THE REPUBLIC OF UGANDA

IN THE HIGH COURT OF UGANDA HOLDEN AT KAMPALA

ANTI CORRUPTION DIVISION

HCT-00-AC-SC-0084-2012

UGANDA ::: PROSECUTOR

VERSUS

A1. GUSTER NSUBUGA	
A2. FAROUK MUGERE NGOBI	**ACCUSED**
A3. OWORA PATRICK	
A4. BYAMUKAMA ROBINHOOD	

BEFORE JUSTICE PAUL K.MUGAMBA

JUDGMENT

Guster Nsubuga (A.1), Mugere Farouk Ngobi (A.2), Owora Patrick (A.3) and Byamukama Robinhood (A.4) are jointly indicted. Four of the charges are derived from the Computer Misuse Act while the other two are drawn from the East African Community Customs Management Act. The charge in count I is unauthorized use and interception of computer services, contrary to sections 15(1) and 20 of the Computer Misuse Act said to have resulted in a loss of shs 2,461,447,275 and 78 cents. In count II the charge is Electronic Fraud, contrary to section 19 of the Computer Misuse Act which is said to have resulted in the loss of shs.2, 461,447,275 and 78 cents. The charge in count III is unauthorized access to data, contrary to sections 12(2) and 20 of the Computer Misuse Act. In count IV the offence is producing, selling or procuring, designing and being in possession of devices, computers, computer programmes designed to overcome security measures for protection of data, contrary to sections 12(3) and 20 of the Computer Misuse Act. The charge in count V is unauthorized access to a customs computerized system, contrary to section 191(1) (a) of the East African Community Customs Management Act 2009 resulting in the loss of tax revenue of shs 2,461,447,275 and 78 cents. The offence charged in count VI is fraudulent evasion of payment of duty, contrary to section 203(e) of the East African Community Customs Management Act 2009.

Twenty six witnesses were called by the prosecution to prove the charges. These witnesses appeared as follows:

PW1: Peter Collins Wasenda (IT Specialist URA)

PW2: Mwebesa Bruno (Customs Officer, Nakawa Enforcement Division)

PW3: Ahimbisibwe Bernard (Bond Keeper, Pacific Parts (U) Ltd)

PW4: Sajjabi Ibrahim (Director, Framas Auto Parts)

PW5: Christine Adeke (Customs Bond Officer)

PW6: Det/Cpl Ruzindana Deo (attached to URA CID)

PW7: Kajumba Winfred (attached to Transit Monitoring Unit Enforcement Division)

PW8: Majwega Ronald Kironde (General Manager, MK Publishers Ltd)

PW9: Manzoor Ahmad (Director, Geo –Investment (U) Ltd)

PW10: Kayemba Isaac (Manager, Forensic Investigations URA)

PW11: Kasule Ronald (Supervisor Human Resource URA)

PW12: Gerald Kavuma Nkwanga (Engineer Comtel Integrators Africa)

PW13: D/IP Elyanu Joseph (Uganda Tax Investigations Department)

PW14: Margaret Mukasa (employed in Customs Warehouse)

PW15: Charity Manase (Country Manager FEDEX, Uganda)

PW16: D/Sgt Itabu Lasio Robert (CID Jinja Road Police Station)

PW17: Rose Mary Kisembo (Manager, Software Engineering, URA)

PW18: Alex Nuwagira (Supervisor, Tax Investigations Department, URA)

PW19: Nabwire Rose Mary Mugenyi (Revenue Officer Grade II, Nakawa)

PW20: Murwon Emmanuel Jacob (Customs Officer URA)

PW21: Teddy Nanfuka (Branch Operations Manager URA Barclays Bank Nakawa)

PW22: Patrick Mpairwe (Supervisor Licensing Motor vehicles, URA)

PW23: Martin Henry Ssaka (Assistant Commissioner, Domestic Department, URA)

PW24: Nampanga Mary Concepta (Customer service, Stanbic Bank, Busia)

PW25: Irumba Bob (Customer Consultant, Stanbic Bank City Branch, Kampala)

PW26: Sarah Nakyagaba (Police Officer attached to URA).

At the close of the case for the prosecution the option of each of the accused persons was that they would make no statement in their defence. None of them had witnesses to call.

The prosecution case is that at some time Uganda Revenue Authority got the sense that their computer system was being compromised. Internal investigations were started. In June 2012 following a tip that there was a suspect vehicle in the proximity of URA at Nakawa, four men were arrested inside the vehicle. The men inside the vehicle, which was a car, were A1, A2, A3 and another who was not indicted. Inside the car the men had with them three laptops, an inverter, an external hard disk and other electronic paraphernalia which were all seized. The men were arrested as suspects in order to carry out further investigations. The seized items were stored with a view to serving as exhibits. Also impounded for further inquiries was the car in which the suspects were found. Within one week of the arrest of the suspects, A.4 was picked up at his place of work at MTN. The computer belonging to his employers, MTN, which he was allocated to use was seized also and taken to be used in ongoing investigations. The fourth man arrested together with A1, A2 and A3 was later released while A.4 was detained on suspicion of having collaborated with others of the accused in committing the crimes alleged. This prosecution thus ensued.

Before I proceed to consider the evidence I am obliged to relate to a few matters that emerged in the course of hearing which call for determination.

