# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Keshav Kumar Mahatha  UWE ID: **23045175** | Exam commenced | 15/12/2023 to 28/12/2023 | | Other relevant information | Any relevant information? | Software used, versions and licensing | Autopsy (V. 4.20.0), AccessData FTK Imager (V. 4.5.0.3), Hash my files (V. 1.90), Registry Ripper (V.3.0), Event Log Explorer forensic edition version 5.4 (Build 5.4.1.4521), Ophcrack (V 3.8.0) |   Note: If you decide to omit a process, then you should provide your reasons for doing so. You may add additional rows, as appropriate. |  |  |

| Action | Done? | Date | Time | Notes |
| --- | --- | --- | --- | --- |
| Load case and verify image | Yes | 15/12/2023 | 2:14 PM | * Autopsy (V. 4.20.0) was opened and then the following interface popped up,      * New Case option was selected,      * All the information like the case name, and the base directory was chosen where all the temporary and permanent files will be stored during our case study. * After filling all the information, another optional information tab popped out,      * In optional information tab, all the information like case number, examiner name, phone and email were given, * after clicking next, computer started processing and then another tab opened,      * Default options were left as it was and then after clicking next, new tab opened, * Disk Image or VM file option was chosen because I have been provided with Image file to process,      * The path of image file (name: Hunter XP for Dongled v6.E01) was given, * Also, the Time Zone was set to (GMT +0.00) UTC and all other options were left as default.      * All ingest modules were selected except Virtual machine extractor, Android Analyzer(aLEAPP), DJI drone Analyzer, YARA Analyzer, iOS Analyzer(iLEAPP), GPX parser and android Analyzer.      * After doing all that, computer started its processing,        * After the completion of the process, the integrity of the file was checked by verifying the Hash Values, * The Hash Value was: dfcfe9ab9a60c6ad4a314656b687226b |
| Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items | Yes | 15/12/2023 | 3:27 PM | 1. **Before uploading,**    * + AccessData FTK Imager (V. 4.5.0.3) was used to again verify the Hash values for dual verification,     In AccessData FTK Imager,  Following steps were taken,  First the evidence file was uploaded,  Process: **File>Add evidence item>Image file>path of the evidence file**     * + - After uploading the file, following interface popped up,      * + - After that following steps were taken,   **File>Verify Drive/Image**      Hash Value: **dfcfe9ab9a60c6ad4a314656b687226b**   1. **After uploading in autopsy**   Process: **Ingest message>Data source Integrity**    Hash Value: **dfcfe9ab9a60c6ad4a314656b687226b** |
| Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items | Yes | 20/12/2023 | 9:20 AM | **In Autopsy,**  Hex view mode was selected by choosing **Hex** view mode and the following artefact was seen,  I also compared the corresponding hex values,    **Magnified,**    **In AccessData FTK Imager,**  Hex view mode was chosen, and similar artefact was seen,  In similar way I compared the corresponding hex values,    **Magnified,**     * Here we can see that in both applications (Autopsy and Access data FTK manager), when examined, I got the identical message stored at identical address.   Hence other main artefact is also verified. |
| Time Zone Adjusted?  Report Time Zone used for Analysis. | Yes | 20/12/2023 | 9:35 AM | Steps: **Autopsy>Tools>options>view**      Here, I adjusted the report time zone for analysis. The time was set as **(GMT+0:00) UTC** |
| Recover lost folders  (NTFS, FAT16&32). | yes | 20/12/2023 | 9:50 AM | Steps: **Autopsy>Tools>Run Ingest Modules>File name (Hunter XP for Dongled V6.E01)**    After using **photoRec Carver** as an ingest modules, I recovered certain deleted files. |
