An alternative to COFEE

AN INTRODUCTION TO T.E.A.

A some-what sophisticated Batch file created by M. SOUTHBY to help automate the collection and analysis of forensic evidence on a live machine.

2012-12-21

DISCLAIMER: Warning, ETC

- As this tool is intended for LAW ENFORCEMENT ONLY, it should be treated much in the same way other investigative tools are treated. Please do no publish this on the internet.
- This tool was designed for my own personal use, I can explain what it does. Validate it prior to use and use at your own risk.
- I'd prefer that it is not modified and taken credit for. Give credit where credit is due, however if you are going to learn from it and make it better I'm not going to stop you.
- Please do no distribute or provide copies without permission. I am trying to keep track of who has it incase an issue comes up and I need to notify users of problems or critical updates.

M. SOUTHBY Who?

"He's just this guy, you know?" – Hitchhikers guide to the Galaxy

- I'm a lowly Tech Crime Investigator who focuses on learning Live Forensics and Critical Infrastructure Forensics.
- I have been with LE since 2006 and doing Tech Crime Unit things since 2009.
- I'm A+ Certified!
  (I may have a bit of other training too)

Contact Information

Fire off a quick email to let me know you have this tool and would like to be notified of any updates.

mark.southby@rcmp-grc.gc.ca

TEA, earl grey, hot.

- Back when COFEE was slated to come out, I was told it would be a batch file which could be easily explained if required. It would also automatically detect which windows was running and work.
- It didn't. At least not the version we had to sacrifice our young in order to obtain.
  It was failing at search scenes on 64 bit systems and this was unacceptable.

Technical Evidence Acquisition

A little history first…

- With no fixes at that time (the problem I believe has since been solves), I decided to create a simple batch file to automate some basic tools to assist in gathering pertinent information on Live computer systems prior to them being shut down.

- This soon turned into a sophisticated batch file. More so for my own understanding of command line and personal use, however I tried to keep it simple enough for other investigators to use if the so desired.

Technical Evidence Acquisition

The Good…

- The main benefit over the older COFEE are:
- TEA can detect windows XP or Vista/7 operating systems. It can also detect 32bit / 64bit architecture.
- It hashes it output / reports which can be verified.
- It is extremely light weight both for configuring and running.
- It can be 'autorun' using HMI Automation (more on this later)

Technical Evidence Acquisition

The Bad…

- The main Detriment over COFEE are:
- You can't change the order of when tools are run with out editing the batch, which is complicated.
- You can't simply add new tools with out editing the batch, which is complicated.
- I haven't implemented a simple way for grabbing updated hash values of legitimate Microsoft Operating system files for new OS versions and service packs.

Technical Evidence Acquisition

The Ugly

- As the file is the source code, it makes it easy to be manipulated. This could be good, or bad depending on your stance.
- I suppose I need to find a way to maintain an inform people of updates, for now this is only a proof of concept 'prototype' batch file distributed to a few LE personnel. You can contact me directly if you need updates or have any issues / suggestions.

Technical Evidence Acquisition

The Future

- I hope one day to have enough time to re-do this program in a proper programming language and host updates from a secure site.
- I hope to also complete my HMI (Human Interface) Automation device which would have a screen with a menu and work as a stand alone incident response device. However my mentor on this project has relocated so I have no immediate plans to continue development.

Technical Evidence Acquisition

How it works:

- Obtain a clean USB Storage Device larger than your suspected targets memory capacity. External Hard Drive is preferred.
- Format as NTFS and Name said device to “TEA”. This is important as HMI devices, and future scripts will require this.

Technical Evidence Acquisition

How it works:

- Copy the folder "TEA _1.0.121221b" to your USB device and rename the folder to "TEA"

NOTE: The last set of numbers on the original folder is the version. It is the date the batch was last updates, followed by a letter denoting the iteration for that day.

So in this example: 2012-Dec-21
second update for the day.

Technical Evidence Acquisition

How it works:

- Run "BREW" to prepare "TEA" on your USB device for the system you wish to acquire.

