Milan Djuric – Naloga 6 Digitalna Forenzika

**Poročilo**

Za spremembo datotek sem uporabil lastne Python skripte, ki berejo datoteke in spreminjajo njihove metapodatke. Glede na vrsto datoteke se metapodatki vedno razlikujejo. Na primer, Word in Excel sta v ozadju dejansko .zip datoteki, medtem ko imata PDF in JPG svoje specifične lastnosti.

Posnetke zaslona skripte sem priložil spodaj in si jih lahko ogledate.

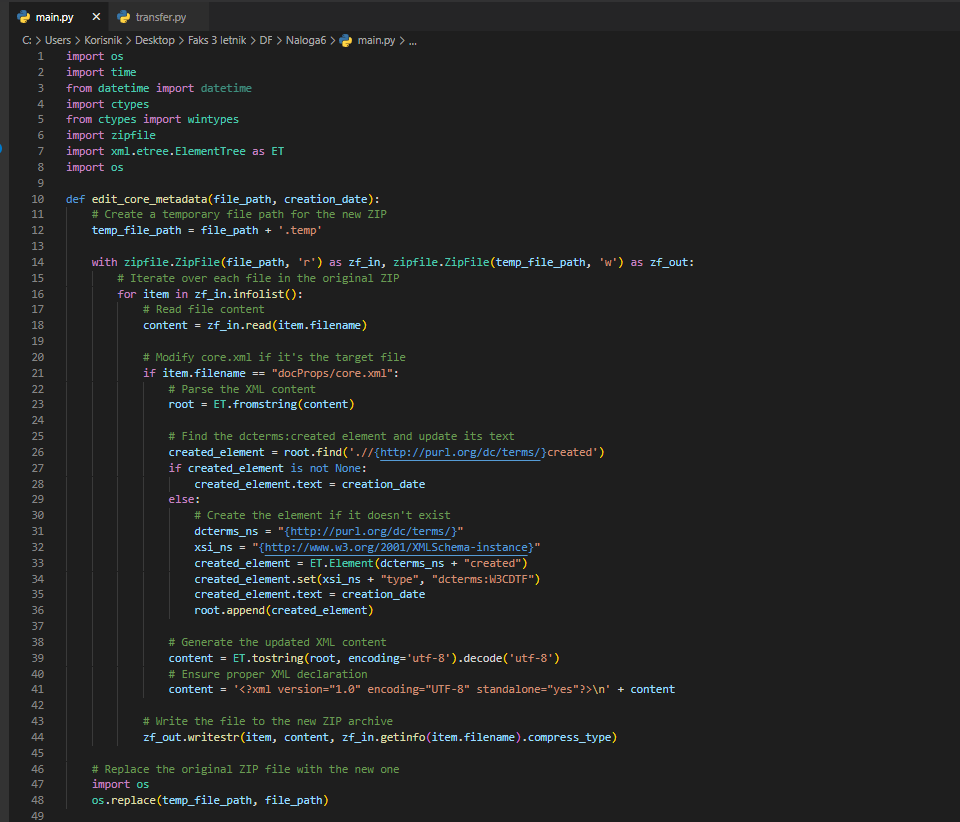
Moja ocena zahtevane stopnje znanja za to nalogo:

