# Forensic Identification of Unique Kali Systems Through the Use of File Hashes and Names

Troy Ward January 25, 2021

# Table of Contents

Introduction	4
Kali Linux	4
Methodology	4
Analysis	5
Unique Names	6
Eth0.lease	6
Font Config	7
LightDM	8
System.Journal	9
Hashes	9
/boot	. 11
Initrd.img	. 11
grub.cfg	. 11
/etc	. 12
adjtime	. 12
cacerts	. 13
fstab	. 14
machine-id	. 14
resume	. 15
server_config.yml	. 15
shadow	
ssh_host_*_key	. 18
ssl cert snakeoil	
Wired Connection 1	. 20
/usr	. 20
.uuid	
classes.isa	.21
pyc files	.21
/var	. 23
Xauthority	. 23
aux-cache	. 23
boot duration	.23
 cookie	.24
default_cert.pem	.24
Index.db	
kali-amd64	. 26
mlocate.db	. 26
MySQL files	. 26
pubring.kbx	
questions.dat	
random-seed	
timestamps	
Conclusion	
Appendix 1: Always Unique Hashes	
Appendix 2: Uniquely Named Files	

# **Table of Tables**

Table 1 Count of Files by Directory	5
Table 2 Top 20 Repeated Hashes	
Table 3 Byte Comparison of /usr/lib/python3/dist-	
packages/IPython/core/ pycache /application.cpython-38.pyc	
Table 4 Always Unique Hash Listing	
Table 5 Uniquely Named Files	

# **Table of Figures**

Figure 1 Network Interface Card UID/Lease Comparison	6
Figure 2 NIC UID Appearances in Logs	
Figure 3 Uniquely named files located in /var/cache/fontfig	7
Figure 4 /etc/machine-id and /var/lib/lightdm/.configure/pulse comparison	8
Figure 5 /etc/machine-id vs /var/log/journal/ <uid> Comparison</uid>	9
Figure 7 /boot/grub/grub.cfg Differences	12
Figure 8 /etc/adjtime differences	13
Figure 9 File Comparission of /etc/ssl/certs/java/cacerts	13
Figure 10 /etc/fstab differences	14
Figure 11 /etc/machine-id Comparison	15
Figure 12 /etc/initramfs-tools/conf.d/resume Differences	15
Figure 13 /etc/king-phisher/server_config.yml Comparison	16
Figure 14 /etc/shadow differences	17
Figure 15 /etc/ssl/certs/ssl-cert-snakeoil.pem comparrision	19
Figure 16 /etc/NetworkManager/system-connections/Wired connection 1 differences	20
Figure 17 /usr/share/.uuid and /var/carche/fontconfig correlation	21
Figure 18 Byte Comparison of /usr/lib/python3.8/pycache/_pyio.cpython-38.pyc	22
Figure 19 /var/lib/lightdm/.Xauthority differences	23
Figure 20 /var/lib/inetsim/certs/default_cert.pem comparison	25
Figure 21 Uniquely named files located within mlocate.db	26
Figure 22 /var/lib/lightdm/.gnupg/pubring.kbx comparison	27
Figure 23 /var/lib/systemd/random-seed	29
Figure 24 /var/lin/NetworkManager/timestamps differences	29

## Introduction

The act of attributing a cyber attack is a long sought after, but rarely attained goal. From a legal perspective, the ability to attribute a cyberattack to an individual or a group is a vital step to lead to its ultimate prosecution in a court of law. In terms of national defense, attributing an attack accurately can be a step towards reprisal or other military responses.

While things such as techniques, IP addresses, and other artifacts can plan an important role in attributing an attack, being able to attribute actions to a specific computer that has been obtained can help provide overwhelming proof of an act.

A primary task of a forensic investigator is identifying information that can be used to tie something to a specific individual computer. As we use a computer, it becomes more and more individualized to its user. This occurs through the use and configuration of software, the creation of documents, and the browsing of websites among many other ways. Many of these actions leave artifacts that can uniquely be tied to a single system.

