# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Anish Adhikari | Exam commenced | 12/04/2025 – 12/23/2025 | | Other relevant information | UWE ID: 24071101 Email Addresses: Anish3.Adhikari@live.uwe.ac.uk  aanish24@tbc.edu.np | 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 | 12/07/2025 | 7:02 PM NTP | I made a folder called **Hunter XP** on my Windows desktop and added two subfolders named **Casefile** and **Evidence**.    Fig : Creation of Folders  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.    Fig: Opening of Autopsy  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**.    Fig: Case Information  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.    Fig: Optional Information  After this, the **Add Data Source** window popped up, where I entered the required information.    Figure: Select Host  We will select the 1st option as itself and click on Next.    Figure: Selected Data Source Type  Here, we selected **Disk Image or VM File** because we are going to analyse a disk image.    Fig : Select Data Source  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**.    Fig : Ingest Module  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.    Fig: Add Data Source  Here it shows that the data has been added to the local database. We proceed further by clicking **Finish**.    Fig: Ingest Message  We clicked on the message type icon that appeared in the top right corner of the page.    Fig: Completion of Data Source Integration module  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.    Figure: Verification of Data Source Integrity module  Finally, the computed hash values were:  Calculate hash: **dfcfe9ab9a60c6ad4a314656b687226b**  Stored hash: **dfcfe9ab9a60c6ad4a314656b687226b**  I cross-checked the image's hash via **FTK Imager**.    Fig: Hash value verified using 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 | Done | 12/08/2025 | 6:28 PM NTP | 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.    Fig: Selection of Registry File    Fig : Extraction of Registry File  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.    Fig: Last shutdown time verified using Access Data Registry Viewer  The previously observed **last shutdown** date was confirmed when I ran **RegRipper** against the ***SYSTEM*** registry file.    Fig: Extraction of content of SYSTEM Registry file using RegRipper.    Fig: Last shutdown time verified using RegRipper  **2nd Artifact:**  Upon examining the ***SOFTWARE*** registry hive using **Access Data Registry Viewer**, the presence of the **Yahoo application** installation was revealed.    Fig: Installation of Yahoo Application verified using Access Data Registry Viewer  Additionally, I validated the **Yahoo installation** with **Reg Ripper** using software registry hive.    Fig: Extraction of content of SOFTWARE Registry file using RegRipper.    Fig: Installation of Yahoo Application verified using RegRipper |
| Time Zone Adjusted?  Report Time Zone used for Analysis. | Done | 12/08/2025 | 6:55 PM NTP | Fig: Time zone Configuration  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**.    Fig : Navigation to Tools    Fig: Navigation to Options    Fig: Configuration of Time zone manually  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). | Done | 12/08/2025 | 8:53 PM NTP | The file system of the examined volume (vol2) was identified as **NTFS**, as confirmed by volume metadata and the presence of NTFS system files.    Fig: Properties of vol2  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.**    Fig: Navigation to Tools  Fig : Navigation to Run Ingest Module        Fig : Installation of PhotoRec Carver module  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).**    Fig : Deleted Files  We saw that some files only had their metadata extracted, while others  were fully recovered.    Fig: Content of Deleted File having only metadata    Fig: Content of Deleted File that is fully recovered |
| Mount archives;  zip, thumbs.db, etc. | Done | 12/09/2025 | 4:47 PM NTP | The archive folder was in **File Views > File Types > By Extension > Archives.**    Fig: Archives    Fig: Content of Archives  The thumbs.db was present in **File Views > File Types > By Extension > Databases.**    Fig: Navigation to Database    Fig: Content of Databases |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) | Done | 12/09/2025 | 7:29 PM NTP | To complete this, I first installed the ingest modules**: Hash Lookup**, **File Type Identification**, **Extension Mismatch Detector** and **Encryption Detection.**    Fig: Installation of required Ingest Modules  Under Analysis Result, we saw that **58** files with extension mismatch were detected.    Fig: Extension Mismatch Detected  At this point, we noticed that the ***wbkC1.tmp*** file, although saved as a **.tmp** extension, was an image file.    Fig: Content of wbkC1.tmp 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.    Fig: Hexadecimal Analysis of wbkC1.tmp file  For Entropy:  Under the **Encryption Suspected** items, there was a file named ***oembios.bin*** that showed a high entropy value of 7.999988.    Fig: Encryption Suspected    Fig: Content of Encryption Suspected |
