window

31. GFI EventsManager creates an HTML report containing all events.
32. Once the report is created, it appears under the **Generated Reports** section in **yyyymmdd-hhmmss** format. Select the report and click **Open** to view the report.
33. Alternatively, you may navigate to the location where you saved the report, and double-click the file to view it.

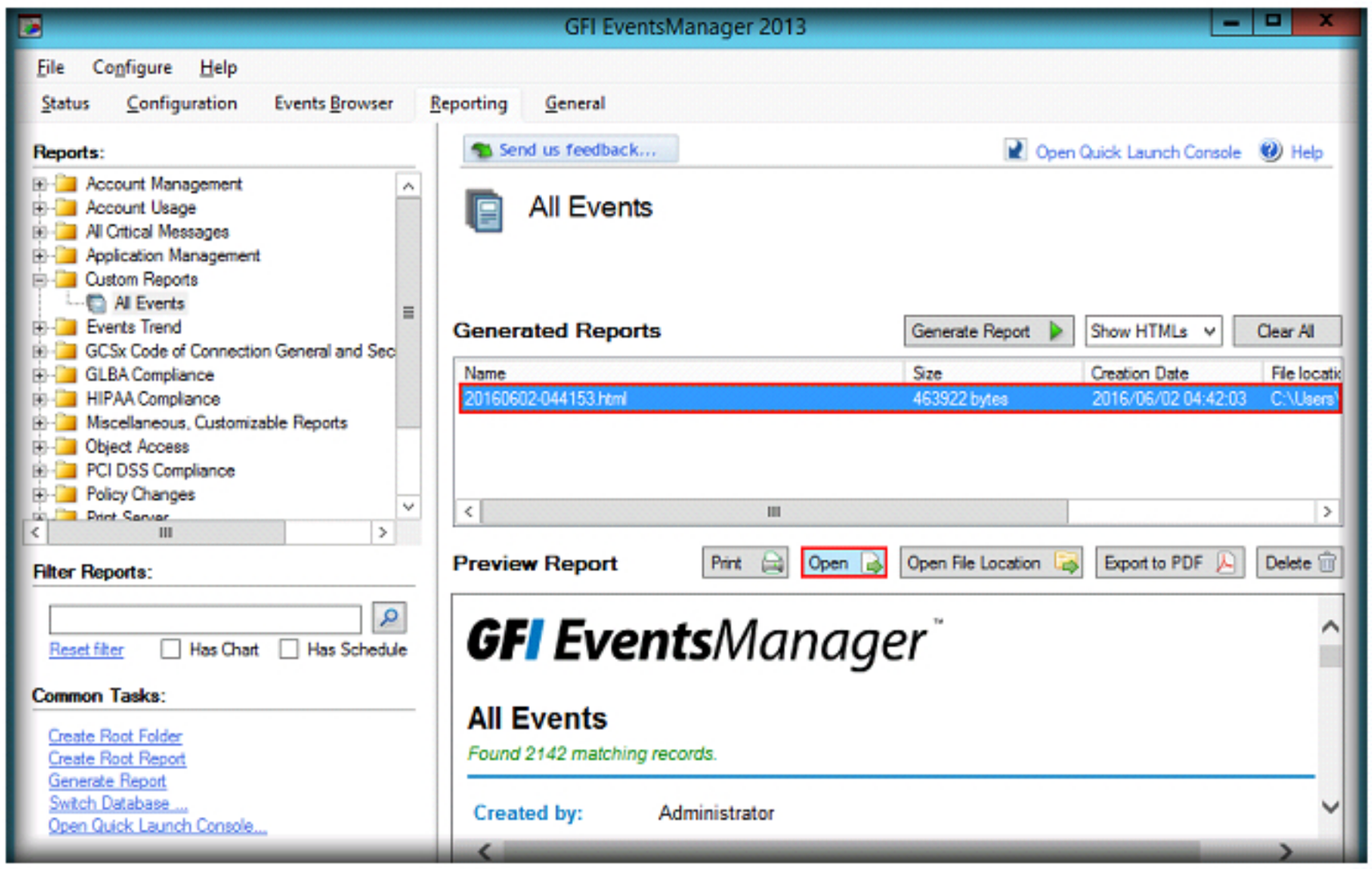

FIGURE 1.27: GFI EventsManager Generated Reports section

34. The report appears in a default web browser as shown in the following screenshot:

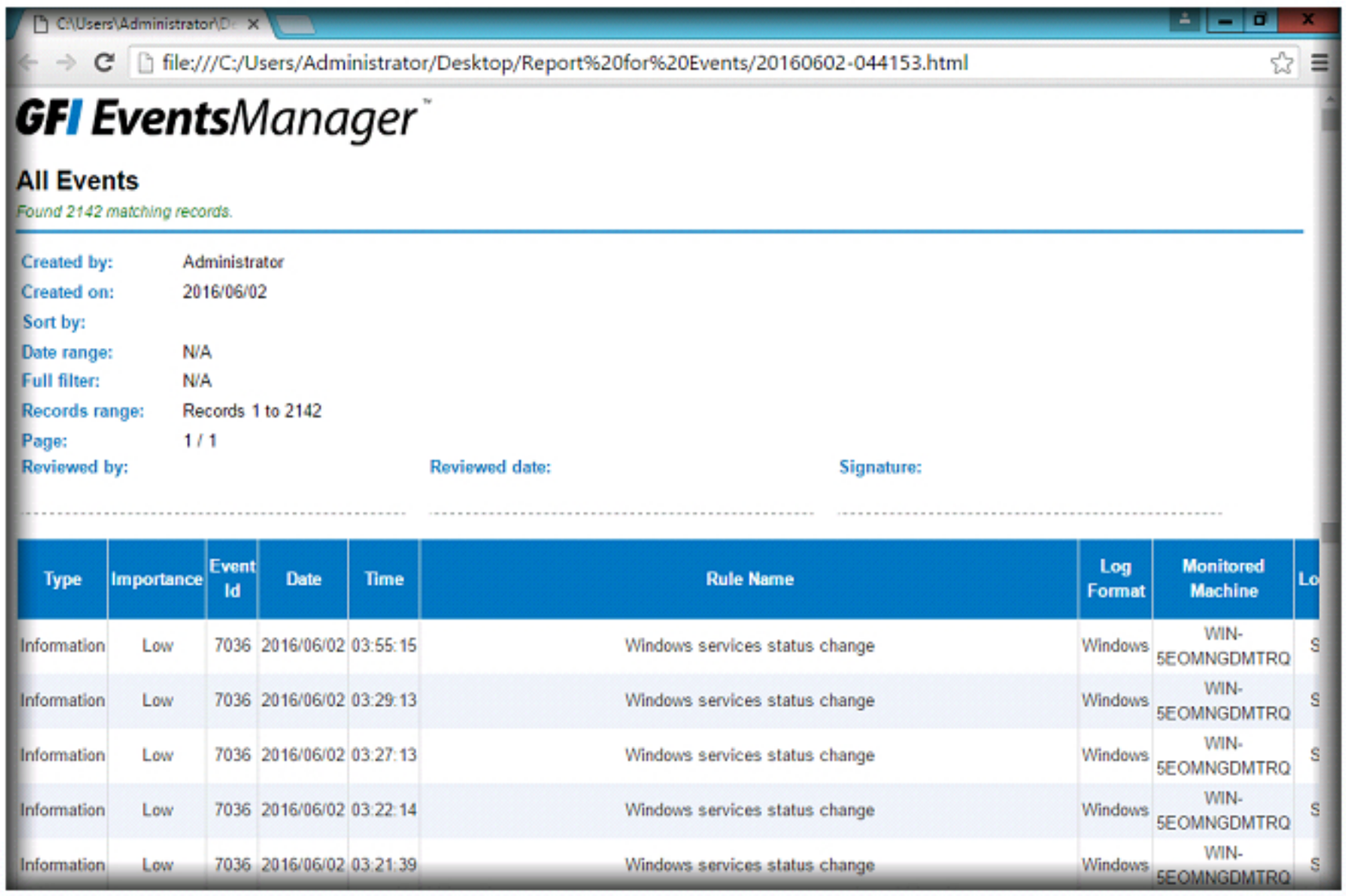

FIGURE 1.28: GFI EventsManager HTML view of events

35. Click the **Status** tab to see the status of the captured logs of the local computer.
36. The **Status** menu shows the status of the GFI EventsManager event processing engine, and other statistical information such as the number of **logon events, critical events,** and **service status events**.

GFI EventsManager helps you monitor a wider range of systems and devices through the centralized logging system and analyzes various log types including Windows events, Syslog, W3C, and SNMP traps that are generated by network resources.

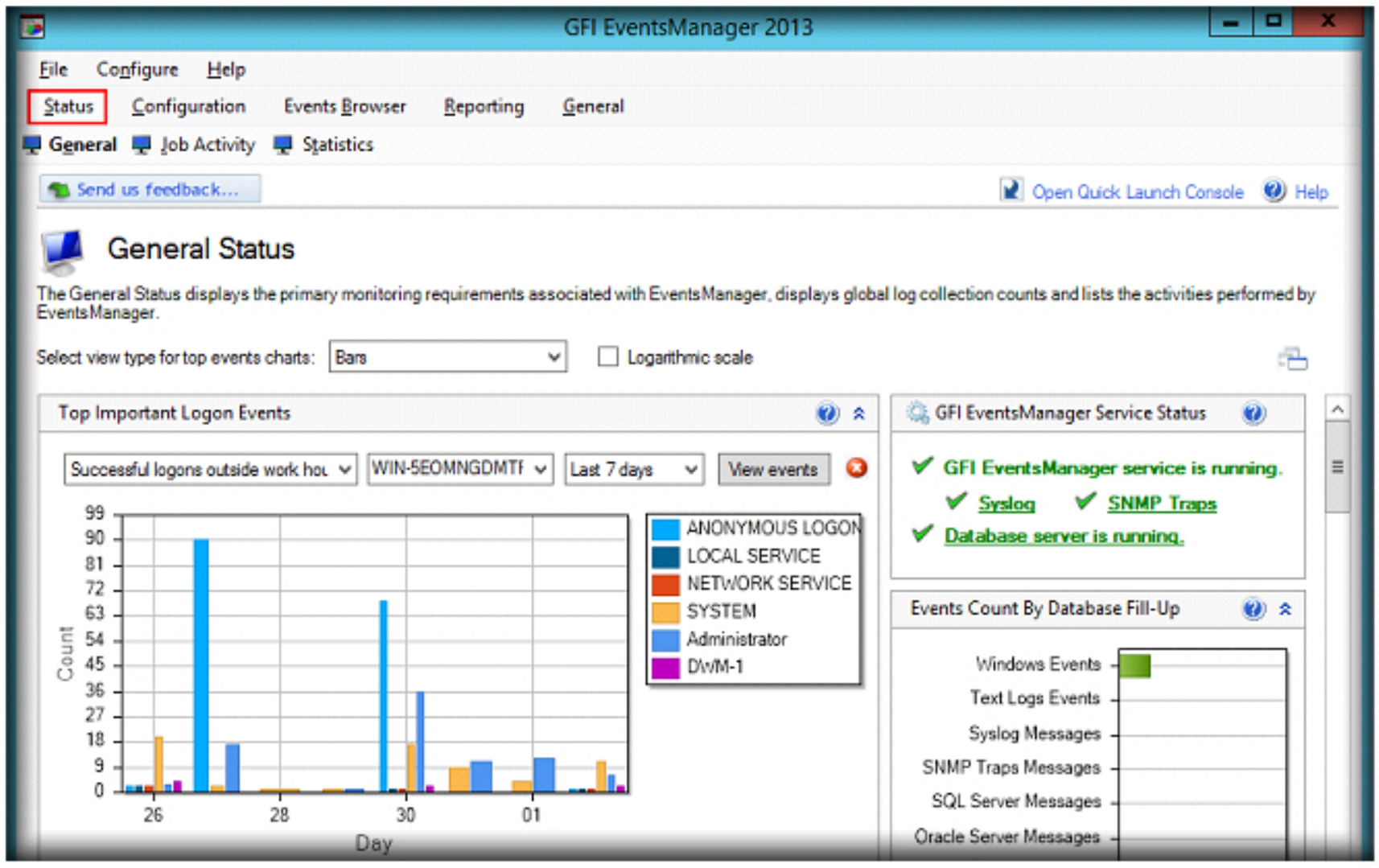

FIGURE 1.29: GFI EventsManager General tab of Status menu

Note: Each color of the bar chart represents a different group of log events. The color representation of the log group is listed beside the chart.

37. Click the **Statistics** tab of the **Status menu** to see the statistics of the processing event.
38. The statistics tab displays the **daily event activity** trends and statistics of a particular computer or of the entire network.

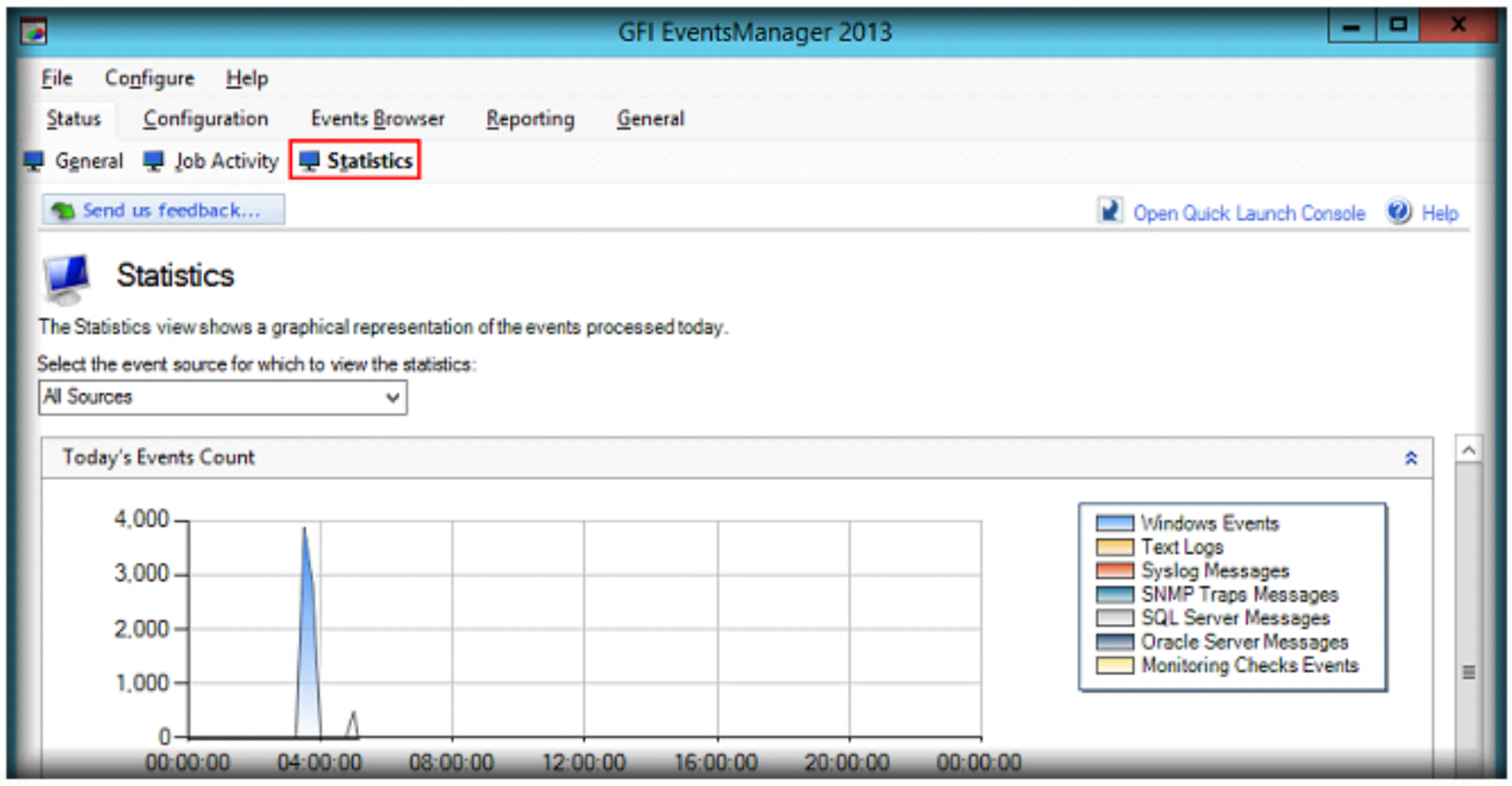

FIGURE 1.30: GFI EventsManager Statistics tab of Status menu

Lab Analysis

Analyze all the security events, application events, and system events and document the results related to the lab exercise. Give your expert opinion on the target computer's security posture and exposure.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs

Lab

2

Investigating System Log Data Using XpoLog Center Suite Tool

XpoLog Compliance suites help organizations meet security policies and ensure compliance with regulatory standards by offering comprehensive auditing and reporting structures for the IT environment.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

IT director of a company observed that the internet usage across the company has increased tremendously in recent times and found that some people have been downloading unnecessary files using the office internet. In order to find the culprits, he assigned an investigator to check and manage **Windows Event logs**.

As a **forensic investigator**, one must have knowledge of how a system creates logs and how to analyze these logs as evidences during security incidents.

Lab Objectives

The objective of this lab is to view the Windows logs. You will learn how to:

- Collect real-time Windows logs
- Detect violation in real-time log monitoring and alerting
- Generate comprehensive reports

Lab Environment

To execute the lab, you need:

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics

- XpoLog Center suite, located at **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\XpoLog Center**.
- You can also download the latest version of **XpoLog Center suite** from the link http://xpolog.com/download.
- If you decide to download the latest version, screenshots shown in the lab might differ.
- A computer running on **Windows Server 2012 virtual machine**.

- Administrative privileges to run the tool.
- A web browser with an **Internet** connection.

Lab Duration

Time: 15 Minutes

Overview of XpoLog Center Suite

You can download the XpoLog Center Suite from http://www.xpolog.com/

XpoLog Center Suite assists organizations to follow the **security policies** and ensure **compliance** with regulatory standards, by offering **comprehensive auditing** and **reporting structures** for the IT environment. Compliance includes the **rules** and **regulations** for data protection, user violations, and **risk detection**.

Lab Task

TASK 1

Launching XpoLog Center Suite

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\XpoLog Center** and double-click **XpoLogCenterSetup.exe**. An **InstallAnywhere** pop-up will appear, wait for the installation to begin.

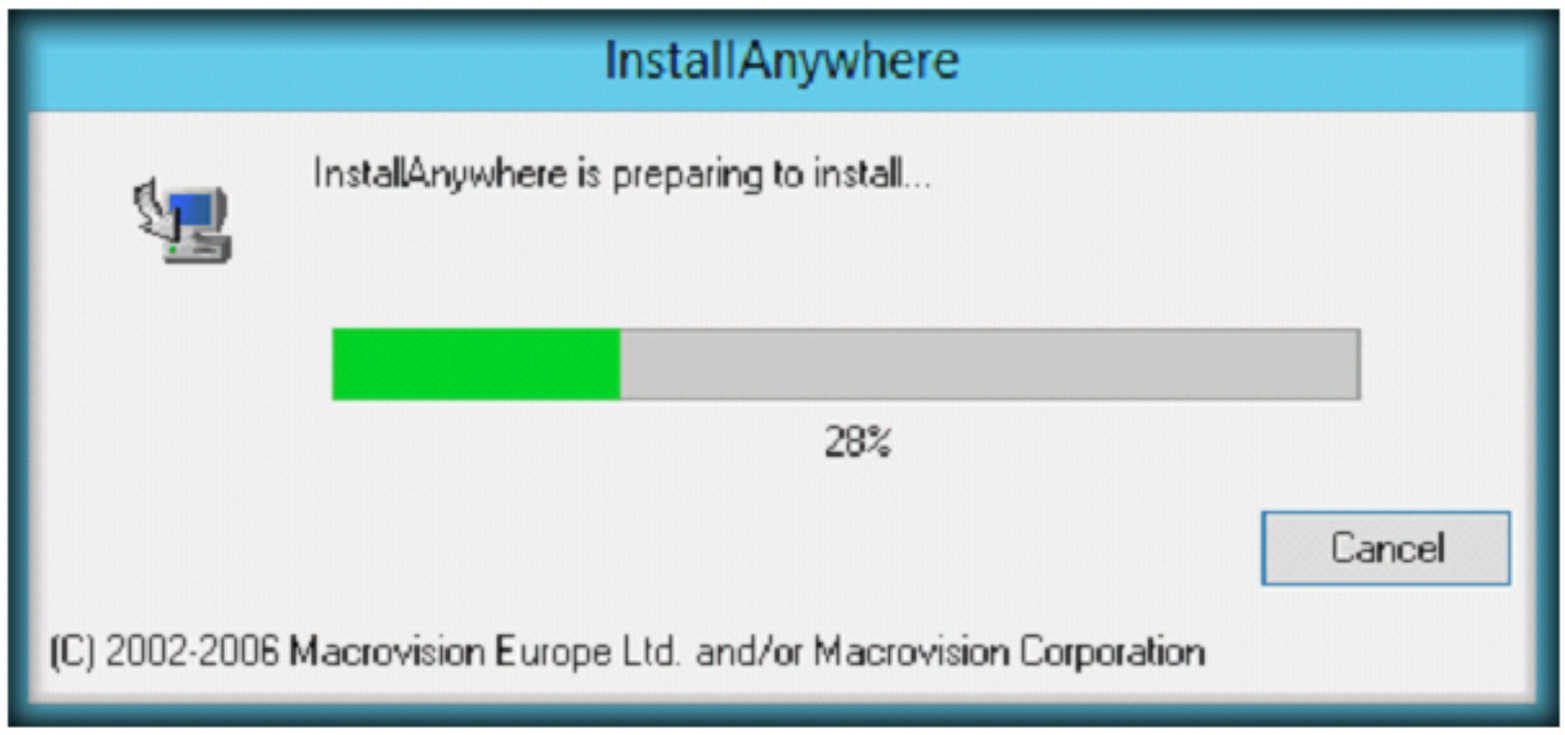

FIGURE 2.1: InstallAnywhere pop-up

2. XpoLog Center Installation wizard will appear. Follow the wizard driven installation steps to install the application.

