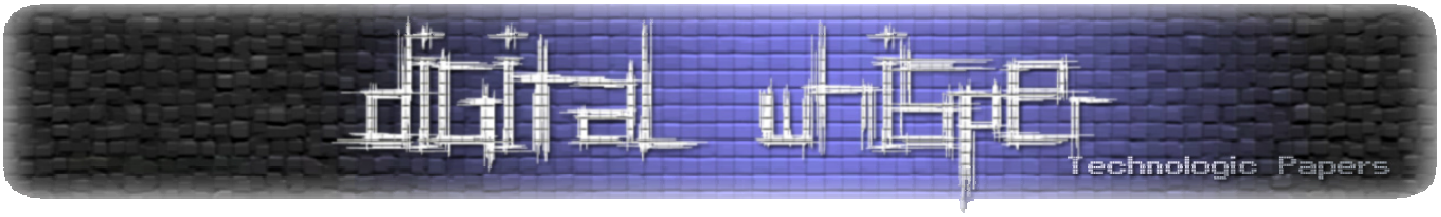


הפסקת קפה

מאת צבי קופר

אם אתה לא איש רשויות החוק או סוכן FBI לצורך העניין, סביר להניח כי לא תוכל לקבל קפה מחברת מיקרוסופט לצורך עבודתך...

רקע

Cofee, או בשמו המלא- **Computer Online Forensic Evidence Extractor**, הוא למעשה כלי למטרות Forensics או יותר נכון טרום Forensics למערכות מבוססות Windows שפותח ע"י מיקרוסופט ומופץ דרך NW3C (National White Collar Crime Center). הכלי מיועד לסייע לאנשי רשויות החוק לבצע איסוף נתונים מהיר ONLINE בזירת הפשע. התהליך מתוכנן לרוץ על גבי מדיה נתיקה ובמינימום מעורבות של החוקר. כלומר, החוקר מגיע לזירת הפשע, מחבר את ה-DOK שהוכן מראש. הכלי רץ על התחנה החשודה בצורה אוטומטית, אוסף את המידע הרלוונטי ושומר אותו על גבי ה-DOK. צורת העבודה יעילה ופשוטה ואמורה לספק יכולת איסוף נתונים קריטיים גם לאנשי חוק ללא רקע טכנולוגי מעמיק.

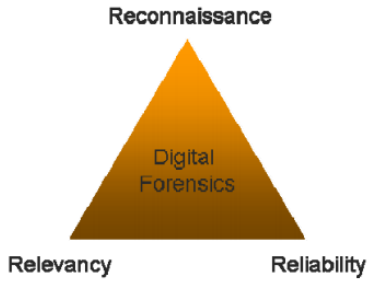
בשנה האחרונה הסתובבו ברשת שמועות רבות סביב הכלי החסוי והסודי הזה שדלף לרשת בחודשים האחרונים ואף הספיק להכתב לו כלי אנטי-פורנזי בשם **DECAF** שיוצרו קיבל "המלצה" מהאינטרפול להורידו מהרשת ואכן האתר ירד לכמה חדשים אך בדצמבר 2009 הוא חזר לפעילות.

במאמר זה אתאר את יכולתיו של הכלי וכיצד הם מיושמים בו .

ONLINE FORENSICS – על קצה קצה המזלג.

אחת הבעיות הגדולות בחקירה פורנזית היא איבוד הנתונים הפוטנציאלי שעלול להתרחש כתוצאה מכיבוי המחשב וניתוקו. נתונים כגון: **תהליכים המוטענים לזיכרון, נתוני רשת, קבצים פתוחים, שיתופים וגישות למחשבים מרוחקים, תוכנות התקשרות הפועלות ברקע, הצפנות, שמות משתמשים, שירותים מופעלים, נתוני גלישה, DNS, טבלאות ניתוב, מידע הנשמר בקבצים זמניים**, כל אלה הם "הלחם והחמאה" של החוקר הפורנזי והסיכון באיבודם גבוה עד וודאי בניתוק המחשב מהחשמל והרשת.

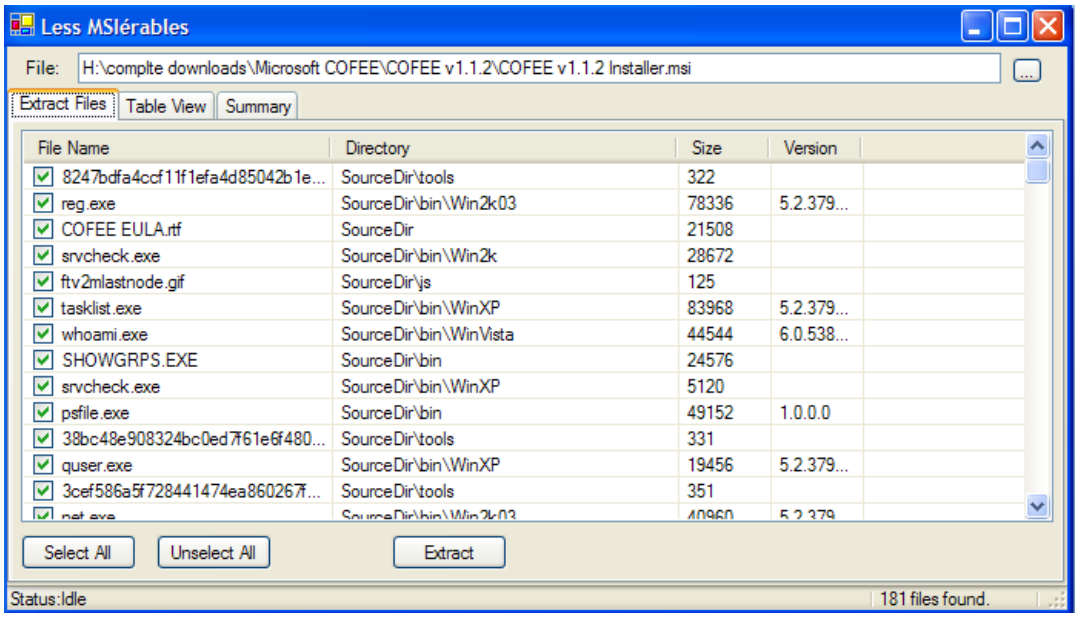
נושא חשוב נוסף הינו המשולש הפורנזי.



