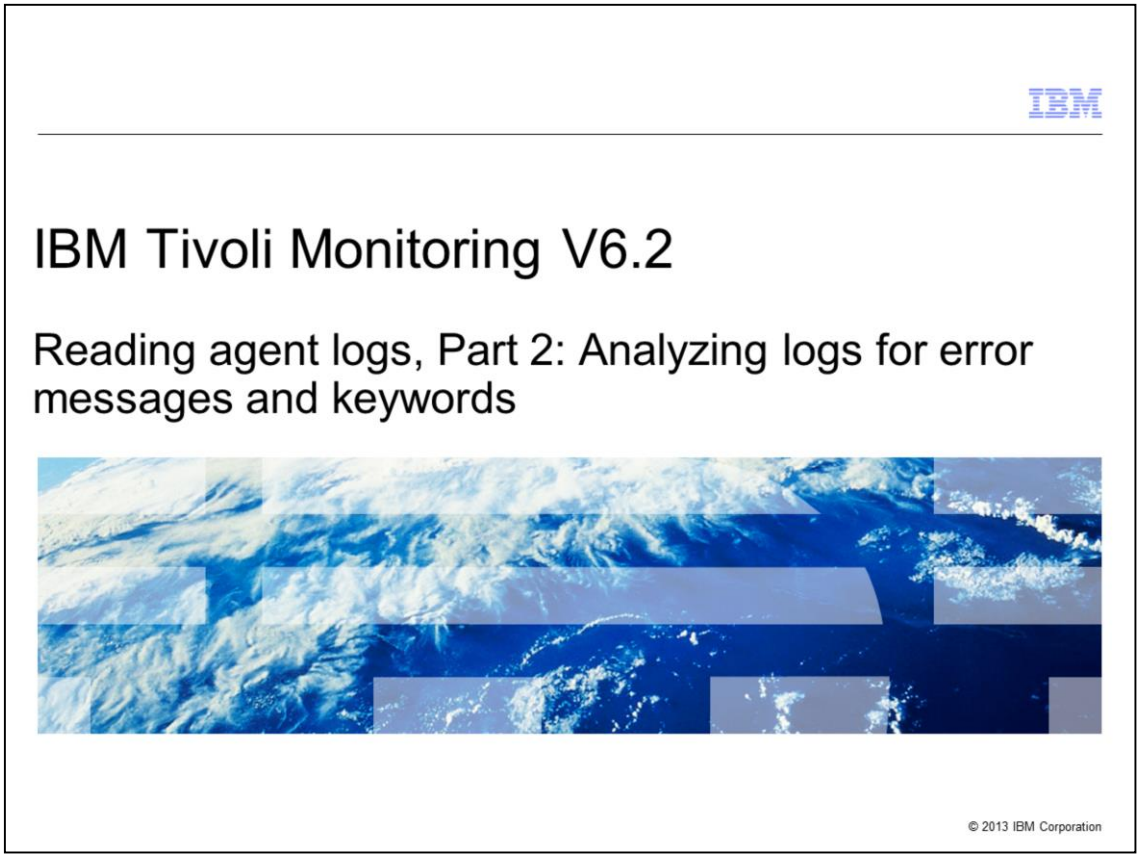
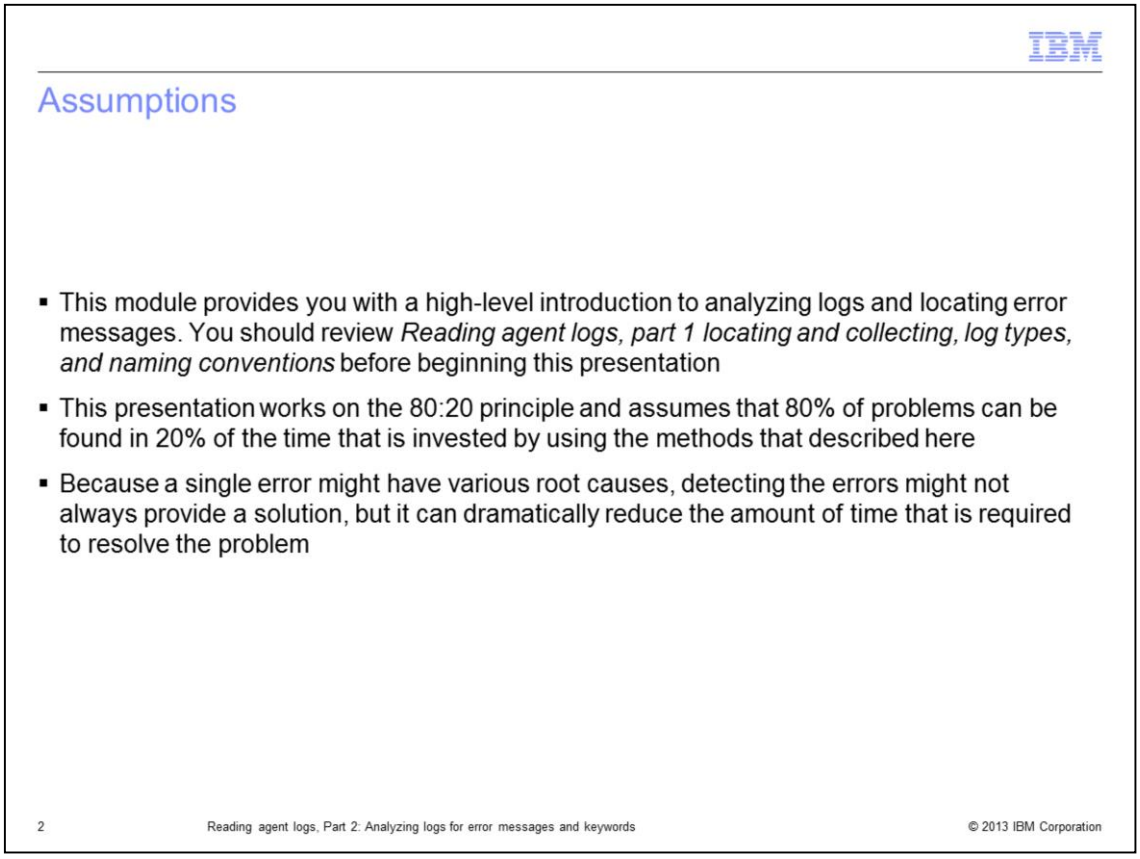


IBM Tivoli® Monitoring V6.2, Reading agent logs, part 2 analyzing logs for error messages and keywords.



This presentation is the second of three modules on Tivoli Monitoring, reading agent logs. The first module provided you guidelines on how to collect and identify IBM Tivoli Monitoring agent logs. This module provides you a high-level introduction to analyzing logs and locating error messages. You should review *Reading agent logs, part 1 locating and collecting, log types, and naming conventions* before beginning this presentation.

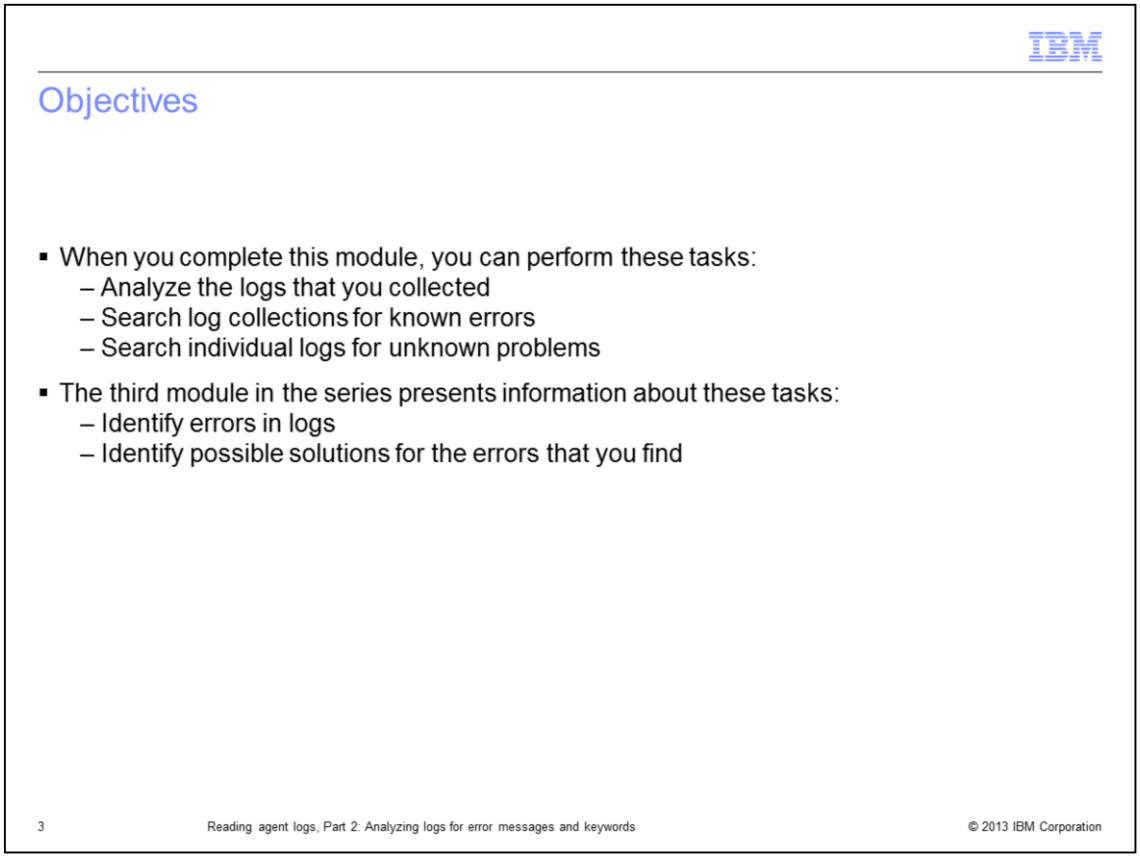
The third module provides examples of problems that can been identified and resolved in frequently used logs. It also provides suggestions on how to proceed after you identify a suspected problem.