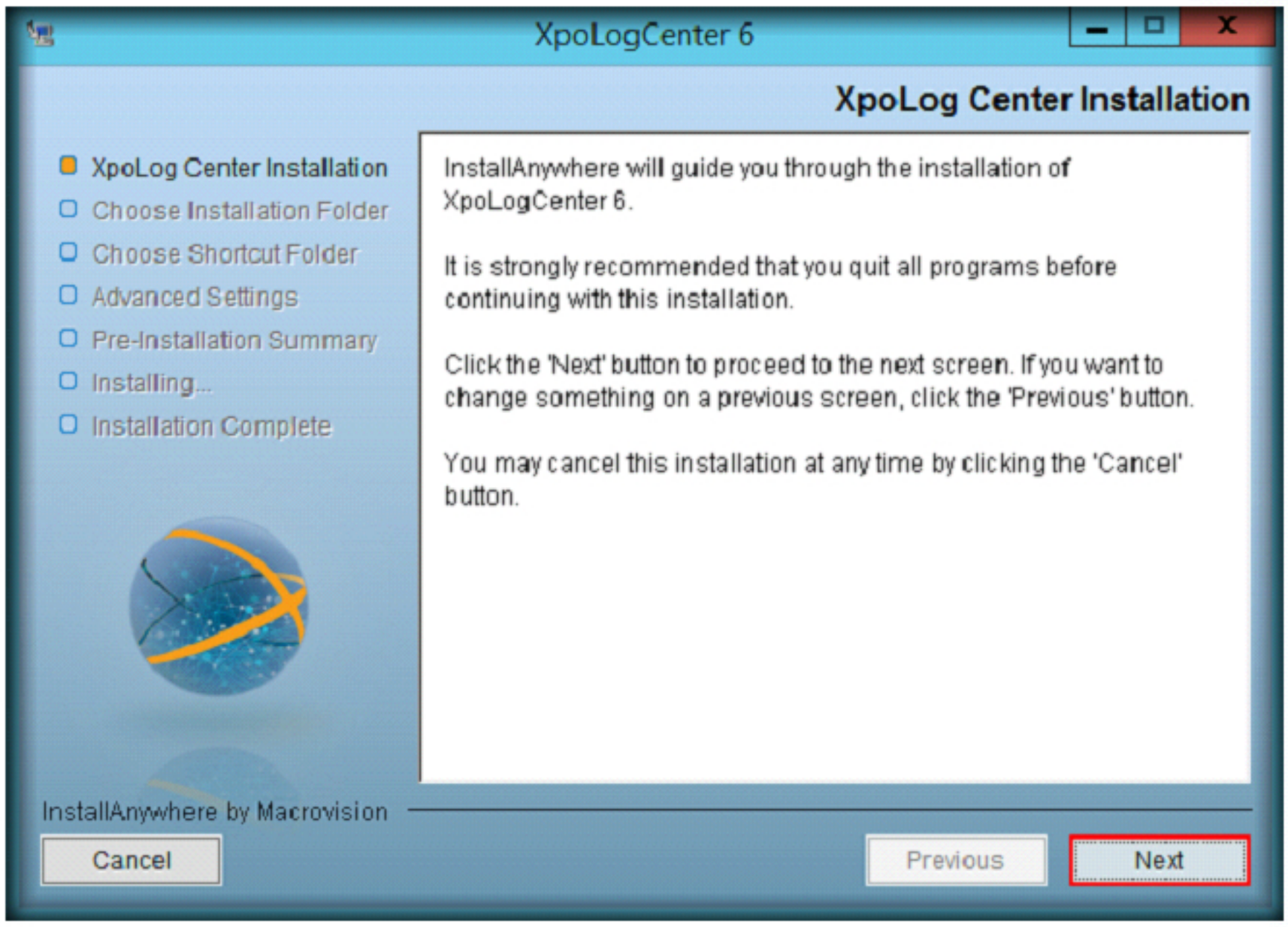

FIGURE 2.2: XpoLog Center Installation wizard

3. On completing the installation, click **Done**.

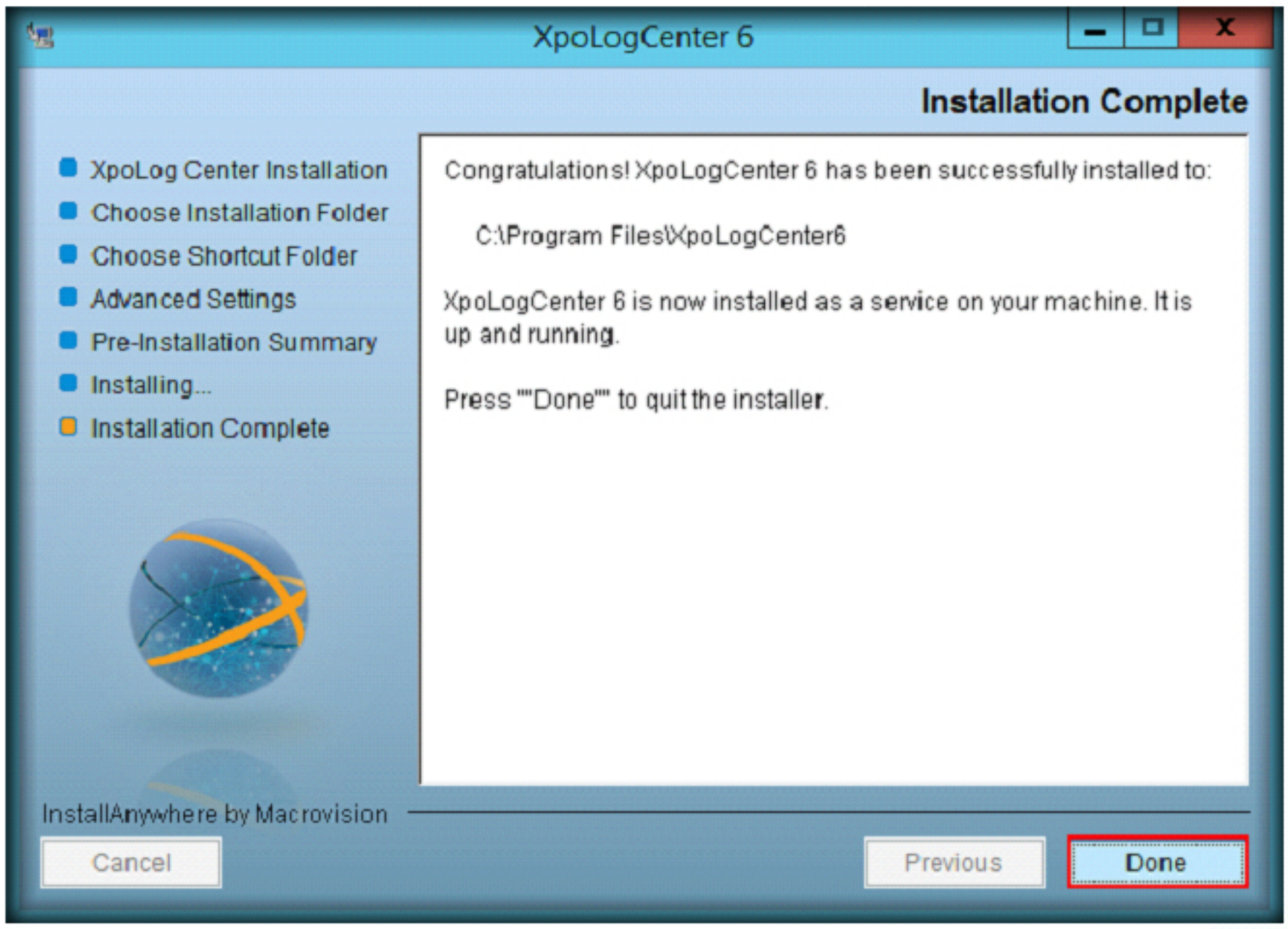

FIGURE 2.3: XpoLog Center Installation wizard

4. Once you click **Done**, XpoLog GUI appears in the default web browser (URL: http://localhost:30303/logeye/root.html), click **Win Event**.

XpoLog contains an advanced monitoring engine that verifies the log contents and executes different types of alerts.

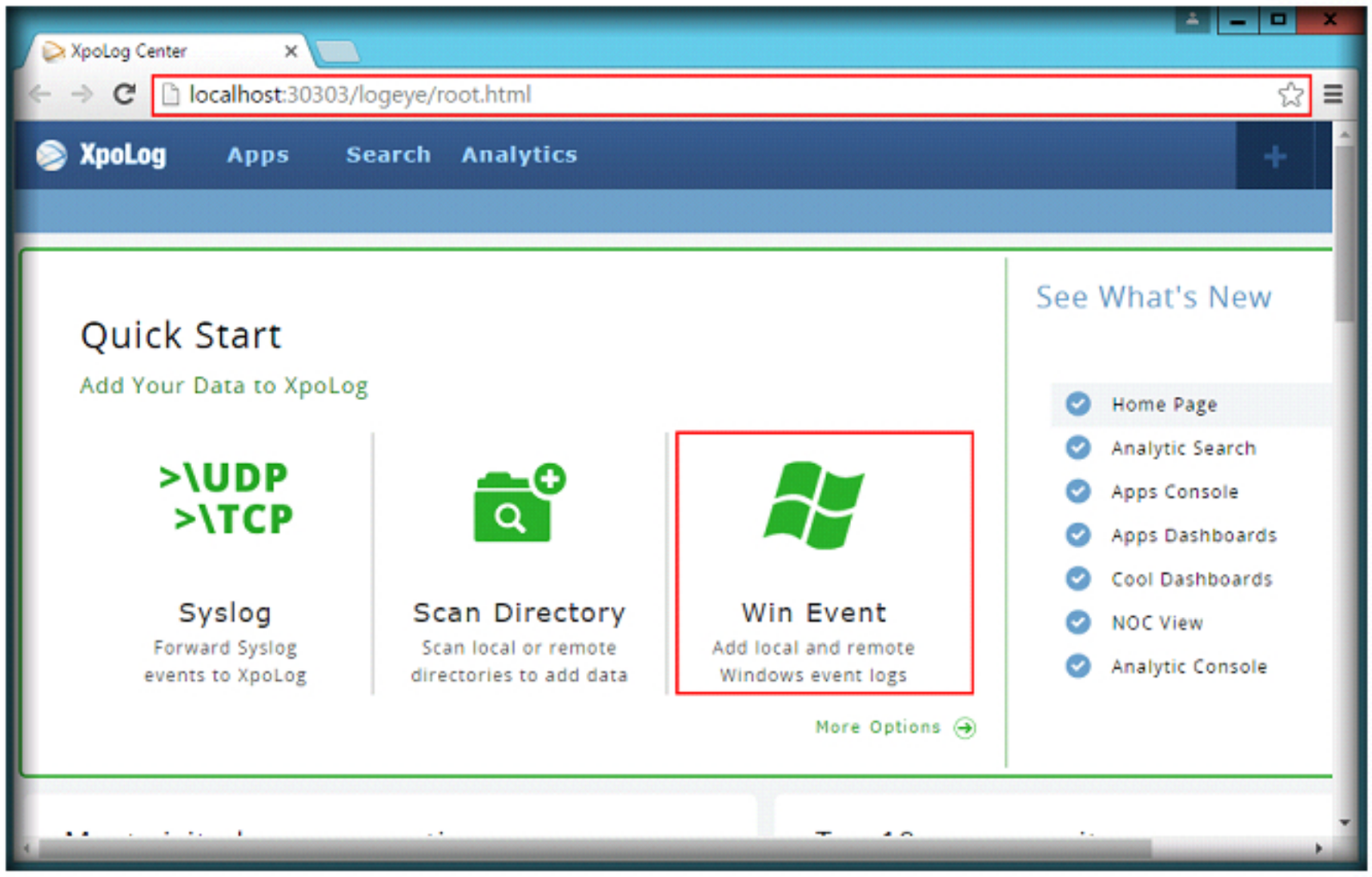

FIGURE 2.4: XpoLog GUI

Note: If an **XpoLog Center Mail Settings** pop-up appears, close it.

TASK 2

Viewing the Event Logs

5. In this lab, we shall examine the logs that were recorded on a remote machine. These logs are stored at **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\XpoLog Center\Logs**.

6. Hover the mouse cursor on **Tools** and click **Import Folder**.

The Main pane displays the parsed content of the log based on the log definition.

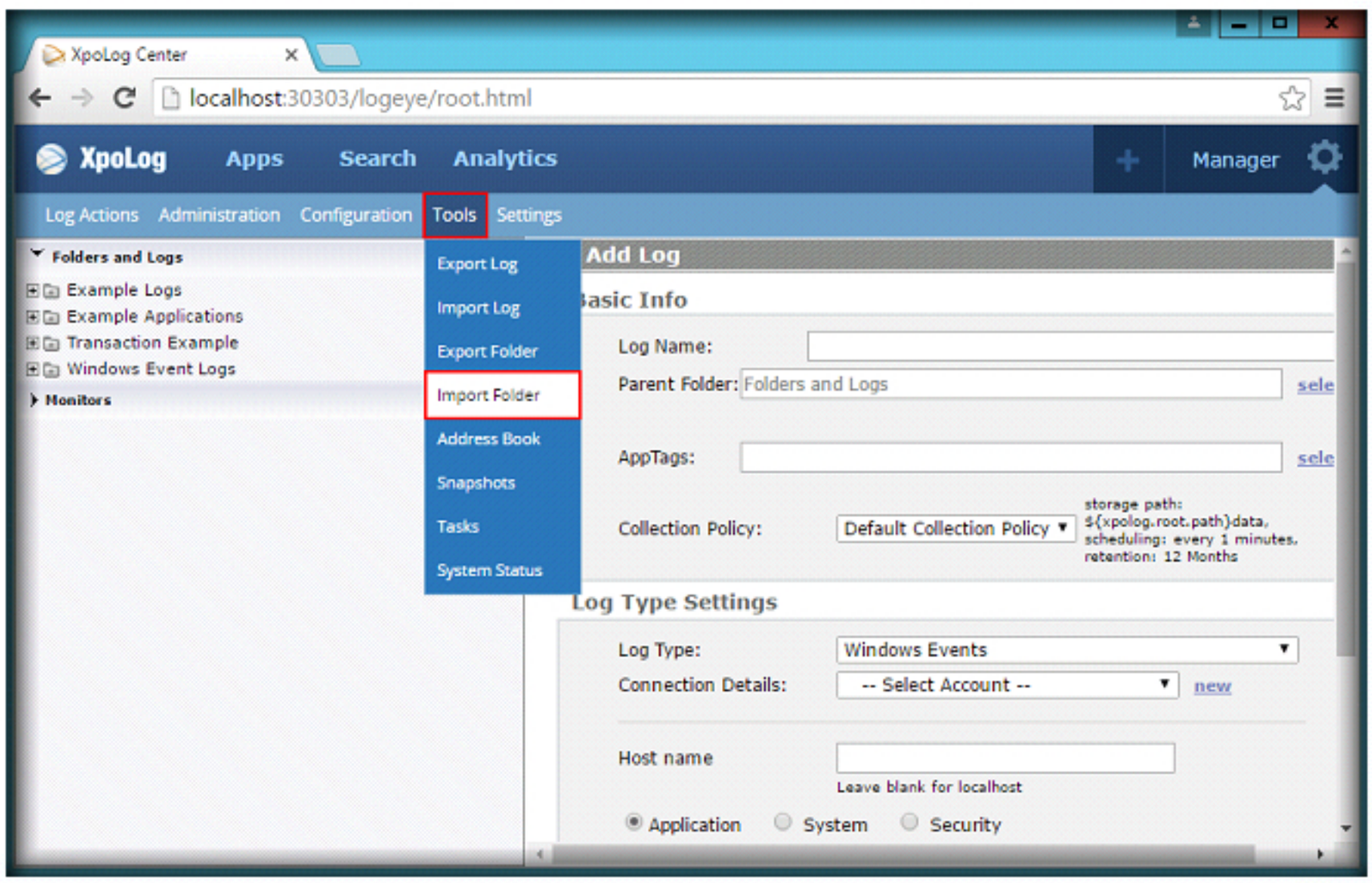

FIGURE 2.5: XpoLog GUI Import Folder

7. **Archive Location** section will appear, click **Choose File** button.

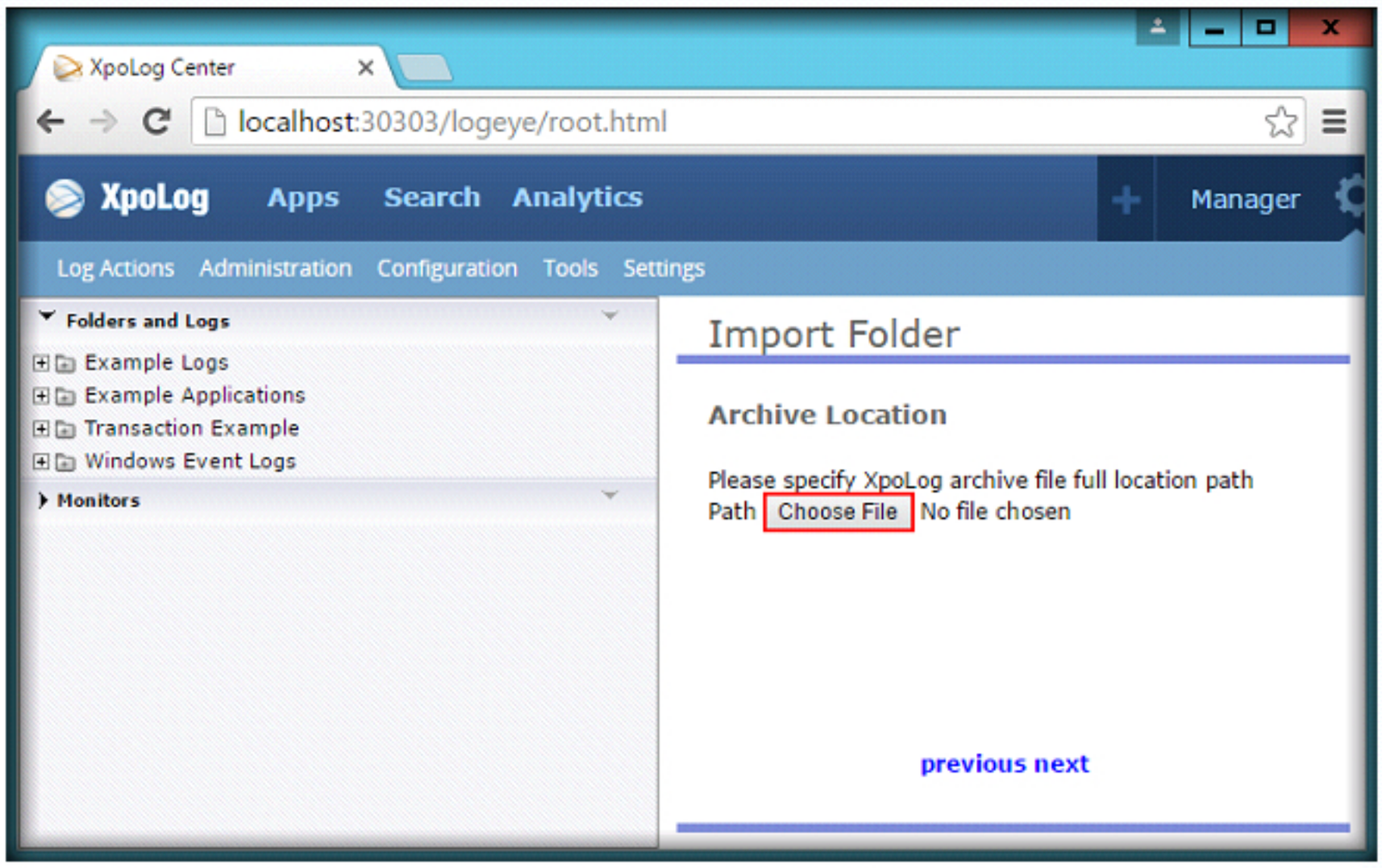

FIGURE 2.6: XpoLog GUI Archive Location section

8. Navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\XpoLog Center\Logs**, select **rootModule.zip** and click **Open**.

