Blue Team Level 1 Certification (Standard)

Introduction to BTL1
- Welcome to Blue Team Level 1! — 4 Topics
- Lab and Forum Access

SECURITY FUNDAMENTALS DOMAIN
- Introduction to Security Fundamentals — 1 Topic
- Soft Skills — 7 Topics
- Security Controls — 5 Topics | 1 Quiz
- Networking 101 — 6 Topics | 1 Quiz
- Management Principles — 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN
- PA1) Introduction to Emails and Phishing — 7 Topics | 1 Quiz
- PA2) Types of Phishing Emails — 10 Topics | 2 Quizzes
- PA3) Tactics and Techniques Used — 12 Topics | 2 Quizzes
- PA4) Investigating a Phishing Email — 8 Topics | 2 Quizzes
- PA5) Analysing URLs, Attachments, and Artifacts — 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions — 12 Topics | 1 Quiz
- PA7) Report Writing — 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge — 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN
- TI1) Introduction to Threat Intelligence — 7 Topics
- TI2) Threat Actors & APTs — 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence — 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence — 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

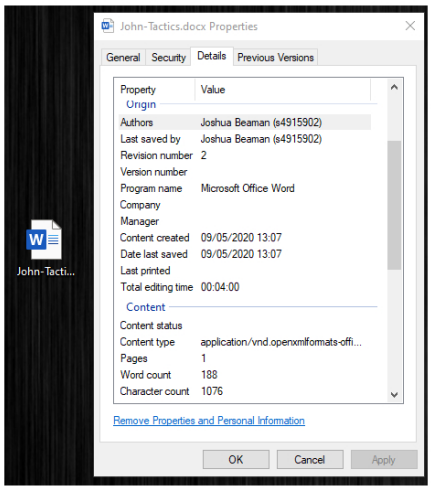
DIGITAL FORENSICS DOMAIN
- DF1) Introduction to Digital Forensics — 5 Topics
- DF2) Forensics Fundamentals — 10 Topics | 5 Quizzes

Metadata and File Carving

This lesson is going to cover what metadata is and how it can contain valuable information, and what file carving is, and how we can retrieve files that have been hidden inside other files. Metadata is "data about data", which sounds confusing, but is relatively straightforward. If you have a Microsoft Word document that contains text, that text is data. Metadata is information that describes the data and can include details such as the author of the document, and in photos, it can contain the camera settings, GPS location, resolution, and much more. File carving is a process of searching for files in a data stream and is used to carve deleted files from disk images, so we can investigate files that have been deleted by a user, provided they haven't been overwritten with new data.

METADATA

Let's take a look at some metadata by viewing file properties inside the Windows OS. By right-clicking on a Microsoft Word file and clicking on the 'Details' tab we can see some useful information including the author, when the file was created, last saved, and the word count.



We can also retrieve metadata in a Linux system by using the same method as above, right-clicking on a file and viewing the properties, or using two commands, `ls -lisap <file>` and `stat <file>`, as shown below. In this case, we're provided with information such as the read/write permissions we have, the file name and size, and the times for when the file was last accessed and modified.

```
root@SBTLab2:~/Desktop# ls -lisap John-Tactics.docx
1075391 16 -rwxrw-rw- 1 root root 12943 May 11 12:23 John-Tactics.docx
root@SBTLab2:~/Desktop# stat John-Tactics.docx
  File: John-Tactics.docx
  Size: 12943           Blocks: 32         IO Block: 4096   regular file
Device: 801h/2049d      Inode: 1075391     Links: 1
Access: (0766/-rwxrw-rw-)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2020-05-11 12:23:46.745563000 +0100
Modify: 2020-05-11 12:23:46.745563000 +0100
Change: 2020-05-22 12:10:46.786990524 +0100
 Birth: -
```

A great command-line tool we can use in Kali Linux is `exiftool`, which works to retrieve metadata from files. Type "exiftool" to see if you have it installed, and if not, use `sudo apt-get install exiftool` to download and install the tool.

