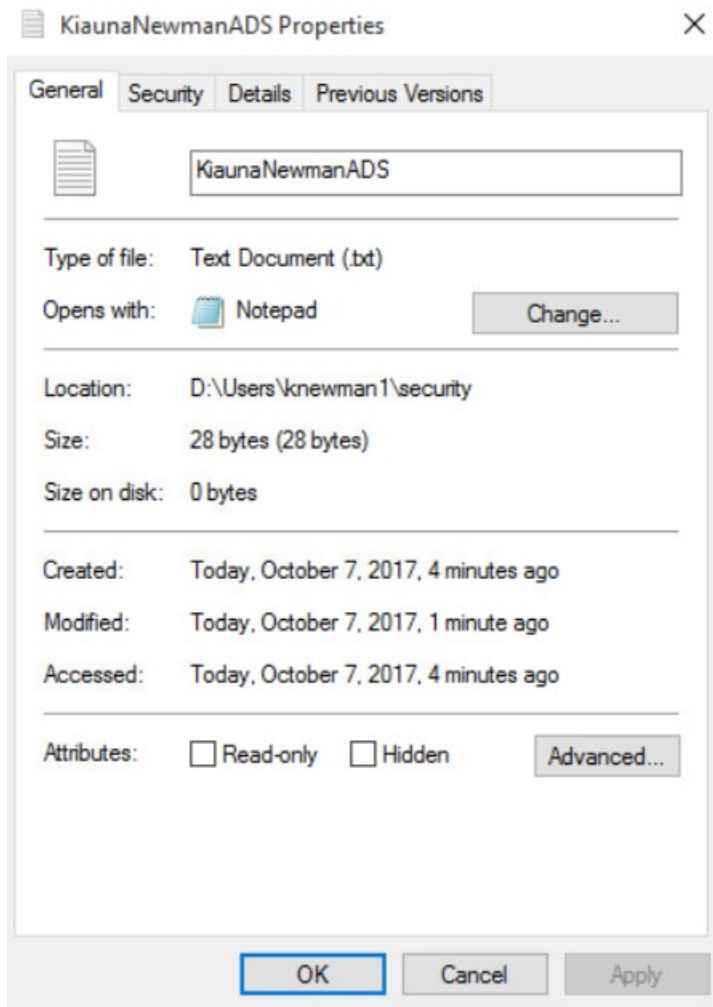


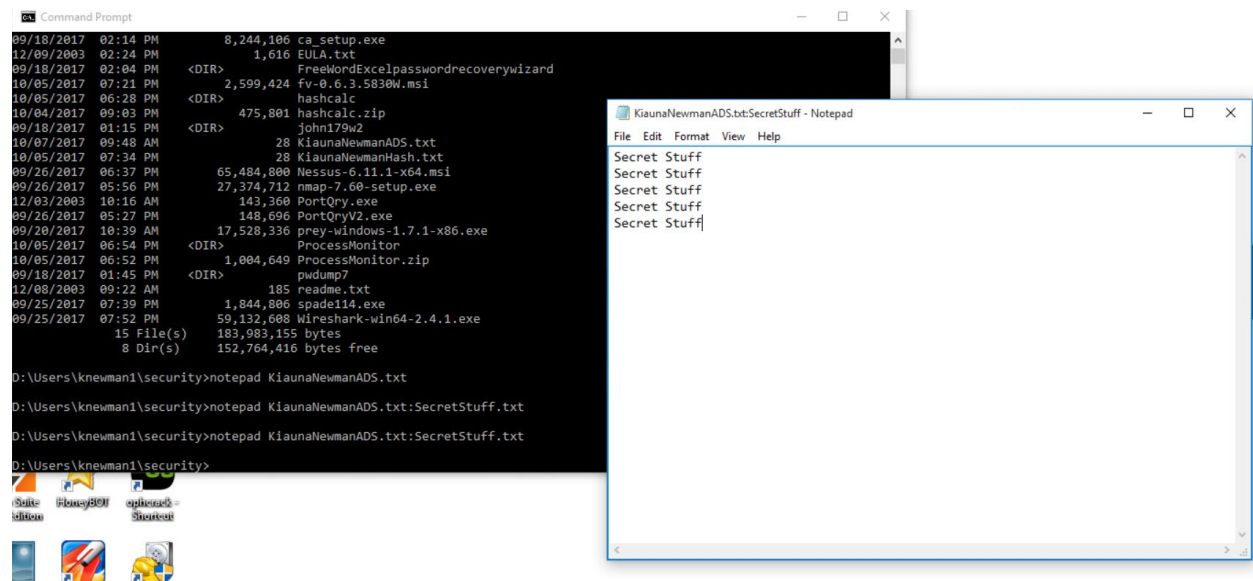
14.1 Create an ADS



```
Command Prompt

10/07/2017 09:45 AM <DIR> .
10/07/2017 09:45 AM <DIR> ..
09/18/2017 01:13 PM <DIR> boyle1e_student_project_files
09/18/2017 02:14 PM      8,244,106 ca_setup.exe
12/09/2003 02:24 PM      1,616 EULA.txt
09/18/2017 02:04 PM <DIR> FreeWordExcelpasswordrecoverywizard
10/05/2017 07:21 PM      2,599,424 fv-0.6.3.5830W.msi
10/05/2017 06:28 PM <DIR> hashcalc
10/04/2017 09:03 PM      475,801 hashcalc.zip
09/18/2017 01:15 PM <DIR> john179w2
10/07/2017 09:48 AM      28 KiaunaNewmanADS.txt
10/05/2017 07:34 PM      28 KiaunaNewmanHash.txt
09/26/2017 06:37 PM      65,484,800 Nessus-6.11.1-x64.msi
09/26/2017 05:56 PM      27,374,712 nmap-7.60-setup.exe
12/03/2003 10:16 AM      143,360 PortQry.exe
09/26/2017 05:27 PM      148,696 PortQryV2.exe
09/20/2017 10:39 AM      17,528,336 prey-windows-1.7.1-x86.exe
10/05/2017 06:54 PM <DIR> ProcessMonitor
10/05/2017 06:52 PM      1,004,649 ProcessMonitor.zip
09/18/2017 01:45 PM <DIR> pwdump7
12/08/2003 09:22 AM      185 readme.txt
09/25/2017 07:39 PM      1,844,806 spade114.exe
09/25/2017 07:52 PM      59,132,608 Wireshark-win64-2.4.1.exe
      15 File(s)      183,983,155 bytes
      8 Dir(s)       152,764,416 bytes free

D:\Users\knewman1\security>notepad KiaunaNewmanADS.txt
D:\Users\knewman1\security>notepad KiaunaNewmanADS.txt:SecretStuff.txt
```