This presentation uses the 80:20 principle and assumes that 80% of problems can be found in 20% of the time by using the methodology described here.

Because a single error might have various root causes, detecting the errors might not always provide a solution, but it can dramatically reduce the amount of time that is required to resolve the problem.

You should have a good understanding of how IBM Tivoli Monitoring is installed and configured in your environment. For example, you should understand which agents are installed, the host names the agents are installed on, the Tivoli Enterprise Monitoring Server, and the Tivoli Enterprise Portal Servers these agents report to.

The developer assumes that you understand the directory structure that Tivoli Monitoring is installed into and that you have a good understanding of the Windows® or UNIX® operating systems.



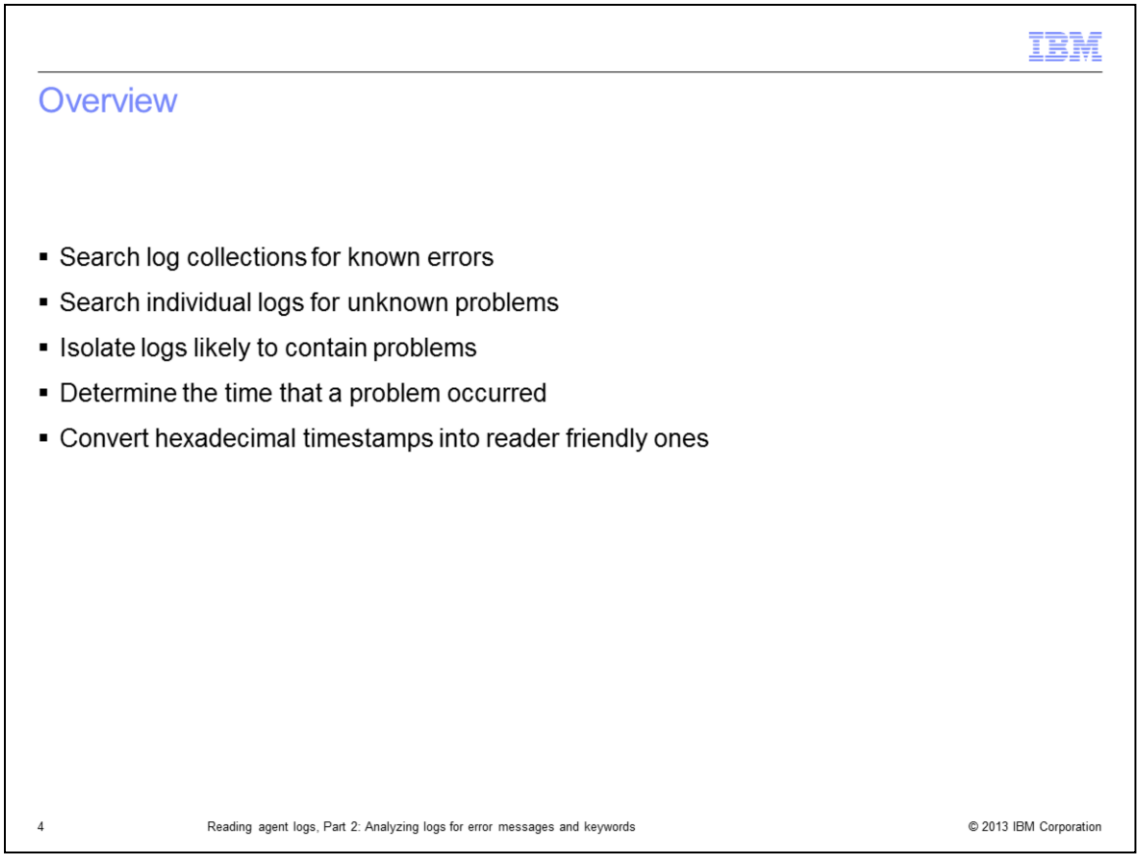
When you complete this module, you can perform these tasks:

- Analyze the logs that you collected

- Search log collections for known errors

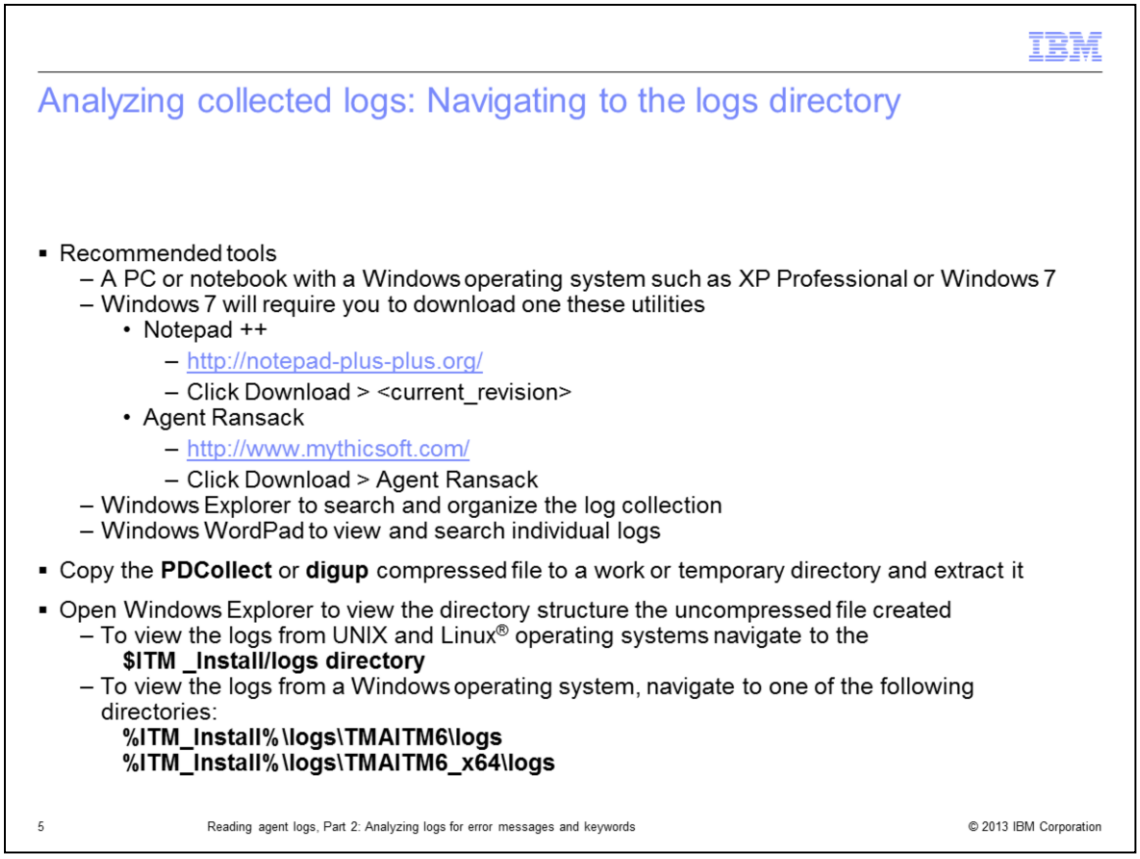
- Search individual logs for unknown problems …

The third module in this series presents information about how to identify errors in logs and identifying possible solutions for the errors that you find.



The steps to resolve error that are presented in this lesson are:

1. Search log collections for known errors
2. Search individual logs for unknown problems
3. Isolate logs likely to contain problems
4. Determine the time that a problem occurred
5. Convert hexadecimal timestamps into conventional ones



Most log files can be analyzed on any current notebook or workstation.