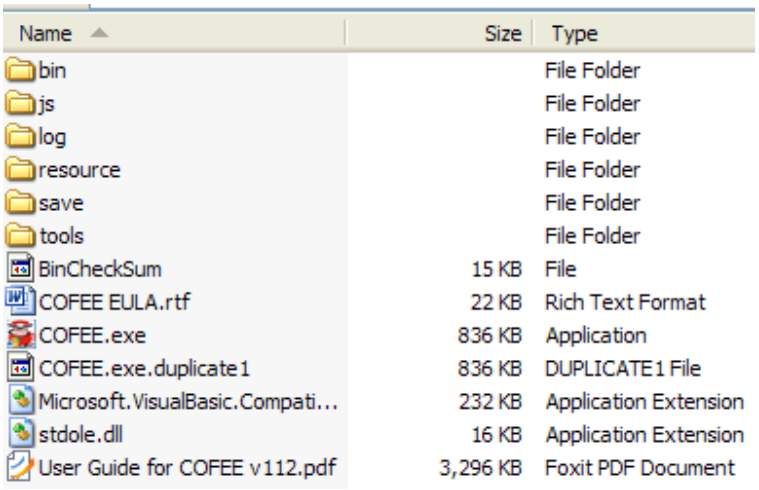
המטרה היא לשמור על איזון בין איסוף כמות רבה של נתונים, מידת הרלוונטיות של הממצאים לחקירה ומידת האמינות של החומר הנאסף. בנוסף תהליך איסוף הנתונים אמור לשאוף להשארת מינימום עקבות (FOOTPRINT) על האובייקט הנבדק וכן לאפשר מנגנון בקרה וחתימה המאשר כי הנתונים מהימנים ולא עברו על שינוי במהלך הבדיקה. העובדה שכלים כמו coffee משמשים לאיסוף נתונים ONLINE בסביבה לא מבוקרת ולעתים בידי ידיים לא מקצועיות, מחייבת את המפתחים לשמור על כללי המשולש ביתר שאת.

בואו נצלול לפרטים הטכניים:

ההתקנה המתגלגלת ברשתות שיתוף הקבצים מגיעה כקובץ MSI אך לא ניתן להתקין אותו ישירות מסיבה לא ברורה ולכן נשתמש באחת מתוכנות ה-MSI EXTRACT ונחלץ את הקבצים לספריות בהתאמה.

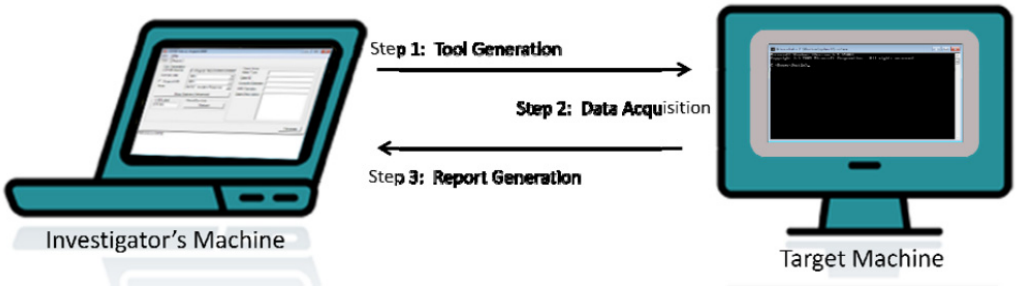


התוצאה שאמורה להתקבל היא מערך הספריות הבא:



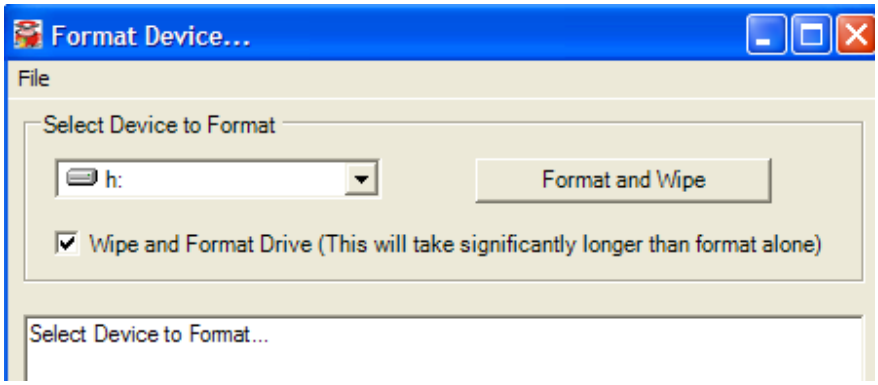
השימוש ב-COFEE מחולק לשלושה שלבים:

1. יצירת הכלי
2. איסוף המידע
3. יצירת הדו"ח



1. יצירת הכלי

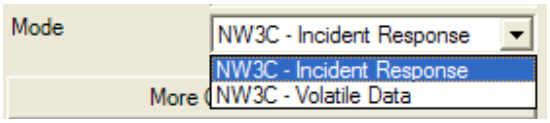
בשלב הראשון נכין מדיה נתיקה נקייה ללא חשש משיירי מידע קודמים – התוכנה מאפשרת מחיקה עמוקה (SDELETE-wipe) ופירמוט למדיה שנבחר. גודל המדיה המומלץ הוא לפחות 2GB והפירמוט הוא ל-fat32.



