# Lab 3

## File System Forensics

---

**Shrutika Joshi – HA72777**

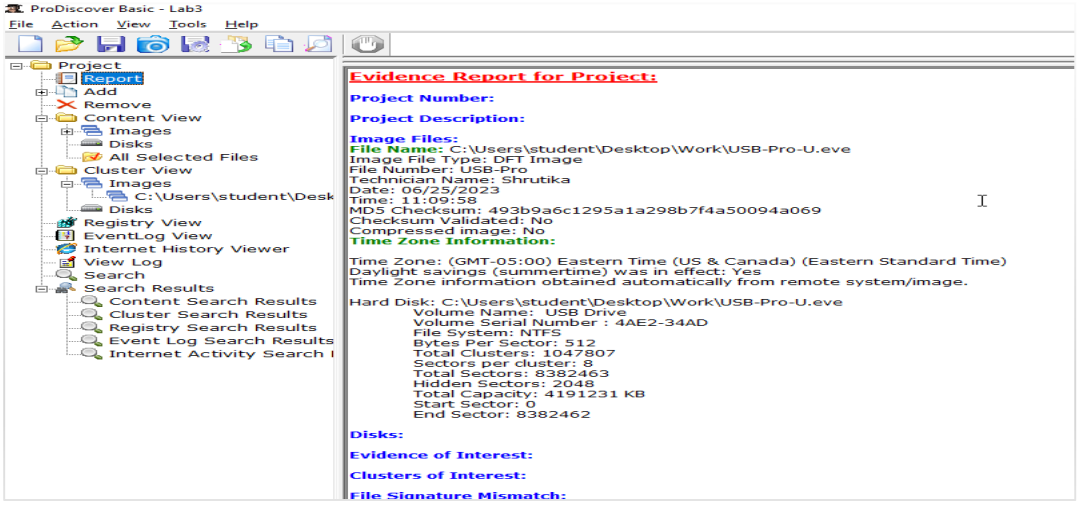
**Date – 26June23**

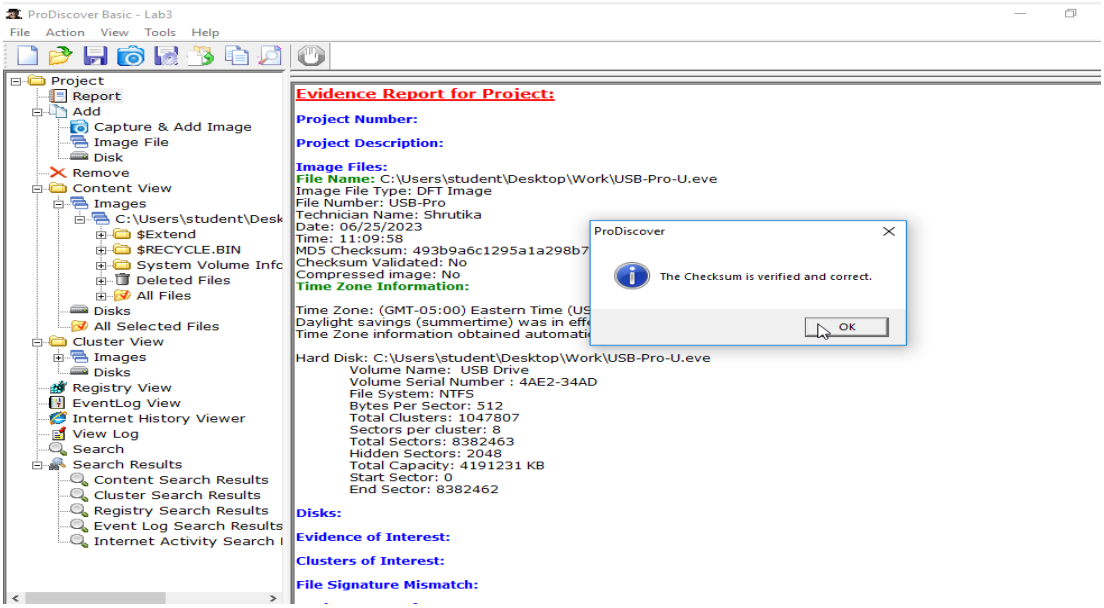
**Introduction –** As a forensics investigator, the goal is to analyze image of evidence which was collected before in working folder using image acquisition technique. This document outlines all steps and findings involve in analyzing the forensic image using ProDiscover and FTK Image tools.

**Equipment and Tools –** During this investigation ProDiscover and FTK Imager tools are being used to capture forensic image from USB drive.

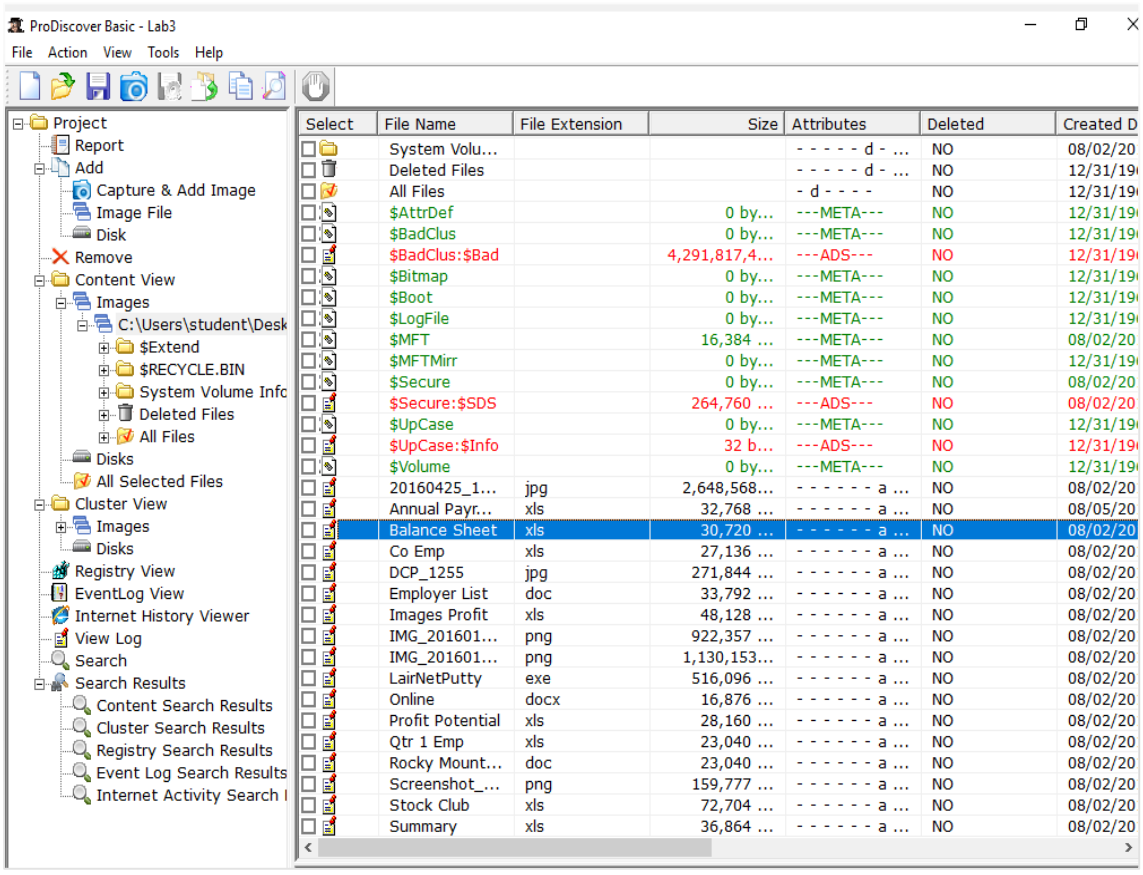
**Forensics Image Analysis using ProDiscover of drive (U :) –**