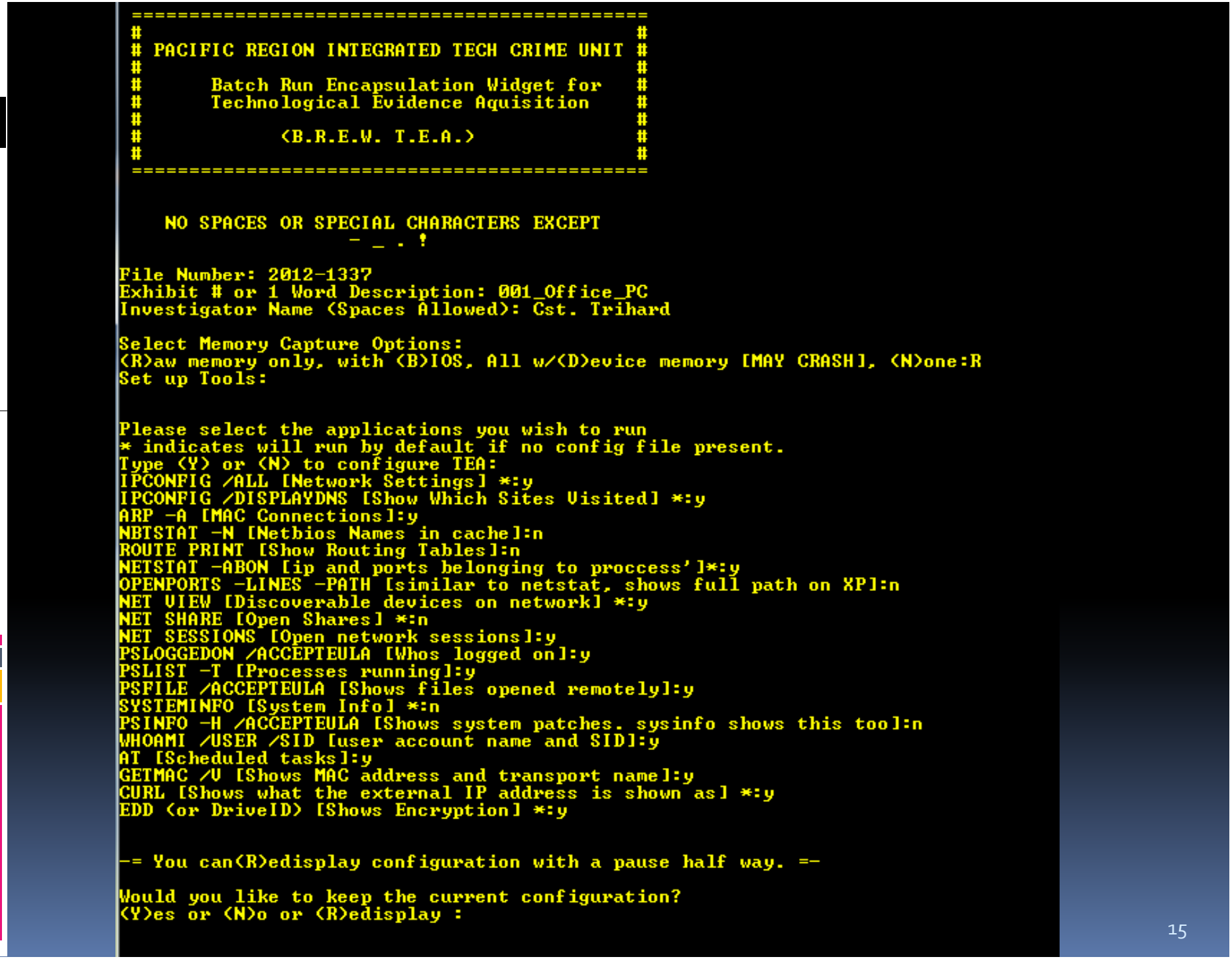
  BREW = "Batch Run Encapsulation Widget"

- This allows you to configure the file number, exhibit number, Investigating Officer, and which tools you wish to run.