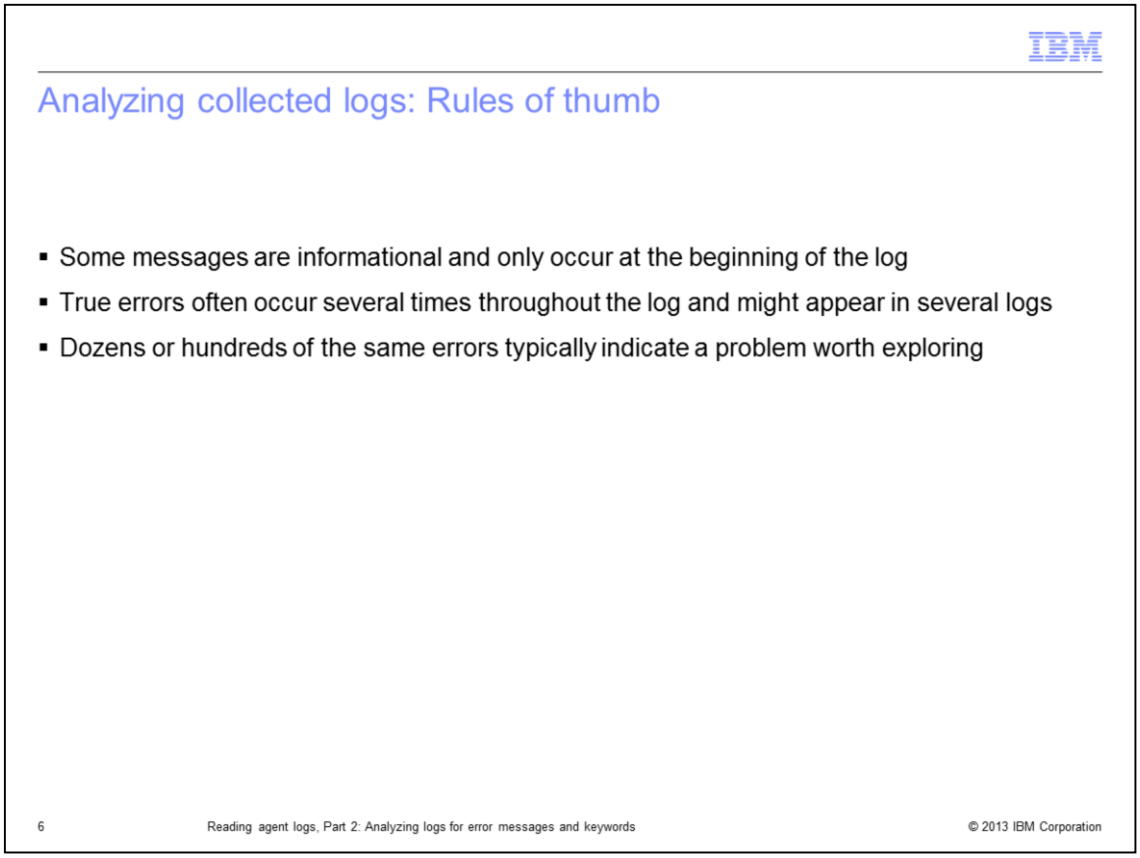
As stated earlier, this presentation shows how to work with logs on a Windows operating system, with Windows Explorer software to search and organize the logs.

Windows WordPad is used to view individual log files because WordPad retains the format of the original log file.

Copy the compressed **PDCollect** or **digup** file to a work or temporary directory and extract it.

Open Windows Explorer to view the directory structure the uncompressed file created.

To view the logs you want to work with, use Windows Explorer to navigate to the appropriate directory shown in this slide.

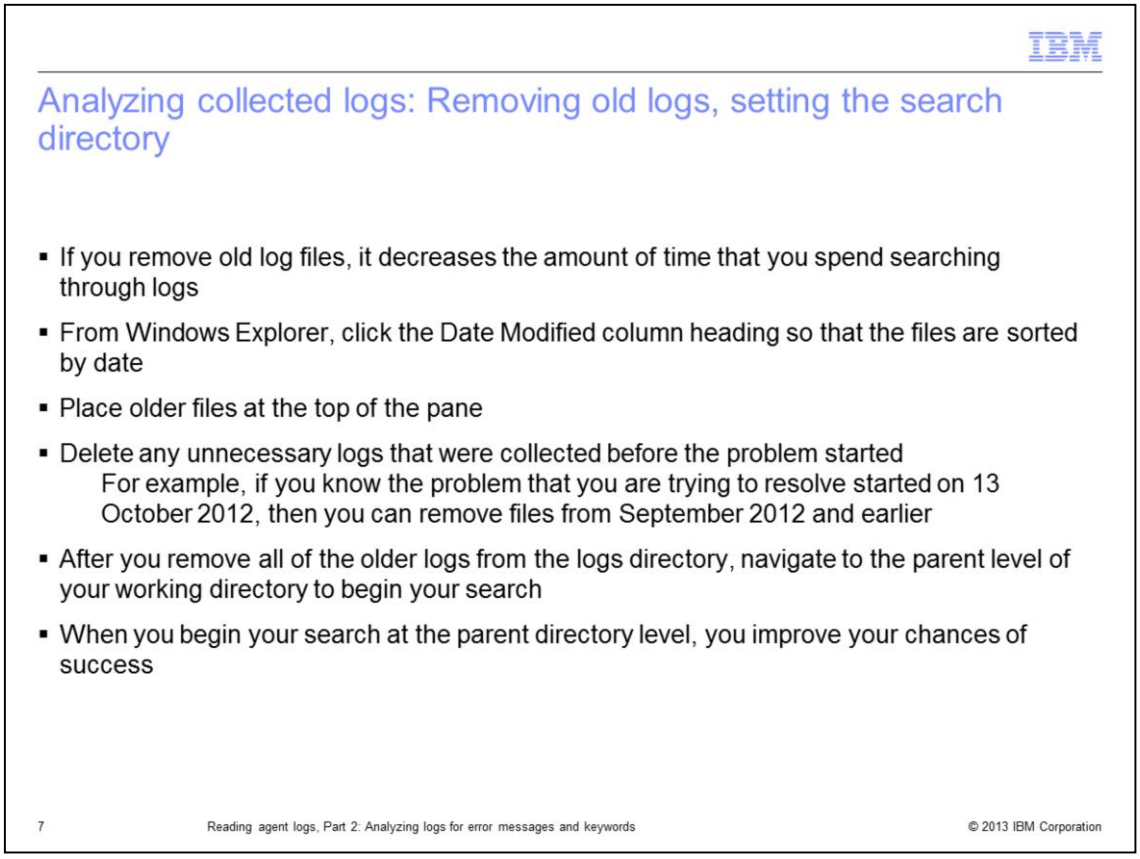


Here are few rules to remember when reviewing log files.

Some messages are informational and only occur at the beginning of the log.

True errors often repeat several times throughout the log and might appear in several log files.

Dozens or hundreds of the same errors typically indicate a problem worth exploring.



When you use the methodology that is described here, you work with a copy of the original files that remain on the system where **PDCollect** or **digup** was run.

You can safely delete the older files that were created before the problem started.

If you delete old log files, it takes less time to search the remaining log files.

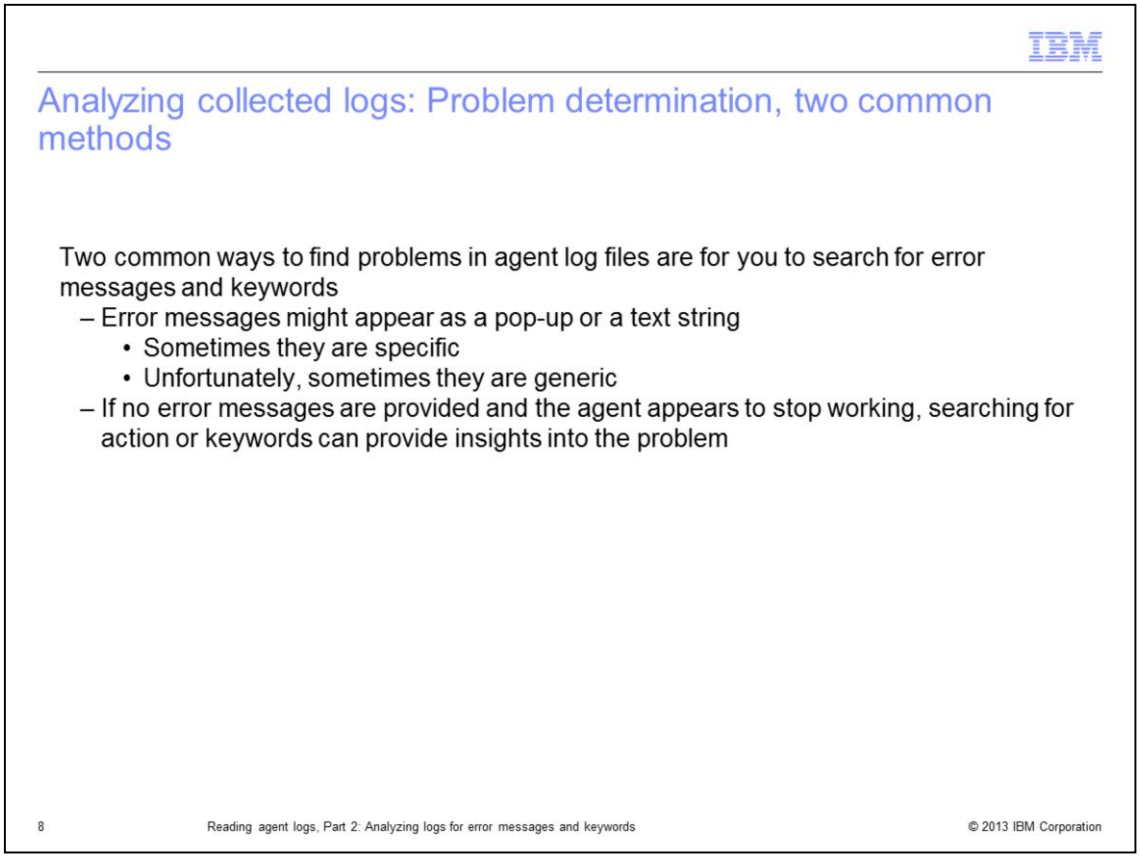
From Windows Explorer, click the Date Modified column heading to sort the files by date. You might need to click a second time to sort the files into descending date order which places the oldest files at the top of the list.

Delete any unnecessary files that are collected before the first problem occurrence. For example, if you know the problem that you are trying to resolve started on 13 October 2012, then you can remove files from September 2012 and earlier.

After you remove all of the older logs from the logs directory, navigate up to the parent level of your working directory and begin your search.

Most of the log files you need to work with are found in the **/logs** directory. Occasionally you might find log files where you do not expect to find them.

