
CTF Session 2: Steganography and Forensics

tinyurl.com/CTFslides2

Anyone want to compete in a CTF together?

We'll act as mentors and teammates :)

- School CTF (Beginner Friendly)
 - Nov 5, Sunday, Week 6
 - <https://school-ctf.org/>
 - RC3 CTF 2017 (Intermediate)
 - Nov 18, Saturday, Week 7
 - <https://rc3ctf.rc3.club/>
 - TU CTF (Beginner friendly)
 - Nov 26, Sunday, Week 9
 - <https://tuctf.asciioverflow.com/>
 - Check out ctftime.org for more CTF dates! Let me know if there's one that catches your eye :)
-

Forensics

Adjective

relating to or denoting the application of scientific methods and techniques to the investigation of crime: *forensic evidence*



Forensics (in CTFs)

Usually involves extraction of data, including from network captures, process image dumps, and hard disk images



Examples of Forensics Questions

1. There is a secret contained in this pcap dump of an app communicating with its server. Find it.
2. Here is a disk image of a USB drive. The secret file has been deleted. Try to “undelete” it.
3. We snatched this running computer from a criminal and immediately placed it in liquid nitrogen within a faraday cage to extract its RAM. (Sounds cool doesn't it?) We are sure the criminal is editing a Word doc but he hasn't saved it. Can you recover it?

Real World Forensics vs CTF Forensics

From "The CTF Field Guide":

*Unlike most CTF forensics challenges, a real-world computer forensics task would hardly ever involve unraveling a scheme of cleverly encoded bytes, hidden data, matroshka-like files-within-files, or other such **brain-teaser puzzles**. One would typically not bust a criminal case by carefully reassembling a corrupted PNG file, revealing a photo of a QR code that decodes to a password for a zip archive containing an NES ROM that when played will output the confession. Rather, real-world forensics typically requires that a practitioner find **indirect evidence of maliciousness**: either the traces of an attacker on a system, or the traces of "insider threat" behavior. [...]*

This disconnect between the somewhat artificial puzzle-game CTF "Forensics" and the way that forensics is actually done in the field [...]

Forensics 1: Undeleting Files

Q: What happens when you delete a file?

A:

It doesn't matter if you use the Finder/Explorer GUI or commands like `rm(1)` or system calls like `unlink(2)`. Ultimately it asks the filesystem to remove the file.

But the filesystem does not actually remove the file! It simply removes a reference to the file in the directory entries (metadata).

This means file contents are still there on the disk.

Forensics 1: Undeleting Files

A great utility to undelete files (and more) is called **TestDisk** as well as its simpler cousin **PhotoRec**.