- Run the ProDiscover tool as an administrator and click on File → Open Image. Browse the image folder and add the image of (U :) drive created before.
- MD5 of file which wasn't verified. So I verified the checksum and below is a evidence report of after and before checksum verification.

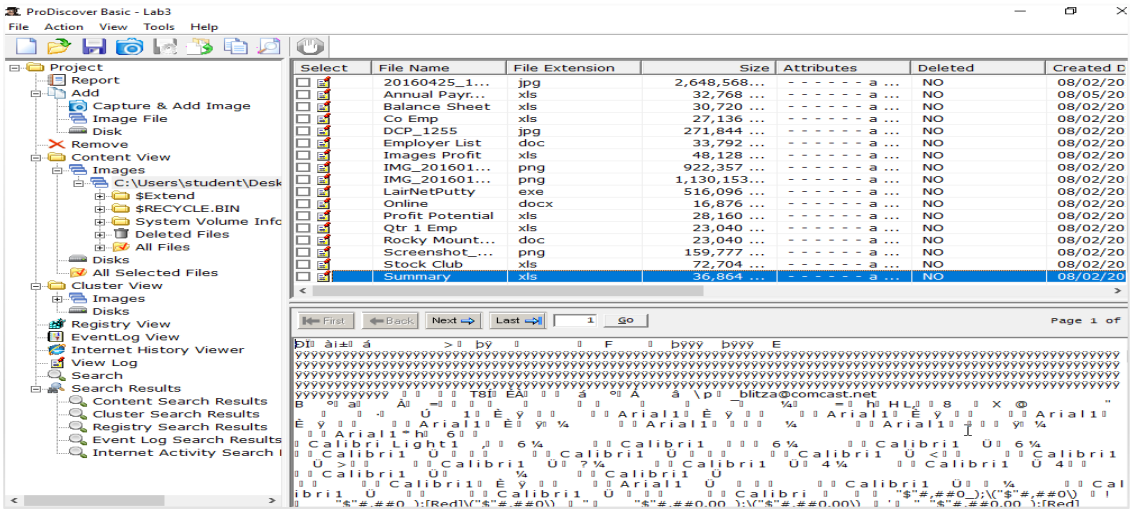




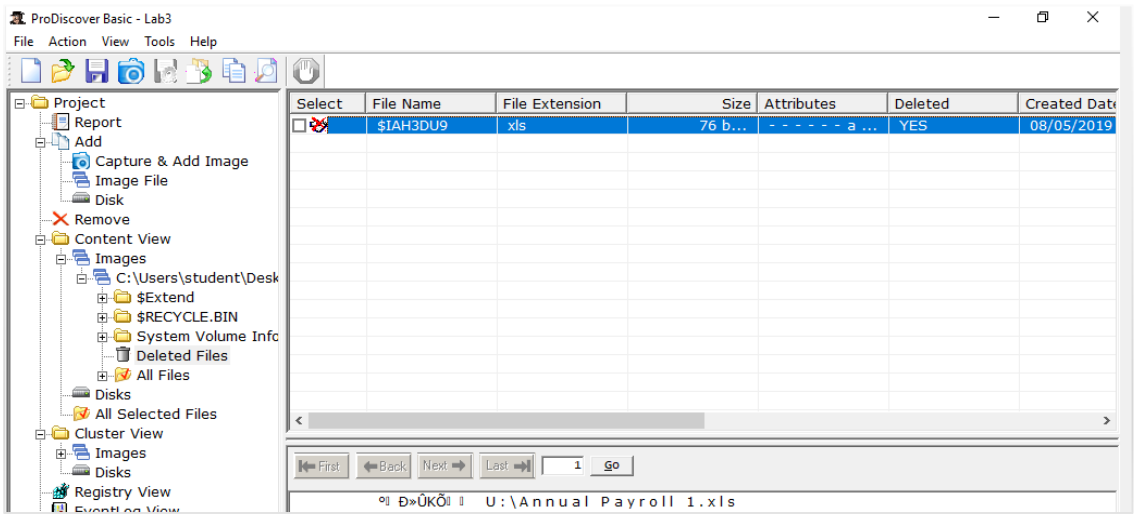

- Below image shows all the details of files and it shows LairNetPutty application which is suspicious to have. Also can see Annual Payroll files, Balance sheet, Employer list files which can have confidential or financial details attacker was looking for.



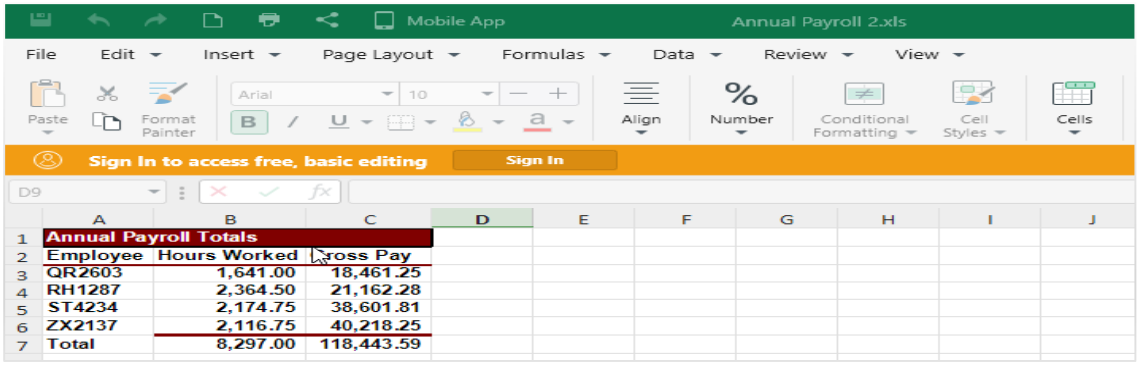
- From all the files content one domain is common I can see is **blitza@comcast.net** which is common in all this files