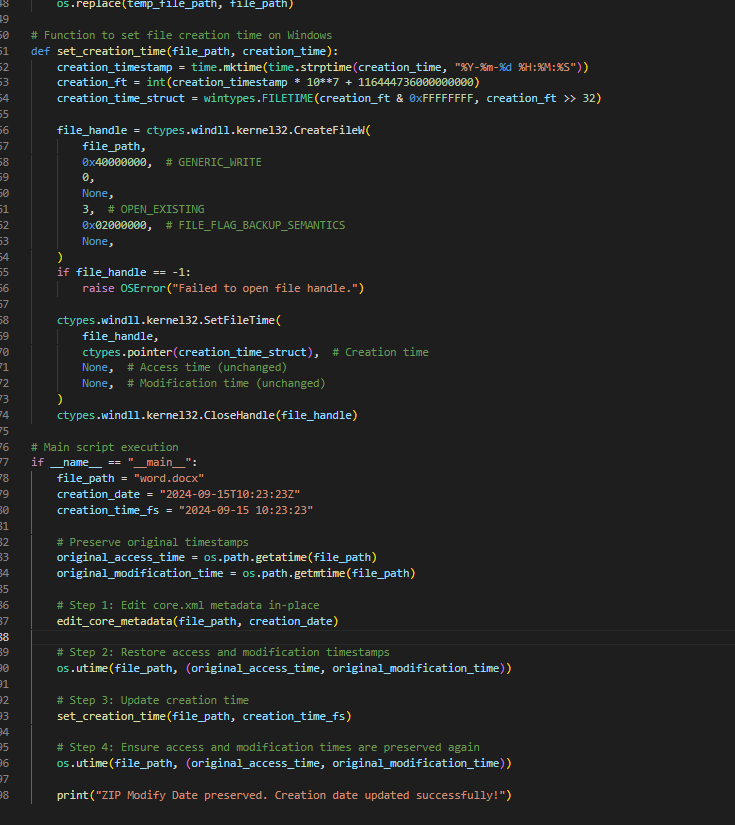
**VISOKA.** Zakaj?   
  
Na prvi pogled se zdi, da gre za enostavno nalogo, vendar sem po več urah dela (približno 6–8 ur) ugotovil, da to ni tako preprosto. Še vedno nisem prepričan, ali sem popolnoma dosegel to, kar sem si zamislil. Kje vse bi lahko bili zabeleženi podatki o spremembah, ki sem jih naredil? Potrudil sem se skriti spremembe od operacijskega Sistema in metapodatke datoteke, vendar je možno, da bi nekdo z uporabo forenzične slike diska lahko odkril podatke o tem, kdaj sem to skripto izvedel.

Prav tako se sprašujem, kaj se zgodi z atributom "last accessed"? Tega mi ni uspelo spremeniti. Je to pomembno in kako pomembno? Menim, da je za popolno skrivanje sledi potrebno zelo visoko znanje in natančnost. Tega ne more storiti nekdo brez poznavanja računalnikov in programiranja.

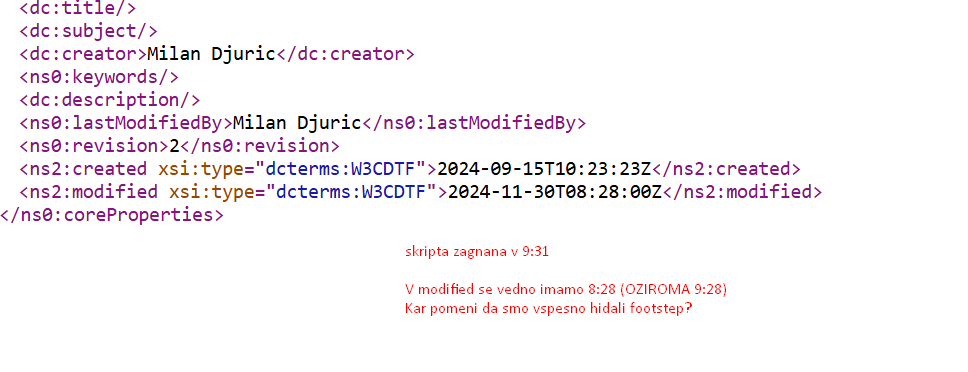
Pisanje Python skript je bila moja izbira, vendar nisem prepričan, ali obstajajo boljša orodja v Kali Linuxu ali morda jeziki z dodatnimi knjižnicami, ki to nalogo rešujejo bolje. Tega ne vem zagotovo.

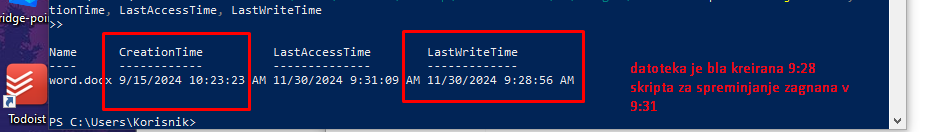
Koraki ->  
  
Za preverjanje sem uporabil exiftool. In powershel commande  
  
Kjer exiftool nima support za spreminjanje docx datoteke. Sem se odlocil da naredim custom python scriptu ki bo to za mene spreminjala.  
  