Website: <http://www.cgsecurity.org>

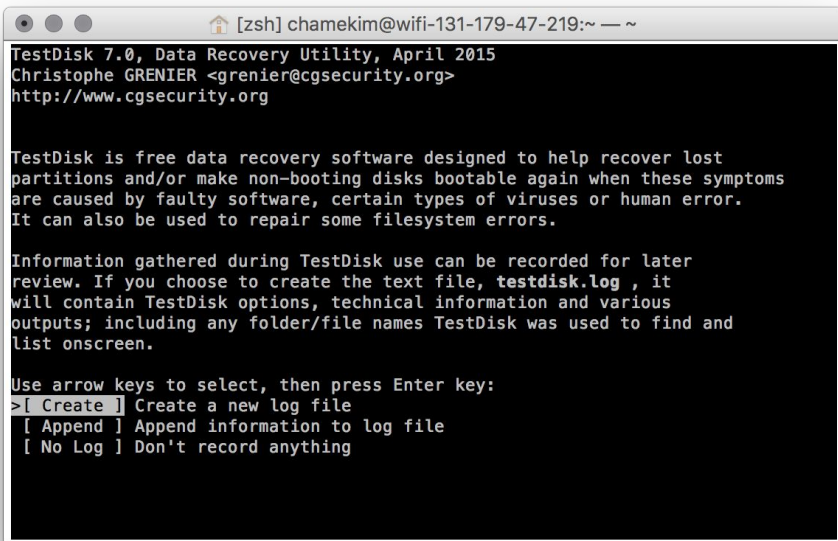
On Mac: `brew install testdisk`

On Windows: Download tinyurl.com/ctf-testdisk-win and extract it

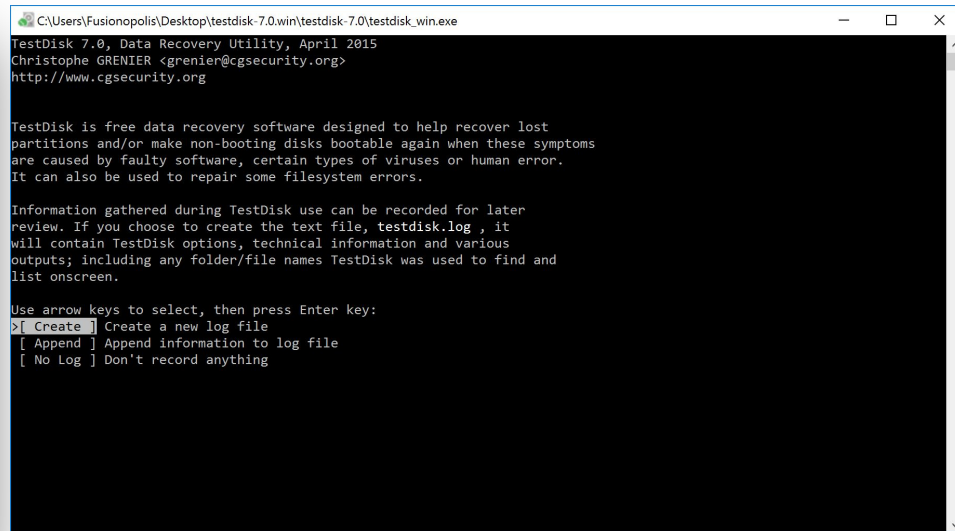
On Kali Linux: Already Installed! Type `testdisk` in a Terminal to start it.

Forensics 1: Undeleting Files

You should see the following when you are running testdisk successfully:



```
[zsh] chamekim@wifi-131-179-47-219:~ -- ~  
TestDisk 7.0, Data Recovery Utility, April 2015  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
TestDisk is free data recovery software designed to help recover lost  
partitions and/or make non-booting disks bootable again when these symptoms  
are caused by faulty software, certain types of viruses or human error.  
It can also be used to repair some filesystem errors.  
  
Information gathered during TestDisk use can be recorded for later  
review. If you choose to create the text file, testdisk.log, it  
will contain TestDisk options, technical information and various  
outputs; including any folder/file names TestDisk was used to find and  
list onscreen.  
  
Use arrow keys to select, then press Enter key:  
> [ Create ] Create a new log file  
[ Append ] Append information to log file  
[ No Log ] Don't record anything
```



```
C:\Users\Fusionopolis\Desktop\testdisk-7.0.win\testdisk-7.0\testdisk_win.exe  
TestDisk 7.0, Data Recovery Utility, April 2015  
Christophe GRENIER <grenier@cgsecurity.org>  
http://www.cgsecurity.org  
  
TestDisk is free data recovery software designed to help recover lost  
partitions and/or make non-booting disks bootable again when these symptoms  
are caused by faulty software, certain types of viruses or human error.  
It can also be used to repair some filesystem errors.  
  
Information gathered during TestDisk use can be recorded for later  
review. If you choose to create the text file, testdisk.log, it  
will contain TestDisk options, technical information and various  
outputs; including any folder/file names TestDisk was used to find and  
list onscreen.  
  
Use arrow keys to select, then press Enter key:  
> [ Create ] Create a new log file  
[ Append ] Append information to log file  
[ No Log ] Don't record anything
```

Forensics 1: Undeleting Files

Here's an exercise: download this DMG file and recover a deleted photo inside it: tinyurl.com/ctf-deleted

(It is a Mac disk image but no worries, Windows and Linux versions of testdisk can extract deleted files from it too.)

Testdisk's UI is old-fashioned but feel free to explore and figure it out yourself.

Once you succeed, you'll be able to see a pretty picture of ... something ...

Forensics 2: A Tale of Two Filesystems

Download this artificially constructed (and a bit contrived) CD image:

tinyurl.com/ctf-forensics-img

You can double-click the file to open it in Windows 10 or Mac.

What do you see?

Does the disc image really only contain what you see?

Forensics 2: A Tale of Two Filesystems

Eject the disk image and try opening the file with a hex editor. What if you try to search for the string “Annabel” in your hex editor?

Also try using testdisk/photorec. Can it recover anything?

Hint: pycdlib

Hint 2: isoinfo

Forensics 2: A Tale of Two Filesystems

The secret: This is a CD image that contains two different file systems.

In one of the filesystems (Joliet), there is only one file in it.