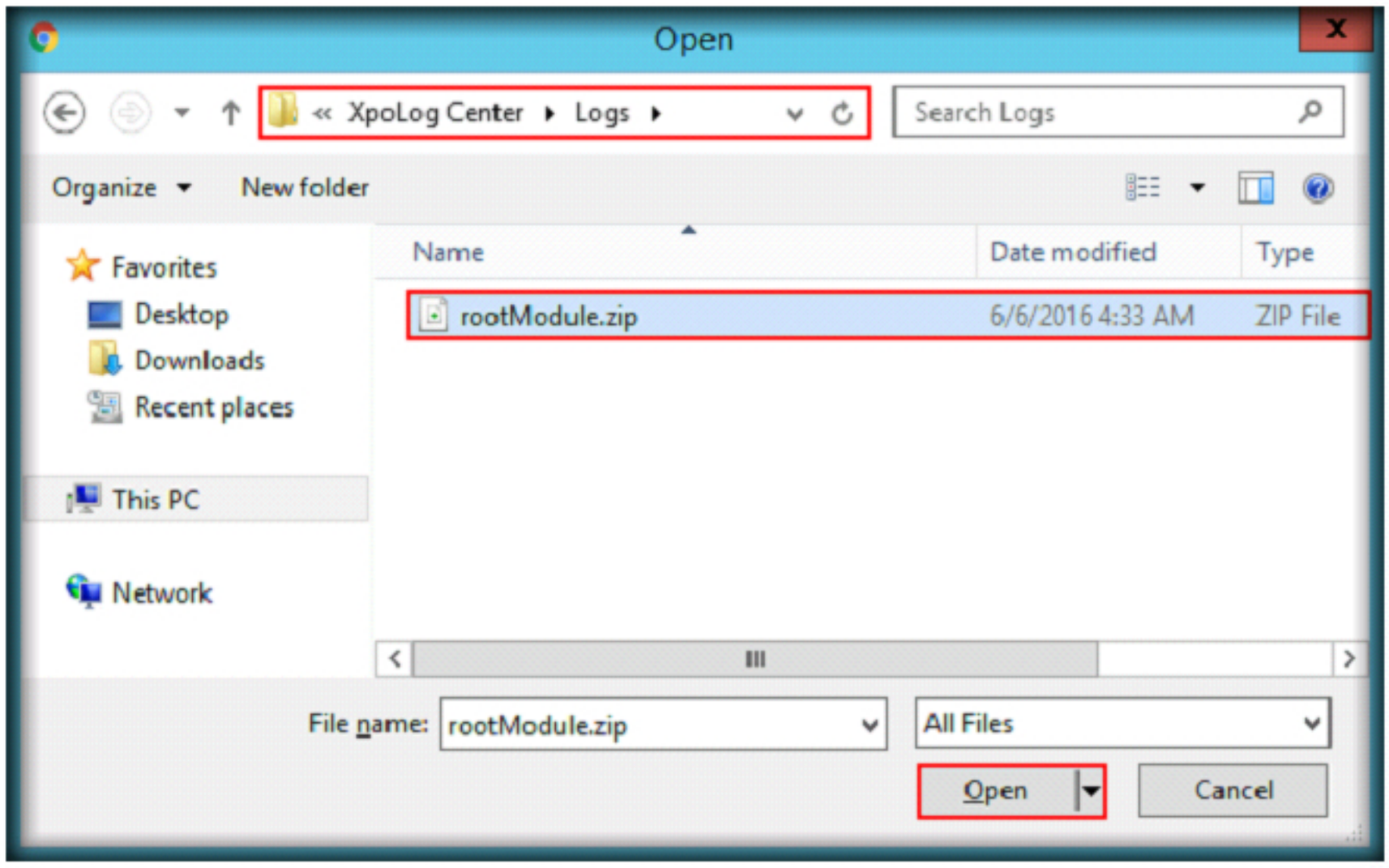

FIGURE 2.7: rootModule.zip

9. The file is now selected, click **next**.

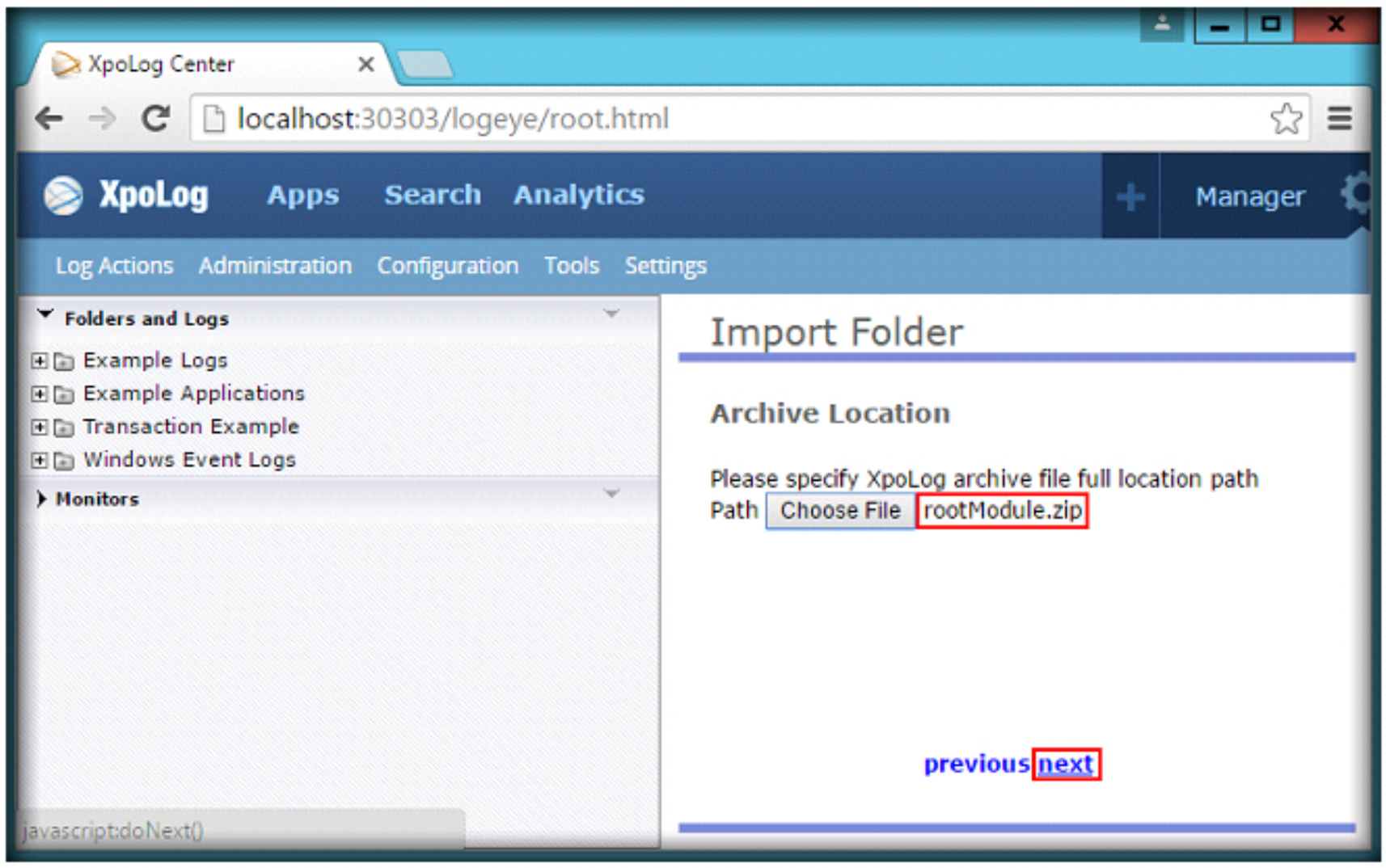

FIGURE 2.8: XpoLog GUI Archive Location section

10. Parent Folder Selection section will appear, click **select** to select the parent folder.

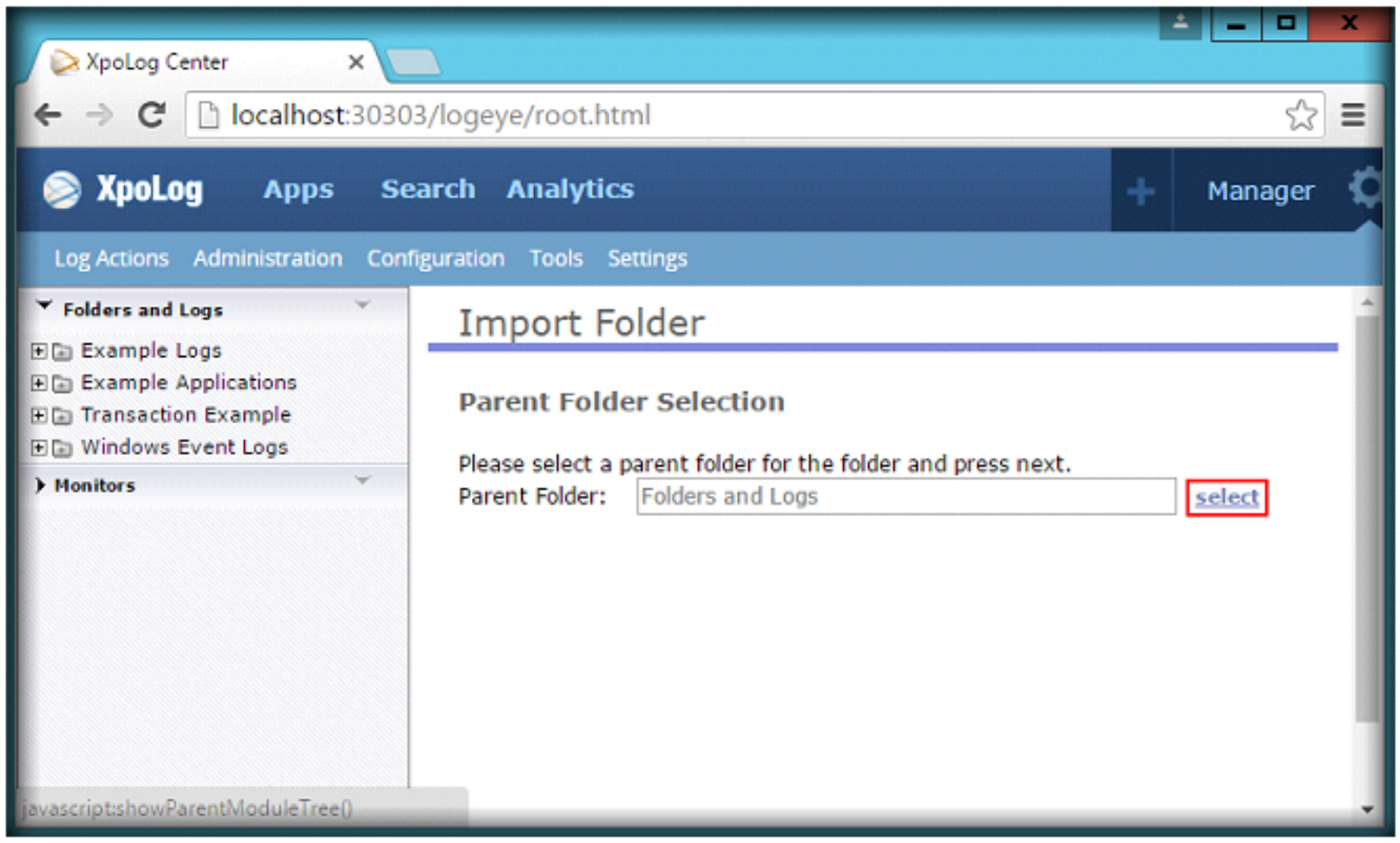

FIGURE 2.9: XpoLog GUI Parent Folder Selection section

11. Here, you will create a new parent folder for the log folder that you have selected in the earlier steps.

12. Parent Folder section will appear, click **Create New**.

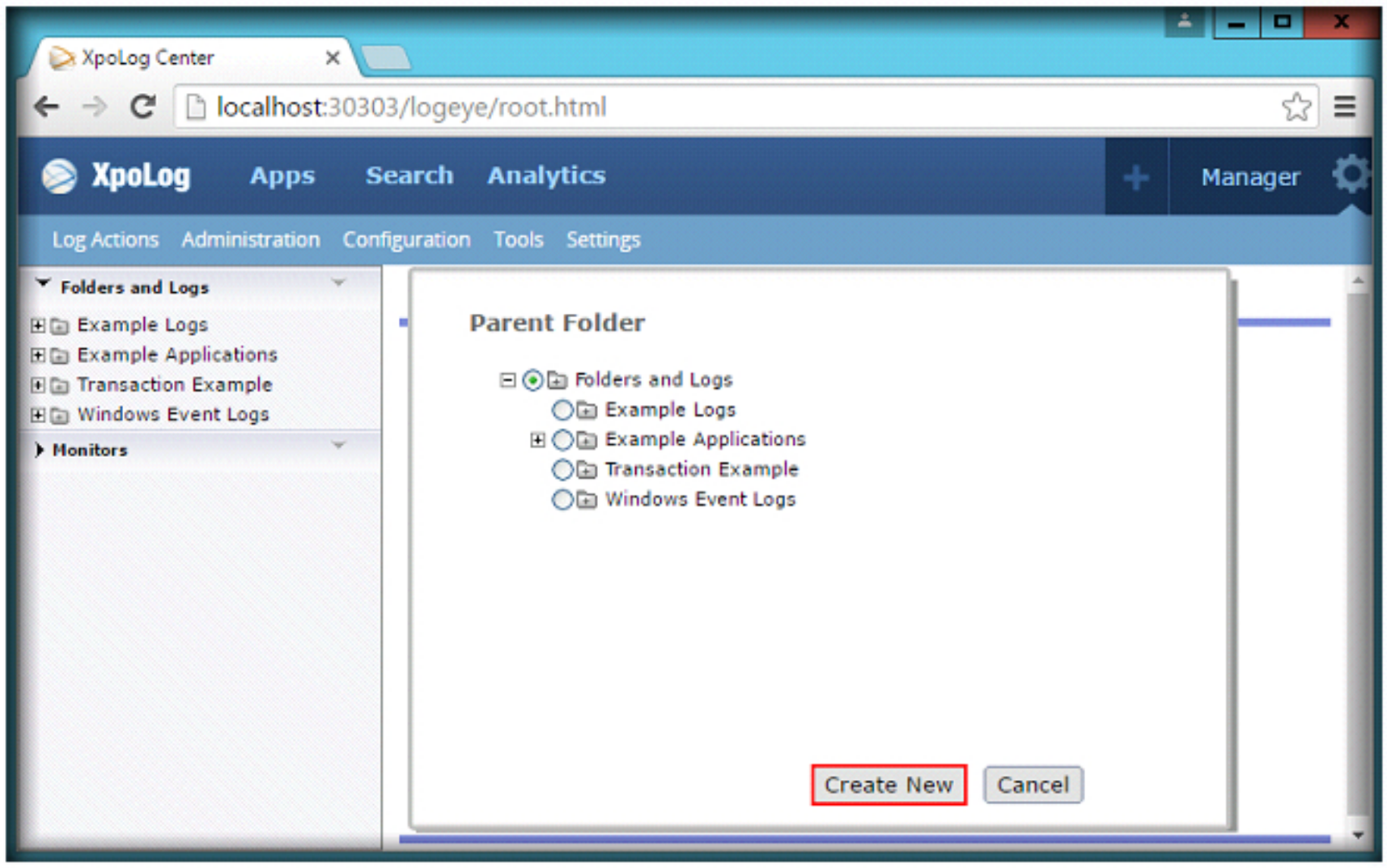

FIGURE 2.10: XpoLog GUI Parent Folder section

13. Enter the folder name as **Windows 10 Event Logs**, select **Folders and Logs** radio button and click **Save**.

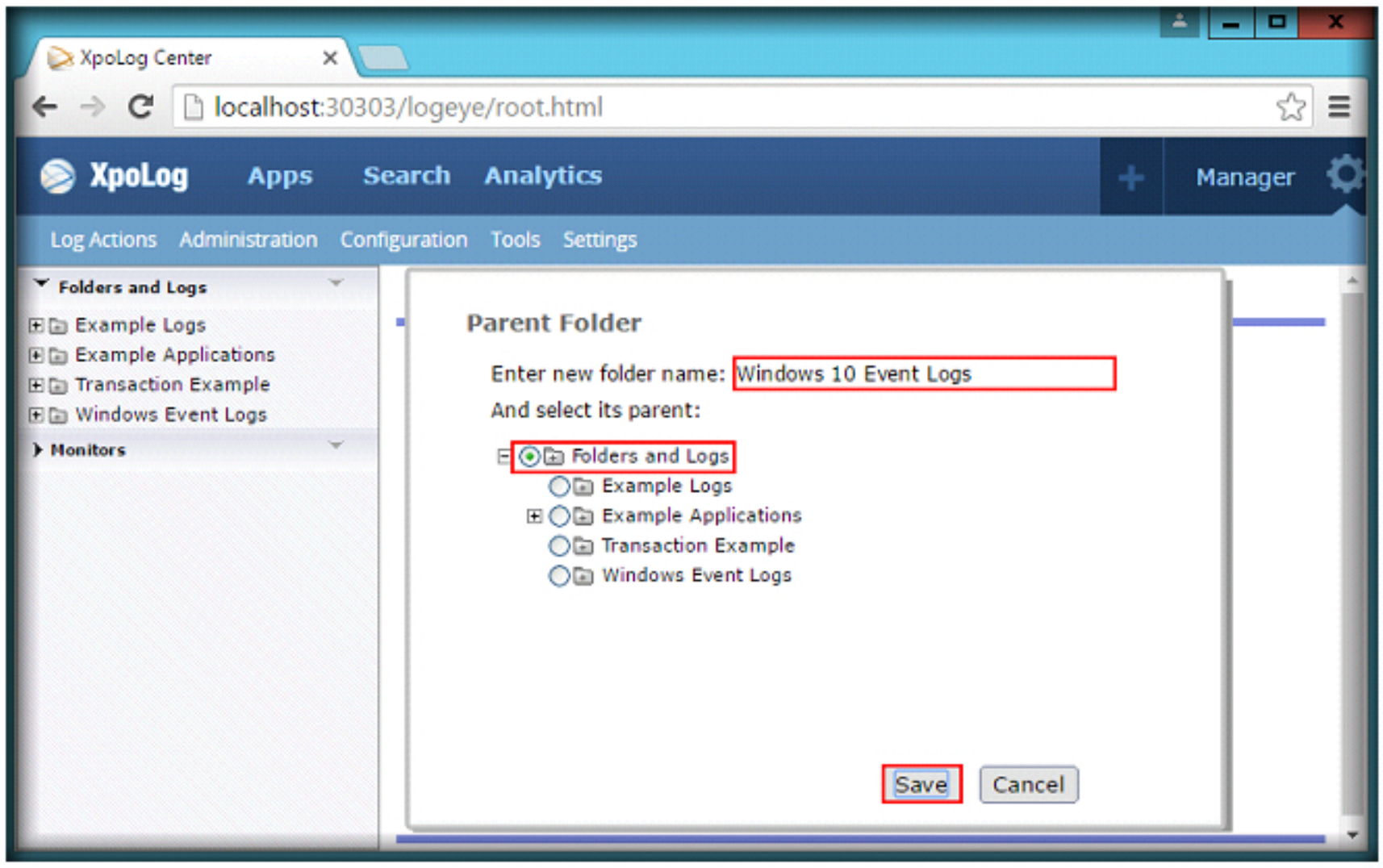

FIGURE 2.11: XpoLog GUI Parent Folder section

14. The newly created parent folder will now appear in the **Parent Folder** field, click **next**.

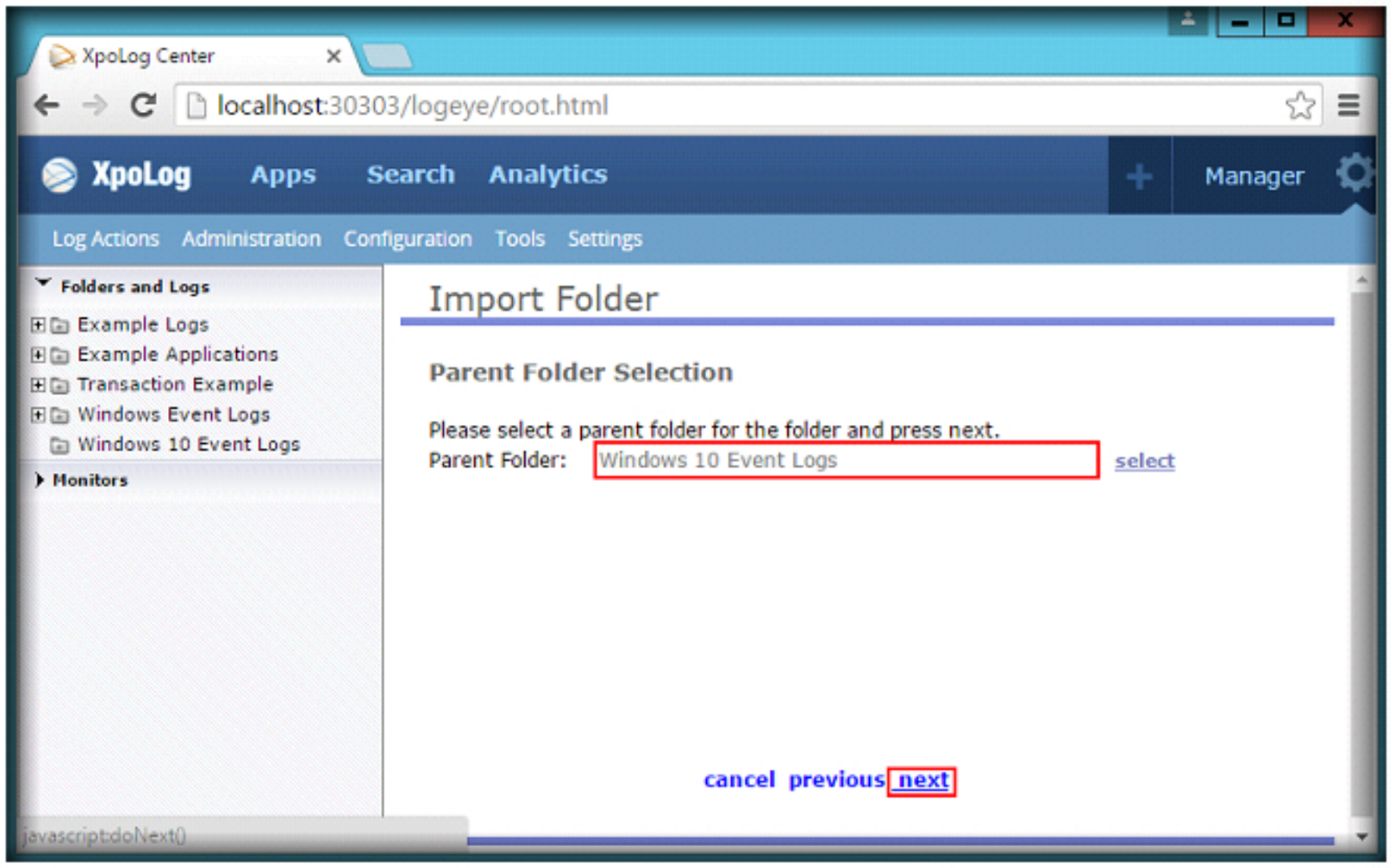

FIGURE 2.12: XpoLog GUI new Parent Folder

15. The newly imported folder (**Windows Event Logs**) will appear in the left pane under **Windows 10 Event Logs**.

16. Expand Windows 10 Event Logs → Windows Event Logs. You will observe three types of logs under the **Windows Event Logs** i.e., **Application** logs, **Security** logs and **System** logs.

The Storage panel presents the logs that are being collected by XpoLog.

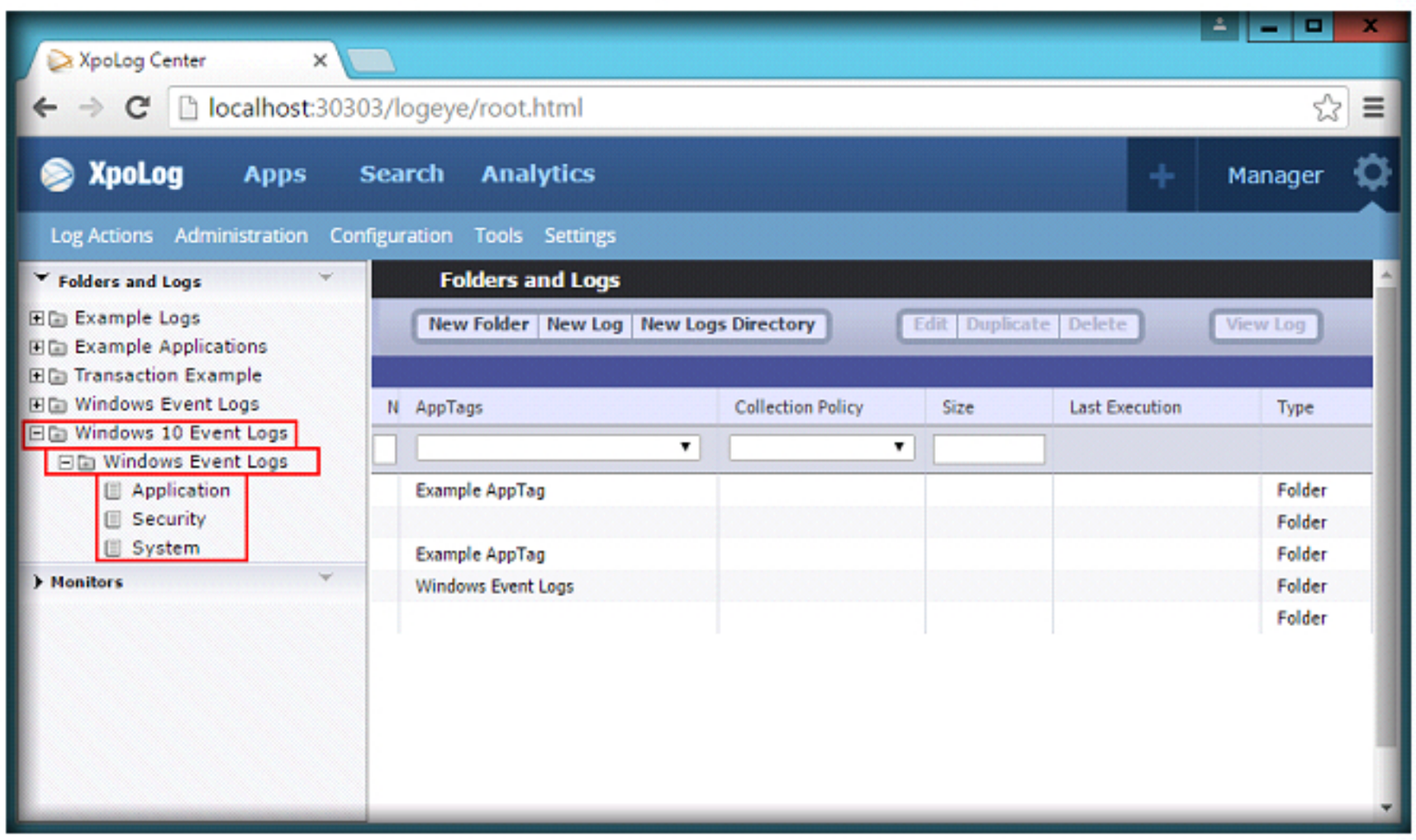

FIGURE 2.13: XpoLog GUI Expand Windows 10 Event Logs

17. To view Windows application logs, click **Application** under Windows Event Logs. All the application logs appear as shown in the following screenshot:

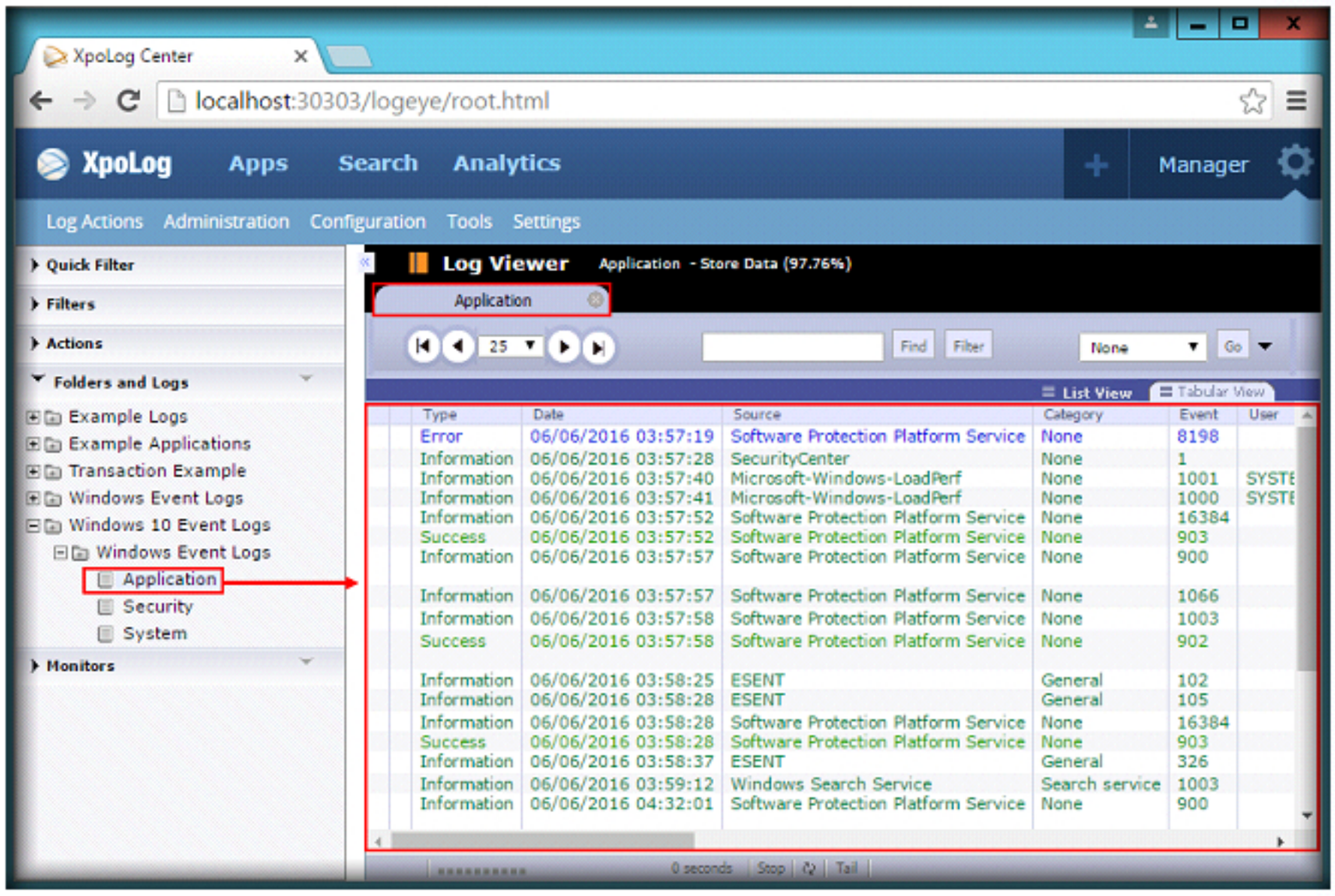

FIGURE 2.14: Windows application logs results

18. To view Windows Security logs, click **Security** under Windows Event Logs. All the Security related logs will appear as shown in the following screenshot:

Create Monitor button to open the Add Monitor page and add a new monitor based on rules defined on log data.

