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.

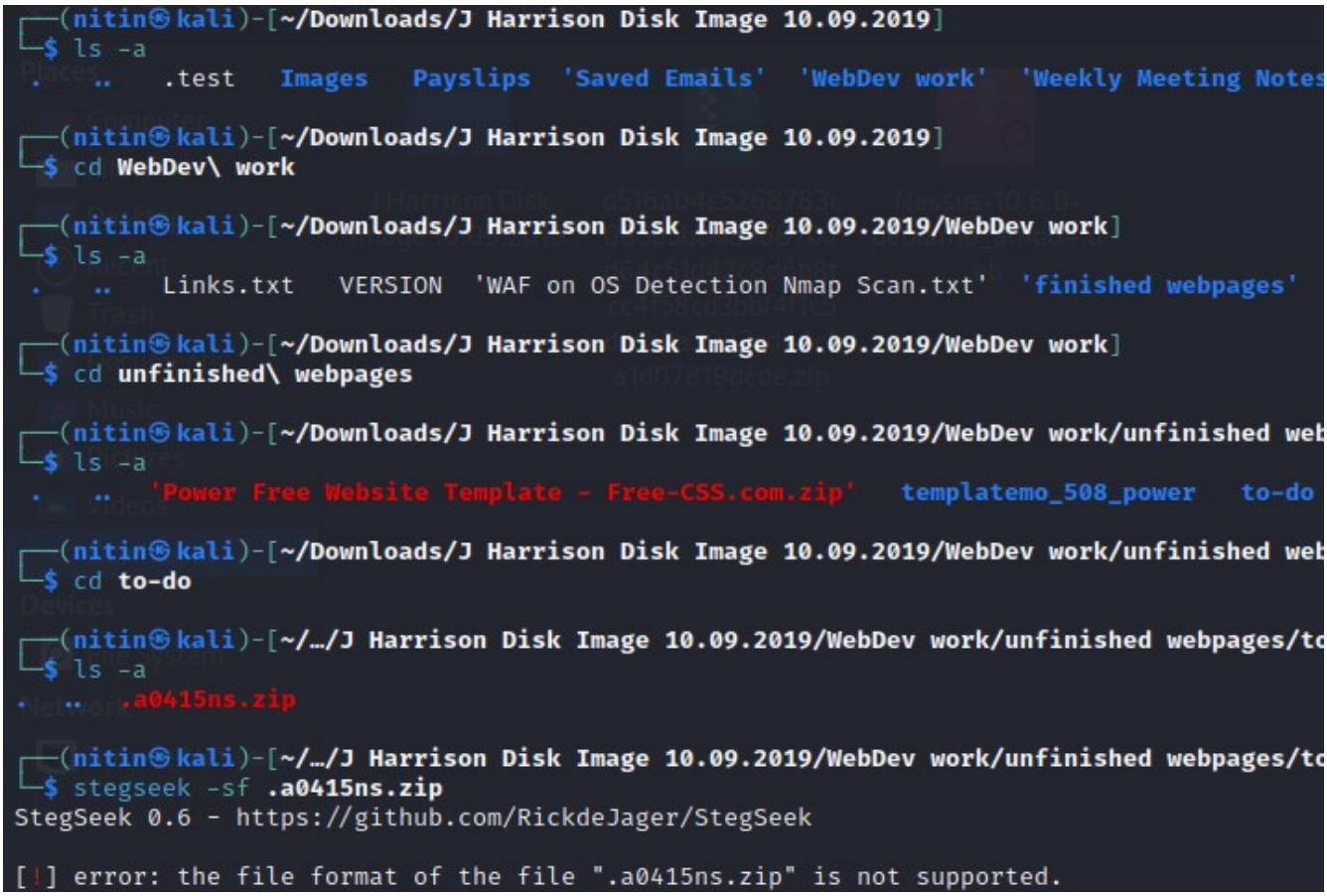
8.What does HTCIA stand for in regard to Digital Forensics?
High Technology Crime Investigation Association

