**Contemporaneous Notes**

**Cyber Crime and Digital Evidence**

**A logo with blue and red text

Description automatically generated**

**Submitted by**

Name: Sidhant Kumar Chaurasiya

Student ID:10487

Cyber Security and digital forensics

Kathmandu, Nepal

# Contemporaneous Notes

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | Examiner | Sidhant Kumar Chaurasiya | Exam commenced | November 26th 2024 | | Other relevant information | Student number:- 24000865 | Software used, versions, and licensing | FTK Imager 4.7.12  Registry viewer 1.8.0.5  Autopsy 4.19.2  Event Log Explorer 4.8  Reg ripper 3.0  Is the software used in the investigation |   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 | Nov 26th 2024 | 12 A.M | For loading the image I use the FTK imager.  1. go to add evidence item. click on it to open.  2. select the sources evidence types as ”image file” .select next    3. select the image sources path. Click on finish    4. after clicking to finish we see the file like the screenshot given below.    5. after the image is successfully loaded. Left-click on the image and select the “verify drive image”.it takes some time to give the value after clicking on it.  6. after some time values are seen where there is the hash value of the file “ Hunter XP” which we are going to analyse |
| Load Case into a second forensic tool for dual verification of at least 2 key artifacts, evidence items | yes | Nov 26th 2024 | 12:20 P.M | The second tool I use to check the dual verification of at least 2 key artifacts in the autopsy  1. Double-click the autopsy tool to open it.  2. after opening the autopsy it looks like this.  3. to load a Case Select the new case. and give the case name and the path of the base directory. And check the case type (if you are doing it alone select single-user or if you are doing it in the group then choose multi-user)    4. after that give the optional information they ask for to know about the examiner select finished after the details given and it takes some time to make a new case file  5.select host and click next  6. then select the disk image or VM file and click next    7. select data sources and give the local disk location where there is a file for the image. Then select the time zone to the country where you are for easy understanding of file details    8. then select the configuration to ingest and click next    9. click on Hunter XP and go to the metadata. Check the hash value and verify it from the above imaging file of the FTK image if both are the same then the file is not changed/written by anyone |
| Time Zone Adjusted?  Report Time Zone used for Analysis. | yes | Nov  26th 2024 | 1 P.M | I adjusted the Time zone of the Hunter XP image file as per the UK local time which is (GMT +0:00) GMT Because the case is executed from the UK but we are doing forensics from Nepal. So for a better understanding of the case, we analysed the case in the UK time zone |
| Recover lost folders  (NTFS, FAT16&32). | yes | Nov 26th 2024 | 1:30 P.M | 1. The NTFS file can be found when we go to the tools and then go to the Run ingest Modules and select Hunter xp for dongled v6 E01    2. after that go to the photoRec Carver select it and click on the finished    3. after that go  Files Type🡪Deleted Files 🡪 Files System |
| Mount archives;  zip, thumbs.db, etc. | yes | Nov  26th 2024 | 2 P.M | 1. To find the Mount archived Zip file we must go to the file view go to file types, and then select by extension where we can see the archived files  Link:- /img\_Hunter XP for Dongled v6.E01/vol\_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df389.zip    2. to find the thumbs.db file we must go to HunterXP\volvol2\Documents & Settings\bobhunter\My Documents\My Pictures\HunterPics\Sabina & Christina location where we can find the file thumbs. DB |
| File signature analysis (any interesting file mismatch?); Compute hash values (enable entropy computation) | yes | Nov 26th 2024 | 3 P.M | 1. files signature analysis (any interesting mismatch) can be found when we go to the tools and then go to the Run ingest Modules and select Hunter xp for dongled v6 E01    2. then select encryption detection and then select finish.    3. Go to the Analysis Result🡪 Extension Mismatch Detected    4. here we can find the different file's signature mismatch we analyzed one file from extension mismatch detection by finding the hash value of that file from it    5. analysis the hash value of this file in HDX setup where we can hash value of the file where the first 4 values define the file types    6. then we check the hash value of aim10.tmp to verify that the file signature of that files is changed or not    From here we can say that the file signature is changed the file name is aim10.tmp which is a GIF file  7. also check the other to know how many file signatures are changed here we analyze an image    Here I see that these files we can see are actually JPEG and the files/evidence is tempering |