It was argued on behalf of the defence that the indictment was defective given that it was not consented to by the Director of Public Prosecutions. I have looked at the indictment itself. It was signed by Mary Kamuli Kuteesa for the Director of Public Prosecutions. Article 120 of the Constitution relates to the office of the Director of Public Prosecution. Article 120 clause (3) paragraph (b) gives one of the functions of the Director of Public Prosecutions as institution of criminal proceedings against any person or authority in any court with competent jurisdiction other than a court martial. Then there is clause (4) paragraph (a) of the Article which notably states that the functions conferred on the Director of Public Prosecution under clause (3) of the article cited:

> ` (a) May in the case of the functions under clause……….
>
> 3(b)…………of this article, be exercised by him or her in person or by officers authorized by him or her in accordance with general or specified instructions………'

In the premises the signature of the person authorized to sign for the Director of Public Prosecution suffices and there should be nothing amiss. Needless to say where there is a requirement for the Director of Public Prosecutions to give his consent to a charge the law states so expressly. None of the charges in this indictment fall under that category. It is therefore not profitable to argue as the defence does that this indictment is not instituted by Director of Public Prosecutions. That should take care of that concern.

The other concern is that after court had allowed the prosecution to make an amendment to the indictment the accused persons were not allowed to plead again to the amended charges. This concern came at the time the defence made its submission and was not expressed in real time. Initially the four accused persons had pleaded to an indictment which gave the span in time as 'during the years 2010-2012'. They all pleaded not guilty to the charges and pleas of not guilty were accordingly entered against all of them. The amendment sought was to have the period set as `during the period from April 15th 2011-June 2012' clearly a shorter span. The other amendment concerned the amount of money said to have been involved in the charges. Initially it had been computed at shs 2,164,833,894/= but the amended indictment would have it be shs 2,461,447,275 and 78 cents. The accused persons were represented by counsel who when asked whether they had an objection to the amendment said they had none. Hearing thus proceeded with the amended indictment. For the record, the pleas of not guilty were undisturbed. Accused persons were not prejudiced thereby given that the amendment was not fundamental, that the defence was not opposed to the amendment, that evidence had not been called and that their pleas of guilty were never affected by way of alteration.

It was argued on behalf of the defence that section 28 of the Computer Misuse Act was not complied with and that as such evidence could not be generated from items seized without the requisite search warrant. Indeed Section 28 of the Computer Misuse Act states in subsection (3) thereof:

> ` (3) A computer system referred to in subsection (2) may be seized or samples or copies of applications or data may be taken, only by virtue of a search warrant.'

Simply put, without a search warrant no one can seize the articles specified therein. The provision doubtless is grounded in Article 27 of the Constitution which provides:

> `(1) No person shall be subjected to-
>
> (a) unlawful search of the person, home or other property of that person; or
>
> (b) unlawful entry by others of the premises of that person.
>
> (2) No person shall be subjected to interference with the privacy of that person's home, correspondence, connection or other property.'

The article doubtless makes the privacy of the individual, the individual's home and property virtually sacrosanct. But then article 43 of the Constitution provides inter alia that in the enjoyment of the rights and freedoms bestowed by article 27 for example no person shall prejudice the fundamental or other human rights and freedoms of others. Suffice it to say a balance must be struck so that whatever is done is acceptable and demonstrably justifiable in a free and democratic society and is in concert with the Constitution. In that respect for example section 6(2) of the Criminal Procedure Act provides that a public officer may search any person who has been arrested and may take possession of anything found on the person which might reasonably be used as evidence in any criminal proceedings. This is done on those occasions where it is not practical to go looking for a search warrant at the risk of the search soon after turning irreversibly nugatory. While the experience of Uganda has been to treat searches without warrant as very occasional, the position in the United States of America where the Fourth Amendment to their Constitution is treasured and iconic is instructive. The Supreme court has held on various occasions that searches conducted outside the judicial process without prior approval by a judicial officer, are perse unreasonable under the Fourth Amendment except for a few specially established and well delineated exceptions. See ***G.M Leasing Corp V United States, 429 U.S 338,352-53,355***. Indeed in ***Mc Donald V United States, 335 U.S 451,456(1948)*** it was stated that exceptions to the requirement for search warrants are jealously and carefully drawn and that those who seek exception to the requirement ought to show that the exigencies of the situation made the course imperative. In ***State V Allison, 298 N.C 135, 257 S.E 2d 417(1979)*** a warrantless search was held not to be unconstitutional when probable cause to search exists and the government satisfies its burden of demonstrating that the circumstances of the situation made a warrantless search imperative. Yet another American case on the matter is ***State V Goode, 350 N.C 247,512 S.E .2d414(1999)*** where court affirmed that in the course of search incident to arrest, police may take from an arrested person any property which the arrested person may have about him, and which is connected with the crime charged or which may be required as evidence. Implemented to the letter S.28 (3) of the Computer Misuse Act would have both human experience and the law held in a strait jacket. It would be a nightmare for minders of law and order but next to nirvana for the prospective offenders. There must be a way to circumvent the unwanted results of S.28(3) of the Computer Misuse Act, and that is that exceptions must be made where evidence shows the exigencies of the situation could not await a search warrant as is already the position under the Criminal Procedure Code Act and as the persuasive American experiences cited justify. Certainly to construe section 28(3) of the Computer Misuse Act strictly is a venture into absurdity which this court will eschew for good public order. Given the evidence of PW2, PW6 and PW26 the prevailing circumstances were such that instant response had to be given to a situation that had presented itself. They did not act unreasonably in the circumstances and as such I hold the search and subsequent seizure done on the occasion of the arrest of A1, A2 and A3 to be lawful.