Technical Evidence Acquisition

How it works:

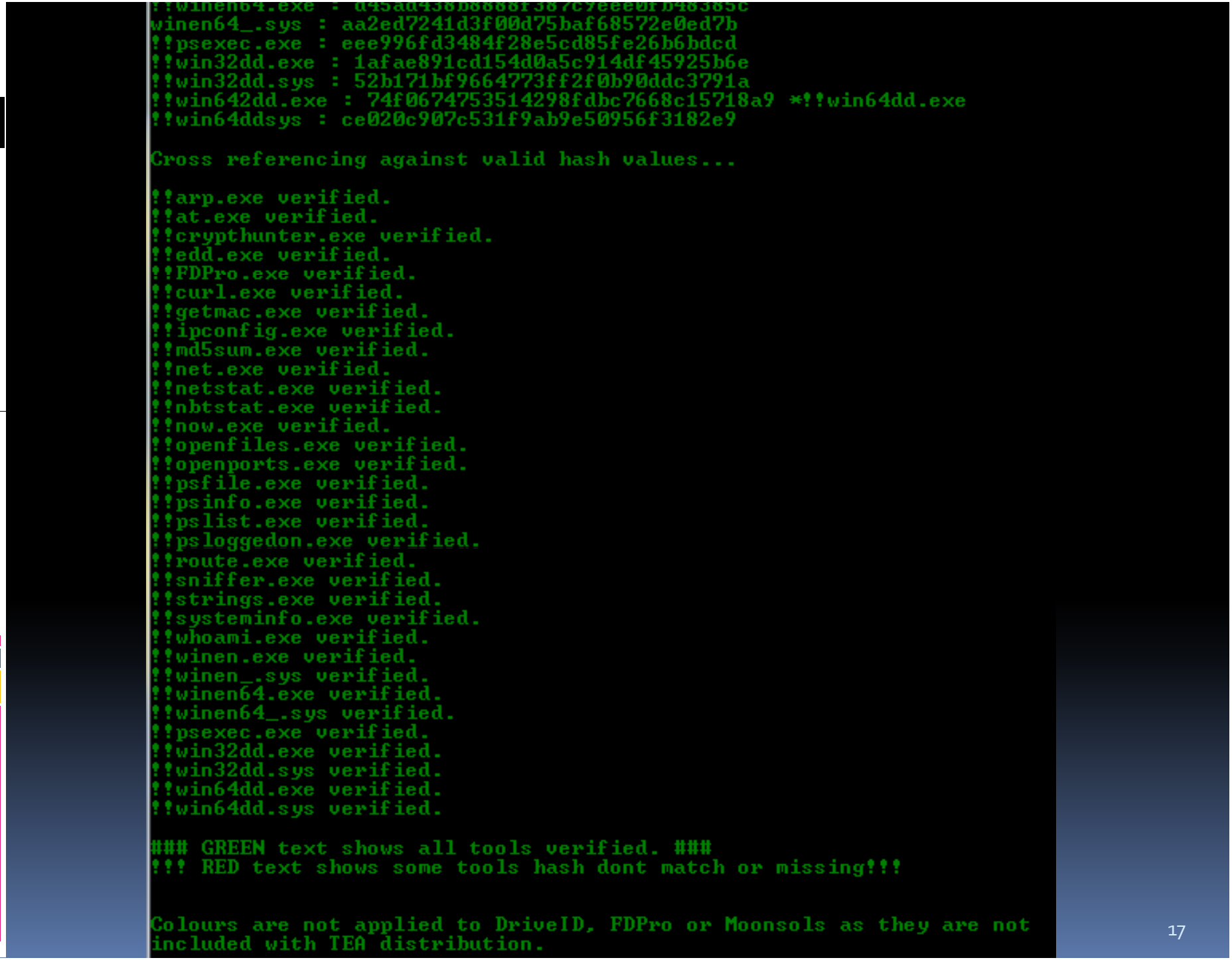
- READ THE ONSCREEN PROMPTS CAREFULLY!
- Putting in spaces or special characters when told not to will break it, format your drive and get you pregnant. I have not spent the time doing error checking for every possible idiotic entry. This is not the time to get creative with your answers!
- You've been warned.