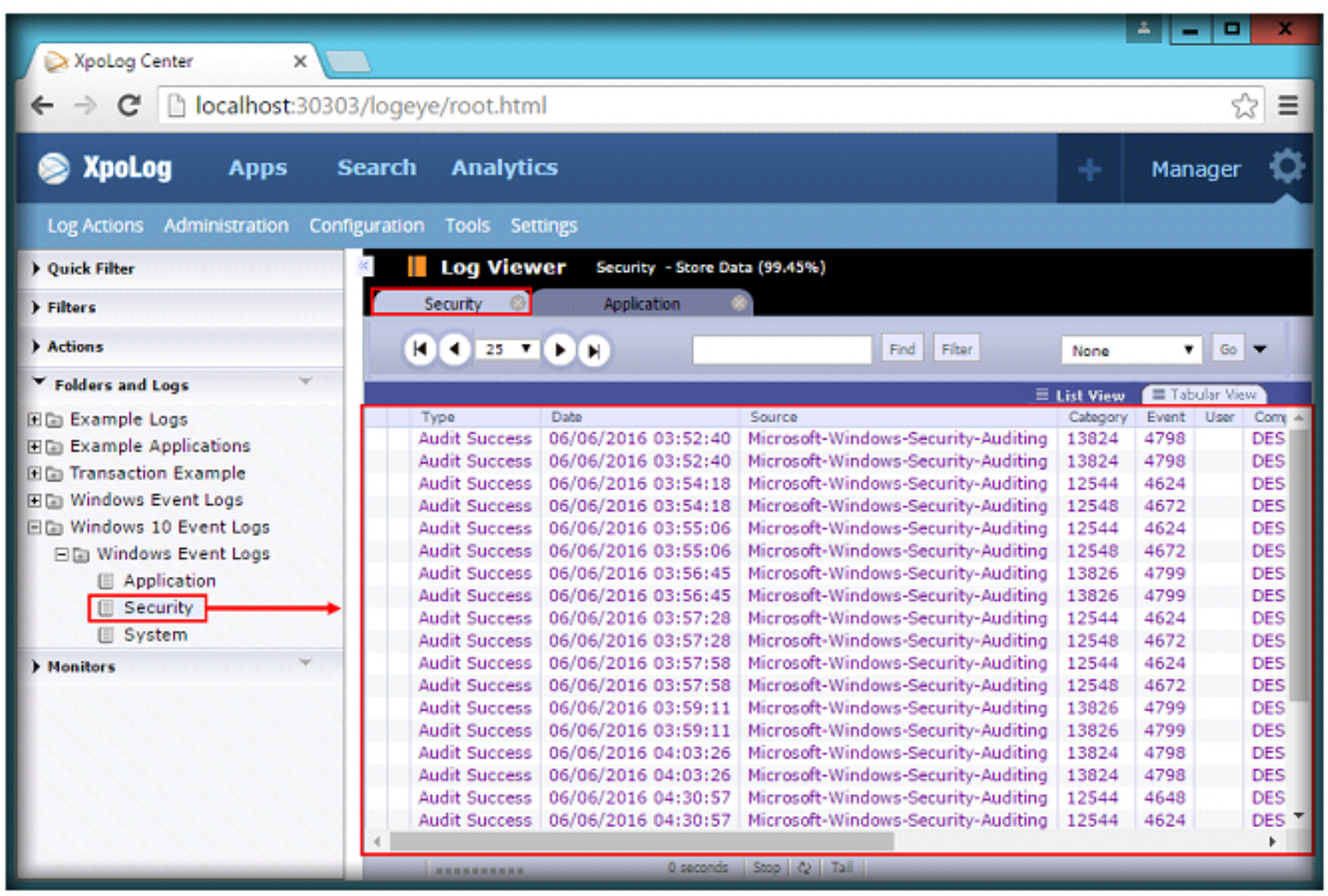

FIGURE 2.15: Windows security logs results

19. To view Windows System logs, click **System** under Windows Event Logs. All the System related logs will appear as shown in the following screenshot:

Environment analysis is an automatic report that is generated on an environment (i.e., folders that contain logs).

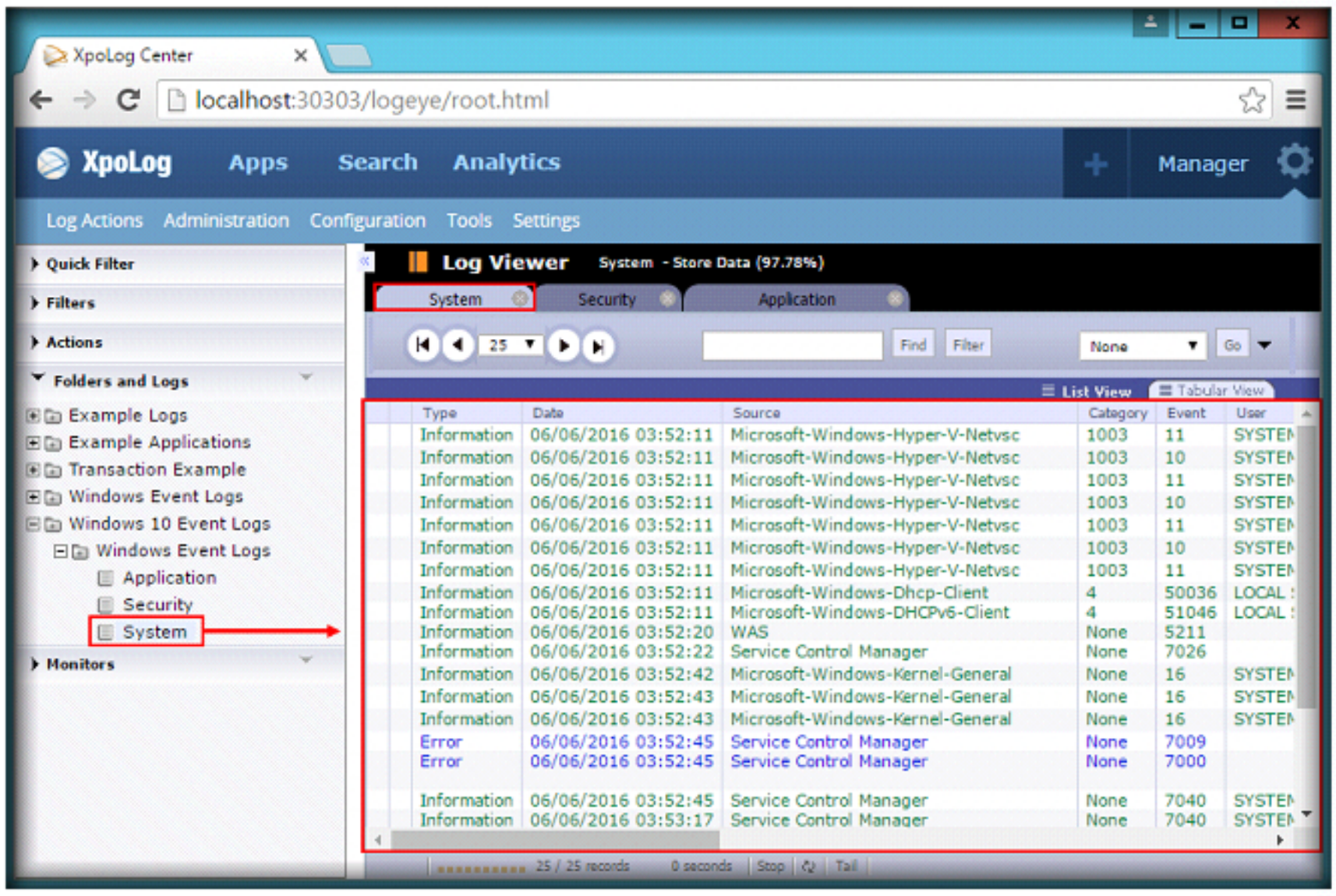

FIGURE 2.16: Windows system logs results

20. To view an analytical representation of Windows event logs, click the **Analytics** icon.

XpoLog contains an advanced monitoring engine that verifies the log contents and executes different types of alerts when a rule is matched to the log records.

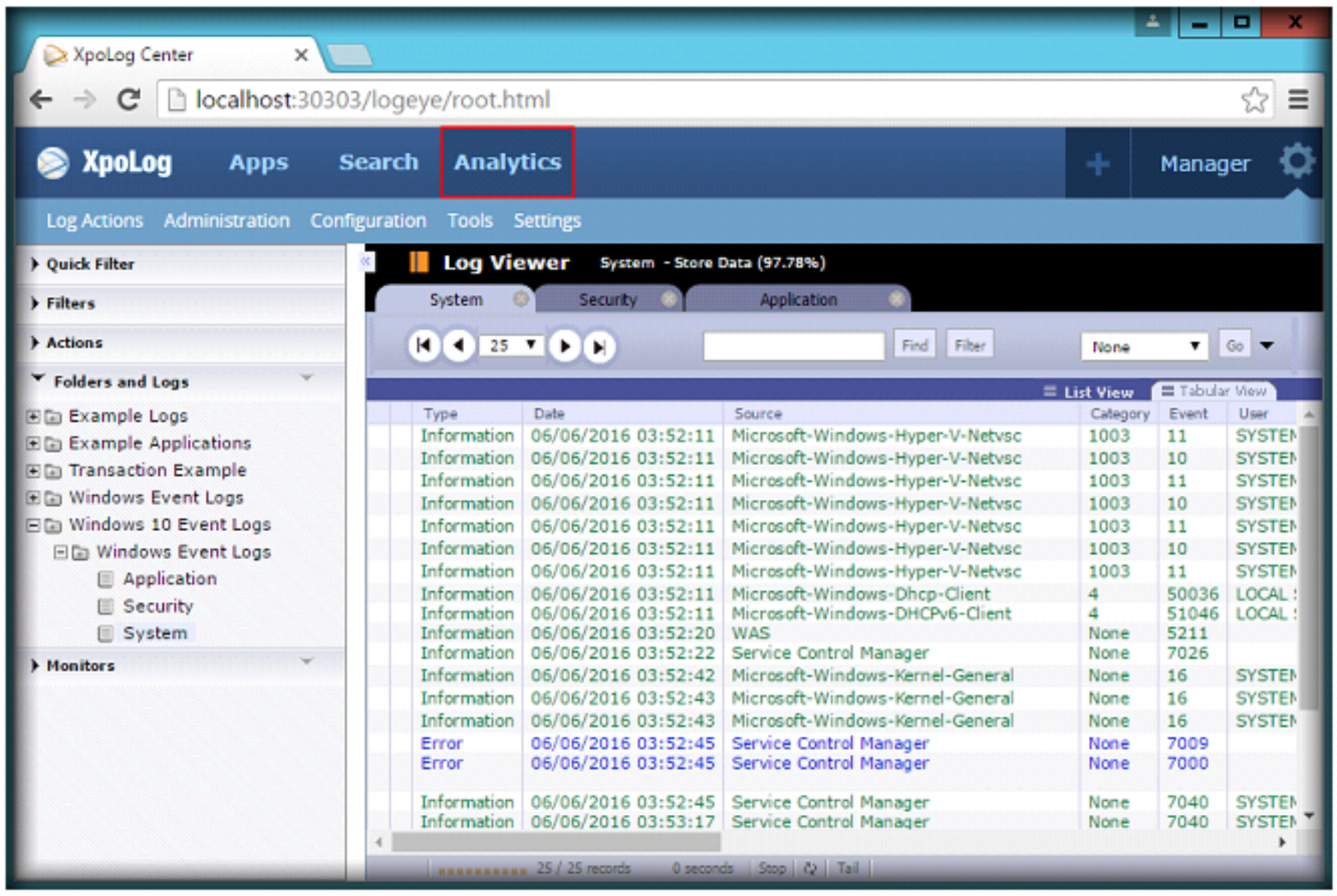

FIGURE 2.17: Analytics summary of Windows system logs

21. To view the complete analytical information of Windows logs, click the **Analytics** tab.

XpoLog contains an advanced reporting engine that can be used for rules aggregation, statistics, compliance, and business intelligence.

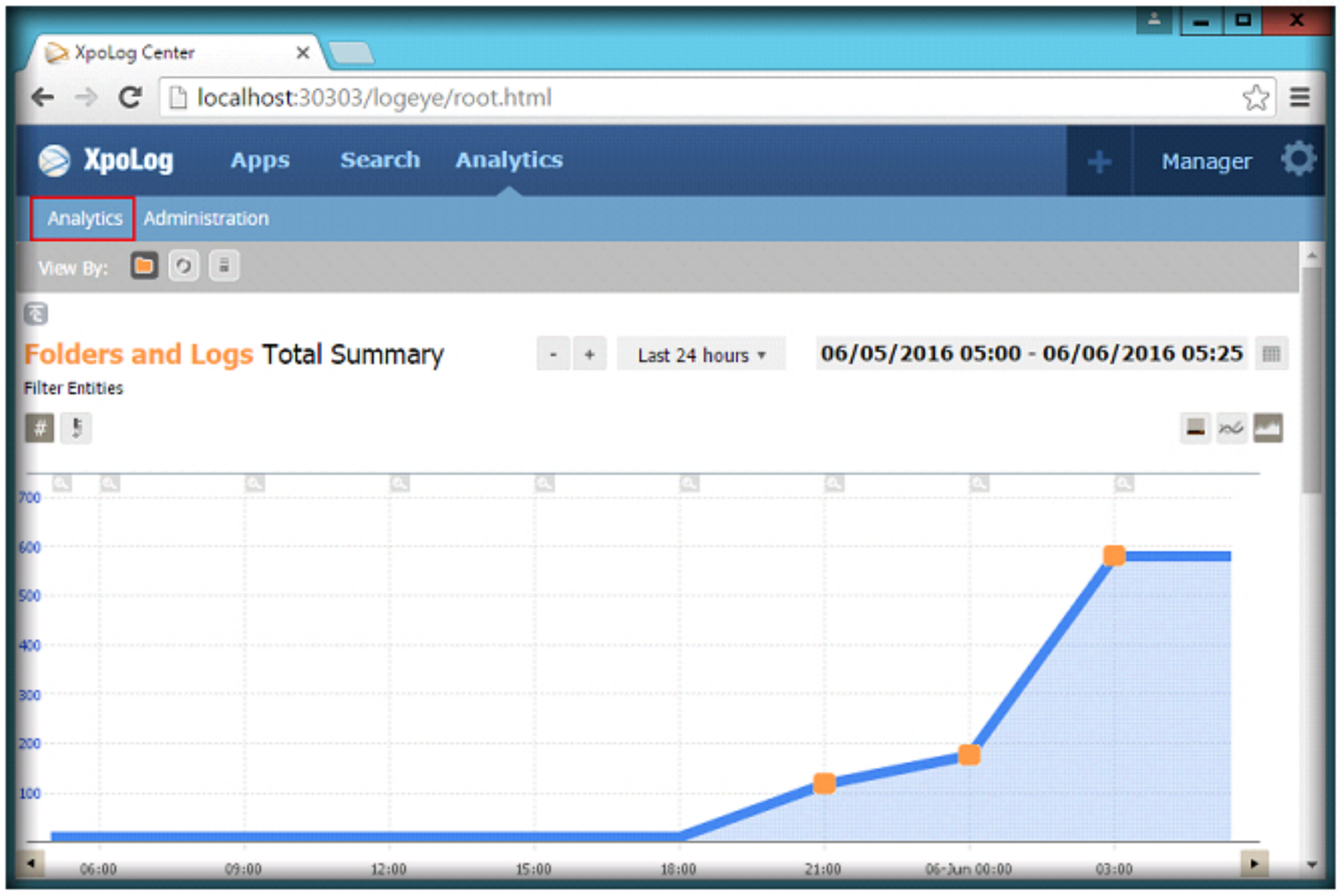

FIGURE 2.18: Complete information of Windows event log

22. Scroll the window to view the complete information, and examine the logs.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

3

Investigating Network Attacks Using Kiwi Log Viewer

Kiwi Log Viewer is a Windows based tool that enables monitoring a log file for changes made. It can display changes in real-time and lets you automatically monitor log file entries for specific keywords, phrases or patterns.

ICON KEY

- Valuable information
- Test your knowledge
- Web exercise
- Workbook review

Lab Scenario

A trainee investigator is assigned a task of finding evidence from logs pertaining to a huge network of a company. What tools and processes should he follow to monitor the files, analyze them and gather evidences from the network's logs.

As an expert **forensic investigator** of an organization, you should know how to view and examine the **logs pertaining to a network**.

Lab Objectives

The objective of this lab is to view the logs recorded in a network. You will learn how to:

- View real-time network logs

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics

Lab Environment

To execute the lab, you need:

- A **Windows Server 2012** virtual machine.
- Kiwi Log Viewer, located at **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\Kiwi Log Viewer**.
- You can also register and download the latest version of **Kiwi Syslog Server** from the link http://www.kiwisyslog.com/products/kiwi-log-viewer/product-overview.aspx.
- To download the tool from Kiwi Syslog Server's website, you need to fill the registration form.

- If you decide to download the latest version, screenshots shown in the lab might differ.
- Administrative privileges to run the tool.
- A web browser with **Internet** connection.

You can download the Kiwi Syslog Server from http://www.kiwisyslog.com/kiwi-syslog-server-overview/

Lab Duration

Time: 15 Minutes

Overview of kiwi Log Viewer

Kiwi Syslog Server is a Windows-based syslog server available in the market. It offers a solution for investigating the **receiving**, **logging**, **displaying**, **alerting**, and **forwarding** syslog and SNMP trap messages from network devices, such as routers, switches, Linux and Unix hosts, and other syslog and trap-enabled devices.

Lab Task

TASK 1

Launching Kiwi Syslog Server

1. Log on to Windows Server 2012 virtual machine.
2. Navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Log Capturing and Analysis Tools\Kiwi Log Viewer**. Double-click **Kiwi_LogViewer_2.1.0_Win32.setup.exe**, accept the license agreement and follow the wizard driven installation steps to install the application.

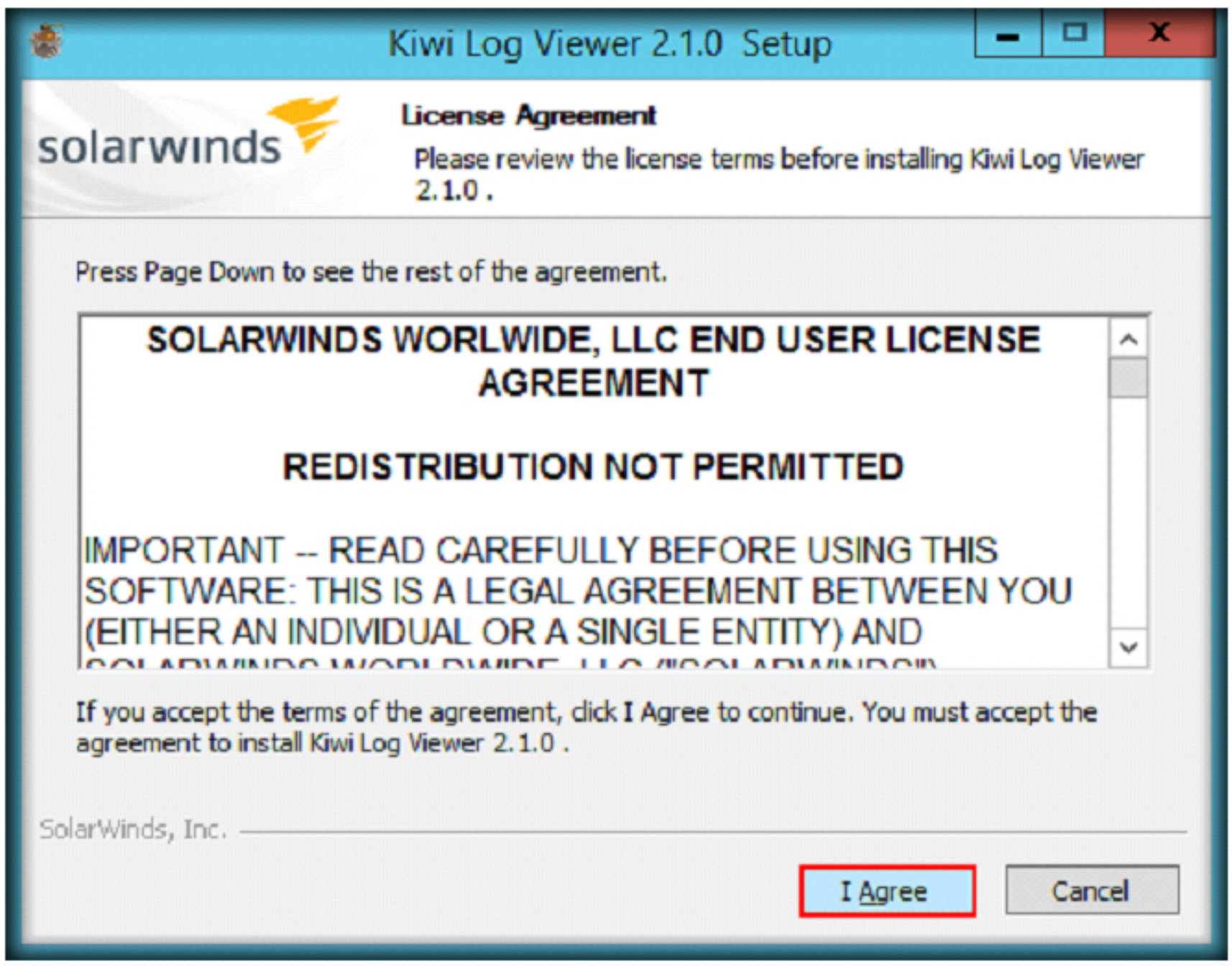

FIGURE 3.1: Kiwi Log Viewer license agreement wizard

3. On completing the installation, check **Run Kiwi Log Viewer 2.1.0** option and click **Finish**.

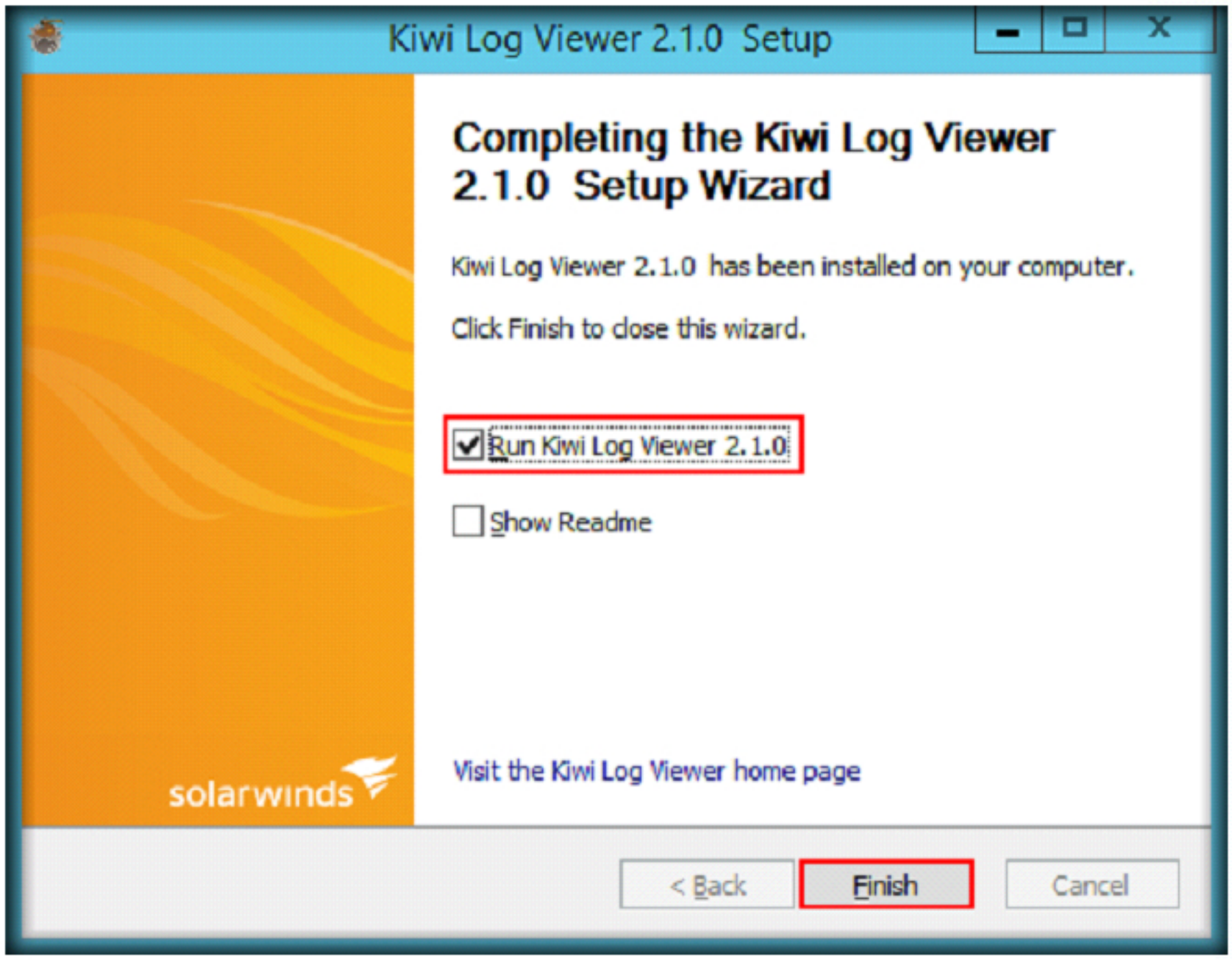

FIGURE 3.2: Kiwi Log Viewer Setup wizard completion

4. Kiwi Log Viewer GUI will appear. Click **File** from the menu bar and select **Open File...**.

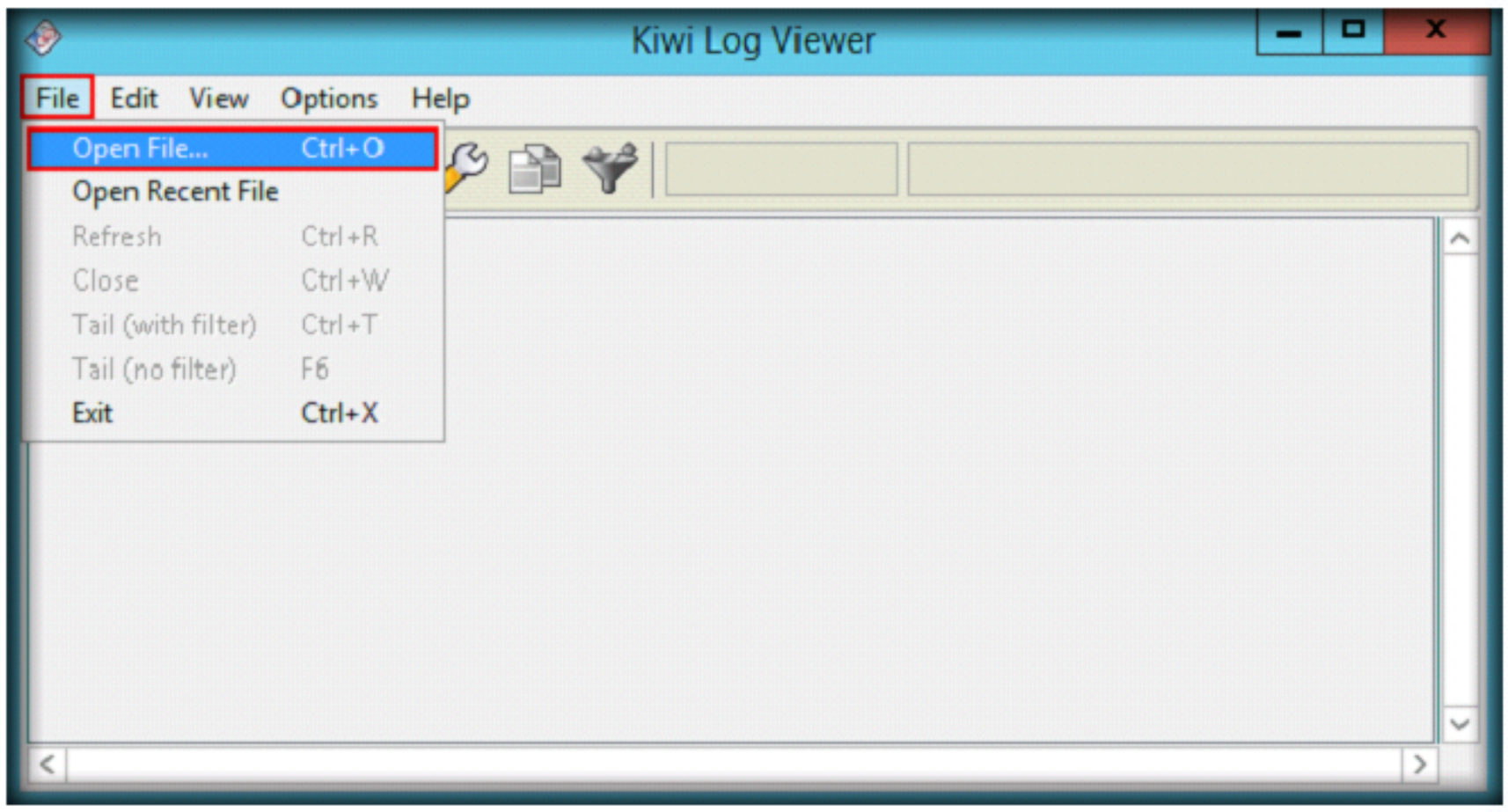

FIGURE 3.3: Kiwi Log Viewer GUI

5. **Select a log file to open** window will appear, navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Traffic Capturing and Analysis Tools\Wireshark\Capture Files**, select **All files** from the File Type drop-down list, select **Trojan** and then, click **Open**.