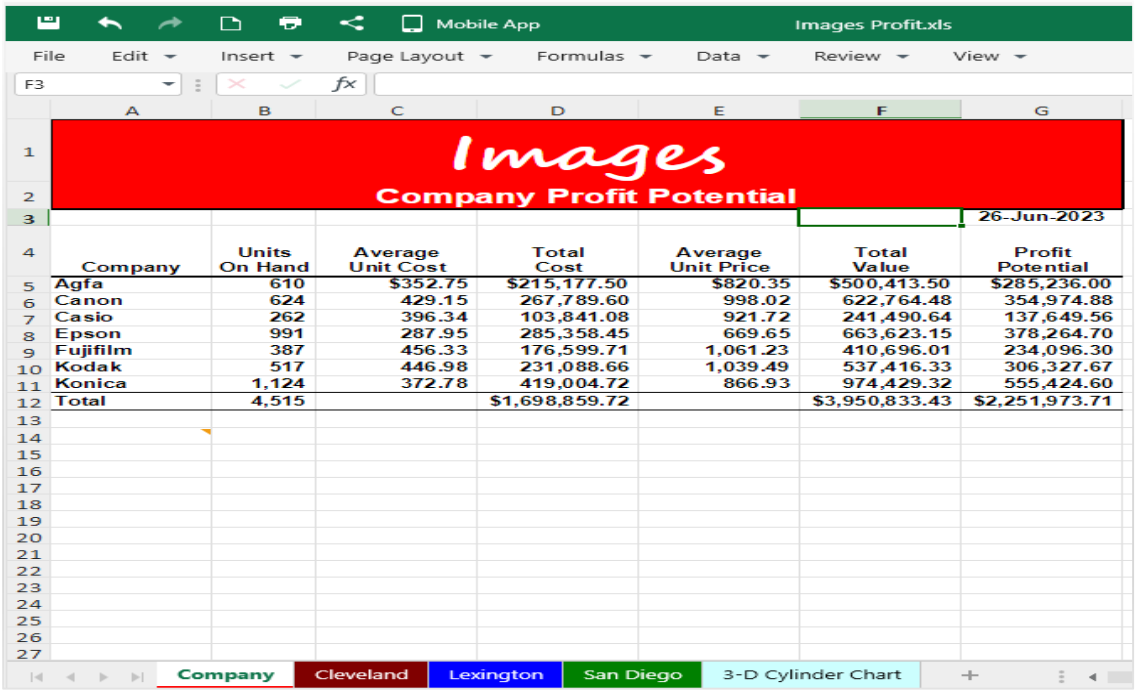

- Also can see Annual Payroll report file which was deleted. I am able to export the file but unable to view the content of file using excel.




- Below is a content of  Annual payroll, company profit details and Stock financial details report which are confidential files.



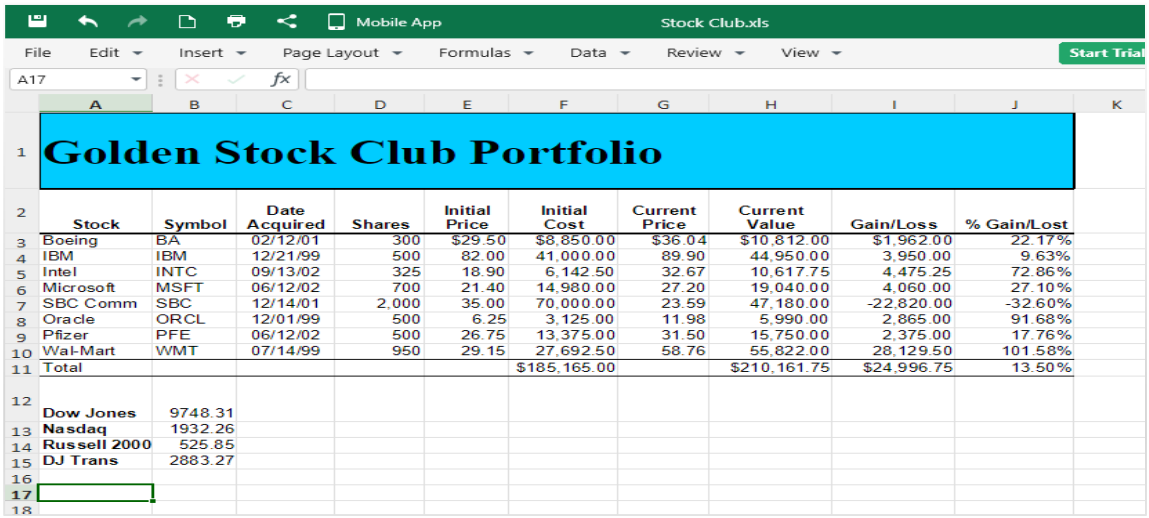

| Annual Payroll Totals | | |
|---|---|---|
| Employee | Hours Worked | Gross Pay |
| QR2603 | 1,641.00 | 18,461.25 |
| RH1287 | 2,364.50 | 21,162.28 |
| ST4234 | 2,174.75 | 38,601.81 |
| ZX2137 | 2,116.75 | 40,218.25 |
| Total | 8,297.00 | 118,443.59 |




# Images
## Company Profit Potential

26-Jun-2023

| Company | Units On Hand | Average Unit Cost | Total Cost | Average Unit Price | Total Value | Profit Potential |
|---|---|---|---|---|---|---|
| Agfa | 610 | $352.75 | $215,177.50 | $820.35 | $500,413.50 | $285,236.00 |
| Canon | 624 | 429.15 | 267,789.60 | 998.02 | 622,764.48 | 354,974.88 |
| Casio | 262 | 396.34 | 103,841.08 | 921.72 | 241,490.64 | 137,649.56 |
| Epson | 991 | 287.95 | 285,358.45 | 669.65 | 663,623.15 | 378,264.70 |
| Fujifilm | 387 | 456.33 | 176,599.71 | 1,061.23 | 410,696.01 | 234,096.30 |
| Kodak | 517 | 446.98 | 231,088.66 | 1,039.49 | 537,416.33 | 306,327.67 |
| Konica | 1,124 | 372.78 | 419,004.72 | 866.93 | 974,429.32 | 555,424.60 |
| Total | 4,515 | | $1,698,859.72 | | $3,950,833.43 | $2,251,973.71 |



