Mission Name

Reassembling

Background

Ethan and Claire discuss their confusion and speculate reasons why Atali would want to investigate his own company / order the release of code snippets. Dr Pinche shows the evidence that Atali ordered Jailnor to be killed. This evidence needs to be reassembled to get information.

Technical High-Level Overview

An unknown file is provided to the player. This file is based on Remote Desktop Protocol Cache. This cache contains multiple BMP fragments to order, and finally, get a password. Player must identify this file examining HEX header and name provided.

Short Description

Your goal is to try to get a password related to the camera system.

Mission Description

A camera fragment based on Jailnor murder is provided to you. Your goal is to try to open the provided fragment and get the password inside it.

Location

- RECON CAR - AIR

Tools

- HxD Editor
- https://github.com/ANSSI-FR/bmc-tools
- https://github.com/BSI-Bund/RdpCacheStitcher

Questions

How many files were extracted?

- 390

Which is the main header of the evidence provided?

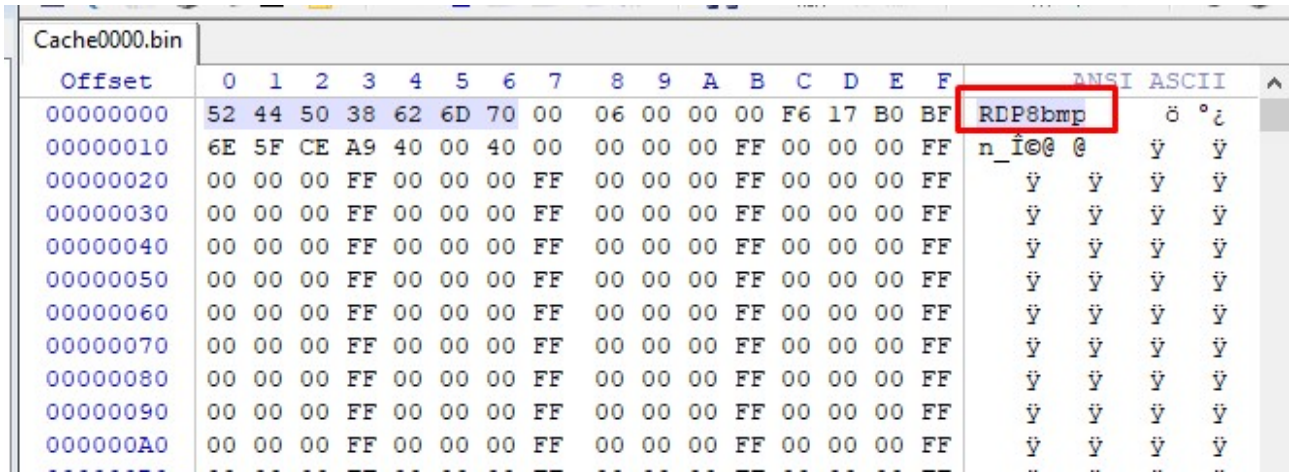
- RDP8BMP

Items

1. Check file´s header.
2. Investigate Remote Desktop Protocol Cache files
3. Use any tool to extract BITMAP cache

Write Up

Player must analyse file header in order to know which type os file has been provided:



Cache0000.bin

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	ANSI ASCII
00000000	52	44	50	38	62	6D	70	00	06	00	00	00	F6	17	B0	BF	RDP8bmp ö °¿
00000010	6E	5F	CE	A9	40	00	40	00	00	00	00	FF	00	00	00	FF	n_Î©@ @ ÿ ÿ
00000020	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000030	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000040	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000050	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000060	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000070	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000080	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
00000090	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ
000000A0	00	00	00	FF	00	00	00	FF	00	00	00	FF	00	00	00	FF	ÿ ÿ ÿ ÿ

Figure 1

Other way to investigate, would be locate the name on Google:

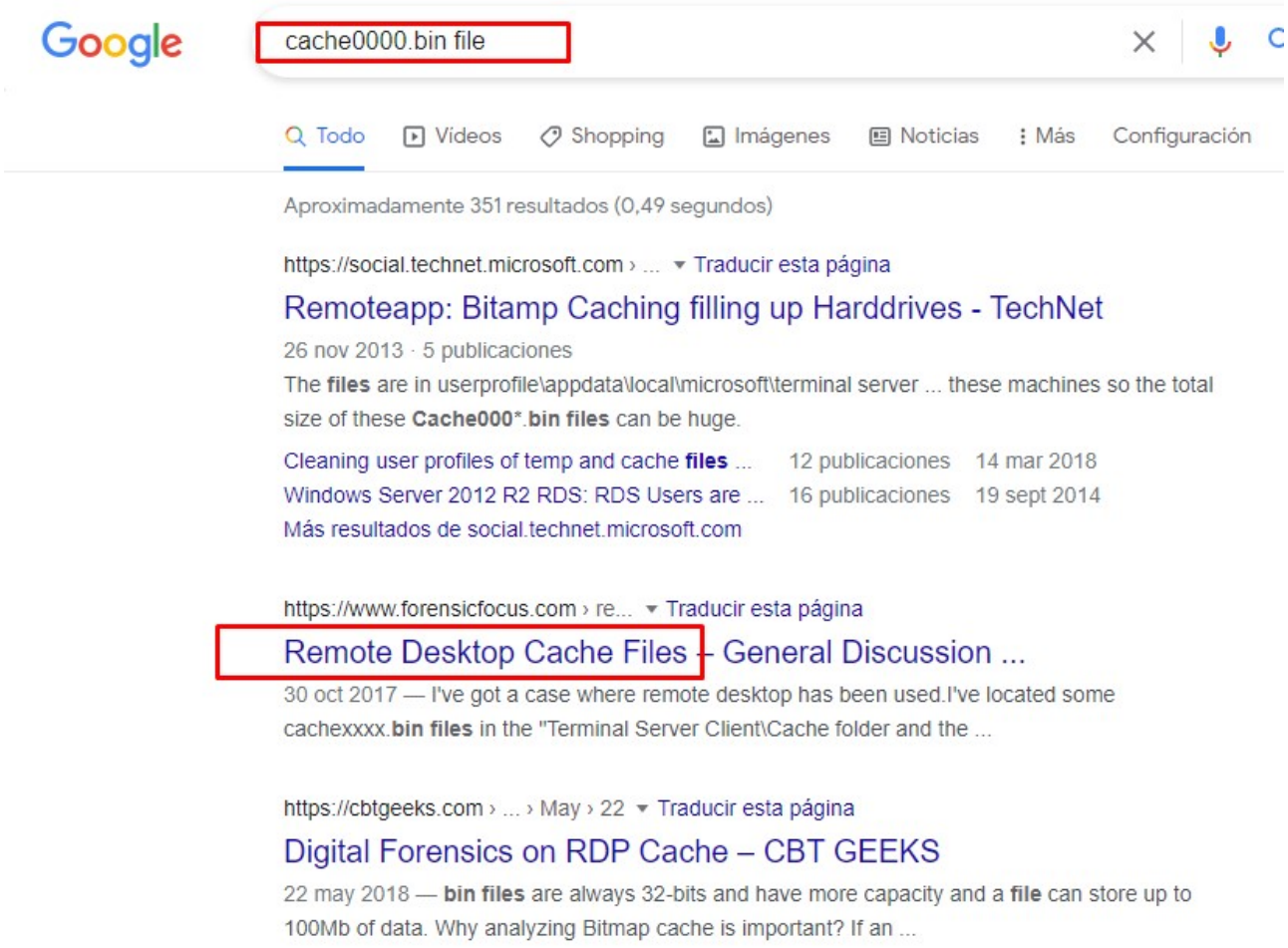


Figure 2

Above picture, indicates that we are facing a BITMAP cache file related to Remote Desktop Protocol. Next step would be to use any tool which allows to extract BMP files, like https://github.com/ANSSI-FR/bmc-tools

