DIGITAL EVIDENCE - THE GATHERING STORM

REID WITTLIFF
1209 NUECES ST.
AUSTIN, TEXAS 78701

(512) 960-4866

REID@WITTLIFFCUTTER.COM

WITTLIFF | CUTTER PLLC

R3 Digital Forensics www.r3forensics.com

1

DIGITAL FORENSICS – PROLIFERATION OF DIGITAL EVIDENCE

- Recover "deleted" files
- Get Stuff user never "saved"
  - Swap file or Page file
  - Hiberfil.sys
  - Temporary Internet Files
- Help you understand what occurred on the device
  - Registry files
  - Link Files
  - JumpList
  - USBStor
  - Windows Timeline
  - SQLite Database examination
- IOT
  - Watches, Alexa, Car Devices and on and on
- Extract Data from Mobile Devices
  - Tablets
  - Smart Phones
- Capture Web Based Data
  - Gmail
  - Dropbox, Box etc.
- Collect Social Media Data
  - Facebook
  - Instagram
  - Twitter
  - Etc.

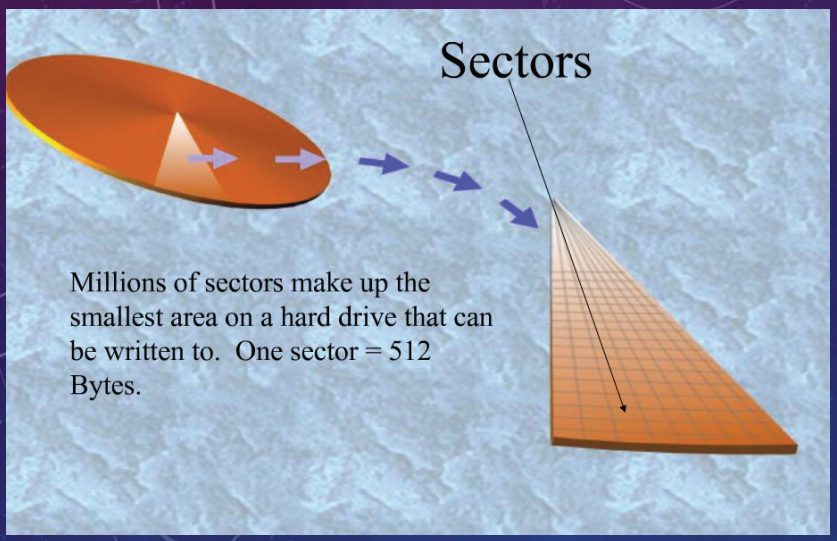
2

“It May Be Recoverable”

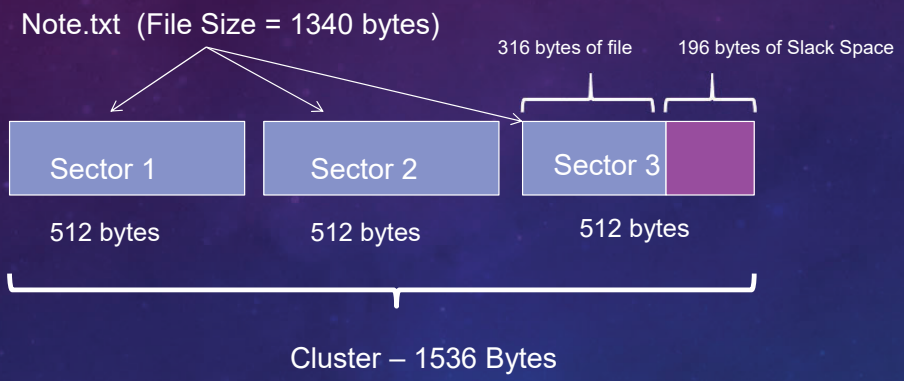
- “01010010” “00110011”
- Stored as a series of magnetic charges on disk platters and external media.

R3 Digital Forensics

A “Sector” is

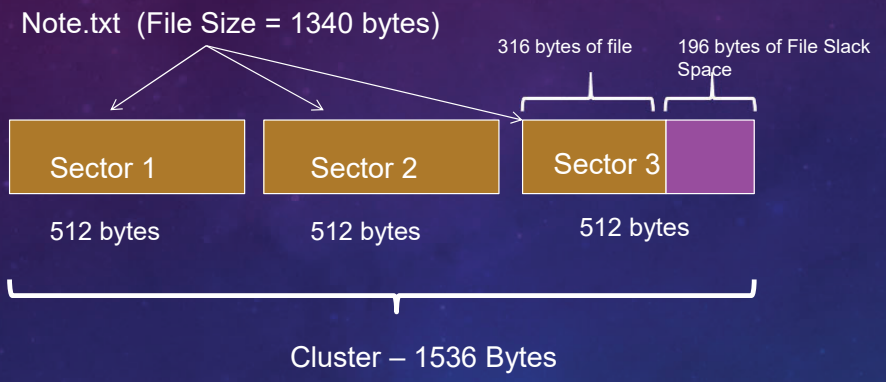


WHY DELETED FILES MAY BE RECOVERABLE



5

NOTE.TXT IS DELETED BY THE USER



The data is still there in the exact same place. The File System just marks the location of Note.txt as available or Unallocated Space

6

Title search: Digital Evidence: The Gathering Storm

First appeared as part of the conference materials for the
33rd Annual Technology Law Conference session
"Digital Evidence: The Gathering Storm"