Jak sam tytuł dziś zajmę się dziedziną działań informatycznych, które kojarzą się nam z programami typu CSI. IT Forensic polega na wykryciu i zabezpieczenia jak największej ilości dowodów na przestępstwo lub uzyskaniu informacji na temat danej sytuacji. Miejscem, gdzie wykorzystuję podstawowe procedury zabezpieczenia dowodów jest sytuacja gdy jestem proszony o usunięcie złośliwego oprogramowania. Dziś pokażę jak to się odbywa.

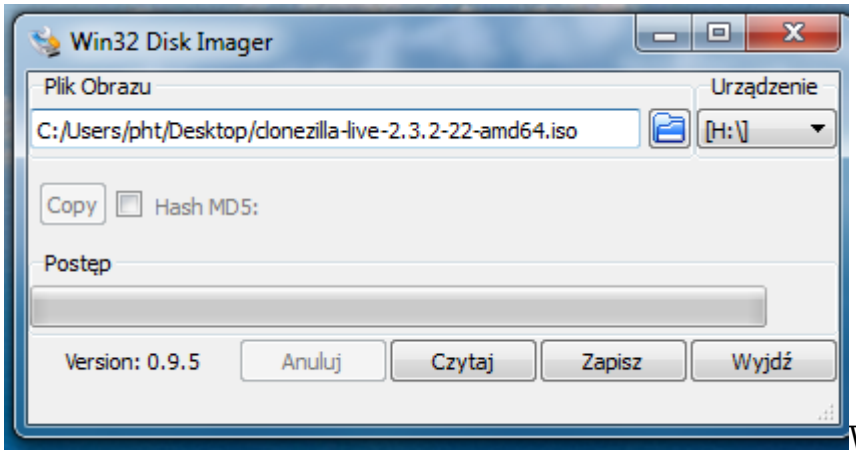
Spis treści

1. Przygotowanie

Naszym zadaniem jest zbadanie dowodu w taki sposób by nie wprowadzić w nim zmian uniemożliwiających przeprowadzenie weryfikacji naszych wniosków. Pierwszym co będzie nam potrzebnym będzie zestaw:

- Komputer który będziemy badać.
- Dysk twardy o pojemności większej niz dysk badanego komputera.
- Pendrive z wypalonym obrazem Clonezilla (lub dowolny inny Linux, jednakże zalecany Clonezilla)

