# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Anish Adhikari | Exam commenced | 2025 December – 2026 January | | Other relevant information | Any relevant information? | Software used, versions and licensing | Autopsy 4.22.1  Exterro FTK Imager 4.7.3.81  AccessData Registry Viewer 2.0.0.7  RegRipper3.0-master  Ophcrack 3.8.0  Event Log Explorer 5.7 |   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 | Done |  |  | I made a folder called **Hunter XP** on my Windows desktop and added two subfolders named **Casefile** and **Evidence**.    The **Casefile** folder served as the database for Autopsy, which I loaded during the analysis. The **Evidence** folder contained the Hunter XP disk image (EO1 format).  Next, I used Autopsy to load and analyse the disk image.    This was the interface that appeared when I opened Autopsy for the first time. Since I was starting a new investigation, I clicked **New Case**.    After selecting **New Case**, I entered the required information, including the ***Case Name*** and the ***Base Directory*** as shown above.  In the **Optional Information** section, I entered the ***Case Number***, ***Name***, ***Phone***, and **Email**, and then clicked Finish.    After this, the **Add Data Source** window popped up, where I entered the required information.    We will select the 1st option as itself and click on Next.    Here, we selected **Disk Image or VM File** because we were going to analyse a disk image.    We then selected the disk image and specified its location, which was inside the Evidence folder, as mentioned earlier. Additionally, we set the time zone to **(GMT +0:00) GMT**.    We selected only the Ingest**Data Source Integrity** module at first because the task was to load the case and verify the image. The other ingest modules were enabled later as needed.    Here it shows that the data has been added to the local database. We proceed further by clicking **Finish**.    We clicked on the message type icon that appeared in the top right corner of the page.    Here we could see that the **Data Source Integrity** of the image file was verified.  Next, we clicked on the verified item and checked the hash value of the image.    Finally, the computed hash values were:  Calculate hash: **dfcfe9ab9a60c6ad4a314656b687226b**  Stored hash: **dfcfe9ab9a60c6ad4a314656b687226b**  I cross-checked the image's hash via **FTK Imager**.    Both the hash value matches.  Calculate hash: **dfcfe9ab9a60c6ad4a314656b687226b**  Stored hash: **dfcfe9ab9a60c6ad4a314656b687226b** |
| Load Case into second forensic tool for dual verification of at least 2 key artefacts, evidence items |  |  |  | For dual verification, I used **Access Data Registry Viewer** and **Reg Ripper**.  The first step involved using Autopsy to retrieve the ***SAM*, *SOFTWARE*, *SYSTEM***, and ***SECURITY*** registry hives from the Windows/system32/config path and saving them locally.      It was saved on my PC locally.  **1st Artifact :**  Accessing the SYSTEM hive's **ShutdownTime** value via the path SYSTEM \ ControlSet001 \ Control \ Windows in the **Access Data Registry Viewer** indicated that the last shutdown occurred on 6/4/2002 at 22:58:42 UTC.    The previously observed **last shutdown** date was confirmed when I ran **RegRipper** against the ***SYSTEM*** registry file.    **2nd Artifact:**  Upon examining the ***SOFTWARE*** registry hive using **Access Data Registry Viewer**, the presence of the **Yahoo application** installation was revealed.    Additionally, I validated the **Yahoo installation** with **Reg Ripper** using software registry hive. |
| Time Zone Adjusted?  Report Time Zone used for Analysis. |  |  |  | At the very beginning, the time zone was selected to **(GMT +0:00) GMT.**  We can also configure the time zone by clicking **Tools > Options > View**.        In the picture above, we saw that we could set the time zone by clicking **Use another time zone** and then clicking **Apply**. |
| Recover lost folders  (NTFS, FAT16&32). |  |  |  | To recover the lost folder, I first installed the **PhotoRec Carver** module by navigating to **Tools > Run Ingest Modules > Hunter XP for Dongled v6.E01.**          We clicked on "Finish" after selecting the PhotoRec Carver module.  Top of Form  After clicking "Finish," it took about 20 to 30 seconds to load the image from the PhotoRec Carver module.  We navigated to **File view > Deleted Files > All (2137).**    We saw that some files only had their metadata extracted, while others  were fully recovered. |
| Mount archives;  zip, thumbs.db, etc. |  |  |  | The archive folder was in **File Views > File Types > By Extension > Archives.**    The thumbs.db was present in **File Views > File Types > By Extension > Databases.** |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) |  |  |  | To complete this, I first installed the ingest modules**: Hash Lookup**, **File Type Identification**, **Extension Mismatch Detector** and **Encryption Detection.**    Under Analysis Result, we saw that **58** files with extension mismatch were detected.    At this point, we noticed that the ***wbkC1.tmp*** file, although saved as a .tmp extension, was an image file.    Hexadecimal analysis revealed that although the file was saved as ***wbkc1.tmp***, its header began with **FF D8 FF**, confirming it was a JPEG image.    For Entropy:  Under the **Encryption Suspected** items, there was a file named ***oembios.bin*** that showed a high entropy value of 7.999988. |
