Universidad Carlos III de Madrid

Reporte de Data carving - Floppy Disk

Juan Diego Llano Miraval

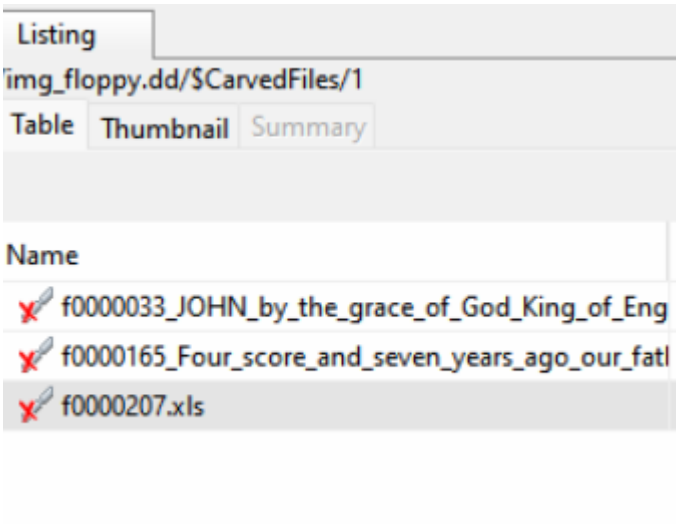
Fecha: 18/05/2024

Procedure

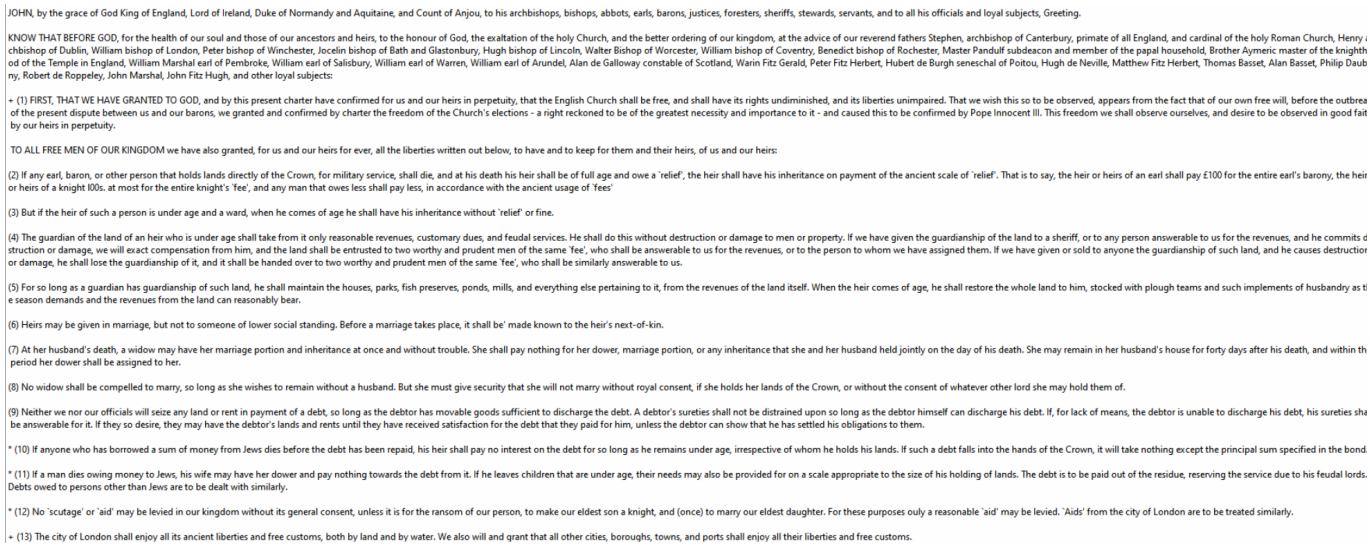
The first step was checking the sha256:

```
root@z:/home/zud/Desktop/floppy# sha256sum floppy.dd
15fab9d7c0993b02ca720b7e6d014b584874553fbacf6bca457f8b85fa89a940  floppy.dd
```

it is correct to say this is the same as the provided, so we mount the disk into autopsy, and got 3:



I also found another document but it was a copy of the second document in the image. From this we can see 2 documents of text, and 1 microsoft excel file. When we checked the first file:



JOHN, by the grace of God King of England, Lord of Ireland, Duke of Normandy and Aquitaine, and Count of Anjou, to his archbishops, bishops, abbots, earls, barons, justices, foresters, sheriffs, stewards, servants, and to all his officials and loyal subjects, Greeting.