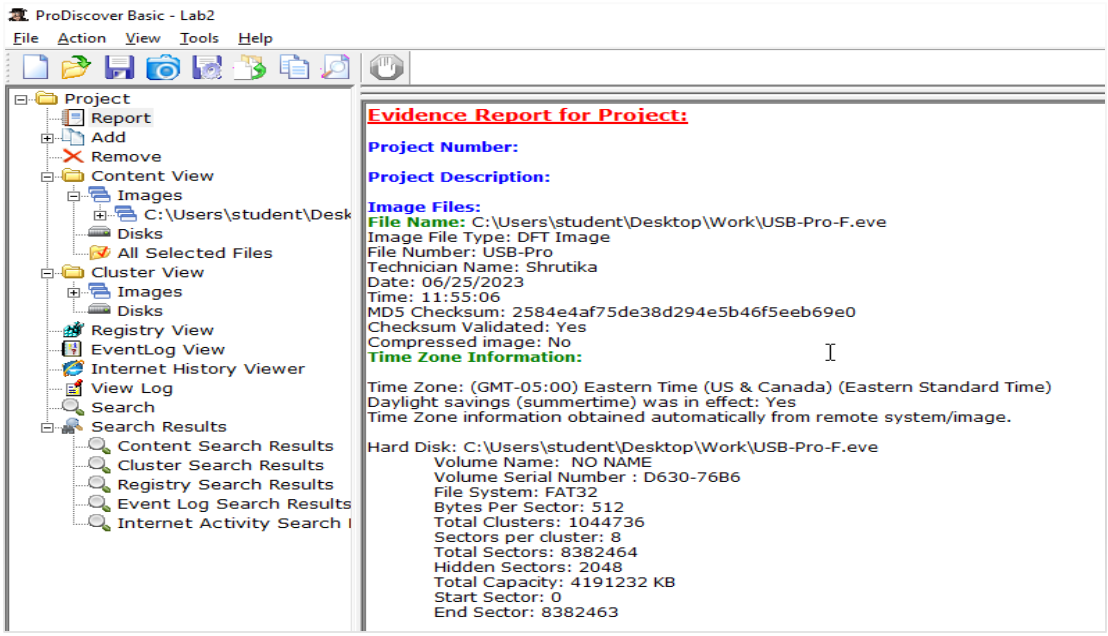

# Golden Stock Club Portfolio

| Stock | Symbol | Date Acquired | Shares | Initial Price | Initial Cost | Current Price | Current Value | Gain/Loss | % Gain/Lost |
|---|---|---|---|---|---|---|---|---|---|
| Boeing | BA | 02/12/01 | 300 | $29.50 | $8,850.00 | $36.04 | $10,812.00 | $1,962.00 | 22.17% |
| IBM | IBM | 12/21/99 | 500 | 82.00 | 41,000.00 | 89.90 | 44,950.00 | 3,950.00 | 9.63% |
| Intel | INTC | 09/13/02 | 325 | 18.90 | 6,142.50 | 32.67 | 10,617.75 | 4,475.25 | 72.86% |
| Microsoft | MSFT | 06/12/02 | 700 | 21.40 | 14,980.00 | 27.20 | 19,040.00 | 4,060.00 | 27.10% |
| SBC Comm | SBC | 12/14/01 | 2,000 | 35.00 | 70,000.00 | 23.59 | 47,180.00 | -22,820.00 | -32.60% |
| Oracle | ORCL | 12/01/99 | 500 | 6.25 | 3,125.00 | 11.98 | 5,990.00 | 2,865.00 | 91.68% |
| Pfizer | PFE | 06/12/02 | 500 | 26.75 | 13,375.00 | 31.50 | 15,750.00 | 2,375.00 | 17.76% |
| Wal-Mart | WMT | 07/14/99 | 950 | 29.15 | 27,692.50 | 58.76 | 55,822.00 | 28,129.50 | 101.58% |
| Total | | | | | $185,165.00 | | $210,161.75 | $24,996.75 | 13.50% |

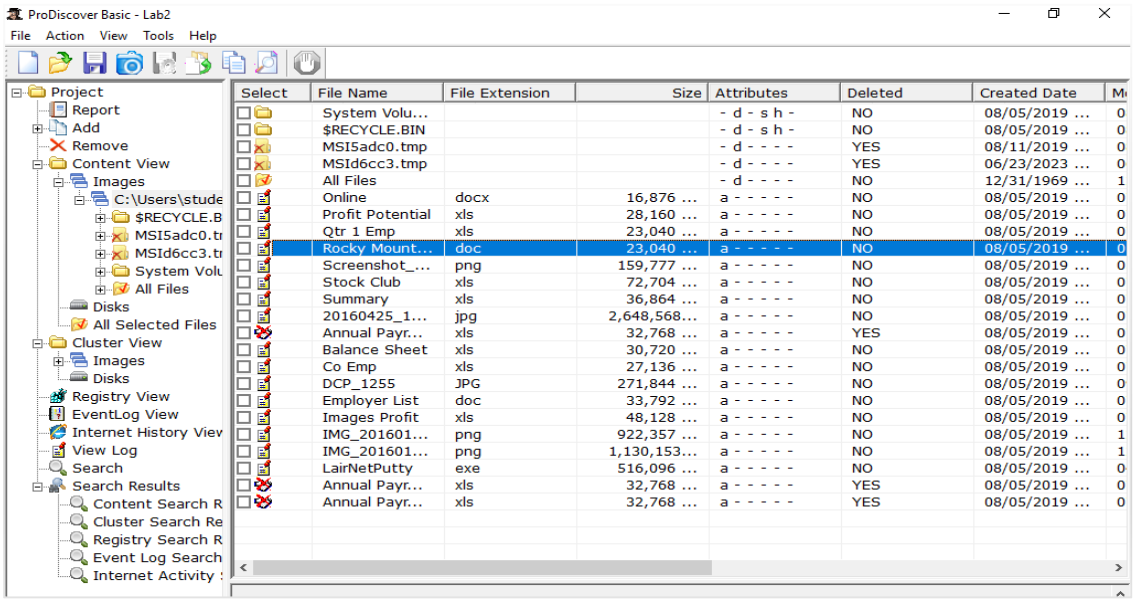
| | |
|---|---|
| Dow Jones | 9748.31 |
| Nasdaq | 1932.26 |
| Russell 2000 | 525.85 |
| DJ Trans | 2883.27 |

## Forensics Image Analysis using ProDiscover of drive (F :)–

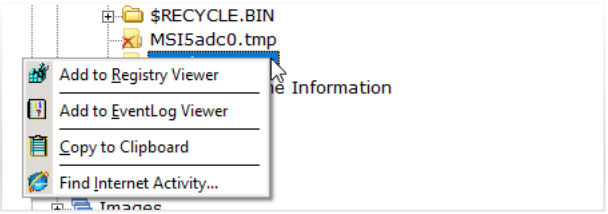
- After following the same steps and verified the checksum below is a evidence report generated by ProDiscover and MDF5 hash given

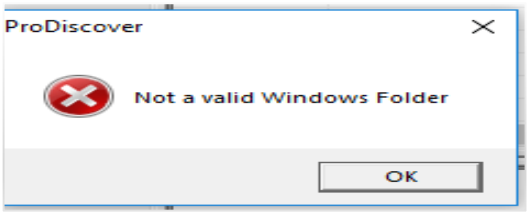



- Below are the total files capture in the forensic image which contains all the financial and confidential details files such as Annual Payroll, Balance sheet and also contain two temp folders (MSI5adc0.tmp, MSId6cc3.tmp) which I am not able to export but after checking the registry of file it did seems suspicious.

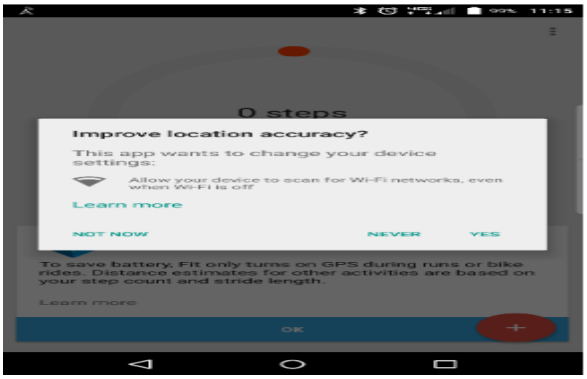


- After checking the registry of temp files it is showing not a valid windows folder which is kind of suspicious.



