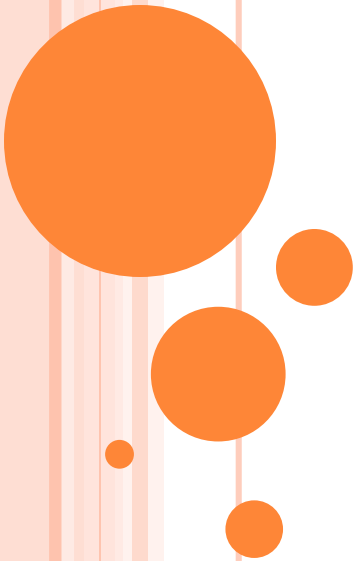


INVESTIGATING WINDOWS ENVIRONMENT---PART1

INCIDENT RESPONSE METHODOLOGY

- **Detection of incidents**
- **Initial response**
- **Formulate response strategy**
- ***Investigate the incident***
- **Reporting**
- **Resolution**

WHEN INVESTIGATION SHOULD START?

- Initial response has been conducted and further investigation is needed.
- Consulted from legal counsel.
- Performed a forensic duplication of evidence drive using some imaging tool.

WHERE EVIDENCE RESIDES ON WINDOWS SYSTEMS?

- Volatile data in kernel structures
- **Slack space**, where you can obtain information from previously deleted files that are unrecoverable
- Free or unallocated space, where you can obtain previously deleted files,
- including damaged or inaccessible clusters

CONTD….

- The logical file system
- The event logs
- The Registry, which you should think of as an enormous log file etc

CONDUCTING A WINDOWS INVESTIGATION.

- Review all pertinent logs.
- Perform keyword searches.
- Review relevant files.
- Identify unauthorized user accounts or groups.
- Identify rogue processes and services.
- Look for unusual or hidden files/directories.
- Check for unauthorized access points.
- Examine jobs run by the Scheduler service.
- Analyze trust relationships.
- Review security identifiers.

LOG FILES

The Windows NT, 2000, XP, Win7 and Win10 operating systems maintain three separate log files

System log

Application log

Security log

LOG FILES

- System processes and device driver activities are recorded in the **System log.**
- Activities related to user programs and commercial off-the-shelf applications populate the **Application log.**
- System auditing and the security processes used by Windows are found in the **Security log.**
- **Any user can view the Application and System logs, but only administrators can read the Security log.**

Reviewing All Pertinent Logs

- Determine which users have been accessing specific files
- Determine who has been successfully logging on to a system
- Determine who has been trying unsuccessfully to log on to a system
- Track usage of specific applications
- Track alterations to the audit policy
- Track changes to user permissions (such as increased access)