| Internet History, favourites, etc.  Other browsers? | Done | 12/11/2025 | 11:55 AM NTP | First, I installed module named **Recent Activity**.    Fig: Installation of Recent Activity Module  Under **Data Artifacts**, we were able to see the ***Web History***.    Fig: Web History  We could see the many websites that the user, Bob Hunter, had visited.    Fig: Website Visited by Bob Hunter  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.    Fig: Website Bookmarked by Bob Hunter  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.    Fig: Use of Internet Explorer    Fig: Installation of Internet Explorer  However, it was observed that the user had also installed **Microsoft Edge**, which was visible under **Ingest Message > Browser Results**.    Fig: Browser Data Result |
| Emails, local and web-based. | Done | 12/11/2025 | 6:23 PM NTP | To complete this, I first installed two modules: **Keyword Search** and **Email Parser**.    Fig: Installation of Keyword Search and Email Parser module  When I navigated to **Data Artifacts > Installed Programs**, I observed that **Outlook Express**, a local email application, was installed on the system.    Fig: Installed Programs    Fig: Installation of Outlook Express  I examined the **Web Bookmarks** and observed that the user had **Hotmail**, which is a web-based email service.    Fig: Hotmail homepage Bookmarked  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** .    Fig: Email addresses with high messages  Upon reviewing the **Web History**, I observed evidence of **Yahoo**, which is also a web-based email service.    Fig: Visiting the website of Yahoo |
| Retrieve operating system information, accounts information, software, time zone information etc.). | Done | 12/11/2025 | 9:27 PM NTP | Under **Data Artifacts**, there was a section called **Operating System** **Information**, where we found some details about the Operating System.    Fig: Operating System Information    Fig: Details Regarding Operating System  Upon Zooming:    Fig: Details Regarding 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**:    Fig: Content of User Account information using Access Data Registry Viewer  Contents from **RegRipper:**        Fig: Content of User Account information using Reg Ripper  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.    Fig: Installed Programs    Fig: List of Installed Applications  To determine the ***time zones*** used by the system, I analysed the ***System*** registry file with **RegRipper** and obtained the relevant details.    Fig: Extraction of content of SYSTEM registry file using RegRipper    Fig: Time zone Information  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. | Done | 12/14/2025 | 2:45 PM NTP | To look at the timeline analysis, we first installed the **Plaso** ingest module.    Fig: Installation of Plaso Ingest Module  We navigated to **Timeline**.    Fig: Navigation 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.    Fig: Timeline content  We observed that **IMAPI.EXE** was the final program utilized on the computer after navigating to ***Details*** and scrolling to the end.    Fig: Last program executed  **IMAPI.EXE** executed between ***2002-06-05 00:40:01*** to ***2002-06-05 00:40:02***    Fig: Executed time of IMAPI.EXE  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.    Fig: System shutdown time |
| Registry analysis and  Registry protected area | Done | 12/14/2025 | 7:03 PM NTP | 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.    Fig: Extraction of Registry File content RegRipper    Fig: Extraction of contents of all Registry File using RegRipper  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.    Fig: SAM Registry File content  It was interesting to note the absence of **RID 1003**, which suggested a user account with that identifier had been deleted.    Fig: Other users  Using the **SecEvent.Evt** file located at windows/system32/config, I identified a deleted user with **RID 1003**.    Fig: Deletion of User Account named Owner  The **timezone** was taken from the ***SYSTEM*** registry file.    Fig: Time zone  During my analysis of the ***SOFTWARE*** registry file, I discovered which applications were installed on the system.        Fig: List of Installed Applications  The device was identified as **PC-V770KUX75EHT**, and no login credentials were configured.    Fig: System Information  During the analysis of the **system** registry hive, I identified multiple storage devices that were connected to the computer. Evidence of a primary hard drive, a floppy disk drive, and two optical disc drives was found. The examination also revealed that several removable storage devices were recognized by the system in February and June 2002. Additionally, two unique hardware identifiers were extracted, which may be associated with previously connected devices.      Fig: Mounted Devices |