Skripta izgleda takoj ->

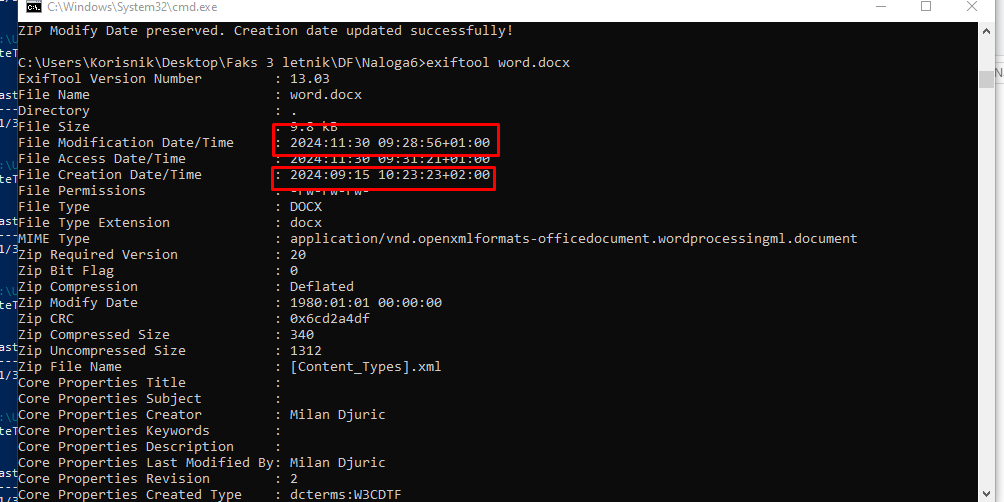




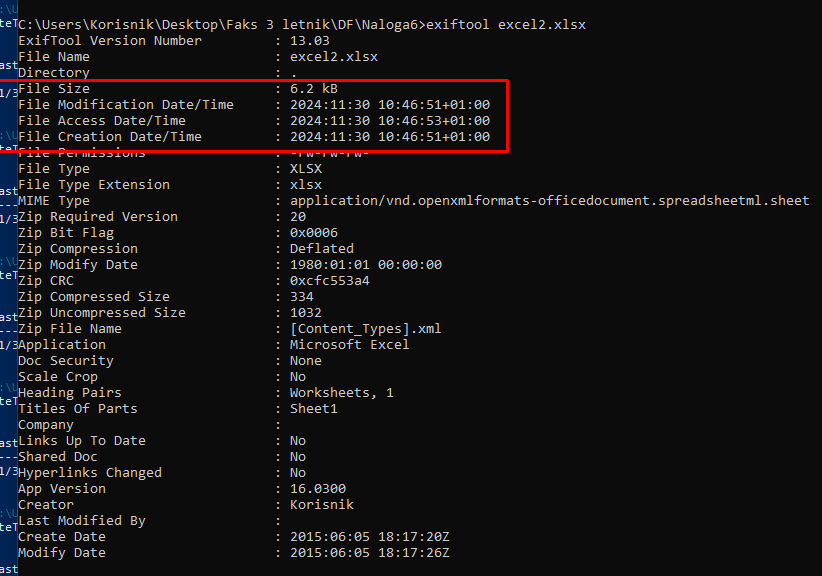
Spremenili smo metadata podatke v wordu in tudi v OS metadata

