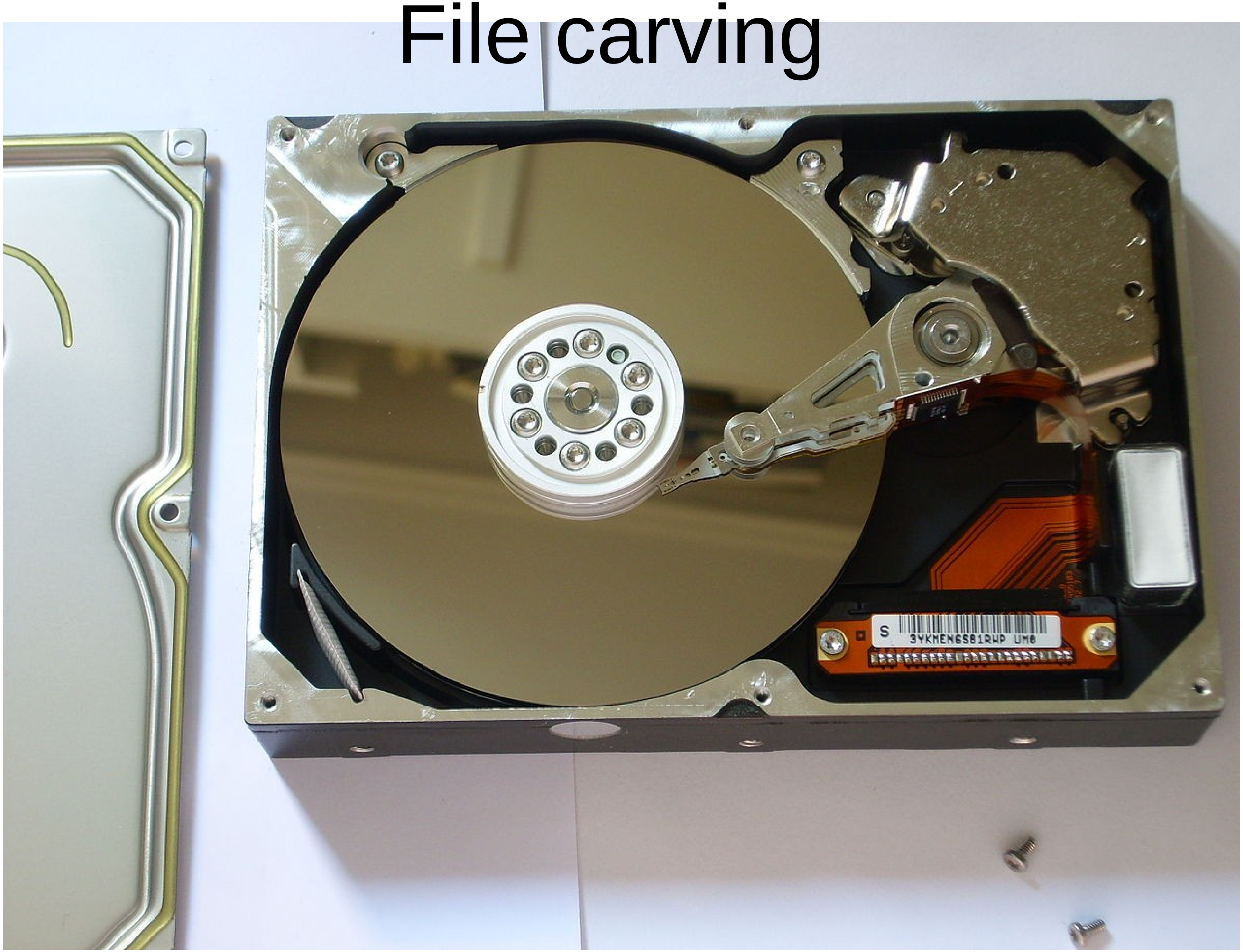
Digital forensics and malware

Digital forensics

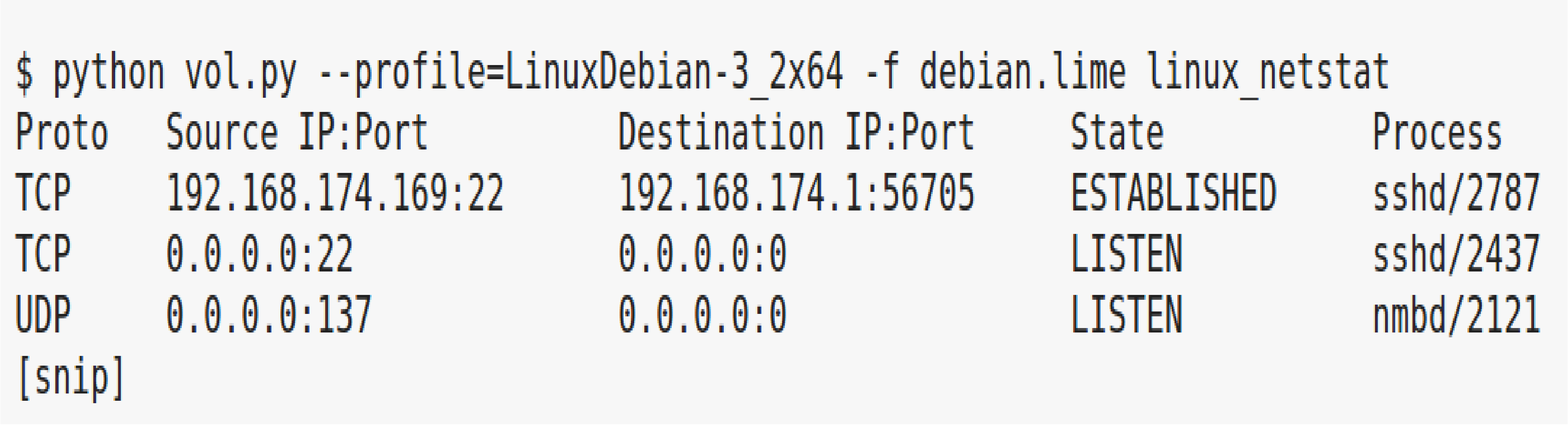
- According to Wikipedia, you could be looking for: attribution, alibis and statements, intent, evaluation of source, document authentication
- File carving (*e.g.*, bifragment gap carving)