KNOW THAT BEFORE GOD, for the health of our soul and those of our ancestors and heirs, to the honour of God, the exaltation of the holy Church, and the better ordering of our kingdom, at the advice of our reverend fathers Stephen, archbishop of Canterbury, primate of all England, and cardinal of the holy Roman Church, Henry chbishop of Dublin, William bishop of London, Peter bishop of Winchester, Jocelin bishop of Bath and Glastonbury, Hugh bishop of Lincoln, Walter Bishop of Worcester, William bishop of Coventry, Benedict bishop of Rochester, Master Pandulf subdeacon and member of the papal household, Brother Aymeric master of the knighth od of the Temple in England, William Marshal earl of Pembroke, William earl of Salisbury, William earl of Warren, William earl of Arundel, Alan de Galloway constable of Scotland, Warin Fitz Gerald, Peter Fitz Herbert, Hubert de Burgh seneschal of Poitou, Hugh de Neville, Matthew Fitz Herbert, Thomas Basset, Alan Basset, Philip Daub ny, Robert de Roppeley, John Marshal, John Fitz Hugh, and other loyal subjects:

+ (1) FIRST, THAT WE HAVE GRANTED TO GOD, and by this present charter have confirmed for us and our heirs in perpetuity, that the English Church shall be free, and shall have its rights undiminished, and its liberties unimpaired. That we wish this so to be observed, appears from the fact that of our own free will, before the outbrea of the present dispute between us and our barons, we granted and confirmed by charter the freedom of the Church's elections - a right reckoned to be of the greatest necessity and importance to it - and caused this to be confirmed by Pope Innocent III. This freedom we shall observe ourselves, and desire to be observed in good fait by our heirs in perpetuity.

TO ALL FREE MEN OF OUR KINGDOM we have also granted, for us and our heirs for ever, all the liberties written out below, to have and to keep for them and their heirs, of us and our heirs:

(2) If any earl, baron, or other person that holds lands directly of the Crown, for military service, shall die, and at his death his heir shall be of full age and owe a `relief', the heir shall have his inheritance on payment of the ancient scale of `relief'. That is to say, the heir or heirs of an earl shall pay £100 for the entire earl's barony, the heir or heirs of a knight l00s. at most for the entire knight's `fee', and any man that owes less shall pay less, in accordance with the ancient usage of `fees'

(3) But if the heir of such a person is under age and a ward, when he comes of age he shall have his inheritance without `relief' or fine.

(4) The guardian of the land of an heir who is under age shall take from it only reasonable revenues, customary dues, and feudal services. He shall do this without destruction or damage to men or property. If we have given the guardianship of the land to a sheriff, or to any person answerable to us for the revenues, and he commits d struction or damage, we will exact compensation from him, and the land shall be entrusted to two worthy and prudent men of the same `fee', who shall be answerable to us for the revenues, or to the person to whom we have assigned them. If we have given or sold to anyone the guardianship of such land, and he causes destructio or damage, he shall lose the guardianship of it, and it shall be handed over to two worthy and prudent men of the same `fee', who shall be similarly answerable to us.

(5) For so long as a guardian has guardianship of such land, he shall maintain the houses, parks, fish preserves, ponds, mills, and everything else pertaining to it, from the revenues of the land itself. When the heir comes of age, he shall restore the whole land to him, stocked with plough teams and such implements of husbandry as t e season demands and the revenues from the land can reasonably bear.

(6) Heirs may be given in marriage, but not to someone of lower social standing. Before a marriage takes place, it shall be' made known to the heir's next-of-kin.