In the other filesystem (ISO 9660), there are three files in it.

```
import pycdlib
iso = pycdlib.PyCdlib()
iso.open('CTF Forensics.iso')
list(c.file_identifier() for c in iso.list_dir('/'))
```

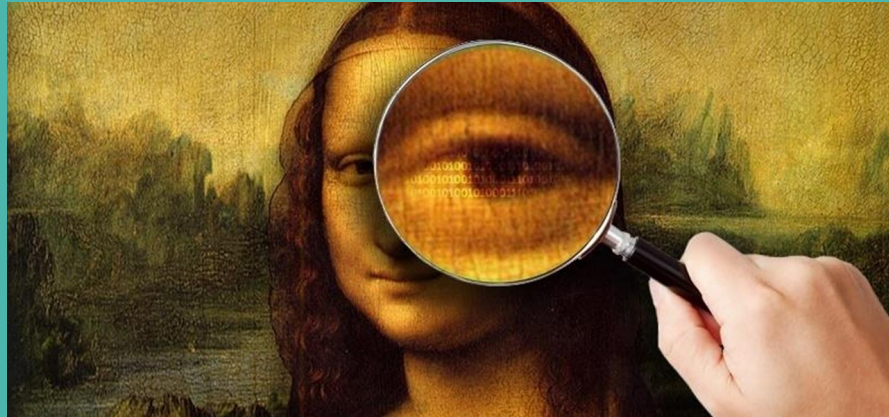
Forensics 3: Network Captures

- Sometimes in forensics, you are handed a pcap file and asked to find things in it.
- pcap means “packet capture”
 - When a computer communicates over the network, it does so through a series of IPv4 or IPv6 packets, encoded into a format corresponding to relevant physical media: Ethernet, Wi-Fi, Point-to-Point, Bluetooth, etc.
 - We usually don’t care about lower level details about the physical media.
- But raw IP packets are extremely rare. We usually use protocols on top of IP packets: TCP, UDP, SCTP, etc.
- You can use tcpdump or wireshark to capture network traffic

Forensics 3: Network Captures

- A large number of exercises if you want to go into network traffic analysis in depth: <http://malware-traffic-analysis.net/training-exercises.html>
- Here is a tiny, tiny example to get you started:
 - Download tinyurl.com/ctf-traffic
 - Answer these things:
 - What protocol is being used?
 - What's the username used to login?
 - What's the password?
 - What's the secret file?
- Wireshark looks intimidating but feel free to explore!

Steganography



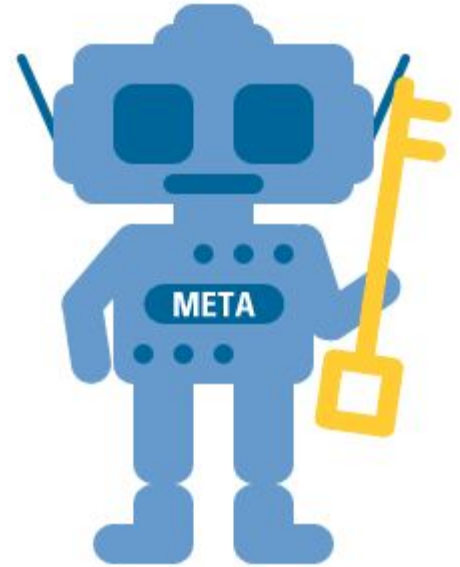
Wait... So, what's steganography again?

- It is the practice of concealing a file, message, image, or video within another file, message, image, or video.
- In CTFs, steganography usually involves finding the hints or flags that have been hidden with steganography. Most commonly a media file will be given as a task with no further instructions, and the participants have to be able to uncover the message that has been encoded in the media.



Metadata

- Metadata is data about the digital document it is attached to, such as the author of a document, when it was last updated, the software used to create or save the document etc.
- More importantly, sometimes you can actually see where and when the photo was taken.
- All of the cool information about the creator of the photo and date and the location together form Administrative metadata.



EXIF Data (Exchangeable Image File Format)

- Exchangeable image file format is a standard that specifies the formats for images, sound, and other systems handling image and sound files recorded by digital cameras.
- It can even tell you the model of your camera!
- Common command line tools include exif and exiftool.
- exiftool is platform independent and can be downloaded here:
 - <https://www.sno.phy.queensu.ca/~phil/exiftool/index.html>
- Fun fact! John McAfee, founder of McAfee and once international criminal, was caught because a reporter who interviewed him posted a picture with Exif geolocation metadata
- Exif data is a subset of metadata, it doesn't get erased when you upload it over the web.

**Let's walk through extracting information from
images!**



Exercise

Find out where and when we
took this picture. :)

tinyurl.com/findwhereiam



So, we can view Metadata and EXIF data...

Can we modify this data?