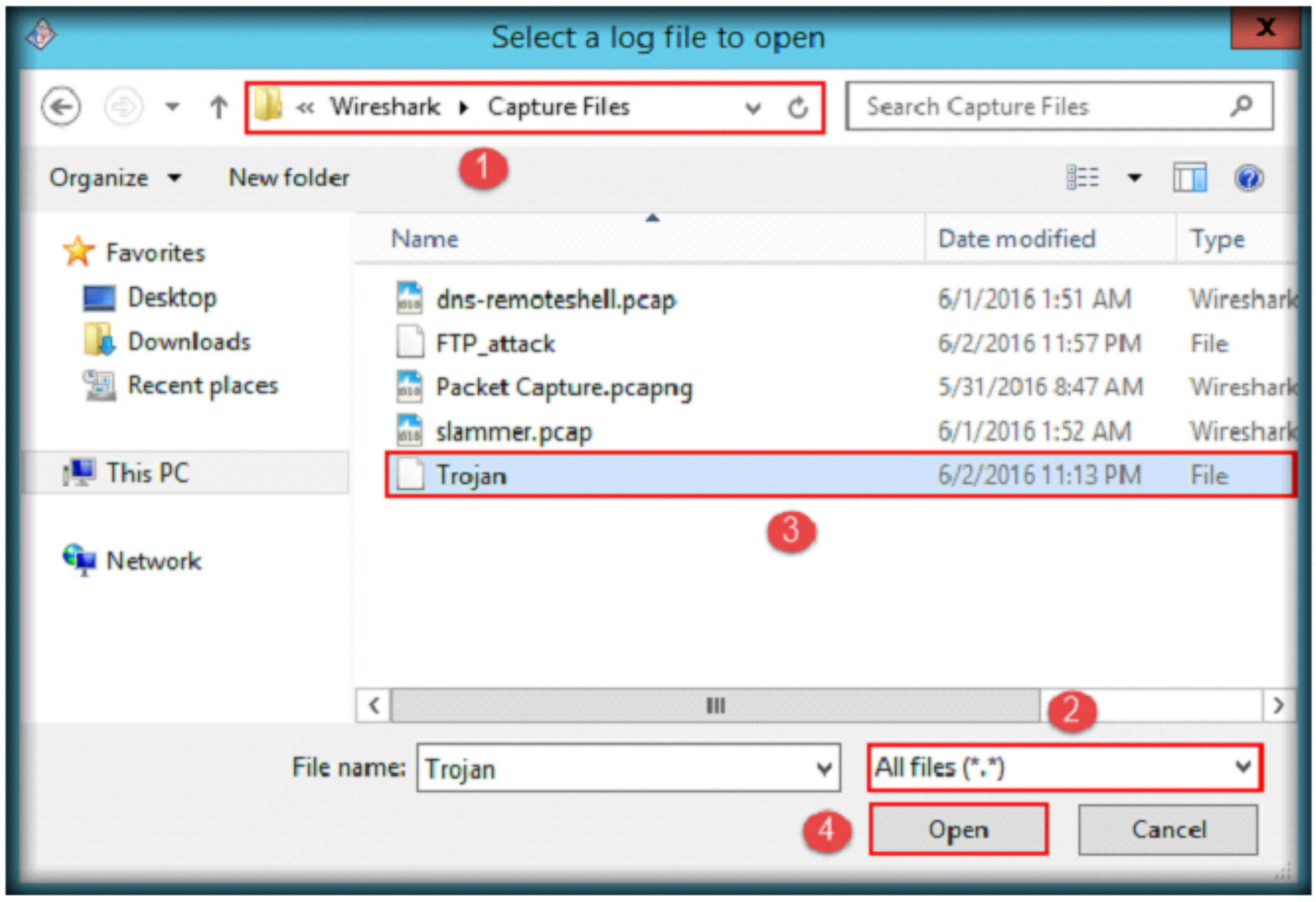

FIGURE 3.4: Selection of Trojan file

6. Kiwi Log Viewer displays all the logs of the selected file. You can analyze these logs, to determine if there was any malicious activity in the network.

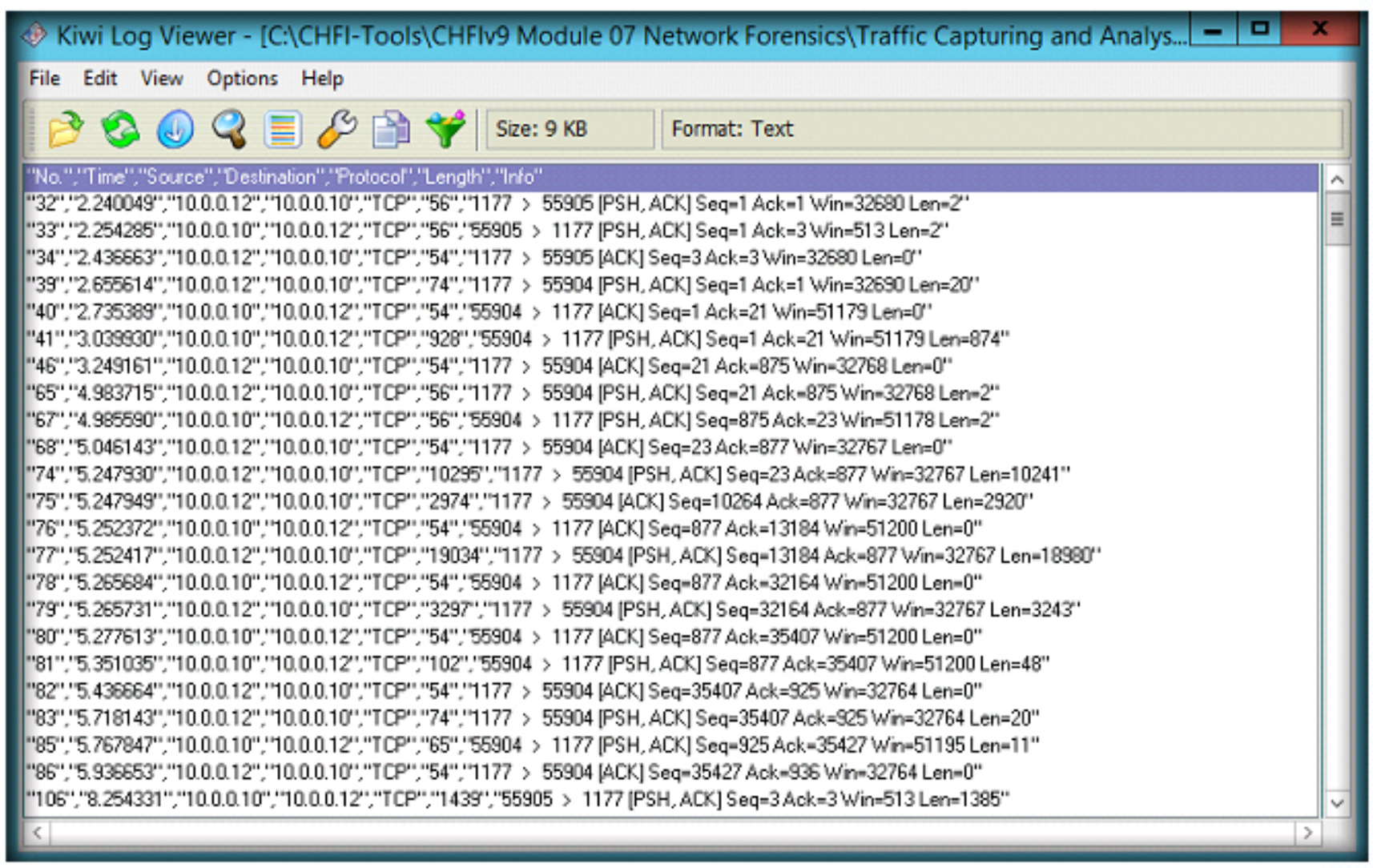

FIGURE 3.5: Logs of the selected file

7. The traffic displayed in the logs indicate that the communication took place between two machines over port 1177, which is the default port used by njRAT. In the highlighted tag, the traffic is flowing from 10.0.0.12 (on port 1177) to 10.0.0.10 (on port 55904).
8. This infers that njRAT client is running on 10.0.0.12 machine, which is found to be the attacker machine.

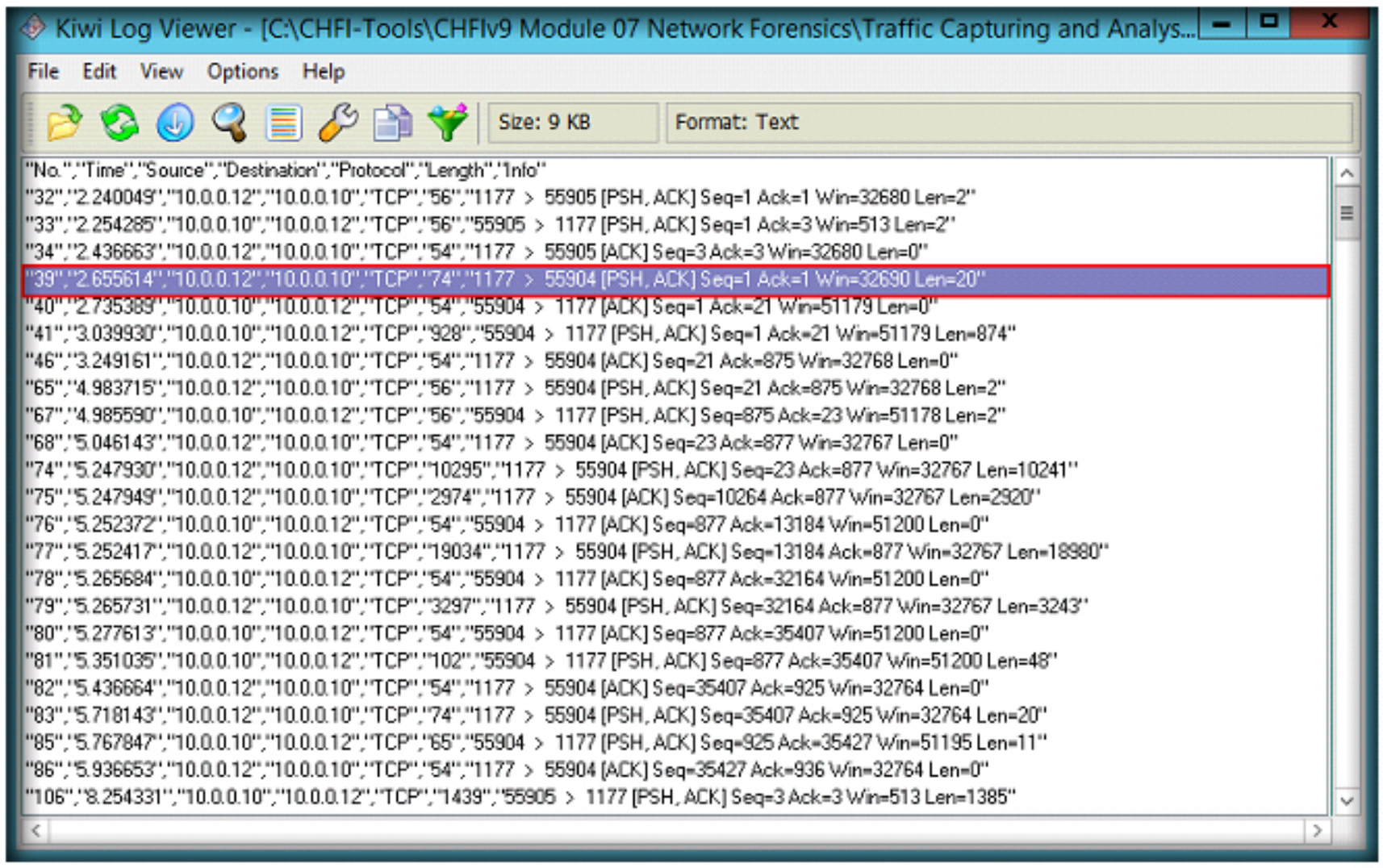

FIGURE 3.6: njRAT client

9. Now, we will look at another file that contains logs which were recorded during a bruteforce attack. Select **File** from the menu bar and click **Open File...**.

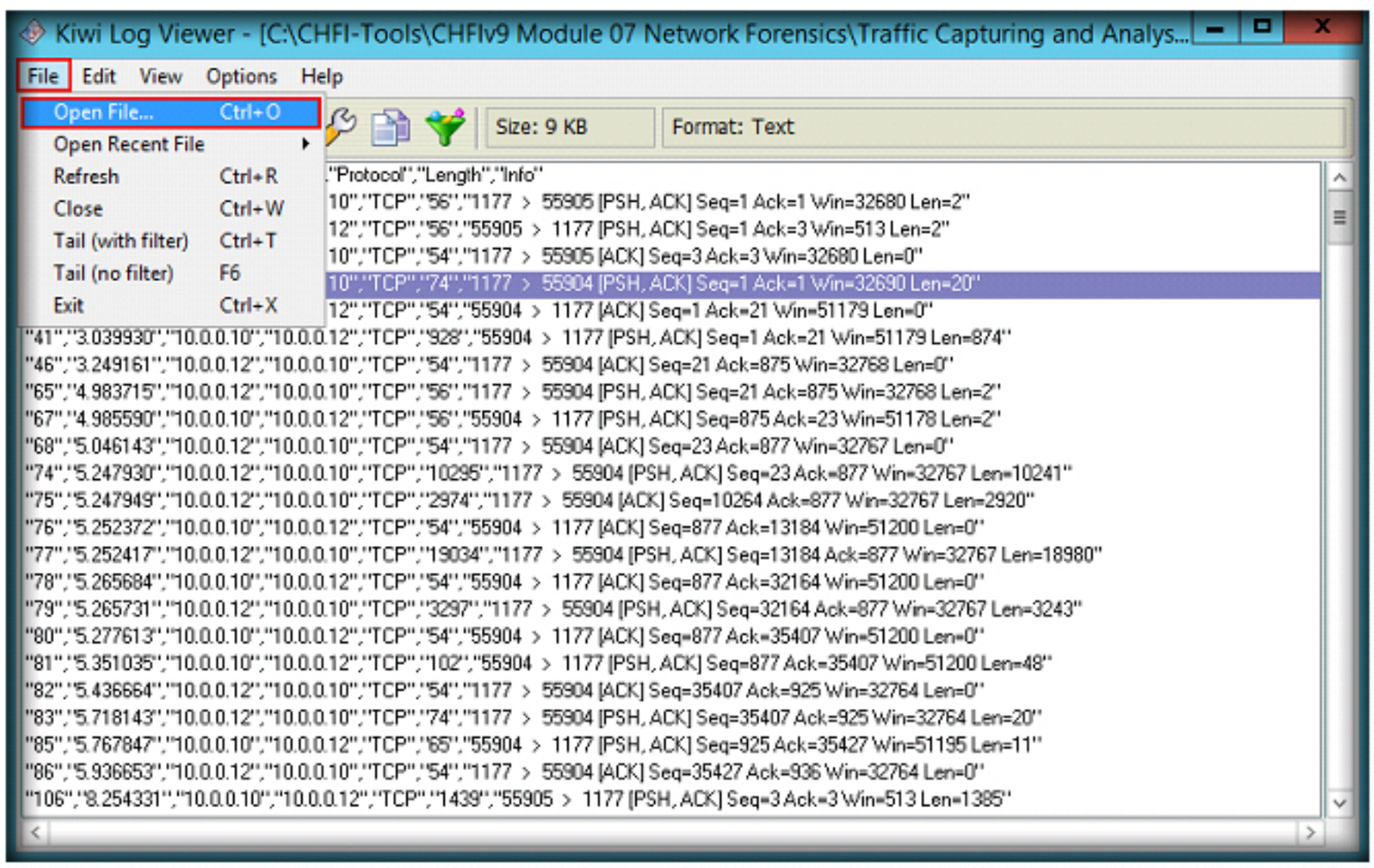

FIGURE 3.7: Open the intrusive log

10. The same location appears from where you have selected the Trojan file. Select **FTP_attack** and click **Open**.

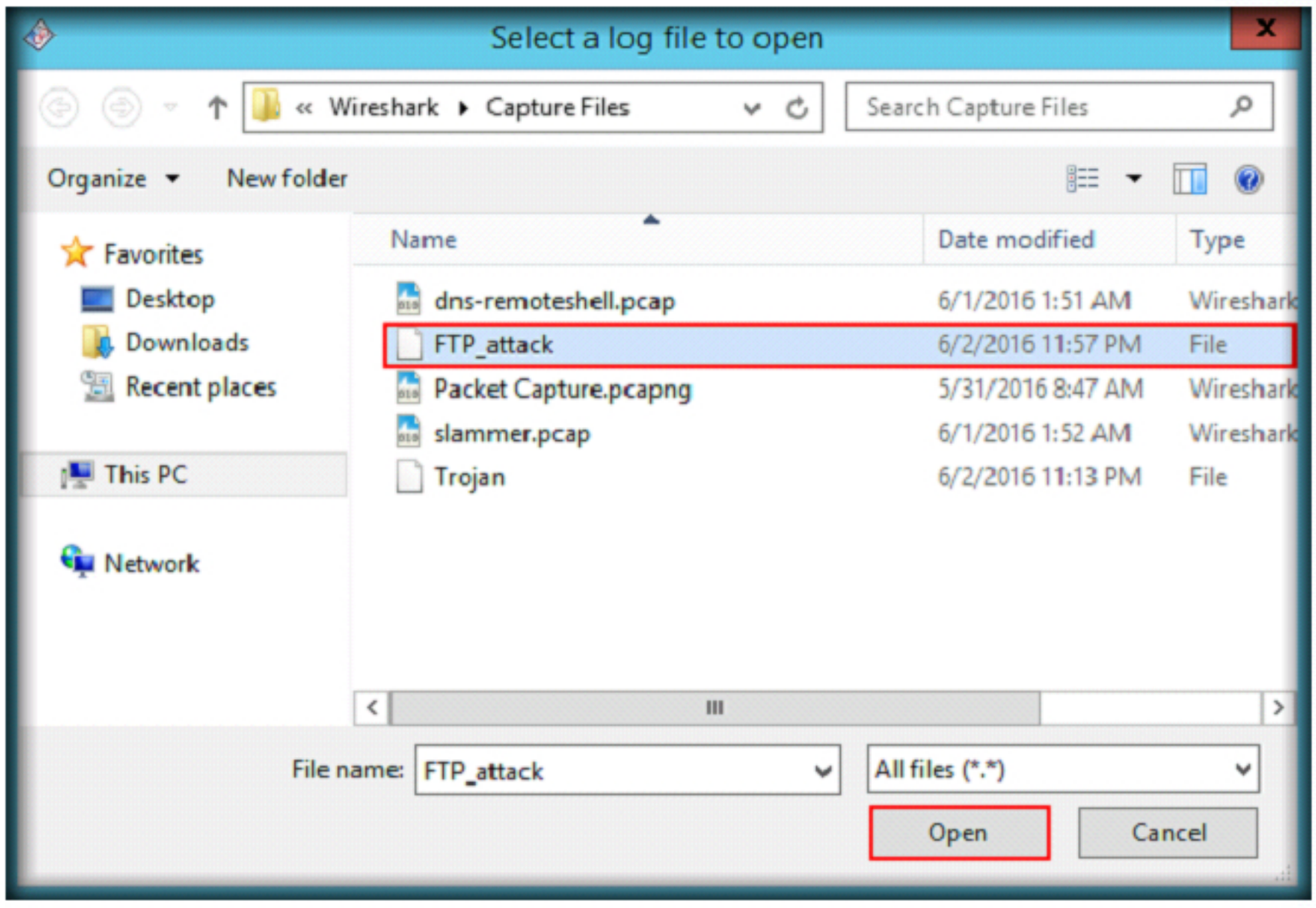

FIGURE 3.8: Open FTP_attack

11. Kiwi Log Viewer application displays all the logs of the file as shown in the following screenshot:

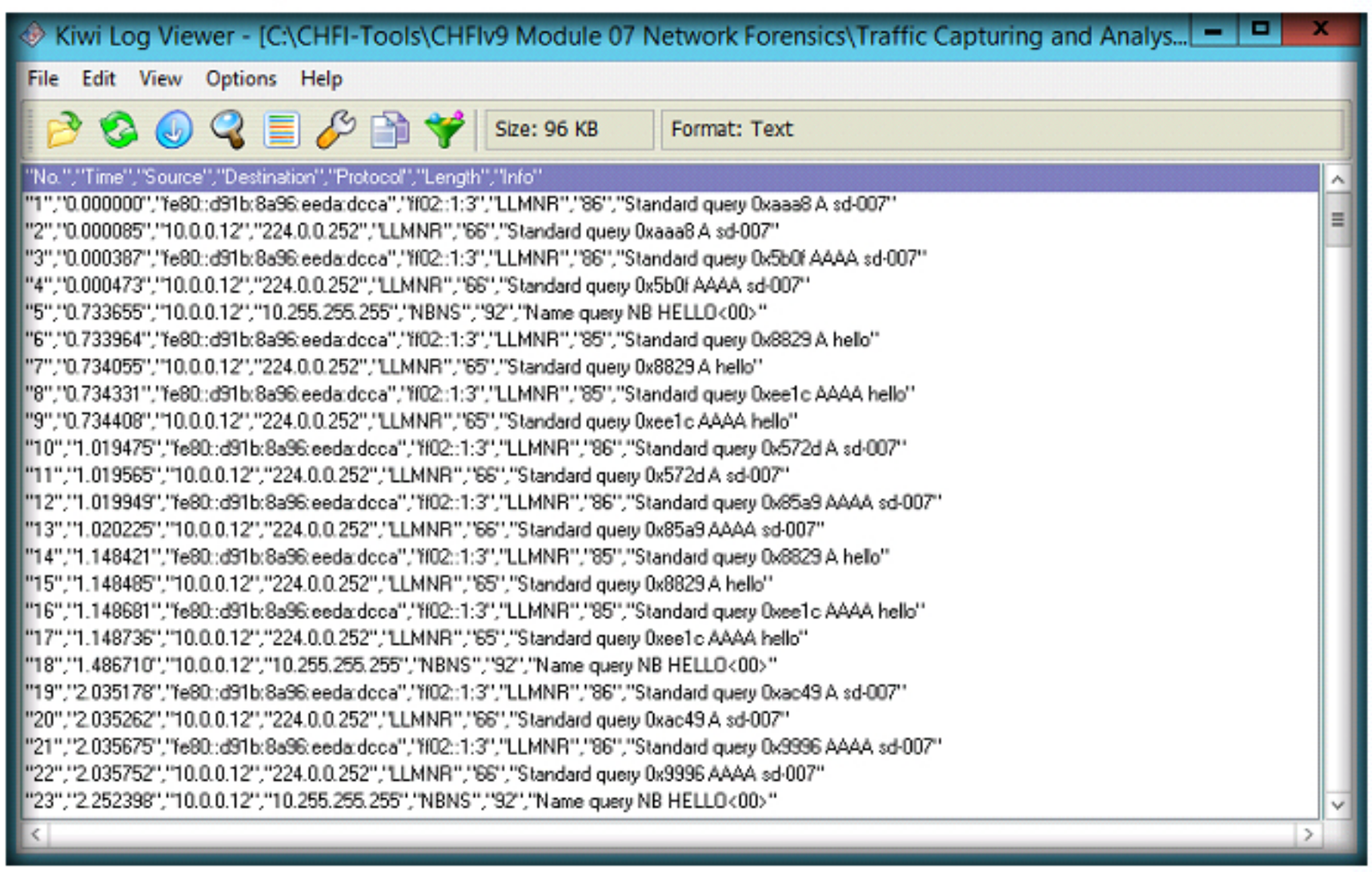

FIGURE 3.9: Kiwi Log Viewer application displays logs of the file

12. Generally, in an attempt to login to an FTP server, when a client enters invalid credentials/valid credentials/no credentials, the server returns various kinds of responses such as Response: 530, Reponse: 230, Response

331, etc. based on the requests. As we are examining logs associated with FTP traffic, we will stress more on the responses, in order to analyze what kind of requests came from the other machine (attacker's machine).