One way to minimize the ability to find artifacts that are unique to a system is to use a freshly installed operating system. This can be done through the use of a live-boot operating system, or just creating a freshly installed system. In theory, there is nothing that differentiates two copies of an operating system if they are installed the same way. In reality, though, there are a small number of artifacts that uniquely identify a system as soon as the operating system is installed.

This paper documents the first of what I expect will be several experiments designed to identify a method to uniquely identify a particular system. The hope is to find artifacts that are resistant to reboot, cloning of virtual machines, or intentional/unintentional modification.

## Kali Linux

Kali Linux is a highly popular Linux distribution known for its use by "hackers". Under the hood, Kali is a highly modified and customized version of Debian which is maintained by Offensive Security<sup>1</sup>. The operating system comes with a large number of tools already installed and configured to allow for use from "out of the box".

## Methodology

This first set of experiments is designed to look for identifiable unique signatures that can be observed by a user with root access to the system. While advanced forensic tools were used during the examination of the system disks, this was only done for ease of use. The techniques used to identify "interesting" files only required tools that are inherent on most versions of Linux to a user with root access.

The factors that I looked at include:

• The presence of uniquely named files

<sup>&</sup>lt;sup>1</sup> https://www.kali.org/

• The presence of commonly named files with unique MD5 hashes<sup>2</sup>

The experiment made use of four identically installed and configured Kali systems. Each system was initially created on 7/22/2020. The same installation media and procedures were used to create each image. All systems were built using a copy of Kali 2020.2 AMD64 iso with a MD5 hash of 9efa96f1069aaa2fcacd56bcd55330824f290e21. All systems were installed on a virtual machine being hosted on VMWare Player 15.5.6. Each system had 20 GB hard drives, 2 GB of RAM, and 1 CPU core. All default installation values were accepted for each install. Upon the completion of the installation, the system was rebooted, and then immediately turned off once it arrived at the login screen (no systems were logged into).

The system's virtual hard drive was mounted in a read-only configuration to the analysis operating system to allow for a view of the disk without the risk of modifying any data present on it. Once mounted, a script was run that traversed across the entire mounted disk and performed an MD5 hash of all files encountered as well as recording other vital information such as owner/group of the file, permissions, file access, modification, and creation times, and other information. This is all information that any person with root access to the actual device would be able to determine themselves.

The results of the MD5 hashes and file metadata were fed into a Splunk instance which was then used to do the data analysis and identify "interesting" files. To aid in the analysis of individual files, the virtual hard drives were ingested into Autopsy to allow for further indexing and hex level examination of individual files.

## Analysis

The initial examination of each system image found a total of 284,996 files on the disk. The files were spread out across six directories (see Table 1). What I find interesting in the table is what isn't here. If you notice, there were no files found within /bin, /sbin, or /lib. It's because if you do a full directory listing of /, you'll find that they all symbolic links going back to /usr/bin, /usr/sbin, and /usr/lib respectively.

Path	File Count
/boot	305
/etc	1362
/home	6
/root	3
/usr	272,819
/var	10,501

Table 1 Count of Files by Directory

<sup>&</sup>lt;sup>2</sup> I realize that MD5 is a long since insecure hash in a variety of situations, including in some instances, digital forensics, but given the fact that it is faster to run on my test systems vs. SHA1 and SHA256, and the fact that there is little chance of a file purposely being manipulated to "appear" to be common, I think that this is an acceptable trade-off.

## **Unique Names**

An initial examination of the nearly 285K files found that only 45 files per image (0.01%) had a unique filename<sup>3</sup>. In addition to the 45 unique file names, a single directory on each system image was also found to have a unique name

## Eth0.lease

Located within the /var/lib/NetworkManager directory is a file named internal-<UUID>-<Interface ID>.lease (i.e. internal-bdf3e5cc-852d-47f8-b8c3-aaaa604e78d1-eth0.lease). The UID in the name refers to the UID that is assigned to that particular interface in "/etc/NetworkManager/system-connections/Wired connection 1" (see Figure 1).