| Link files and Recycle Bin | Done | 12/14/2025 | 10:48 PM NTP | The path to the link files was **Hunter XP for Dongled v6.E01 > vol2 > Documents and Settings > Bob Hunter > Recents**.    Fig: Link Files  The deleted files were located at **RECYCLER**.    Fig: Content of Recycle Bin |
| Instant Messaging clients | Done | 12/15/2025 | 8:33 PM NTP | I navigated to **Data Artifacts >** **Installed Programs** and saw two applications: **AOL Instant Messenger** and **Yahoo Messenger**, which were instant messaging client applications.    Fig: Installed Programs    Fig: Installation of AOL and Yahoo  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.    Fig: Timeline showing execution of AOL.exe |
| Clean-up/Wiping utilities. Check log files. Anything used? | Done | 12/16/2025 | 3:55 PM NTP | 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.    Fig: Run Programs    Fig: Execution of CLEANMGR.EXE  I opened the executable's activity in the timeline.    Fig: Execution of CLEANMGR.EXE seen through Timeline  The execution of **CLEANMGR.EXE** occurred a day prior to the system's final shutdown.    Fig: System final shutdown time |
| External drives; Network connections | Done | 12/17/2025 | 6:42 PM NTP | At first, we navigated to **Data Artifacts > USB Device Attached**.    Fig: 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.    Fig: Type of Devices Connected  In the ***SYSTEM*** Registry file, I found evidence of two connected **USB devices** along with their connection timestamps.    Fig : Connected USB Devices  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.    Fig: Network Information  I also found that the **RDP** service was enabled and listening on the default port **3389**, with no account lockout policy configured.    Fig: RDP policy and configuration  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.    Fig: Shared folder over network  I navigated to **Hunter XP for Dongled v6.E01 > vol2 > Documents and Settings > All Users > Application Data > Microsoft > Network > Connections > Pbk** and found the file ***rasphone.pbk***, indicating that VPN and remote access functionality had been used on the system.    Fig: Location of Pbk Folder    Fig: rasphone.pbk  I extracted **AppEvent.Evt**, **SecEvent.Evt** and **SysEvent.Evt** by navigating to **/img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/ config**.    Fig: Log files    Fig: Extraction of Files    Fig: Event files on my local machine  I reviewed the **SecEvent.Evt** log file using **Event Log Explorer** and noticed a successful **Logon Type 3**, which indicated that an individual accessed the shared content from over the network.    Fig: Log file content  While examining the **SysEvent.Evt**, I noticed that the computer had communicated with a computer named **RYAN-TOWER**.    Fig: Communication with the computer named RYAN-TOWER |
| Perform data carving | Done | 12/18/2025 | 1:04 AM NTP | **PhotoRec Carver** was chosen to run as an ingest module to perform data carving.    Fig: PhotoRec Carver Module  After executing the **PhotoRec Carver** module, a total of **2,137 deleted files** were recovered.    Fig: Deleted Files    Fig: Contents of Deleted Files  In **vol\_vol2**, a folder named **CarvedFiles** was identified, containing all carved files.    Fig: CarvedFiles    Fig: Contents of CarvedFiles |
| Run relevant keyword searches;  Did you index the evidence file? | Done | 12/18/2025 | 4:59 PM NTP | **1st Search:**  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.    Fig: searched for the term money    Fig: Blackmailing mail    Fig: Bank Account Information shared  **2nd Search:**  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.    Fig: searched for the term storage    Fig: Xdrive Login page    Fig: Transfer of data from FreeDrive to Xdrive  The evidence indicated that data was transferred successfully from **FreeDrive** to **XDrive**.  **3rd Search:**  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.    Fig: Searched for the term wipe    Fig: Web Search of BC Wipe    Fig: WipeDrive webpage content |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase | Done | 12/19/2025 | 6:44 AM NTP | 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.    Fig: SAM and SYSTEM registry file inside the folder named RecoverPassword  I opened the **Ophcrack** and uploaded the folder to get the **hash value** of the password.    Fig: Uploading the folder containing SAM and SYSTEM  After that I was presented with the hash value of the User Accounts.    Fig: Hash value of the user accounts  It was observed that three user IDs had the **NTLM** hash value ***31d6cfe0d16ae931b73c59d7e0c089c0***, indicating that no password was set for these 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.    