PACIFIC REGION INTEGRATED TECH CRIME UNIT
Batch Run Encapsulation Widget for
Technological Evidence Aquisition
(B.R.E.W. T.E.A.)
NO SPACES OR SPECIAL CHARACTERS EXCEPT
- _ . !
File Number: 2012-1337
Exhibit # or 1 Word Description: 001_Office_PC
Investigator Name (Spaces Allowed): Cst. Trihard
Select Memory Capture Options:
(R)aw memory only, with (B)IOS, All w/(D)evice memory [MAY CRASH], (N)one:R
Set up Tools:
Please select the applications you wish to run
* indicates will run by default if no config file present.
Type (Y) or (N) to configure TEA:
IPCONFIG /ALL [Network Settings] *:y
IPCONFIG /DISPLAYDNS [Show Which Sites Visited] *:y
ARP -A [MAC Connections]:y
NBTSTAT -N [Netbios Names in cache]:n
ROUTE PRINT [Show Routing Tables]:n
NETSTAT -ABON [ip and ports belonging to proccess']*:y
OPENPORTS -LINES -PATH [similar to netstat, shows full path on XP]:n
NET VIEW [Discoverable devices on network] *:y
NET SHARE [Open Shares] *:n
NET SESSIONS [Open network sessions]:y
PSLOGGEDON /ACCEPTEULA [Whos logged on]:y
PSLIST -T [Processes running]:y
PSFILE /ACCEPTEULA [Shows files opened remotely]:y
SYSTEMINFO [System Info] *:n
PSINFO -H /ACCEPTEULA [Shows system patches. sysinfo shows this too]:n
WHOAMI /USER /SID [user account name and SID]:y
AT [Scheduled tasks]:y
GETMAC /V [Shows MAC address and transport name]:y
CURL [Shows what the external IP address is shown as] *:y
EDD (or DriveID) [Shows Encryption] *:y
-= You can(R)edisplay configuration with a pause half way. =-
Would you like to keep the current configuration?
(Y)es or (N)o or (R)edisplay :

Technical Evidence Acquisition

How it works:

- Once you have accepted your configuration, the tools proceeds to verify your tool set with known MD5 hashes.
- All tools have been renamed to have a dual ! Prefix. This is to ensure the tools on the USB device \TEA folder are run as apposed to local tools that may be compromised that are found in the %path% of the operating system.
- For example: ipconfig


!!winen64.exe : d45ad438b8888f387c7eee0fb48385c
winen64_.sys : aa2ed7241d3f00d75baf68572e0ed7b
!!psexec.exe : eee996fd3484f28e5cd85fe26b6bdcd
!!win32dd.exe : 1afae891cd154d0a5c914df45925b6e
!!win32dd.sys : 52b171bf9664773ff2f0b90ddc3791a
!!win642dd.exe : 74f0674753514298fdbc7668c15718a9 *!!win64dd.exe
!!win64ddsys : ce020c907c531f9ab9e50956f3182e9
Cross referencing against valid hash values...
!!arp.exe verified.
!!at.exe verified.
!!crypthunter.exe verified.
!!edd.exe verified.
!!FDPro.exe verified.
!!curl.exe verified.
!!getmac.exe verified.
!!ipconfig.exe verified.
!!md5sum.exe verified.
!!net.exe verified.
!!netstat.exe verified.
!!nbtstat.exe verified.
!!now.exe verified.
!!openfiles.exe verified.
!!openports.exe verified.
!!psfile.exe verified.
!!psinfo.exe verified.
!!pslist.exe verified.
!!psloggedon.exe verified.
!!route.exe verified.
!!sniffer.exe verified.
!!strings.exe verified.
!!systeminfo.exe verified.
!!whoami.exe verified.
!!winen.exe verified.
!!winen_.sys verified.
!!winen64.exe verified.
!!winen64_.sys verified.
!!psexec.exe verified.
!!win32dd.exe verified.
!!win32dd.sys verified.
!!win64dd.exe verified.
!!win64dd.sys verified.
GREEN text shows all tools verified.
!!! RED text shows some tools hash dont match or missing!!!
Colours are not applied to DriveID, FDPro or Moonsols as they are not
included with TEA distribution.