- Yeah, of course we can! Want people to think you took a picture in NorCal, even though it was taken in the sculpture garden? Let's walk through how to do that.
- The old fashioned way:
 - Doing it on your laptop yourself, we'll walk around to show you how to do that.
- The easier way:
 - Using a website like this:
 - <https://www.thexifer.net/>
 - BEWARE: Don't upload any important/sensitive/secret picture to these websites!

The file and strings command in Linux

- A way to find out the true file type of a file, since Linux doesn't really care about file extensions
 - `file <filename>`
 - `man file` //gives you the manual of the file command
- `strings` returns each string of printable characters in files. It's used to determine the contents of a file and extract text from binary files.
 - `strings <filename>`
 - `man strings` //gives you the manual of the strings command
- Let's see what the results look like

Stegsolve

- Stegsolve is a tool that performs an analysis of the file structure. It can combine images in a variety of ways.
- Anyone who has a Mac/Linux, run this on your terminal
 - `curl http://www.caesum.com/handbook/Stegsolve.jar -O stegsolve.jar`
 - Change curl to wget if you have a Linux machine
 - `chmod + x stegsolve.jar`
 - `mv stegsolve.jar bin /`
- Anyone who has Windows:
 - Download Stegsolve from <http://www.caesum.com/handbook/Stegsolve.jar>
 - For it to work also it is necessary to install Java Runtime Environment
 - <http://goo.gl/LKvNof>

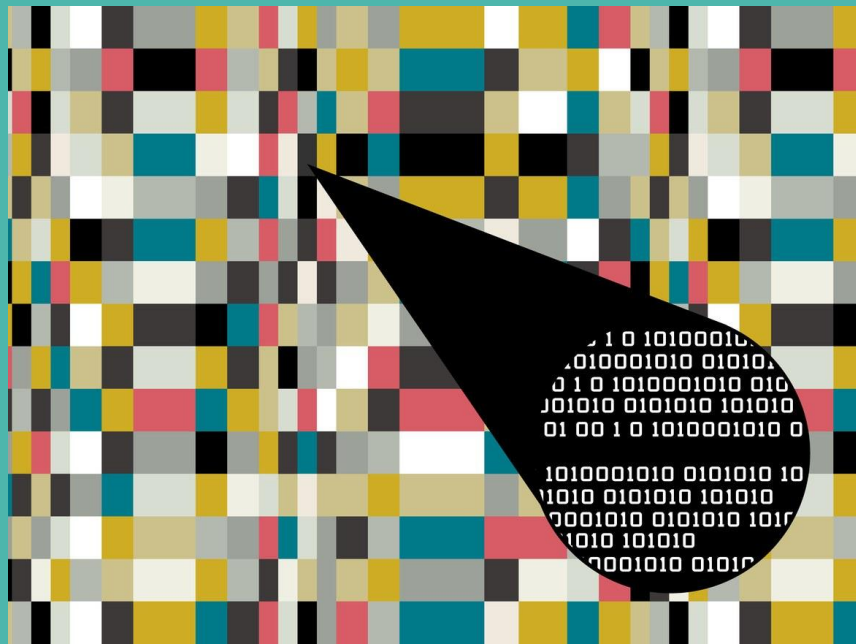
Binwalk

- Extracts files found in firmware images
- Scans firmware images to see if there are any embedded file types in it
 - (Think of firmware as 'software for hardware', super low level software that deals with hardware.
- Syntax:
 - `binwalk -options <filename>`
 - Use `-e` to extract files.
- If you have a Windows computer and your VM hasn't been set up by now, time to find a friend with a Mac!
 - <https://github.com/devttys0/binwalk/wiki/Quick-Start-Guide>
 - This is the install link, let's walk through it together.

Time for another demo!

This time we'll be using strings,
exiftool and binwalk.

<http://tinyurl.com/binwalkstrings>



Decoding Images with GIMP

- Basically free Photoshop- great way to edit photos
- In CTF, we'll be applying layers on photos to try and see if there's a message hidden somewhere
- <https://www.gimp.org/downloads/>
- We'll be working on hiding text in an image and hiding an image in an image.
- Okay everyone, let's divide up into groups!

Let's learn to encode a message in GIMP

Let's decode the message we just encoded

A little bit of Python scripting

- So, some steganography questions require Python scripting
- Beginner/Advanced Python tutorial options
 - <http://thepythonguru.com>
- This module is used in most python steganography scripts
 - <http://pillow.readthedocs.io/en/3.4.x/reference/Image.html>
- Mentors will be walking around to give help groups out who are trying out scripting questions.

Find the message in this image

You need to use binwalk and
then steghide



Thank you for coming!

tinyurl.com/ctfsession2