If you begin your search at the parent directory level, you improve your chances to successfully locate the log files that contain useful information to solve problems.

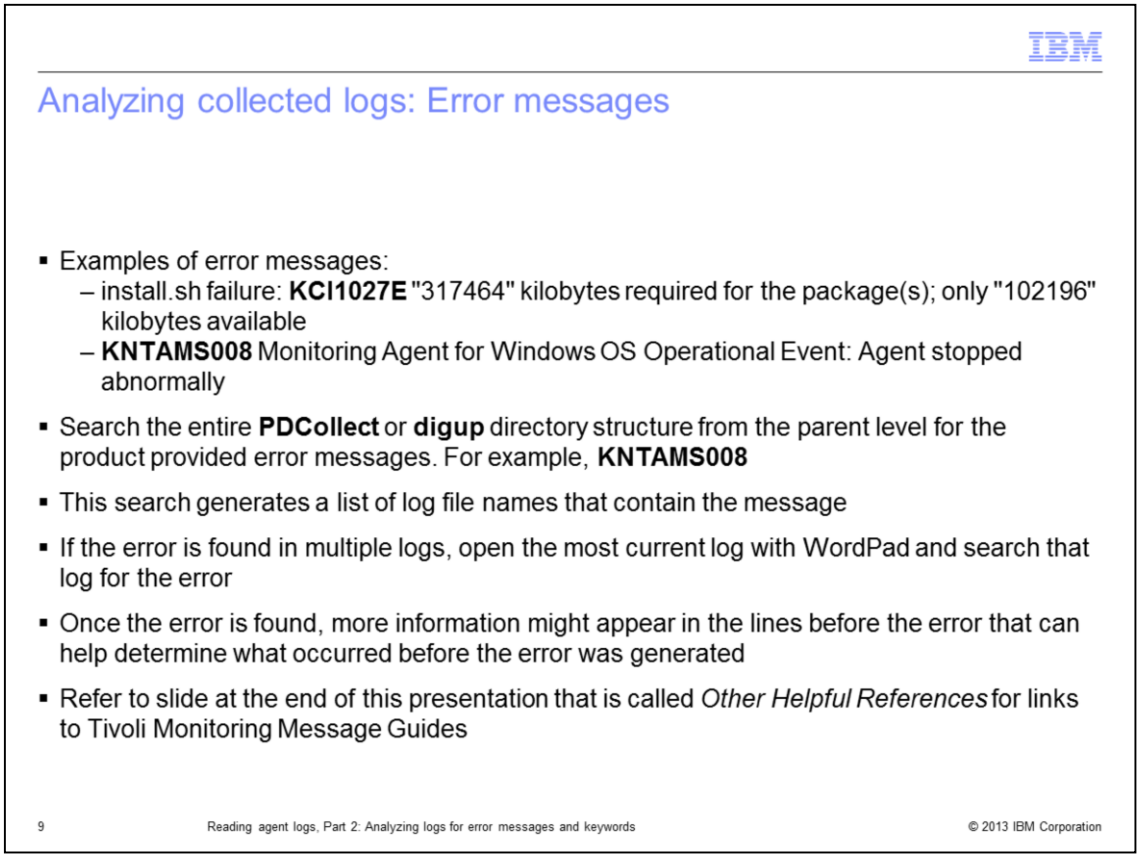


This presentation describes two common ways to find problems in agent log files. The next few slides describe how to search for error messages and keywords in the log files that you identify and collect.

Some error messages pop-up on your screen when a problem or unexpected condition arises. Sometimes the messages are specific and unfortunately, sometimes they are generic.

IBM software developers attempt to write meaningful error messages. Occasionally problems arise that cannot be anticipated and generic messages display.

Keywords can be helpful when you encounter a generic message and you have to determine the cause of the problem.



Some error messages are clear and present an obvious solution to resolve them as depicted in the first error that is shown on this slide. Other messages are generic and require logic and investigation to determine their cause.

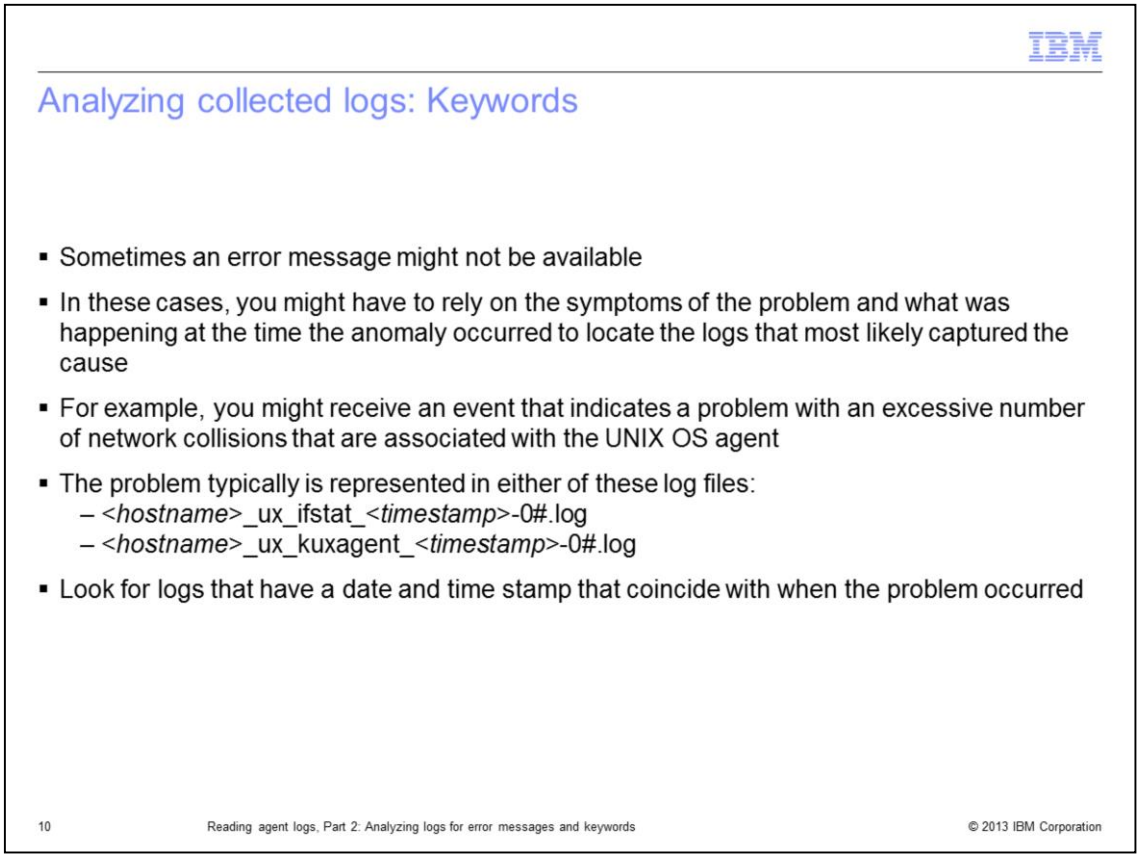
The recommended approach to locate this type of error message is to search the entire **PDCollect** or **digup** directory structure from the parent level for the product provided error messages. For example, search for **KNTAMS008**.

Remember to set the search criteria for file contents and not file names.

This search generates a list of log names that contain the message. If the error is found in several log files, open the most current file with WordPad and search that file for the error.

After the error is found, more information might appear in the lines before the error that can help determine what occurred before the error is generated.

More details are provided later in this presentation on searching for errors in individual log files.



Sometimes an error message might not be available.

In these cases, you might have to rely on the symptoms of the problem and what was happening at the time the anomaly occurred to locate the logs that most likely captured the cause.

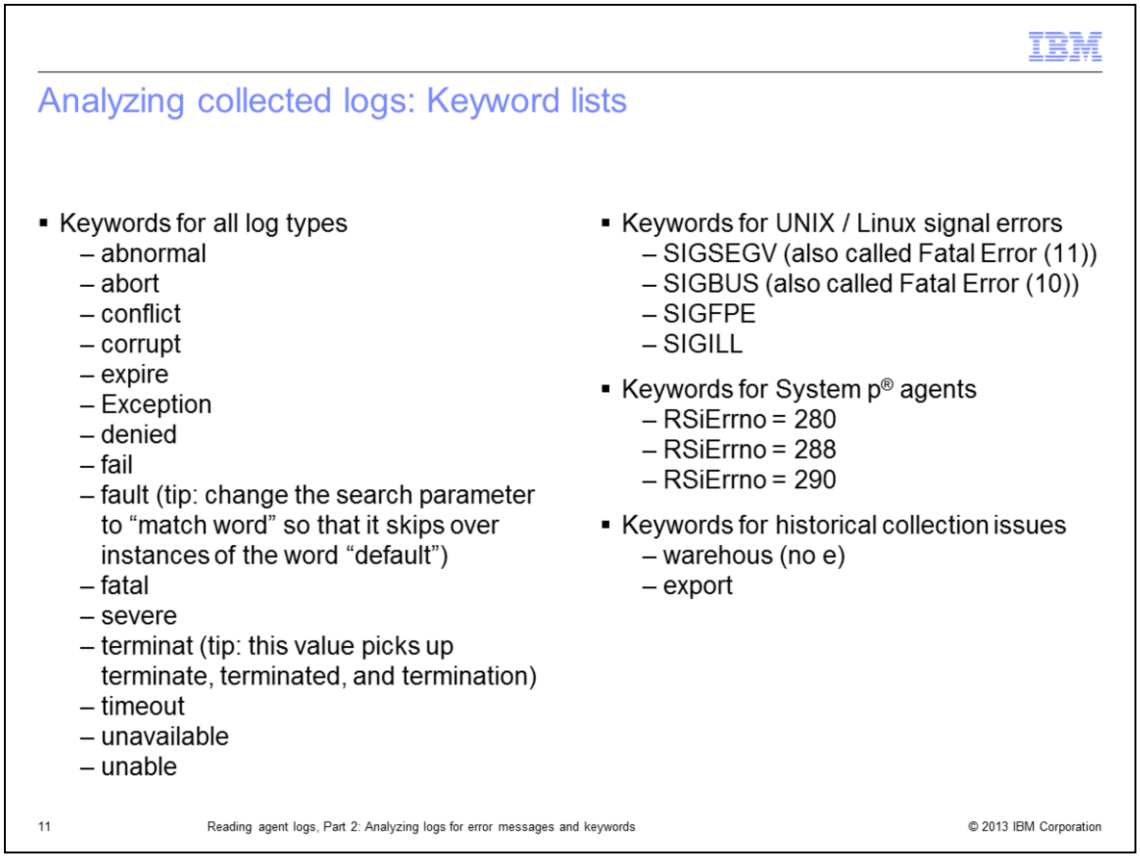
For example, you might receive an event that indicates a problem with an excessive number of network collisions that are associated with the UNIX OS agent.

