masterskill
education through innovation

aci LEARNING | SKILL LABS

Digital Forensics Fundamentals, Skill Labs

Course Specifications

Course Number: ACI76-048SL_rev1.0
Lab Length: Approximately 15 hours

Introduction to File Systems

Introduction
Objective

GIAC Digital Forensic Examiner Objective:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

According to CyberSecurity Magazine, "digital forensics is the process of investigating crimes committed using any type of computing device." Digital forensics is also responsible for investigating cyber attacks. One area that a digital forensics specialist must understand is how data is stored on any type of computing device. Digital forensic investigators acquire, preserve, examine, and present digital evidence that can be used in a court of law. This lab investigates the common file systems that are used by Windows, Mac, and Linux operating systems.

Outcomes:

In this lab, you will learn to:

1. Examine different Windows and Linux file systems
2. Partition and formatting file systems in Windows
3. Format and wiping Linux file system

1	Key Term	Description
1	FAT	File Allocation Table is a table that holds information about where files are stored on a volume. When a file is deleted from the disk, the entry or entries for those files are removed from the table and the space is marked as available. However, the file, or parts of the file, will remain on the disk until overwritten by information from new files that are written to the disk.
2	NTFS	New Technology File System was originally introduced with the Windows NT. NTFS is a journaling file system which means it keeps a log of changes being written to the disk. If a computer is shut down improperly, it will have a better chance of recovery if it has a journaling file system. Files and folder access can

1	Key Term	Description
		be restricted with the security feature of NTFS. Starting with Windows 2000, Microsoft included the Encrypted File System, or EFS, as an NTFS feature. EFS allows users to encrypt files to protect against unauthorized access.
3	EXT2/3/4	The Extended File Systems 2, 3, and 4 are used by the Linux operating systems. Both EXT3 and EXT4 are journaling file systems. EXT2 does not have journaling.
4	Format	A format will not erase the data from the volume. Rather, it will delete the references to the file in the FAT or Master File Table ($MFT) and make those spaces on the disk as available. Forensic recovery of files may be possible on a formatted disk.
5	Wipe	A wipe will erase all of the 0's and 1's written to the hard disk. If a wipe is done correctly, all data will be erased and recovery of artifacts will be near impossible.

Common Locations of Windows Artifacts

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Analysis and Profiling of Systems and Devices, Host and Application Event Log Analysis

- The candidate will demonstrate an understanding of the artifacts created by the Windows operating system during the execution of programs, system start up and use of removable devices.

Overview

The development of this document is funded by the Department of Labor's (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will enumerate hosts on the network using various tools by evaluating event, web, and tasks. Also, you will explore the startup, windows, and system32 folders.

Outcomes:

In this lab, you will learn to:

4. Examine Windows Event Logs, IIS Logs, and Scheduled Tasks
5. Examine the Startup, Windows, and System32 Folders

	Key Term	Description
1	Users Folder	This folder stores the user's profiles in Windows Vista, Windows 7, Windows 8, Server 2008, and Server 2012. In order for a user's profile to be created within Microsoft Windows, the user must log in to the system at least one time.

	Key Term	Description
2	Startup Folder	This location can be utilized by administrators (or hackers) to launch programs automatically at startup. A batch file or executable can be stored in a user's startup folder or it can be stored where it will run for all users accessing the system.
3	Documents and Settings	This folder stores the user's profiles in Windows 2000, XP, and Server 2003. In order for a user's profile to be created, the user must log in to the system at least one time. Documents and Settings has been replaced by Users folder in current versions of the operating systems. However, it still exits as a reparse point on the newer versions.
4	Scheduled Tasks	Located in the Tasks folder within the Windows folder, this is the location where AT jobs are stored. AT jobs are tasks that are scheduled to run automatically, like backups or disks defragments. When hackers compromise a system, they may schedule malware to run automatically which provides them a backdoor.
5	Prefetch	This folder exists so that the Windows operating system can load certain executable files faster after system startup. The prefetch files have a .pf extension and often can provide someone investigating a system clues about what programs ran.

Hashing Data Sets

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

In this lab, you will be learning how to image disks, hash the image, and verify the hash. Digital forensic specialists image disks before they start an investigation. They also record the hashes so they are able to prove in a court of law that the image has not been tampered with.