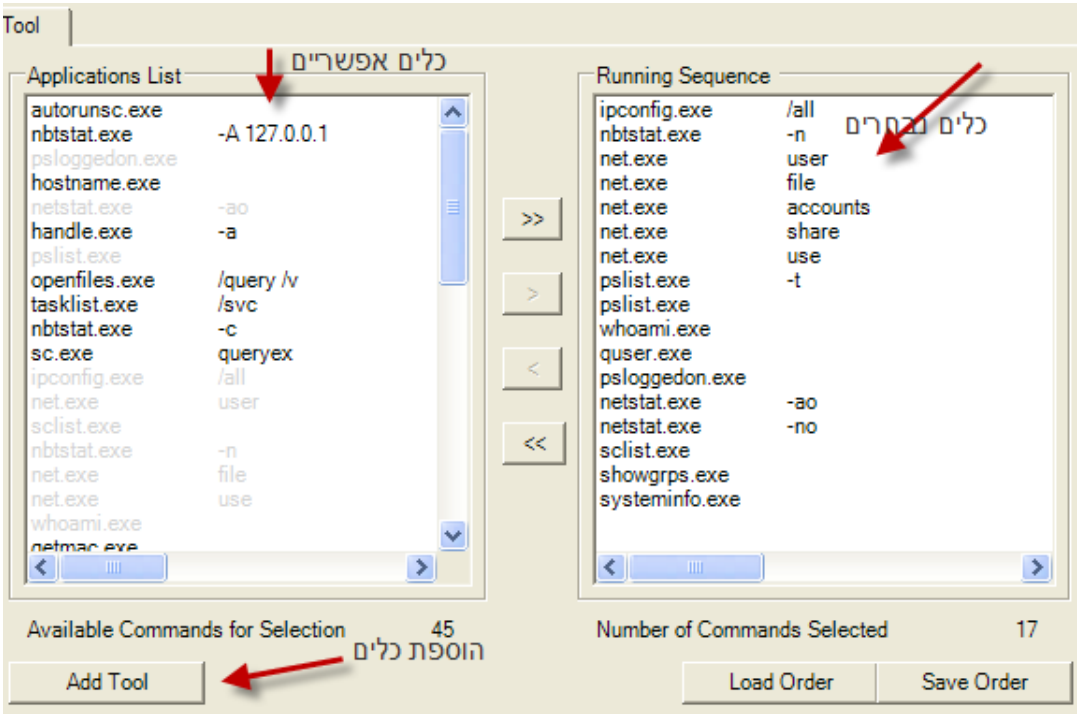

```
SDelete - Secure Delete v1.51
Copyright (C) 1999-2005 Mark Russinovich
Sysinternals - www.sysinternals.com

SDelete is set for 1 pass.
Cleaning free space on j:: 1%
```

לאחר שהכנו את ה-DOK, ניגש לבניית הכלי עצמו:

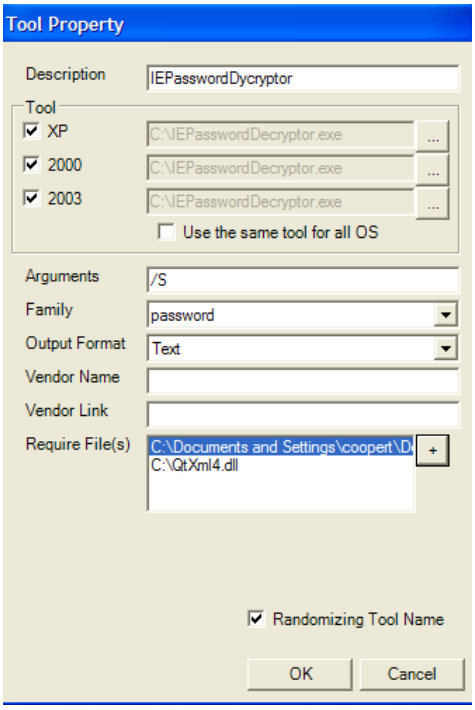
COFEE מגיע עם אוסף כלים המיועדים לאיסוף מידע ONLINE ומחולקים ל-2 פרופילים: incident response ו-volatile data. ההבדל בין הפרופילים הוא בכמות הפעולות שיופעלו על המחשב הנחקר כאשר incident response היא המעמיקה מביניהם .



בנוסף הכלי מאפשר הוספה והתאמה של כלים נוספים כולל הוספת פרמטרים וקבצי DLL הדרושים עבור ההרצה. כאן באמת אפשר "לחגוג" ולהוסיף כלים פיקנטיים. לשליפת ססמאות, צילומי מסך ועוד. אך יש כמובן לזכור כי הכלי מיועד לפעולה מהירה...



דוגמא לכלי שהוספתי לתיעוד סיסמאות מה-internet explorer:



התוכנה טוענת את הקבצים ומוסיפה אותם לרשימה האפשרית להרצה.

אוסף הכלים המגיעים עם COFEE מבוססים על כלי מיקרוסופט ידועים ופקודות מוכרות. הדבר עלול לגרום לחלק מהקוראים להרמת גבה אך יש לזכור כי הכוח כאן הוא בקיבוץ התוכניות תחת מנגנון אחד, יכולות ההרחבה שראינו והאוטומציה המלאה ONLINE.

כמו כן קיימות פקודות שונות המבצעות את אותה עבודה וזאת לצורך בדיקה השוואתית ואימות התוצאות המוצגות בד"ח הסופי.

היבט נוסף שנלקח בחשבון הינו האמינות המשפטית. כלומר, מהי הבדיקה שמתבצעת והאם הכלי עושה את מה שהוא אמור לעשות ולא דבר אחר? האם הפקודה משנה ערכים במחשב הניבדק? לצורך כך מיקרוסופט מספקת עם ההתקנה 200MB של מידע מפורט בקבצי EXCEL על פעילות הפקודות.