The evidence of PW10 was that as the manager of Forensic Investigations, URA he was handed various items for forensic imaging and analysis. He received the items, which were sealed in exhibit bags, from PW6.Those items he said were:

1. A Lenovo laptop computer serial number CBU0058195 and its disk serial number WXE 109VSA411.

2. A Samsung external hard disk serial no.SITSTD08702704

3. Samsung laptop serial number EZT 293LB400017K and its disk serial number WD-WX61A3162935.

4. A Dell laptop serial number F553CA00 (MTN 64815) and its hard disk drive serial number WD-WXHOA79U7063.

It was the evidence of PW10 that upon receipt of a computer he removed the attached disk and identified it for necessary imaging. He said he did this with regard to all the three computers mentioned above. It was his evidence that while in most cases imaging was done in the forensic laboratory in Kampala, in the case of the disk for the Samsung laptop the disk was taken by him to South Africa for faster image acquisition which was not available locally. The witness testified that he proceeded to work on the contents acquired from the storage devices. Exhibits P3, P24, P25 and P26 were proffered in evidence as such. PW10 testified that upon analysis he found evidence that the Dell laptop had been used to gain access to URA computers and servers. He found that the gmail address rbyamukama@gmail.com which chatted with another gmail address guxznguster@gmail.com belongs to A.4. Several URA software programmes were evident under the computer name Byamukr. Those programmes according to PW10 included MOVIS which is software programme for URA motor vehicle registration. In addition he learnt from PW1 of the existence of URA passwords, script for accessing URA system externally, the URA Raddex server password and the URA Web interface text. It was established also that the Dell laptop used an ID CRE-WS-200 which PW1 identified as one which gained unauthorized access to URA systems and further that it belonged to MTN. There was evidence ASYCUDA had been installed on the computer on 16th February 2011 and had last been accessed on 7th January 2012 before it was deleted. There were several other modules which had been installed and later discovered. In addition PW10 mentioned the installation of spyware on the computer. Tim viewer was downloaded and installed on the computer. It was created on 8th September 2011 and last accessed on 19th June 2012. Significantly it was not deleted. That information PW10 got from the disk found with the Dell laptop and is contained in Exhibit P.24.

PW10 said also that he analysed the image of the external hard disk said to have been recovered from A1. It is worthy of note that this and several other items found with him (A1) he disowned. He said and noted that they belonged not to him but to one Kabanda Mike. Forensic analysis of the disk revealed an e-acknowledgment receipt which confirmed A1's application for a Tax Identification Number (TIN). The names of A1 are evident as is a contact number 0701939225.The record of proceedings contains a chat at page 454. In the gmail chat between rbyamukama@gmail.com and guxznguster@gmail.com that contact number features. Exhibit P.44 tendered by PW23 is relevant on this matter.

The testimony of PW10 also refers to the external hard disk which contained several payment registration receipts in the names of Cargo Supplies Ltd, employers of A1, A2 and A3. The external hard disk image also contained names of URA domain administrators such as E. Kasule, Pwasenda and A. Higenyi. These were contained in a folder named Backtrack files. He said that the disk contained also a long list of URA staff Network User ID's with corresponding password hashes. The file was found on Backtrack files. Of course hashes are passwords stored in encrypted form. That they featured is of significance. Then there were over one million motor vehicles contained in a module of the motor vehicle registration system MOVIS. In it were particulars of chasis and engine. The customs system Asycuda also had modules of it on the same disk. According to PW10 this information was contained in Exhibit P.26 .It was his evidence nothing relating to a Kabanda Mike was seen. PW10 testified that his role in all this was to do the systems audit. It was PW1 who stated that the system had had unauthorized access, he added.

The evidence of PW11 was that on 23rd January 2006 URA had appointed A.4 a software programmer. This evidence is supported by that of PW17 who is manager, software Engineering, URA. PW17 testified that she supervised A4 for 3½ years. It was her evidence that through a Gmail address bmugishaura@gmail.com information from select e-mails in

URA was being gathered and was being compromised by computers outside the URA system. This particularly applied to the URA data base. She cited as example motor vehicles imported for MK Publishers Ltd which were given registration numbers UAQ 697Q, UAQ 747Q, and UAQ 773Q whereas the numbers had previously been assigned to other vehicles. She noted that physical files showed information which was different from that contained in the digital data base. The witness noted that at one time the Samsung laptop was designated nhq-ws-966 yet at another it was nhq-ws-2227. She stated that the computer was used to make unauthorized changes on the motor vehicle data base. In this connection PW4 in his testimony said he received registration cards for motor vehicles UAQ 697Q, UAQ 747Q, and UAQ 773Q from A1. It was the evidence of PW8 that A1 gave these cards to PW8.

Another case cited by PW17 was that of motor vehicle UAH 035P which is the subject of chats between guxznguster@gmail.com and me. This is in Exhibit P.3 Batch 11, extracts 17 and 18.There guxznguster tells his interlocutor to get the details from UAL 849T and use them to update UAH 035P and then get ownership details from UAN 849T,the ID of Nuwagaba Eugene being available. In the event the vehicle in issue changed from a Nissan Caravan to a Subaru Forester in the electronic data base. The changes affected both the chasis and the engine. PW17 testified that a screen image of A.4's laptop in Encase environment shows a folder with an Asycuda++ client installation. The installation is used by registered clearing agents and members of staff of URA restrictively. It is important to note PW17's observation that in September 2012 when the image was obtained A.4 did not qualify to use the system. It was also the evidence of PW17 that given the screen shots of the image of A.4's hard disk it was apparent a key logger software Winspy was available. Equally confirmed, according to PW17, was configuration of that software to send e-mails to an e-mail address bmugishaura@gmail.com from URA's mail server and that the owner visited remote spy web sit who issue that tool. Equally revealing is the evidence of PW17 concerning Batch 4 which she said is shared scripts viewing information in the ASYCUDA data base found in Batch 8 of the image of A.4's laptop. It was her testimony the same was found in the Samsung laptop image.