Outcomes:

In this lab, you will learn to:

1. Image and Hash a Disk and Verifying the Hashes of the Image
2. Use Kali to Hash Images, Disks, and Partitions

3. Use HashCalc to Verify Hashes

	Key Term	Description
1	EnCase Imager	EnCase Imager is a GUI program that will allow a user to create a disk image from within Windows. You can run into complications imaging a disk while on Windows because certain files are locked by the OS. EnCase Imager is a free product.
2	HashCalc	A free program from http://www.slavasoft.com/hashcalc/ that allows you to calculate the MD5, SHA-256, SHA-384, SHA-512, and other hash values of data sets.
3	MD5	Message Digest 5 is a 128-bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original. Other hashes, like SHA-1, which is 160 bits, are more accurate than the 128-bit MD5.
4	SHA1	Secure Hash Algorithm is a 160-bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original. There are also 256-, 384-, and 512-bit versions of SHA that are more accurate.
5	Kali	Kali is a free Ubuntu Linux-based Live DVD. Kali is used for forensics and penetration testing. Both the 32-bit and 64-bit versions of Kali are available for download free at the following link: https://www.kali.org/downloads/

Drive Letter Assignments in Linux

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

A forensics specialist is responsible for doing investigations of disks. You must know the internals of how disks function and work. Mechanical hard drives work different from solid state drives (SSD). Operating systems file systems have as the number of computers with SSDs continues to increase and the number of mechanical disks in use continues to decline. Thankfully, the file systems handle the details, but it is good for a forensics analyst to understand how each type of storage system works. It will help in the investigations of these drives because often someone can delete a file but a forensic investigator can still recover it. In this lab, you will learn how to partition and format disks in Linux.

Outcomes:

In this lab, you will learn to:

6. Examine Linux Drive Letter Assignments and Mounting Drives
7. Create Primary and Extended Partitions in Linux
8. Format Disks in Linux and Utilizing the Storage

	Key Term	Description
1	fdisk	This Linux command allows users to view disks and partitions. This command can be utilized to create and delete partitions as well as change the partition ID of a disk.
2	mount	This Linux command allows users to view which disks are currently mounted as well as mount local or remote disks. Disks can be mounted as read-only in Linux.
3	umount	This Linux command will allow users to unmount disks currently mounted.
4	mkfs	This Linux command allows users to format unmounted partitions with various file systems including FAT, NTFS, EXT2, EXT3, EXT4, and the ReiserFS.
5	df	The Linux df command will display the available disk space on the system's drives.

The Imaging Process

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, and identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Foundations of Digital Forensics Acquisitions

The candidate will demonstrate an understanding of the methodologies and tools used to collect and process digital forensic evidence.

Overview

This lab is part of a series of lab exercises intended to support courseware for ethical hacker training. The development of this document is funded by the Department of Labor's (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

Digital forensic imaging is defined as a process of copying physical storage without modifying its contents used in gathering evidence and conducting a digital forensic investigation after an organization's system has been compromised. The examination could be related to a crime, network instruction, or other reasons. The image is a complete bit-by-bit replica of the original. Hashing is used to make sure that images are exact copies of the original and the copies are forensically equivalent. In this lab, students will image disks using various tools in Windows and Linux.

Outcomes:

In this lab, you will learn to:

- Use FTK Imager.
- Use HELIX to image a system.
- Use Kali 2 to image a system.

	Key Term	Description
1	FTK Imager	FTK Imager is a GUI Program that will allow a user to create a disk image from within Windows. You can run into complications imaging a disk while in Windows because certain files are locked by the OS. FTK Imager allows you to image a disk or a logical drive.
2	dd	A Unix/Linux program that allows you to backup media. You can create a bit-by-bit copy of the original media, one that is forensically equivalent to the original source.
3	dcfldd	An improved version of the dd program that includes a hashing function.
4	HELIX	HELIX is a combination of a Live CD and an Incident Response CD. The free version, also known as HELIX 3, is available from e-fense at http://www.e-fense.com/products.php. The newest version is based off the Ubuntu CD. When you boot to the HELIX Live CD, it will not automatically mount drives so disk contamination can be avoided.
5	MD5	Message Digest 5 is a 128-bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original. Other hashes, such as SHA-160, which is 160 bits, are more accurate than the 128-bit MD5.

Introduction to Single Purpose Forensic Tools

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Foundations of Digital Forensics Acquisitions

The candidate will demonstrate an understanding of the methodologies and tools used to collect and process digital forensic evidence.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

Hashing is the process of taking in a stream of plain text and transforming the data into a hashed text using a hashing algorithm. You can use the hash to make sure that a message was not modified during transmission. That hash can make sure that the disk image was not tampered with. Hashed images are used in forensics investigations. Hashing is also used on files, passwords, and other pieces of data.

In this lab, you are going to image a disk and create a hash of that disk, verify integrity using file hashing tools, use Foremost to carve and recover deleted files from a disk and use a hex editor to review files.

Outcomes:

In this lab, you will learn to:

1. Use file hashing tools to verify integrity
2. Mount a partition with deleted files and folders
3. Use Foremost to carve files
4. Use a HEX editor

	Key Term	Description
1	Foremost	Foremost is a file carving utility that allows you to carve files that were "deleted" out of a disk image or a mounted partition. Foremost was created by Jesse Kornblum and is available for download from this link: http://foremost.sourceforge.net/
2	Hexadecimal	A numbering system where numbers 0–9 and letters A–F are used. Also known as base 16, hexadecimal is commonly used in computer forensics and networking.
3	HEX Editor	A Graphical User Interface (GUI) or command line tool that can be utilized to analyze the hexadecimal code of files. File headers have hexadecimal signatures that are unique to a particular type of file. For example, a JPEG file has a file signature of JFIF.
4	md5sum	A command that is used from the terminal to verify an MD5 hash. Message Digest 5 is a 128-bit hashing algorithm that aids forensic examiners by

	Key Term	Description
		"proving" that the copy of the media they are working on is "equivalent" to the original.
5	sha1sum	A command that is used from the terminal to verify a sha1 hash. Secure Hash Algorithm is a 160-bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original.

Introduction to Autopsy Forensic Browser

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Foundations of Digital Forensics Acquisitions

The candidate will demonstrate an understanding of the methodologies and tools used to collect and process digital forensic evidence.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

There is different digital forensic investigation software available to digital forensic specialists. We will investigate the Autopsy Forensic Browser, which is a free and open-source tool that can be used to examine disk images and perform forensic investigations. In this lab, students will use the Autopsy Forensic Browser as part of the forensic process.

Outcomes:

In this lab, you will learn to:

5. Install the Autopsy Forensic Browser
6. Create a case in Autopsy Forensic Browser
7. Examine an image with Autopsy
8. Generate a report

	Key Term	Description
1	Autopsy	The open-source digital investigation tool (digital forensic tool), Autopsy, runs on Windows, Linux, OS X, and other UNIX systems. Autopsy can be used to analyze disk images and perform in-depth analysis of file systems such as NTFS

	Key Term	Description
		and FAT.
2	Bookmark	Within a case, relevant items can be designated important or bookmarked.
3	Forensic Report	Forensic software such as FTK, EnCase, and Autopsy allow examiners to generate forensic reports, which contain relevant bookmarks of important artifacts.
4	The Sleuth Kit	The Sleuth Kit (TSK) is a collection of command line tools that are utilized by the Autopsy forensic browser. The Sleuth Kit tools can be utilized without Autopsy.
5	E01 File	A proprietary imaging format developed by Guidance Software (the makers of EnCase). This image format is supported by other tools, such as FTK, PTK, and Autopsy.

FAT File System

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

Digital devices store information in Random Access Memory (RAM) or on storage systems like a hard disk or a solid-state drive (SSD). We will investigate the different file systems from Windows. Normally, operating systems provide this service "behind the scenes," but it is critical that you understand how these file systems work as a digital forensics specialist. File systems that are common to Microsoft operating systems include FAT (File Allocation Table) and NTFS (New Technology File System). There are several versions of FAT, including FAT12, FAT16, FAT32, exFAT, and FATX. The NTFS offers security, whereas the FAT file system is known for its compatibility with many operating systems. This lab investigates the common file systems that are utilized by Windows.