Fig: Installation of Rainbow Table    Fig: Content of the Rainbow Table inside the Folder named Table  Then, I clicked on **Tables** and provided the file path as shown below.    Fig: Navigation to Tables    Fig: Selection of the Folder  After that I clicked on **Crack**.    Fig: Crack    Fig: Password Cracking Result  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 | Done | 12/20/2025 | 10:33 AM NTP | 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**, **.dll**, **.txt**, **.exe**, and **.bat**, which I then categorized within the **'File Views'** section by their respective extensions.    Fig: Different File Types  **Images:**  **Navigation**: **File Views > File Types > By Extension > Images**    Fig: Contents of Images  **Videos:**  **Navigation**: **File Views > File Types > By Extension > Videos**    Fig: Contents of Videos  **Audio:**  **Navigation**: **File Views > File Types > By Extension > Audio**    Fig: Contents of Audio  **Archives:**  **Navigation**: **File Views > File Types > By Extension > Archives**    Fig: Contents of Archives  **Databases:**  **Navigation**: **File Views > File Types > By Extension > Databases**    Fig: Contents of Databases  **HTML:**  **Navigation**: **File Views > File Types > Documents > HTML**    Fig: Contents of HTML  **Office:**  **Navigation**: **File Views > File Types > By Extension > Office**    Fig: Contents of Office  **Plain Text:**  **Navigation**: **File Views > File Types > By Extension > Plain Text**    Fig: Contents of Plain Text  **.exe:**  **Navigation**: **File Views > File Types > Executables > .exe**    Fig: Contents of .exe  **.dll:**  **Navigation**: **File Views > File Types > Executables > .dll**    Fig: Contents of .dll  **.bat:**  **Navigation**: **File Views > File Types > Executables > .bat**    Fig: Contents of .bat  **.cmd:**  **Navigation**: **File Views > File Types > Executables > .cmd**    Fig: Contents of .cmd  **.com:**  **Navigation**: **File Views > File Types > Executables > .com**    Fig: Contents of .com |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) | Done | 12/20/2025 | 11:30 AM NTP | 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.    Fig: Encryption Suspected    Fig: Analysis Result |
| Print artefacts | Done | 12/21/2025 | 1:22 PM NTP | The navigation path followed was **Hunter XP for Dongled v6.E01 > vol2 > Windows > System32 > Spool > Printers**.    Fig: Shadow file content    Fig: Shadow file content  Therefore, the print artifacts showed that print jobs were sent to the **‘HP LaserJet 2000 Series PCL’** and **‘Lexmark 252 Color Jetprinter’** printer, along with related spool (.spl) and shadow (.shd) files and their timestamps, which helped in tracing printed documents and system activity.  I also opened the ***SYSTEM*** registry file using **RegRipper** and observed entries indicating a printer connected to the PC.    Fig: Printer Information using SYSTEM Registry File  I also checked the **SysEvent.Evt** file using **Event Log Explorer** and observed connections for both printers shown in the ***SYSTEM*** registry analysis.    Fig: Log file indicating use of Printer    Fig: Log file indicating use of Printer |
| CD/DVD burning apps; check log files | Done | 12/23/2025 | 9:28 PM NTP | **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.    Fig: IMAPI.EXE present on computer  During timeline analysis, it was seen that **IMAPI.EXE** was the last program executed on the PC.  I extracted **AppEvent.Evt**, **SecEvent.Evt** and **SysEvent.Evt** by navigating to **/img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/ config**.    Fig: Log files    Fig: Extraction of Files    Fig: Event files on my local machine  Upon examining the **SysEvent.Evt** file using **Event Log Explorer**, I discovered that **IMAPI.EXE** had been executed.  Fig: IMAPI.EXE executed  **IMAPI.EXE** was executed multiple times on different days.      Fig: IMAPI.EXE executed on multiple days |
| Validate evidence integrity at the end of the examination | Done | 12/23/2025 | 12:10 PM NTP | At the end, the **Data Source Integrity** module was executed again to verify the hash value.  Navigation: Tools> Run Ingest Modules> Data Source Integrity    Fig: Data Source Integrity module  We clicked on the message type icon that appeared in the top right corner of the page.    Fig: Ingest Messages  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.    Fig: Completion of Data Source Integration module    Fig: Verification of Data Source Integration module  Finally, the computed hash values were:  Calculate hash: **dfcfe9ab9a60c6ad4a314656b687226b**  Stored hash: **dfcfe9ab9a60c6ad4a314656b687226b**  It was observed that the hash values recorded at the beginning and at the end of the examination remained unchanged, indicating that the evidence was neither altered nor corrupted during the forensic analysis. |

**Additional Notes/Artefacts Examined:**

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

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