In his testimony PW12 said he was sent notice of shipment addressed to A.4 at his place of work. The address on the notice was that of PW12. It was his evidence on several occasions he gave his visa card to A.4 to enable him purchase items of his choice but that he saw none of those items. He agreed his account would be debited in the process. There is evidence of a purchase of spyware from Plimus International using his visa card. The transaction was for shs 100,117/=

PW13 in his evidence said he was present when the hard disks were removed from computers. He searched the home of A.4 and recovered various documents. A document in the names of A.4 and titled 'Implementation of e-Banking Framework' for the Faculty of Computing and Information Technology was recovered on the occasion. It bore certain particulars. There is the address rbyamukama@gmail.com and the telephone number +256772575818 .Exhibit P.32 was proffered to this end. There is a conversation which PW17 cited in Batch 3 of Exhibit P.3. That conversation involved one Byamukama and one Stewart. There the former stated that he wanted to test the link to URA and was sending the file then. Thereafter follows the names of A.4 and at page 4 of Batch 3 rbyamukama@gmail.com. Next is a message confirming that Nkwanga Kavuma Gerald (PW12) had made a purchase. At page 5 of Batch 3 at the top of the rectangle the particulars rbyamukama@gmail.com appear but in the middle of the box is Robinhood mobile +256772275818 below which is +256717440347,the last number according to PW17 being one A.4 had been issued while he was employed by URA. Batch 3 page 4 has in the middle of the screen shot e-mail key log to bmugishaura@gmail.com and the server mail: ura.go.ug. There appears on the screen shot the words ` I wanna test a link'.

PW20 was a customs officer with URA. He had super user rights. In early September 2011 there was suspicion someone who did not belong to the unit where PW20 worked or to URA had caused an entry to be registered. Even though PW20 had not created any user rights in the previous 5 months such had been created. Later spyware were discovered in the desk top of PW20. It was the evidence of PW20 some people were eventually arrested in the vicinity of URA premises. He added that following the apprehension he discovered his user name emurwon, his password and modules of ASYCUDA++ software had been compromised. He testified that some of the modules are meant to be for the exclusive use of those entitled. It was his evidence the users created through interference with the URA system were created by the owners of the laptops such as the Samsung found with A.1 and the laptop found with A.4. He stated that each of the computers has a line below indicating a path and the path could show whether the computer involved was that of A.1 or A.4.He was definite payments appearing to have been made to the bank were actually never made.

In her evidence PW21 the Branch operations manager for Barclays Bank at Nakawa, denied knowledge of Barclays-Phiona. She added that the bank code for Barclays Nakawa is not the purported 0218 but 0215. She was emphatic the stamp which appears is not that of the bank. It is noteworthy PW19 in her evidence denied hers to be the signature apparent on the log books in Exhibit P.16:for UAQ 747Q,UAQ 773Q and UAQ 697Q specifically.

The testimony of PW22 shows his work as overseeing motor vehicle applications and processing as well as keeping custody of files relating to registration. He mentioned some cases where information in the electronic data differed from that in the physical files relating to particular vehicles.

PW18 is Supervisor, Tax Investigation Department, URA. It is his computation that through diverse defaults relating to compromise of the URA computer system a loss of shs 2,461,447,275 and 78 cents was incurred. Exhibit P.40 was tendered for effect. The witness said his calculations were based on evidence provided by PW17 and PW10 as well as his checks for unpaid taxes. He related to Exhibit P.4 and said the first 11 vehicles were declared and cleared through the falsified ASYCUDA Account, Barclays-Phiona. Others were those said to be for re-export by MK Publishers Ltd and vehicle number UAQ 018T.He noted that others on a list of 150 vehicles were never declared. He stated that vehicles were cleared for re-export by removing them from customs through tampering with the Asycuda system. Thereafter false registration was done through insertion of some information in the motor vehicle data. As an instance he gave Saul Malagwe’s motor vehicle number UAQ 232T which had a file of its particulars missing and lacked particulars of its entry and declaration to customs. The vehicle should be a Nissan Navarra but what record exists on it shows it is a Subaru Forester.

The evidence of PW18 relates to what transpired the day A1, A2 and A.3 were apprehended. He testified that he was not present at the time the suspects were arrested in the car. He said however that he joined PW2 soon afterwards. He added that that PW2 handed the seized items to PW6 and that the suspects had eventually been taken to the headquarters of the Special Investigations Unit at Kireka. The arrangement was he sat in a Pajero vehicle in the company of PW6 and another policeman who was armed. They had the exhibits in the vehicle where they sat. In addition there was a pickup which was occupied by the four suspects, two enforcement soldiers and two enforcement officers. Later that night the exhibits were deposited in the stores at the Tax Investigations Department, Nakasero. He testified that earlier in the evening PW10 had kept them company in order to ensure necessary procedures were followed (known as first respondent procedure) concerning the computers and other digital devices. As an instance no one was to switch on any of the computers. PW10 assisted in reading serial numbers and sealing evidence bags where exhibits were put.