- Section Introduction, Forensics Fundamentals
- Introduction to Data Representation
- Activity) Data Representation
- Hard Disk Drive Basics
- SSD Drive Basics
- File Systems
- Lab) File Systems
- Digital Evidence and Handling
- Order of Volatility
- Metadata and File Carving
- Lab) Metadata and File Carving
- Memory, Pagefile and Hibernation File
- Hashing and Integrity
- Lab) Hashing and Integrity
- Activity) End of Section Review, Forensics Fundamentals

DF3) Digital Evidence Collection
8 Topics | 1 Quiz

DF4) Windows Investigations
3 Topics | 3 Quizzes

DF5) Linux Investigations
4 Topics | 2 Quizzes

DF6) Volatility
3 Topics | 1 Quiz

DF7) Autopsy
4 Topics | 1 Quiz

SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN

SI1) Introduction to SIEM
7 Topics | 1 Quiz

SI2) Logging
6 Topics | 2 Quizzes

SI3) Aggregation
2 Topics | 1 Quiz

SI4) Correlation
6 Topics | 1 Quiz

SI5) Using Splunk
5 Topics | 2 Quizzes

INCIDENT RESPONSE DOMAIN

IR1) Introduction to Incident Response
8 Topics | 1 Quiz

IR2) Preparation Phase
10 Topics | 2 Quizzes

IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes

IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz

IR5) Lessons Learned and Reporting
7 Topics

IR6) MITRE ATT&CK
13 Topics | 2 Quizzes

BTL1 EXAM

Exam Preparation

tool.

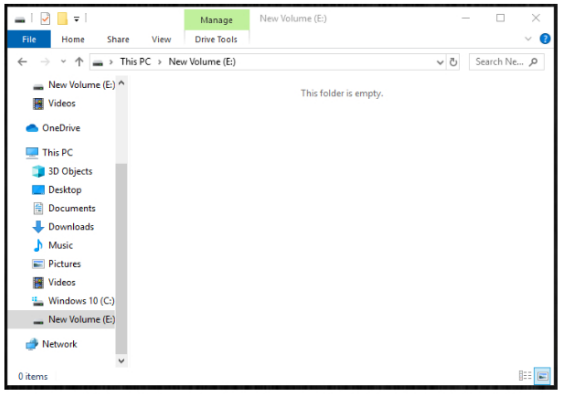
```
root@SBTLab2:~/Desktop# exiftool
bash: exiftool: command not found
root@SBTLab2:~/Desktop# sudo apt-get install exiftool
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
Note, selecting 'libimage-exiftool-perl' instead of 'exiftool'
The following additional packages will be installed:
  libarchive-zip-perl libmime-charset-perl libposix-strptime-perl libsombok3 libunicode-linebreak-perl
Suggested packages:
  libencode-hanextra-perl libpod2-base-perl
The following NEW packages will be installed:
  libarchive-zip-perl libimage-exiftool-perl libmime-charset-perl libposix-strptime-perl libsombok3
  libunicode-linebreak-perl
0 upgraded, 6 newly installed, 0 to remove and 1167 not upgraded.
Need to get 3,829 kB of archives.
After this operation, 22.3 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

The tool is straightforward to use, just type **`exiftool <filename>`** and we can retrieve a ton of useful information, as shown in the GIF demonstration below.

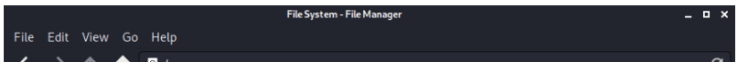
```
File  Actions  Edit  View  Help
root@SBTLab2: ~/Desktop

MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Profile CMM Type                : Linotronic
Profile Version                 : 2.1.0
Profile Class                   : Display Device Profile
Color Space Data                : RGB
Profile Connection Space        : XYZ
Profile Date Time               : 1998:02:09 06:49:00
Profile File Signature          : acsp
Primary Platform                : Microsoft Corporation
CMM Flags                       : Not Embedded, Independent
Device Manufacturer             : Hewlett-Packard
Device Model                    : sRGB
Device Attributes               : Reflective, Glossy, Positive, Color
Rendering Intent                : Perceptual
Connection Space Illuminant     : 0.9642 1 0.82491
Profile Creator                 : Hewlett-Packard
Profile ID                      : 0
Profile Copyright               : Copyright (c) 1998 Hewlett-Packard Company
Profile Description             : sRGB IEC61966-2.1
Media White Point               : 0.95045 1 1.08905
Media Black Point               : 0 0 0
Red Matrix Column               : 0.43607 0.22249 0.01392
Green Matrix Column             : 0.38515 0.71687 0.09708
Blue Matrix Column              : 0.14307 0.06061 0.7141
Device Mfg Desc                 : IEC http://www.iec.ch
Device Model Desc               : IEC 61966-2.1 Default RGB colour space - sRGB
Viewing Cond Desc               : Reference Viewing Condition in IEC61966-2.1
Viewing Cond Illuminant         : 19.6445 20.3718 16.8089
Viewing Cond Surround           : 3.92889 4.07439 3.36179
```

FILE CARVING

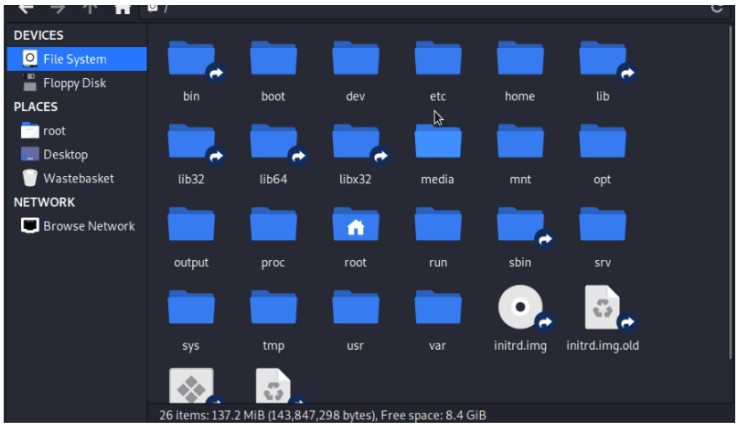
We're going to show you how to retrieve deleted files using the Linux command-line tool **`scalpel`**. If you haven't used this tool before, use the command **`man scalpel`** to see what it can do! When attempting to use scalpel on a disk image file (.img) the tool will communicate with it's configuration file, which is located at **`/etc/scalpel/scalpel.conf`** by default. This configuration file allows us to define what file types we're trying to search for. Let's walk through an example where we believe a suspect has deleted a .jpg image file containing sensitive information, and we need to retrieve it as digital evidence. The hard drive appeared empty when collected from the crime scene, but a bit-by-bit disk image was taken, so we can identify any deleted files.



First things first, we need to edit the **`scalpel.conf`** file to tell scalpel that we want to identify and extract Microsoft Office Word files. You can use command-line text editors such as nano or vim, but it's easier to use the file system GUI and navigate to the file yourself. The file path is **/etc/scalpel/scalpel.conf.**



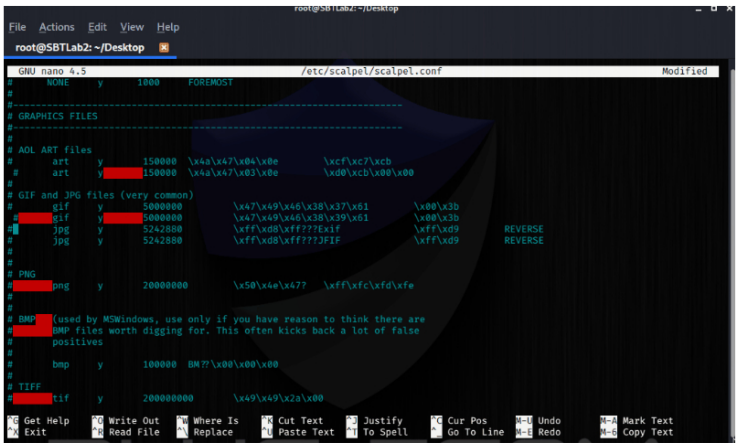
- Using RDP and SSH
- How to Start Your Exam



Once you've found and opened the config file in your choice of text editor, you'll be presented with a file that looks like the below screenshot, where we're looking at the section for Microsoft Office document profiles. The "#" at the start of each line means they are commented out and are not read by the program when the .config file is called.

