Assignment No:02 Remart sign None: hayush Dipat chalke Raine: 13, class: 8(A) Subject: DF 1) What is Winders Forensic Analysis? Explain forensic Artifacts in detail • rinders forensic Analysis is the process of collecting explaining, and analyzine digital evidence from minders operating systems to investigate cybercrime poly violations, or security incidents. It focuses on itentifying user activities, system usage, file access, execution history, and maikcious actions without altering the original evidence: • Main objectives of mindows forensic Analysis: - Recover deleted or hidden data. - Establish timeline of events. - Support legal and coforate investigations - Detect Malware actirity and persistense - identify who did what, when, and how on a windors system. * forensic Artifacts forensic artifacts are digital traces automatically created by the wintons Of that record unser actions and system behavior. These artifacts are crucial for reconstructing events:. Teacher's Sica.:. Dato Discuss in detail windoms Recycle bin forensic 1: - The windows recycle bin holds files that have been removed by users but are still it when a user deletes a file This is hor windous operates by O deafuatt but a used can change the settings for the recycle bin to parman ently remove files without putting them there the windous recycle bin has a finite amount of storage Space the default timing for recycle bin in mindoris open a command - line terminal and change the unckeng directory to the $recycle Bin folder on the C: disk using the CO command. use the DIR Command with tkela switch to display contents of folder - use can use the co command to access the target account's recycle bin Once use knor rhich one it belongs to.!." the windors recycle bin has a finite anount of storage space, The datault timing for recycle bin in windor is 10% Of the arail able hard tire Spare. Teacher's Sign.: e Dote_ Forensic Artifacts: user Actirity : Recent filesl. docx, typet URLS Chat history. Program! - Install locations / timestamps Devices CusB): Mounted trines, USB history Netvork /logons s- Cachet credentials. lost logor Search for usemames or app licenses reveals peripherals, meb history and more. Q 3) A) Discuss in détail the investigating unix Syster : $\rightarrow$: The unix operating system is flexible poverfall and extreanty funtional - The unix operating. system funtionality makes it so poverfull and usefull as well as makes it a ehallenge to protect and investigate a You will use the data you collected during the initial response for the inrestigation Steps are as follons. Teacher's Sign.: