William Adoukonou

UCB

Cyber forsensics assignment 2

Expert Witness Report

Title of the action:

**Court reference number:** FROM YOUR CASE SETTING

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Final report of** William Adoukonou **for the** Supreme Court

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Dated** |  |
| **Specialist field:** | Cyber Forensic |
| **On behalf of the Claimant/** |  |
| **Defendant (or both if single** | Claimant / West Midlands Police |
| **joint expert):** |  |
| **On the instructions of:** | Senior Officer |
| **Subject matter:** |  |

**Name – William Adoukonou**

**Work place – National Department For Cyber Security**

**Number - 07712345678**

**Email – william.1@mail.com**

**Table of Content**

[1 Introduction 8](#_Toc150756333)

[1.1 The writer 8](#_Toc150756334)

[1.2 Summary background of the case 8](#_Toc150756335)

[1.3 Summary of my conclusions 8](#_Toc150756336)

[1.4 Those involved 8](#_Toc150756337)

[1.5 Technical terms and explanations 9](#_Toc150756338)

[2 The issues to be addressed and a statement of instructions 9](#_Toc150756339)

[2.1 Nature of Instructions 9](#_Toc150756340)

[2.2 Source of Instructions 9](#_Toc150756341)

[2.3 Materials Considered 9](#_Toc150756342)

[2.4 The purpose of the report. 9](#_Toc150756343)

[3 My investigation of the facts 10](#_Toc150756344)

[3.1 Forensic Hygiene 10](#_Toc150756345)

[3.1.1 Tools 10](#_Toc150756346)

[3.1.2 The investigations’ machine 11](#_Toc150756347)

[3.1.3 The suspect’s machine 11](#_Toc150756348)

[3.2 Chain of Custody 12](#_Toc150756349)

[3.3 My investigation of the facts 12](#_Toc150756350)

[3.3.1 Assumed facts 12](#_Toc150756351)

[3.3.2Enquiries/investigation into facts by the expert 13](#_Toc150756352)

[3.3.3 Documents 17](#_Toc150756353)

[3.4 Research 17](#_Toc150756354)

[4 My opinion 18](#_Toc150756355)

[4.1 Opinions’ summary with reason 18](#_Toc150756356)

[4.1 Further Investigation 19](#_Toc150756357)

[5 Relevant issues 19](#_Toc150756358)

[Statement of compliance 20](#_Toc150756359)

[Declaration of Truth 20](#_Toc150756360)

[Statement of conflicts 20](#_Toc150756361)

## 1Introduction

# **1.1** **The writer**

Years of unwavering dedication have solidified me as a leading cyber forensics expert. My expertise is multifaceted. Throughout your academic journey, you honed your skills in digital evidence recovery, analysis, and presentation, holding industry-recognized certifications like the: Certified Forensic Examiner award.

1.2 Summary background of the case

A man named Mr. Evil has been suspected of using cyber spyware to commit fraudulent activities. This was achieved by using an antenna at local bank branches and supermarkets to pick up frequencies which carry information over the air.

# 1.3 Summary of my conclusions

# 1.4 Those involved

Mr. Evil: (suspect), [ACOMPLICES TOOK PLEA DEAL TO TESTIFY AGAINST MR.EVIL AND GIVE UP ALL INFORMATION. PAUL DJANKO, DENISE (Dinny) DJANKO, BRAHAM LUDWIG]

# 1.5 Technical terms and explanations

I have indicated any technical terms in **bold type**. I have defined these terms when first used and included them in a glossary in the appendix. I have also included in the appendix extracts of published works I refer to in my report, and throughout the writing, diagrams and photographs to assist in the understanding of the case.

# 2 The issues to be addressed and a statement of instructions

# 2.1 Nature of Instructions

At 11AM on 1st January 2024, West Midshires Police executed a warrant residence, resulting in his arrest due to intelligence connecting him to a fraud case. Following the arrest, two items—a laptop and a directional antenna were seized. These items have been imaged and are now available for examination as provided by West Midshires Police.

# 2.2 Source of Instructions

The senior officer has issued these instructions within the framework of an active investigation into the fraud and spyware case. I am tasked with performing a digital forensic analysis on the laptop and antenna to respond to address specific queries raised by the senior officer.

2.3 Materials Considered

The materials submitted for examination:





# 2.4 The purpose of the report.

This report seeks to offer an in-depth examination of the laptop. Its purpose is to respond to address specific queries raised by the senior officer and offer significant insights into the ongoing investigation concerning Mr. Evil, the issues I will address are:

1. Establishing Link to the Victim
2. Assessment of Proximity to the Fruad
3. Corroboration of Statements
4. Identification of Additional Suspects
5. Reporting of Relevant Issues

# 3 My investigation of the facts

The expert conducted all examinations, measurements, and experiments pertaining to the digital image of the accused's laptop and dash camera. Those findings, upon which the expert relies and have been summarized.

# 3.1 Forensic Hygiene

## 3.1.1 Tools

The forensic tools employed in the process of the investigations are: FTK Imager, Autopsy 4.19.3, VirusTotal, Registry viewer

* **Artifact Extraction and Analysis-** Autopsy 4.19.3

Autopsy is a digital forensics software program. It's a GUI for a collection of tools called The Sleuth Kit. As the name suggests, these tools allow us to take a deeper dive into a computer system to find evidence that may be relevant in a criminal case. Some of its main features include creating and examining disk images, viewing computer content such as messages and emails and the ability to add custom modules for additional functionalities such as verification checks.

## 3.1.2 The investigations’ machine

Installed Virtual Machine on HP PROBOOK Laptop with Intel(R) Core (TM) i7-8550U CPU @ 1.80GHz 1.99 GHz processor used to perform the investigation.

**The suspect’s machine**

16 gb of RAM

Intel i5 3320M (Ivy Bridge)

NVidia NVS 5400M (1GB VRAM)

(Judging by the higher quality specs for a Windows XP machine, this is most likely a custom-built Laptop.)

Investigation’s Machine malware check:

1. The machine was disconnected from the network during the investigation.
2. MacAfee total protection software is used to check that the workstation is malware free.

See Appendix 3

* Based on the expert knowledge, the software mentioned used 4 KEY ISSUES which would invalidate its findings. (SEE RELEVANT ISSUES)

## 3.1.3 The suspect’s machine

After investigating the **DFI** and **registry** files, facts about the suspect’s machine revealed which shows his digital behavior before the assault day.

See Appendix 3 to validate the summary data of the DFI and the following table of registry information.

|  |  |
| --- | --- |
| Operating System (OS) | Microsoft Windows XP Ver. 1.511.1 |
| Operating System installation date | Thu, 19 Aug 2004 |
| User who installed OS | Greg Schardt |
| Name of Computer | N-1A9ODN6ZXK4LQ |
| Accounts on the system | Default user name listed as: Mr. Evil |
| Last Login | 08.19.2024 @ 17:17:29PM |
| Recently Run Programs | Telnet, Google, Command Prompt, CNN |
| Time zone | CST (Central Standard Time) |
| Autorun Programs | Messenger |
| USB devices | Sony Memory Stick, Camera were found last connected to |
| Last shutdown | July 21st 2008 |
| Internet Service Provider (ISP) | Could Not Find |
| Last executed program | WinPcap (ran at 15:11:19 PM on 27/08/2004) |
| **Lease Obtained Time** | App 1: Friday, 27 August 2004 15:30:17  App 2: Friday, 27 August 2004 15:46:18 |
| **Lease Terminated Time** | App 1: Friday, 27 August 2004 16:30:17  App 2: Friday, 27 August 2004 16:46:18 |
| **\*extra\* Deleted Values** | Various entries tied to the users Internet Protocol were deleted, these would tie the suspect to certain locations at given times |
| **IP and MAC Address** |  |
| **Network Cards installed** |  |
| **Applications used to hack**  **Full list in apendix** |  |

From the table we can prove that the ownership of the device belongs to Paul Djanko who is the registered owner, and we from the investigation we did the **malware** check as following:

Subsect’s Machine **malware** check:

if there is any virus you can say

* Based on investigation and expert knowledge, the virus is a trojan horse. Its A program that disguises itself as a genuine program. Once executed, it infects the entire system from the inside. The whole system is based on disguise. It could even pretend to be something like an antivirus.