In part 1 of this series, in the section Types of Logs: UNIX OS agent process, daemons, and subdaemons you learned that the **UX** agent **ifstat** subdaemon collects network interface statistics and populates the file **<*hostname*>_ux_ifstat_<*timestamp*>-0#.log**.

With this knowledge, you can sort your collected logs by name and assume that you captured the problem in one of the logs with a syntax that starts with **<*hostname*>_ux_***.

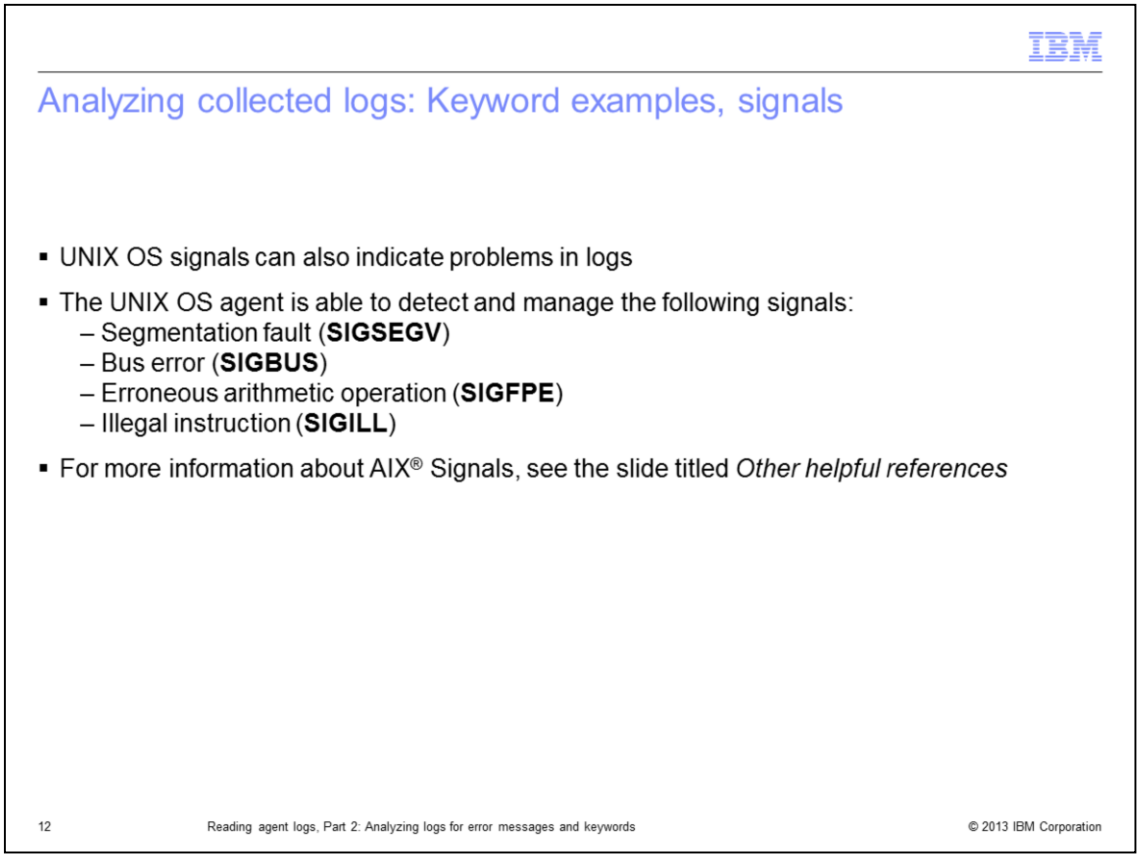
The problem data is probably contained in either of the two files shown.

Look for logs that have a date and time stamp that coincide with when the problem occurred.



This slide presents keywords that can help locate problems within the short list of logs that were identified.

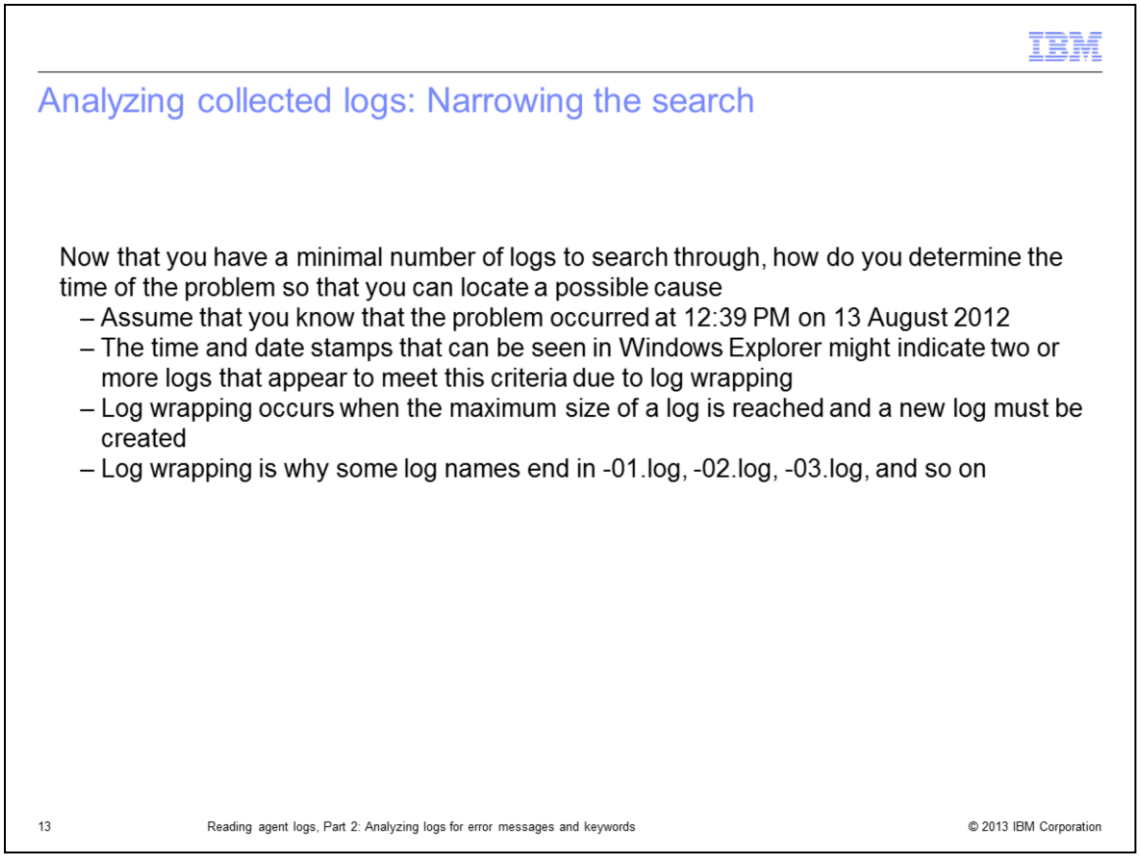
The presentation describes these keywords and how you can use them to locate problem indicators in more detail in the following slides.



Signals and **Fatal Errors** are another type of keyword that can also indicate problems within logs.

For more information about AIX Signals, see the slide titled *Other helpful references*.

Part 3 of this presentation shows examples of how to find signal related problems and errors in the logs.



Now that you minimized the number of logs to search, how can you pinpoint the time of the problem so that you can locate a possible cause?

Assume that you know that the problem occurred at 12:39 PM on 13 August 2012.