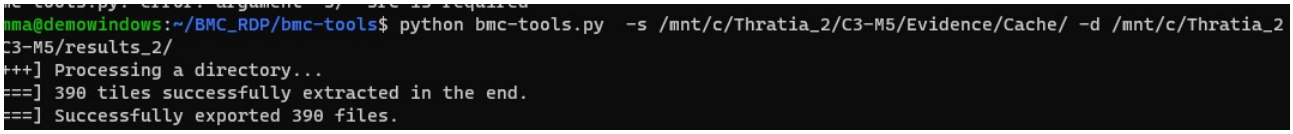


Figure 3

Once Extracted, player has multiple files to order the puzzle an get the password:

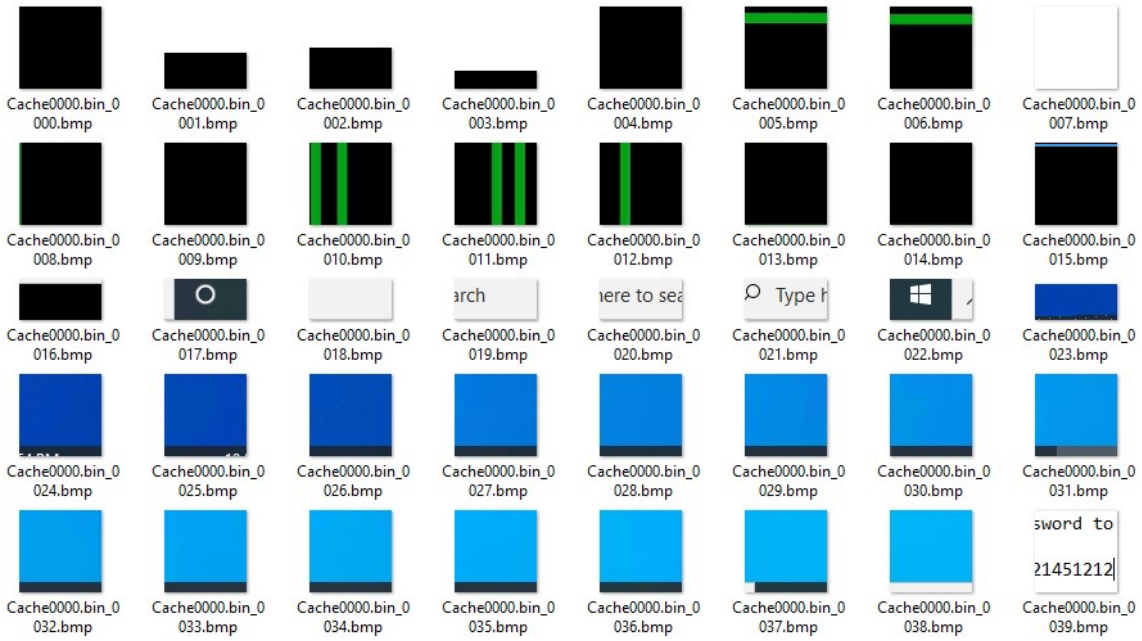


Figure 4

One specialized tool in this function is RdpCacheStitcher