| Mount archives;  zip, thumbs.dB, etc. | yes | 20/12/2023 | 10:00  AM | Archives files were thoroughly checked, and these files were found.    Here, some files were extracted for **analysing** and I got interesting information.    The link of above file is here, [File](suspected%20files/RAClient.htm).  MD5: **ae94ef97e5b755ea568a717aca695967**  SHA1: **fc48685d7226e3acf6fd623e37ab9b0f34fd1b51**  Modified time: **8/17/2001 1:29:38 PM**  Created time: **8/17/2001 1:29:38 PM**  File Size: **45,414 bytes**    The link of above file is here, [File2](suspected%20files/helpeeaccept.htm).  MD5: **29ab9ccadb0d63259f6e330bd2e6ab74**  SHA1: **c2f49a5802e1ed6bb26d7fa1c8a53175dab4127f**  Modified time: **8/17/2001 1:29:38 PM**  Created time: **8/17/2001 1:29:38 PM**  File Size: **3,907 bytes**  Here, we can see that this PC contains some files which indicates that this user may have given remote assistance of his PC to his friend/friends. |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) | Yes | 20/12/2023 | 3:43 PM | New ingest modules were selected and ran,  Ingest module **Encryption detection** was selected for entropy.  Steps: **Autopsy>Tools>Run ingest modules>file name (Hunter XP for Dongled V6.E01)**    After the PC finished the analysing process, I got interesting results.      Many files did have extension mismatch, some jpg files were saved as tmp files.    Here, we can see, file that was saved as **wbkA1.tmp** was a jpg file.      In its **Hex** value also, we can see that the first **Hex** value is **FF**, and we know that **FF** indicates it’s a jpg file. |
| Internet History, favourites, etc.  Other browsers? | Yes | 25/12/2023 | 6:00 PM | To check which browser the user has installed,  I went to the windows registry file by,  **Data Sources>Hunter XP for Dongled V6.E01\_1 Host>vol 2>Windows>system32>config**  And then I extracted **SAV** files named as **Software.**  After the files were extracted,  **File1**[**suspected files to link in word\14134-software**](suspected%20files%20to%20link%20in%20word/14134-software)  **MD5: dbda9a624d0ca6c78f2a76dfe4e17f30**  **SHA1:** **548002bad420b98736d4b1d8f2f76868d976ff5f**  **File2** [**suspected files to link in word\14138-software.sav**](suspected%20files%20to%20link%20in%20word/14138-software.sav)  **MD5: bdc7c1fe94437178718e750f8a90415a**  **SHA1:** **c3686502f34be1c265f024843f3c242b38029a65**  **File3**[**suspected files to link in word\14145-system.sav**](suspected%20files%20to%20link%20in%20word/14145-system.sav)  **MD5:** **ee98e03db81c7f2c5679bdc1ef4fefec**  **SHA1:** **2fcc5dce0c122ef2d336a82e6f753edb2afd2b75**  Reg ripper (v.3.0) was used to save these files in human readable format.    In **Hive** file-the **location** of Sav file was given  In Report file- the **location and name** of **Note** file (Output) were given  The **ripped** files are,  File1[suspected files to link in word\14134-software 1.txt](suspected%20files%20to%20link%20in%20word/14134-software%201.txt)  **MD5:** **06065f810c35149506beab86dea08b5b**  **SHA1:** **c05307e57f75f2a49b75a7455ea8262d23728801**  File2[suspected files to link in word\14138-software 11.txt](suspected%20files%20to%20link%20in%20word/14138-software%2011.txt)  **MD5:** **9dd3d90ea4ac15ffc930cac9b75622f9**  **SHA1:** **792944306acd60f3b25e096bbab2d922ac7739ef**  File3[suspected files to link in word\14145-system 111.txt](suspected%20files%20to%20link%20in%20word/14145-system%20111.txt)  **MD5:** **21415ed2534fd7cd3c9841da69c12c89**  **SHA1:** **c24cba86317463b0669380273a6c7ab068b81174**  After examining these ripped files, I got the list of software that were installed on the suspects computer and from there I got the name of browser from where I  will be collecting **Internet History, favourites, etc. Other browsers.**    Here, we can see that user had installed **Internet Explorer browser.**    These are the **Web history** of the user.    These are the **web cookies** of user.    These are the **web bookmarks** of user. |
| Emails, local and web-based. | Yes | 25/12/2023 | 7:00 PM | Magnified,    Here, we can see the emails, local and web-based files. |
| Retrieve operating system information, accounts information, software, time zone information etc.). | Yes | 25/12/2023 | 8:00 PM | The information about operating system was taken from here,    Magnified,    **Also,**  The information was again verified from registry.  First, **System.sav** file was extracted from registry **(Data Sources>Hunter XP for Dongled V6.E01\_1 Host>vol 2>Windows>system32>config)**  File1[suspected files to link in word\system files\14141-system](suspected%20files%20to%20link%20in%20word/system%20files/14141-system)  File2[suspected files to link in word\system files\14145-system.sav](suspected%20files%20to%20link%20in%20word/system%20files/14145-system.sav)    Then these files were Ripped using Reg ripper,  File1[suspected files to link in word\system files\14145-system1.txt](suspected%20files%20to%20link%20in%20word/system%20files/14145-system1.txt)  File2[suspected files to link in word\system files\14141-system0.txt](suspected%20files%20to%20link%20in%20word/system%20files/14141-system0.txt)  After examining the ripped files,  **Time zone** is:    It looks like this is the **Central time zone of the United States of America.