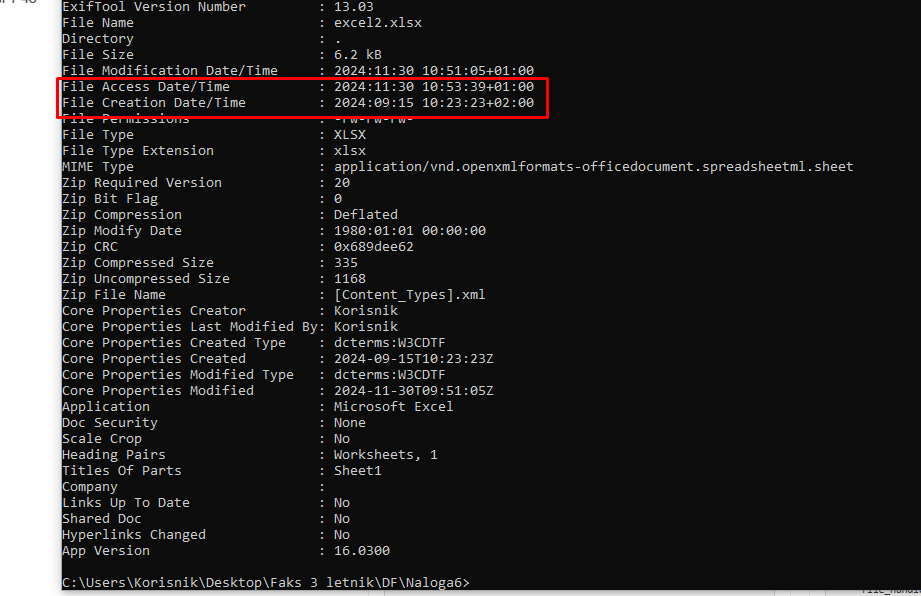
SKRIPTA JE BLA ZAGNANA V 9:31, DATOTEKA KREIRANA V 9:28  
  
V XML-u preverimo  


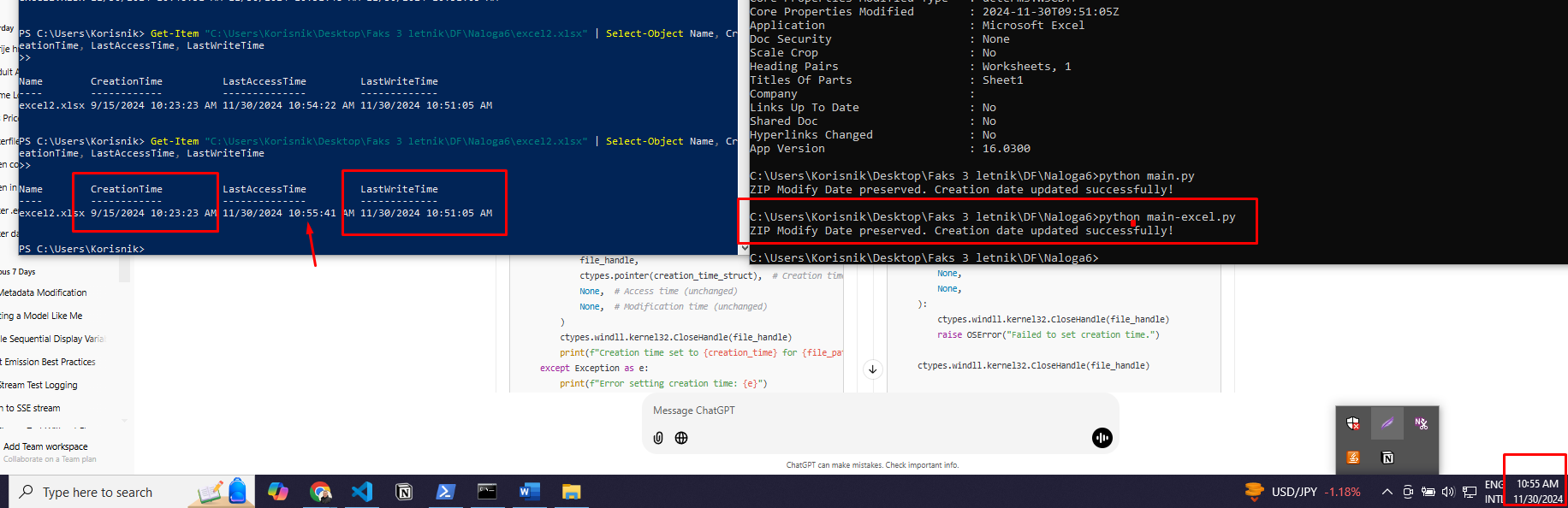


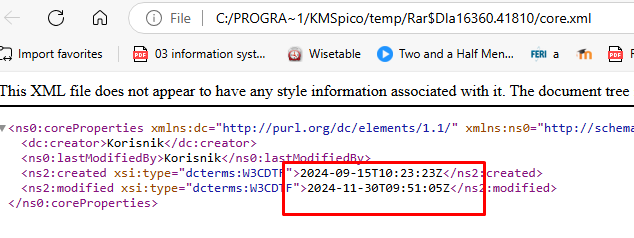
  
  
V autopsiju sem naloadal logicno datoteko in kot vidimo nikje nimamo 9:31 footstep da je datoteka spremenjena.  
  