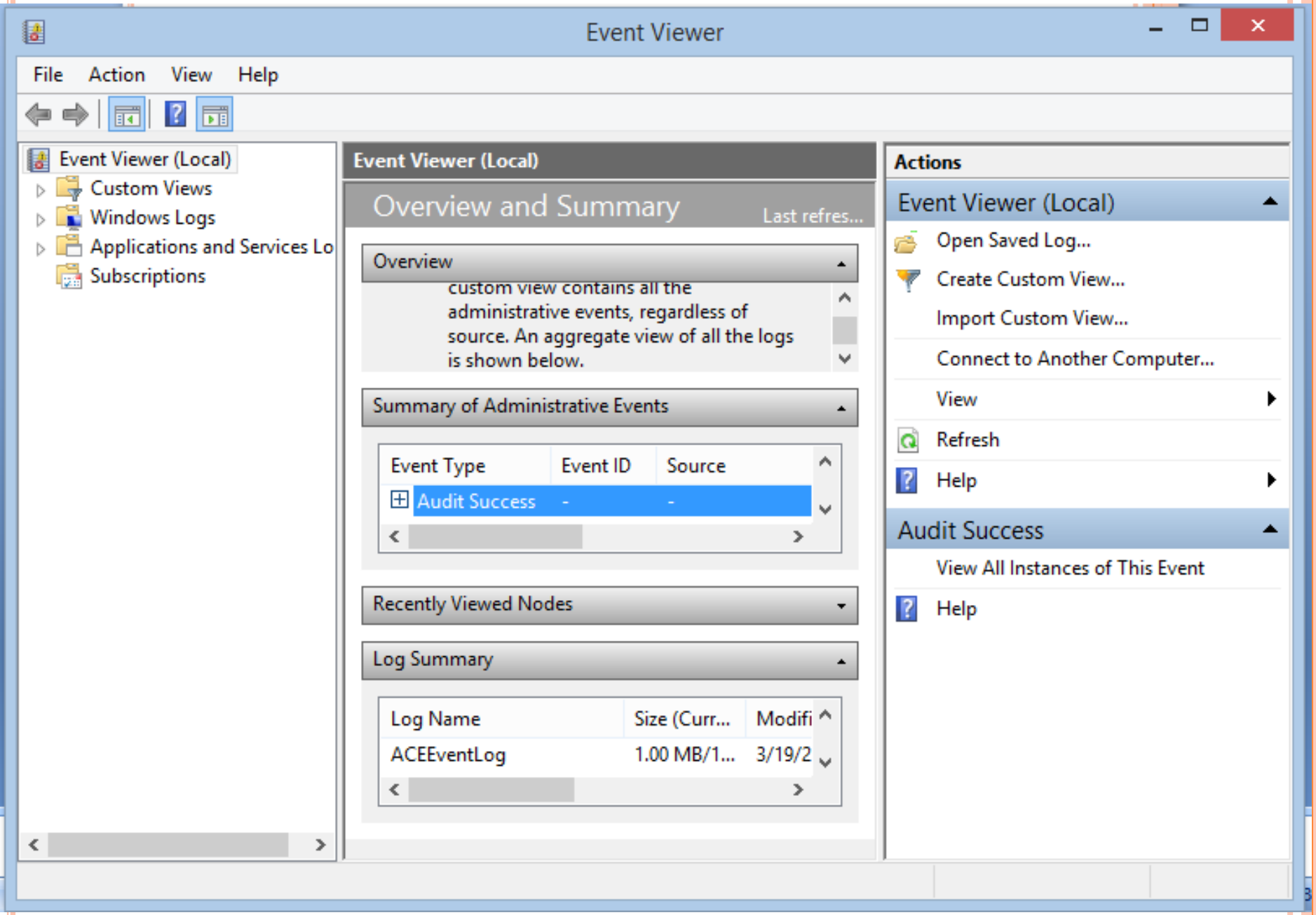
LOGS ON LIVE SYSTEMS

- Windows provide a utility called **Event viewer to** access the **audit logs** on local host.

- **PATH TO START**

Select Start | *Programs* | *Administrative Tools* | *EventViewer* to open Event Viewer.

In Event Viewer, select the log that you wish to view from the Log menu.


Event Viewer
File
Action
View
Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Lo
Subscriptions
Event Viewer (Local)
Overview and Summary
Last refres...
Overview
custom view contains all the
administrative events, regardless of
source. An aggregate view of all the logs
is shown below.
Summary of Administrative Events
Event Type
Event ID
Source
Audit Success
-
-
Recently Viewed Nodes
Log Summary
Log Name
Size (Curr...
Modifi
ACEEventLog
1.00 MB/1...
3/19/2
Actions
Event Viewer (Local)
Open Saved Log...
Create Custom View...
Import Custom View...
Connect to Another Computer...
View
Refresh
Help
Audit Success
View All Instances of This Event
Help

For example

- In Event Viewer, select **Log | Open** and specify the path to the copied .evt files
- You select the log type (Security, Application, or System) when choosing the .evt file to review.