13. As we can see, the FTP server hosted on a machine was constantly responding with 530 Response, which is generated on entering a wrong password.

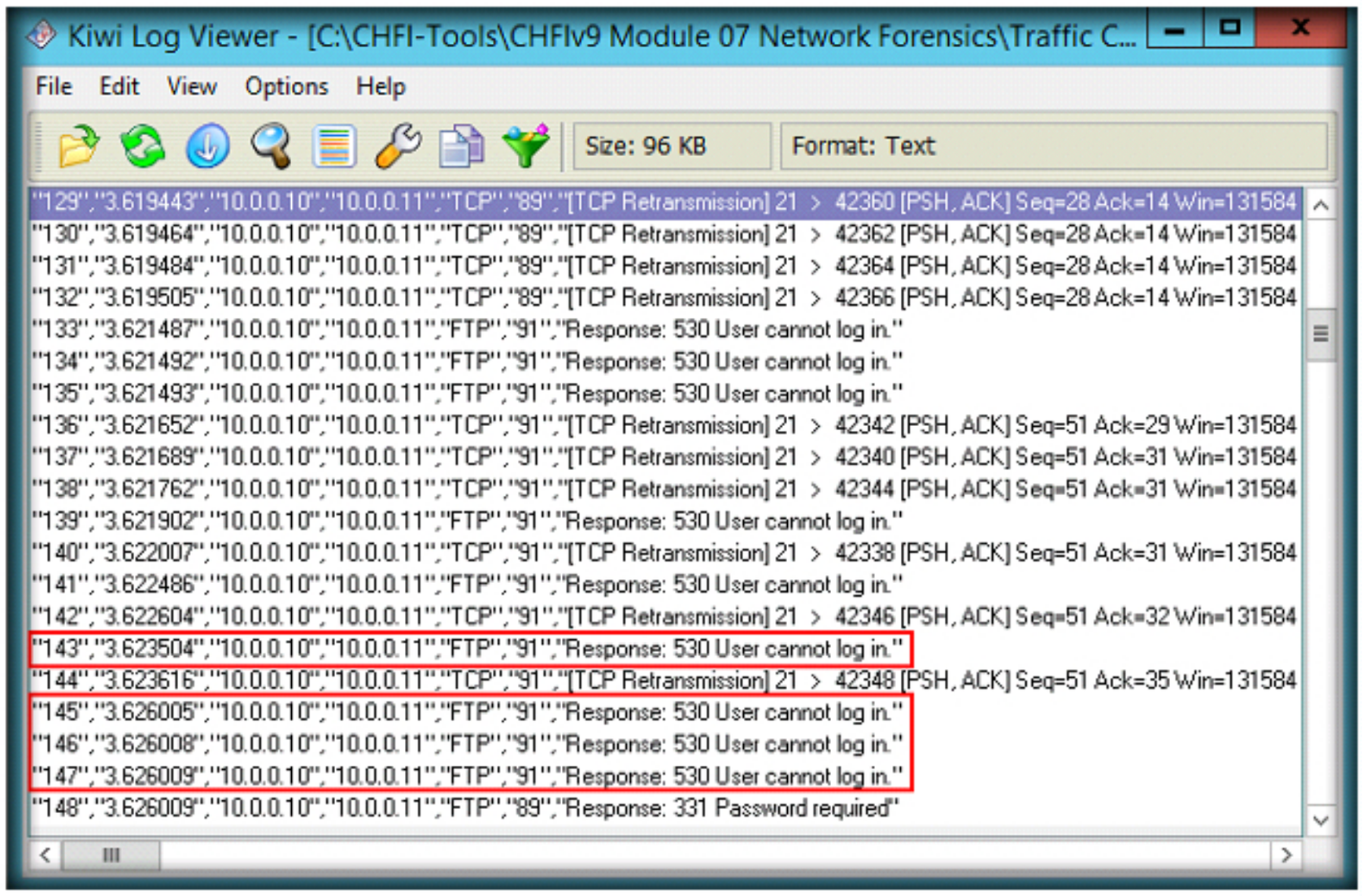

FIGURE 3.10: Kiwi Log Viewer application displays logs of the file

14. To differentiate the responses, we will assign color highlights to the responses. To do so, go to **Options** and select **Highlighting...**.

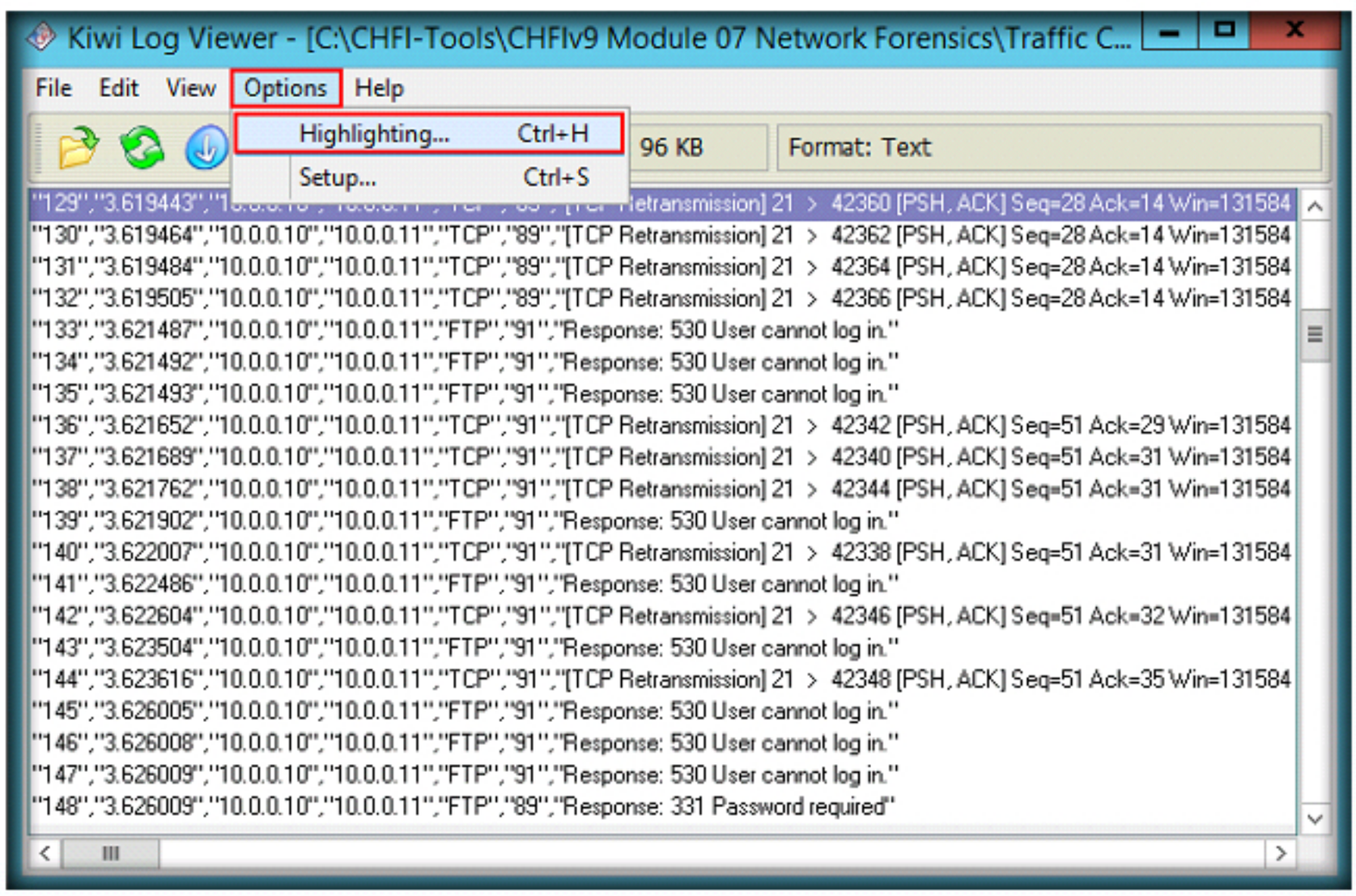

FIGURE 3.11: Kiwi Log Viewer application select Highlighting…

15. Highlighting Options window will appear, click **+** icon. A highlight item appears under the **Highlight items** section. Select the item and enter the string **Response: 530** in the String to match field. Leave the default background color as **Red**.

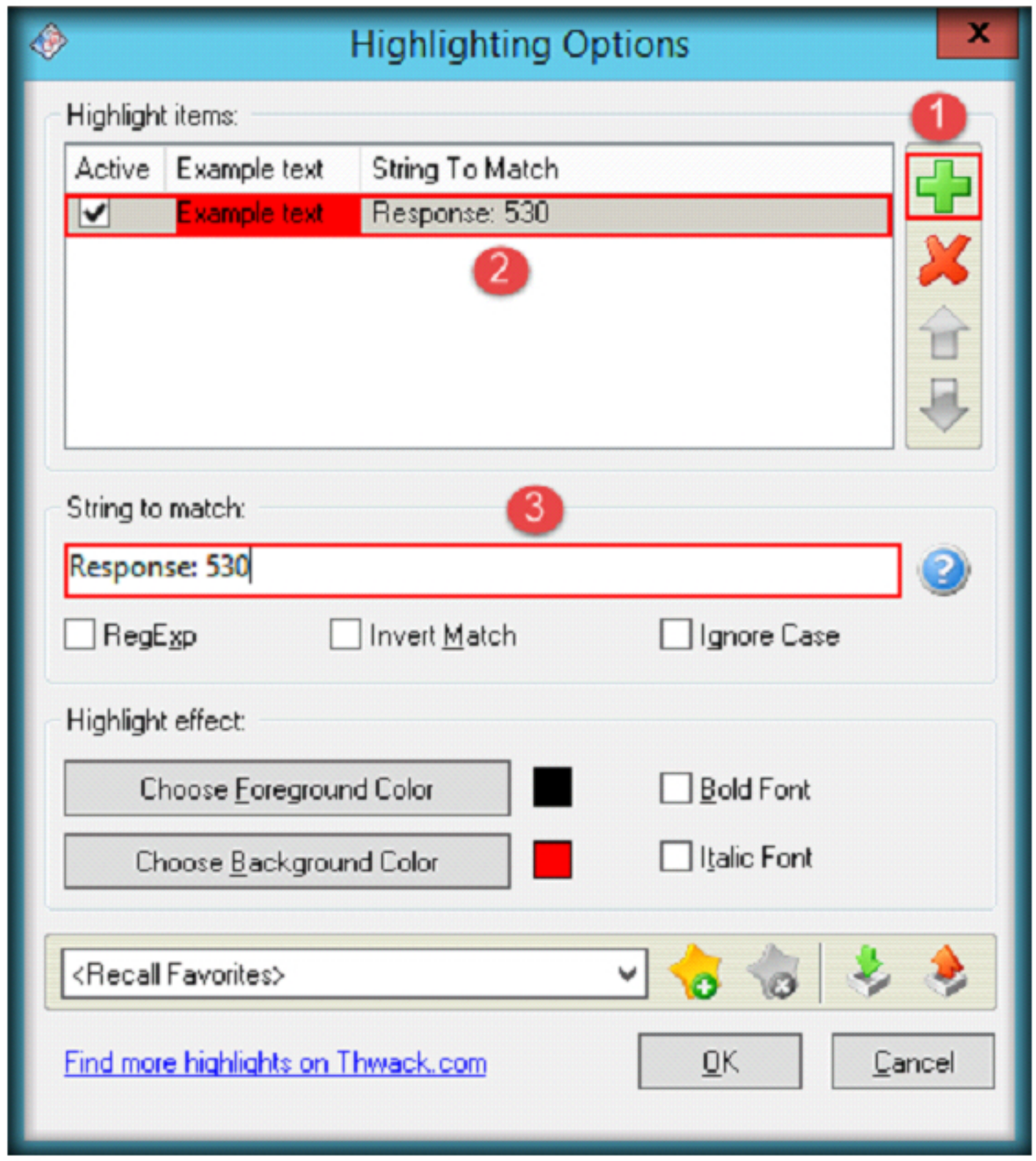

FIGURE 3.12: Kiwi Log Viewer Highlighting Options window

16. By doing this, all the logs containing string **Response: 530** will be highlighted in **Red** color. This will highlight all the logs containing Response: 530 which represents invalid login attempt (wrong password).

17. In the same way, add one more item, issue the string as **Response: 230** to the item, click the **Choose Background Color** option from **Highlight effect** section, select **Green** color and click **OK**. This will highlight all the logs containing Response: 230 which represent successful login occurred by entering valid login credentials.

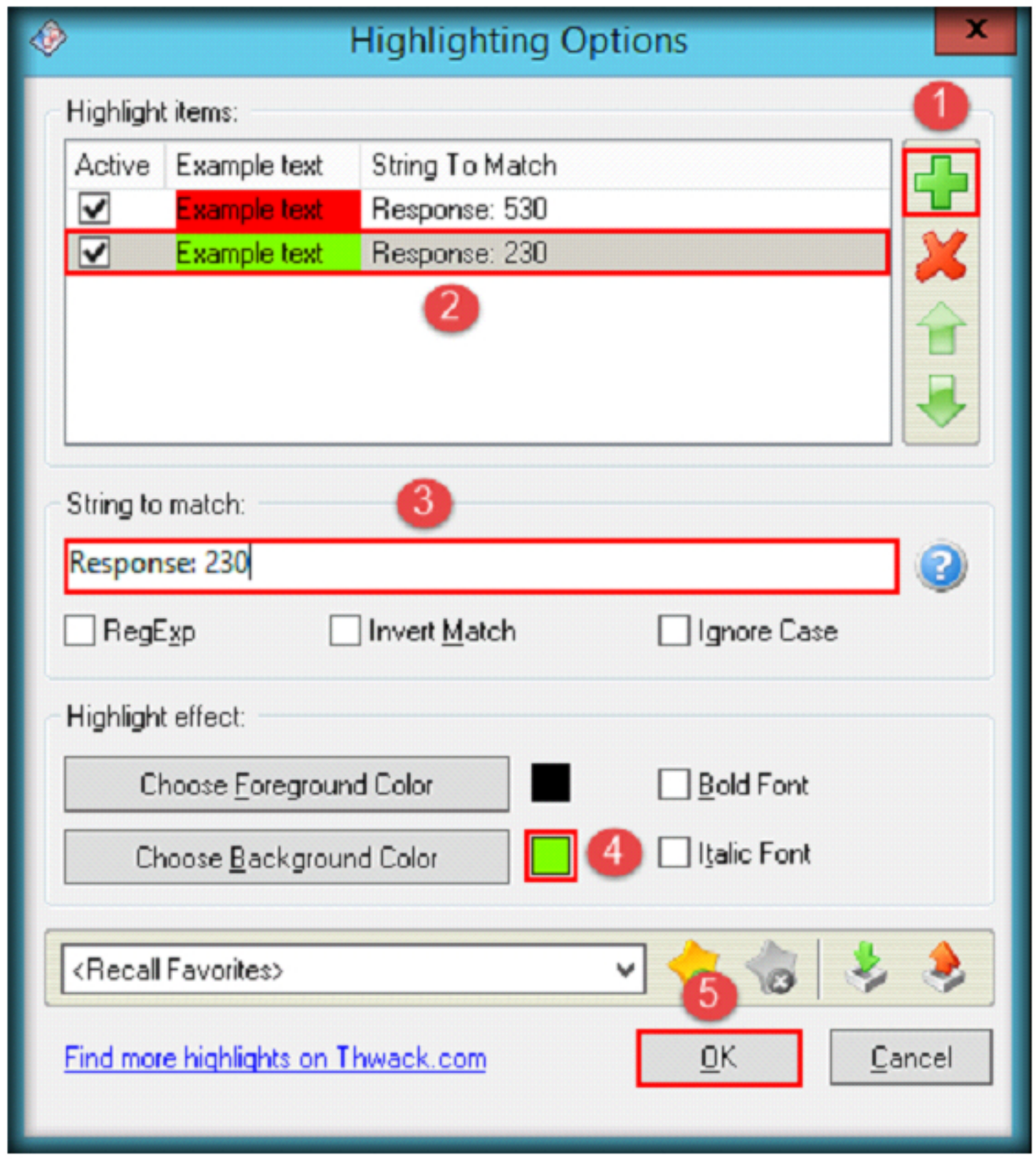

FIGURE 3.13: Kiwi Log Viewer Highlighting Options window

18. Now, you will observe the logs being highlighted as shown in the following screenshot:

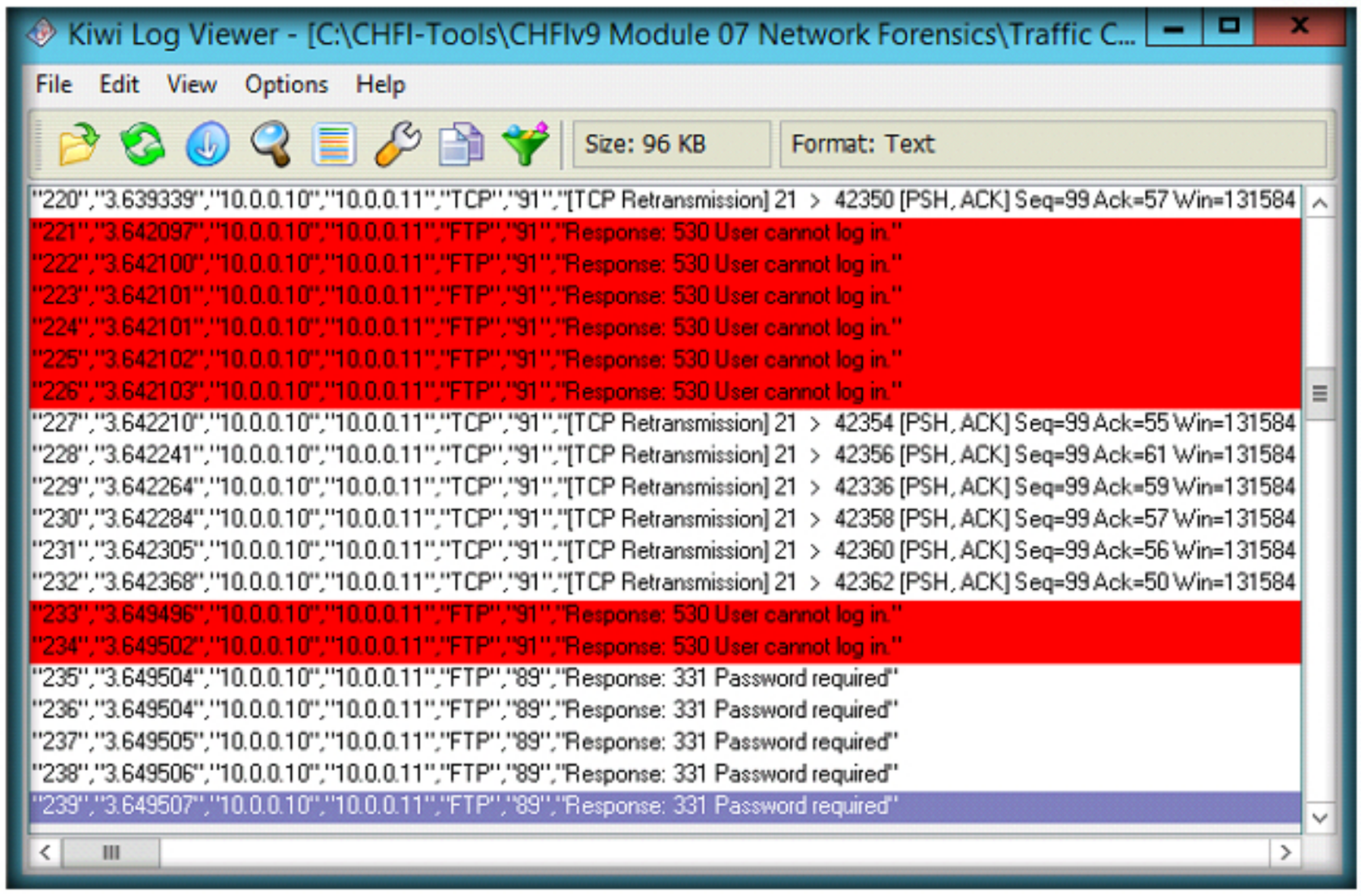

FIGURE 3.14: Kiwi Log Viewer red highlighted logs

19. It is seen that there are more number of logs with red highlight, which infers that huge number of login attempts have occurred on the server, resulting in a brute force attack.

20. Scroll down the logs. You will observe that one of the logs (log no. 329) is highlighted in green, which means the server responded with 230 code, resulting in a successful brute-force attack.

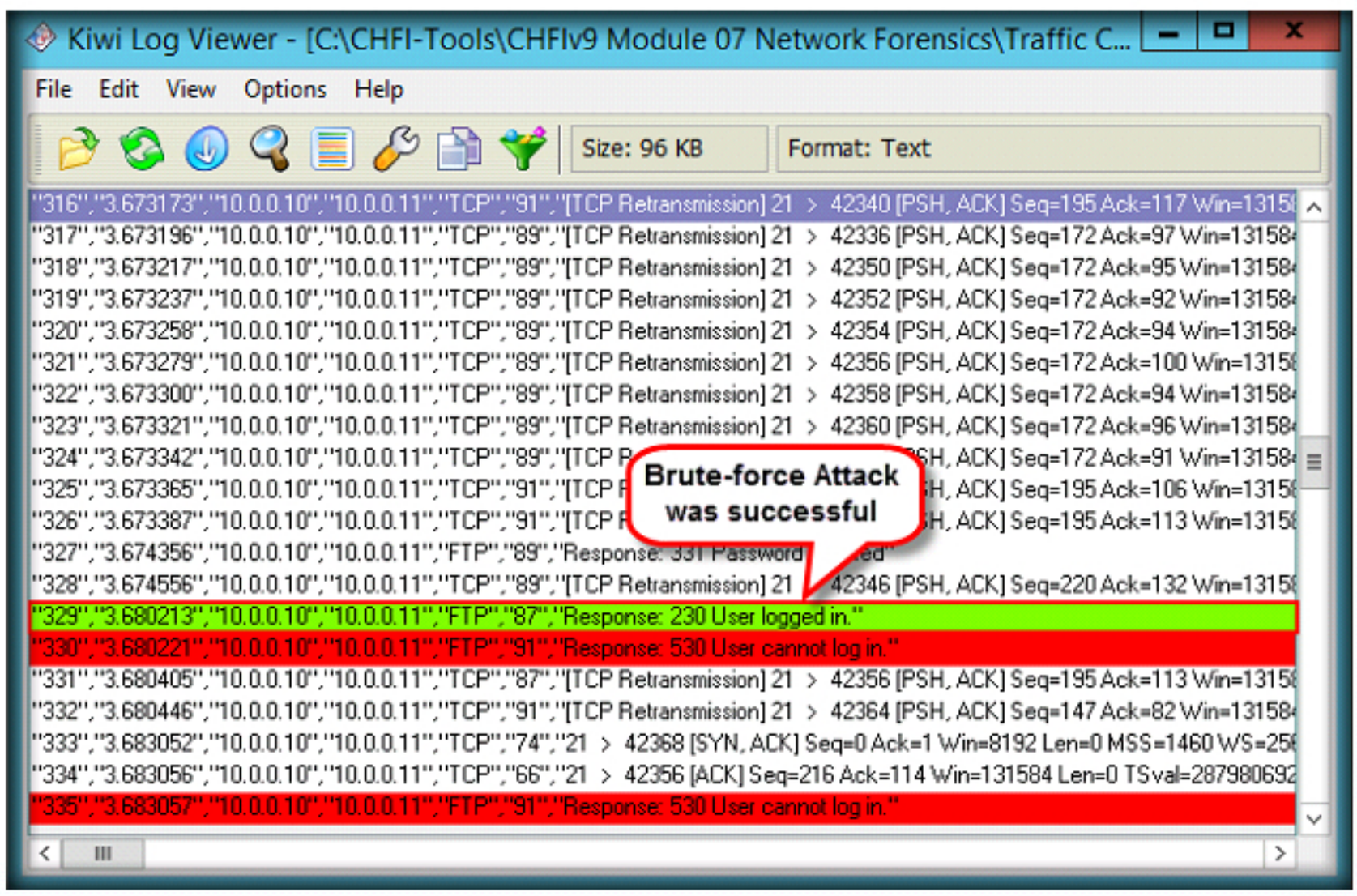

FIGURE 3.15: Kiwi Log Viewer green highlighted log

21. Thus, a forensic investigation has been successfully performed on the log file.

Lab Analysis

Analyze and document the results related to the lab exercise.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☐ Yes	☑ No
Platform Supported	
☑ Classroom	☑ iLabs

Lab

4

Investigating Network Traffic Using Wireshark

Wireshark is a network packet analyzer. A network packet analyzer will try to capture network packets and display packet data in detail.

ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

Lab Scenario

A publishing company has been facing troubles since someone from the company has been leaking its documents. The company has secretly called an investigator to look into the matter without letting the perpetrator know about their plans. In such cases, the investigator should use tools that could help them capture the network traffic.

To be an expert **forensic investigator**, you must have sound knowledge of capturing the live data packets, sniffing the network packets, and analyzing the network traffic.

To be an expert **forensic investigator**, you must have sound knowledge of how to investigate packet capture files in search of anomalies in the network.

Lab Objectives

The objective of this lab is to demonstrate how to capture the live data packets of a network. The primary objectives of this lab are:

- Capturing the packets of a network
- Analyzing incoming and outgoing packets

Tools demonstrated in this lab are available in C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics

Lab Environment

In this lab, you need:

- Wireshark located at **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Traffic Capturing and Analysis Tools\Wireshark**.
- If you decide to download the latest version, screenshots shown in the lab might differ.

- A computer running **Windows Server 2012** virtual machine.
- Administrative privileges to run the tool.
- A web browser with **Internet** connection.
- You can also download the latest version of **Wireshark** from the link https://www.wireshark.org/download.html (click **Windows Installer (64-bit)**).
- If you are installing the latest version of Wireshark, then steps and screenshots might vary from the ones demonstrated in this lab.

Lab Duration

Time: 20 Minutes

Overview of Wireshark

Wireshark is a network packet analyzer. Wireshark uses Winpcap to capture packets, so it can only capture the packets on the networks supported by Winpcap.

Wireshark captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks. A set of filters for customized data display can be refined using a display filter.

Lab Tasks

TASK 1

Launch Wireshark

1. Navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Traffic Capturing and Analysis Tools\Wireshark**.
2. Double-click **Wireshark-win32-1.6.1.exe** to launch the setup and follow the wizard-driven installation instructions.

Note: If an **Open File - Security Warning** pop-up appears, click **Run**.

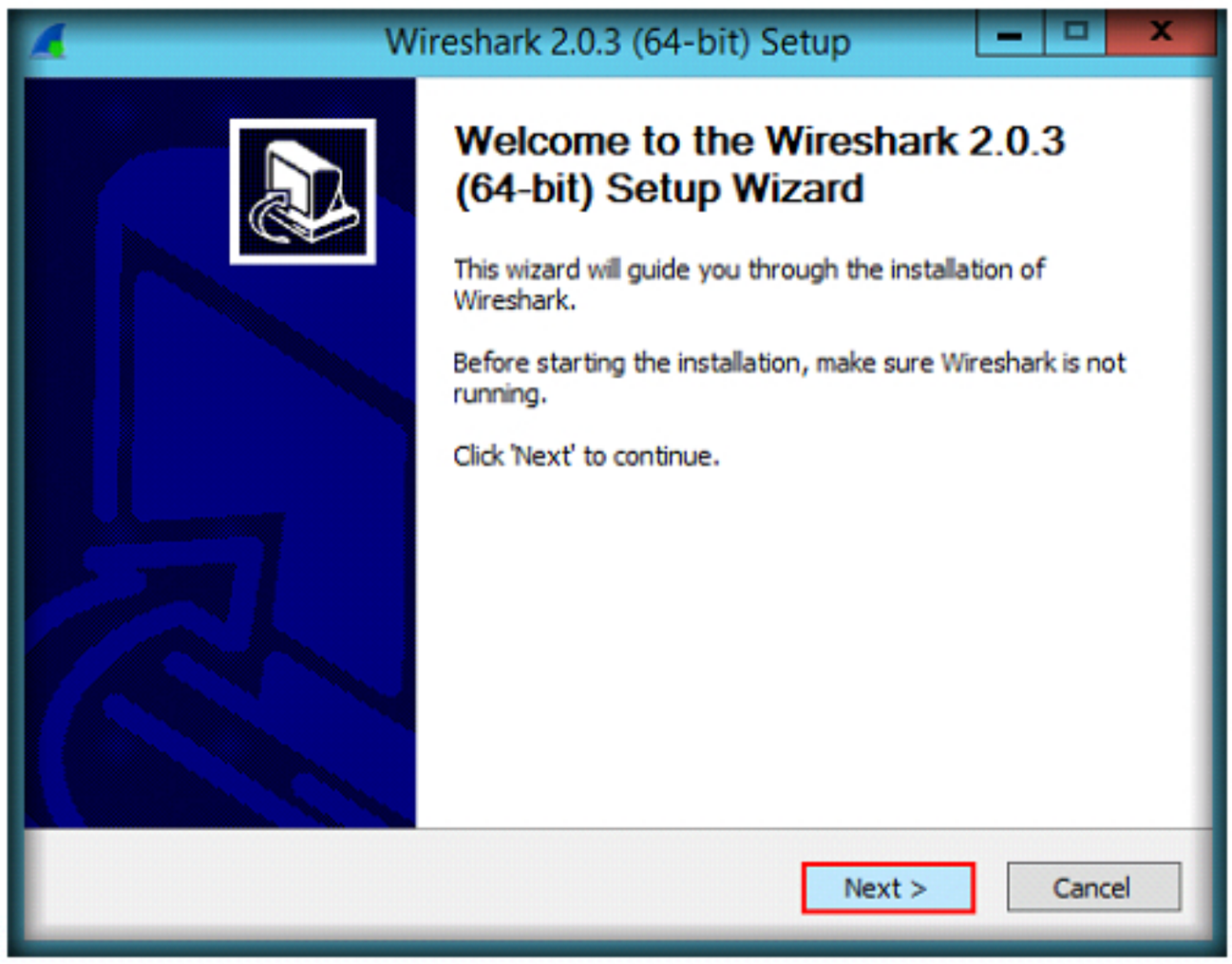

FIGURE 4.1: Wireshark Installation Setup wizard

TASK 2

Investigate for Plain Text Passwords

3. After completing the installation, navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Traffic Capturing and Analysis Tools\Wireshark\Capture Files** and double-click **Packet Capture.pcapng**.

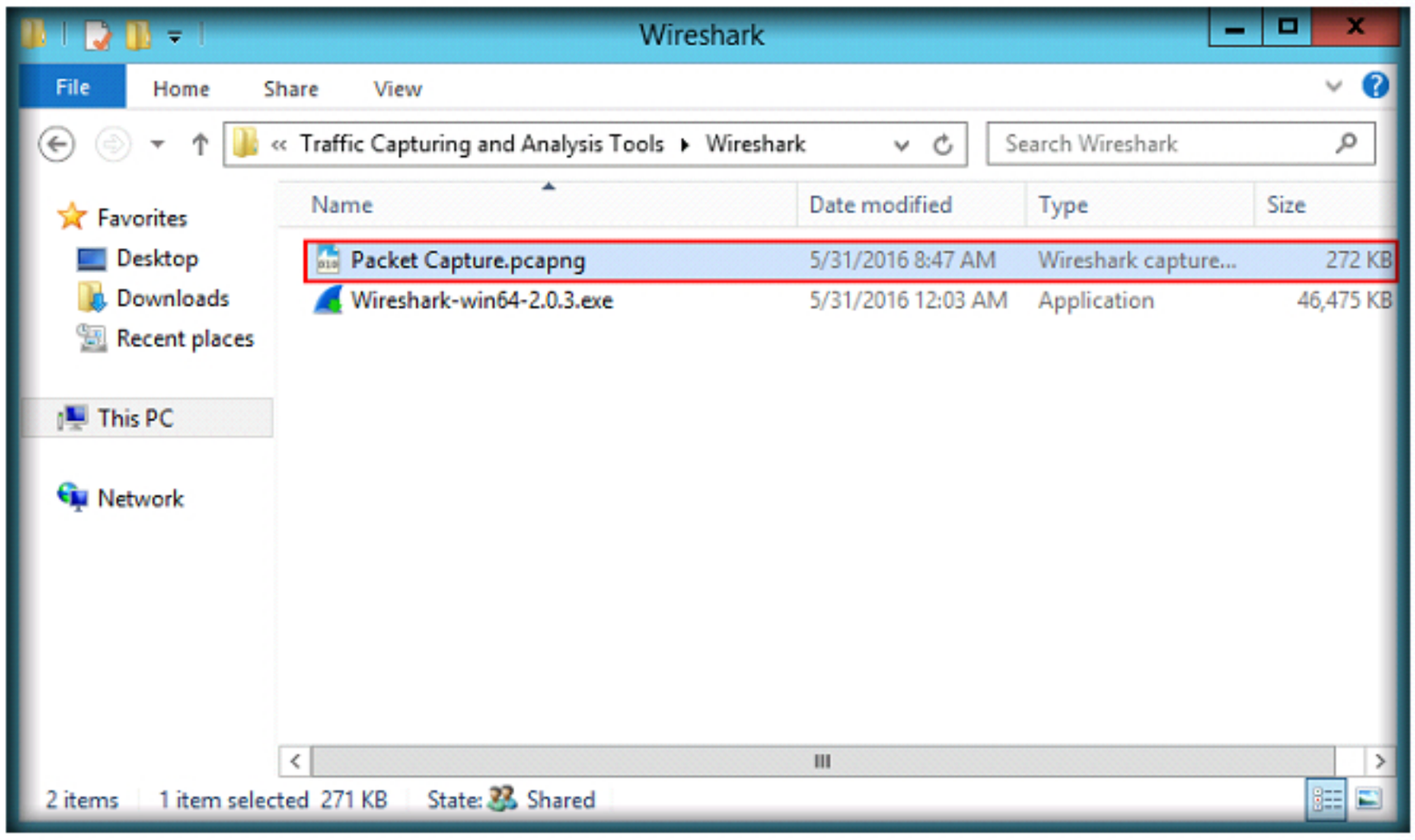

FIGURE 4.2: Packet Capture.pcapng

4. Captured packets appear in Wireshark interface as shown in the following screenshot:

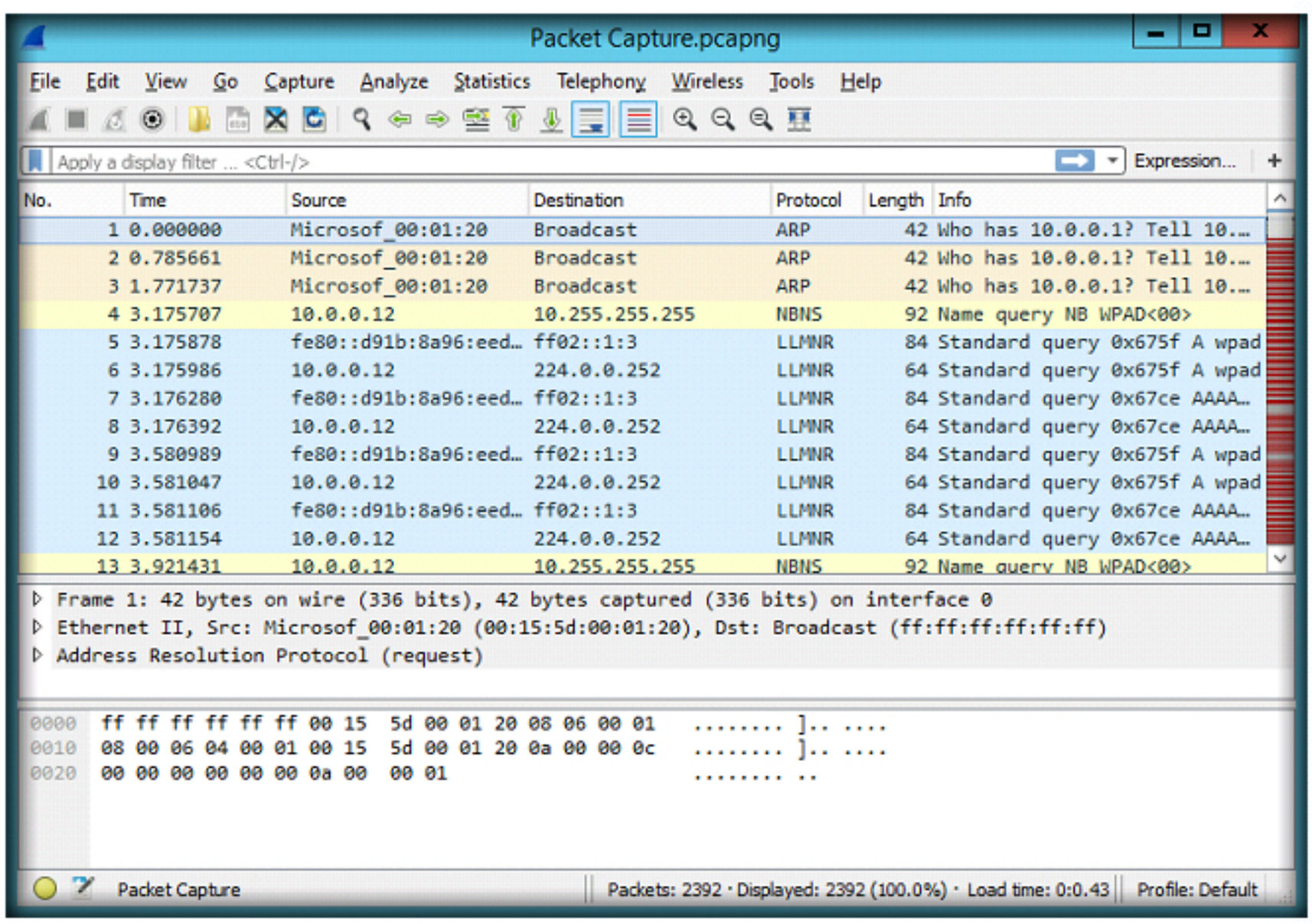

FIGURE 4.3: Wireshark Captured packets

5. Now, we will investigate the traffic to see if there are any plain text passwords stored in it.

6. Type **http** in the **Filter** field and press **Enter** to filter the http traffic.

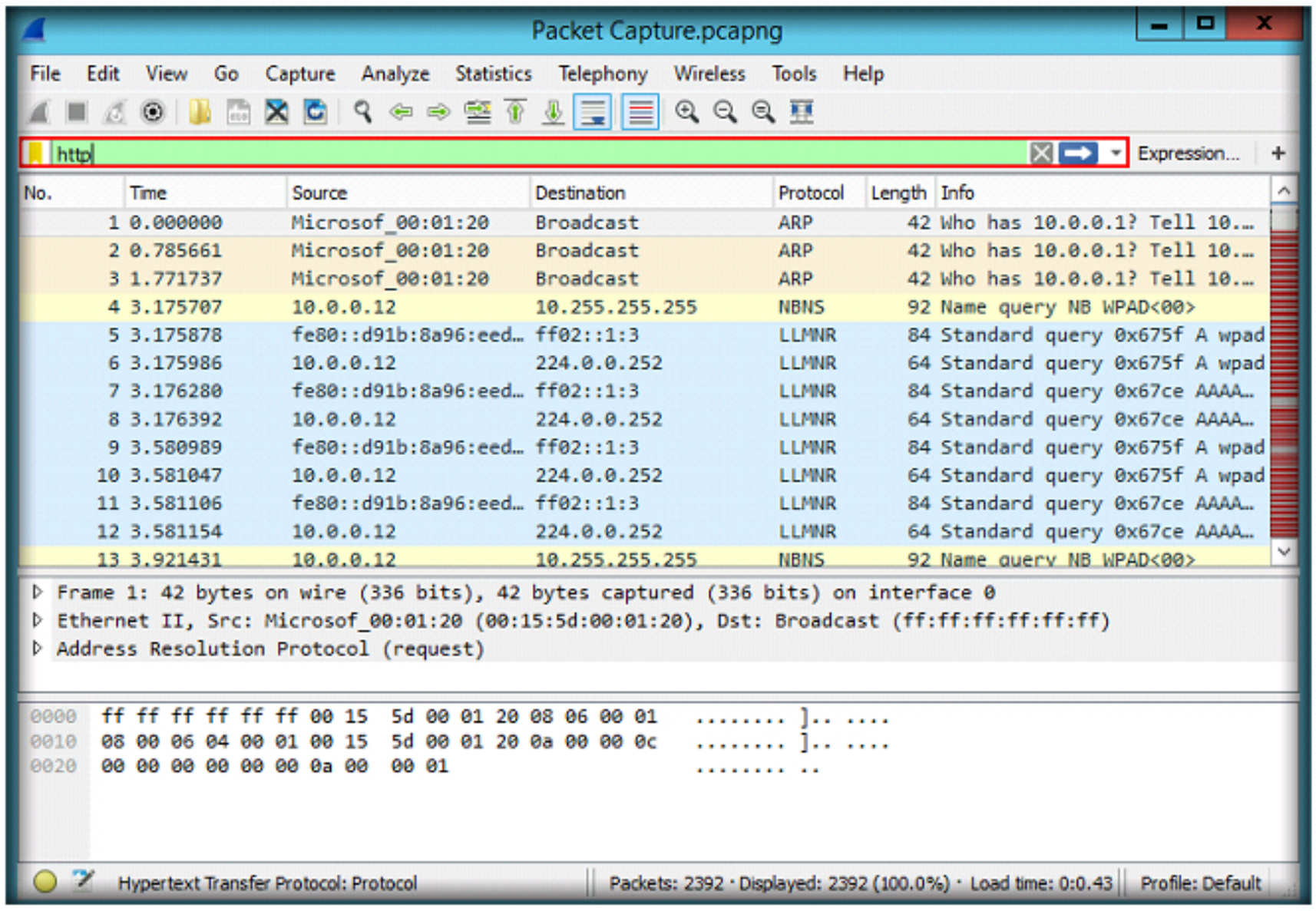

FIGURE 4.4: Wireshark Filter field

Wireshark uses:

- Network administrators use it to troubleshoot network problems.
- Network security engineers use it to examine security problems.
- Developers use it to debug protocol implementations.
- People use it to learn network protocol internals.

7. The screenshot shown below represents the traffic generated through **http**.

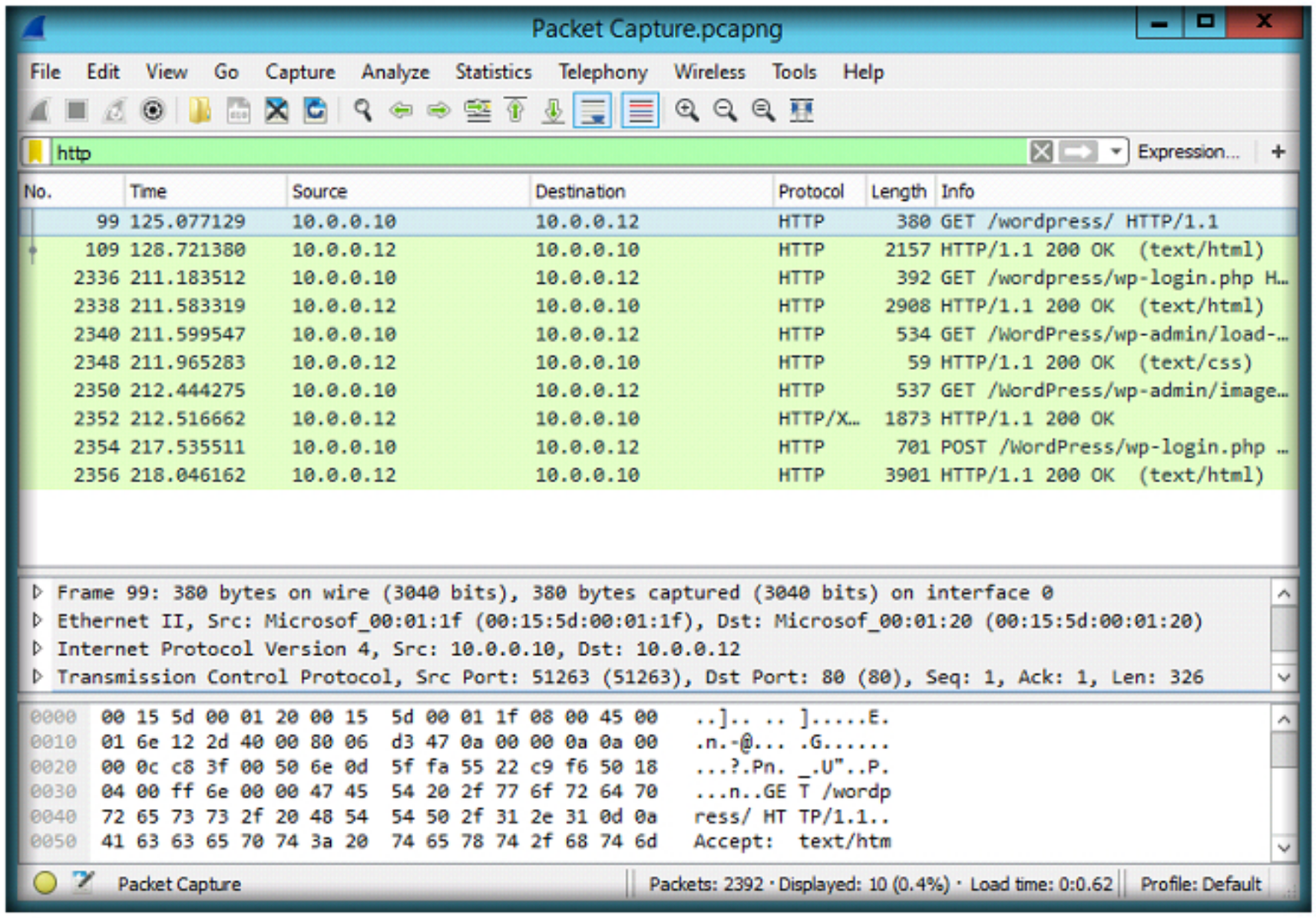

FIGURE 4.5: Wireshark http traffic

8. From the above screenshot, it is evident that the **http** traffic is associated with a WordPress website, and it is travelling in plain text format.

9. Generally, user credentials are stored in the POST requests. So, examining the packet containing the POST request can help you find the user credentials.

10. So, type the filter **http.request.method == POST** in **Filter** field and press **Enter**. Wireshark filters the traffic containing POST requests and displays them as shown in the following screenshot:

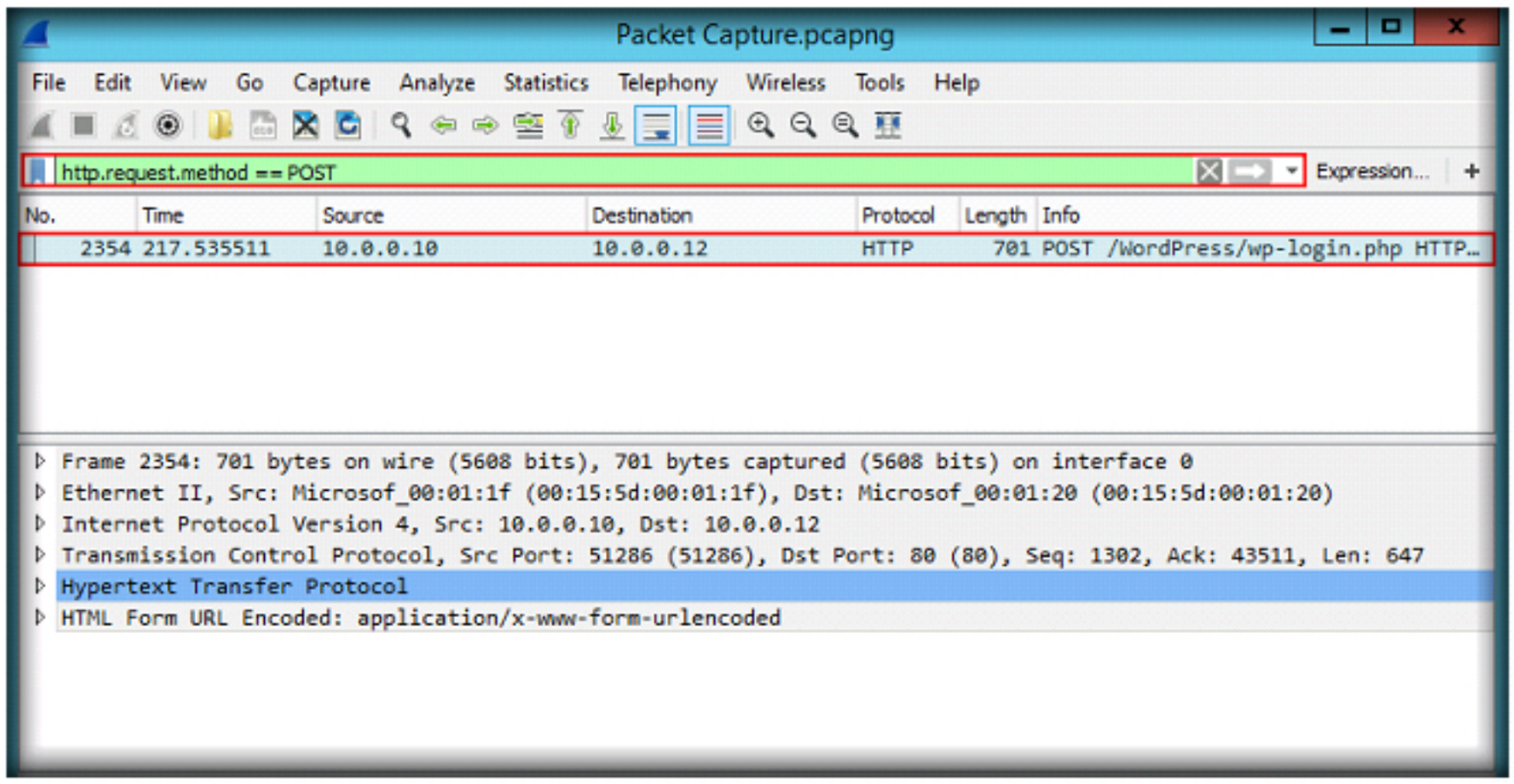

FIGURE 4.6: Wireshark Filtered traffic

11. The user credentials stored in this request can be found under the **Packet Details** pane, under the **HTML Form URL Encoded** node.