Technical Evidence Acquisition

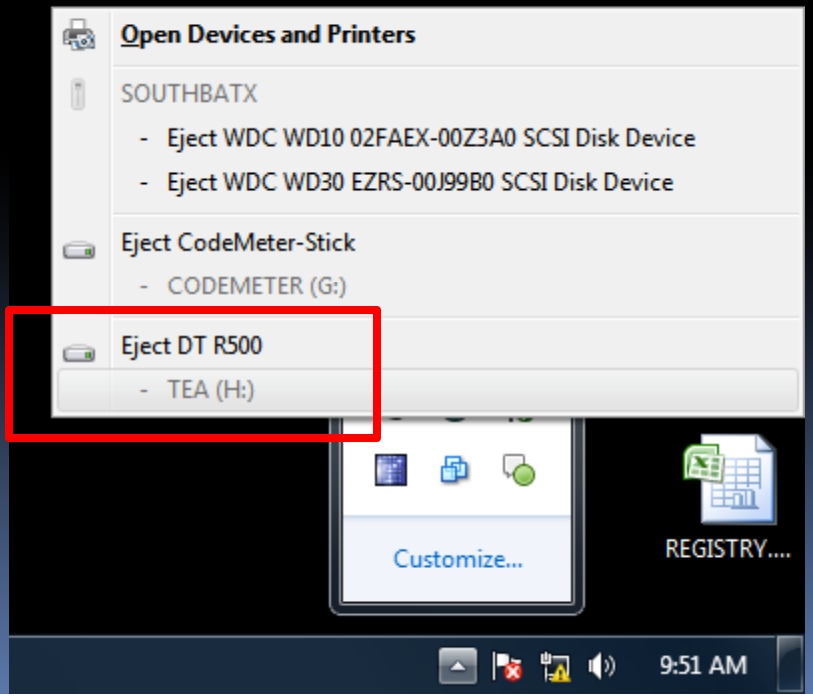
How it works:

- BREW has now generated the tea.cfg file.
- Now the device is ready to be plugged into the target system.

Technical Evidence Acquisition

How it works:

- Note the drive letter assigned to the USB device.



