Deleting Files Report

A Basic Report

1. Fill in the following table using the overview tab of FTK after you import your device.

Area	Number of files found You do not need to put a 0 in areas with no files
File Category (Total)	3793
Archives	2
Databases	1
Documents	986
Email	0
Executable	37
Folders	283
Graphics	1349
Internet / Chat Files	0
Mobile Phone Data	0
Multimedia	126
PS / File System Files	2
Other Encryption Files	0
Other Known Types	249
Presentations	10
Slack / Free Space	386
Spreadsheets	4
Unknown Types	358
User Types	0

2. About what percentage would you say are 0's when using the Hex editor to view the entire drive?

About 5%

Normal Delete

3. How long did it take to delete the files on your device?

Like a Second

4. Fill in the following table using the overview tab of FTK after you import your device.

Area	Number of files found You do not need to put a 0 in areas with no files

File Category (Total)	4618
Archives	2
Databases	1
Documents	852
Email	0
Executable	0
Folders	185
Graphics	2928
Internet / Chat Files	0
Mobile Phone Data	0
Multimedia	21
PS / File System Files	2
Other Encryption Files	0
Other Known Types	263
Presentations	12
Slack / Free Space	148
Spreadsheets	6
Unknown Types	198
User Types	0

5. About what percentage would you say are 0's when using the Hex editor to view the entire drive?

About 5%

6. What are your thoughts about someone quickly erasing a USB device using this method to make files unrecoverable?

I think that if you quickly erase data then it makes it extremely easy to recover, expressly if from the recycling bin

Quick formatting a drive

7. How long did it take to Quick Format your device and how does this compare to a Normal Delete?

About 5 minutes

8. Fill in the following table using the overview tab of FTK after you import your device.

Area	Number of files found You do not need to put a 0 in areas with no files
File Category (Total)	

Archives	73
Databases	0
Documents	6
Email	0
Executable	0
Folders	9
Graphics	0
Internet / Chat Files	0
Mobile Phone Data	0
Multimedia	0
PS / File System Files	2
Other Encryption Files	0
Other Known Types	0
Presentations	0
Slack / Free Space	40
Spreadsheets	0
Unknown Types	16
User Types	0

9. Are there more or less files found now that both deleting and formatting have happened to the device and is this to be expected?

Less files where found, yes I did expect FTK to find less than not deleting, and deleting files.

10. About what percentage would you say are 0's when using the Hex editor to view the entire drive?

About 85%

11. What are your thoughts about someone formatting a USB device to make files unrecoverable.

Some files are going

Full formatting a drive

12. Do you expect that a full formatting will make the files unrecoverable?

I think that some files will still be there, but most of them will be gone and unrecoverable.

Eraser

13. How long did it take to perform a Department of Defense wipe on your device and how does this compare to a Normal Delete and a Quick Format?

15-20 minutes

14. Fill in the following table using the overview tab of FTK after you import your device.

Area	Number of files found You do not need to put a 0 in areas with no files
File Category (Total)	337
Archives	5
Databases	0
Documents	25
Email	0
Executable	0
Folders	19
Graphics	0
Internet / Chat Files	0
Mobile Phone Data	0
Multimedia	0
PS / File System Files	2
Other Encryption Files	0
Other Known Types	0
Presentations	0
Slack / Free Space	133
Spreadsheets	0
Unknown Types	153
User Types	0

15. Are there more or less files found now that deleting, formatting, and a Department of Defense wipe have happened to the device and is this to be expected?

More than formatting and less than deleting. I would expect it would be harder to find stuff on the flash drive.

16. About what percentage would you say are 0's when using the Hex editor to view the entire drive?

Like 5%

17. What are your thoughts about a Department of Defense wipe on a USB device to make files unrecoverable.

Not good enough, no I think that 7 wipes are plenty. I don't think you need quite so many.

18. Eraser can perform a Gutmann wipe with 35 passes. If you had a file that no one else should ever see would you trust a 3 pass wipe or a 35 pass Gutmann or would you smash the device with a hammer after performing both wipes?

The only way to do it! Haha no I think that 35 passes are for the really paranoid.

Final thoughts on deleting files

19. Do you think that a normal person would go to the trouble of using a program like Eraser to delete files they no longer want?

A normal non-educated person yes, most would probably leave crap in the recycle bin.

20. What are the chances of recovering files from a drive if the person does not know you are coming to collect their computer?

Pretty high unless the person is paranoid.

21. What have you learned from this assignment about using a usb or hard drive that contains files from a previous case for a current case?

Don't put my naked photographs on my computer/usb drive or do. Take notes, use a copy, you can recover stuff even after you have deleted it, you are not always guaranteed that your information is gone.