

# Introduction to Digital Forensics

## Challenge Submission

1. When considering the order of volatility, which is the MOST volatile form of evidence?

Cache

2. What is the Chain of Custody in regard to digital forensics? (Multiple Choice)

Paper trail for evidence that shows where it has been, and who has been in possession of it.

3. An employee is under investigation, and you are sent to look at his laptop. You discover that it is locked, but you have the user's password to unlock it. What should you do next? (Multiple Choice)

Wait for the user and get them to sign-in

4. Can social-media posts be counted as a form of electronic evidence? a) Yes, b) No

Yes

5. Which one of the following evidence types holds the most value in court? (Multiple Choice)

Real Evidence

6. When cracking ZIP passwords using fcrackzip, what is the flag used to conduct a brute force attack, with lowercase letters and numbers? format: -(flag) -(flag) (values)

-b -c a1

7. Digital Forensics entails... (Multiple Choice)

The identification, preservation, and analysis of evidence found on electronic devices.

8. What does HTCIA stand for in regard to Digital Forensics?

High Technology Crime Investigation Association

9. Computer Forensics and Data Recovery are the same thing, true or false?

False

10. Corporate Policies can dictate which of the following? (Multiple Choice)

All of the above

[Evidence 1/4]

Check for the hidden files in all the directories. Then check if the extension has been modified using the 'file' command. If modified then use 'stegseek' command to see if the modified file has any hidden data in it. (Before the last step, make sure to unzip the rockyou.txt.gz). If there is a zip file then use 'fcrackzip' command to crack the password for the file.

```
(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019]
$ ls -la
.  ..  .test  Images  Payslips  'Saved Emails'  'WebDev work'  'Weekly Meeting Notes'

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019]
$ cd WebDev\ work

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work]
$ ls -la
.  ..  Links.txt  VERSION  'WAF on OS Detection Nmap Scan.txt'  'finished webpages'

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work]
$ cd unfinished\ webpages

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages]
$ ls -la
.  ..  'Power Free Website Template - Free-CSS.com.zip'  templatemo_508_power  to-do

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ cd to-do

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ ls -la
.  ..  .a0415ns.zip

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ stegseek -sf .a0415ns.zip
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[!] error: the file format of the file ".a0415ns.zip" is not supported.
```

```

[nitin@kali]--[~/../J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ fcrackzip -D -u -p /usr/share/wordlists/rockyou.txt .a0415ns.zip

Devices
PASSWORD FOUND!!!!: pw = vendy13031988

[nitin@kali]--[~/../J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ unzip .a0415ns.zip
Archive:  .a0415ns.zip
[a0415ns.zip] employeeedump password:
  inflating: employeeedump

[nitin@kali]--[~/../J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ ls -a
.  ..  .a0415ns.zip  employeeedump

[nitin@kali]--[~/../J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/to-do]
$ head employeeedump
{Part 1 of 4}
,First Name,Last Name,Gender,Country,Age,Date,VPN UserID
1,Dulce,Abril,Female,United States,32,15/10/2017,1562
2,Mara,Hashimoto,Female,Great Britain,25,16/08/2016,1582
3,Philip,Gent,Male,France,36,21/05/2015,2587
4,Kathleen,Hanner,Female,United States,25,15/10/2017,3549
5,Nereida,Magwood,Female,United States,58,16/08/2016,2468
6,Gaston,Brumm,Male,United States,24,21/05/2015,2554
7,Etta,Hurn,Female,Great Britain,56,15/10/2017,3598
8,Earlean,Melgar,Female,United States,27,16/08/2016,2456

```

1.What is the name of the file where the evidence was found? (filename and extension)  
employeeedump.txt

2.What is the name of the directory your in where this evidence was found?  
/to-do/

3.What piece of evidence have you found? (Multiple Choice)  
Employee information

[Evidence 2/4]

Check for the hidden files in all the directories. Then check if the extension has been modified using the 'file' command. If modified then use 'stegseek' command to see if the modified file has any hidden data in it.(Before the last step, make sure to unzip the rockyou.txt.gz)

```
(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019]
$ ls -a
.  ..  .test  Images  Payslips  'Saved Emails'  'WebDev work'  'Weekly Meeting Notes'
$ cd Images
(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Images]
$ ls -a
.  ..  'desk stock img.mp3'  exploratory.jpg  'office 2.jpg'  website-stock-photo.jpg
..  'drupal 8 logo Stacked CMYK 300.png'  laptop.jpg  'office pic1.jpg'  wireframe-design-guide.png
$ file *
desk stock img.mp3:          JPEG image data, JFIF standard 1.01, resolution (DPI),
direntries=8, manufacturer=SONY, model=ILCE-7M2, xresolution=126, yresolution=134, resolut
02:06 02:37:36], baseline, precision 8, 1080x720, components 3
drupal 8 logo Stacked CMYK 300.png: PNG image data, 500 x 513, 8-bit/color RGBA, non-inter
exploratory.jpg:             JPEG image data, JFIF standard 1.01, aspect ratio, dens
laptop.jpg:                  JPEG image data, JFIF standard 1.01, resolution (DPI),
office 2.jpg:                 JPEG image data, JFIF standard 1.01, resolution (DPI),
office pic1.jpg:             JPEG image data, JFIF standard 1.01, resolution (DPI),
direntries=1, description=Interior view of a modern office, business template. Left side o
ion 8, 612x344, components 3
website-stock-photo.jpg:     JPEG image data, JFIF standard 1.01, resolution (DPI),
direntries=1, description=3d rendering of devices on table with responsive design\377\341\
wireframe-design-guide.png:  PNG image data, 750 x 480, 8-bit colormap, non-interlac
```

```
(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Images]
$ stegseek -sf laptop.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "password"
[i] Original filename: "passwords".
[i] Extracting to "laptop.jpg.out".

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Images]
$ ls -a
.  ..  'desk stock img.mp3'  exploratory.jpg  laptop.jpg.out
..  'drupal 8 logo Stacked CMYK 300.png'  laptop.jpg  'office 2.jpg'
$ cat laptop.jpg.out
{2/4}
a123456
vincent
Usuckballz1
spooky
qweasd
cumshot
free
frankie
```

1.What is the name of the file where the evidence was found? (filename and extension)

laptop.jpg

2.What is the name of the directory your in where this evidence was found?

/Images/

3.What piece of evidence have you found?(*Multiple Choice*)

List of employee passwords



[Evidence 3/4]

Check for the hidden files in all the directories. Then check if the extension has been modified using the 'file' command. If modified then use 'stegseek' command to see if the modified file has any hidden data in it.(Before the last step, make sure to unzip the rockyou.txt.gz). If nothing is hidden then try changing the file to the original extension.

```
(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019]
$ ls -a
.  ..  .test  Images  Payslips  'Saved Emails'  'WebDev work'  'Weekly Meeting Notes'

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019]
$ cd Weekly\ Meeting\ Notes

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes]
$ ls -a
.  ..  'Week 10'  'Week 9'

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes]
$ cd Week\ 10

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
$ ls -a
.  ..  posidon.xml  tue

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
$ file *
posidon.xml: PNG image data, 162 x 147, 8-bit/color RGB, non-interlaced
tue:        ASCII text

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
$ stegseek -sf posidon.xml
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[!] error: the file format of the file "posidon.xml" is not supported.

(nitin@kali)-[~/Downloads/J Harrison Disk Image 10.09.2019/Weekly Meeting Notes/Week 10]
$ stegseek -sf tue
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[!] error: the file format of the file "tue" is not supported.
```

{3/4}

OFFICES//  
UK LONDON  
UK MANCHESTER  
US WASHINGTON  
UK EXETER  
US TAMPA, FL

- 1.What is the name of the file where the evidence was found? (filename and extension) posidon.xml
- 2.What is the name of the directory your in where this evidence was found? /Week 10/
- 3.What piece of evidence have you found?(*Multiple Choice*) *Office locations*

[Evidence 4/4]

Check for the hidden files in all the directories. Then check if the extension has been modified using the 'file' command. If modified then use 'stegseek' command to see if the modified file has any hidden data in it.(Before the last step, make sure to unzip the rockyou.txt.gz). Also check all text files, to make it easier try using grep command for the string "4 of 4".

```
(nitin@kali)-[~/.../J Harrison Disk Image 10.09.2019/WebDev work/unfinished webpages/templatemo_508_power]
$ cd css

(nitin@kali)-[~/.../WebDev work/unfinished webpages/templatemo_508_power/css]
$ ls -a
. .. animate.css bootstrap.min.abc bootstrap.min.css font-awesome.css owl-carousel.css templatemo_misc.

(nitin@kali)-[~/.../WebDev work/unfinished webpages/templatemo_508_power/css]
$ file *
animate.css:      ASCII text, with very long lines (460)
bootstrap.min.abc: ASCII text, with very long lines (65005)
bootstrap.min.css: ASCII text, with very long lines (65019)
font-awesome.css: troff or preprocessor input, ASCII text, with very long lines (305)
owl-carousel.css:  ASCII text, with CRLF line terminators
templatemo_misc.css: ASCII text, with CRLF line terminators
templatemo_style.css: ASCII text, with CRLF line terminators

(nitin@kali)-[~/.../WebDev work/unfinished webpages/templatemo_508_power/css]
$ cat bootstrap.min.abc
/*!
 * Bootstrap v3.1.1 (http://getbootstrap.com)
 * Copyright 2011-2014 Twitter, Inc.
 * Licensed under MIT (https://github.com/twbs/bootstrap/blob/master/LICENSE)
 */

/*! {Part 4 of 4}
 * This is in case Colin tries to screw me. I'll expose him.
 * Colin Andrews
 * 31 years old
 * lives in Suffolk, UK
 * drives a Kia Sportage
 * buys and sells valid company credentials to hackers
 * phishing attacks, malware distribution

 * (still got his email addresses, domains, mobile no. and BTC wallet address on my personal PC)
 */
```

1.What is the name of the file where the evidence was found? (filename and extension)

bootstrap.min.abc

2.What is the name of the directory your in where this evidence was found?

/css/

3.What piece of evidence have you found?(Multiple Choice)

Colin information