לדוגמא חלק מתיעוד הרצת קובץ at.exe:

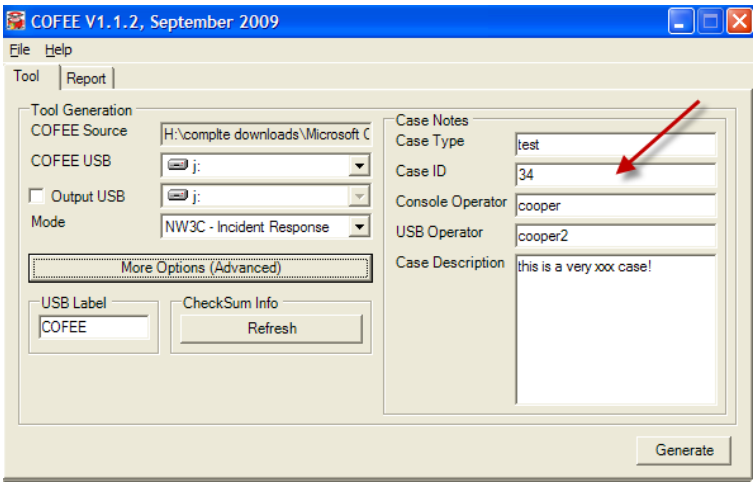
	A	B	C	D	E	F	
1	Time of Day	Process Name	PID	Operation	Path	Result	Detail
2	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c900000, Image Size: 0xb0000
3	52:26.0	at.exe	3336	CreateFile	C:\WINDOWS\Prefetch\AT.EXE-1891128A.pf	SUCCESS	Desired Access: Generic Read, Disposition: Ope
4	52:26.0	at.exe	3336	QueryStandardInformationFile	C:\WINDOWS\Prefetch\AT.EXE-1891128A.pf	SUCCESS	AllocationSize: 16,384, EndOfFile: 13,062, Numb
5	52:26.0	at.exe	3336	ReadFile	C:\WINDOWS\Prefetch\AT.EXE-1891128A.pf	SUCCESS	Offset: 0, Length: 13,062
6	52:26.0	at.exe	3336	CloseFile	C:\WINDOWS\Prefetch\AT.EXE-1891128A.pf	SUCCESS	
7	52:26.0	at.exe	3336	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\at.exe	NAME NOT FOUND	Desired Access: Read
8	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c800000, Image Size: 0xf4000
9	52:26.0	at.exe	3336	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
10	52:26.0	at.exe	3336	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
11	52:26.0	at.exe	3336	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
12	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c10000, Image Size: 0x58000
13	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77dd0000, Image Size: 0x90000
14	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e70000, Image Size: 0x91000
15	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\netapi32.dll	SUCCESS	Image Base: 0x5b860000, Image Size: 0x54000
16	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\shell32.dll	SUCCESS	Image Base: 0x7c9c0000, Image Size: 0x814000
17	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\qdi32.dll	SUCCESS	Image Base: 0x77f10000, Image Size: 0x46000
18	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x77d40000, Image Size: 0x90000
19	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\shlwapi.dll	SUCCESS	Image Base: 0x77f60000, Image Size: 0x76000
20	52:26.0	at.exe	3336	QueryOpen	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	CreationTime: 8/4/2004 12:56:46 AM, LastAccess
21	52:26.0	at.exe	3336	CreateFile	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize,
22	52:26.0	at.exe	3336	CreateFileMapping	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtect
23	52:26.0	at.exe	3336	CreateFileMapping	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	SyncType: SyncTypeOther
24	52:26.0	at.exe	3336	RegOpenKey	HKLM\System\CurrentControlSet\Control\SafeBoot\Option	NAME NOT FOUND	Desired Access: Query Value, Set Value
25	52:26.0	at.exe	3336	RegOpenKey	HKLM\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	Desired Access: Query Value
26	52:26.0	at.exe	3336	RegQueryValue	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1
27	52:26.0	at.exe	3336	RegCloseKey	HKLM\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers	SUCCESS	
28	52:26.0	at.exe	3336	RegOpenKey	HKCU\Software\Policies\Microsoft\Windows\Safer\CodeIdentifiers	NAME NOT FOUND	Desired Access: Query Value
29	52:26.0	at.exe	3336	CloseFile	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	
30	52:26.0	at.exe	3336	Load Image	C:\WINDOWS\system32\shlmenq.dll	SUCCESS	Image Base: 0x5cb70000, Image Size: 0x26000
31	52:26.0	at.exe	3336	CreateFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	Desired Access: Generic Read, Disposition: Ope
32	52:26.0	at.exe	3336	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1,191,936, EndOfFile: 1,190,796,
33	52:26.0	at.exe	3336	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeCreateSection, PageProtect
34	52:26.0	at.exe	3336	QueryStandardInformationFile	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	AllocationSize: 1,191,936, EndOfFile: 1,190,796,
35	52:26.0	at.exe	3336	CreateFileMapping	C:\WINDOWS\AppPatch\sysmain.sdb	SUCCESS	SyncType: SyncTypeOther

להלן כמה מקבצי ההרצה והפקודות המגיעות עם coffee:

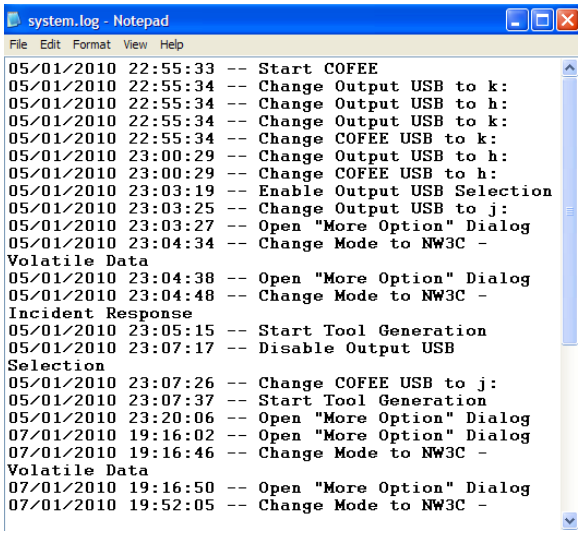
1. Arp –a תיעוד כתובת ה-MAC של התחנה.
2. autorunsc.exe – תיעוד התוכנות העולות אוטומטית באתחול התחנה.
3. handle.exe -a –תיעוד הגישה של תהליכים פתוחים לקבצים, רשומות PORTS REG ועוד.
4. getmac.exe – תיעוד נוסף של כתובות ה-MAC בתחנה (מפורט יותר מ-arp ומקיף את כל התקני הרשת).
5. at.exe – תיעוד משימות מתוזמנות במערכת.
6. Ipconfig /all – תיעוד כתובות ה-GATEWAY IP DHCP וכו'.
7. Hostname- תיעוד שם התחנה.
8. msinfo32.exe –תיעוד פרטי מערכת רבים.
9. psloggedon.exe- תיעוד שמות משתמשים ב-LOGON מקומי ומרוחק דרך שיתופים.
10. netstat –ao – תיעוד פורטים והתקשרויות ברשת + קישור התחברות לתוכנה ספציפית בתחנה (PID).
11. pslist.exe – תיעוד תהליכים (processes) המוטענים לזיכרון.
12. openfiles.exe /query /v- תיעוד קבצים פתוחים מקומית ועל גבי שיתופים מרוחקים.
13. Taskkist.exe /svc – תיעוד נוסף של processes אך עם יכולת לראות תת פרוססים

14. Nbtstat.exe -c- תיעוד טבלאות NetBIOS בתחנה הכוללים שמות תחנות מרוחקות וכתובת ה-IP שלהם.
15. Sc.exe queryex – תיעוד השירותים הרצים על התחנה (במצב running).
16. net user- תיעוד שמות משתמש בתחנה.
17. Net file- תיעוד נוסף של קבצים פתוחים.
18. Net use- תיעוד מיפויי כוננים מקומיים ומרוחקים.
19. Net view – שיתופים פתוחים עם אפשרות לראות את כל השיתופים הפתוחים ב-DOMAIN.
20. Net localgroup – תיעוד קבוצות security מקומיות על התחנה.
21. Net localgroup administrators- תיעוד שמות המשתמשים החברים בקבוצת האדמין המקומי.
22. net session – תיעוד ה-sessions הפתוחים הקיימים כרגע על התחנה.
23. SHOWGRPS.EXE – תיעוד נוסף של חברות המשתמש הפעיל בקבוצות.
24. SCLIST.EXE – ע"ע 15.
25. Whoami.exe – זיהוי נוסף של שם המשתמש הנמצא ב-LOGIN.
26. Pstat.exe- תיעוד מידע נוסף ומפורט על PROCCESS הרצים במערכת, הדגש כאן הוא על ה-DRIVERS הפועלים במערכת (מצויין בסוף שורת הפלט)
27. uptime.exe – תיעוד זמן המערכת מה-RESTART האחרון.
28. route print – תיעוד טבלאות הניתוב.

לאחר שבחרנו כלים רצויים והוספנו כלים משלנו, כל שנותר לעשות הוא למלא את פרטי המקרה (CASE) שם החוקר, הערות וכו', ולייצר את ה-DOK הסופי שלנו.

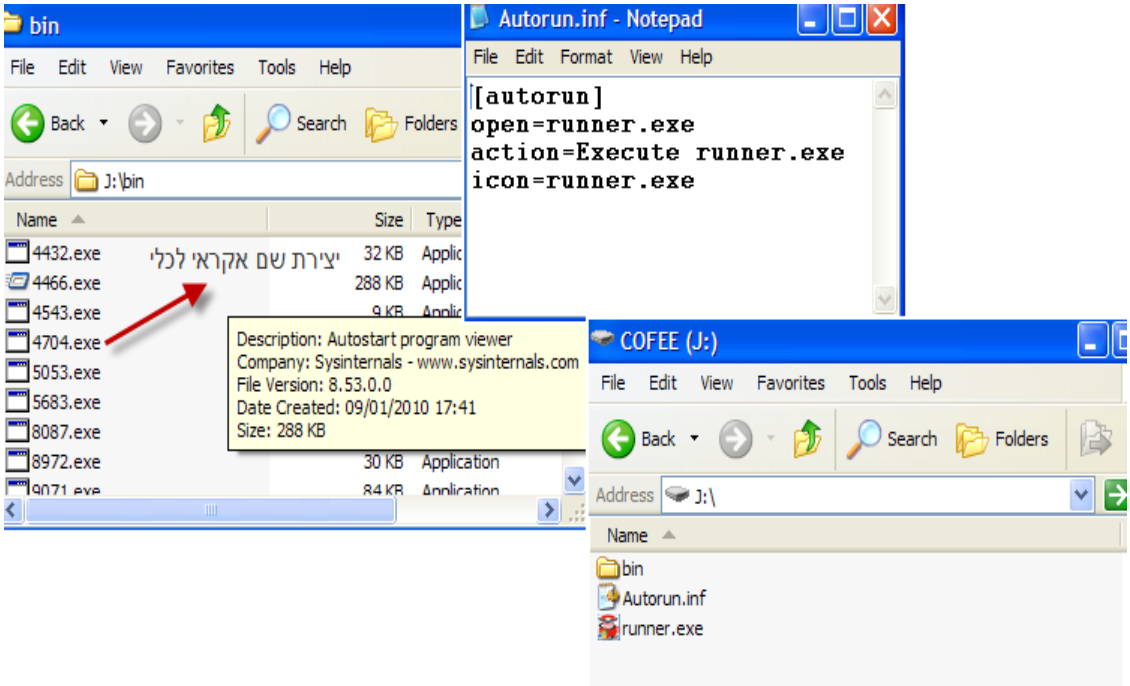


רגע לפני יצירת ה-DOK אציין כי קיים קובץ LOG לכל הפעולות הנעשות בכלי (כראוי).

