When and Why should you use VFC?

Iain Nash 05/05/2017

MD5
evidence you can trust

- **What does VFC enable you to do?**
    - Work directly from a write-blocked hard-drive in the field
    - Virtualise a suspect computer in seconds
    - Bypass Password Protection to access a suspect's desktop almost instantly
    - Have "a quick look at their computer" without affecting forensic information
    - Use VFC as a triage tool to:
        - Identify date of last use/password-protected user accounts etc.
        - Reduce the number of devices seized (or help prioritise them) by checking:
            - User Accounts
            - Password Protection
            - Last Used Date
            - Last Boot Up
            - Last Shut Down

- **What are the benefits of using VFC to generate a Virtual Machine (VM)?**
    - VFC will fix all known errors to save the examiner time in setting up the VM in the first place
        - If you can virtualise a machine in seconds rather than hours, you are saving time and therefore money
        - Virtualising a computer without VFC can take anywhere from 3 hours to 3 days
        - Investigators can look at more cases in shorter time-frames (therefore reducing backlogs)
        - The cost in man-hours for time spent fixing errors could easily exceed the cost of the licenses of VFC
    - Bypassing Windows passwords negates the requirement to actually crack it or extract it – VFC patches the VM so no password is required meaning access is almost immediate
        - Extracting or cracking a password can be done with other tools but with VFC Password Bypass, accessing the User account is almost instant
        - This inbuilt feature removes the need for other tools – in turn removing the need for the department to invest in additional password bypass software

- **What are the benefits of using a Virtual Machine (VM) during investigations?**
    - Being able to show a suspect their own (password protected) computer's desktop in interview can lead to an early guilty plea, even if nothing has been actually found yet
    - "A picture speaks a thousand words"
        - Screen shots of a suspect device can explain possibly tricky concepts simply and easily
        - Being able to show a suspect's desktop, or evidence of e.g. a "jump list" or internet history pointing to incriminating files or sites, in an environment they understand, helps demonstrate a person's recent activity to a non-technical person such as a judge, a member of the jury or a solicitor
        - Showing someone a picture means you don't need to write as much to explain it – saving time
    - If you can't read a database file in a forensic examination tool such as EnCase, you can use inherent software installed on the suspect's machine (therefore available on the VM) to look at the data.
        - Additional investment in software (e.g. Sage) is not required to look at cached information on devices
        - Spreadsheets (e.g. financials) can easily be exported and shared with financial investigators
    - You can view the contents of a suspect's PC in its native environment –
        - Obvious "accessible" files and folders can be quickly identified
        - Recent file history can be accessed from jump lists or recent items in Windows Explorer
        - Internet history can be viewed
        - P2P/torrent downloads and shares can be seen in plain text
    - The VM can be used as a Directional tool to help point forensic examiners where to look
        - Investigators can utilise standard Windows Search tools to find information and files
        - Non-forensic specialists such as fraud investigators can identify files of interest and then ask the HTCU to provenance only specific files, saving time
    - By using a write-blocker or forensic disc image, the VM works from a snapshot in time so you can run scripts or install software on the system with no fear of breaking it; you can always "rewind" it back to the initial state

- **How can VFC or a VM be used to augment a forensic investigation?**

  VFC can/will (Please note, this list is not exhaustive):

  - Produce a **standalone VM** to enable a non-forensic-specialist investigator to "**have a look around**" the suspect's computer
  - Utilise the log files to help crack User Passwords
    - VFC reads the registry to identify if multiple User Accounts exist on the device and if those accounts are password protected.
    - **VFC extracts the hash value(s) of ALL User Account passwords** which can then be ingested into alternative tools (e.g. Rainbow Tables, HashKiller, CrackStation)
    - The automatic extraction of the user password hash value means cracking the password can be set to run concurrent to any VFC investigation
  - Demonstrate **accessibility** of information or where details were kept
    - e.g. a specific folder or file located on the desktop
    - Background **Wallpaper** may be incriminating
    - Utilise screenshots of folder-trees and file organisation in reports
      - The "**Show Hidden Files**" and "Show Common Extensions" features can be very helpful for non-technical audiences
    - Utilise screen-capture software (e.g. Camtasia) to record how easy it is to access certain data
  - Use inherent software to look at accounts or files:
    - If they have a **Password Manager**, sometimes the stored passwords can be found in plain text within the Password Manager files
    - if they have e.g. **Sage or QuickBooks**, you can look at their financial records using their own installation and license and export data for review elsewhere
    - **Internet browsers** can contain powerful
      - View **browser history** and saved bookmarks
      - If they have set up auto-populated passwords, the computer will automatically log into Facebook or email accounts (requires internet connectivity *please refer to RIPA*)
      - Google Chrome and Mozilla Firefox will show saved passwords in plain text – these can be used to help identify or give clues towards potential passwords for additional devices
    - Check **Anti-Virus software**:
      - Demonstrate virus definitions were up to date to negate any arguments that "a virus did it"
      - Access Antivirus logs to see how they were set up, what may have been quarantined or what sites have been blocked
    - Identify **cleaning software** which may be scheduled to auto-run on start-up
      - raises questions and highlights more advanced technical knowledge and possibly "something to hide"
    - Identify **P2P/torrent software** which may be scheduled to auto-run on start-up and in which you can:
      - View any files being actively shared (or seeded)
      - View partial downloads to trace activity
      - Identify the "Save to folder" to demonstrate interaction and evidence a higher-level user
  - Connect **encrypted USB drives** to the machine to see if the decryption password is auto-saved
    - The original encryption software can then be used to remove the encryption from the device so it can be forensically imaged
    - TrueCrypt and even EnCase can be run from a shared drive so they don't need to be installed directly on the VM
  - Connect **encrypted iPhones** to the VM and **use iTunes to remove the encryption** from the device so it can be forensically imaged using other tools (this may require the device to be unlocked or the passcode known)
  - Explain system **time slippage** by checking the last sync date to demonstrate it's been "off the grid"
  - Install software or **run your own scripts directly on the VM** to help locate specific data/files
  - Rewind a machine to an earlier state using **Restore Point Forensics**
    - See Shortcuts that were saved on the desktop in an earlier version of the machine – such as links to websites of ill-repute or shortcuts to files which may no longer exist – which could prove the machine has been cleaned up, obstructing the course of justice