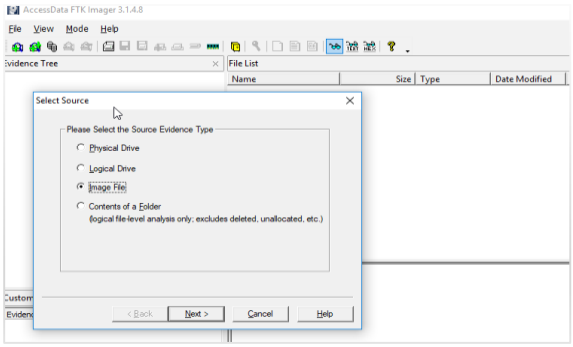



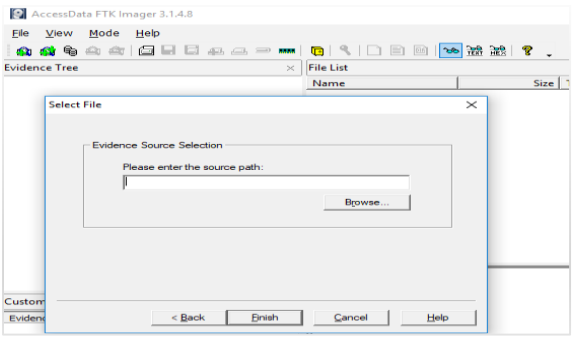

- Below image shows that some application might have tried to change the device settings and asking permission to scan for wifi networks. This can be the entry point of attack. So more analysis should be done on this which is the app and what changes this application have done.



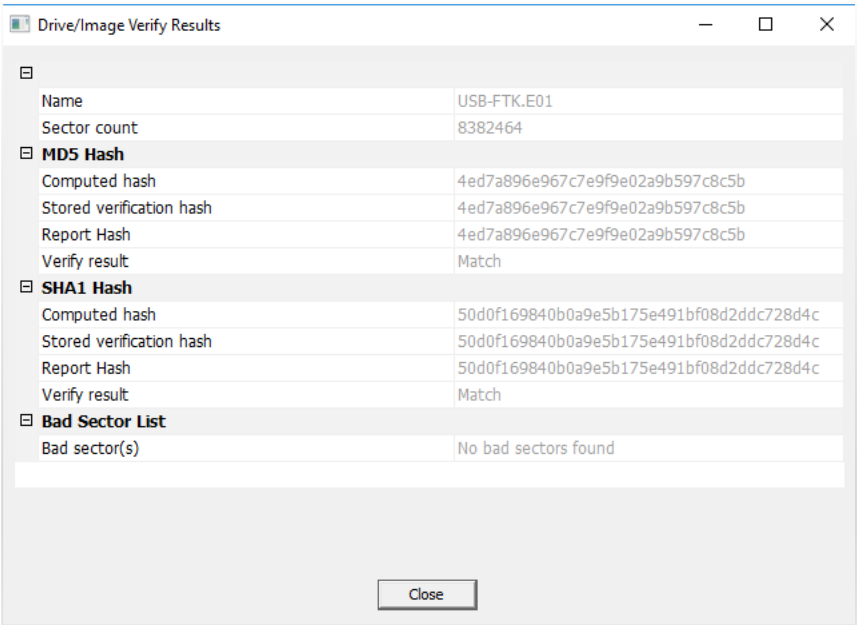

## Forensics Image Analysis using FTK Imager of drive (U:) –

- Run the FTK Imager tools as an administrator and click on file option from top left corner, then File → Add Evidence Item. In the select source select ‘Image File’ option and click ‘Next’.You will get option to select source path of image. Click on Browse option and select the image which need to analyze and click on Finish button. It will load the image for analysis.