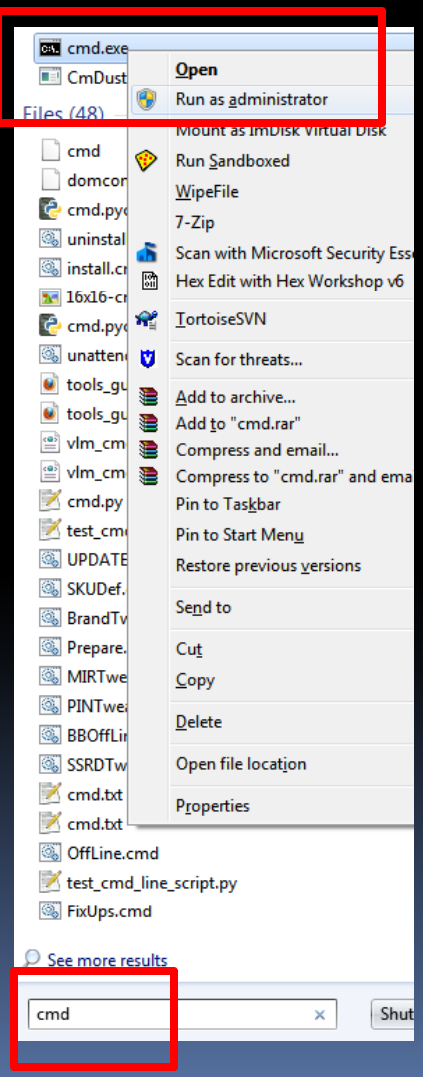
Technical Evidence Acquisition

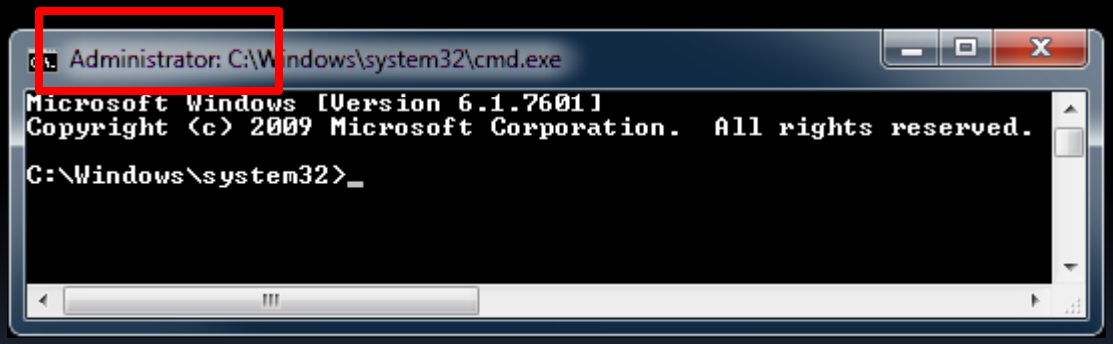
How it works:

- Open up a command prompt as the administrator.
- In Windows 7 this is relatively simple:
  - Press Windows Key
  - Type "**cmd**"
  - Right click and select "**run as administrator**"
  - Make sure the CLI window has "**Administrator:**" in the title.

Technical Evidence Acquisition

How it works:





Technical Evidence Acquisition

How it works:

- Navigate to the USB device drive letter noted in the previous step
- Change directory to **TEA**
- Run **TEA**

```
C:\Users\msouthby>h:

H:\>cd tea

H:\TEA>tea
```

Technical Evidence Acquisition

Things didn't go as planned!

- If things didn't go as expected, try Man_Tea.
- This will allow you to generate a new file number, exhibit number, investigator name and most importantly, allow you to change your memory capture options while still using the other configured tools in the tea.cfg file.

Technical Evidence Acquisition

Things didn't go as planned!

- If for some reason your config file is missing and you don't want to run BREW, both TEA and Man_Tea will give you the option to run a set of default tools.
- Memory capture is not included in this!

Technical Evidence Acquisition

Things didn't go as planned!

```
   PACIFIC REGION INTEGRATED TECH CRIME UNIT

        Technological Evidence Aquisition
                   (T.E.A.)

              Checking Configuration...
No config file found. Would you like to run default tools?
[IPCONFIG, NETSTAT, NET SHARE, NET VIEW, SYSTEMINFO, GET EXTERNAL IP, CHECK for ENCRYPTION]
(Y)es or (N)o:n


NO CONFIG FILE FOUND, please run BREW
(Recommended running on analysis machine not target!)
```

Technical Evidence Acquisition

Now What?

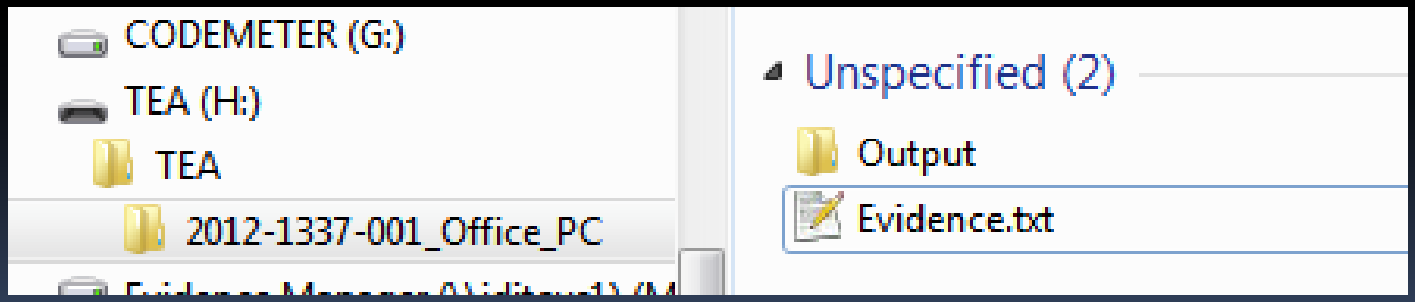
- Hopefully TEA performed all its tasks without any issue. You can now eject the drive and proceed with your standard procedure.