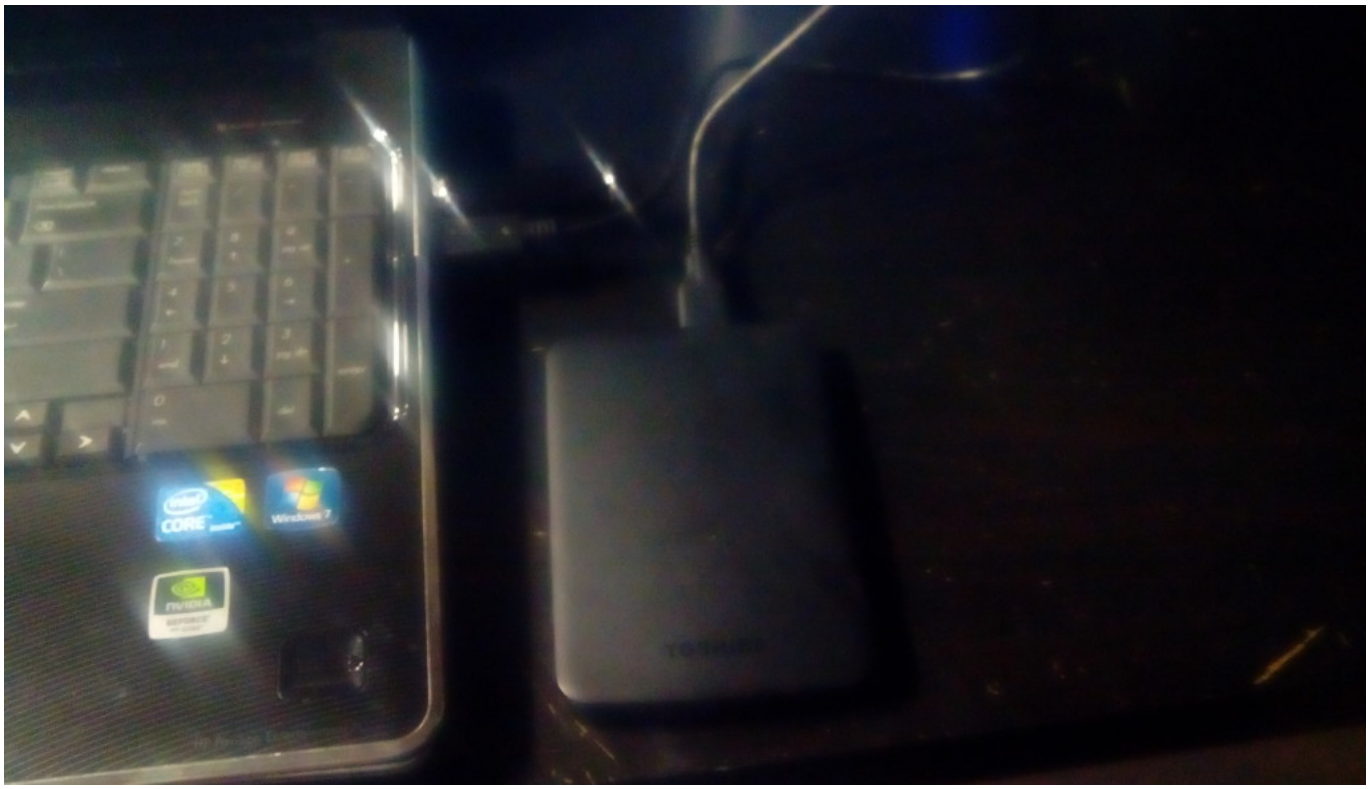
Zaczniemy od pobrania i wypalenia na pendrive Clonezilli. Po pobraniu do wypalenia obrazu na pendrive możemy użyć np Win32 Disk Imager (dla windows) lub dd (dla linuksów).