Vspelo mi ni spremeniti file access time  
Ne vem Koliko je to pomembno, mislim da je to tudi odvisno od situacije.

EXCEL

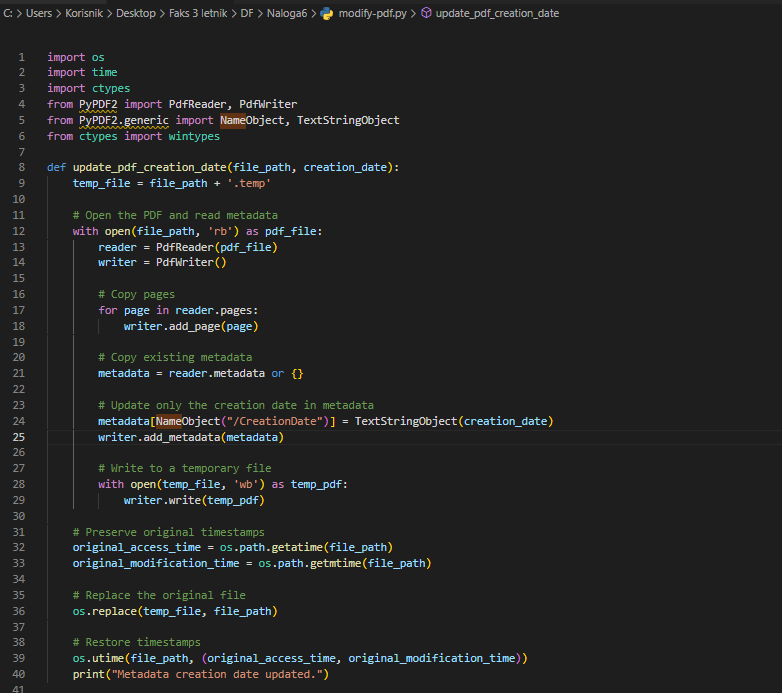
Pre kreiranja ->  
Datum kreiranja 10:46 (potem ena sprememba da dam datum je bla 20s kasneje)  