  - Electron microscopes
- Memory forensics (Volatility)
- Network forensics (PCAPs, NetFlow records, NIDS logs)
- Database forensics
- Timestamps in document or log file analysis
- Steganography
- Digital forensic processes
- Benford's law

File carving



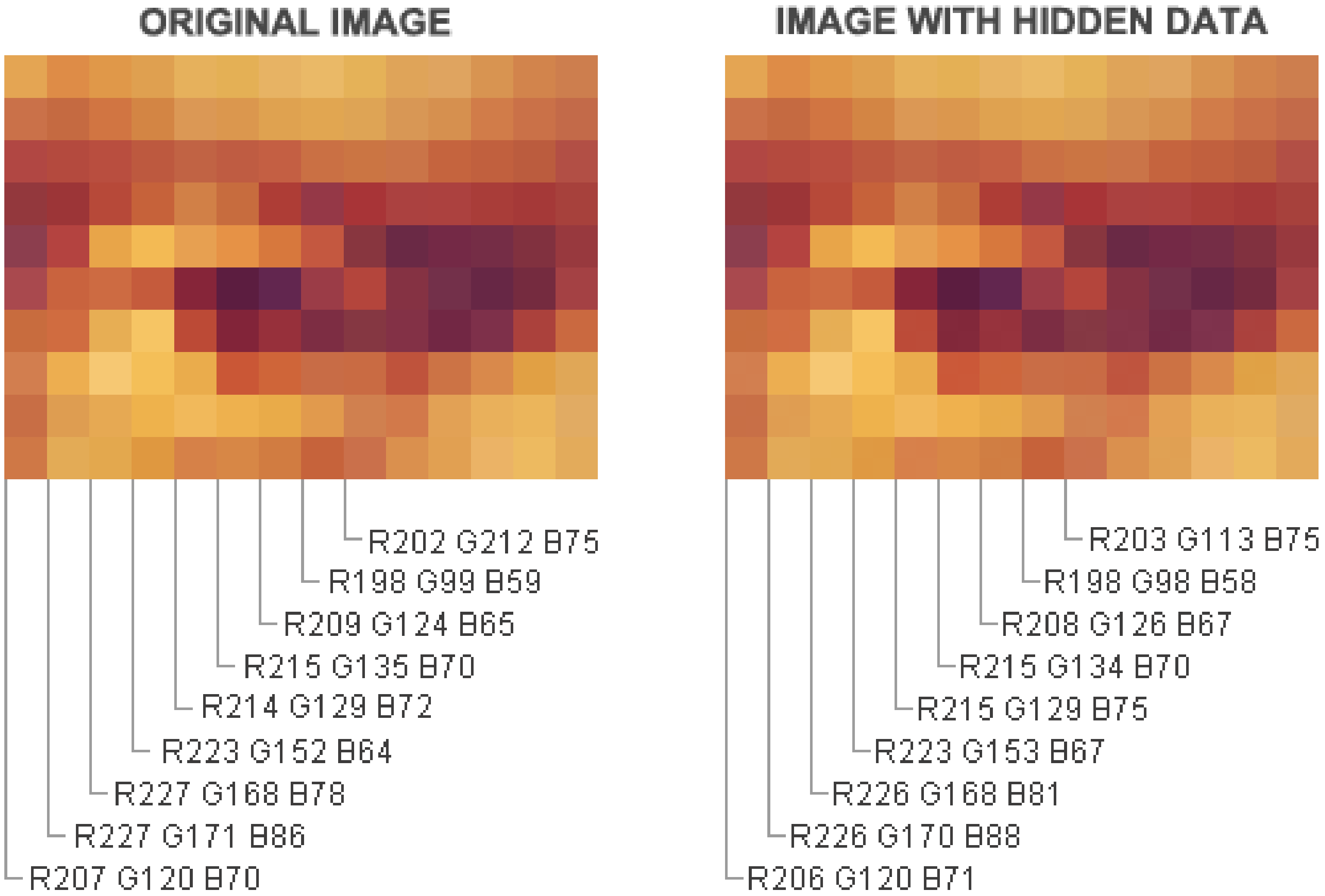
Alessio Sbarbaro User_talk:Yoggysot - Own work