(7) At her husband's death, a widow may have her marriage portion and inheritance at once and without trouble. She shall pay nothing for her dower, marriage portion, or any inheritance that she and her husband held jointly on the day of his death. She may remain in her husband's house for forty days after his death, and within th period her dower shall be assigned to her.

(8) No widow shall be compelled to marry, so long as she wishes to remain without a husband. But she must give security that she will not marry without royal consent, if she holds her lands of the Crown, or without the consent of whatever other lord she may hold them of.

(9) Neither we nor our officials will seize any land or rent in payment of a debt, so long as the debtor has movable goods sufficient to discharge the debt. A debtor's sureties shall not be distrained upon so long as the debtor himself can discharge his debt. If, for lack of means, the debtor is unable to discharge his debt, his sureties sha be answerable for it. If they so desire, they may have the debtor's lands and rents until they have received satisfaction for the debt that they paid for him, unless the debtor can show that he has settled his obligations to them.

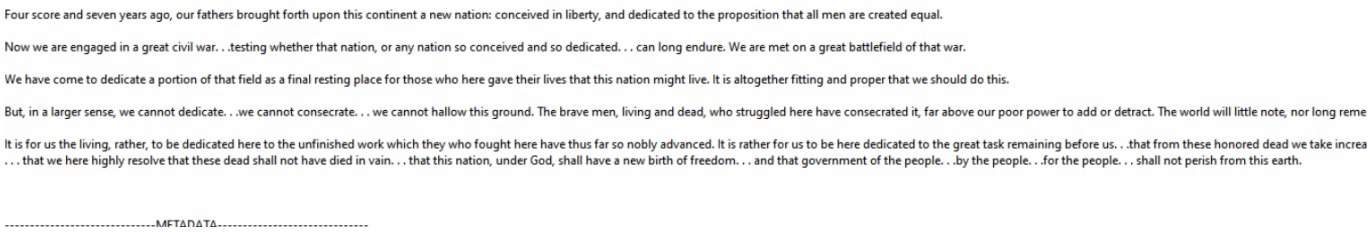
* (10) If anyone who has borrowed a sum of money from Jews dies before the debt has been repaid, his heir shall pay no interest on the debt for so long as he remains under age, irrespective of whom he holds his lands. If such a debt falls into the hands of the Crown, it will take nothing except the principal sum specified in the bond.

* (11) If a man dies owing money to Jews, his wife may have her dower and pay nothing towards the debt from it. If he leaves children that are under age, their needs may also be provided for on a scale appropriate to the size of his holding of lands. The debt is to be paid out of the residue, reserving the service due to his feudal lords. Debts owed to persons other than Jews are to be dealt with similarly.

* (12) No `scutage' or `aid' may be levied in our kingdom without its general consent, unless it is for the ransom of our person, to make our eldest son a knight, and (once) to marry our eldest daughter. For these purposes ouly a reasonable `aid' may be levied. `Aids' from the city of London are to be treated similarly.

+ (13) The city of London shall enjoy all its ancient liberties and free customs, both by land and by water. We also will and grant that all other cities, boroughs, towns, and ports shall enjoy all their liberties and free customs.

it is just text that is not relevant to the case, but in the metadata we can confirm that Emma Crook was the creator of the file, so she might be the owner of the floppy disk. The second file is similar as the first one, there is no relevant information related to the investigation:



Four score and seven years ago, our fathers brought forth upon this continent a new nation: conceived in liberty, and dedicated to the proposition that all men are created equal.

Now we are engaged in a great civil war. . .testing whether that nation, or any nation so conceived and so dedicated. . . can long endure. We are met on a great battlefield of that war.