Outcomes:

In this lab, you will learn to:

1. Examine the FAT and NTFS File Systems
2. Use a HEX Editor to Explore a FAT Partition
3. Verify and view image details

4. Analyze a FAT Partition with Autopsy

	Key Term	Description
1	Autopsy	The open-source digital investigation tool (digital forensic tool), Autopsy, runs on Windows, Linux, OS X, and other UNIX systems. Autopsy can be used to analyze disk images and perform in-depth analysis of file systems such as NTFS and FAT.
2	FAT	The acronym FAT stands for File Allocation Table. FAT table holds information about where files are stored on a volume. When a file is deleted from the disk, the entry or entries for those files are removed from the table and the space is marked as available. However, the file, or parts of the file, will remain on the disk until overwritten by information from new files.
3	FAT12	The FAT12 file system is typically used on floppy disks. A FAT12 partition is limited to 32 megabytes. The use of this file system is uncommon in modern times. However, FAT12 partitions can be read with modern operating systems such as Windows 8.
4	FAT16	A FAT16 partition can be up to 2 gigabytes. The FAT16 file system was used primarily with MS-DOS, Windows 3.11, Windows 95a, and Windows NT. None of those operating systems can read the FAT32 file system without third party drivers. Although FAT16 partitions can be read with modern operating systems such as Windows 8 (as well as Linux and Mac OS X), its use is in decline because of the 2-gigabyte limitation.
5	FAT32	A FAT32 partition can be up to 2 terabytes. (There are workarounds to make larger FAT32 partitions.) It is also important to know that a FAT32 volume cannot hold a file that is larger than 4 gigabytes. This limitation makes FAT32 less practical than NTFS.
6	NTFS	The New Technology File System (NTFS) was originally introduced with the Windows NT. NTFS is a journaling file system, which means it keeps a log of changes being written to the disk. If a computer is shut down improperly, it will have a better chance of recovery if it has a journaling file system. Files and folder access can be restricted with the security feature of NTFS. Starting with Windows 2000, Microsoft included the Encrypted File System, or EFS, as an NTFS feature. EFS allows users to encrypt files to protect against unauthorized access.
7	Wipe	A wipe will erase all of the 0's and 1's written to the hard disk. If a wipe is done correctly, all data will be erased and recovery of artifacts will be near impossible.

The NTFS File System

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

This lab investigates the New Technology File System (NTFS) which is one of the most commonly used file systems by the Microsoft Windows operating system. The NTFS is robust and includes many useful features such as the ability to set security permissions on files and folders.

Outcomes:

In this lab, you will learn to:

1. Examine the NTFS File System
2. Use a HEX Editor to explore an NTFS Partition
3. Verify and view the image details
4. Analyze an NTFS Partition With Autopsy

	Key Term	Description
1	NTFS	The acronym NTFS stands for New Technology File System. The NTFS File System was originally introduced with the Windows NT. NTFS is a journaling file system which means it keeps a log of changes being written to the disk. If a computer is shut down improperly, it will have a better chance of recovery if it has a journaling file system. Files and folder access can be restricted with the security feature of NTFS. Starting with Windows 2000, Microsoft included the Encrypted File System, or EFS, as an NTFS feature. EFS allows users to encrypt files to protect against unauthorized access.
2	EFS	A feature of the NTFS file system that allows you to encrypt files and folders. The feature became available on the NTFS file system starting with Windows 2000 and is still available today on Windows 10 and Server 2016.
3	ADS	An Alternate Data Stream, or ADS, is a feature of the NTFS file system that allowed compatibility with older versions of the Mac OS. The feature can be utilized by an individual who is attempting to hide data on their system with an NTFS volume.

	Key Term	Description
4	timestomp	The timestomp command allows you to change file Modified, Access, and Created times. The command can only change MAC times on an NTFS volume.
5	$MFT	The Master File Table is basically like the Table of Contents for an NTFS volume.

Browser Artifact Analysis

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Microsoft Browser Forensics

The candidate will demonstrate an understanding of the artifacts created by Microsoft browsers during user activity.

Third-Party Browser Forensics and Browser Artifact Analysis

The candidate will demonstrate an understanding of the artifacts created by third-party browsers and when privacy settings are applied during user activity.

Windows Registry Artifact Analysis

The candidate will demonstrate an understanding of the registry artifacts created by the system and user activity.

Windows Registry Fundamentals

The candidate will demonstrate an understanding of the structure and purpose of the Windows registry and the types of tools used to analyze and parse the data.

Overview

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG), funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746.

The World Wide Web (www), known as the Web, is a client/server application that hosts resources such as documents, multimedia, images, etc. These resources are identified by Uniform Resource Locators (URLs) and are transferred between a web client/browser and web server using a special protocol called hypertext transfer protocol (HTTP). Documents on the web are created using a markup language called hypertext markup language (HTML). These HTML documents contain hyperlinks that allow you to visit different URLs through these links. By the end of this lab, the student will analyze three major browsers: Internet Explorer, Google Chrome, and Mozilla Firefox.