12. Expand the **HTML Form URL Encoded** node. The user credentials of one of the user accounts have been found successfully as shown in the following screenshot:

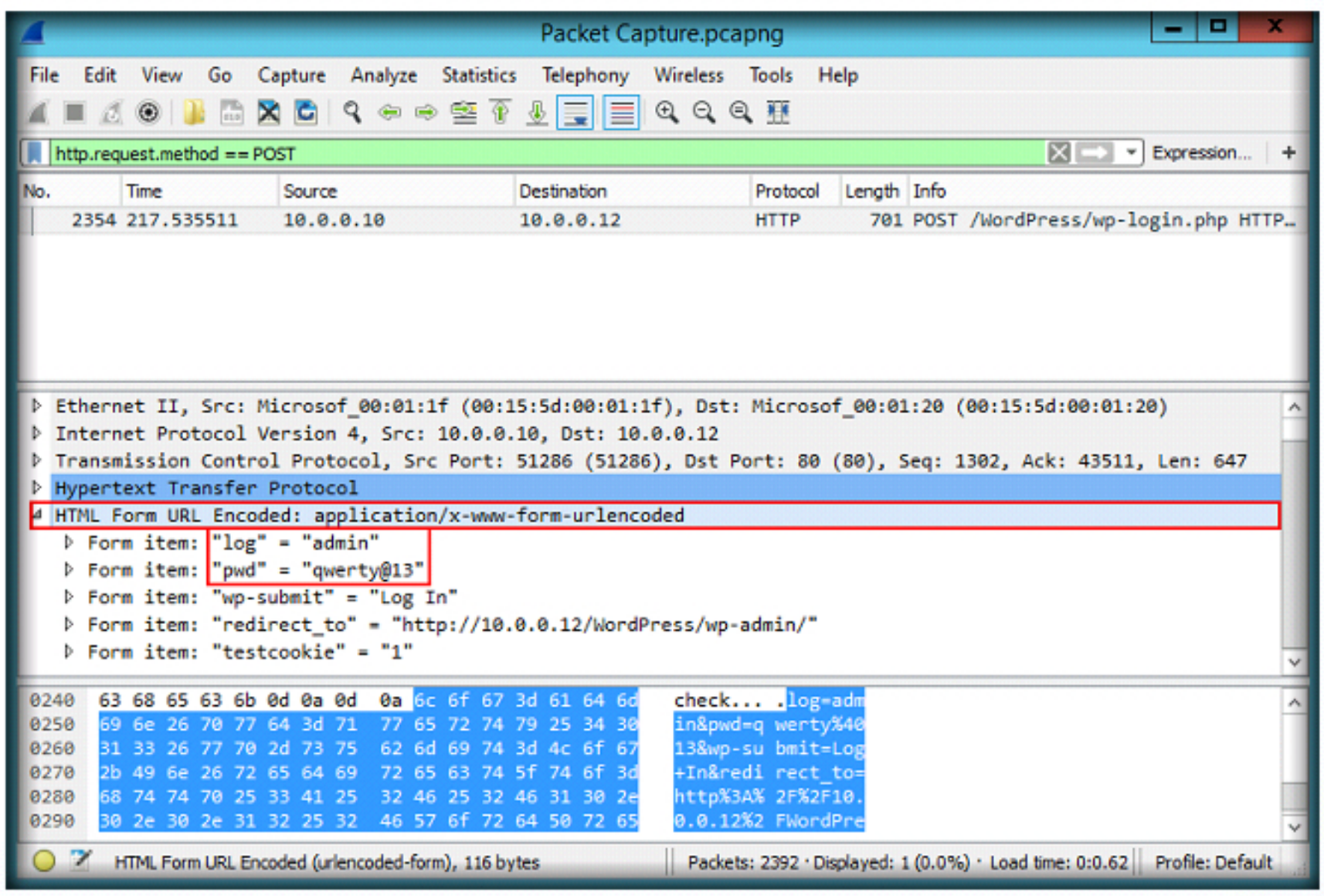

FIGURE 4.7: Wireshark Expanded HTML Form URL Encoded node

TASK 3

Investigate for DNS Anomalies

13. Now, we shall look for DNS Anomalies in the network. Close the current packet capture file in Wireshark.

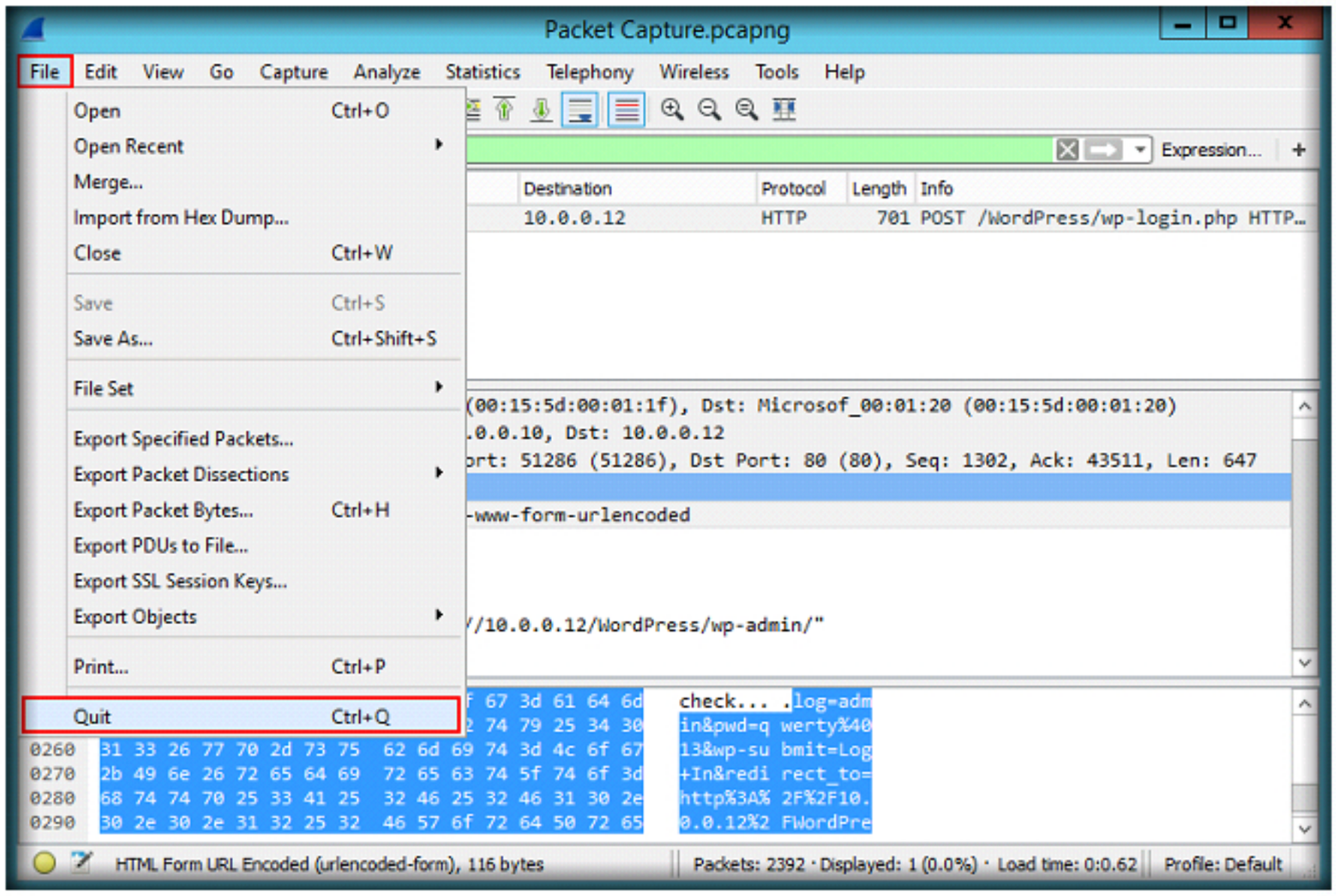

FIGURE 4.8: Wireshark close packet capture file

14. Navigate to **C:\CHFI-Tools\CHFIv9 Module 07 Network Forensics\Traffic Capturing and Analysis Tools\Wireshark\Capture Files** and double-click **dns-remoteshell.pcap**. The capture file opens in Wireshark as shown in the following screenshot:

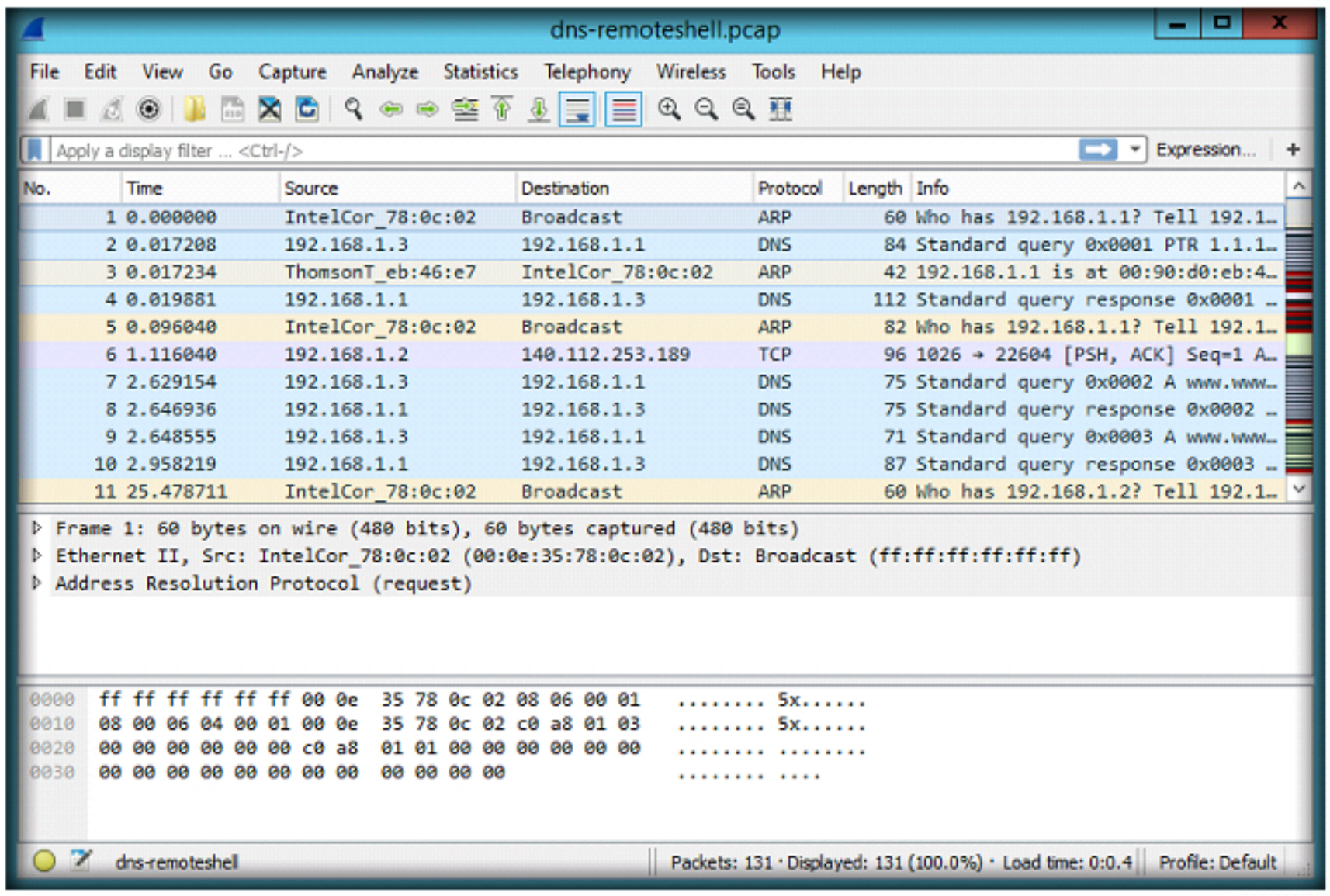

FIGURE 4.9: Wireshark DNS Anomalies

15. In this lab, we will demonstrate a DNS anomaly caused by remote shell riding on DNS port.
16. Since DNS uses port 53 for communication, we shall be filtering the traffic flowing on port number 53. To filter, type the command **tcp.port == 53** in the **Filter** field and press **Enter**. Wireshark filters the traffic flowing on port 53 and displays it as shown in the following screenshot:

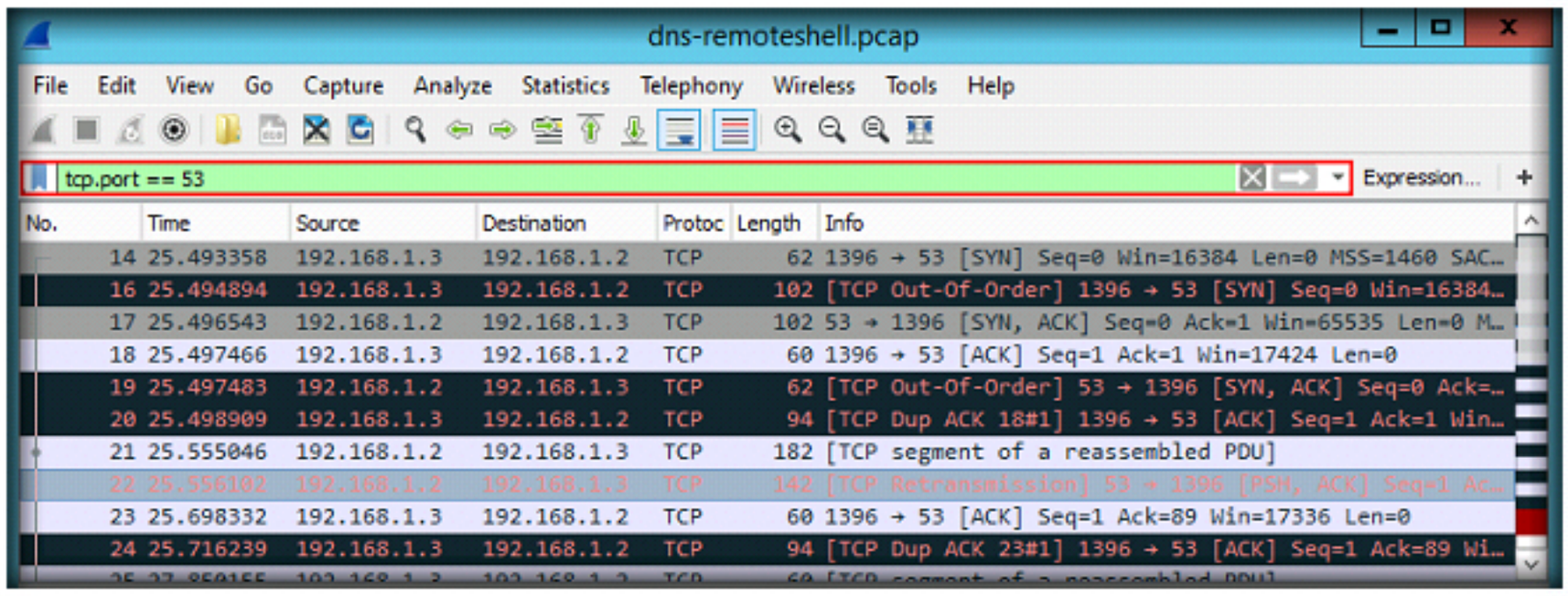

FIGURE 4.10: Wireshark Filtered traffic

17. To view the data in a sequence, we will use **Follow TCP Stream** option in Wireshark.
18. Now, you need to examine the data flowing though these packets. To view the data in a sequence, we will use **Follow TCP Stream** option in Wireshark.
19. Right-click on any one of the packets between 14 and 38 (here, packet **16**), select **Follow** and click **TCP Stream** from the drop-down list.

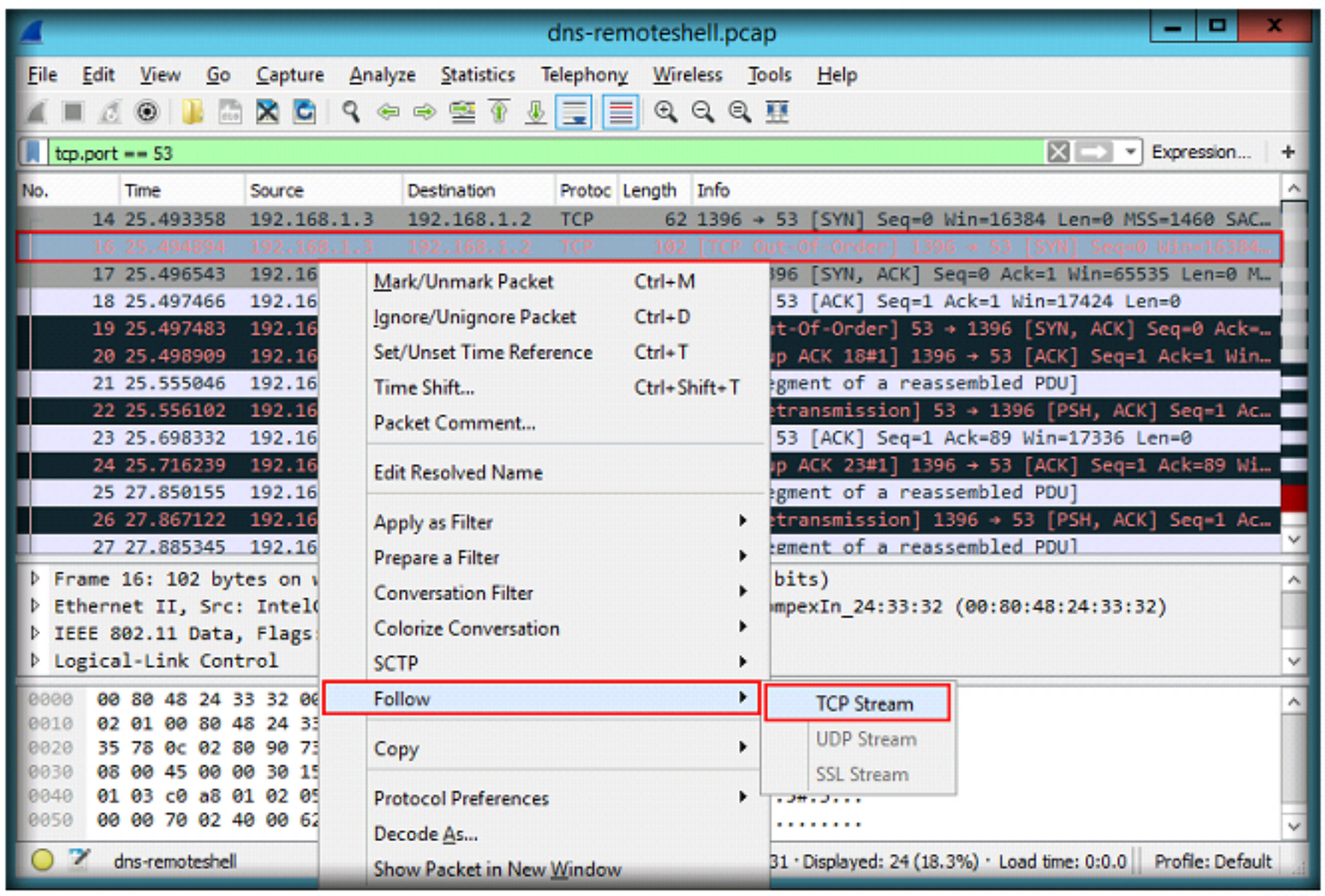

FIGURE 4.11: Wireshark TCP Stream

20. You can observe that a remote shell has been established on port 53, and the directory listing has been performed on the remote machine; which is evident from the following screenshot:

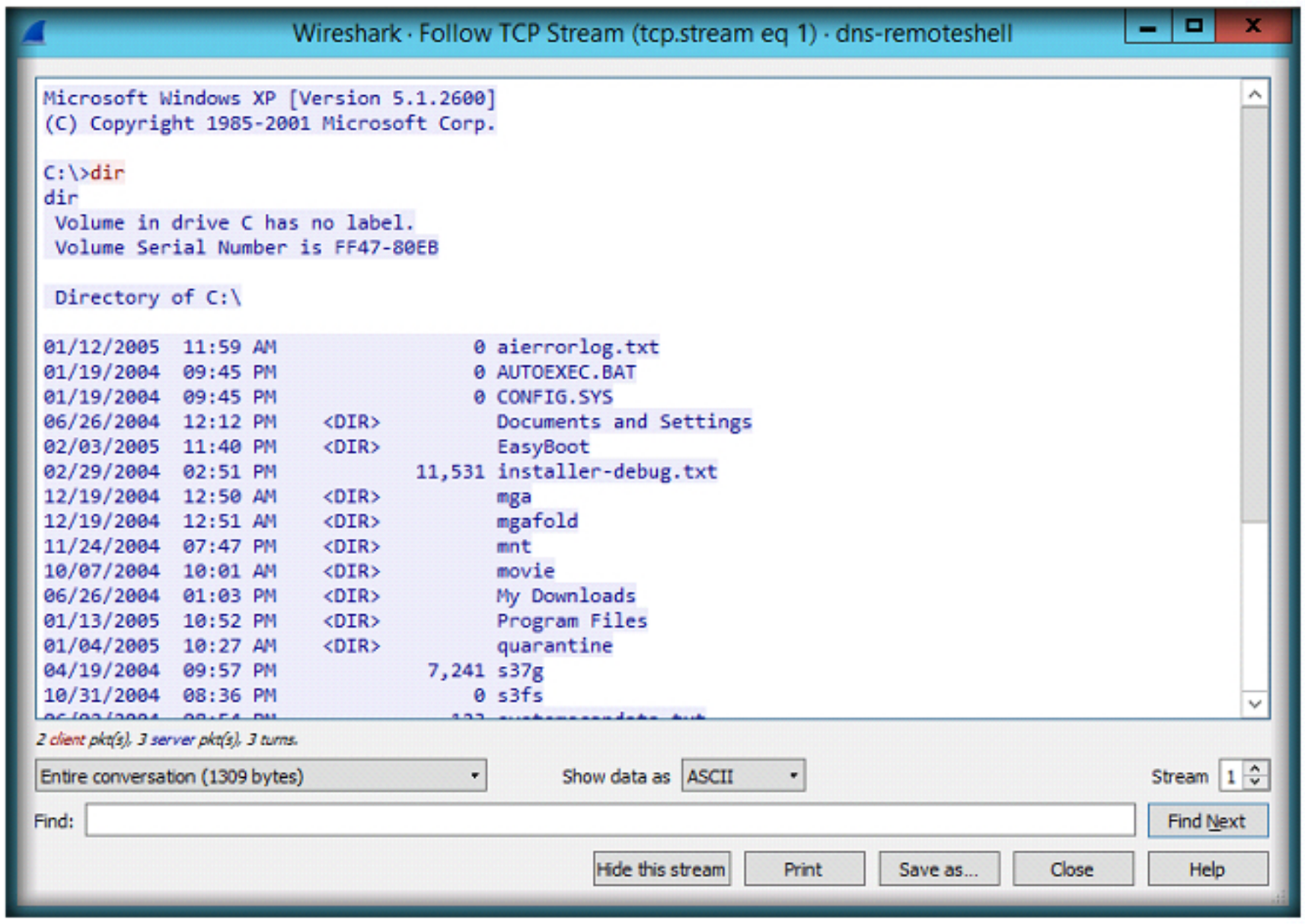

FIGURE 4.12: Wireshark TCP Stream result

21. This way, you may analyze the capture file, as a part of forensic investigation.

Lab Analysis

Analyze the captured packets and document the results related to the lab exercise. Give your expert opinion on the target network.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS RELATED TO THIS LAB.

Internet Connection Required	
☑ Yes	☐ No
Platform Supported	
☑ Classroom	☐ iLabs