# 3.2 My investigation

## 3.2.1 Assumed facts

According to the report's objectives, I focused on obtaining evidence to support our investigations. This is to ensure that anything brought up by my findings is relevant to the case. This is important as spending time deciding whether evidence is crucial to the case can take up lots of time and impact the case in a negative way

|  |  |  |
| --- | --- | --- |
| Evidence Class | Description | Type |
| 1 | Multiple Emails found on the suspects computer in connection with Hacking and The Scanner that was initially seized by authorities | Emails Pdf Images |
| 2 | Images yielded results for .EXE icons for applications using in covering networking traces. While not specifically incriminating, does pertain to the case as suspect conversated about network hacking | Videos Map |

Those findings lead me to the assumed facts:

1. The suspect is computer savvy and most likely works in the IT industry
2. The suspect is interested in their digital footprint and cyber security online
3. Suspect is travelling outside of the country frequently based on Images

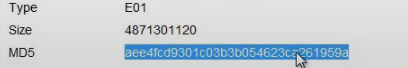
## 3.2.2 Enquiries/investigation into facts by the expert

Evidence Class 1 -

The evidence artifacts were acquired through the examination of active directory, **operating system** artifacts, and file system artifacts

The **hash value** for each file has been calculated to confirm that the expert has maintained the original data integrity. Its important to ensure that when any piece of evidence is following a chain of custody, it hasn't been tampered with**.**

**EXHIBIT A**

****

After The scrutiny of 853 email on the suspect’s artifact, we got exhibit A which presents a tangible connection is established between the suspect Greg and the Alias Mr. Evil. In one correspondence via email, the suspect stated he was “Known for the Netware hack” as seen in the image.

A screenshot of a computer error

Description automatically generated

Following a thorough examination of the entire correspondence, it becomes evident that Mr. Evil is a network/computer hacker that has ties to the crimes explained by the West Midlands Police. In the same email, Mr. Evil is seen explaining how to use Pandora, which is a tool used for account hacking, this is shown in the image below.

A screenshot of a computer

Description automatically generated

Evidence Class 2 -

To obtain this exhibit, I examined 21 videos visually this is where the suspect had multiple EXE icons for programs which are used maliciously this is show in the exhibit below. There are also images of popups from the application Netware. This directly links the application and the suspect together since they had mentioned the hack in the first place.

A box with a logo

Description automatically generatedA screenshot of a computer error

Description automatically generated

## 3.2.3 Documents

# 3.3 Research

Many documents were reviewed and consulted in the preparation of the report, incorporating best practices for presenting artifacts, admissible facts, evidence, and tools. The report was crafted to adhere to court standards and is presented in a professional manner.

**4 My opinion**

# **4.1 Opinions’ summary with reason**

Based on deep investigations and the previously mentioned facts, there is **clear** evidence prove that Greg committed the crime because:

1- They had already exposed their past about hacking

As shown by the emails to multiple people describing their attacks in detail

2- there is clear evidence of the suspect explaining how to perform other cyber-attacks as well as the ones they are on trial for

As seen by the numerous programs installed on the suspect’s machine such as Look@LAN, mIRC and Cain

3- Registry of the system shows a clear link between the suspect, the Alias Mr. Evil and the seized computer system

Administrator and Mr. Evil were the first few accounts made on the system. Mr. Evil was also the last logged in

# 4.2 Further Investigation

I have created a diagram to show the links between the evidence found.