** which observes Central Standard Time (CST) during the standard time and switches to Central Daylight Time (CDT) during daylight saving time. The offset from UTC is 6 hours during standard time (CST) and 5 hours during daylight saving time (CDT).    **Last Write: [2002-06-05 00:06:15] UTC**      **Last Clean shutdown: 04-Jun-02 10:58:38 PM UTC**  Because **6006**  is the event ID of Shutdown and last shutdown was at that date.  Ripped Registry files.  **Softare11**[**suspected files to link in word\Ripped files\14134-software1.log**](suspected%20files%20to%20link%20in%20word/Ripped%20files/14134-software1.log)  **Software12**[**suspected files to link in word\Ripped files\14134-software1.txt**](suspected%20files%20to%20link%20in%20word/Ripped%20files/14134-software1.txt)  **Software21**[**suspected files to link in word\Ripped files\14138-software2.log**](suspected%20files%20to%20link%20in%20word/Ripped%20files/14138-software2.log)  **Software22**[**suspected files to link in word\Ripped files\14138-software2.txt**](suspected%20files%20to%20link%20in%20word/Ripped%20files/14138-software2.txt)    **Windows version & build info**  **ProductName - Microsoft Windows XP**  **Build Lab - 2600.xpclnt\_qfe.010827- 1803.**  **Registered Organization - PC User Company**  **Registered Owner - PC User**  **Install Date - 2002-02-28 22:02:39 UTC.**  **Installed programs are, (From Autopsy)**        **Installed programs are, (from registry, ripped file)** |
| Timeline analysis-  Note date of last activity on the computer. System profiling. | Yes | 26/12/2023 | 12:10 PM | **Last Write Time 2002-02-28 15:25:16 UTC**  **The Region value is: 244.**  **The Country Is: United States**  **ProductName - Microsoft Windows XP**  **Build Lab - 2600.xpclnt\_qfe.010827-1803.**  **Registered Organization - PC User Company**  **Registered Owner - PC User**  **Install Date - 2002-02-28 22:02:39 UTC.**        This information was taken from ripped SAV registry files.        This information was taken from Event log explorer. |
| Registry analysis and  Registry protected area | Yes | 26/12/2023 | 12:59 PM | Registry was accessed from: **Data Sources>Hunter XP for Dongled V6.E01\_1 Host>vol 2>Windows>system32>config>**  And the registry files were extracted.  All the extracted files were then analysed.  The ripped registry files are,  File1[suspected files to link in word\14125-SAM1.log](suspected%20files%20to%20link%20in%20word/14125-SAM1.log)  **MD5: 4bb4eeb190f413054fc1963b6a5d5df0**  **SHA1: a9931121e63227365563be41e23a259d065c6430**  File2[suspected files to link in word\14125-SAM1.txt](suspected%20files%20to%20link%20in%20word/14125-SAM1.txt)  File3[suspected files to link in word\14134-software 1.log](suspected%20files%20to%20link%20in%20word/14134-software%201.log)  **MD5:** **fbf136d8df04a1b24f3e59d9b617352c**  **SHA1:** **d5b22a0c980409bd68873fc9ceae2209a632c6b9**  **MD5:** **4b90011f5357a93c512ad9782f284af4**  **SHA1:** **6f17660d2a2dc25335bfe05aa0d2e19c810d3550**  File4[suspected files to link in word\14134-software 1.txt](suspected%20files%20to%20link%20in%20word/14134-software%201.txt)  **MD5: 06065f810c35149506beab86dea08b5b**  **SHA1: c05307e57f75f2a49b75a7455ea8262d23728801**  File5[suspected files to link in word\14138-software 11.log](suspected%20files%20to%20link%20in%20word/14138-software%2011.log)  **MD5: 0265f80f04caeb431fd21976077f5e33**  **SHA1: d2a7304bd272725d657667ba6e4578608933ca17**  File6[suspected files to link in word\14138-software 11.txt](suspected%20files%20to%20link%20in%20word/14138-software%2011.txt)  **MD5: 9dd3d90ea4ac15ffc930cac9b75622f9**  **SHA1: 792944306acd60f3b25e096bbab2d922ac7739ef**  File7[suspected files to link in word\14145-system 111.log](suspected%20files%20to%20link%20in%20word/14145-system%20111.log)  File8[suspected files to link in word\14145-system 111.txt](suspected%20files%20to%20link%20in%20word/14145-system%20111.txt)  **MD5: 036f6b043cd6aba1c3811e8bb86f06f9**  **SHA1: 22b73a4d208f58a8ad87b64c466decb72b350dfe**  **MD5: 21415ed2534fd7cd3c9841da69c12c89**  **SHA1: c24cba86317463b0669380273a6c7ab068b81174**  File9[suspected files to link in word\default1.txt](suspected%20files%20to%20link%20in%20word/default1.txt)  **MD5: 22780483a92379d234141d93636d93cb**  **SHA1: 39cffd3b475fb0f169072939876861059f0a654a**  File10[suspected files to link in word\default1.log](suspected%20files%20to%20link%20in%20word/default1.log)  **MD5: aa334e13a0a94cba249caf4cdfade8f8**  **SHA1: c15c6ca6dbac8b15c1391d8734faf507947fd069**  File11[suspected files to link in word\default2.log](suspected%20files%20to%20link%20in%20word/default2.log)  File12[suspected files to link in word\default2.txt](suspected%20files%20to%20link%20in%20word/default2.txt)  **MD5: aeb17556146f0e62181daa88d37ffa05**  **SHA1: 02fe1dbe5e0a06394f2b3521592aedb9503c2b58**  **MD5: 90f2513970458f6eed854ece544c8176**  **SHA1: fd3d534c4f2e86317bb8aadfeaf63c67925a34ec**          Default file,      Software file,              SAM file, |