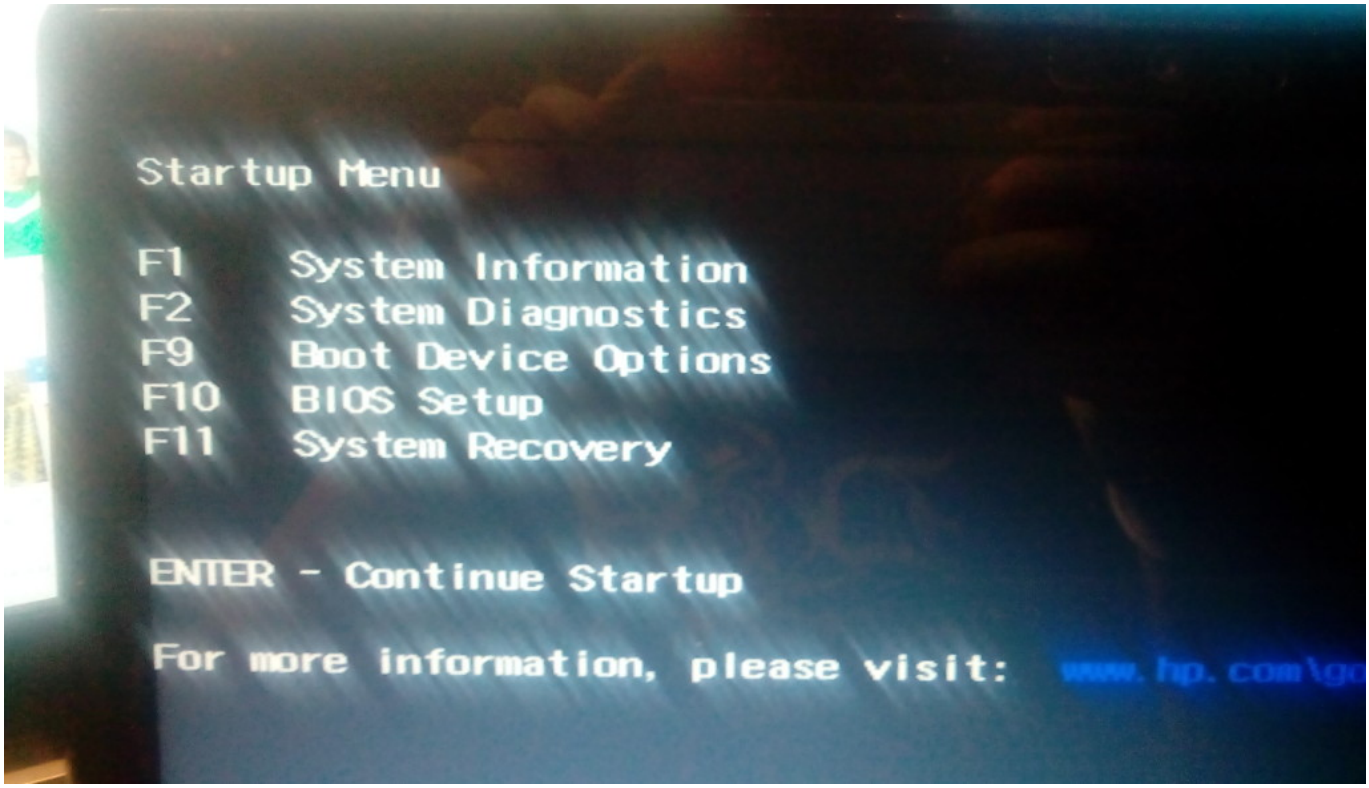
Wybieramy interesujący nas obraz, urządzenie na którym chcemy wypalić obraz Clonezilli i klikamy zapisz.