14.2 ADS Executable

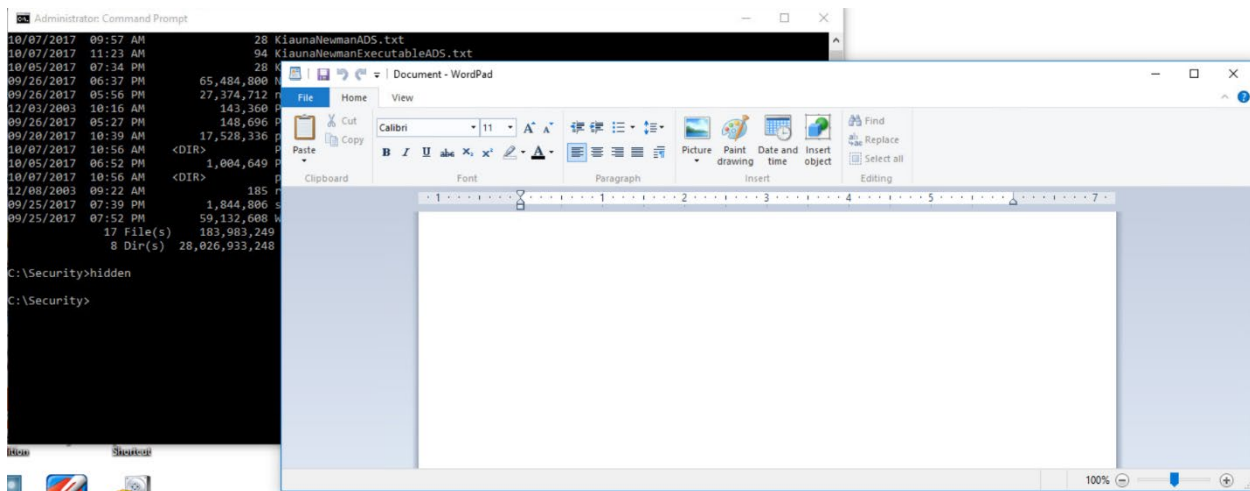
```
Administrator: Command Prompt
10/05/2017 07:21 PM          2,599,424 fv-0.6.3.5830W.msi
10/07/2017 10:56 AM      <DIR>          hashcalc
10/04/2017 09:03 PM          475,801 hashcalc.zip
10/07/2017 10:56 AM      <DIR>          john179w2
10/07/2017 09:57 AM          28 KiaunaNewmanADS.txt
10/07/2017 10:10 AM          94 KiaunaNewmanExecutableADS.txt
10/05/2017 07:34 PM          28 KiaunaNewmanHash.txt
09/26/2017 06:37 PM        65,484,800 Nessus-6.11.1-x64.msi
09/26/2017 05:56 PM        27,374,712 nmap-7.60-setup.exe
12/03/2003 10:16 AM          143,360 PortQry.exe
09/26/2017 05:27 PM          148,696 PortQryV2.exe
09/20/2017 10:39 AM        17,528,336 prey-windows-1.7.1-x86.exe
10/07/2017 10:56 AM      <DIR>          ProcessMonitor