Memory forensics



```
$ python vol.py --profile=LinuxDebian-3_2x64 -f debian.lime linux_netstat
Proto   Source IP:Port          Destination IP:Port     State           Process
TCP     192.168.174.169:22      192.168.174.1:56705     ESTABLISHED     sshd/2787
TCP     0.0.0.0:22              0.0.0.0:0               LISTEN          sshd/2437
UDP     0.0.0.0:137             0.0.0.0:0               LISTEN          nmbd/2121
[snip]
```

Steganography



From https://www.tech2hack.com/steganography-hide-data-in-audio-video-image-files/

Forensics tools

- File carvers
  - *E.g.*, Scalpel and foremost
- Log parsers
- Parsers/viewers for different kinds of files
  - SQLite, EXIF, *etc.*
- Linux commands that might be useful:
  - file, exif, sqlite3, losetup, mount, dd, ssdeep, grep, strings

Malware

- *Cryptovirology* by Young and Yung
- *The Art of Computer Virus Research and Defense* by Szor
  - Common theme since the turn of the millennium: stay in memory and don't go out to disk
- Elk Cloner in 1981 (Skrenta)
- “Virus” coined by Cohen in 1983 (“Information only has meaning in that it is subject to interpretation”)
  - https://web.eecs.umich.edu/~aprakash/eecs588/handouts/cohen-viruses.html
- “Worm” came from John Brunner's *The Shockwave Rider* in 1975
  - Creeper in 1971 for TENEX systems
  - ANIMAL in 1975
  - Morris Worm in 1988
  - Code Red in 2001

Interesting types of malware

- Macroviruses
  - “On error resume next”
- Botnets
  - Command and Control (C&C), from IRC and hierarchical to fastflux and beyond
- Targeted threats
  - E.g., Tibetan exile community, Syria/Egypt, Mexico
  - Google “Citizen Lab” or watch “Black Code”

Malware analysis

- Static *vs.* dynamic
- IDA Pro, Ollydbg, etc.
- Cuckoo Sandbox
- Decompilation
- Armoring, packing, *etc.*

Anomaly detection

- A Sense of Self for Unix Processes (Forrest *et al.* in 1996)

Resources

- *Practical Malware Analysis* by Honig and Sikorski
- http://www.forensicswiki.org/wiki/Tools

Conferences you should check out

- IEEE Symposium on Security and Privacy (Oakland)
- USENIX Security Symposium
  - Also check out the workshops like FOCI and WOOT
- ACM Conference on Computer and Communications Security (CCS)
- Network and Distributed System Security Symposium (NDSS)
- Privacy-Enhancing Technologies Symposium (PETS)
  - Also PoPETS
- Also RAID for intrusion detection, DFRWS for forensics, CSF for policy and theory, Eurocrypt and Crypto, Blackhat, DEFCON, phrack, 2600 magazine, WPES and WEIS