2. Zabezpieczenie dowodów

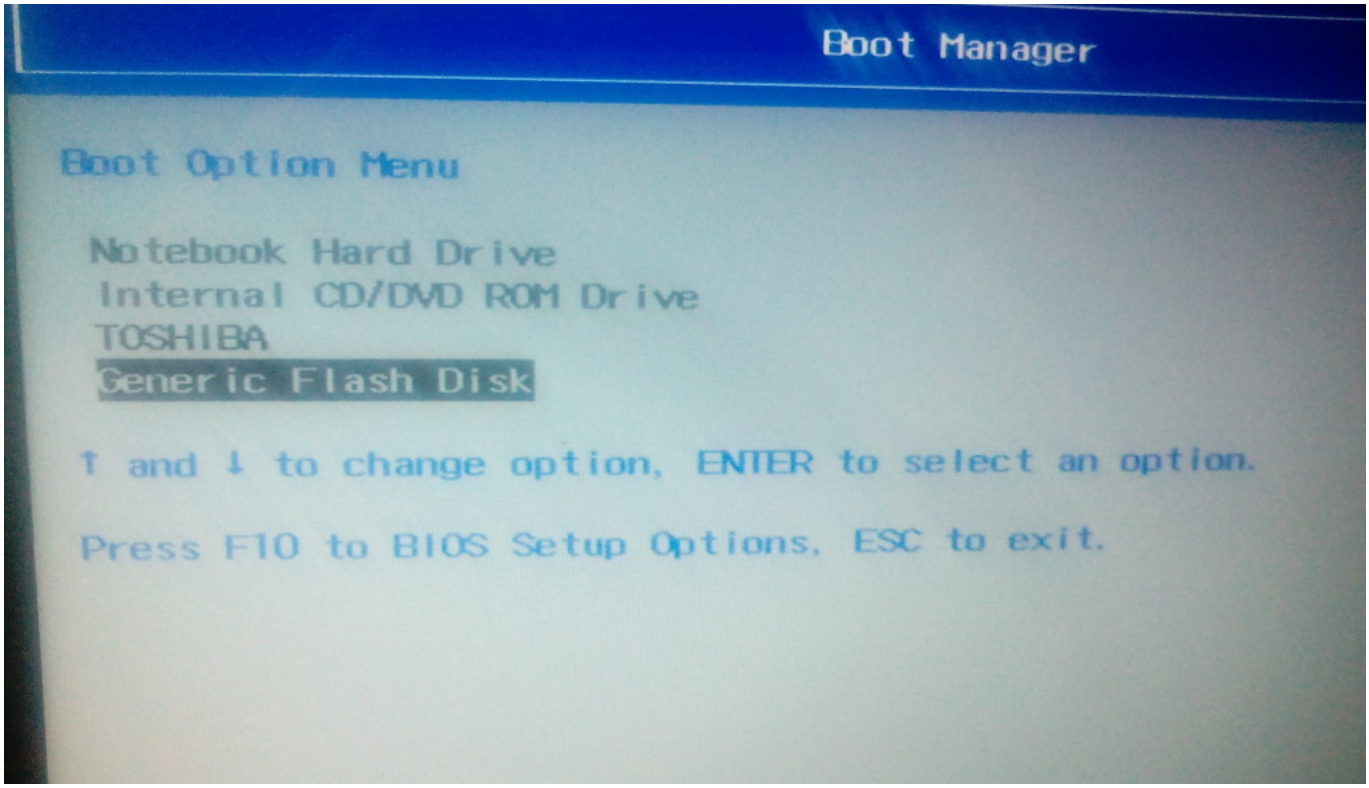
Następnym krokiem, który jest **OBOWIĄZKOWY** jest wykonanie kopi dysku twardego na którym będziemy przeprowadzać dalsze działanie. jest to wymagany krok, ponieważ gdybyśmy zaczęli wykonywać na oryginalnym systemie, moglibyśmy swoja działalnością zatrzeć ślady. Przystąpmy zatem do zabezpieczenia. Samo zabezpieczenie jest identyczne do wykonywania typowego backupu. Wpinamy usb i nasz dodatkowy dysk do komputera będącego przedmiotem dochodzenia.



Następnie uruchamiamy komputer w sposób umożliwiający nam **JEDNORAZOWE** bootowanie z naszego pendrive. Jednorazowe dlatego, iż nie chcemy wprowadzać zmian nawet na poziomie BIOS-u.



Po wciśnięciu „F9” po chwili naszym oczom ukazuje się okno wyboru urządzeń z których możemy zabootować system. Wybieramy nasz pendrive.



Dokładny opis jak wykonać kopie dysku można znaleźć tu. Próbowałem znaleźć link do autora aby powiadomić go o zalinkowaniu, niestety się nie udało.

3. Odwzorowanie badanego systemu

Ten punkt jest dość krótki i łatwy do zrobienia. Pozwolę sobie pokrótce go opisać. Wystarczy nam wirtualna maszyna odpowiadająca wielkością dysku oryginalnej(ja osobiście preferuje VMware, ale może być też VirtualBox). Oczywiście ilość RAM-u też powinna być adekwatna do oryginalnej, jednakże można minimalnie zwiększyć dla naszej wygody. Korzystając z wyżej wymienionego poradnika na temat Clonezilli odtwarzamy dysk. Po chwili uzyskujemy dokładna kopie maszyny, którą chcemy zbadać. Możemy dokonać wielu inwazyjnych testów bez obaw o zniszczenie dowodów.

Po wykonaniu powyższych trzech kroków nie zostaje nam nic innego, jak zabrać się do badań danych na dysku. W ten sposób możemy nie tylko badać komputer pod katem dowodów, ale i na naszej kopi odnaleźć złośliwe oprogramowanie i je usunąć tym samym bezpiecznie opracowując procedure usunięcia bez narażania oryginalnego systemu.