10/05/2017 06:52 PM        1,004,649 ProcessMonitor.zip
10/07/2017 10:56 AM      <DIR>          pwdump7
12/08/2003 09:22 AM          185 readme.txt
09/25/2017 07:39 PM        1,844,806 spade114.exe
09/25/2017 07:52 PM        59,132,608 Wireshark-win64-2.4.1.exe
16 File(s)          183,983,249 bytes
8 Dir(s)          28,028,809,216 bytes free

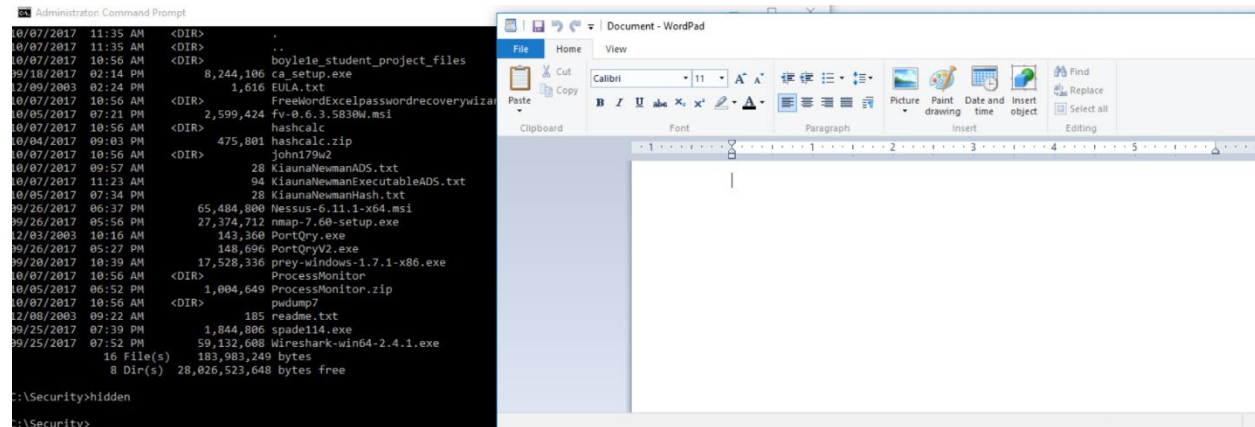
C:\Security>copy C:\Windows\System32\write.exe C:\Security
1 file(s) copied.

C:\Security>type write.exe > C:\Security\KiaunaNewmanExecutableADS.txt:write.exe

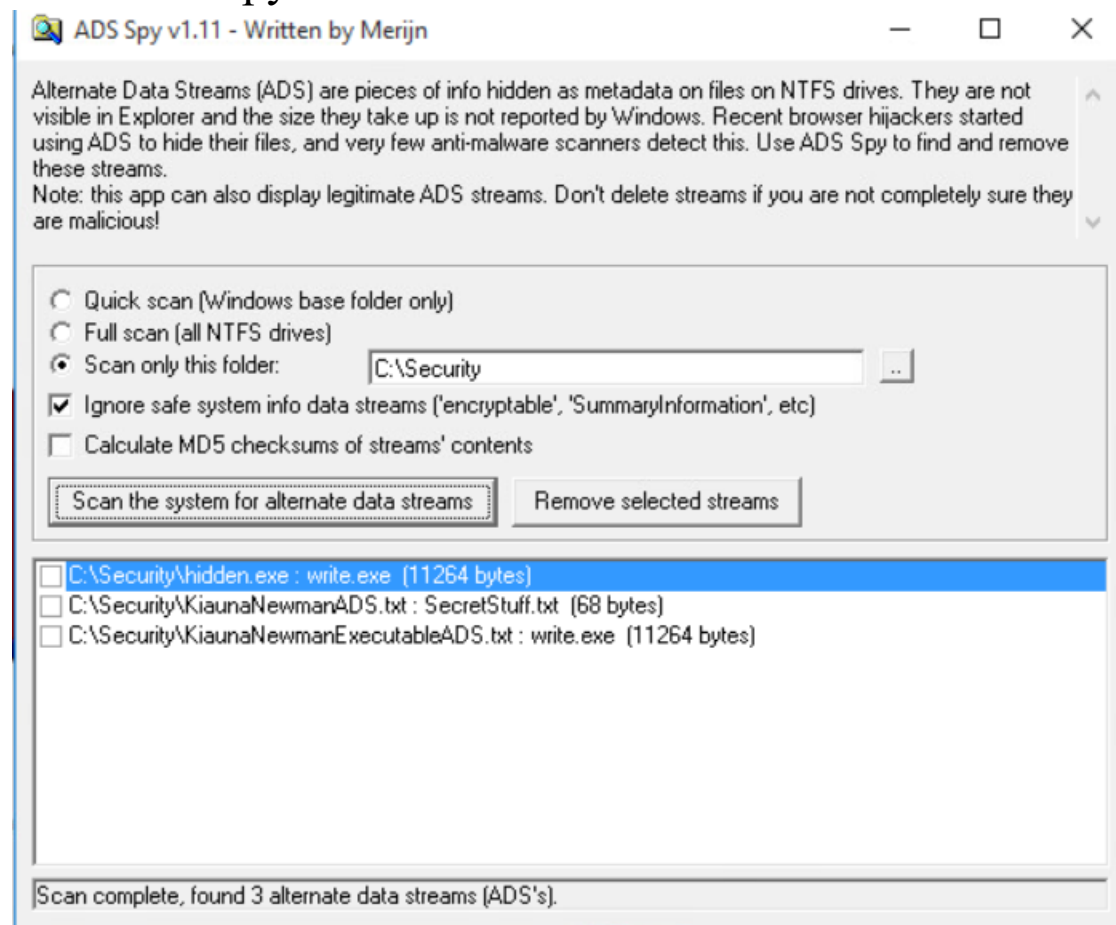
C:\Security>mklink hidden.exe C:\Security\KiaunaNewmanExecutableADS.txt:write.exe
symbolic link created for hidden.exe <====> C:\Security\KiaunaNewmanExecutableADS.txt:write.exe

C:\Security>
```