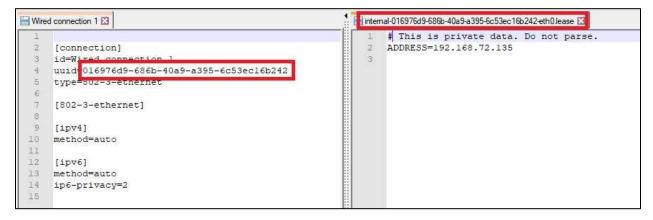


Figure 1 Network Interface Card UID/Lease Comparison

The UID for the NIC makes numerous appearances within /var/log/syslog, as the system boots up (see Figure 2).

L CRINO	Ang, KaW2H.cm	dunol vegneckughriskig	2020-07-02-13-00113-040	2020-07-2213.00.13.001	2003-07-02 13:44/01 0/01	2820-07-22 13:49:51 684	
Wired connection 1	Ang Juli 1. m	didvel_collines/Network/Merager/system	2020-07-02 13:40(34 GMT	2000-07-22 13-49-34 GPT	1000-07-22 13;49:01 GPT	2020-07-22 13 49-34 (2011	18
< []]							
Hex Text File Hetodate R	esuite Annotations Other Occur	WICHS					
Strenge Indexed Text							
Page: 5 of 5 Page 💿 🕘 Hatches on page: 1	L of 3 Heath 🗧 🔶 100	≤ ØØ Reset					Tes
Jul 21 09 49:00 sals second: 1 9.90	salatj penetit dodd of d	1.3 ethi link up					
Jul 13 09:40:54 Kali HetmutHanager (4)	64): <info> (1586425764</info>	(1122) device (eth); carrie	a: link connected				
	system) Successfully						
341 22 00:40:54 kali dhun-daemum(465) 341 22 05:40:54 kali systemd(1): Ptart		artivated service 'urg.freed					
241 22 00:49:54 kali dhun-daemon(#65)	ted Wetwork Hansger Sori;	artivated service 'urg.freed	eektop nu_dispatcher'				
<pre>Jul 22 09:49:54 kals dbus-daemon(#45) Jul 22 09:40:54 kals systemd(1): Ptart</pre>	ted Wetwork Hanager Sori; 66]: -info- (1595425794	artivated service "urg freed pt Dispatcher Service.	eektop nu_diepatober' hateger evailable	discontected insann.	'none', averiface share	te: 'menaped')	
241 22 00:40:54 tal: dbuo-daemon(065) 241 22 00:40:54 tal: systemd(1): Ptart 241 22 00:40:54 tal: Servortlansger(44	ted Wetwork Hanager Scrip 661: -info- (1196421794 661: -info- (1195421794	artivated service 'urg.fixed pt Dispetcher Service. .2001) modem-manager: Hoderfi	Besktop nu_diepetober' Anager evailable change: unevailable =>				
Del 20 00 40:54 mai: shun-sheemen(46) Del 20 00:40:54 mai: systems(1): Part Del 20 00:40:54 mai: systems(1): Part Del 20 00:40:54 mai: BetworkNemaper(44 Del 20 00:40:55 mai: DetworkNemaper(44 Del 20 00:40:55 mai: DetworkNemaper(44)	ted Vetwork Hansger Scrij 661: -into- (1555428754 661: -into- (1555428754 661: -into- (1555428754	artivated service "urg fleed pt Dispatcher Service. 2001) modem-manager: Hoderfl 27451 device (eth2): state	Weaktop nu_diepatoker' hanager available change: unavailable == ng connection 'Wires' co	niversion 1* 101897649	-2008-40a5-a555-5c53e	c166242)	
2al 22 00 40 54 bals dhun-dhemarn (465) 2al 23 05 45 54 bals system (11) Fran- 2d 23 05 45 54 bals meroschlanger (4 2d 23 05 45 54 bals meroschlanger (4 2d 23 05 45 54 bals Meroschlanger (4 2d 23 05 45 46 bals Metoschlanger (4	ted Detwork Hanager Scrij 661: -info- 11535425734 661: -info- 11535425734 661: -info- 11535425734 661: -info- 11535425734 661: -info- 11535425734	artivated service 'urg fised pt Dispatcher Service. 2001) moden manager: HodenN 27493 device (etb): state 09991 policy: ento-activati	Besktop na_dispatcher' hanger evailable change: mavailable ing convertion "Bired or hiom: eterting moment)	nnection 1º 1016376d2	-2010-4045-4395-6553e 21. 101497645-4946-494	e165242) 6-a155-6455ae160242)	
Jul 20         00-40-54         ball dhun-daemum (865)           Jul 20         00-40-54         ball syntemet (11)         band           Jul 20         00-40-54         ball memorylamaper (4)         ball 20           Jul 20         00-40-54         ball memorylamaper (4)         ball 21           Jul 20         00-40-54         ball memorylamaper (4)         ball 21           Jul 21         00-40-54         ball memorylamaper (4)         ball 22	ted Wetsigit Hanager Sori; GG): "info" [1555425794 GG): "info" [1555425794 GG]: "info" [1555425794 GG]: "info" [1555425794 GG]: "info" [1555425794 GG]: "info" [1555425794	artivated service "urg.freed pt Dispatcher Service. 2001) modetrmanager: Hoderfi 27451 device (etb0): stete. 00551 policy: extorectiveti 09191 device (etb0): Artiva	Weitop nu_dispatcher' inneger evailable changer innvailable ing convertion "Wired on dion; starting converti change: disconverted	nnechina I <sup>+</sup> 101657665 Am "Miles a mechian prepara thermal and	-2010-4045-4395-6553e 21. 101497645-4946-494	e165242) 6-a155-6455ae160242)	