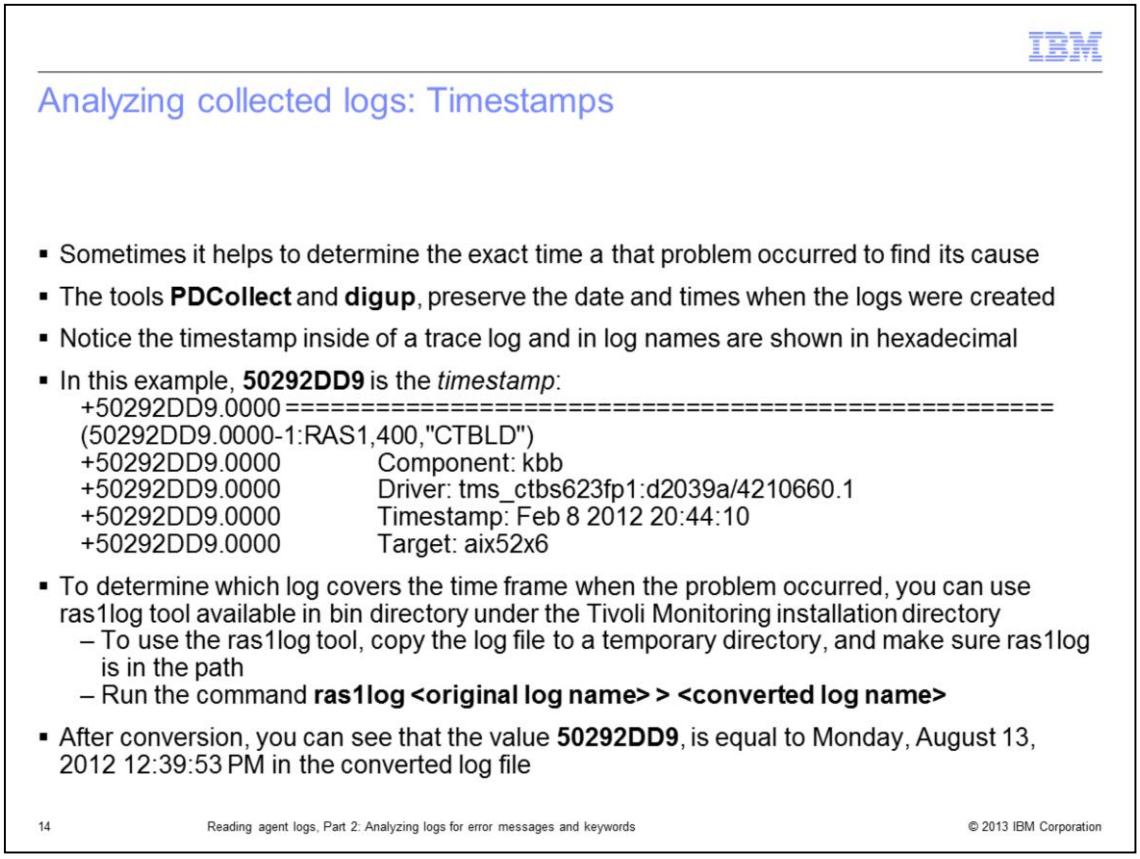
You can see the time and date stamps in Windows Explorer might indicate two or more logs meet this criteria.

There might be more that one file because of log wrapping.

Log wrapping occurs when the maximum size of a log is reached and the software must create a new log file.

When a log wraps, new logs are generated with names ending with -01.log, -02.log, -03.log, and so on.

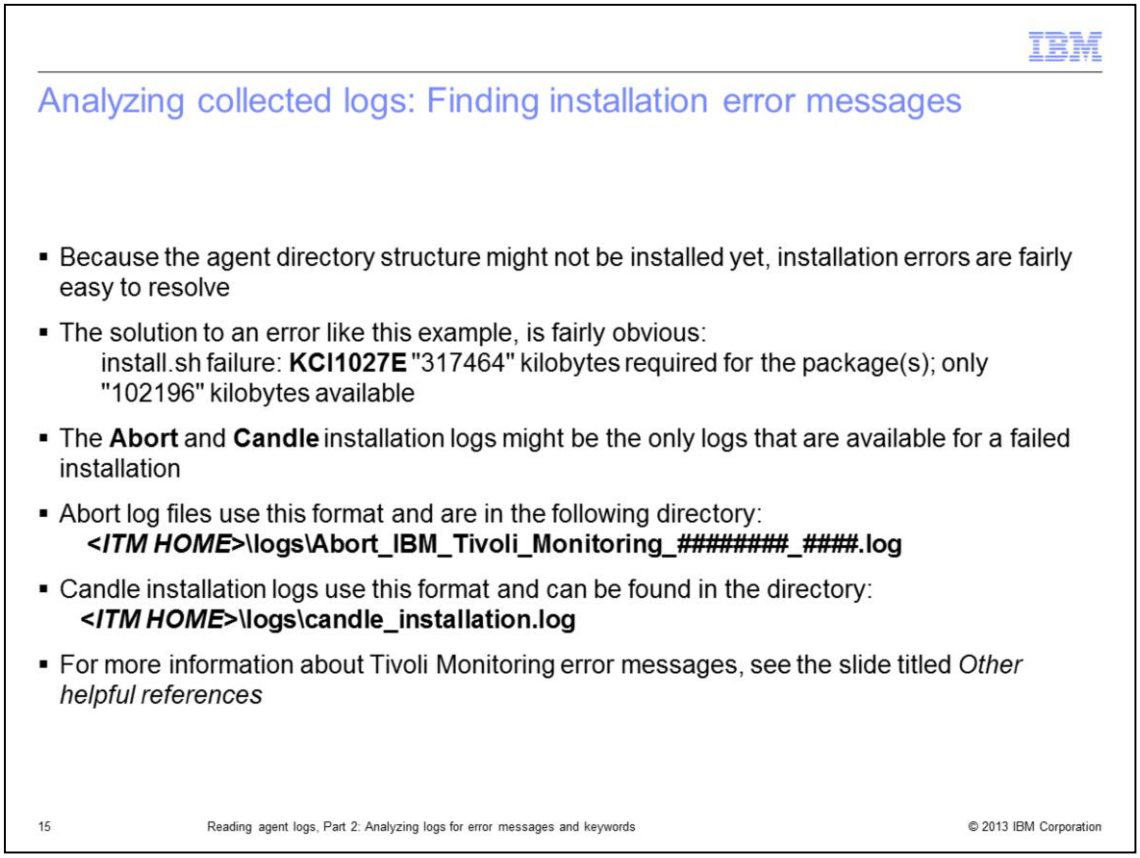
The next slide shows how to convert a hexadecimal timestamp, found inside of an agent log or log name, to a reader friendly equivalent.



Sometimes it helps to find the exact time a that problem occurred to determine its cause.

The **PDCollect** and **digup** tools preserve the date and times of when the logs were created. Notice the timestamp inside of a trace log and in log names are shown in hexadecimal. In the example, 50292DD9 is the timestamp.

By converting a log file with the ras1log tool, you can determine that 50292DD9 HEX is equal to Monday, August 13, 2012 12:39:53 PM.



Assume that you received error messages while installing a new agent.

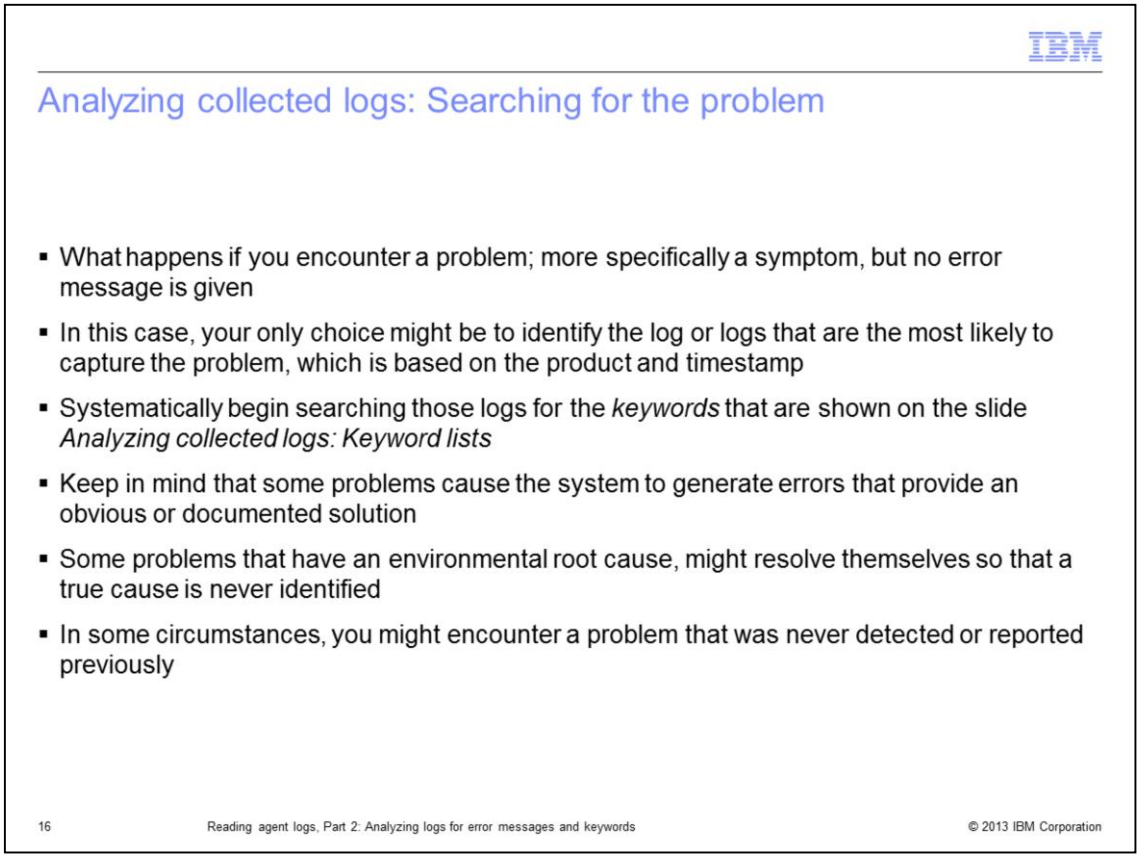
Because the agent directory structure might not be created yet, some installation errors are easy to resolve. If the **Abort** and **Candle** installation log files are the only logs that are available for a failed installation, there are fewer logs to analyze for errors. The solution to an error like the one shown, is fairly obvious.