14.3 ADS Spy



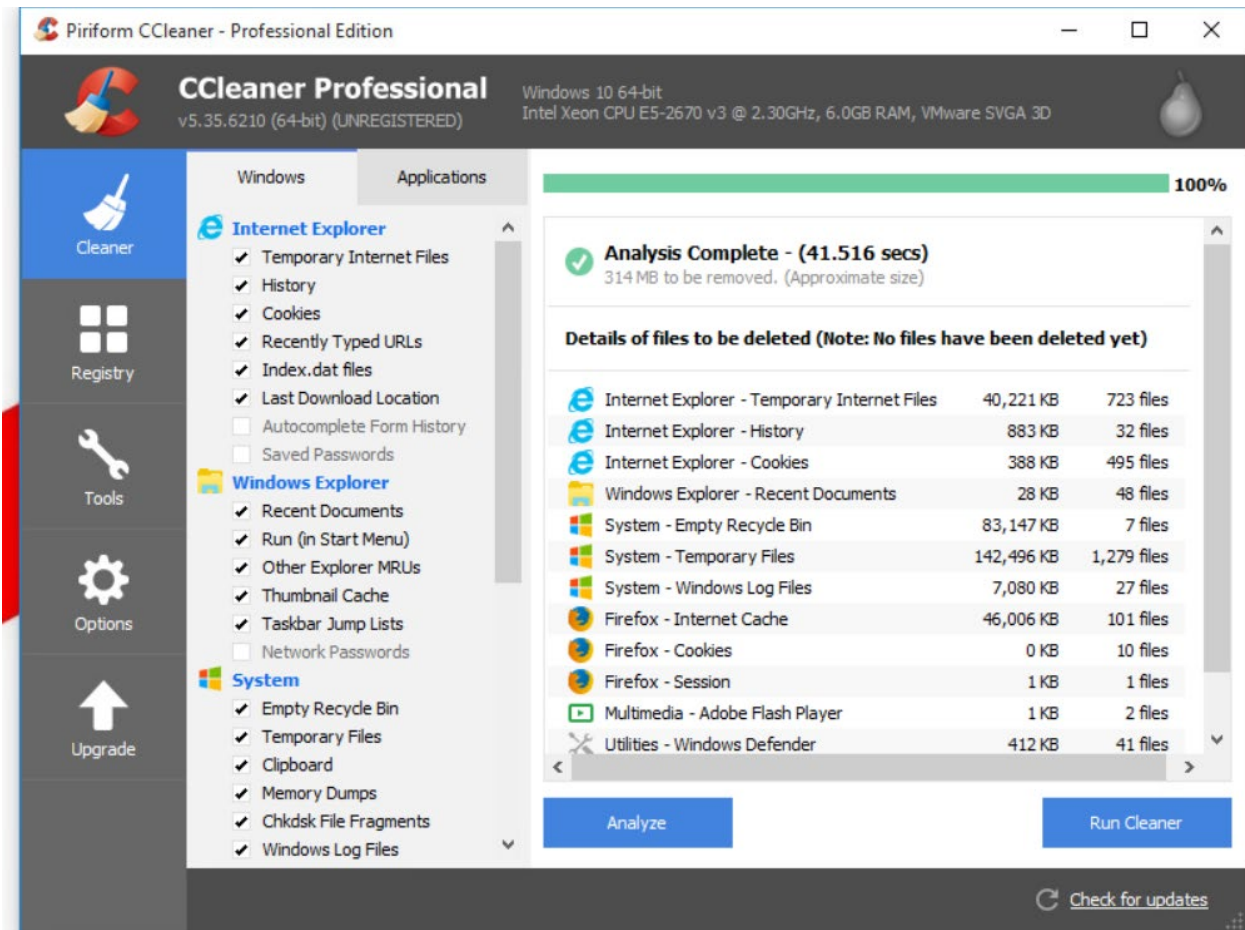
Kiauna Newman
10/9/17

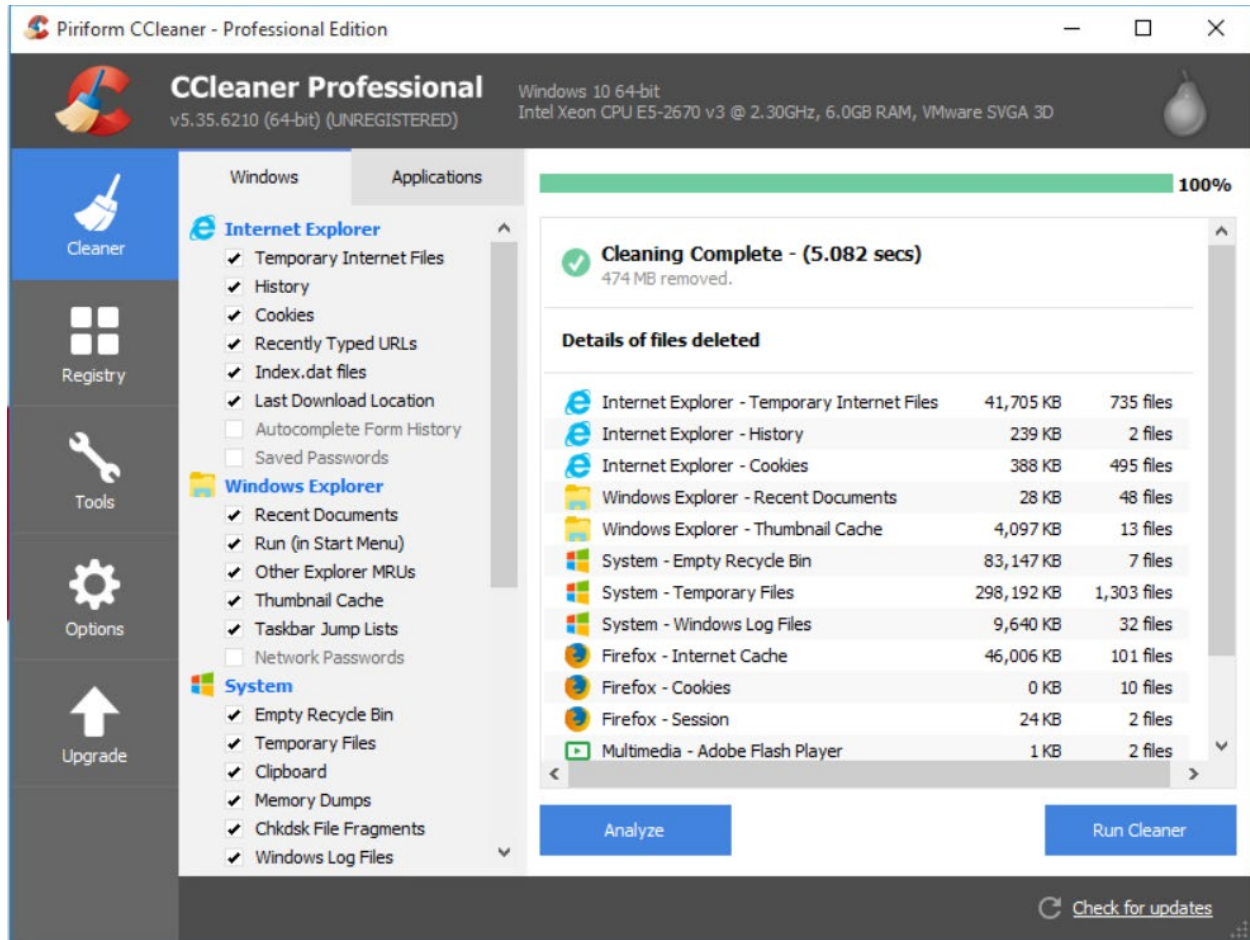
Lab 6: Alternate Data Streams, Data Recovery/Secure Deletion, and Steganography