The above evidence apart, PW18 stated that he was the one who led a team of investigators to get the laptop which A.4 used at MTN. He said he was with A.4, PW13 and PW10. It was his evidence the laptop was identified to them by a Mr. Gitta of MTN. He referred also to three Toyota Noah motor vehicles which had been imported by MK Publishers Ltd and said that the physical files showed the registration numbers had earlier been allotted to Caterpillars. He said the Toyota Noah vehicles and their acquired registration numbers had been fraudulently inserted into the URA data base. He added that the three Toyota Noah vehicles had earlier been declared to URA for export to Burundi through Katuna customs post. It was his evidence that directors at MK Publishers had told him they had given money for payment of taxes to PW4.PW4 had told him that he gave that money to a clearing agent known as Guster Nsubuga. PW18 said Barclays Bank had not received the money shown in the MOVIS system to have been paid for registration of some motor vehicles and that the user account Barclays Phiona together with its password were found on the devices found with the suspects. It was his evidence he found motor vehicles had been taken out of customs control through tampering with the Asycuda system. Having compiled and computed the loss in taxes he came up with a sum of shs 2,461,447,275 and 78 cents. This is comprised in Exhibit P.40.

In this connection the evidence of PW4 is apt. As noted earlier he testified that he handed money he received for tax clearance of the three Toyota Noah vehicles imported by MK Publishers Ltd to A.1. He said after some time A.1 had given him three registration cards and keys for the three vehicles. He was definite there were no instructions to re-export the vehicles to Burundi. Then there is evidence of PW3who testified that Cargo Supplies Ltd were the clearing agents for the three Toyota Noah vehicles but that the vehicles were taken away for re-export to Burundi by Nagoya Company Ltd.

As regards Cargo Supplies Ltd, PW10 testified that the Samsung hard disk contained a letter head signed by A3 in his capacity as Managing Director of the company. The disk had a file named Cargo Biz Card bearing three e-mail addresses named as follows:

Cargosupplies@hotmail.com

guxznguster@hotmail.com

guxznguster@gmail.com

The gmail identity is similar to that in chats with rbyamukama@gmail.com said to have been featuring in the research paper of A.4 as testified by PW13.

According to PW1 the computer systems of URA were compromised. He said super user privileges were used to install spying software. He said Backdoor programmes were installed in the URA systems between September 2011 and June 2012.One remote logging tool he mentioned as having been employed was Dame ware and that this was found to have been used by both A.1 and A.4 in their laptops. In addition the witness A.4 had a TimViewer. The witness said his role was to look at data and identify data which matched with hacking incidents which occurred on URA systems.

According to PW1 authentic URA email addresses like ckyaligonza@ura.go.ug, jbotim@ura.go.com were used to forward communications to address bmugishaura@gmail.com. The witness used screen shot D.1 to illustrate his point. It was his evidence that bmugishaura@gmail.com was an account without a verifiable owner and that he hacked with it using recovery options. He was emphatic spy software had been installed in the Kampala Business Customs Centre in the Finance Division in Malaba and in Busia. Indeed PW17 testified that the email address bmugishaura@gmail.com exists on the image of the laptop recovered from A.4.

PW26 testified that the user name Barclays-Phiona was used to make payments but that it was false. There is evidence in Exhibit P.3 in the chats showing a break of about 2 months in the chats. In the chats there is a reference to Luzira. PW26 stated that she enquired and learnt from the Chief Magistrate's court, Buganda Road, that A.1 was on remand between 25th January 2011 and 1st March 2011.The chats show there was conversation between A.1 and his interlocutor which had been continuous until 11th January 2011. It stopped then but resumed on 4th March 2011. Significantly when the interlocutor asks then guxznguster gives the contact as number 0701939225.

It is seemly to consider testimonies regarding persons who were in the laboratory when PW10 extracted the disks. PW10 said there were A1,A2, A3,one Kibalama, PW26, Milton Sabiiti, PW13 and PW10 himself.PW1 said present were PW10, PW26 and PW18. On the other hand PW13 testified that besides himself there were A1, A2, A3, PW10 and PW26. I note that the extraction was done in the presence of others found necessary.

The charge in Count I is drafted as unauthorized use and interception of computer services, contrary to sections 15(1) and 20 of the Computer Misuse Act. The emphasis is mine. In the statute book the offence reads: Unauthorized use or interception of computer service. Emphasis added. It is argued by the defence that by adding the word and the prosecution is combining two offences, one being of use and the other of interception, in one count making the charge duplex and therefore defective. The law against duplicity thrives on the tenet that an accused person should know the offence he is alleged to have committed so that he can prepare his defence. In the Tanzanian case of ***Nyanga Manyika V R [1980] TLR 141*** which the defence has advanced in support of their contention court held that while charges should not be duplex as much as possible, there is a limitation to the application of the rule and that when a series of acts which constitute a series of the same offence are committed in such circumstances as to amount to one single transaction then, in reality, there is committed one offence which ought to be charged in one count. The particulars in this charge read in part:

'…………………caused and used computers and other devices directly and indirectly without authority to secure access to URA computerized systems, databases and servers and thereby obtained services of the same computers illegally, actions that led to loss…………..'

I find the interception and use alleged are part of the same transaction. There is no way the charge can be said to be duplex in the circumstances. All the accused persons have to do is prepare their defence against the accusation. It is prosecution evidence one needs to get authorization in order for one to use URA computer services.

