Done by: Assylbek Bugybay, Alperen Sarac

1. File carving is a technique used in computer forensics to extract a formatted file or data from a disk drive or other storage device without the assistance of the filesystem that originally created the file.

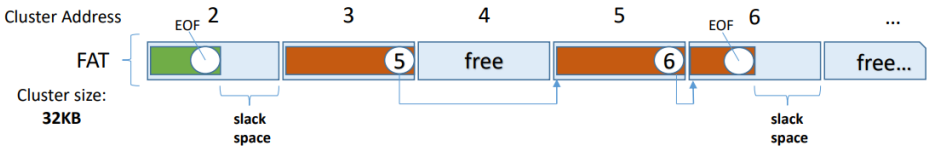
IT is used in: Criminal Investigations, Counter Intelligence (Business/Military), Simple Data Recovery

Criminal Investigations- File Carving is used to gather information, that can later be used as evidence in court and/or to find the perpetrator

Counter Intelligence (Business/Military)- In a military context for e.g. drones, computers and captured intel in general. Also internal investigations (e.g. KSK, racism scandal german police, etc.). In a business context to find out, how hackers infiltrated the systems, how employees stole data etc.

Meta data as- creation date, last modification date, location-GPS co-ordinates contained in image files such as *.jpeg, author, title can give more information.

2. The most widely used file system for removable media is the FAT file system. Each file has a FAT Directory Entry that lists the file name, starting cluster and length. Another location for metadata is the File Allocation Table (FAT) that maintains 3 pieces of information, Address, cluster allocation status and which clusters a given file occupies.



Directory entries:

[imba.txt | starting cluster: 3 | 80KB | metadata]

Logical size = 80KB
Physic. size = 96KB → 16KB of **slack space**!

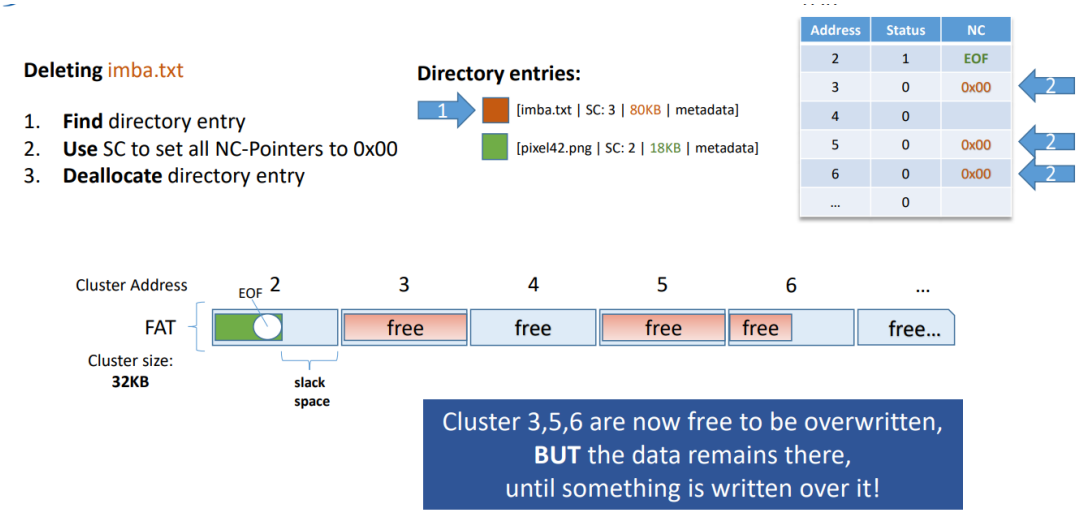
[pixel42.png | starting cluster: 2 | 18KB | metadata]

Logical size = 18KB
Physic. size = 32KB → 14KB of **slack space**!