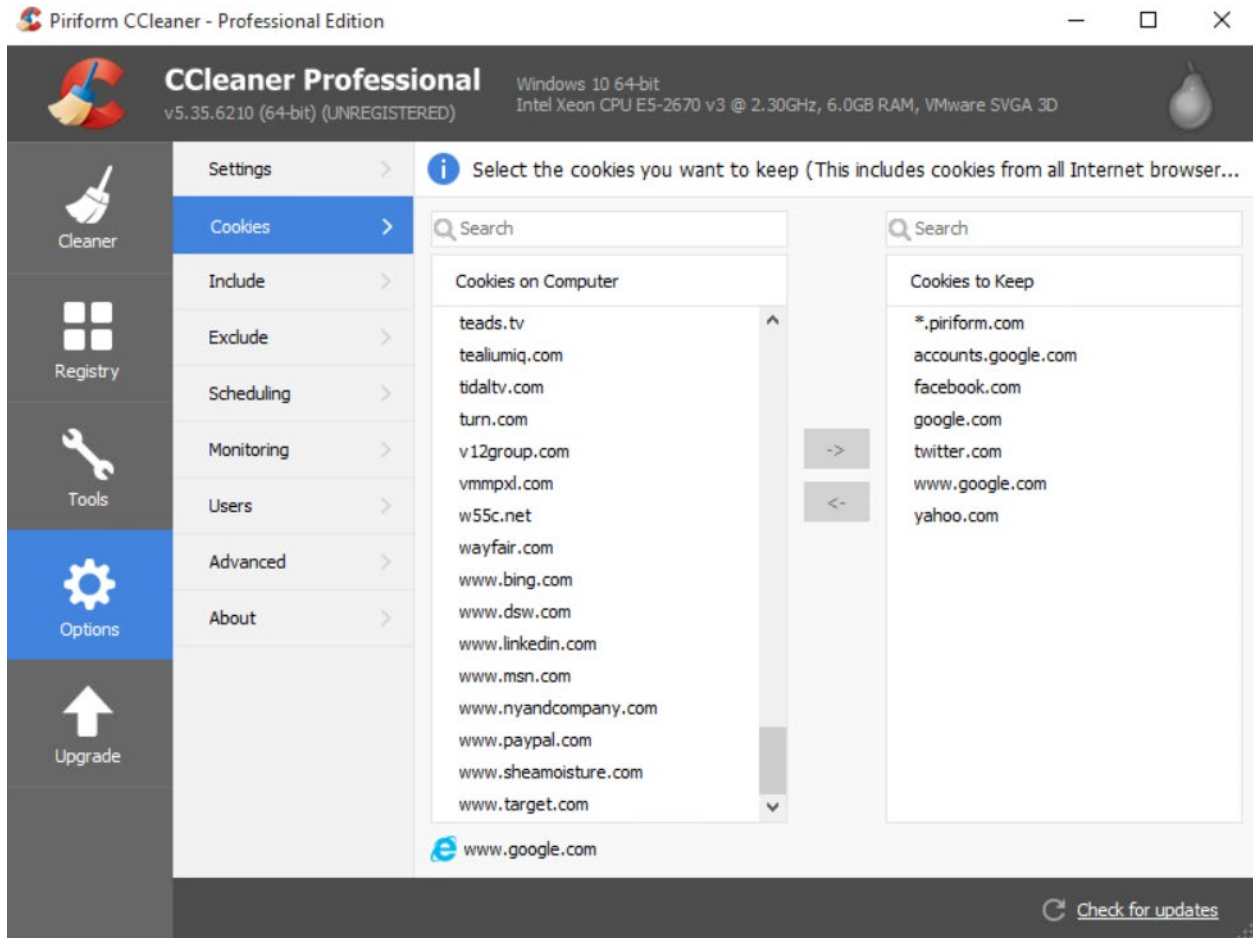
```
Command Prompt
10/04/2017 09:03 PM          475,801 hashcalc.zip
                             26 hashcalc.zip:Zone.Identifier:$DATA
10/07/2017 10:56 AM      <DIR>          john179w2
10/07/2017 09:57 AM          28 KiaunaNewmanADS.txt
                             68 KiaunaNewmanADS.txt:SecretStuff.txt:$DATA
10/07/2017 11:23 AM          94 KiaunaNewmanExecutableADS.txt
                             11,264 KiaunaNewmanExecutableADS.txt:write.exe:$DATA
10/05/2017 07:34 PM          28 KiaunaNewmanHash.txt
09/26/2017 06:37 PM     65,484,800 Nessus-6.11.1-x64.msi
                             29 Nessus-6.11.1-x64.msi:Zone.Identifier:$DATA
09/26/2017 05:56 PM     27,374,712 nmap-7.60-setup.exe
                             29 nmap-7.60-setup.exe:Zone.Identifier:$DATA
12/03/2003 10:16 AM      143,360 PortQry.exe
09/26/2017 05:27 PM      148,696 PortQryV2.exe
                             29 PortQryV2.exe:Zone.Identifier:$DATA
09/20/2017 10:39 AM     17,528,336 prey-windows-1.7.1-x86.exe
                             29 prey-windows-1.7.1-x86.exe:Zone.Identifier:$DATA
10/07/2017 10:56 AM      <DIR>          ProcessMonitor
10/05/2017 06:52 PM     1,004,649 ProcessMonitor.zip
                             26 ProcessMonitor.zip:Zone.Identifier:$DATA
10/07/2017 10:56 AM      <DIR>          pwdump7
12/08/2003 09:22 AM      185 readme.txt
09/25/2017 07:39 PM     1,844,806 spade114.exe
                             29 spade114.exe:Zone.Identifier:$DATA
09/25/2017 07:52 PM     59,132,608 Wireshark-win64-2.4.1.exe
                             29 Wireshark-win64-2.4.1.exe:Zone.Identifier:$DATA
      17 File(s)      184,021,137 bytes
      8 Dir(s)      28,024,766,464 bytes free

C:\Security>
```