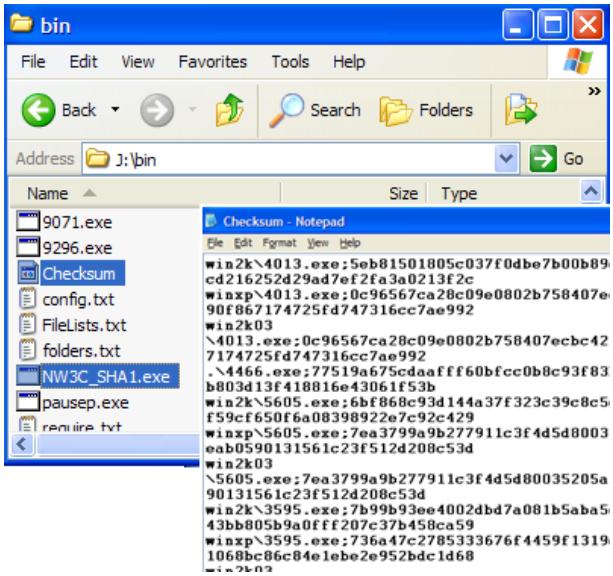


זהו. אם עשינו הכל נכון, נקבל DOK מוכן המשתמש בפונקצית ה-AUTORUN לצורך הרצה אוטומטית.

התוצאה נראית ככה:

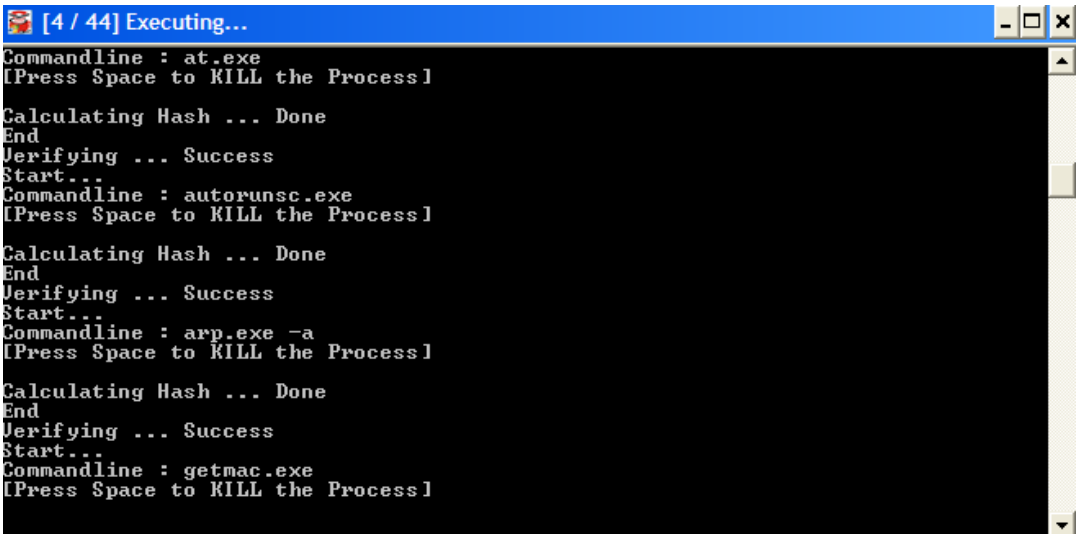


כמובן לא נתעלם מה-checksum המוודא כי תכולת ה DOK לא תשתנה:

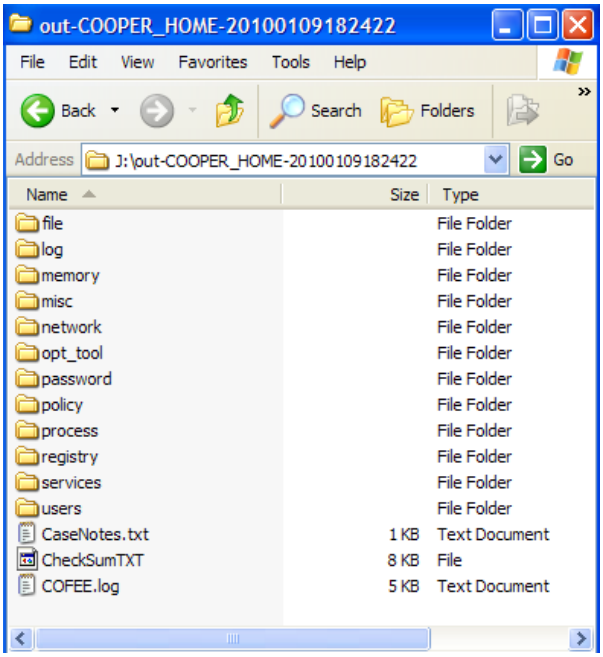


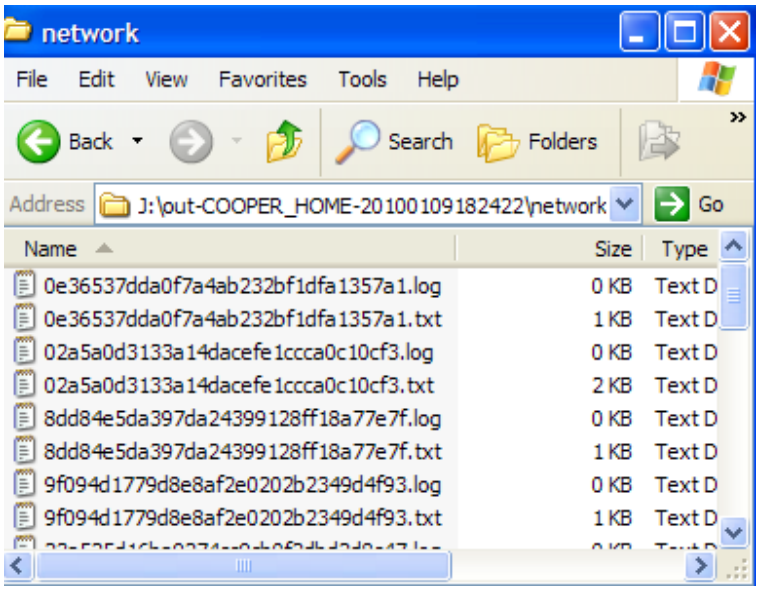
2. איסוף המידע

כאשר נחבר את ה-DOK לתחנה החשודה, הכלי יטען דרך ה-AUTORUN. במידה ופונקציה זו מבוטלת בתחנה, נאלץ להריץ את ה-RUNNER ידנית. הכלים ירוצו אחד אחרי השני כאשר קיימת אפשרות לבצע KILL לכלי ולעבור לכלי הבא. כמו כן מתבצע HASH על כל תוצאה שמתקבלת.



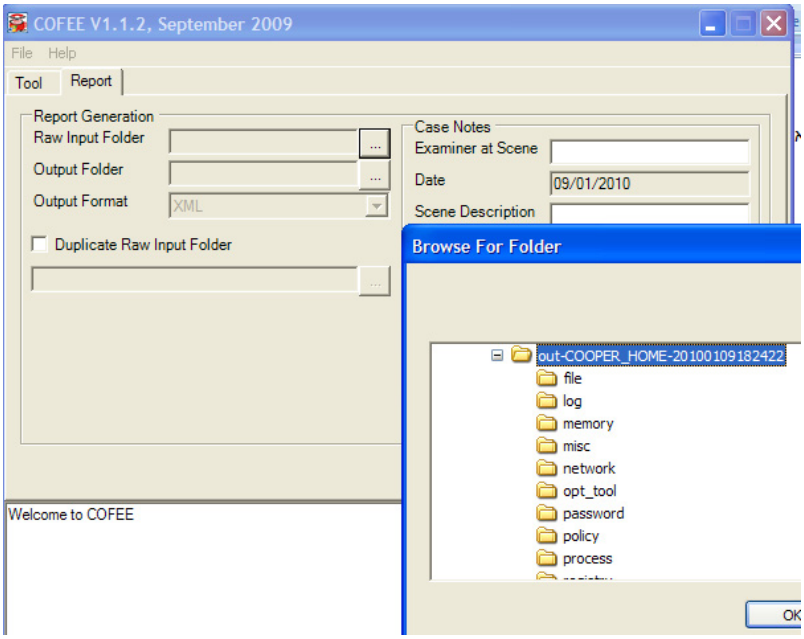
התוצאות נשמרות על ה-DOK ומחולקות לתיקיות לפי נושא הבדיקה כאשר שמות הקבצים הם ה-HASH המחושב בסוף הבדיקה. קיים לוג נוסף המתעד את פעילות הכלים.



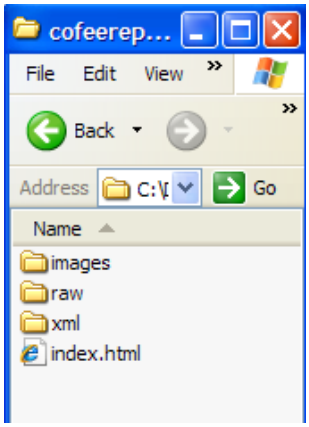


3. יצירת הדוח

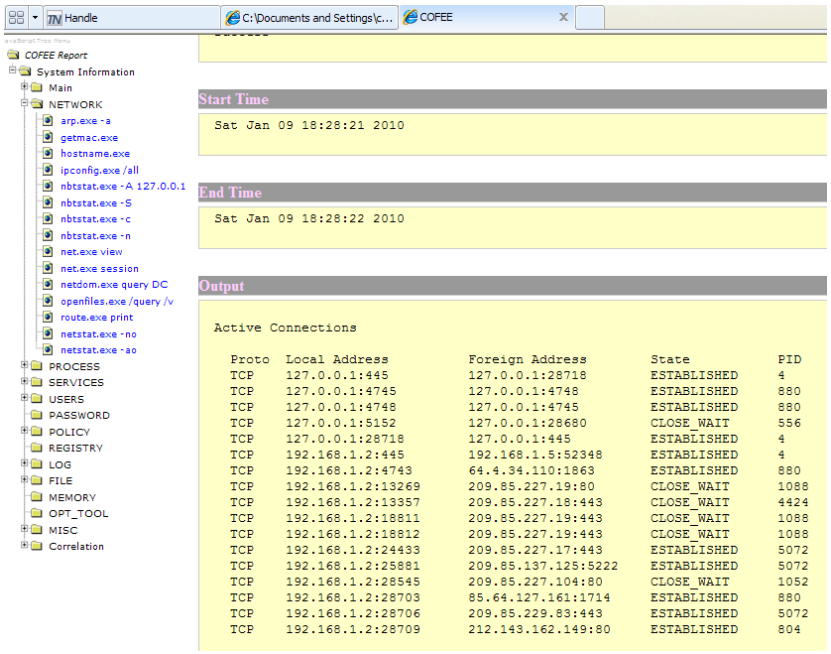
סיימנו עם איסוף הנתונים, כעת ניתן לנתק את ה-DOK ולטעון את הקבצים בעמדת העבודה :