701         20         00         60         FA HALI disamined[1]           701         20         60         64         HALI disamined[1]         Ftani           701         20         64         64         Intervolutionage         14           701         20         64         64         Intervolutionage         14	ted Versick Hanager Sori GG1: "info" (155420754 GG1: "info" (1555420754 GG1: "info" (1555420754 GG1: "info" (1555420754 GG1: "info" (1555420756 GG1: "info" (1555420756 GG1: "info" (1555420756	artivated service 'urg freed pt Dispecter Ferrice. 2007) modernmanager: Hoderff 27451 device (etb0): state 00051 policy external etb0; 07191 device (etb0): state 02041 device (etb0): state	sektop nu dispatokar' knager evallable change: unavallable ng convention 'Pired on hion: etasting unaveri change: disconnected change i disconnected ch	niweraion I <sup>4</sup> 101697605 on "Wilsed or meetaon prepara 1000000 "NOT THO	-1945-4045-4095-65534 11 101497645-4045-65534 11 101497645-4045-6546	e169242) 9-8591-14554e140242) -8292[837]	
Dal 22 00:40:54 bals dhun-dawman 8461           Dal 23 00:40:54 bals synewed [1]) Finar           Dal 20 00:40:54 bals           Dan 20 00:40:54 bals	ted Wetwork Hanager Sori GG1: -Linfo- (1359438794 GG1: -Linfo- (1359428794 GG1: -Linfo- (1359428794 GG1: -Linfo- (1359428794 GG1: -Linfo- (1359428794 GG1: -Linfo- (1356428794 GG1: -Linfo- (1356428794 GG1: -Linfo- (1556428794	entimated service 'ung fixed pt Dispective Service. 2001) modern manager Hodeff 27401 device (wtb0): state 20001 policy entron-activati 2010 device (wtb0): state 2010 device (wtb0): state 2020] manager: Metanzolang 2024] device (wtb0): state	<pre>sektop nm_dispatcher' https: unsvallable change: unsvallable =- ing consention "Wirst or iduon seasching unswarl change: disconnected net state is nov commert mange; prepare com </pre>	niwenion I <sup>1</sup> [0,1378d] an "Mijed monethion "prepare (person non ING ING	-1286-4045-4335-5554 1' (11957645-4346-434 8', (VE-12854-43446 4-11946-41410) 'manap	c10541) 5-4151-(4554c100141) "800(99") 95")	
341 22 09:45:54 bal: dbus-dbeens 445) 341 22 09:45:54 bal: systemd[1]: Start 341 22 09:45:54 bal: BetwortHinager[44 341 22 09:45:54 bal: BetwortHinager[44	ted Wetwick Hanager Scrij GG1: winfo: (1359428794 GG1: winfo: (1359428794 GG1: winfo: (1359428794 GG1: winfo: (1359428794 GG1: winfo: (1359428794 GG1: winfo: (1359428794 GG1: winfo: (155428794 GG1: winfo: (155428794	aritvirad service "ung freed pr Dispatcher Service. 2003) podermanager: Hoderff 27453 device (etb0): state 00033 policy: sobt aritvir 00031 policy: sobt aritvir 00131 device (etb0): Aritvi 00241 device (etb0): state 0223 manager: Seturbilanag	seitop mydispatcher hanger svallable change: unsvallable ing connection "Mirred or hior: eisething sommeric dange: disconnected prestate is now COMMAN change: prepare com dange outig ip-or hange outig ip-or	ntwomion 1° 10,137607 An "Mised momention propose (setton "non THO LQ ITEASON 'DODA', 47 mfly (TEASON 'DODA', 47	-1785-4045-4375-5534 1' 11457645-4395-504 8'' WY-114576-414 s-lface-state: "manap sps-lface-state: "man	c10541) 5-4151-(4554c100141) "800(99") 95")	