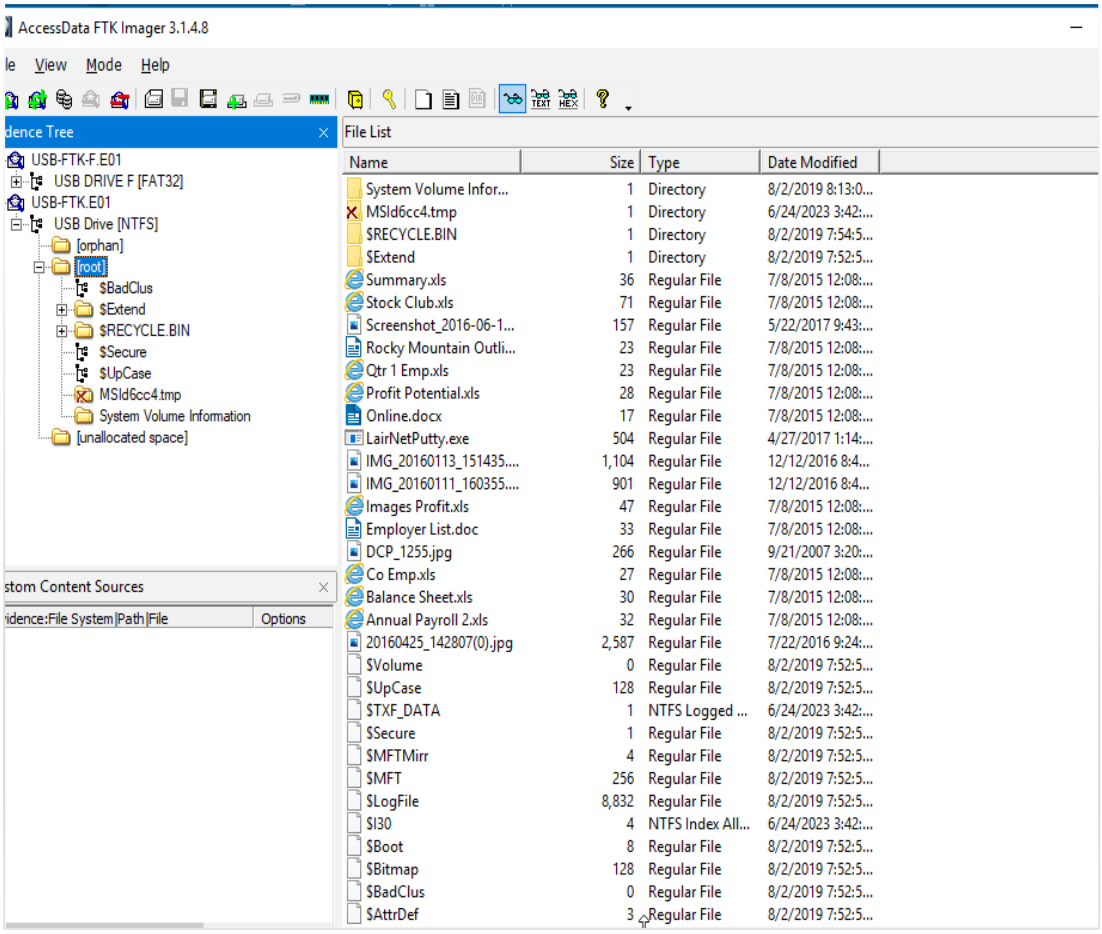


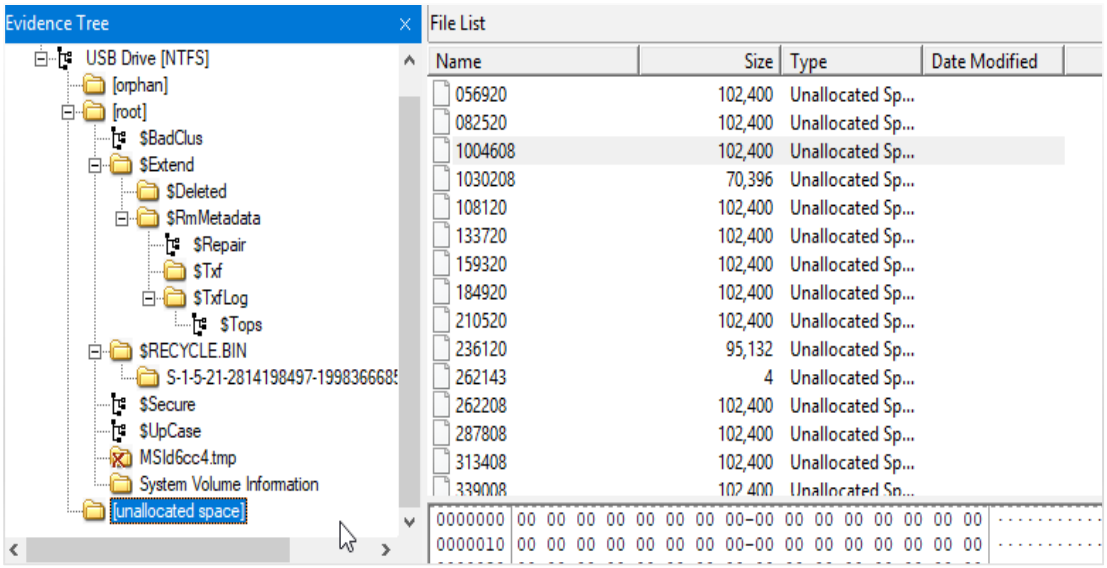
- Below are hash of file in MD5 and SHA1 format




- After loading the image it shows all folders and files from the USB drive, including the files which were deleted, metadata of files, orphan files, and unallocated space and file system slack. It also shows the files from recycle bin and all temp files. It is important to check all this as this files may contain some evidence we are looking for.
- During forensics investigation, unallocated space is often examined to recover deleted or hidden data/information because this space may contain remnants of deleted files, temporary files, data fragments or other artifacts of forensic interest
- While looking at the USB drive it is clear that this image is taken from windows machine as NTFS file system is a default file system used by Windows.
- There is one deleted temp folder and one file namely MSId6cc4.tmp and $IAH3DU9.xls and I am able to recover the file and folder. But there is no content in the folder MSId6cc4.tmp and it seems file **'$IAH3DU9.xls'** is an **'Annual Payroll file'** by looking at the metadata of file.
- There are no files in Orphan folder.

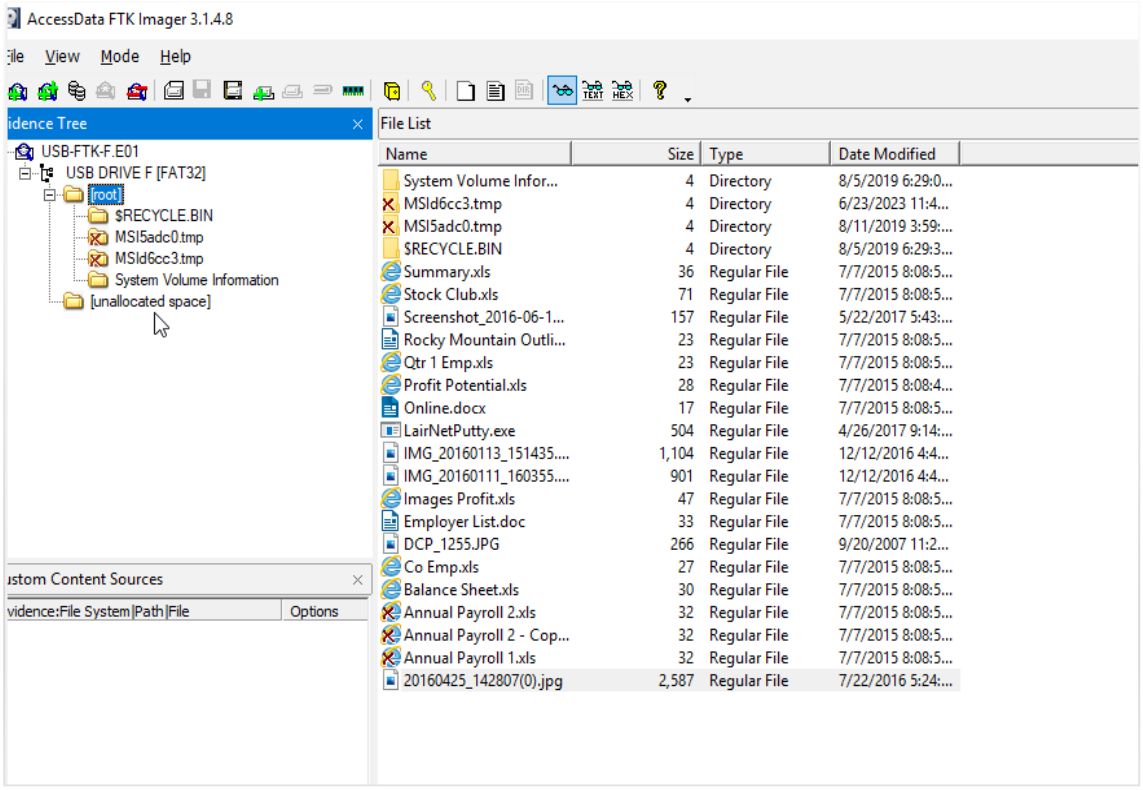



- There are many files in unallocated space as well. But since the image is logical, file details cannot be extracted from this files.