The prosecution alleges that changes were made on the data base using the Data Base Owner (DBO). Proper Licensing officers' details were used to make it appear the changes were effected by persons who were authorized. It is alleged further that computers which were not registered on the URA domain were used and appeared as nhq-ws-966, nhq-ws-2227 and nhq-pvt-204.It was the Samsung laptop which had been recovered from A.1 that was found to have been used. It contained details of changes found also in the data base. This was manifest in the evidence of PW17 also who confirmed this using Batch 6 of Exhibit P.36. It was in regard to vehicles which in Exhibit 36 were serial numbers 113,117 and 120 as instances of this. Those vehicles were given registration numbers UAQ 697Q, UAQ 747Q and UAQ 773Q respectively. The vehicles in issue were Toyota Noah but they were assigned registration numbers which had already been given to Caterpillars and construction equipment. The prosecution evidence is to the effect that fictitious accounts were created to further the transactions. For example A. Ntumwa was used to release goods, E. Mubiru was used to exit goods, Barclays Phiona was used to receive payments and to have the goods released P Musitwa was used. The Samsung laptop had on it URA Teleworker profile for the VPN remote access yet this is restricted to staff of URA. A member of URA staff C. Nalwanga for example. She was a member of URA staff and her credentials were stolen after the owner of the Samsung laptop accessed the URA computer system, according to PW10. Further evidence was tendered of Exhibit P.25 with a list of URA staff user names and passwords on the external hard disk recovered in A.1's possession. The disk contained details of URA computers from Crested Towers, Busia, Katuna and several other posts. Administrator passwords and domains of URA staff were also available on the hard disk of the Samsung laptop as shown by Exhibit P.26.Then Batch 8 of Exhibit P.37 contains evidence of A.4's installation of Asycuda++ wholly. It was the evidence of PW10 that computer Cre-ws-200 had been identified by PW1 and IT security to have gained access to the URA system. That computer belonged to MTN where A.4 worked. The computer was in his possession. Then there was the evidence of PW17 who testified that there had been logging into the system by mtnuga. The user ID was Movis which is a system responsible for motor vehicles under URA.As a result, PW17 testified, there had been unauthorized changes in the motor vehicle system.

Asycuda++ was found also on the Samsung laptop recovered from A.1. Batch 4 of Exhibit 37 shows A.4 entered URA system using remote spyware. Further illustration of this is at page 5 of the Batch. The same exhibit in Batch 7 shows installation of Movis on A.4's machine. To show account bmugishaura@gmail.com was used in compromising the URA computer system through installation of remote spyware there is Exhibit P.37 Batch 3 at pages 3 and 6 where A.4 sent the e-mail he had created to URA Asycuda server. According to PW20 the modules found in the Samsung laptop, the external hard disk and the computer recovered from MTN which A.4 used were files for customs related transactions and one had to be a URA customs officer or staff of URA in order to access the utility files found on the devices A.1 and A.4 had had in their possession. One needed to be authorized in order for one to access URA computer system. Section 15 of the Computer Misuse Act relates not only to use but also interception requiring authorization. No evidence has been adduced to show there was authorization to use or intercept URA computer system be it Asycuda, Movis or any other. What is on record is uncontroverted evidence of computers and devices belonging to A.1 and A.4 accessing the URA computer system. There was evidence also of chats between A.1 and A.4 in Exhibit P.3 regarding plans to access the URA computer system. Account bmugishaura@gmail.com was used as the Trojan Horse to infiltrate the system. There is no way the transactions apparent on the URA motor vehicle data base and Asycuda could have been encumbered with digital footprints of the various laptops if the laptops had not intercepted and used the URA computer system. Similarly there is no way the various laptops and devices could have data restricted to URA computer systems if the laptops and devices had not been used to access the URA computer system.

The evidence of PW17 and Exhibit P.36 show that after they intercepted the URA computer service the accused went ahead and registered motor vehicles without paying the necessary taxes.

It was the evidence of PW17 that certain vehicles contained in Exhibit P.36 were inserted into the motor vehicle data base using a Samsung laptop which adopted different identities such as nhq-ws-966, nhq-ws-2227 and nhq-pvt-204. Alterations were made in consequence. It was her evidence three of the motor vehicles in Exhibit P.36 which bear serial numbers 113,117 and 120 had been registered as caterpillars and construction equipment but that as a result of the aforesaid insertions they appeared as Toyota Noah vehicles. Another example pointed out by PW17 is of motor vehicle UAQ 232T whose update statement was found on the Samsung laptop. It is vehicle number 91 which appears on page 3 of Batch 6 in Exhibit P.36. The owner was changed from Nuwagaba Eugene to Malagwe Saul and the vehicle is changed from a Subaru Forester to a Nissan Navarra. No taxes were paid for the Nissan Navarra in the event and loss resulted doubtless.

From the evidence above I am satisfied the prosecution has proved beyond reasonable doubt that A.1 and A.4 committed the offence in count I of the indictment and in agreement with the gentleman assessor I convict them accordingly. However I agree with the gentleman assessor that no evidence has been forthcoming against A2 and A3 to implicate them. I do acquit those accordingly.