| Internet History, favorites, etc.  Other browsers? | yes | NOV  27TH  2024 | 10A.M | 1.here to find internet history I go to the   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/Documents and Settings/Bob Hunter/Local Settings/History/History.IE5/MSHist012002060320020604/index.dat. here I can see every file of the Internet history | |  |  |   2. here I can see all the internet history of Bob Hunter    These all are the websites visited by suspected “bob hunter”. In this index.dat file, we can see here that there are a lot of alleged app  3. for favourites I must go   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/Documents and Settings/Bob Hunter/Favorites |     All the favourite files are    3. to find another browser I go to web history and check all file program names and find that there is only one browser used which is Internet Explorer    Another method to find Internet History, favorites, etc.  Other browsers are simply go to the  Data Artifacts🡪Web Bookmarks/Web Cookies/Web History |
| Emails, local and web-based. | yes | NOV  27TH 2024 | 11:20 A.M | 1. to find the email I go to the files   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/getmsg[2]/getmsg[2]/0 |   Here I can see that there is an email ID of [friend@bemine.com](mailto:friend@bemine.com) and [chaser1191@hotmail.com](mailto:chaser1191@hotmail.com) also the email of chaser friend [billyray150b@netscape.com](mailto:billyray150b@netscape.com) here from the given screenshot I can also find out that Billyray was also involved in the case and share the email of father.        3. also I found more details of the case by analysing the email where I see the details of the discussion for ransomware and the file path of the image is   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad/memopad.dat |     4. by analyzing deeply I can find the conversation on the case and bargaining of the ransomware for the crime. The location of the file   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/Documents and Settings/Bob Hunter/Local Settings/Temporary Internet Files/Content.IE5/6ZSJ6T6D/or\_else[1].htm | |  |  | | |
| Retrieve operating system information, accounts information, software, time zone information etc.). | yes | NOV  27TH 2024 | 12 A.M | 1. I can found the information on the operation system of Hunter XP on the file data artifacts after that I go to the operating system information where I can see the whole details of OS and the source's path for the file is img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/config/software    2. I can find the account information by go to the LOCATION: Hunterxp/Partition 1/Noname/root/windows/system32/config and then left click it and export files after that I analyze the file name SAM by putting it into the reg ripper and convert that files into SAM.txt    Here we find the details about all the account user information where there is only one active user “Bob Hunter” and others are the system generated user    The other system generated users are    3. I can also find the time zone information from the above-exported files config where there is a file name system. where I can find the time zone information by analyzing the system file in reg ripper    From the daylight name which is Central Daylight Time, I can find out that the time zone is North America so the crime must be happening in North America |
| Timeline analysis-  Note date of last activity on the computer.system profiling | yes | NOV  27TH  2024 | 12:35 P.M | **1.** I can find the time analysis at the same file location at the SAM.txt whose converting process has been done on the above, here data of the last activity on the computer are found inside the SAM  Last Login Date : Tue Jun 4 23:01:54 2002 Z    I also found the last login date of the guest Last Login Date: Mon Jun 3 16:49:37 2002 Z    For timeline analysis    I can also go through the tool🡪Run ingest Modules🡪Hunter Xp 🡪 Plaso    After that click on the timeline    Here I get the details of File System, Web Activity and other at the yearly use |
| Registry analysis and  Registry protected area | yes | NOV  27TH  2024 | 12:50 P.M | I find the registry analysis and registry-protected area at the location   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/config/  Here I analyze the file that cannot be opened and copied by the system but can be exported by FTK Imager here I analyze file SAM, System, and others in the reg ripper | |
| Link files and Recycle Bin | yes | NOV  27TH  2024 | 1 P.M | 1. I found the link files at the location  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/Documents and Settings/Bob Hunter/Recent/ where I can see all 40 files link    2. I found 747 deleted files/images in the recycle bin where there is also an image suspected image captured in the recycle bin  At the location:   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df826.JPG |     As dived deep into the recycle bin I found the conversation between Chaser and Billy at the location:   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1040/HunterB/memopad/memopad.bak where they discuss about the family information and discuss about money |  |  |  | | --- | --- | |  |  | | |
| Instant Messaging clients | yes | NOV  27TH  22024 | 1:20 P.M | I found the instant massaging clients by opening the tool and selecting run to ingest module then selecting the file type identification and clicking on finished    After that I go to the location  /img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/config/software  Here I found the two massaging apps used that are  1. Yahoo messenger  2. AOL instant messenger |