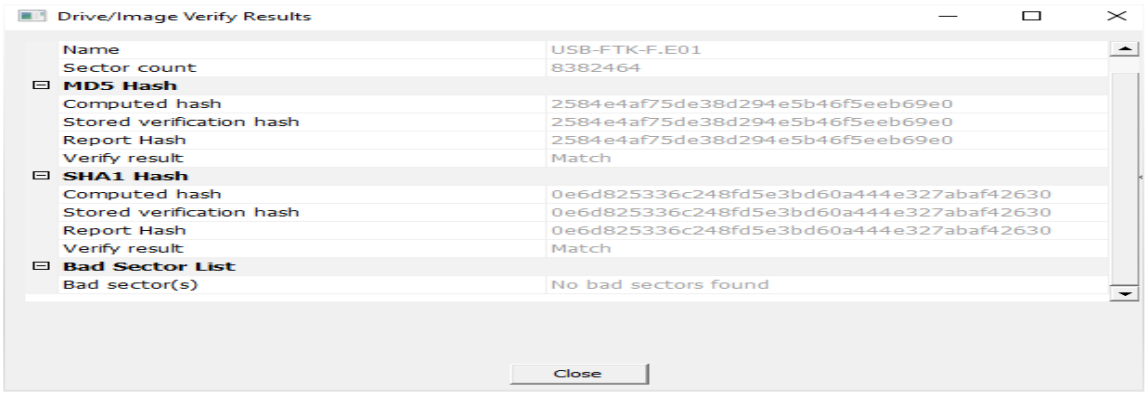


## Forensics Image Analysis using FTK Imager of drive (F:) –

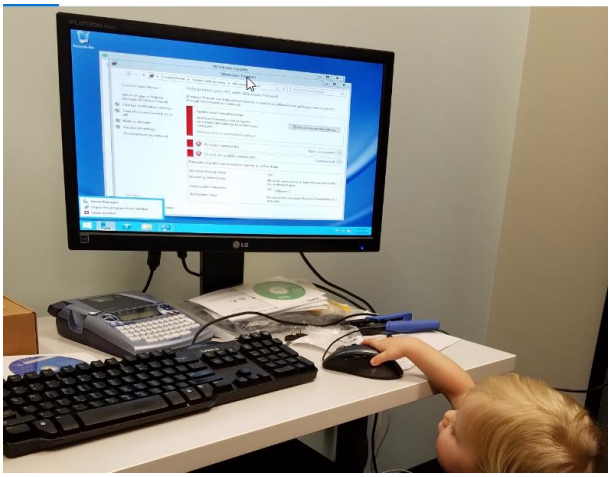
- After performing the same steps for loading the forensic image below are all the files from USB drive (F:) image. I tried to extract details from temp folders but there no files showing after extracting the folders. Also this image contains all the confidential financial files such as Annual Payroll and Balance sheet. LairNetPutty.exe application is allows to run program on remote computer which attacker can as well use to run malicious payloads.

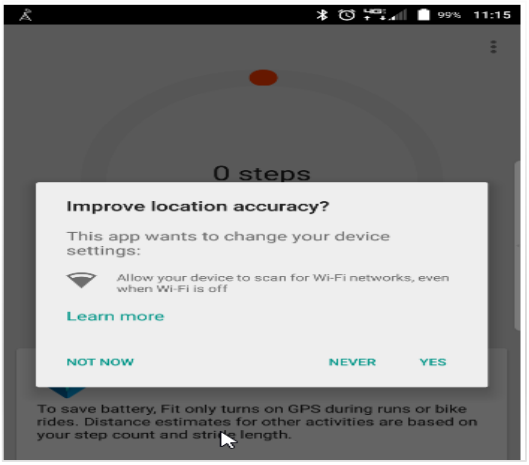



- Below are hash of file in MD5 and SHA1 format

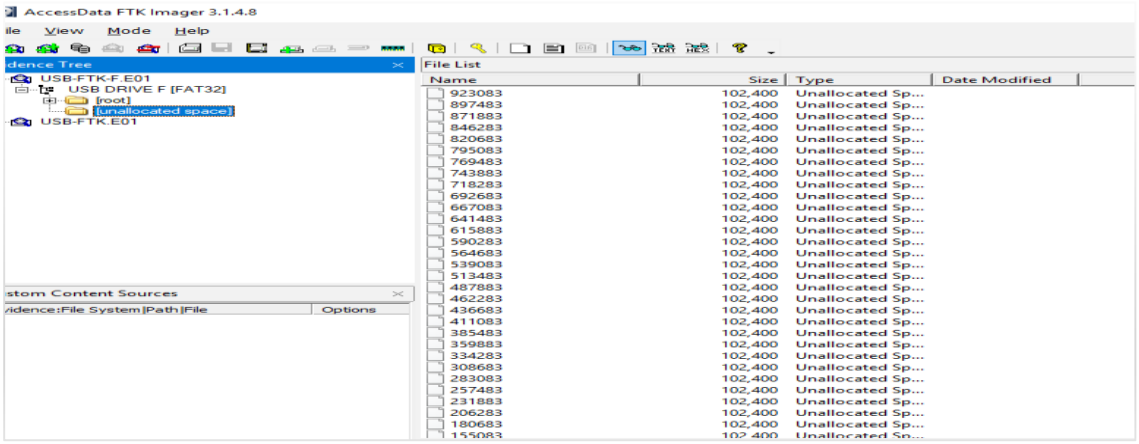


- Below is an evidence of a child closing the turning off firewall setting on windows which might have allowed malicious application. Also shows one more application making changes to device setting and allowing wifi scanning which looks suspicious.