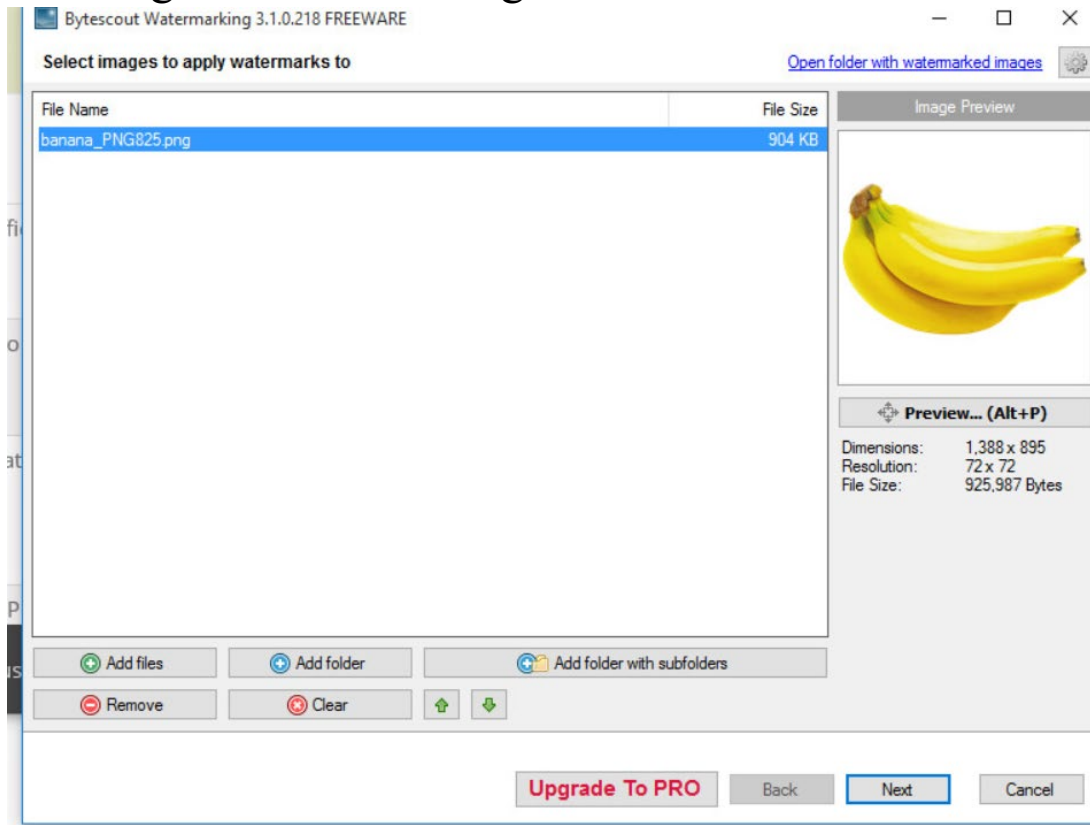

15.3 CCLEANER

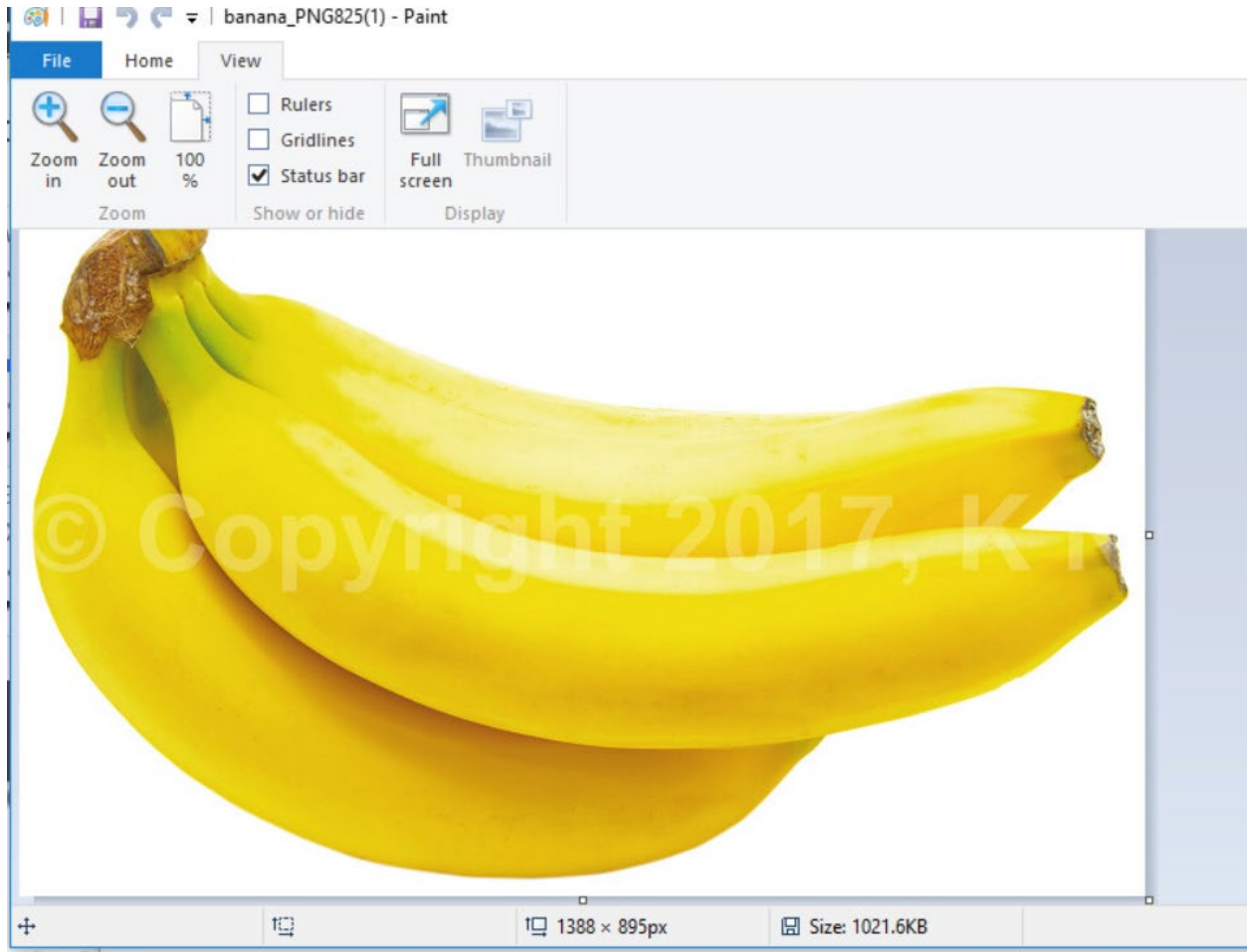




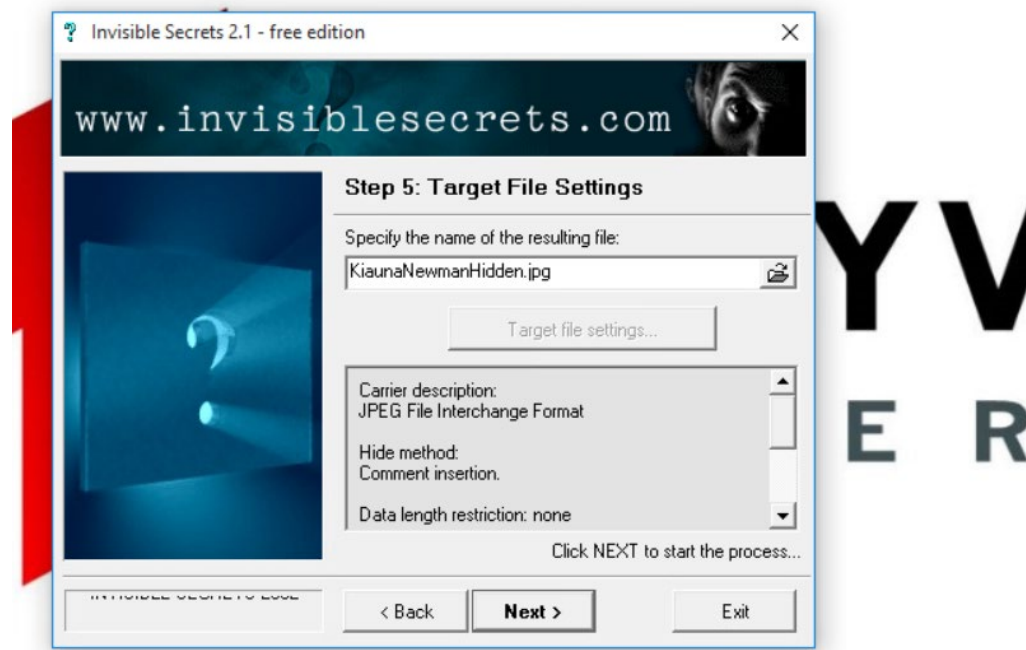