| Clean-up/Wiping utilities. Check log files. Anything used? | yes | NOV  27TH 2024 | 1:40P.M | I can find the clean-up/wiping utilities at the location   |  |  | | --- | --- | |  | /img\_Hunter XP for Dongled v6.E01/vol\_vol2//$CarvedFiles/f0003340\_BestCrypt\_v\_7\_for\_Windows\_95\_98\_ME\_NT\_2000\_XP.html |   Here I found BCWipe software and  BestCrypt software and these both software is used for cleaning and wiping the disk |
| External drives; Network connections | yes | NOV 27TH  2024 | 2 P.M | 1.i can find out the network connection details/information at the location:   |  |  |  | | --- | --- | --- | |  | | /img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/drivers/etc/networks | |  | |  | |  | I can find the information about the external drives at the location  Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/Scsi , in this image Microsoft USB IntelliMouse Explorer is connected externally.    I also found other external drives connected at the LOCATION: Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/HID which is USB root Hub    I also found the other external drives at the LOCATION: Hunterxp/Partion1/Noname/root/windows/system32/control2set/enum/USB which is a CD-ROM Drive | | |
| Perform data carving | yes | NOV  27TH  2024 | 2:20P.M | 1. perform data carving to find deleted files that need to be recovered and also unallocated space needs to be analyzed for hidden or residual data. I find it by going to the tool opening run ingest module and then selecting Photorec carver    Then go to the location  /img\_Hunter XP for Dongled v6.E01/vol\_vol2//$CarvedFiles/    Here I can see all the deleted files |
| Run relevant keyword searches;  Did you index the evidence file? | yes | NOV  27TH  2024 | 2:40 P.M | I searched for relevant keywords to find the exact evidence file for Hunter that is mention in the screenshot    From this search, I found the details of the conversation between the father and chaser in the file “old\_index[1].htm” |
| Recover Log-on passwords –  use SAMInside/Ophcrack/Encase | yes | NOV  27TH  2024 | 3:10 P.M | To recover the log-on password I used the tool ophcrack in Linux. For this, I exported the config file from Windows to Linux where I used samdump2 to analyze it.    After doing this I put the output file which I get by using the command samdump2 system SAM -o and save it by name hello.txt and put the file hello.txt in ophcrack where the file analyzed and I get the result    From this hash value of Bob Hunter its proved that there is no login password |
| Examine different file types:  Export doc/office and exe files; look at Metadata if required | yes | NOV  27TH  2024 | 3:30 P.M | I found doc/office files by going to  files views and opening it and then selecting files types after that select by extension here you will see a document folder open it and click on office here we see all the doc/office files    Here I can see all the file types used that are doc, ppt, xls and the  File Metadata |
| Encryption, Steganalysis (any indications? Entropy or Autopsy can be used) | yes | NOV  27TH  2024 | 4:10 P.M | 1 I can find the encryption by going to the tool and then selecting run ingest modules and then selecting Encryption detection and then select  Finished    After that I go to the location  /img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/oembios.bin where I can found the Files with suspected encryption due to high entropy |
| Print artefacts | yes | NOV  27TH  2024 | 4:35 P.M | 1. I find the print artifacts at the location  /img\_Hunter XP for Dongled v6.E01/vol\_vol2/WINDOWS/system32/spool/PRINTERS/  Here I can see that there is two types of printer used. The name of the printer is Lexmark Z52 Color Jetprinter and the HP LaserJet 2200 Series PCL    Here I can also see that there is two types of files SHD and SPL.  SPL files Contain the raw print job data, including text, images, and formatting.  SHD files store metadata about the print job, such as job details and user information. |
| CD/DVD burning apps; check log files | yes | NOV  27TH  2024 | 4:45 P.M | I found the information and the app of CD/DVD burning at the location  /img\_Hunter XP for Dongled v6.E01/vol\_vol2/RECYCLER/S-1-5-21-1229272821-1580818891-854245398-1004/Df1017.JPG  Here I found the IMAPI It is a Microsoft API that provides developers with the ability to create applications capable of writing data to optical discs such as CDs, DVDs, and Blu-rays. It is not specifically designed for forensics but can be used to create accurate disc images or burn data for preservation or analysis. |
| Validate evidence integrity at the end of the examination | yes | NOV  27TH  2024 | 5:20 P.M | 1.for the validation of evidence integrity.  Tools🡪 Run ingest modules 🡪 Hunter Xp🡪Data Sources integrity    Here I find the details on email box which is located at the right sside corner    By clicking in it I can verify that my data integrity is maintained by checking the hash |

**Additional Notes/Artefacts Examined:**

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

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