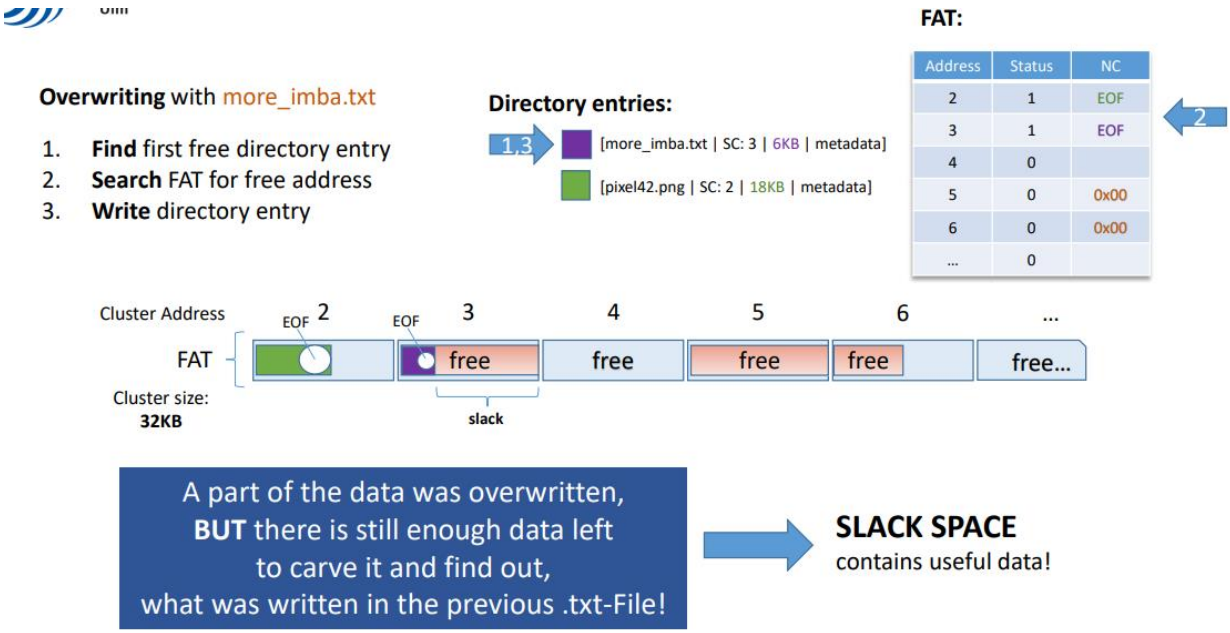
FAT:

Address	Status	Next Cl.
2	1	EOF
3	1	5
4	0	
5	1	6
6	1	EOF
...	0	

a) File was deleted:



Clusters can be overwritten but still contains data until new data is written on them. This existing data can be carved by a tool such as Disk Digger or Recuva.



"Slack" contains data further to be carved.

b) File system was re-formatted (quick formatting):

Performing a quick format simply clears the digital storage media's partition table, which allows for new data to be written without impediment.

When reformatted, the size of the new File allocation table stays the same as the previous file allocation table, unless changed manually. The new file system will irreversibly wipe all the old data and linking them with disk sectors that actually store data. T**herefore, the actual data still remains on the disk, and can be recovered using tools.**

Usually restored data contains metadata.

4. There are numerous applications that can securely wipe information from hard drives. Special algorithms are developed that fill disk space previously occupied by sensitive

information with cryptographically strong random data. If one of such applications has been used, data carving is impossible.

5.

1) What's the name of the Captain? Is the being intelligent (yes/no) and why?

Jean Luc Pickard. Yes, he is intelligent because it was trying to communicate

Extracted Audio file from file "WAV file at sector 24833" by the use of Disk Digger

2) After an Xtensive search, you need to find out which key has a creation date. Name the creation date and the corresponding key!