Electronic fraud is the charge under count II. Deception is the main ingredient here, deliberately performed with the intention of securing an unfair or unlawful gain where part of a communication is sent through a computer network or any other communication and another part through the action of the victim of the offence or the action is performed through a computer network or both. In the instant case evidence has been led to show that there existed communication between A.1 and A.4 which aimed to deceive the URA by accessing its communication system using spyware in order to gain unfair and unlawful gain. They did indeed install the spyware which accessed the computer system of URA and went ahead to make the impugned insertions. It was the evidence of PW1 that computer name cre-ws-200 appearing in screen shot C2 of Exhibit P.1 had the ID Byamukr logged on as Movis. The evidence of PW10 regarding Exhibit P.24 confirmed that at one time A.4's laptop was cre-ws-200. This appears at pages 52 and 53.Ofcourse this was intended to deceive those in IT security at URA that it was a Crested Towers based computer of URA. On the other side the Samsung was also involved in deception like when PW10 points out that the URA ID Pwasenda was used by the user of the Samsung laptop to perform certain activities. Through impersonating Wasenda a command was given and a directory was obtained. Then followed a list of domain controllers and their passwords. It was then the Samsung user proceeded to use some of the credentials and to make it appear like what was done was done legitimately by a person with the requisite rights, whereas not.

In count II I find A.1 and A.4 guilty on the charge therein and in agreement with the gentleman assessor I convict them accordingly. However there is no evidence incriminating A2 and A3 and in agreement with the assessor I acquit both A.2 and A.3 on this count.

Count III charges the accused persons with unauthorized access by intentionally and without authority to do so interfering with data in a manner that causes the programme or data to be modified, damaged, destroyed or rendered ineffective. Needless to say data comprises electronic representations of information in any form. Section 7 of the Computer Misuse Act provides that a modification of the contents of any computer concerned or any other computer connected to it result into-

(a) A programme, data or data message held in the computer concerned being altered or erased, or

(b) A programme, data or data message being added to its contents.

In her testimony PW17 showed how modification in the Asycuda dispensation had taken place. Other users were created with unlimited access to the customs functions. This is evident in Exhibit P.37 which shows Asycuda installed and Batch 8 manifests the changes that result. This follows a request to a URA server for data. The installation of Movis by A.4 appears in Batch 7 of Exhibit P.37 .Then there is Exhibit 38. Batch 3 where guxzn (A.1) gives a command which clears all the event logs. Evidently all the above activities were done intentionally without authorization and they had the effect of altering and modifying the data base.

These activities show the involvement of both A.1 and A.4 who interfered with data to the extent that they modified it and to a certain extent damaged it. I find both A.1 and A.4 culpable and in agreement with the gentleman assessor I convict both A.1 and A.4 under count III. In agreement with the assessor I find A2 and A3 not guilty and acquit them.

The prosecution case against the four accused in count IV relates to procurement, possession of devices designed to overcome security measures or perform acts regarding a password, access code or any other similar kind of data.

It was the evidence of PW12 that from time to time A.4 would use his credit card to make orders and purchases. Curious as this may sound PW12 did not bother to find out much about the purchases his card was used for. There was evidence of when A.4 placed an order for a remote spy contraption. It was placed to a company called PLIMAS by Byamukama Robinhood whose email address turned out to be rbyamukama@gmail.com. PW12 stated that though his credit card was involved in the purchase, he personally had never made an order for the spy contraption indicated. There was evidence also of a key logger ordered from Florida by A4 using PW12's credit card. The evidence of PW12 is that when the order arrived he was contacted but he referred the matter to A.4 instead because A.4 had made the order using his credit card. The chats in Exhibit P.3 as well as evidence in Exhibit P.37 show that indeed A.4 made purchases of spyware.

As for possession of spyware there is evidence from PW10 that he found the programme Cain and Abel downloaded on A.4's laptop. Such evidence is found in Exhibit P.25 at page 58. There were also Back track files which had been installed in the URA computer system. The evidence of PW17 shows legion spyware discovered on A.4's laptop as well as tutorials on how to use them. All this is in Batch 1 and 2 of Exhibit P.37. As a matter of fact Exhibit P.3 is replete with chats between A1 and A4 relating to installation of spyware in the URA computer system. There is evidence of spyware used by A.1 and A4 in Exhibit P.37 particularly pages 1-11 thereof. The evidence of PW1, PW10 and PW17 connects both A1 and A4 to the devices. Indeed PW1 stated that from A1 devices such as Timviewer and remote desktop were recovered while from A.4 beside the Timviewer Dame ware was also recovered.

The evidence above shows A.1 and A4 did have in their possession spyware.A.4 procured spyware in addition to having it in his possession. I agree with the gentleman assessor that A1 and A2 should be found guilty on this count. However in agreement with the assessor I do not find A2 and A3 culpable in any way. Consequently I convict A1 and A4 on this count but acquit A2 and A3.

Count V states that a person commits an offence if he or she knowingly and without lawful authority by any means gains access to or attempts to gain access to any customs computerized system. The offence is under S.191 (1) (a) of the East African Community

Customs Management Act. The East African Community Customs Management Act in section 2 defines customs as the customs department of the Partner States. Uganda Revenue Authority is the customs department of Uganda doubtless. Evidence has been adduced in this case showing that the computerized system of URA such as Asycuda and Movis was interfered with when it was accessed and modifications and alterations were made to the data. There is evidence of chats between A1 and A4 regarding the preparations to effect compromising of the system as evidenced in Exhibit P.3. Needless to say those activities had no authorization of URA.

The gentleman assessor advised me to find A1 and A4 guilty as charged on this count. I agree with him regarding A2 and A3 who I find have not been incriminated by the evidence. Similarly I agree with his verdict regarding A1 and A4. I find A1 and A4 guilty of the charge in count V and convict both accordingly.