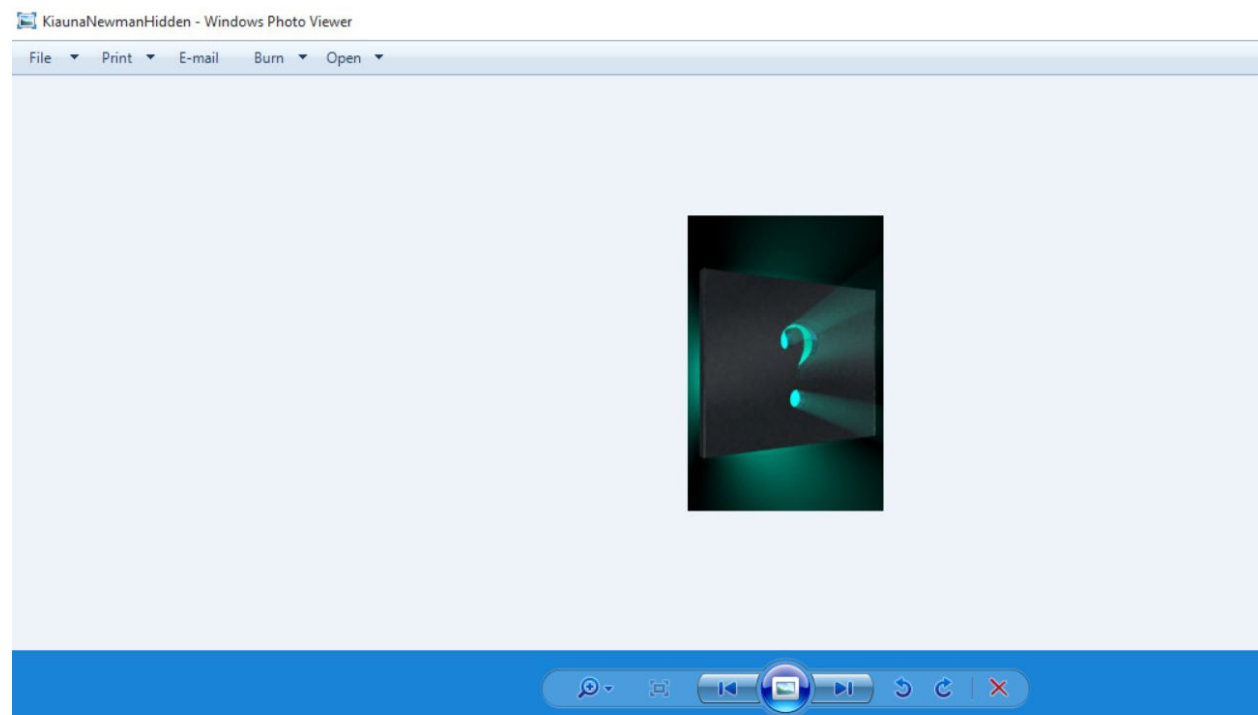
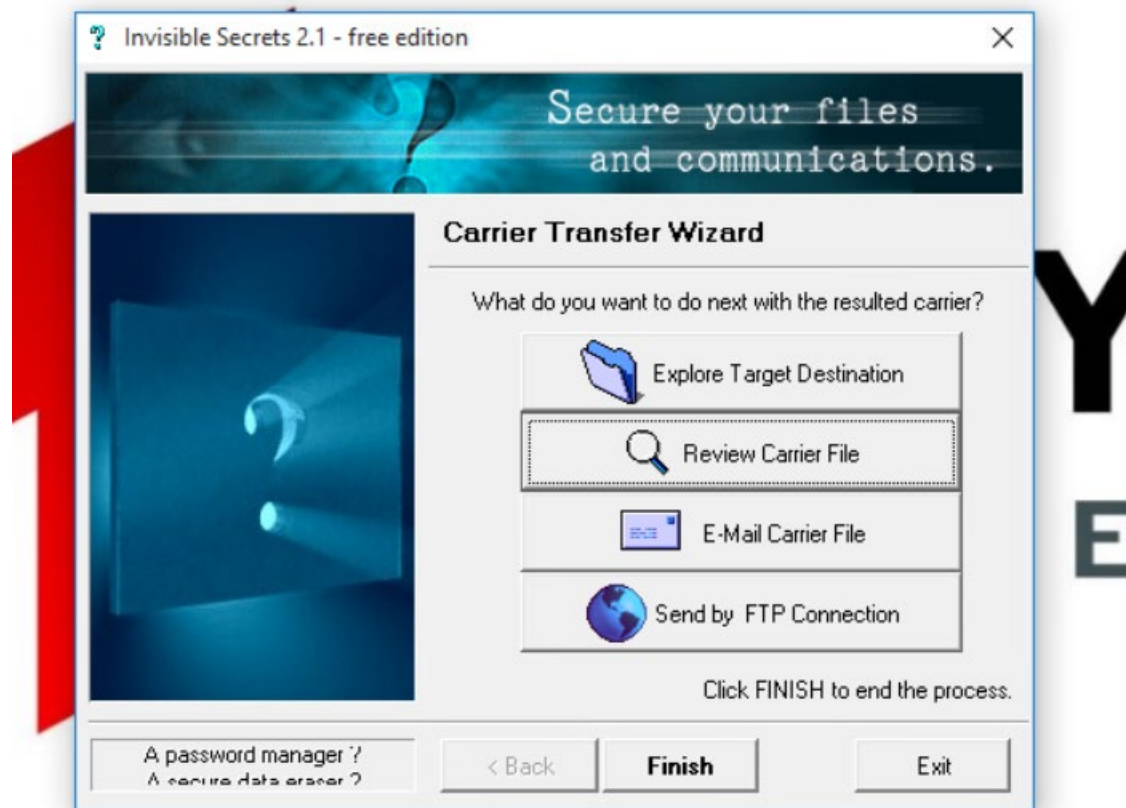
17.1 Digital Watermarking