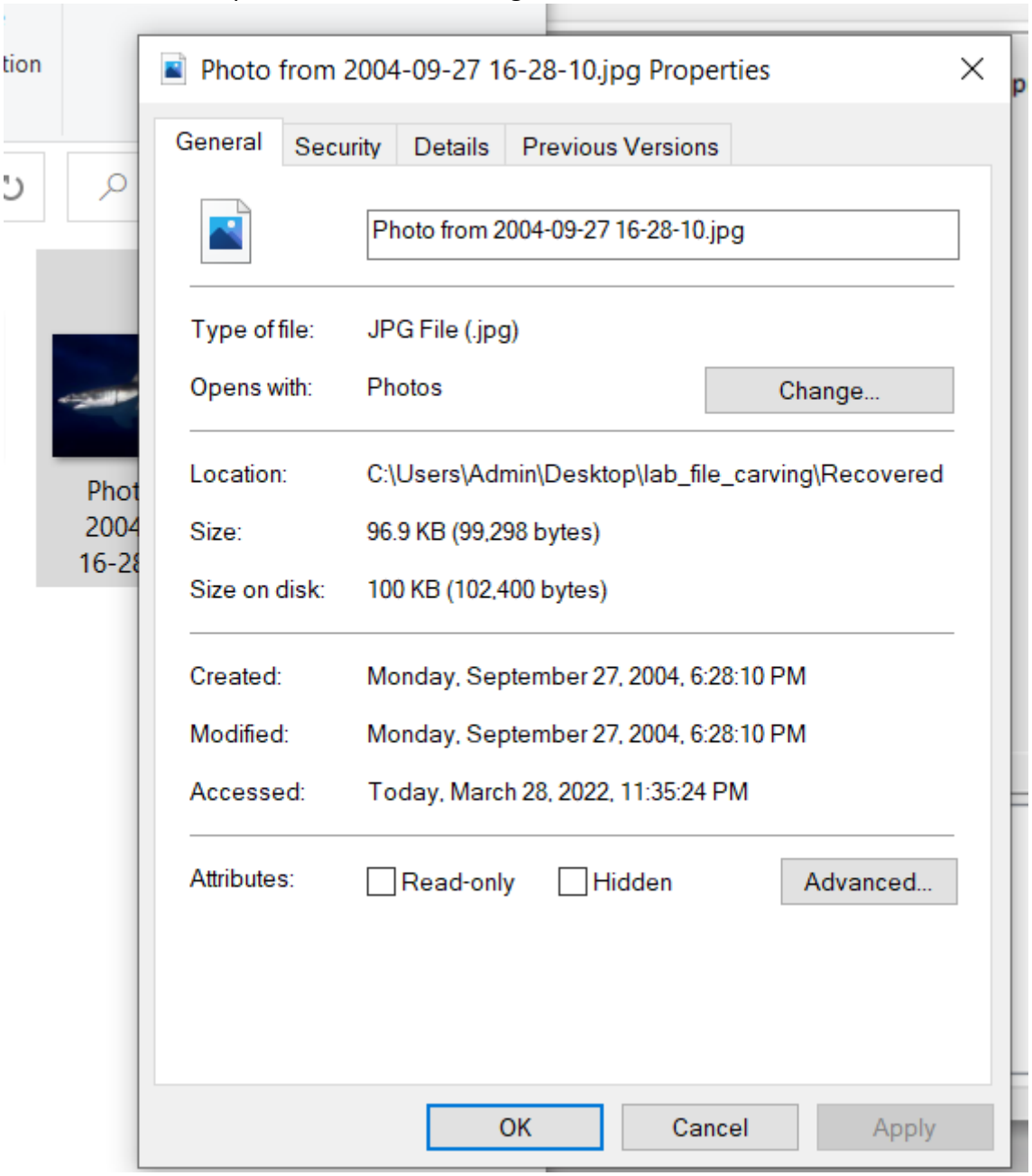
Name: 0B39027F-A1D1-4761-84DF-C6716E256A3D , Date: 2018-03-14T16:07:53Z

Method: found in "XML file at sector 4737"

3) Someone shot the shark! What type of Canon did he use?

Type: Canon EOS 20D

Method: in the Properties of the shark image



4) There is a famous broom hidden inside of all this mess and he has a message for us! What font did she use to type this message? What's the message? Was it all a test?

Font: Times new Roman but there was mention of other fonts like Nimbus Roman No 9, HG Mincho Light, MS Gothic and Starsymbol

Message: I am a Pretty girl, yes it was a test

Method: opening PPT "PPT file at sector 21633"

5) Someone is riding on something, what a cool video! What's his name and on what is he riding?

