# Case 1337

Graphical user interface, text, application

Description automatically generated Hash Value.

No information was given about which case this VHD is from as file was not opened to minimise data contamination. So, I have been searching through all the data to see what evidence I can find and see what crimes if any have been committed by the owner.

First, I have created a new case on autopsy and uploaded the VHD onto it and let it do its thing and extract information from it that I can search through to see if I can find any evidence against this person.

## Appendix of Evidence Gathered in Timeline Structure :

Graphical user interface, text, application

Description automatically generatedEvidence extracted from VHD.

Table

Description automatically generatedWindows XP OS. Downloaded 29/08/03. Keith Lockhart.

Table

Description automatically generated

Table

Description automatically generated

9 accounts on the system. Elvis Admin was last to logon.

Graphical user interface, text, table

Description automatically generated

Table

Description automatically generated

Suspicious password protected files.



Text, letter

Description automatically generated

Graphical user interface, table

Description automatically generated

A picture containing diagram

Description automatically generated A picture containing text

Description automatically generated

Diagram

Description automatically generated26/09/03 10.31.04 – 10.34.06

Shape, rectangle

Description automatically generated Easy Target?Graphical user interface, text, application, Word

Description automatically generated26/09/03 10.36.50

Text, letter

Description automatically generated26/09/03 17.39.18

A picture containing chart

Description automatically generatedText, letter

Description automatically generated 26/09/03 10.49.20

Text

Description automatically generated

Text

Description automatically generated

Text

Description automatically generated

Graphical user interface, text

Description automatically generated

password protected suspicious file.

Text

Description automatically generated with medium confidence

All from the same account. (Secret User).

Graphical user interface, text

Description automatically generated



# Final Reporting

From the evidence I have gathered through the VHD I have reasonable suspicion that the owner of the device (Keith Lockhart) has committed crimes such as forgery of legal documents and fraud.

The owner of the VHD downloaded an operating system for this device on 29/08/03 under the name Keith Lockhart. All evidence gathered was from events taken place soon after installing this OS with time stamps.

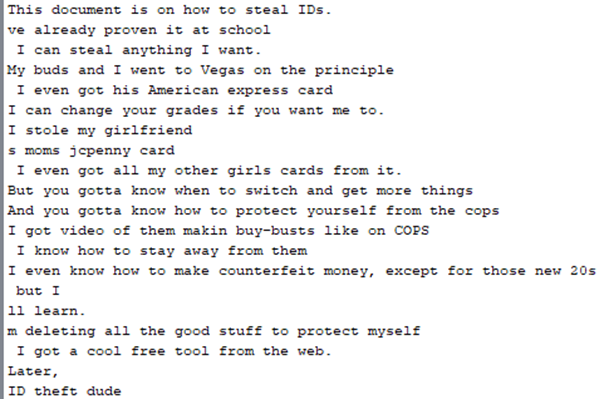
On the VHD I have found there to be an email address owned by the owner of the system. The email address itself is very obviously named and looking through more evidence we can see that the user does not seem to try and hide suspicious files. These files seem to just be named for what they are to make it easier for him and us to find. Email address is [id.theft.dude@fakeid.com](mailto:id.theft.dude@fakeid.com).

Evidence 4 shows many password protected files with highly suspicious file names. If the pattern remains the same, then these file names should be very literal with what is inside them and I believe if we are able to gain access to these files, we will find even more incriminating evidence. The file names are things like “Card Numbers” and “customer base”.

Table

Description automatically generated

Evidence 5 shows either a journal type document or a message he is sending to someone else to gloat. The user sounds very young and talks about how he goes to school in other screenshots of text documents. From these documents it sounds like he enjoys scamming people as he gets a rush from it. The document shows him admitting that he knows how to make counterfeit money and him saying “I can steal anything I want”. Just looking at the document there’s a lot of things he has admitted incriminating himself such as stealing credit cards from girlfriends’ mothers and stealing American express cards from the principal of his school.



Evidence 6 just shows after everything previously spoken of the user then uploads images of many different things from passports to licenses to detailed images of bills. Most likely so he can create counterfeits of each. After this Keith uploads/saves a html document of a fake website. I believe this is to attract unsuspecting individuals in order to get their private information from them in order to create more fake documents/cards. A few minutes later an image is uploaded of an email of a customer. The image is saved as ‘’this is why JC Penny’’ to show reason of his choice of attacking this brand and its customer base. In the screenshot we can see JC Penny is receiving complaints for its bad customer service as this customer has been clearly scammed of her money and there was fraud being done on her account, but JC Penny did not do anything about it. So, this user sees this company and its customers as a very easy target as they rarely take action.

Not much more evidence is found for that time period, of September, until a few months later in November. The next few pieces of evidence have been last edited by the user between 30/11/03 10.34am – 30/11/03 12.56pm. Evidence 10 is a document explaining how when he was in summer school (again showing how he is of young age and in school) that he stole his principles wallet and his credit card which he then used to buy plane tickets which he never used. All these documents end with him referring to himself as “ID Dude”. In the rest of the evidence between these times you can see “ID Dude” confessing to what crimes he has committed in a gloat type manner as if he is proud of himself and what he has been doing.

All of the evidence for those documents and most of the others were all from the user ‘secret user’ showing he somewhat tried to hide who was doing it.

Either Keith Lockhart is the ID theft Dude, or he has connections with him and knows something that can be useful to us due to evidence number 17 showing us Keith being in contact with him on multiple occasions.

In conclusion I believe I have found enough evidence to prove that the owner of this system has been dealing in fraud and counterfeits of different kinds. Keith Lockhart is either behind it, is working with the criminal or has information on the one behind it all. However, he is the owner of the VHD as it is under his name and the evidence points to him being the one creating fake IDS and other crimes such as stealing wallets and cards from people he knows.