University of Sunderland

Cyber Crime Unit (CCU)

WITNESS STATEMENT

Statement of	**:**	Michael Musoke
Occupation	**:**	Junior Digital Forensic Analyst

This statement (consisting of 007 page(s) is true to the best of my knowledge and belief and I make it knowing that, if it is tendered in evidence, I shall be liable to prosecution if I have wilfully stated in it anything which I know to be false or do not believe to be true.

Date	**:**	06/05/2023
Signature	**:**	*M. Musoke*

1. Introduction

1.1. I have been commissioned to produce this report by University of Sunderland's Cyber Crime Unit (CCU). This is an investigation of a network capture, exhibit ev001_exABC.pcap, which contains data that was transmitted over the network. This report will include the recovery of data that was transmitted, the method used to recover the data and the value of the evidence that data holds. This report will also show how the exhibit ev001_exABC.pcap's integrity was maintained throughout the process.

1.2. This report describes my findings and contemporaneous notes of my actions are available in Appendix A of this document (notes_ev001_evABC).

2. Instructions

2.1. I have been instructed to examine the exhibit ev001_exABC, which contains a network capture and construct a report which answers the following **two** questions:

Question 1 – What files have been transferred in the network capture?
From the exhibit ev001_exABC files were transferred using protocol ftp-data and contained:

1. STOR PLAN.odt – contains instructions on what each member of the group was going to be positioned.
2. STOR exterior_gb.JPG -An image of the exterior of a building
3. STOR gb_blueprint.jpg – An image of layout of a banking institution
4. STOR escape_route.JPG- An image of an empty street.
5. STOR equipment_list.ods- A spreadsheet of list of items.

Question 2 – What intelligence can you gather on the type of crime being planned?
The evidence gathered the from the exhibit ev001_exABC would suggest that the crime being planned is a bank heist. The instructions in STOC PLAN.odt has headings Target Gotham Bank and instructions for the team to take up position in the bank. An image of the blueprint of the bank helps the individuals know where to be before the heist begins. The image escape route shows where the team would use to get away. The spreadsheet shows a list of items that are going to be used during the heist.

3. Forensic Examination of ev001_exABC

3.1. At approximately 10:30 on 06/05/2023, I commenced examination of exhibit ev001_exABC. This is a network capture file, captured using Wireshark (v3.6.6) on 04/12/2022.

3.2. The MD5 of ev001_exABC was found to be "95548375fc8b1685002fe3943b7b01e3", which was checked against the chain of custody prepared by the seizing officer. The evidence file MD5 and the MD5 recorded on the chain of custody were identical, meaning that no data has been altered since I received the file.

3.3. The Association of Chief Police Officers (ACPO) have produced a Good Practice Guide for Digital Evidence, which is structured on four principles. These principles have been upheld through this investigation as follows:

3.3.1. Principle 1:

Principle 1 states that no action taken by the law enforcement agencies, persons employed within those agencies, or their agents should change the data which may subsequently be relied upon in court. Any changes would make the evidence inadmissible in court. I achieved this by comparing the MD5 checksum before and after my investigation. Refer to Appendix A Figure 1 of this document.

3.3.2. Principle 2:

Principal 2 states that in circumstances where a person finds it necessary to access the original data, that person must be competent to do so and able to give evidence explaining relevance and implications of their actions. I adhered to this principle because of the training I undertook in Network recovery module, where I learnt the techniques of how recovery data that has been transmitted on a network. CCU has commissioned me to produce a report of the findings of the investigation. To do this I need to access the evidence.

3.3.3. Principle 3:

I have kept contemporaneous notes throughout my investigation. These notes can be found in Appendix A of this document (notes_ev001_evABC)

3.3.4. Principle 4:

The officer in charge CETM30 has been kept informed of my progress in the investigation and all of the evidence that is presented in this document has been collected with integrity.

4. Question 1 – What files have been transferred in the network capture?

4.1. Exhibit ev001_exABC was found to contain,

Filename	Transfer Protocol	Timestamp	Description
	ftp	2022-12-04 12:51:12	Login details: student password sunderland
STOR Plan.odt	ftp_data	2022-12-04 12:51:29	Instructions for individuals to execute.
STOR exterior_gb.JPG	ftp_data	2022-12-04 12:53:21	An image of the exterior s building
STOR gb_blueprint.jpg	ftp_data	2022-12-04 12:55:04	A blueprint of the interior a bank/ financial institution
STOR escape_route.JPG	ftp_data	2022-12-04 12:55:44	An image of a street.
STOR equipment_list.ods	ftp_data	2022-12-04 12:57:03	An excel spreadsheet of a list of items.

5. Question 2 - What intelligence can you gather on the type of crime being planned?

5.1. In this section, you will first highlight the type of crime you believe is being planned (e.g. 5.1. Examination of exhibit ev001_exABC showed evidence that a XXXX was being planned.), you should then use additional subpoints to highlight any areas of intelligence you have been able to gather. 5.2 and 5.3 provide examples of this.

Examination of exhibit ev001_exABC showed evidence that a bank heist was being planned.From the files recovered was STOR equipment_list.ods a spreadsheet that contained a list items that were going to be used in the crime including masks for disguise. STOR Plan.odt had the instructions was for individuals to take up their positions. After the last individual takes up his position the instruction clearly states the heist can begin. In the transmitted documents were three images one of the exterior of the targeted premises. A second of the blueprint of the premises
And a third of the escape route

5.2. The following files were found, which suggest that a Bank Heist was being planned.

Filename	Description
Provide the name and extension here.	Provide a brief description of the file and the evidence it contains.
STOR PLAN.odt	Instruction of the position each team member was to be positioned before the heist begins. Title heading “Target Gotham National Bank” and the names of the team to execute the plan.
STOR exterior_gb.JPG	An image of the exterior building where the crime was going to take place
STOR gb_blueprint.jpg	A blueprint of the layout of the bank showing the offices and different sections of the bank
STOR escape_route.jpg	An image of the street presumably to be used by the team to make their escape.
STOR equipment_list.ods	A spreadsheet containing a list of items the team intend to use to compete the plan includes masks for disguise.

5.3. Add any additional intelligence that you can gather in here. You may find it effective to display your findings in a table.

Filename	Protocol	Descriprion
Username	ftp	Username student used to log on to the system
password	ftp	Sunderland password of student used to gain access to the system

6. Summary

6.1. ev001_exABC is a network capture file, which was captured using Wireshark (v3.6.6) on 04/12/2022, with an MD5 of 95548375fc8b1685002fe3943b7b01e3.

6.2. Provide a summary of your findings in relation to the evidence and intelligence you have gathered.

At 12:51:12 pm on the 12/04/2022, username student and password were used to login to a computer IP address 192.168.100.130 using the ftp protocol files were transferred to a second computer IP address 192.168.100.20. With the command ftp student@192.168.100.20 13 seconds after log in the first file STOR PLAN.odt was transferred. At 12:53:21 second file STOR exterior_gb.JPG was transferred. Third file STOR gb_blueprint.jpg begun transferring at 12:55:04. The fourth file STOR

escape_route.JPG begun transferring at 12:55:44. The last file STOR equipment_list.ods was transferred at 12:57:03. All these files were transmitted from address 192.168.100.130 to IP address 192.168.100.20 both were Linux devices

Appendix A – notes_ev001_exABC

This section will contain your contemporaneous notes to support Principle 3. It should therefore describe every Action that you have taken throughout your investigation and include all required information for the action to be reproduced.

Action #	Action	Software / Hardware Used	Date / Time	Notes
0001	Downloaded ev001_exABC.pcap to my device for investigation.		06/05/2023	Downloaded files in my downloads
0002	Made copy of evidence		06/05/2023	Saved evidence to my desktop
0003	Run MD5checksum.	WinMD5Free	06/05/2023	Checksum matched indicating ev001_exABC.pcap had not been altered.
0004	Opened ev001_exABC.pcap	Network Miner	06/05/2023	2 files
0005	Run MD5checksum.	WinMD5Free	06/05/2023	Checksum indicates making a copy and saving to my desktop did not alter the evidence.
0006	Opened ev001_exABC.pcap	Wireshark	06/05/2023	45,494 packets in captured pcap
0007	Filtered to display largest conversations by size in bytes	Wireshark	06/05/2023	In Wireshark under Statistics tab -> conversations. Under IPv4. Click on the byte's column twice. Lots of conversations originating from IP address 192.168.100.20 and 192.168.100.130.
0008	Filtered to display syn, syn/ack and ack flags == 1	Wireshark	06/05/2023	To show the complete connections that were made in the capture. 323 packets returned with this filter
0009	Filtered to display http protocol	Wireshark	06/05/2023	245 packets returned
0010	Filtered to display tcp protocol	Wireshark	06/05/2023	28574 packets returned
0011	Run MD5Checksum	WinMD5Free	06/05/2023	Checksum matched indicating ev001_exABC.pcap had not been altered
0012	Filtered ftp protocol	Wireshark	06/05/2023	44 packets returned
0013	Filtered ftp-data	Wireshark	06/05/2023	86 packets returned
0014	Selected packet number 18473	Wireshark	06/05/2023	Followed tcp stream saved the ASCII file to Raw file named STOR plan.odt to desktop retrieved the document.
0015	Selected packet 26645	Wireshark	06/05/2023	Followed tcp stream saved the file as a RAW file on desktop and retrieved STOR exterior_gb.JPG

0016	Selected packet 33358	Wireshark	06/05/2023	Followed tcp stream saved the file as a RAW file on desktop and retrieved STOR gb_blueprint.jpg
0017	Selected packet 33369	Wireshark	06/05/2023	Followed tcp stream saved the file as a RAW file on desktop and retrieved STOR escape_route.jpg
0018	Selected packet 34032	Wireshark	06/05/2023	Followed tcp stream saved the file as a RAW file on desktop and retrieved STOR equipment_list.ods
0019	smb	Wireshark	06/05/2023	No packets
0020	nfs	Wireshark	06/05/2023	No packets
0021	quic	Wireshack	06/05/2023	12577 packets displayed. No data could be retrieved because of the encryption.
0022	tls	Wireshark	06/05/2023	6827 packets displayed. No data could be retrieved because of the encryption.
0023	Checksum MD5	WinMD5Free	06/05/2023	Checksum matched indicating ev001_exABC.pcap had not been altered

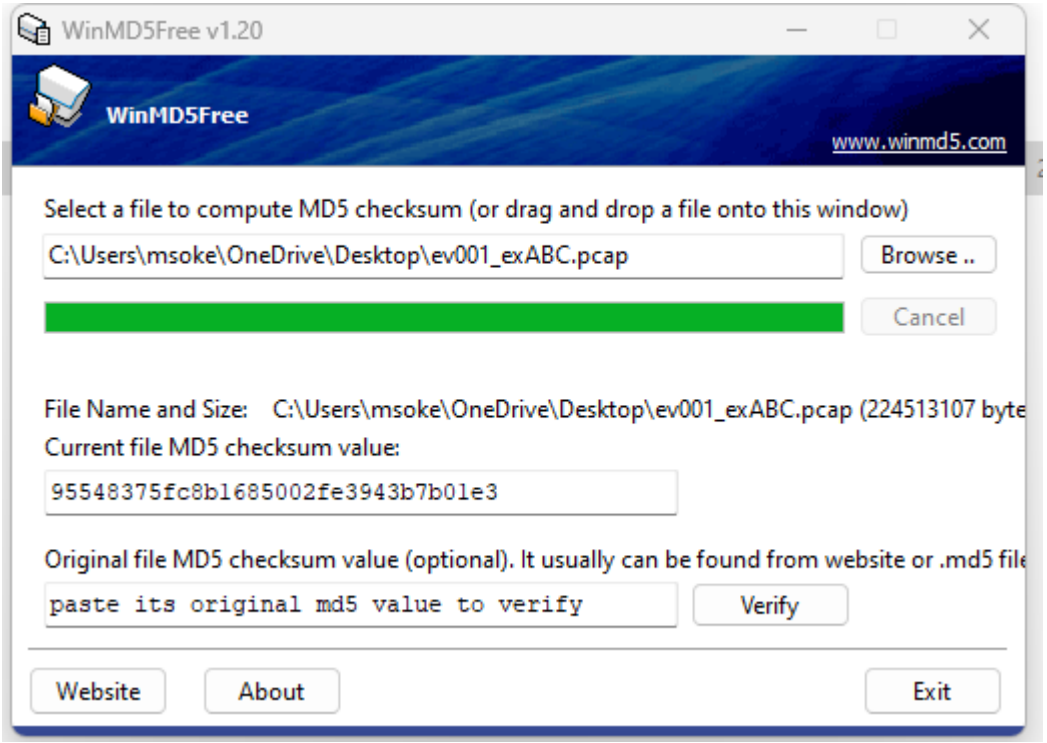
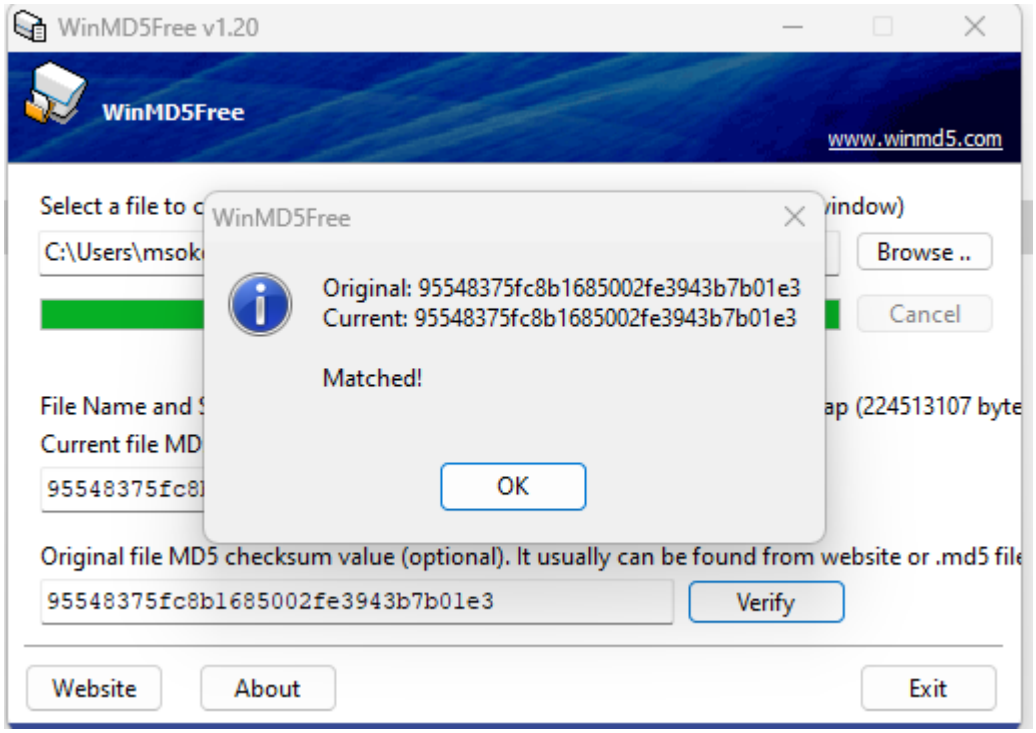


Figure 1 WinMD5Free



References

WinMD5 Free - Windows MD5 Utility Freeware for Windows 7/8/10/11 (no date). Available at: https://www.winmd5.com/ (Accessed: 6 May 2023).