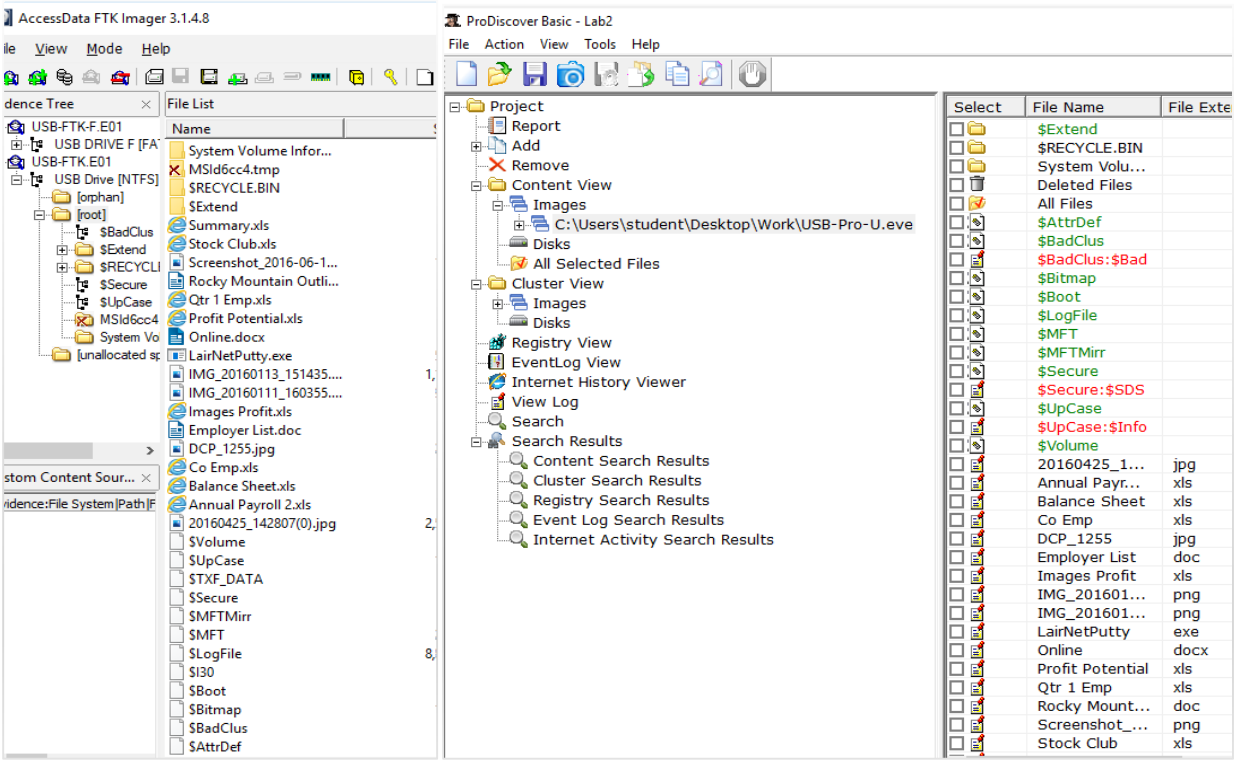

- Below are unallocated spaces but since this is logical forensics image details from this spaces cannot be extracted

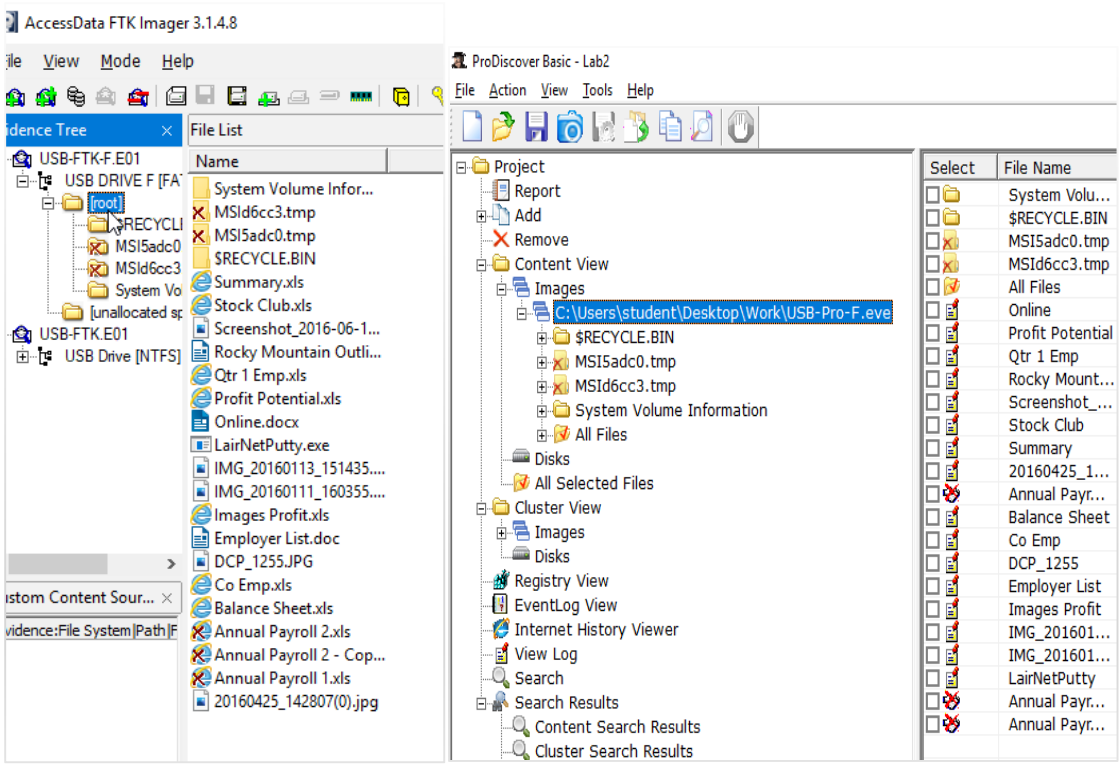



## Analysis and Conclusion of all the forensic images –

- After analyzing USB drive (U: and F:) using ProDiscover and FTK analyzer, it is concluded that forensics image filehash of both drives using ProDiscover and FTK Imager are different as each forensic tool uses different method for analysis and hence there are variations in the analysis and output for the same image.

- Each forensic tool may interpret file formats differently. Also there are algorithmic differences which each forensics tool uses.
- From the above image it is also concluded that each forensic tool extract different metadata such as user information, images unallocated spaces, and files which result in different filehash. Hence during forensic investigation, forensic examiner prefer to use different tools during investigation.
- LairNetPutty is a application showing in all of the images which should be more investigated as Putty application allows to run program on remote computer which attacker can as well use to run malicious code.
- Also there are some temp files which looks suspicious
- **File differences in each tool:** Considering the below snap, most of the files are present in both the folders except unallocated space folder which is visible in FTK Imager






- Personally I would prefer to use ProDiscover tools and it is more user friendly and provides better view of files as compare to FTK imager. Also it provides a wide range of features beyond just imaging. It offers disk imaging, file recovery, keyword searching, and analysis capabilities.
- Comparing forensic images from USB drives (F: and U :), I notice that metadata files are missing in USB drive (F :) . In some cases, perpetrators may intentionally hide or delete metadata files to cover their tracks. They might employ techniques like file encryption, file hiding, or deliberate deletion to make it difficult for investigators to retrieve the metadata files during the imaging process.

## Citations-

[1]. Sethi, Abhinav. “Importance of using MD5 and SHA1 Hash Algorithms in Digital Forensics” Steller Data Recovery Blog, 12June2020, https://www.stellarinfo.com/blog/hash-values-in-digital-forensics/ .

[2]. Ch, Raj, and el. “USB Forensics: Detection & Investigation.” *Hacking Articles*, 9 Sept. 2020, www.hackingarticles.in/usb-forensics-detection-investigation/.

[3]. Smith, J. D. (2015). Forensics Analysis of USB Flash Drives in Educational Environment. Journal of Digital Forensics, Security and Law, 10(2), 123-137. Retrieved from ResearchGate:https://www.researchgate.net/publication/271825884_Forensics_Analysis_of_USB_Flash_Drives_in_Educational_Environment

[4]. Kessler, Gary. “The Impact of MD5 File Hash Collisions on Digital Forensic Imaging.” *Journal of Digital Forensics, Security and Law*, vol. 9, 2016, https://doi.org/10.15394/jdfsl.2016.1431 . Accessed 6 Dec. 2019.

[5]. Jenkinson, Tristan. “The Importance of Data That Doesn’t Exist – Part Three (Missing Metadata – a Case Study).” *The EDiscovery Channel*, 27 Feb. 2023, ediscoverychannel.com/2023/02/27/the-importance-of-data-that-doesnt-exist-part-three-missing-metadata-a-case-study/. Accessed 26 June 2023.