```
#-----------------------------------------------------------------------
# MICROSOFT OFFICE
#-----------------------------------------------------------------------
#
# Word documents
#
#
#       doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 \xd0\xcf\x11\xe0\xa1\xb1\x1a\xe1\x00\x00 NEXT
#       doc     y       10000000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
#       pst     y       500000000       \x21\x42\x4e\xa5\x6f\xb5\xa6
#       ost     y       500000000       \x21\x42\x44\x4e
#
# Outlook Express
#       dbx     y       10000000        \xcf\xad\x12\xfe\xc5\xfd\x74\x6f
#       idx     y       10000000        \x4a\x4d\x46\x39
#       mbx     y       10000000        \x4a\x4d\x46\x36
#
```

As we're looking for .jpg image files, we need to locate the section of the .conf file that references jpg files. In the below screenshot you can see how we're able to remove the hashtags to enable detection for this file type.



Now that we've configured scalpel to understand what files we're looking for, we can summon the tool using the following command: `scalpel -b -o <output> <disk image file>`

- **"scalpel"** calls the tool we want to use
- **"-b"** states we want to carve files out of the disk image file
- **"-o <name>"** provides a directory for recovered files to be stored. This MUST be an empty directory, or the name of a non-existent directory, as scalpel will create one
- **"<disk image file>"** tells scalpel the file we want to search for files inside

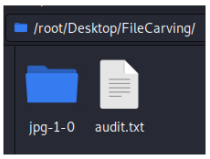
Example command: `scalpel -b -o /root/Desktop/ScalpelOutput DiskImage1.img`

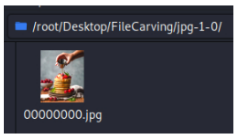
Let's run the command and watch scalpel recover any JPG image files for us!

```
root@SBTLab2:~/Desktop# scalpel -b -o /root/Desktop/FileCarving/ DiskImage.001
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.

Opening target "/root/Desktop/DiskImage.001"

Image file pass 1/2.
DiskImage.001: 100.0% |*****************************************************************************|   24.6 MB    00:00 ETA
Allocating work queues ...
Work queues allocation complete. Building carve lists ...
Carve lists built.  Workload:
```

```
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x45\x78\x69\x66" and footer "\xff\xd9" --> 0 files
jpg with header "\xff\xd8\xff\x3f\x3f\x3f\x4a\x46\x49\x46" and footer "\xff\xd9" --> 1 files
y with header "\x31\x4c\x54\x42" and footer "" --> 0 files
Carving files from image.
Image file pass 2/2.
DiskImage.001: 100.0% |*****************************************************************************|   24.6 MB    00:00 ETA
Processing of image file complete. Cleaning up...
Done.
Scalpel is done, files carved = 1, elapsed = 0 seconds.
root@SBTLab2:~/Desktop#
```

In the above screenshot we can see that scalpel identified and retrieved one JPG file, based on the message at the bottom of the terminal "Scalpel is done, files carved = 1, elapsed = 0 seconds"! Let's go see what Scalpel found in the output directory we listed. In the below screenshots we can see that Scalpel created a file audit.txt which contains information about the activity the tool has completed, and the jpg directory includes the deleted photo we have retrieved.





It's worth mentioning that profiles in the scalpel.conf file can be created by a user if you need to search for specific or custom files, by altering the file extension, file header, and file footer values. The top of the .conf file has detailed information about writing custom detection profiles for file carving, so give it a read!

Quizzes

Lab) Metadata and File Carving

Previous Topic

Back to Lesson

Next Topic

Privacy & Cookies Policy

Privacy - Terms