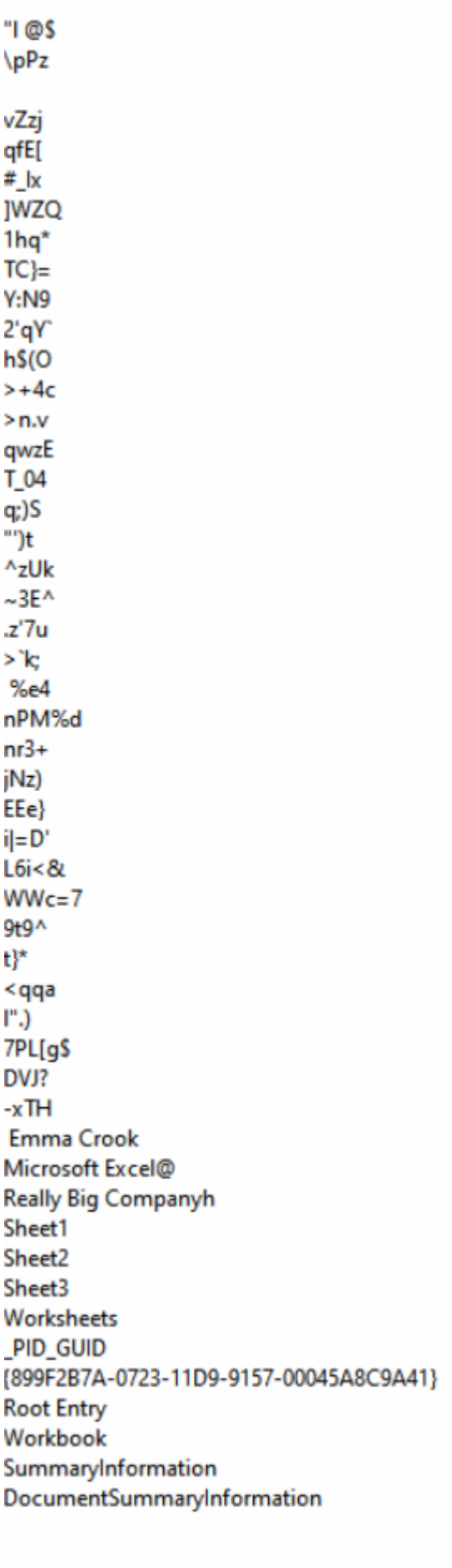
We have come to dedicate a portion of that field as a final resting place for those who here gave their lives that this nation might live. It is altogether fitting and proper that we should do this.

But, in a larger sense, we cannot dedicate. . .we cannot consecrate. . . we cannot hallow this ground. The brave men, living and dead, who struggled here have consecrated it, far above our poor power to add or detract. The world will little note, nor long reme

It is for us the living, rather, to be dedicated here to the unfinished work which they who fought here have thus far so nobly advanced. It is rather for us to be here dedicated to the great task remaining before us. . .that from these honored dead we take increa . . . that we here highly resolve that these dead shall not have died in vain. . . that this nation, under God, shall have a new birth of freedom. . . and that government of the people. . .by the people. . .for the people. . . shall not perish from this earth.

----------METADATA----------

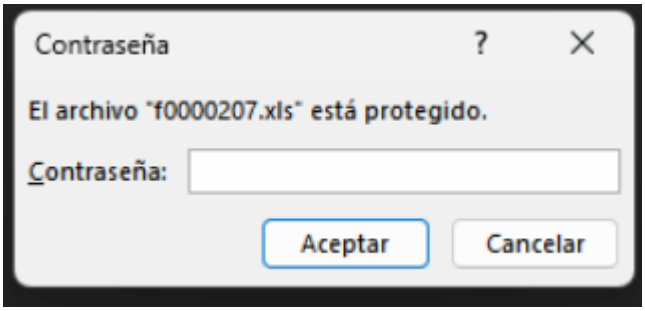
For the third file, it was encrypted:



we exported the .xls for further analysis. We extracted the sha256 from the excel file before proceeding:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sha256sum f0000207.xls
56e1b34930c4742636fd0c327ac0f9926c7acf00ab5fb6723a7a7227ff74c8da  f0000207.xls
```

We confirmed that this is a microsoft excel file and we proceed to open. When we open it requests a password, so it is encrypted:



We took out the hash of the file with the help of john the ripper:

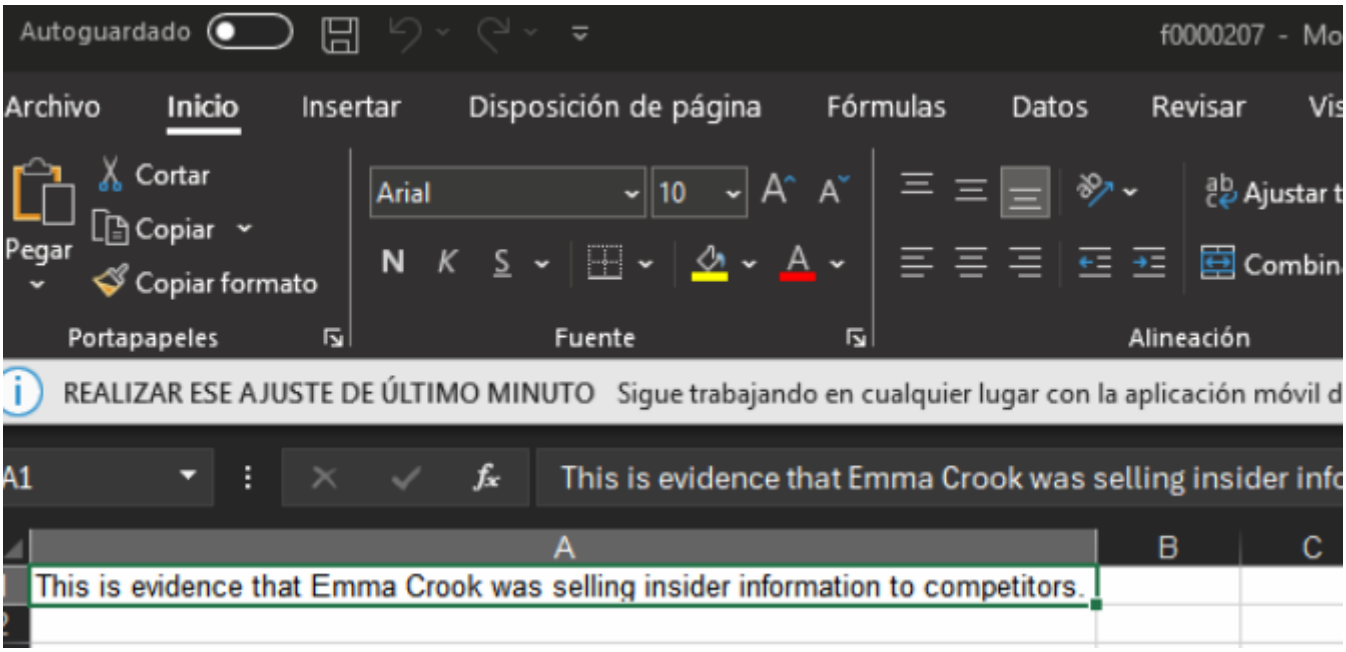
```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# python /usr/share/john/office2john.py f0000207.xls
f0000207.xls:$oldoffice$0*fd8366d381a091ec761dacf4501b79ca*4ab94798dc6cca226c
204024a2829c74*46854c3e0b40d8c236b547756a89e8ad:::::f0000207.xls

┌──(root㉿kali)-[/home/kali/Desktop]
└─# python /usr/share/john/office2john.py f0000207.xls > hash.txt
```

And by running a simple analysis (by accident i was checking the hash was correct) john the ripper got the password from a default password list:

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# john hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (oldoffice, MS Office ⩽ 2003 [MD5/SHA1 RC4 32/64])
Cost 1 (hash type [0-1:MD5+RC4-40 3:SHA1+RC4-40 4:SHA1+RC4-128 5:SHA1+RC4-56]
) is 0 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
crook            (f0000207.xls)
1g 0:00:00:00 DONE 3/3 (2024-05-18 07:00) 1.265g/s 325278p/s 325278c/s 325278
C/s jamum..cez11
Use the "--show --format=oldoffice" options to display all of the cracked pas
swords reliably
Session completed.
```

Another strategy I was planning to use, was an incremental brute force attack. We have finally opened the excel file and got:



This is the evidence requested that Emma Crook was selling information.