Unfortunately, not all errors are so easily resolved.

The **Abort** log files and **Candle** installation log files can be found in the directories that are displayed on this slide.

For more information about Tivoli Monitoring error messages, see the slide titled *Other helpful references*.

Part 3 of this presentation shows some examples of resolving installation problems when error messages are less obvious.



What happens if you encounter a problem or; more specifically a symptom, but no error message is given?

In this example, you might choose to identify the log files that are the most likely to capture the problem, which is based on the product and timestamp.

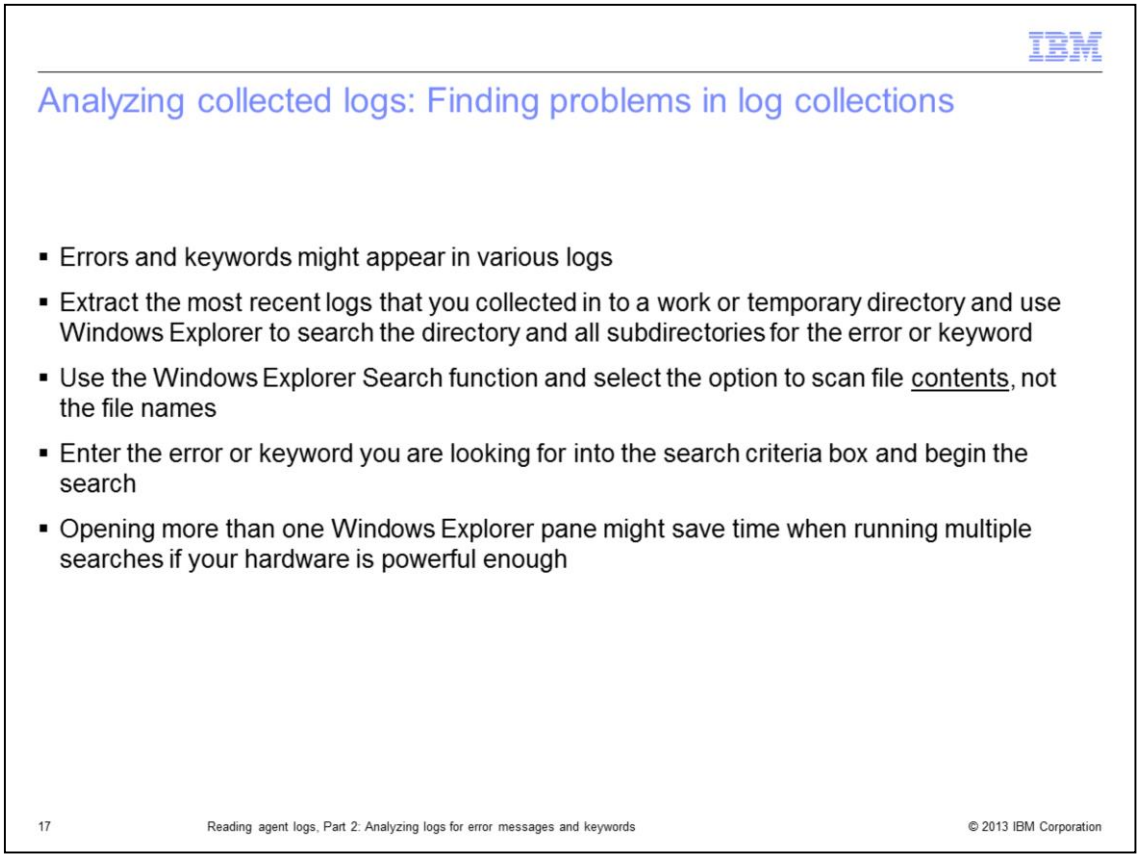
You can then systematically search those logs for the keywords that are shown on the slide Analyzing collected logs: Keyword lists.

With a little practice, you might realize how effective this approach can be.

Keep in mind that some problems, generate errors that provide an obvious or documented solution.

Some problems that have an environmental root cause, might resolve themselves so that a true cause is never identified.

In some circumstances, you might encounter a problem that nobody detected or reported before.



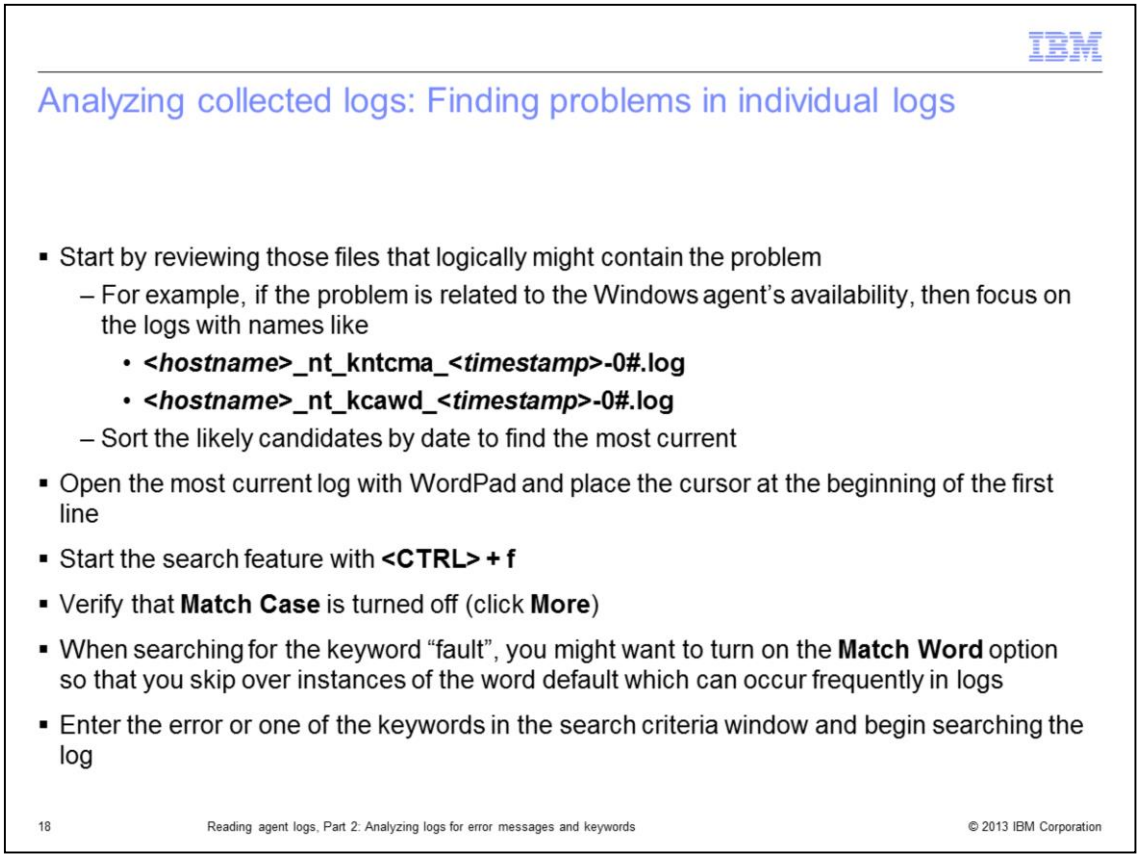
Errors and keywords might appear in various logs.

There is a simple method to find a specific error. Extract the most recent log files that you collected in to a work or temporary directory. Then use Windows Explorer to search the directory and all subdirectories for either the error text or a keyword.

Use the Windows Explorer Search function and select the option to scan file contents, not the file names.

Enter the error or keyword you are looking for into the search criteria box and begin the search.

If you open more than one Windows Explorer pane, you might save time by running multiple searches. That depends on the capability of your hardware.



Determine a list of file names that might contain the keyword or error message.

You can create a list by reviewing those files that logically might contain the problem. For example, if the problem is related to the availability of the Windows agent, then analyze the log files with names like the ones that are listed on the slide.

Sort the likely candidates by date to find the most current.

Open the most current log file with WordPad and place the cursor at the beginning of the first line.