A screenshot of a computer

Description automatically generated

5 Relevant issues

Several pertinent details tied to the primary case need to be presented in court. In the examination of the laptop:

NOTICE OF VULNERABILITIES

The laptop seized by Authorities may belong to Mr. Evil, however tests could not prove that the login was not tampered with by any other login users. To be more specific, the operating system installed was windows XP. Support for this OS has ended since 2014. This means it’s also missing crucial security updates, making it vulnerable to these Major Exploits.

DATE/TIME EXPLOIT ON WINDOWS XP

The Date Time exploit would allow users to configure custom install dates as well as boot/

DFI/bios times. This would severely impact the case if the suspect was found using any of these programs. The evidence proving the load times of the Operating System would NOT be conclusive.

NOTICE OF USER ACCOUNT EXPLOIT

This exploit involves multiple users being able to mask and change which User Account made a change on the OS. If there were any traces of these exploits on the system, the court would not be able to CONLUSIVELY say that Mr. Evil was the one who had downloaded key programs on the system such as Pandora. They would also not be able to definitively say that he was the one that sent the emails on the account.

NOTICE OF VULNERABILITY IN EMAIL CLIENT

Recently there has been a major update in all email clients due to a bug called EvilWare. This bug has been allowing 3rd parties to alter and intercept email boxes. This means that the emails found in Mr. Evil's registry may have areas for doubt when looking at ownership. The user’s emailing client was found in the registry and listed as Outlook Express, Forte Agent, MSN Explorer and Hotmail Email.

## Statement of compliance

I understand my duty as an expert witness to the court to provide independent assistance by way of objective unbiased opinion in relation to matters within my expertise. I have complied with that duty and will continue to comply with it. I will inform all parties and, where appropriate, the court if my opinion changes on material issues. I further understand that my duty to the court overrides any obligation to the party from whom I received instructions. Parts 33.2 (1), (2) and (3) and 33.4(j) Criminal Procedure Rules

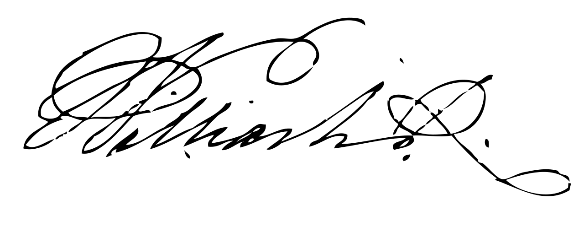
## Declaration of Truth

This statement 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 willfully stated in it anything which I know to be false or do not believe to be true.

## Statement of conflicts

I confirm that I have no conflict of interest of any kind, other than any which I have already set out in this report. I do not consider that any interest which I have disclosed affects my suitability to give expert evidence on any issue on which I have given evidence, and I will advise the party by whom I am instructed if, between the date of this report and the trial, there is any change in circumstances which affects this statement.

## Signature your name Date



23. 05. 2023

All reports must be signed and dated, and the Statement/Declaration of Truth must be verified by a signature/date. Therefore, you are advised to include your Statement/Declaration of Truth as your final item in the report, and to follow it with your signature and the date.

Appendix 1

|  |
| --- |
| A screenshot of a computer  Description automatically generated |
| A screenshot of a computer  Description automatically generated |
|  |
|  |
| A screenshot of a computer  Description automatically generated |
|  |
| A screenshot of a computer  Description automatically generated |
| A close up of a calendar  Description automatically generated  A close up of a calendar  Description automatically generated |
| A screenshot of a computer  Description automatically generated |