  (Power Down suspect computer, or unplug server from the network, leave it alone, etc.)

Technical Evidence Acquisition

Analysis

- You can now plug the USB device back into your analysis machine. In the TEA folder will be a subfolder named `<filenumber>-<exhibitnumber>`
- In our example the folder is 2012-1337-001_Office_PC



Technical Evidence Acquisition

Analysis

- The [**Evidence.txt**] is a compilation of the outputs of the tools run.
- Each tool run has the time it is run, the precise command run with a brief explanation of what was looked for when that command was run. The case information is also displayed on the top of the report.
- In the following example, as the machine was running windows 7, a local copy of IP config was run after the hash was verified.

Technical Evidence Acquisition

Analysis

```
TEA Version: 1.0.120513a
CASE FILE# 2012-1337, Exhibit# 001_Office_PC, Investigator: Cst. Trihard
Application Description [Command run] : Each output seperated by "_____"
Commands run under user: VITCU\msouthby
_____

TIME STARTED [NOW] :

Fri Dec 21 10:25:06 2012

================================================================================
=================[WINDOWS 7 / VISTA ARCHITECTURE DETECTED]=====================
[Tools (ipconfig, route, netstat, at, net, arp) run from C:\Windows/System32/]


C:\Windows\System32\IPCONFIG.exe HASH: cabb20e171770ff64614a54c1f31c033
IPCONFIG.exe Verified. Running application...
NETWORK SETTINGS [IPCONFIG /ALL]:

Fri Dec 21 10:25:06 2012

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SOUTHBATX
   Primary Dns Suffix  . . . . . . . : vitcu.itcu.com
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : vitcu.itcu.com

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82567V-2 Gigabit Network Connection
```

Technical Evidence Acquisition

Things to be aware of

- Each tool run has its own output text file placed in the [**<file#>-<exhibit#>\output**] folder.
- Each of these files are then hashed using MD5 and the hash is stored in [**HASH_VALUES.txt**] within that folder.
- The MD5 hash of [**HASH_VALUES.txt**] is stored at the end of [**Evidence.txt**]