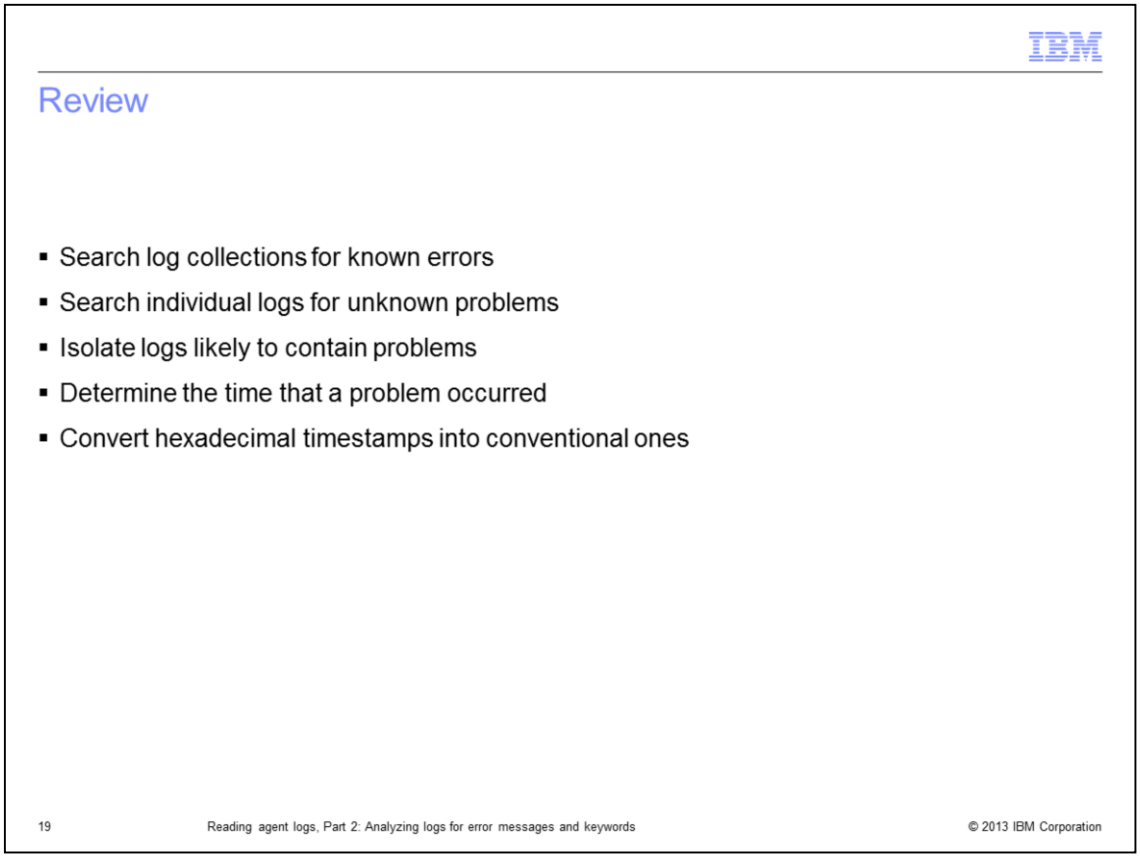
On your keyboard, start the search feature by pressing <CTRL> + f.

Verify that **Match Case** is turned off. You can find this information by clicking **More**.

When you search for the keyword "fault", turn on the **Match Word** option to avoid instances of the word "default" that often occurs in log files.

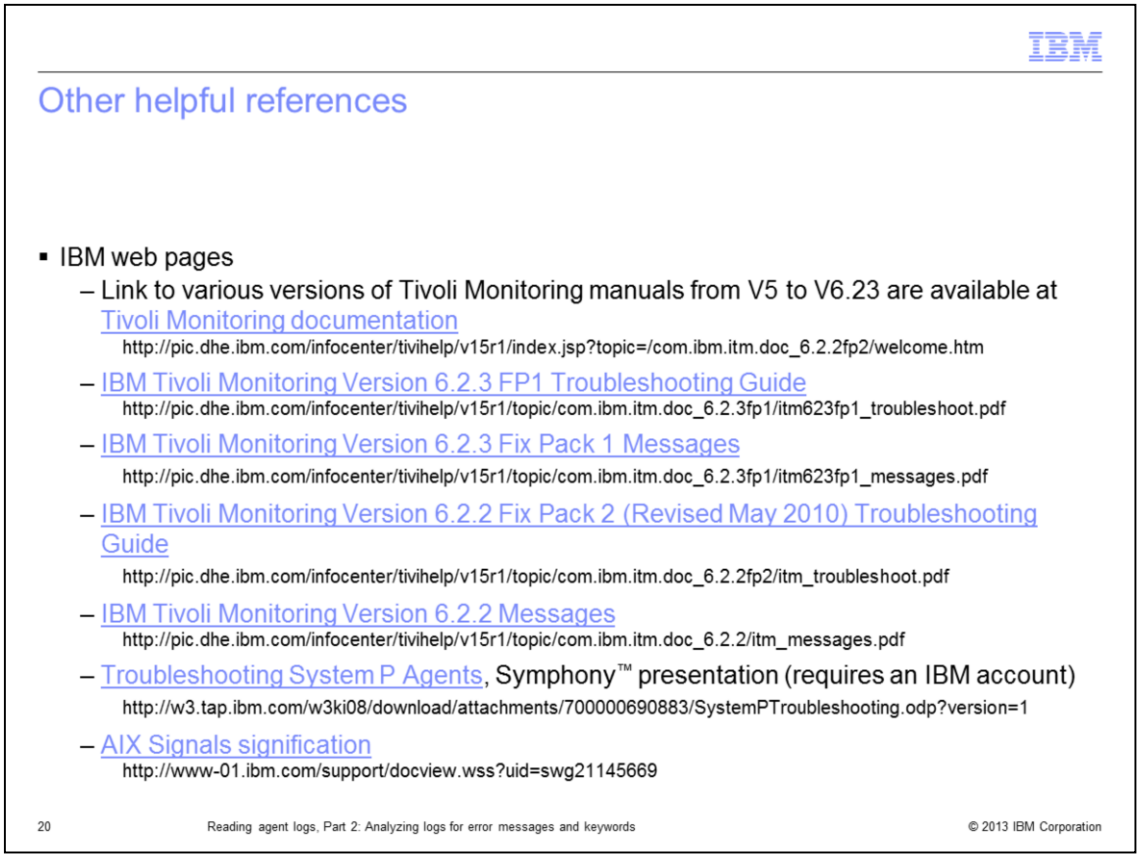
Enter the error or one of the keywords in the search criteria window and begin searching the log for the error message or keyword. See the slide titled *Analyzing collected logs: keyword lists* for useful keywords.

Part 3 of the presentation series shows that various keywords can be clustered near each other when problems are located within a log file.

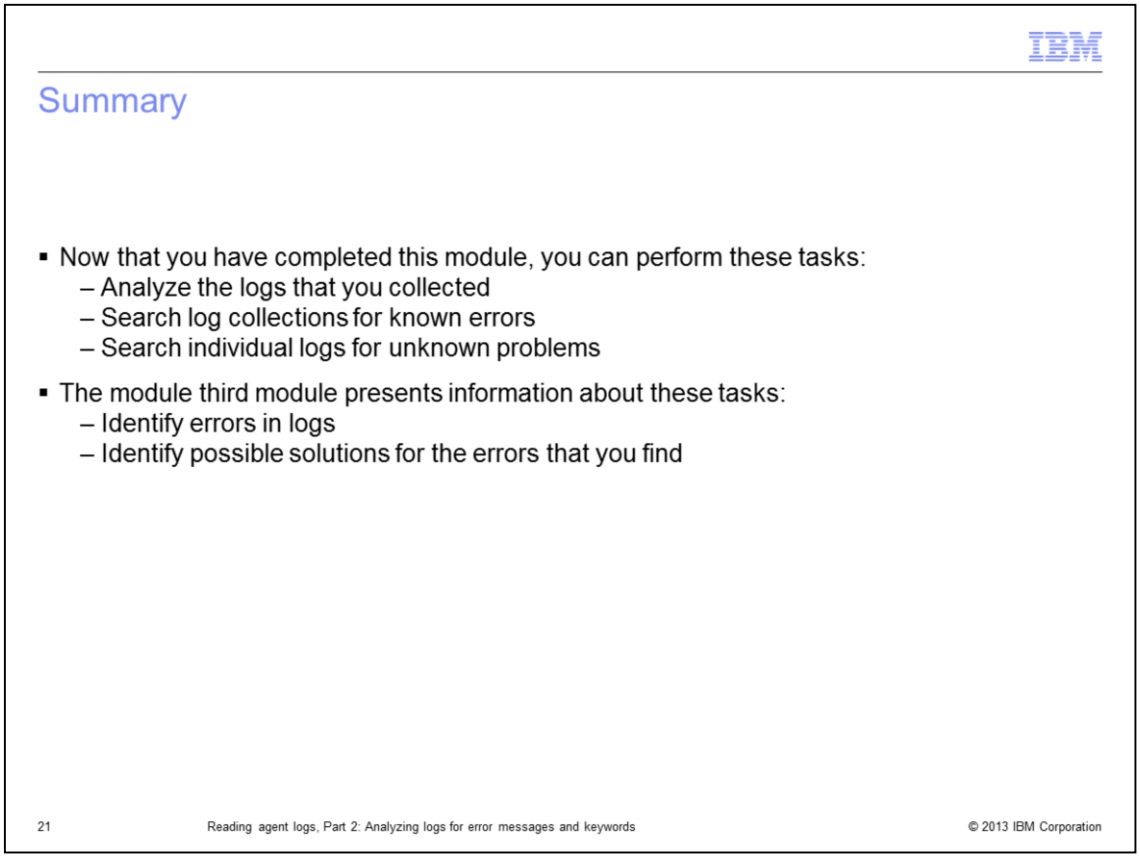


The steps to resolve errors that are presented in this lesson are:

1. Search log collections for known errors.
2. Search individual logs for unknown problems.
3. Isolate logs likely to contain problems.
4. Determine the time that a problem occurred.
5. Convert hexadecimal timestamps into conventional ones.



Here are several helpful references to IBM websites.



Now that you have completed this module, you can perform these tasks:

- Analyze the logs that you collected

- Search log collections for known errors

- Search individual logs for unknown problems …

The third module in this series presents information about how to identify errors in logs and identifying possible solutions for the errors that you find.

Trademarks, disclaimer, and copyright information