Appendix 2

A black computer on a yellow table

Description automatically generated

A satellite dish on a table

Description automatically generated

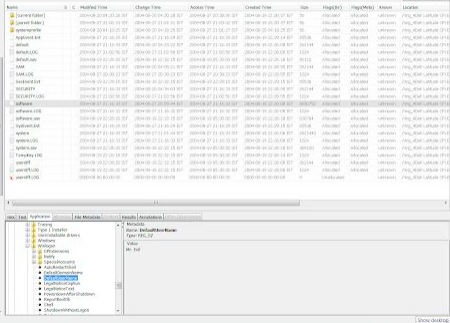
Appendix 3

A screenshot of a computer

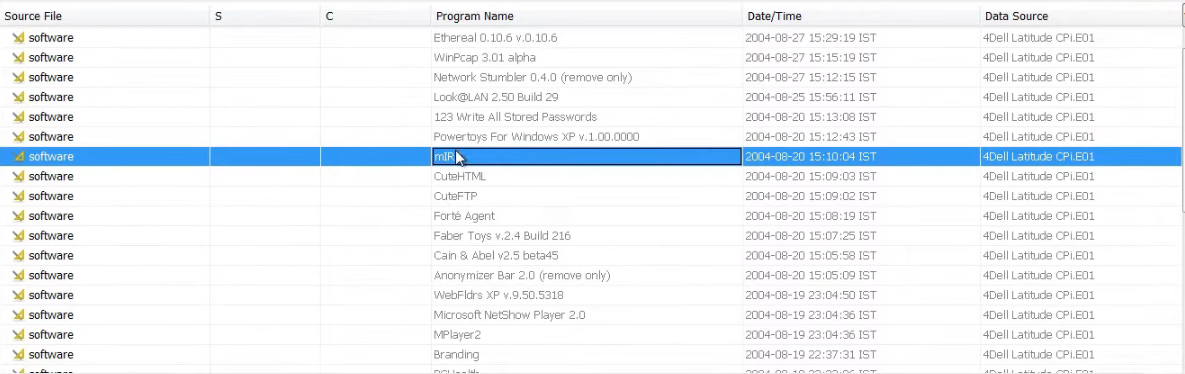
Description automatically generated

Appendix 4

All installed programs



Apendix 5



Forensic Hygiene

A screenshot of a computer

Description automatically generated

Figure 10 Investigator's device - malware check

A screenshot of a computer

Description automatically generated

Figure 11 VirusTotal result

A pie chart with different colored circles

Description automatically generated

Figure 12 Data Summary of Paul's Laptop

A graph showing the number of years

Description automatically generated with medium confidence

Figure 13 Timeline of suspect's laptop

Registry Information

A screenshot of a computer

Description automatically generated

Appendix 4

Appendix 5

|  |  |
| --- | --- |
| **Glossary** | **Meaning** |
| **Digital Forensic Image (DFI)** | snapshot of everything on a computer or device so that investigators can examine it for evidence. |
| **operating system** | Windows XP |
| **MD5 and SHA1 hash** | MD5 AEE4FCD9301C03B3B054623CA261959A  SHA1 ff2bedb4ab9ee139cd4403b2e3424df368673fe2 |
| **Registry** | All files listen in report |
| **Lease Obtained Time** | Friday 27th August 2004 @ 15:30 PM |
| **Lease Terminated Time** | Friday 27th August 2004 @ 16:46 PM |
| **Glossary** | DFI – Digital Forensic Image: File created from a computers entire list of files to be used to investigate |
| **Malware** | Zip Bomb was located on the computer. Was safely quarantined so was not important/impact the case |

Appendix 6

Names of people, emails mentioned in the DFI for further investigations:

Emails

|  |
| --- |
| dinnydjanko@gmail.com |
| Reubenbeethomahler@gmail.com |
| stuarttchaikomsiva@gmail.com |
| Mailer-daemon@googleemail.com |
| pauldjanko@gmail.com |
| Birminghamdrops@gmail.com |
| brahmludwig@gmail.com |

Names

|  |  |
| --- | --- |
| Pedro | Meet Stuart in university of Warwick |
| Brahm Ludwig |  |
| Stuart Tchaikomsiva | Victim |
| Lee | Dinny and Paul’s wanting to visit |
| Bill | Take cash from Stuart in university of Warwick |
| Kevin | Gave Paul number of Birmingham drop |
| Denise Djanko (Dinny) | Djanko’s wife or girl friend |
| Reuben | * Met Dinny in BM meet * She asked him to teach her how to hide files |
| Lez | Play with money in Birmingham |
| Paul Djanko | Suspect |