| Link files and Recycle Bin | Yes | 26/12/2023 | 1:32 PM | These **Deleted Files and Images** were found as deleted files,  Path: **Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>Documents and Settings>Bob Hunter>My Documents>My pictures>Hunter pics**    These **Linked Files** were found,  Path: **Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>Documents and Settings>Bob Hunter>Recent** |
| Instant Messaging clients | Yes | 26/12/2023 | 2:26 PM | **Windows messenger** was already installed.  Path: **Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>Program Files>Messenger**    **AOL Instant Messenger,**   * AOL Instant messenger was an instant messaging and presence computer program created by AOL, which used the propriety OSCAR instant Messaging Protocol and the TOC protocol to allow registered users to communicate in real time.   **Path:** **Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>Program Files>AIM95**    Suspect had also installed **Yahoo Messenger.** |
| Clean-up/Wiping utilities. Check log files. Anything used? | Yes | 27/12/2023 | 2:50 PM | On 2002-06-03 17:08:40 UTC **cleanmgr.exe** was used to clean up the files. |
| External drives; Network connections | Yes | 27/12/2023 | 4:04 PM | **Rasphone.pbk**  The “rasphone” in windows is used to manage remote access phonebooks, and specifically, “61-rasphone” refer to a particular entry or configuration within the Remote Access Service (RAS) phonebook. The RAS phonebook contains information needed to connect to remote networks using dial-up or VPN connections.        **33 USBs were connected.** |
| Perform data carving | Yes | 27/12/2023 | 6:43 PM | PhotoRec carver was chosen to run as an ingest module to perform data carving,    **Carved files,** |
| Run relevant keyword searches;  Did you index the evidence file? | Yes | 27/12/2023 | 5:28 PM | Searched **“Money”**  Results,        From here we can say that suspect may have involved in **ransomware.**  Searched “**Love”,**      Here we can see that suspect is blackmailing someone.  Searched “**Life”**      Here, we can see the conversations. |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase | Yes | 27/12/2023 | 8:30 PM | I Used **Ophcrack (Ophcrack 3.8.0),**  First, I installed virtual machine and in that virtual machine I added Linux because **ophcrack** didn’t work on windows 11 so in that virtual machine ophcrack was installed.  The Results, |
| Examine different file types:  Export doc/office and exe files; look at Metadata if required | Yes | 27/12/2023 | 9:24 PM | Found file types are jpg, Videos (wmv, swf), Audio (.wav), .jar, .zip, .cab, html.gz, .db, .html, .doc, .txt, .exe, .bat etc. |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) | Yes | 27/12/2023 | 6:00 PM | The suspected encryption is 1 i.e., **oembios.bin** |
| Print artefacts | Yes | 27/12/2023 | 8:20 PM | Artefacts,    Also,  Suspect also used Printer.  Details, -**HP LaserJet 2200 Series PCL**  **-WinPrint**  Path:: **Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>WINDOWS>System32>spool>PRINTERS** |
| CD/DVD burning apps; check log files | Yes | 27/12/2023 | 10:52 PM | To check CD/DVD burning apps,  Log files were thoroughly viewed, and the results were,  **Event log explorer was used to view the event logs,**  The extracted logs (from: Data Sources>img\_Hunter XP for Dongled v6.E01>vol\_vol2>WINDOWS>System32>config)  Were added to event log explorer and then the events were checked.  In **System event,**    First, terminal service was started.    Then CD burning was started.  The burning was **IMAPI CD-Burning COM Service** |
| Validate evidence integrity at the end of the examination |  |  |  | At last,  The hash values were again verified,     * + Calculated Hash: **dfcfe9ab9a60c6ad4a314656b687226b**   **Hence, the Data Source integrity was verified.** |

**Additional Notes/Artefacts Examined:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| **Colour-coding Legend** | **Tasks** |
|  | Fundamental |
|  | Basic |
|  | Elementary |
|  | Secondary |
|  | Advanced |
|  | Exceptional |