Figure 2 NIC UID Appearances in Logs

The fact that the name is made up of a UUID that is assigned at the time of creation means that it can be tied to a single system. While it is likely possible to change the UUID present within both the file name and the interface configuration, it would be important to identify all instances where the same UID

<sup>&</sup>lt;sup>3</sup> For this we consider the combination of path and file name to be a file name

appeared within logs on the system. On a system without remote logging, this would be difficult but possible. Because of this, I consider this to be a moderately confident indicator of a particular system.

## **Font Config**

Of the 45 uniquely named files, 38 of them (84%) were located in the /var/cache/fontconfig/ directory. Each of these files had a name consisting of a 36 character Universally Unique Identifier (UUID) followed by "-le64.cache-7" (i.e. a185396b-1e43-43cd-8ca0-31de187f9b4e-le64.cache-7). The UUID in each file name was different from the other files on the same system (see Figure 3).

Name	S (	С	Modified Time	Change Time	Access Time
退 [current folder]			2020-07-22 13:47:31 GMT	2020-07-22 13:47:31 GMT	2020-07-22 13:47:31 GM
📜 [parent folder]			2020-07-22 13:49:52 GMT	2020-07-22 13:49:52 GMT	2020-03-30 20:22:14 GM
02d4f520-a997-4d93-9fff-6082379a324e-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
05d9d9df-8b2b-4c25-91da-3e240196b756-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
0a0e8bb7-3085-40c3-8c39-e823b0f05d36-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
136f21f7-d779-44fe-94bd-9acca931261b-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
19471168-b12b-4cfe-b66d-78fa53b13167-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
bd710f5-632e-46c7-aac0-ccbe00c423dc-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
1e7ae182-406c-4bec-ab4d-2d0c2bb24054-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:49:59 GM
26927276-cfe8-4d8e-b66b-5697d2ba5bb5-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
2955b303-602c-46f4-8e44-4378d47f8400-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:49:59 GM
2c53115d-7f38-4bfc-9172-71687740e27d-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
2ef35129-5b00-4bcd-8bcf-b1bf54d629cb-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
34aff380-48fd-44b1-9b1d-071c52895e13-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
564a544d-a92e-4a43-9a50-5d35b8306f57-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
57934f48-9bfa-45c1-bb8f-66c726d0a2b6-le64.cache-7			2020-07-22 13:47:31 GMT	2020-07-22 13:47:31 GMT	2020-07-22 13:50:01 GM
586e1327-7f72-4fad-b160-c8cc02421c48-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
594ec2e8-d50e-45d2-b381-c21880502f86-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
5d74a0ea-6c03-47df-a268-8df6d3645fff-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
7231c049-01f8-4488-ac0c-b0e5c4b59ecd-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
761618bc-ca18-497b-ab10-b24955b0250d-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM
82323306-e521-49b2-885f-e57265725cf3-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