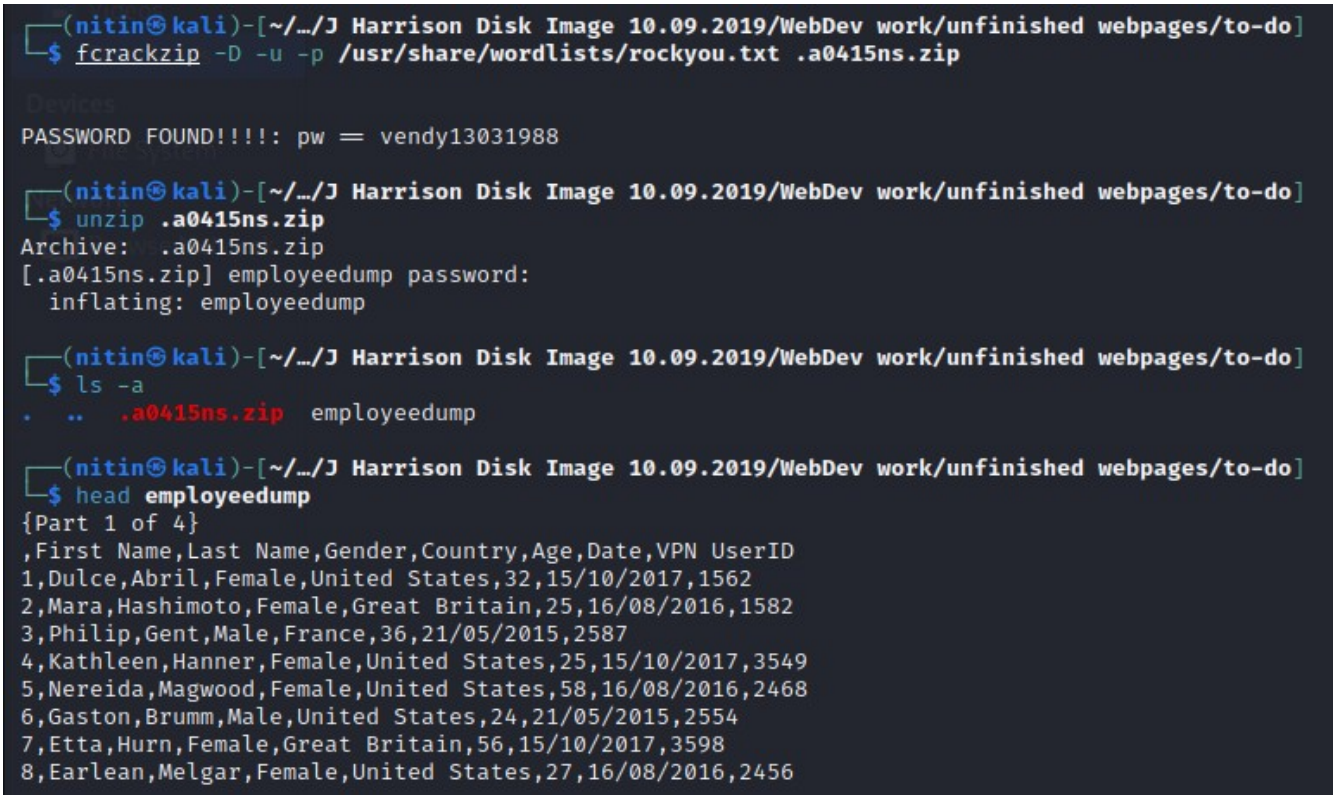
9.Computer Forensics and Data Recovery are the same thing, true or false?
False

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.





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

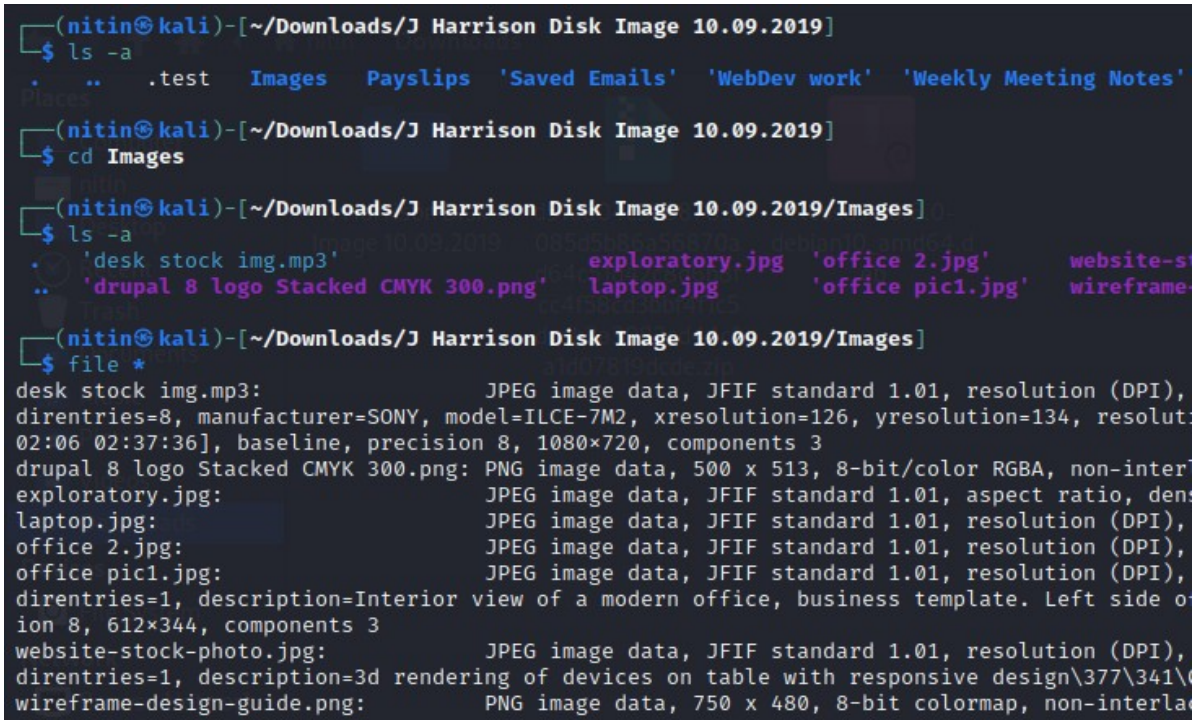
2.What is the name of the directory your in where this evidence was found?