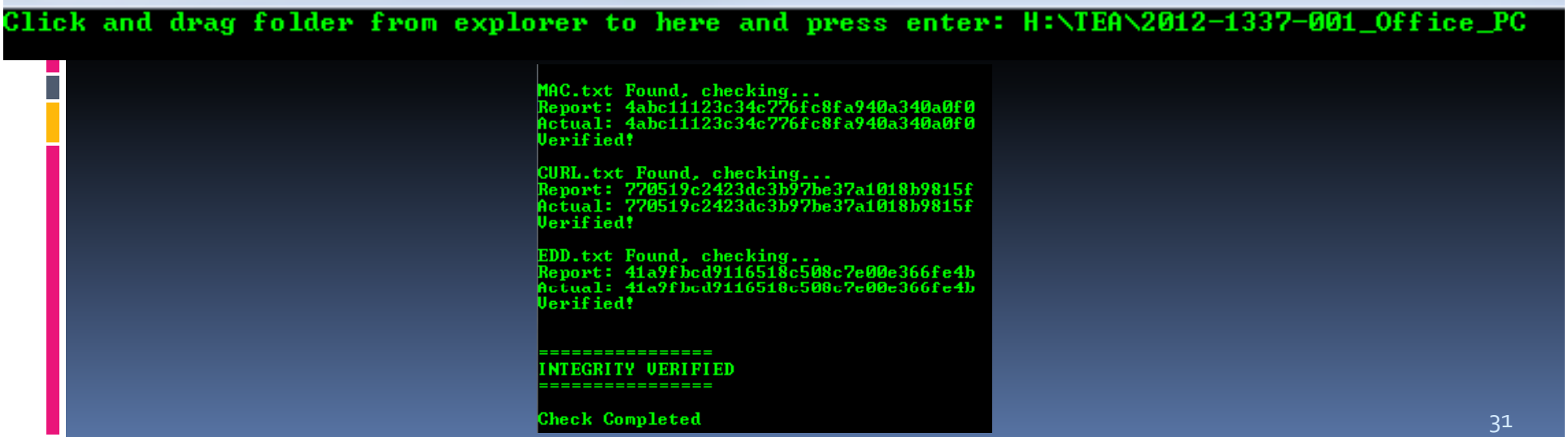
```
HASH_VALUES.txt MD5 HASH:

07d63a5569b57cfe46e6a42b3eea4b2d *2012-1337-001_Office_PC/Output/HASH_VALUES.txt
```

Technical Evidence Acquisition

Verify Report

- You can double click [**Verify_Report.cmd**]
- Then drag the reports folder to the command prompt to check the hash values and verify no output text files have been altered.



Technical Evidence Acquisition

Verify Report

- It is recommended you check to ensure your memory dump worked (if moonsols or FDPro was used, it should be in the:
  [<file#>-<exhibit#>] folder

- It is highly recommended that the evidence.txt is reviewed prior to leaving the scene, as it may provide some useful clues which could lead to more evidence.

Technical Evidence Acquisition

Other things

- There are several other useful tools included in the tool kit:
  - `HIBERNATE.cmd` – If the memory dump failed, this will attempt to place the system into hibernation which should write the memory to the disk. Not tested on all operating systems, so a last resort.
  - `GETSYSTEM.cmd` – Will attempt to use privilege escalation techniques to get NT AUTHORITY\SYSTEM rights. Use whoami to verify it worked.
  - `PROMPT.cmd` – Shows date and time for each command run. Useful when running commands and you photograph the computer monitor.

Technical Evidence Acquisition

Other things

- unHpak.bat – A simple batch for extracting memory and page files from FDPro Hpak files.
- CHECK4KW.cmd – A simple keyword searcher. It allows you to map all files on a drive, then run a keyword search against those lists. Keywords stored in [key_words.tea]. To just map drives have no entries in the [key_words.tea] Keywords stored then manually search the generated files.
- Verify_Tools.cmd – This is run as part of BREW

Technical Evidence Acquisition

Other things

- Other tools in the kit are:
- DumpIt.exe – Free all in one memory dump tool by moonsols. Dumps memory to where ever it is run.
- Winen - (Free EnCase memory dump application)
- DD.exe – A windows version of the linux dd for imaging live systems.

Technical Evidence Acquisition

HMI (Human Interface) Automation

- Vista, Windows 7 and Service pack 3 disabled autorun and made it difficult to run commands as an administrator.
- To get around this, a Teensy (Mini Arduino) device can be used to emulate a keyboard/mouse
- This allows scripts to be made which allow full automation of TEA
- I have a working proof of concept with two payloads, one for Windows XP and one for Windows 7.
- They are proof of concept as I have designed a more effective Teeny device which will have a menu and allow you to select payloads. Right now you have to take it apart and change the payload manually which is impractical.
- However one could have a device for each payload and it would work.

Technical Evidence Acquisition

That's it!

- Thanks for giving it a try!

  Please let me know if you use this tool as I am trying to figure out if people find it useful and generate some statistics to hopefully justify making a better version of it.

  My work email at the front of this document, or mark[at]southby[dot]ca

  I can also be reached at by calling:
  One-50-tec-2-hack