| Internet History, favourites, etc.  Other browsers? |  |  |  | First, I installed module named **Recent Activity**.  Under **Data Artifacts**, we were able to see the ***Web History***.    We could see the many websites that the user, Bob Hunter, had visited.    To locate the favourites, we went to the ***Web Bookmarks*** section and found that the user had bookmarked **16** websites, which were likely his favourites.    The browser mostly used by the user appeared to be **Internet Explorer**. I checked the Installed Programs section and found entries such as **IE40**, **IE5BAKEX**, **IE4Data**, and **IEData**, all of which are components related to Internet Explorer.      However, it was observed that the user had also installed **Microsoft Edge**, which was visible under **Ingest Message > Browser Results**. |
| Emails, local and web-based. |  |  |  | To complete this, I first installed two modules: **Keyword Search** and **Email Parser**.    When I navigated to **Data Artifacts > Installed Programs**, I observed that **Outlook Express**, a local email application, was installed on the system.      I examined the **Web Bookmarks** and observed that the user had **Hotmail**, which is a web-based email service.    When I reviewed **Email Keyword Hits > Email Addresses**, I observed that the two users with the highest level of interaction had also used **Hotmail**, namely **billiray150@hotmail.com** and **chaser1191@hotmail.com** .    Upon reviewing the **Web History**, I observed evidence of **Yahoo**, which is also a web-based email service. |
| Retrieve operating system information, accounts information, software, time zone information etc.). |  |  |  | Under **Data Artifacts**, there was a section called **Operating System** **Information**, where we found some details about the Operating System.      To find the user information, I used two tools:  (i) **Registry Viewer**  (ii) **RegRipper**  First, I extracted the registry file from Autopsy and loaded the SAM file into both Registry Viewer and RegRipper.  Content from **AccessData Registry Viewer**:    Contents from **RegRipper:**        Both applications showed that this Windows OS had a total of **five user accounts**, including built-in and user-created accounts.  To view the software installed on the machine, we went to **Data Artifacts > Installed Programs** and saw the list of software installed on the PC.      To determine the ***time zones*** used by the system, I analysed the ***System*** registry file with **RegRipper** and obtained the relevant details.      The system registered the time as 10:00 AM on a Monday. The time zone it utilized for this recording was Central Daylight Time (CDT), which is an offset of UTC-5:00. This time zone is observed in the United States and Canada during their Daylight-Saving Time period. |
| Timeline analysis-  Note date of last activity on the computer. System profiling. |  |  |  | To look at the timeline analysis, we first installed the **Plaso** ingest module.    We navigated to **Timeline**.    From the timeline, it was clear that the PC was used the most in 2002.  It was also seen that the user’s web activity occurred only in 2002.    We observed that **IMAPI.EXE** was the final program utilized on the computer after navigating to ***Details*** and scrolling to the end.    **IMAPI.EXE** executed between ***2002-06-05 00:40:01*** to ***2002-06-05 00:40:02***    When I checked the last shutdown time in the ***SYSTEM*** registry, I saw the system shut down at 2002-06-04 22:58:42Z, but the **IMAPI.EXE** file last ran after that, at 2002-06-05 00:40:01, which did not correlate. |
| Registry analysis and  Registry protected area |  |  |  | To analyse the Registry, I utilized the **RegRipper** Tool, which extracted the contents of the ***SAM, SYSTEM, SOFTWARE***, and ***SECURITY*** hives into a text file.      The ***SAM*** file revealed a user named **Bob Hunter**, with **RID 1004**, who had no password set and logged in a total of 37 times.    It was interesting to note the absence of **RID 1003**, which suggested a user account with that identifier had been deleted.    Using the **SecEvent.Evt** file located at windows/system32/config, I identified a deleted user with **RID 1003**.    The **timezone** was taken from the ***SYSTEM*** registry file. |
| Link files and Recycle Bin |  |  |  | The path to the link files was **Documents and Settings/Bob Hunter/Recents**.    The deleted files were located at **RECYCLER**. |
| Instant Messaging clients |  |  |  | I navigated to **Data Artifacts >** **Installed Programs** and saw two applications: **AOL Instant Messenger** and **Yahoo Messenger**, which were instant messaging client applications.      The timeline showed that **AOL.exe** was one of the last programs executed on the PC. It ran on the final day, after which only three other applications were executed. |
| Clean-up/Wiping utilities. Check log files. Anything used? |  |  |  | When I navigated to **Data Artifacts > Run Programs**, I found the executable **CLEANMGR.EXE**, a built-in tool designed to free up disk space by identifying and removing unnecessary files.      I opened the executable's activity in the timeline.    The execution of **CLEANMGR.EXE** occurred a day prior to the system's final shutdown.    I performed a keyword search for **'Wipe'** and discovered an HTML file showing that the user previously researched **'BC Wipe**' and **'Wipe Drive’** for securely destroying deleted data. |