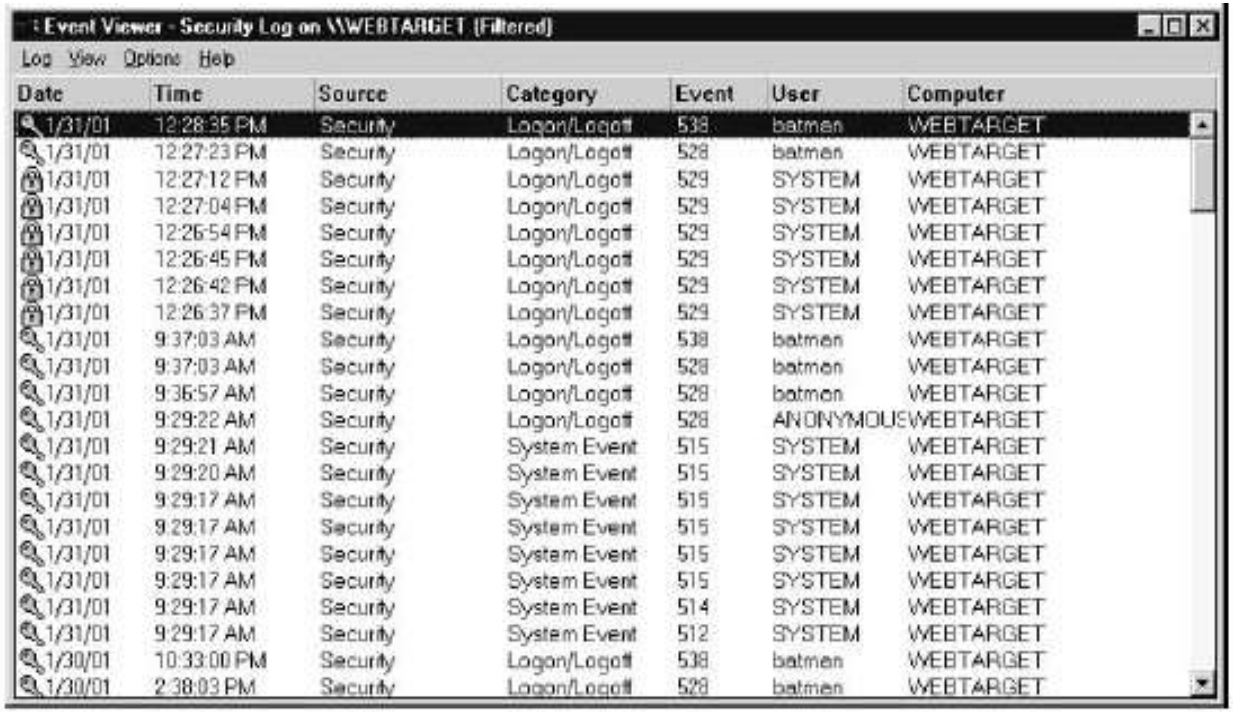


Figure 12-1. The Security log viewed in Event Viewer

- Notice the **key** and **lock** icons in the first column
- on the left. The **key** denotes **a successful log**, the **lock** denotes a **failure** of some kind.

ID	Description
516	Some audit event records discarded
517	Audit log cleared
528	Successful logon
529	Failed logon
531	Failed logon, locked
538	Successful logoff
576	Assignment and use of rights

Table 12-1. Some Security Log Event IDs

- **SECURITY LOG EVENT ID'S**

What Can Happen/situation

- You want to closely monitor all the processes an employee is running on his workstation.
- Your general counsel has advised that your corporate policy supports such logging.

WHERE TO FIND EVIDENCE

- set the audit policy to monitor the success and failure of *detailed tracking*.
- With detailed tracking turned on, you can determine every process a user executes on the system by reviewing the following event IDs:

- **592 A new process has been created**
- **593 A process has exited**

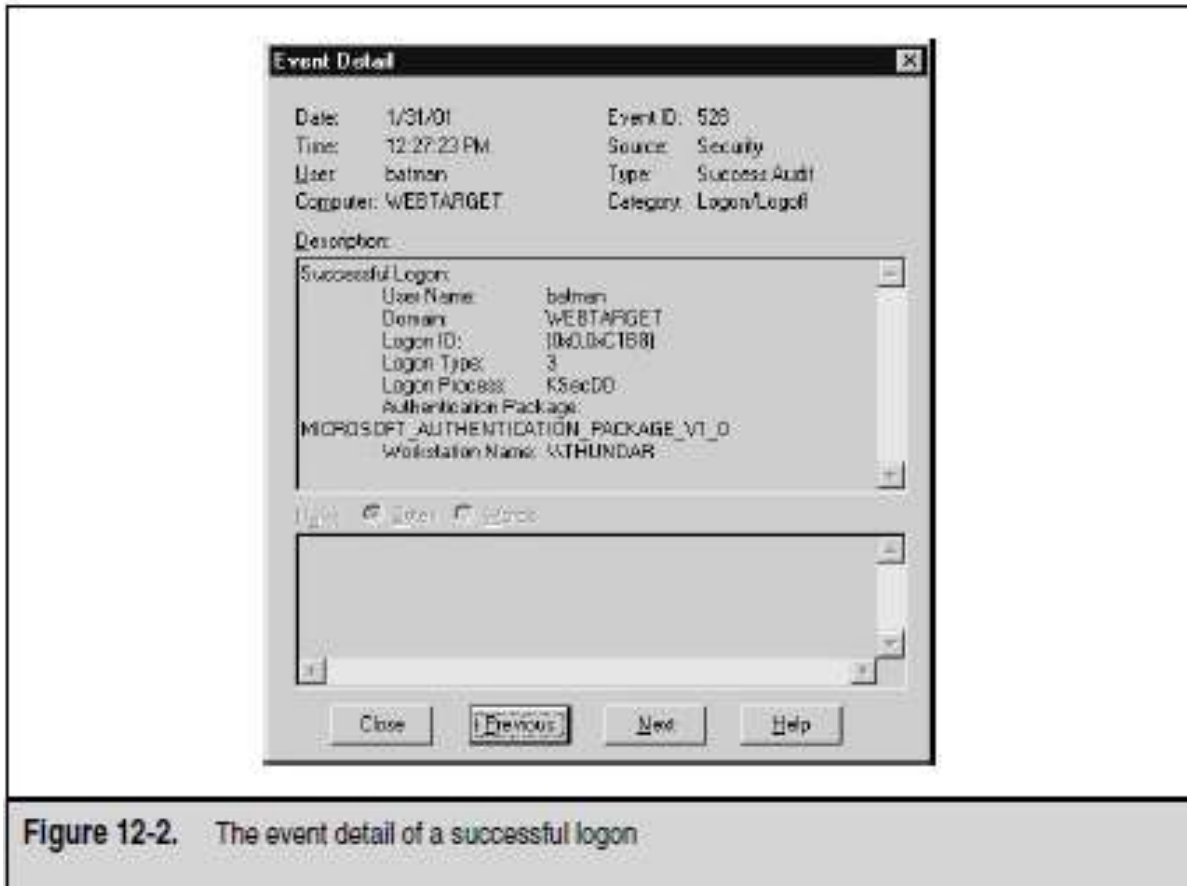


Figure 12-2. The event detail of a successful logon

- You can use this type of process tracking to log virtually every application a user ran or opened, edited, and closed

Offline Investigation of Logs

- To view the event logs from an offline system,you must obtain copies of **secevent.evt,appevent.evt** and **sysevent.evt** files from the forensic duplicate.

- These files are stored in the default location of *\%systemroot%\System32\Config*.

CONTD..

These files can be extracted

- via **a DOS boot disk**
- via **a Linux boot disk** with the appropriate kernel to mount NTFS drives, or

- from your forensic image.

EXCEPTIONS

If forensic workstation will not be able to read the imported event logs:

- 1**. Disable the EventLog service** on the forensic workstation by opening **Control Panel | Services** and selecting Disable for the EventLog option. (This change will not be effective until you reboot the workstation.)
- 2. Use the User Manager to change the forensic workstation's audit policy to log nothing at all. This will prevent your forensic workstation from writing to the evidence Security log.
- 3. Reboot the forensic workstation, and then verify that the EventLog service is not on by viewing Control Panel | Services.

CONTD…

- 4. Place the evidence .evt files into the ***\%systemroot%\System32\Config***

  directory. Since Event Viewer automatically defaults to populating the three .evt files in ***\%systemroot%\System32\Config***,

  you will need to either **rename the forensic workstation's .evt files** or overwrite whatever log files your system was currently using.
- 5. Use Control Panel | Services to start the EventLog service by selecting Manual .Start and then starting the EventLog service.
- 6. Start Event Viewer. You will now be able to view the evidence event logs.

INSTRUCTION

- Merely save the event log as soon as possible to avoid the forensic workstation entries in the logs.

Event log drawbacks

- Windows systems do not log successful logons, files accesses, shutdowns and many other important events.
- Event Viewer allows you to view only a single record at a time.
- these logs only record the source NetBIOS name, rather than the IP address of the remote system.
- size and time length of each log (Security, Application, and System) need to be set individually.

- logs populate the Description field by using values from various dynamically linked library (DLL) files.