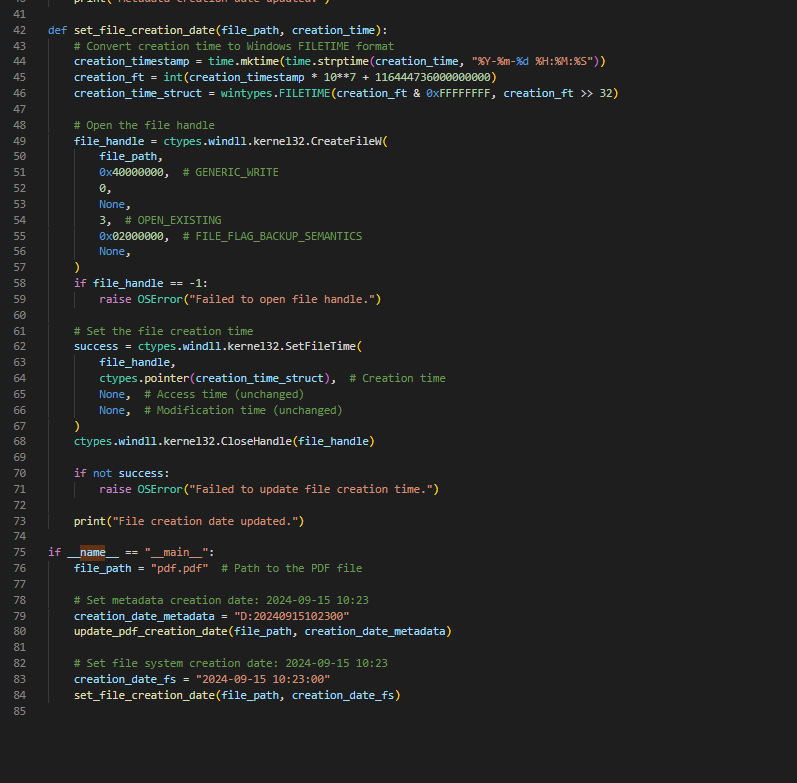
Po runnanju skripte  
  
  
  
Skripto smo malo spremenili

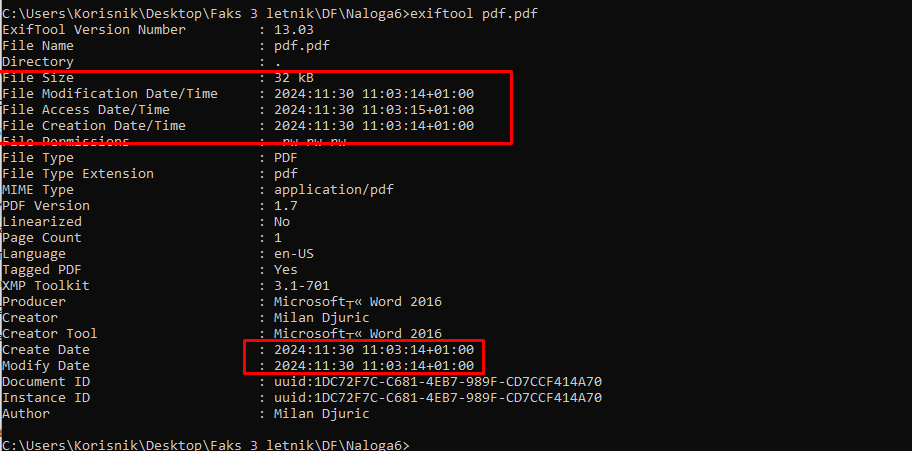


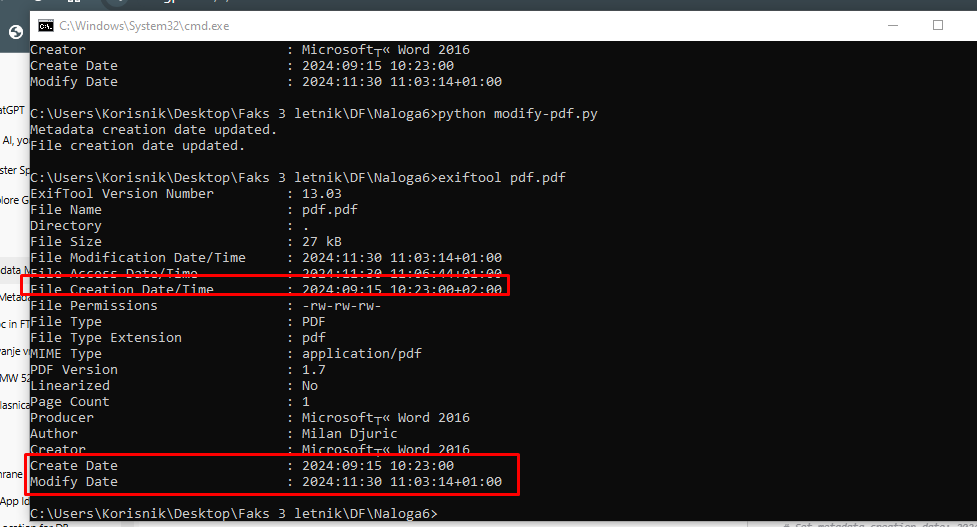


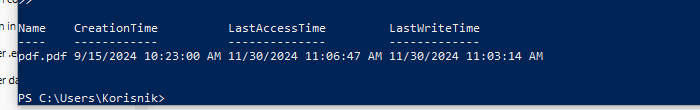
PDF ->





Pre skripte  






JPG ->  