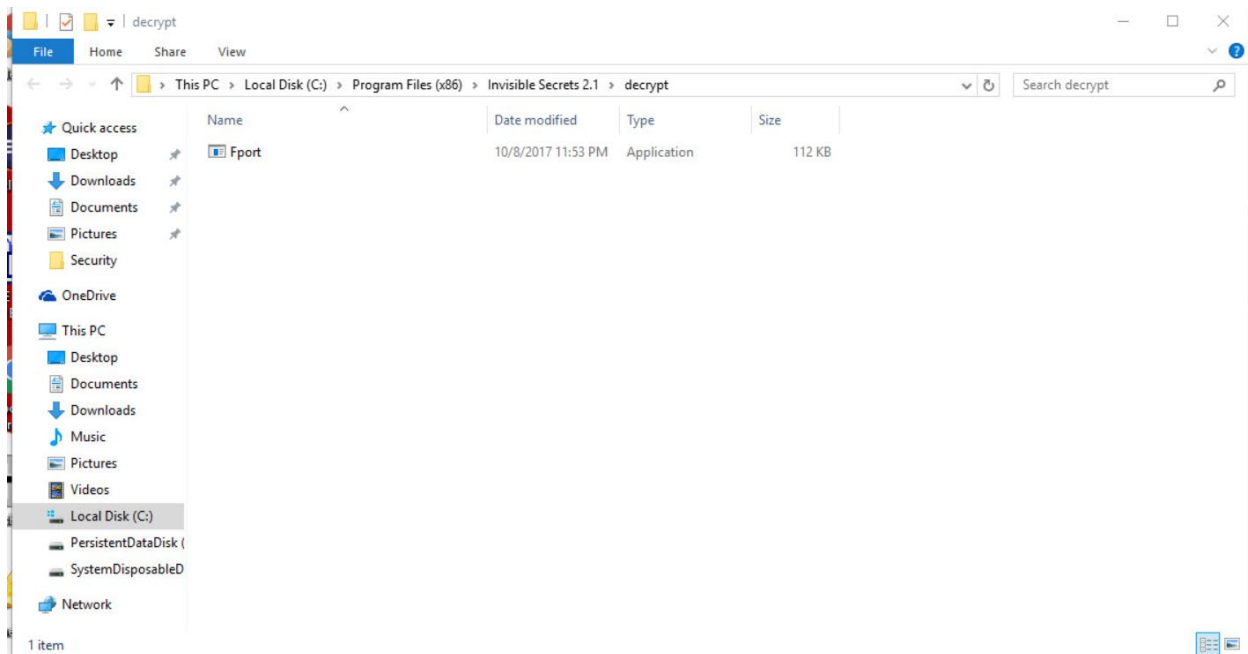
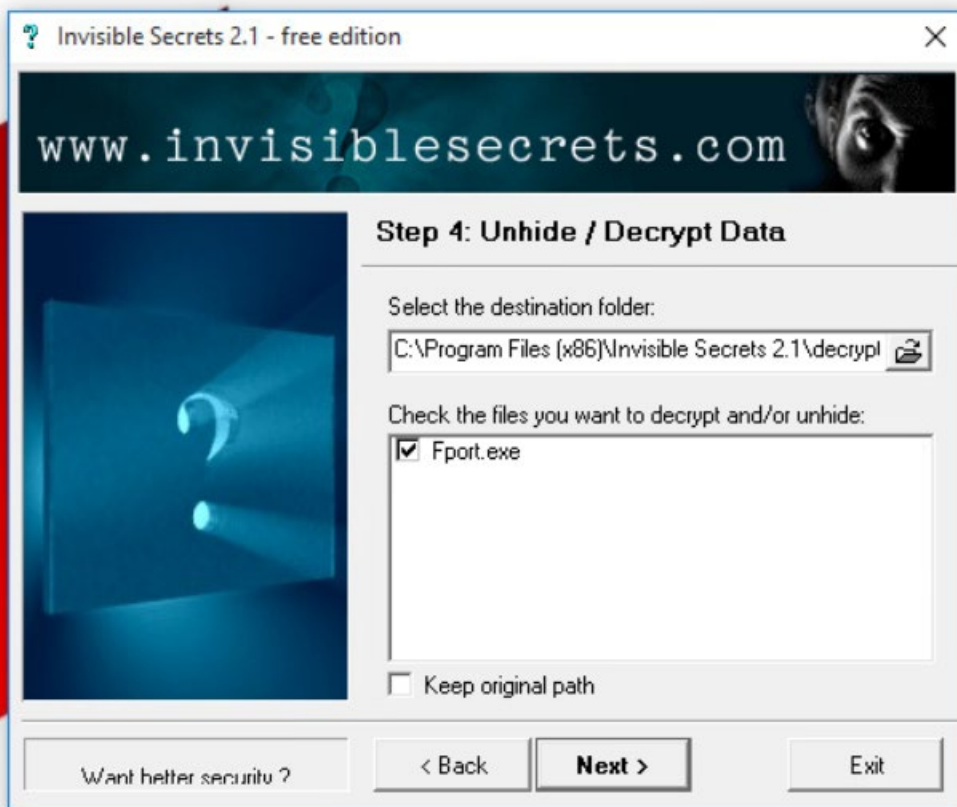




17.2 Invisible Secrets







17.3 StegDetect