Outcomes:

In this lab, you will learn to:

1. Meet your browser

2. Analyze Internet Explorer
3. Analyze Google Chrome
4. Analyze Mozilla Firefox

	Key Term	Description
1	Index.dat Viewer	Reads the index.dat files associated with Internet Explorer
2	History Viewer	Displays the entire history stored by web browsers such as Internet Explorer, Mozilla Firefox, and Google Chrome

Communication Artifacts

Introduction
Objective

GIA Certified Forensic Examiner Objective:

Analysis of User Communication

The candidate will demonstrate an understanding of the forensic examination of user communication applications and methods, including host-based and mobile email applications, instant messaging, and other software and Internet-based user communication applications.

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will examine e-mail and Internet Relay Chat (IRC) traffic on the network using various tools. As a forensic specialist, you will learn to use forensic tools that allow you to capture, examine, and report on digital evidence. In this lab, you will look at e-mail and IRC artifacts.

Outcomes:

In this lab, you will learn to:

1. Analyze email messages and programs
2. Examine emails in Network traffic
3. Understand how Internet relay chat works

	Key Term	Description
1	IRC	Internet Relay Chat is used to communicate with other Internet users. IRC is an older technology and is not really as mainstream today as technologies such as Facebook.
2	POP3	Post Office Protocol Version 3: uses port 110 by default to deliver mail
3	SMTP	Simple Mail Transfer Protocol: uses port 25 by default to send mail

	Key Term	Description
4	Wireshark	A protocol analyzer that can also be used as a sniffer tool. Wireshark is free and can be downloaded from the following link: www.wireshark.org/download.html.
5	NetworkMiner	An NFAT, Network Forensic Analysis Tool. The free version can be downloaded at http://sourceforge.net/projects/networkminer/files/latest/download.

User Profiles and the Windows Registry

Introduction
Objective

GIAC Certified Forensic Examiner Objectives:

Analysis of User Communication

The candidate will demonstrate an understanding of the forensic examination of user communication applications and methods, including host-based and mobile email applications, instant messaging, and other software and Internet-based user communication applications.

Windows Registry Artifact Analysis

The candidate will demonstrate an understanding of the registry artifacts created by system and user activity.

Windows Registry Fundamentals

The candidate will demonstrate an understanding of the structure and purpose of the Windows registry and the types of tools used to analyze and parse the data.

Overview

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG) funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746.

The Windows Registry is a special database that stores low-level settings for the Microsoft Windows Operating Systems and applications that use the Windows Registry. Examples of data stored in the registry are settings and values for both hardware and software stored on Windows including application locations and other special configuration keys that hardware and software need in Windows. By the end of this lab, the student will capture the registry hives of the Windows operating system using a free, commercial tool called FTK Imager. Students will then analyze the registry hives using two open source tools: RegRipper and RegViewer.

Outcomes:

In this lab, you will learn to:

1. Capture a live Windows XP registry
2. Analyze the registry hives using RegViewer

3. Analyze the registry hives using Regripper

	Key Term	Description
1	FTK Imager	FTK Imager allows you to image a disk or a logical drive.
2	RegViewer	A registry analysis tool that can open Windows Registry files. The free tool can be downloaded from this link: http://www.gaijin.at/en/getitpage.php?id=regview
3	RegRipper	A tool that extracts and analyzes Registry information
4	Regedit	A built-in program for viewing registry keys on the Windows operating system
5	Windows Registry	A database that contains user and computer settings for a Windows OS

Log Analysis

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Host and Application Event Log Analysis

The candidate will demonstrate an understanding of the purpose of the various types of Windows event, service and application logs, and the forensic value that they can provide.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

Log analysis is an important task in digital forensic investigations. It can give insight to investigators about potential issues that caused a data breach. Operating systems and applications often document key events in logs. Logs can contain valuable information such as failed login attempts, significant operating system events, user administration events, web server events, and other pertinent information related to security on devices. Applications use logs to document key events and also can be used by the vendor to troubleshoot issues with the application.