| External drives; Network connections |  |  |  | At first, we navigated to **Data Artifacts > USB Device Attached**.    The system was attached to 2 printers, 1 mouse, 1 video capture device, 1 PDA, 2 storage devices, and 4 root/USB hubs.    In the ***SYSTEM*** Registry file, I found evidence of two connected **USB devices** along with their connection timestamps.    During analysis of the ***SYSTEM*** registry file, I found that the computer was connected to a home or small office network and received IP address **192.168.1.130** from router **192.168.1.1** via DHCP. The last network connection occurred on June 5, 2002, at 00:31:54 UTC, with the lease expiring one hour later. This timestamp is critical for correlating file activity or downloads that occurred around this date.    I also found that the **RDP** service was enabled and listening on the default port **3389**, with no account lockout policy configured.    I accessed the list of shared network content and discovered that the ***“F:\DOCUMENTS AND SETTINGS\ALL USERS\DOCUMENTS”*** documents folder was shared across the network.    I reviewed the **SecEvent.Evt** log file and noticed a successful **Logon Type 3**, which indicated that an individual accessed the shared content from over the network.    While examining the **SysEvent.Evt**, I noticed that the computer had communicated with a computer named **RYAN-TOWER**. |
| Perform data carving |  |  |  | **PhotoRec Carver** was chosen to run as an ingest module to perform data carving.    After executing the **PhotoRec Carver** module, a total of **2,137 deleted files** were recovered.      In **vol\_vol2**, a folder named **CarvedFiles** was identified, containing all carved files. |
| Run relevant keyword searches;  Did you index the evidence file? |  |  |  | During the keyword investigation, I searched for the term “**money**” and discovered that the user had blackmailed a father regarding his daughter to demand a ransom.        Next, I searched for the term **“storage”** and found indications that the user may have used an online storage service called **XDrive** to store important files and access them online.        The evidence indicated that data was transferred successfully from **FreeDrive** to **XDrive**. |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase |  |  |  | I utilized the **Ophcrack** tool within my Linux environment to recover log-on passwords, first creating a **RecoverPassword** folder on the Desktop and then placing the necessary ***SAM*** and ***SYSTEM*** registry files extracted from the HunterXP image inside it.    I opened the **Ophcrack** and uploaded the folder to get the **hash value** of the password.    After that I was presented with the hash value of the User Accounts.    To obtain the password, I had to install the **rainbow tables** from the Ophcrack official website. I installed **XP for free quickly** and extracted its zip contents to a folder named **Tables** on the Desktop.      Then, I clicked on **Tables** and provided the file path as shown below.      After that I clicked on **Crack**.      Here, I was able to obtain the password for the user **HelpAssistant**, which was **YQR2AFR**. |
| Examine different file types:  Export doc/office and exe files; look at Metadata if required |  |  |  | I identified various file types with multiple extensions, including images (**.jpg, .png**), videos (**.wmv**, **.swf**), audio (**.wav**), and archives (**.zip**, **.jar**, **.cab**). I also found system and document files such as **.db**, **.html**, **.doc**, **.txt**, **.exe**, and **.bat**, which I then categorized within the **'File Views'** section by their respective extensions. |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) |  |  |  | When I navigated to **Analysis Results > Encryption Suspected**, I saw a file named **oembios.bin** with a high entropy value, indicating that it was likely encrypted. |
| Print artefacts |  |  |  | I opened the ***SYSTEM*** registry file using **RegRipper** and observed entries indicating a printer connected to the PC.    I also checked the **SysEvent.Evt** file using **Event Log Explorer** and observed connections for both printers shown in the ***SYSTEM*** registry analysis. |
| CD/DVD burning apps; check log files |  |  |  | **IMAPI.EXE** allowed programs to burn data or audio to CD-R/RWs. By going to **Data Artifacts > Run Programs**, we found that the **IMAPI.EXE** program had been executed on the system.    During timeline analysis, it was seen that **IMAPI.EXE** was the last program executed on the PC.  I extracted the .evt files from **WINDOWS/system32/config** and opened them using **Event Log Explorer**. Upon examining the **SysEvent.evt** file, I discovered that **IMAPI.EXE** had been executed.    **IMAPI.EXE** was executed multiple times on different days. |
| Validate evidence integrity at the end of the examination |  |  |  |  |

**Additional Notes/Artefacts Examined:**

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

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