Answer: His name is Joe, He is riding a Surfboard

Method: Information found from a video file

6) How many observations were necessary to proof, that he excels at it?

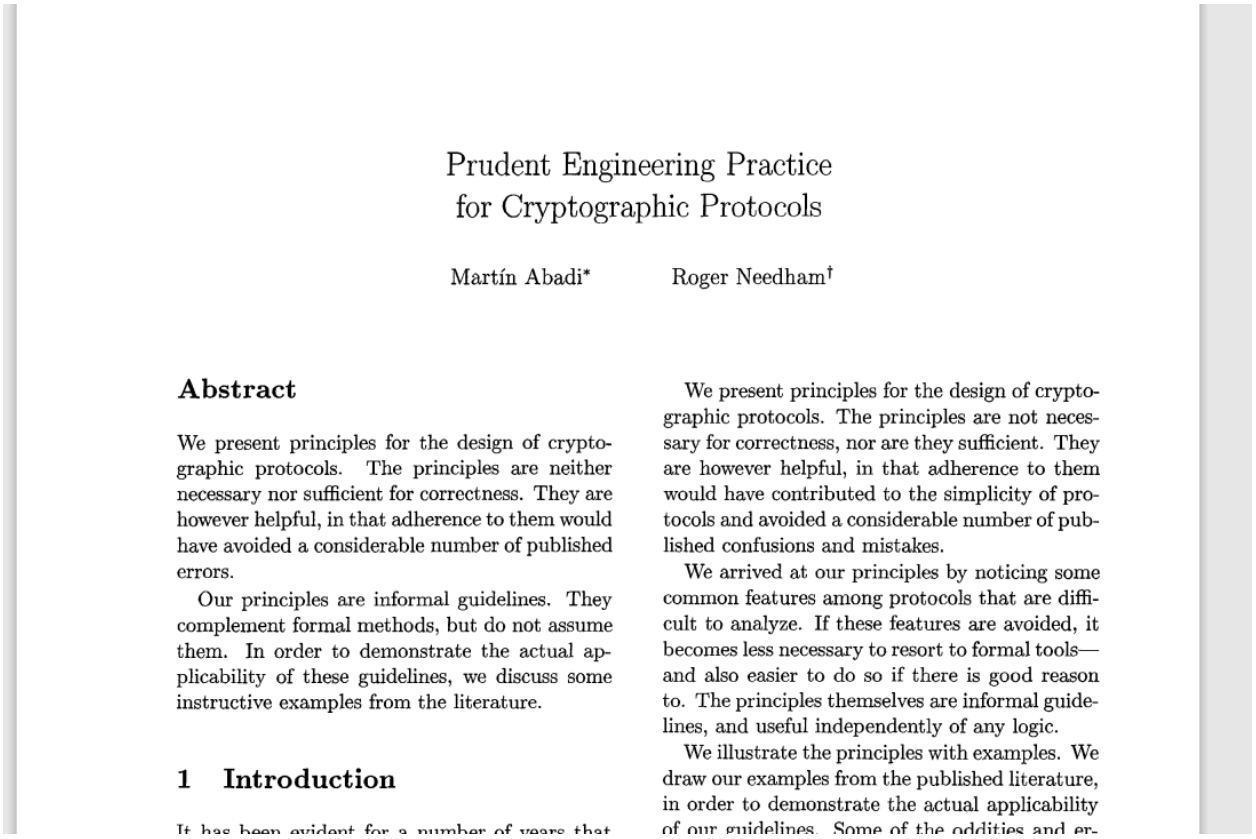
Answer: 10 Method: From ‘excels being written in the question, I opened the .xls file named “XLS file at sector 25473”

7) There’s science in there! What’s the title and who wrote it (2 scientists)?

Answer: Prudent Engineering Practice for Cryptographic Protocols;

Authors: Martin Abadi, Roger Nee

Method: PDF extracted by Recuvo



Prudent Engineering Practice
for Cryptographic Protocols

Martín Abadi* Roger Needham†

Abstract

We present principles for the design of cryptographic protocols. The principles are neither necessary nor sufficient for correctness. They are however helpful, in that adherence to them would have avoided a considerable number of published errors.