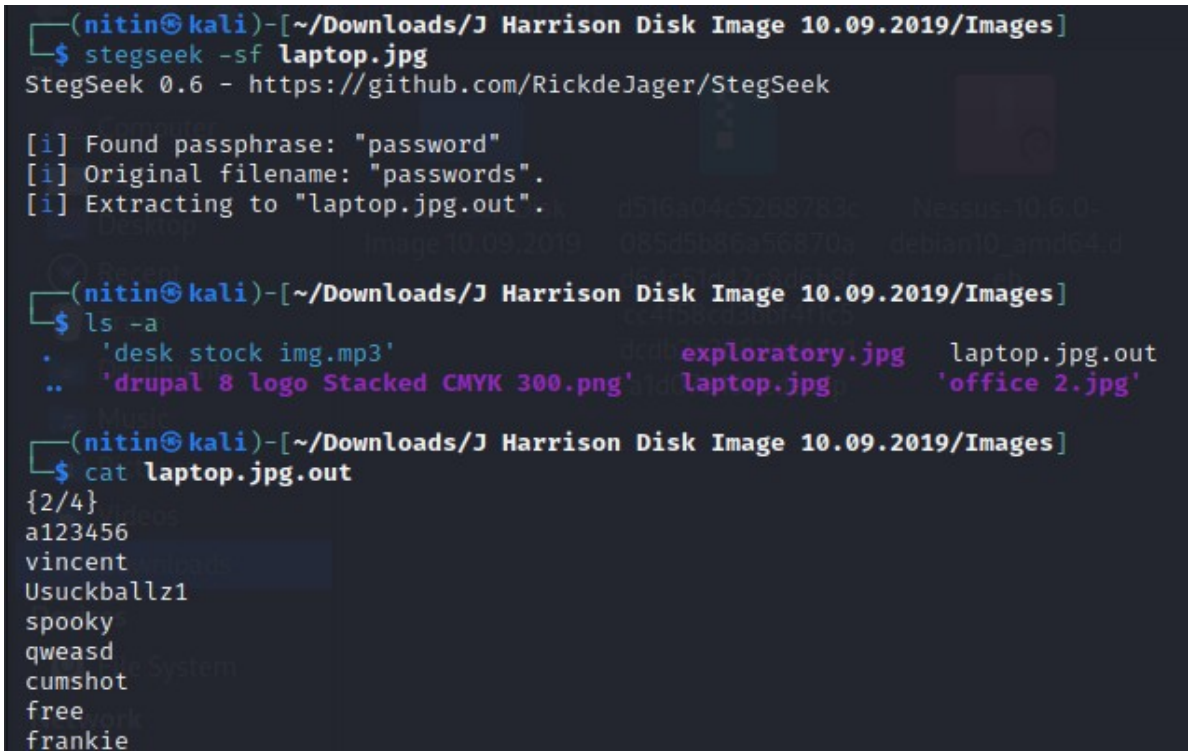
/to-do/

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)