Outcomes:

In this lab, you will learn to:

1. Examine Windows Event Logs
2. Examine Windows IIS Logs
3. Examine Linux Log Files

	Key Term	Description
1	Event Viewer	The Event Viewer keeps track of Windows Events. The three main logs within

	Key Term	Description
		the Windows Event Viewer are the Application, Security, and System log.
2	auth_log	This log file tracks SSH, or Secure Shell, connections. It provides information such as IP addresses and date and time stamps. It also tracks other events related to security such as the creation of new user accounts and new group accounts.
3	access_log	This log file tracks HTTP, or Hyper Text Transfer Protocol, connections. It provides information such as IP addresses, user agents, and date and time stamps.
4	Internet Information System Logs	Internet Information System, or IIS, logs keep track of IP addresses and user agents of systems connecting to Windows servers running Internet services, such as File transfer Protocol (FTP) and World Wide Web (WWW).
5	psloglist	Part of the PsTools suite, this file can dump event log information. The tool can be downloaded here: http://download.sysinternals.com/files/PSTools.zip

Memory Analysis

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Analysis and Profiling of Systems and Devices

The candidate will demonstrate an understanding of the artifacts created by the Windows operating system during the execution of programs, system start up and use of removable devices.

Overview

This lab is part of a series of lab exercises designed through a grant initiative by the Center for Systems Security and Information Assurance (CSSIA) and the Network Development Group (NDG) and funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746.

In this lab, you will use various methods to determine if an attacker attempted a breach or successfully compromised a system. Some information about the attacker, such as the system's IP address, may be lost if the machine is shut down. For this reason, an investigator collects volatile data such as an image of Random Access Memory (RAM) before shutting down a system.

Outcomes:

In this lab, you will learn to:

1. Obtain a dump of physical memory using DumpIt
2. Attack the victim system with Armitage
3. Use volatility to determine remote connections

	Key Term	Description
1	DumpIt	Generates a copy of the system's physical memory and saves it as a file
2	Volatility	an open source analysis tool used for incident response and analysis
3	PsList	Will determine the running processes in RAM along with their corresponding characteristics.
4	connscan	Will determine the network connections (including IP addresses and ports) in RAM
5	Armitage	Metasploit is a very powerful exploitation framework, but it requires that the user be comfortable using the command line. Armitage is a GUI front end for Metasploit that has many powerful capabilities. An attacker can use Armitage to identify and exploit victim machines within an easy to use graphical environment.

Forensic Case Capstone

Introduction
Objective

GIAC Certified Forensic Examiner Objective:

Foundations of Digital Forensics Acquisition

The candidate will demonstrate an understanding of the methodologies and tools used to collect and process digital forensic evidence.

Fundamental Digital Forensics

The candidate will demonstrate an understanding of forensic methodology, key forensic concepts, identifying types of evidence on current Windows operating systems and be familiar with the structure and composition of modern Windows file systems.

Overview

This lab is part of a series of lab exercises intended to support courseware for Forensics training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

These are the two capstone challenges for the Digital Forensics labs.

Forensic Challenge 1 – Analysis and Reporting in Autopsy

Susie Stapleton has gone missing for 3 days. Her husband and kids are worried sick. A police officer has acquired an image of her hard drive.

- Look through her user profile to find any pictures that might reveal where she is
- Bookmark any photos that you find that you deem to be relevant

- Generate a forensic report in HTML format

Forensic Challenge 2 – Analysis and Reporting in Autopsy 64 bit

Jimmy Jamison has been arrested for stealing credit cards. He has used five different credit cards that were not his. A police officer has acquired an image of his hard drive.

- Look through his user profile to find any documents that Jimmy had
- Export the documents and view them to determine if credit card info is present
- Bookmark any documents that you find that you deem to be relevant
- Generate a forensic report in HTML format

Outcomes:

In this lab, you will learn to:

1. Analyze and Report in Autopsy
2. Analyze and Report in Autopsy 64 bit

	Key Term	Description
1	Autopsy	an open source forensic suite that will allow you to analyze disk images
2	Sleuthkit	The sleuthkit, or TSK, is a bunch of command line tools that is utilized by the Autospy forensic browser. The sleuthkit tools can be utilized without Autopsy.
3	MD5	Message Digest 5 is a 128 bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original. Other hashes, such as SHA-1, which is 160 bits, are more accurate than the 128-bit MD5.
4	SHA1	Secure Hash Algorithm is a 160-bit hashing algorithm that aids forensic examiners by "proving" that the copy of the media they are working on is "equivalent" to the original. There are also 256-, 384-, and 512-bit versions of SHA that are more accurate.