Our principles are informal guidelines. They complement formal methods, but do not assume them. In order to demonstrate the actual applicability of these guidelines, we discuss some instructive examples from the literature.

We present principles for the design of cryptographic protocols. The principles are not necessary for correctness, nor are they sufficient. They are however helpful, in that adherence to them would have contributed to the simplicity of protocols and avoided a considerable number of published confusions and mistakes.

We arrived at our principles by noticing some common features among protocols that are difficult to analyze. If these features are avoided, it becomes less necessary to resort to formal tools—and also easier to do so if there is good reason to. The principles themselves are informal guidelines, and useful independently of any logic.

We illustrate the principles with examples. We draw our examples from the published literature, in order to demonstrate the actual applicability of our guidelines. Some of the oddities and er-

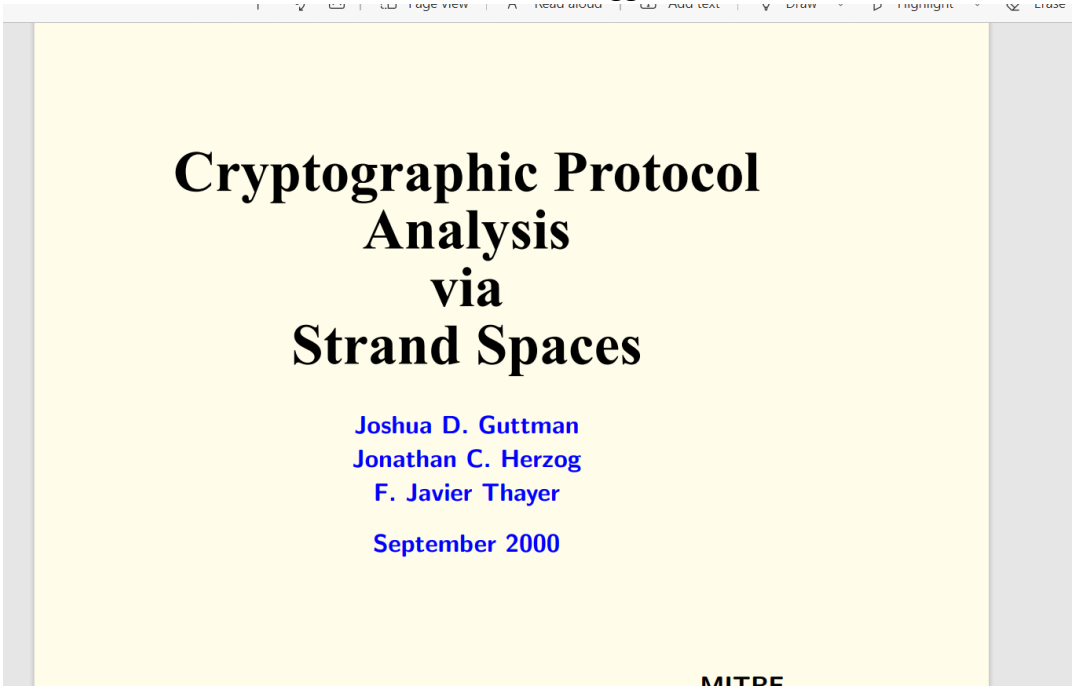
1 Introduction

It has been evident for a number of years that

8) More science! What's the first name of this good man and the rest of his fellow scientists (3 scientists)?

Answer: Joshua D.Guttman, Jonathan C.Herzog, F.Javier Thayer

Method: PDF file extracted with Disk Digger



Cryptographic Protocol Analysis via Strand Spaces

Joshua D. Guttman
Jonathan C. Herzog
F. Javier Thayer

September 2000

MITRE

7. Lab showed that a lot of information can be restored. Disk Digger and Recuva are realy easy and very similar tools to get the data. Recuvo provides more adjustments while restoring the data. But disc digger provides more discriptions to restored data. The queality of the data can be lost. We have also learnt why data can be restored and what are the restrictions for that. Mainly the data can be restored because of the way the data is deleted and stored in the disc. Recuvo exctracts data in a file, while DiskDigger separates them by a file type.