Concerning count VI section 203(e) of the East African Community Customs Management Act states that a person who in any matter relating to the customs in any way is knowingly concerned in any fraudulent evasion of the payment of any duty commits an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding ten thousand dollars. For the record the accused persons are alleged to be responsible for the loss of shs.2, 461,447,275 and 78 cents, being the amount not paid in duty. It was submitted by the State Attorney that the burden to disprove the allegation against the accused rested with the accused themselves. Needless to say the burden of proof usually is on the prosecution as the case of ***Sekitoleko V Uganda [1967] EA 531*** should signify. It is only in very rare cases particularly those dealing with taxation one finds strict liability involved. One is then held culpable for conduct the law has declared criminal. Then there is no need to prove knowledge or intent. Yet in this charge there is need to prove knowledge and this should be proved not by accused but by the person who alleges knowledge, the prosecution. No proof is forthcoming from the prosecution that accused severally had knowledge of the loss of the shs 2,461,447,275 and 78 cents as unpaid duty. Worse still no evidence was tendered to show how that sum was come by. There is neither an audit report nor evidence showing how much each of the accused persons contributed towards the alleged loss. Evidence is lacking also to show that all the four accused or some of them acted in concert to commit the offence. In the absence of proof of common intention the accused persons cannot be lumped together as liable for the alleged loss. In the premises I do not find count VI proved against any of the accused persons. The gentleman assessor advised me to find only A1 and A4 guilty. For the reasons I have given above I do not agree with his advice. I find all the accused not guilty of the offence in count VI and acquit them.

Regarding count V and count VI the Statute from which the charges were derived is the East African Community Customs Management Act. The Act was enacted in 2004, which should be the year it should be mentioned in reference with. There was a reprint of the Act in 2009.That is the year of reprint and not of reference. The prosecution erred when they referred to the Act as the East African Community Customs Management Act of 2009 and not of 2004. I note there is only one such Act, that of 2004 which was reprinted in 2009. There is no evidence the accused persons were in any way prejudiced by the regrettable error on the part of the prosecution. Needless to say the accused pleaded not guilty to the two counts. No miscarriage of justice has resulted in the circumstances.

I must relate also to the manner in which the evidence tendered before this court from the laptops and the external hard disk involved was extracted. I shared the anxiety of many to ensure the best evidence possible was presented. This is primary evidence which is given premium consideration.PW10 testified concerning the Encase investigation solution which was employed. It was described as reliable and that it ensured the integrity of the data was not compromised. In court PW1 was asked by the defence to delete or type into the Encase environment but he was not able to do so. He said it was not possible to delete or type there. Encase solution is used by forensic practitioners who need to conduct efficient forensically sound data collection and investigations which it is said can be repeatable and defensible. Data is acquired from a wide variety of devices and potential evidence is unearthed with disk level forensic analysis. At the same time Encase forensic experts maintain the forensic integrity of their evidence. The Encase Legal Journal, 2011 edition published to serve as a practitioner's guide to legal issues related to digital investigations and electronic discovery relates to the above information on Encase solution and properties. For a court situation the U.S case of ***Armstrong V Executive Office of the President***, IF.3d 1274(D.C.Cir 1993 should come handy. There court held that a 'hard copy' paper printout of an electronic document would not ‘necessarily’ include all the information held in the computer memory as part of the electronic document’. The court further noted that without the retention of a complete digital copy of an electronic document such as an e-mail message, `essential transmittal relevant to a fuller understanding of the context and input of an electric communication will simply vanish’. Fortunately both the devices and the extracts in this case were proffered in evidence .The American case simplifies also the process regarding an electronic record under the Computer Misuse Act. I am satisfied the evidence which was tendered by the prosecution from the extracts was not only authentic but integral.

In the result I find A.2 and A.3 not guilty of any offence in the indictment and order that they be set at liberty forthwith. A.1 and A.4 are convicted on all counts save for count VI.

……………………

Paul K. Mugamba

Judge

3rd April 2013.

SENTENCE

Nsubuga Guster, the first convict, and Robin hood Byamukama, the other convict, singularly and through their counsel express their regret for what they did and ask this court to be lenient when passing sentence. Besides their young age both told court that they have families and that they are bread winners for their respective families. The state on the other hand seeks for a stiff sentence to be handed down to each of the convicts arguing that what they did resulted in tremendous loss to the exchequer of URA and compromised the security system of the country. Doubtless it shakes the faith people here and abroad have in that body fondly known as URA. Ramifications of Cyber crime are not as obvious as those of robbery for instance in the short term. In the long run one notices the greed of those who seek to disinherit the poorest of the poor through discreet methods such as the convicts sought to employ and did apply to sordid effect.

I have anxiously considered the recommendation of the prosecution to invoke S.20 of the Computer Misuse Act where convicts in like offences are liable to life imprisonment for offences under count 1, count 3 and count 4. I note the convicts have no previous record and that they are relatively young men. I have taken into account the period they have spent on remand and the fact that they have young families. Of course I bear in mind their remorse. Consequently I sentence each of the convicts to 12 years' imprisonment on count 2. On count 1, 3, and 4 I sentence each one of them to 8 years' imprisonment. On count 5 each of the convicts is sentenced to a fine US$4,500. The custodial sentences are to run concurrently.

Concerning pecuniary losses possibilities may be sought elsewhere if applicable.

Paul K. Mugamba

Judge

3rd April 2013.