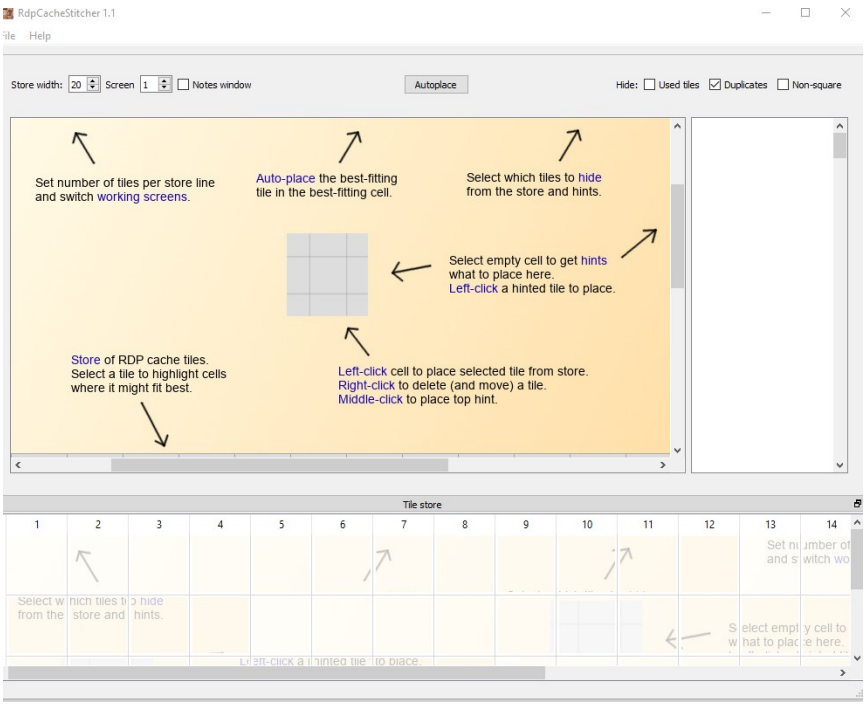


Figure 5

Player must to create a new case :

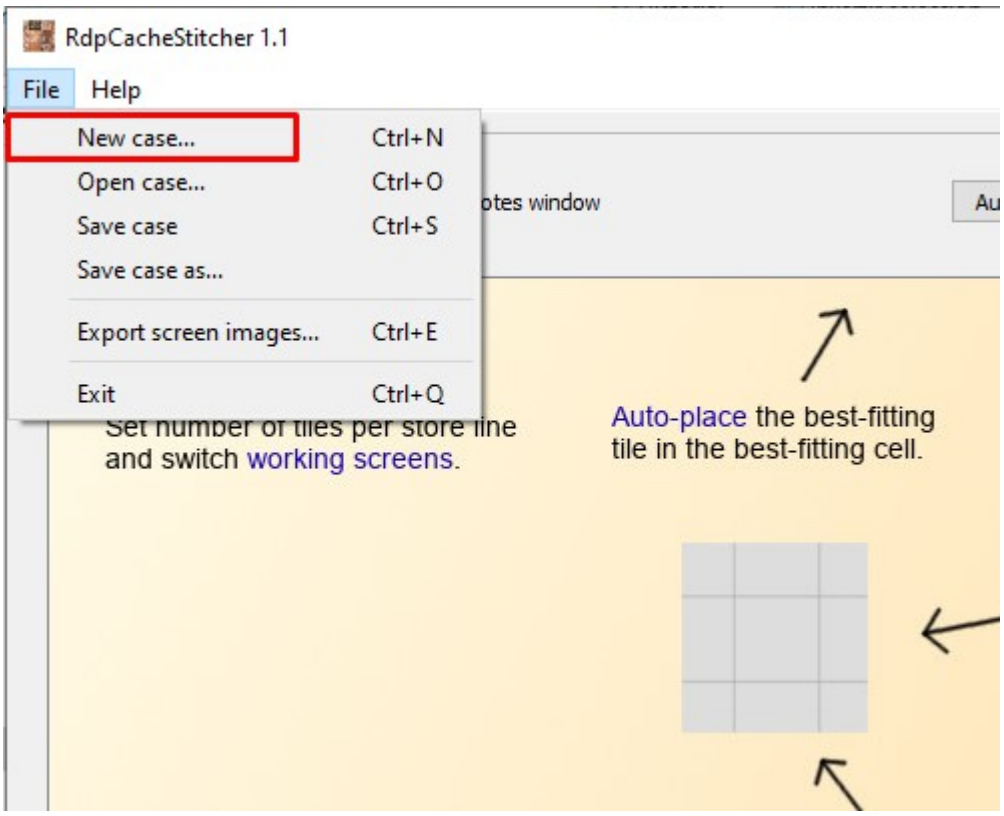


Figure 6

Once created, player must select folder that contains BMP files, that were previously extracted:

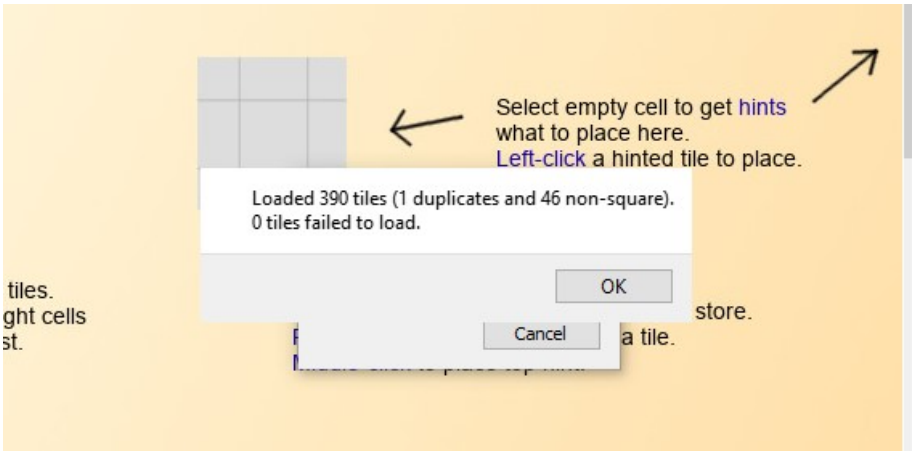


Figure 7

Once loaded the case, player must to order the puzzle to get password:

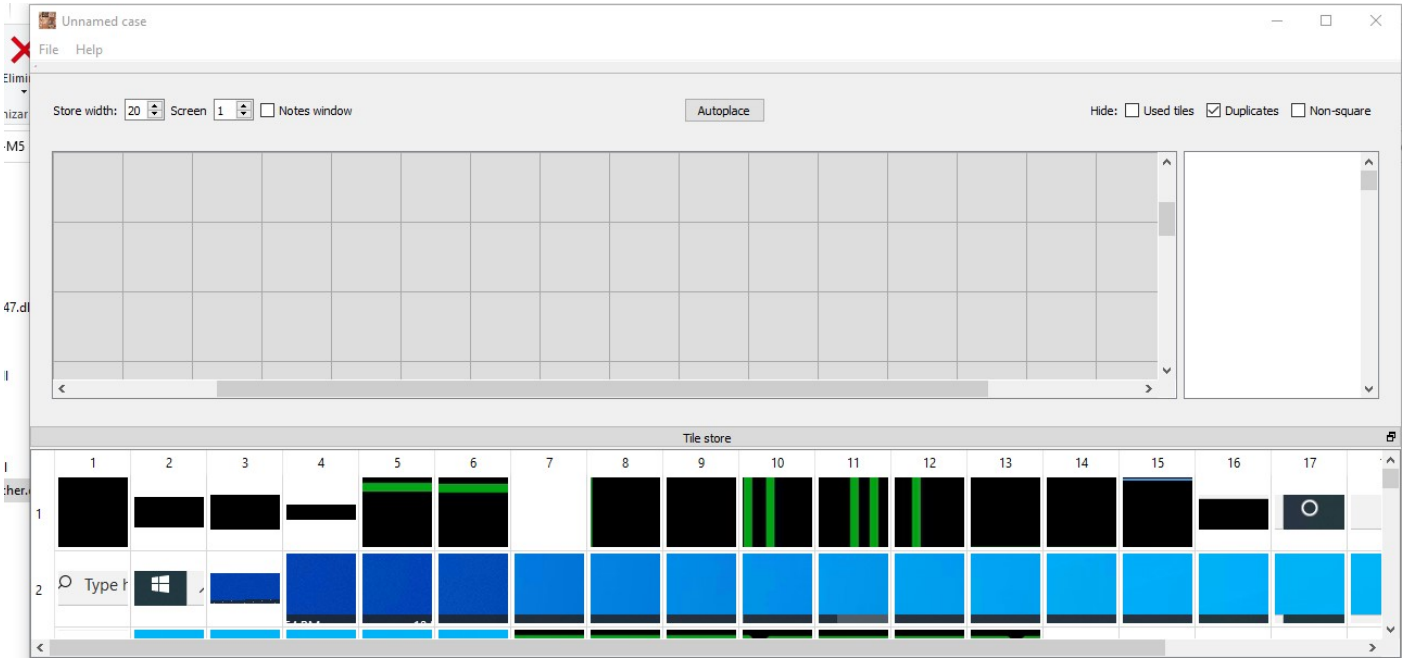


Figure 8

And finally put the necessary pictures among to get the password:

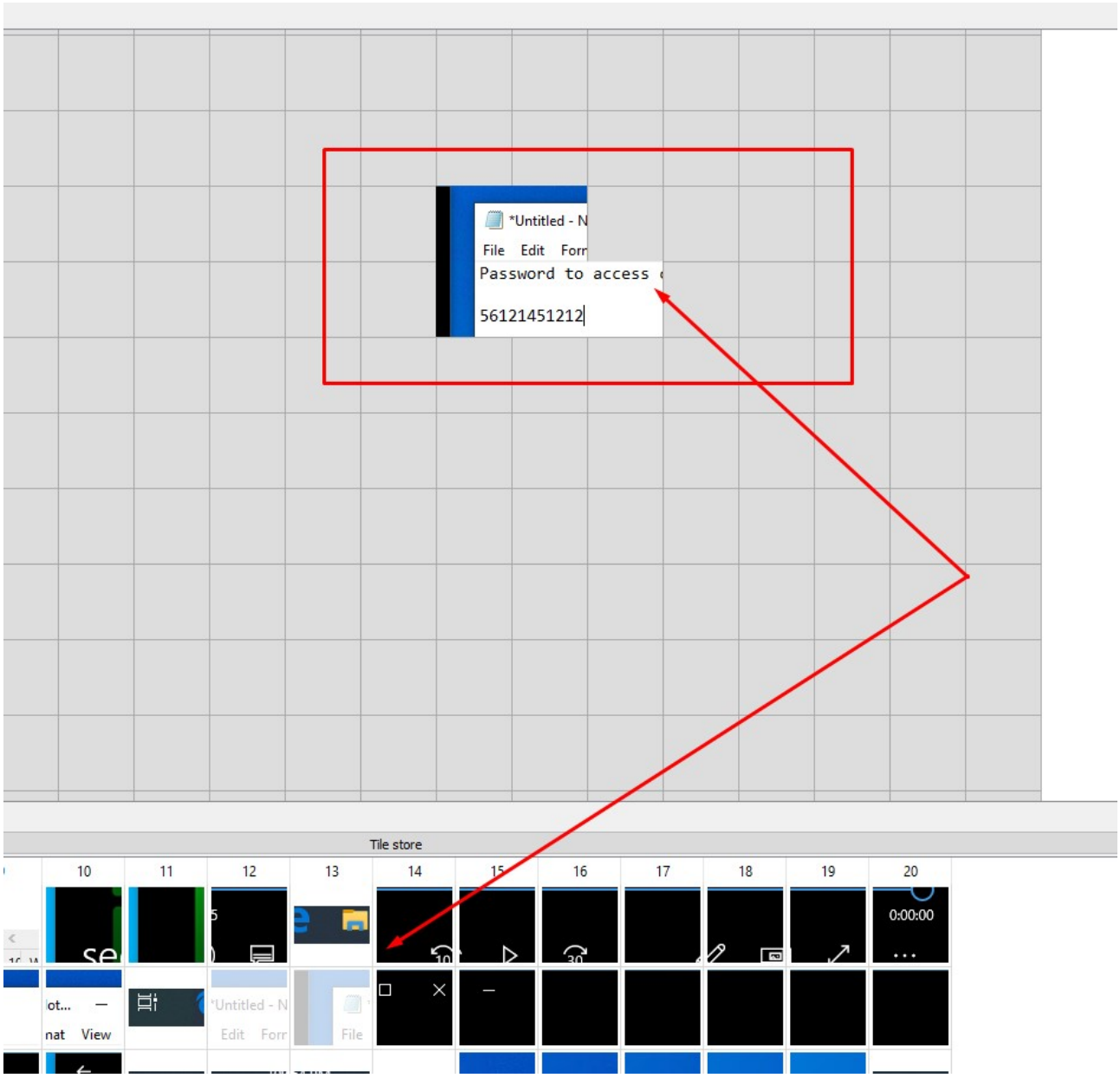


Figure 9

Finally player could get password: 561214511212

Flag Information

flag{561214511212}