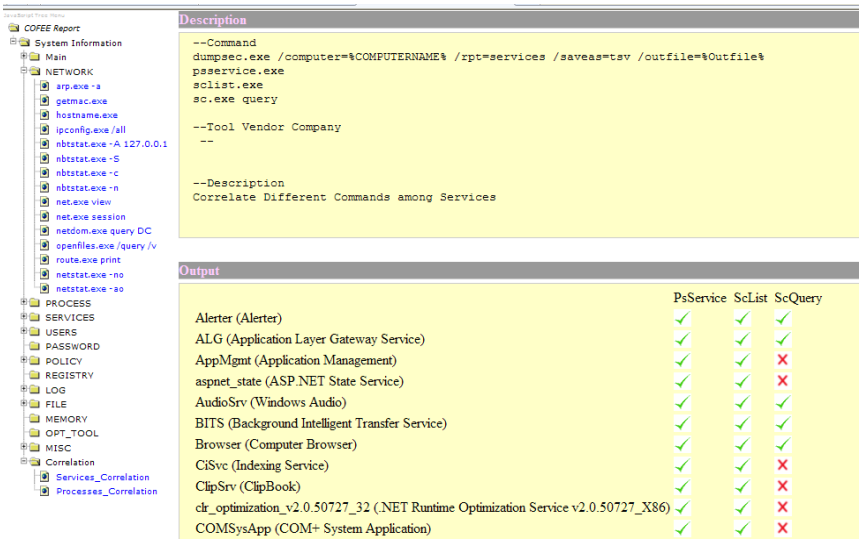
נבחר ספריה מקומית לשמירת הדו"ח, נבצע GENERATE – ה-checksum יבדק ותחל המרת הקבצים ל-XML. בסיום התהליך יווצרו הקבצים והתיקיות הבאים:



התוצאה הסופית שמתקבלת היא דו"ח HTML מפורט ומסודר לפי קטגוריות :



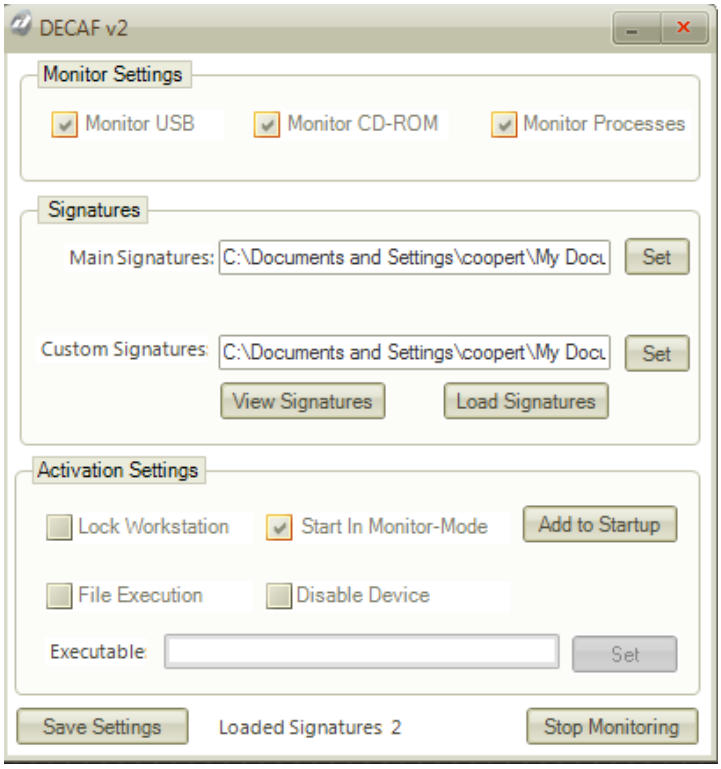
שימו לב לרובריקת ה-correlation אשר מציגה נתונים השוואתיים בין כלים שונים המבצעים אותה עבודה וזאת לצורך אימות נתונים נוסף.

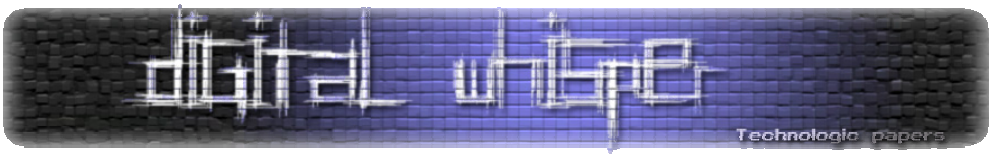


לא רע ל-10 דקות עבודה, לא?

Coffee and more anti forensic tool-DECAF

נכון לזמן פרסום מאמר זה, פורסמה גרסה שניה לכלי שאמור לזהות חיבור coffee לתחנה ולנטרלו. נכון לעת כתיבת שורות אלו, לא הצלחתי לגרום ל-decaf לזהות את coffee למרות כל הנסיונות, המתכנת אכן רשם באתר כי קיימות שגיאות בקוד והוא עובד עליהם לגרסה הבאה... כנראה שבשלב זה נמשיך לקבל את הגרסה רבת הקפאין...:)





לסיכום

דיברנו קצת על ONLINE FORENSICS ועל הצרכים המיוחדים הדרושים לעבודה זו. ניתחנו לעומק כלי פשוט ויעיל, ובעל יכולות הרחבה השומר ככל שניתן על המשולש הפורנזי ועובד by the book בכל שלב ושלב על מנת לשמר את האיזון בין הכמות, הרלוונטיות והאמינות של הנתונים.

"The debate isn't security versus privacy. It's liberty versus control." –ברוס שנייר

לקריאה נוספת:

- http://news.cnet.com/8301-10789_3-9932600-57.html
- http://www.interpol.int/public/ICPO/PressReleases/PR2009/PR200937.asp
- https://cofee.nw3c.org/
- DECAF - http://www.decafme.org/

כלים ללינוקס:

- http://www.securityfocus.com/infocus/1503