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/

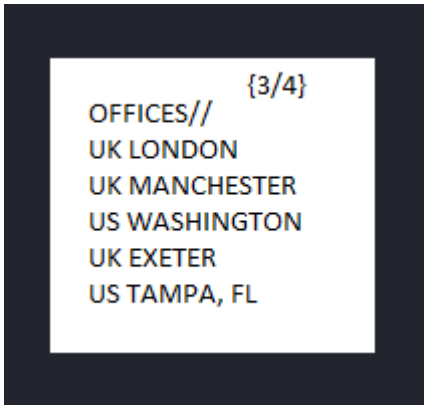
3.What piece of evidence have you found?*(Multiple Choice)*

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.
```



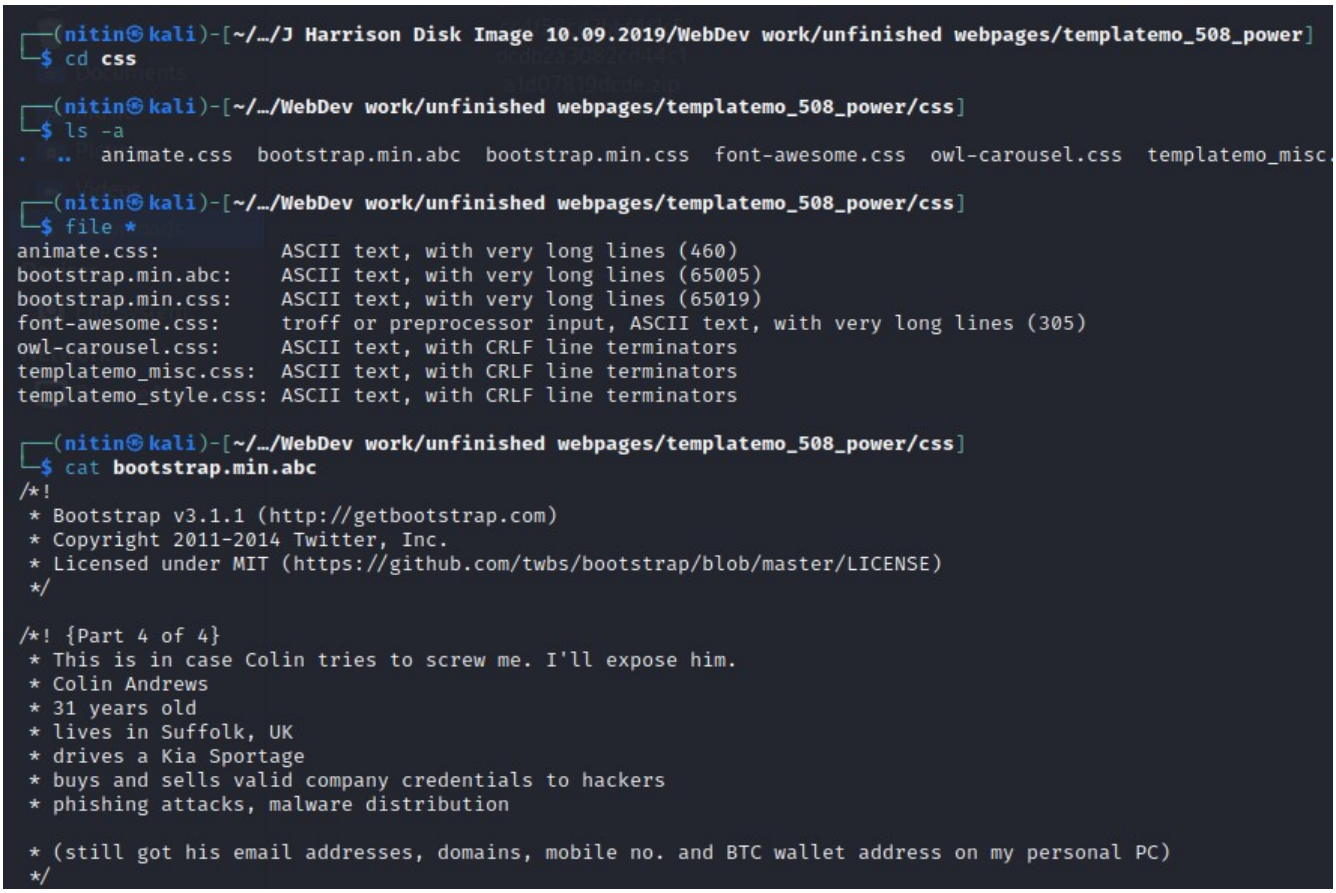
1.What is the name of the file where the evidence was found? (filename and extension) posidon.xml

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”.



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