90833a27-c08d-4e82-94df-92d24ecebbe2-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
9cf6e8b1-bfcc-4fb9-800c-c080822c6433-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
a 1214b3a-75c4-4241-ad6f-692e75b8c09f-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:49:59 GM
a437f435-1eb7-44d5-be3d-dc6bce27adfa-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:49:59 GM
a5e62240-c06e-4786-a111-1d916b98e579-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
ac2ede34-3e40-4594-9f86-03729fd892cc-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GM
bda66590-93bf-4994-a514-50b9e2ec119f-le64.cache-7			2020-07-22 13:47:31 GMT	2020-07-22 13:47:31 GMT	2020-07-22 13:49:59 GN
c0b0467c-cc0f-4844-9c8a-27e4ffbc4834-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:01 GN
c4fa06ad-f49f-4925-a331-caffb2d66b77-le64.cache-7			2020-07-22 13:47:30 GMT	2020-07-22 13:47:30 GMT	2020-07-22 13:50:00 GM

Figure 3 Uniquely named files located in /var/cache/fontfig

Font Config is a library designed to configure and manage various fonts on the system. When an application needs to make use of a font that has been installed on the system, Font Config provides access to the requested font. If the requested font isn't available, Font Config attempts to find a similar

one<sup>4</sup>. To speed up system operation, Font Config creates a cache of all fonts installed on the system. These \*-le64.cache-7 files are those font caches.

Because these file names are made up of actual UUIDs that are generated at the time of creation, they are unique to that particular system. That being said though because it is a cache, the files can safely be deleted but it will impact system performance. The cache can be regenerated through the fc-cache -f command which will force a cache regeneration<sup>5</sup>.

## LightDM

Another five of the uniquely named files are located in /var/lib/lightdm/.config/pulse/. These files all consisted of a single 32-character ID<sup>6</sup>, followed by one of the following:

- -stream-volumes.tdb
- -device-volumes.tdb
- -default-source
- -default-sink
- -card-database.tdb

An example of this is /var/lib/lightdm/.config/pulse/d94a20e2919f456db65752d2fa3df4d8-stream-volumes.tdb. It is important to note that all five of the files exist on each system. The ID string at the start of each file name is actually the same value found within /etc/machine-id (see Figure 4).

ame	s	С	Modified Time	Change Time	Access
cookie	0		2020-07-22 13:50:01 GMT	2020-07-22 13:50:01 GMT	2020-0
[parent folder]			2020-07-22 13:49:59 GMT	2020-07-22 13:49:59 GMT	2020-0
[arrent folder]			2020-07-22 13:50:06 GMT	2020-07-22 13:50:06 GMT	2020-0
6419ad21b7384371a12b5877060147c5-tream-volumes.tdb			2020-07-22 13:49:59 GMT	2020-07-22 13:49:59 GMT	2020-0
6419ad21b7384371a12b5877060147c5- evice-volumes.tdb			2020-07-22 13:50:01 GMT	2020-07-22 13:50:01 GMT	2020-0
6419ad21b7384371a12b5877060147c5tefault-source			2020-07-22 13:50:06 GMT	2020-07-22 13:50:06 GMT	2020-0
6419ad21b7384371a12b5877060147c5 efault-sink			2020-07-22 13:50:06 GMT	2020-07-22 13:50:06 GMT	2020-0
6419ad21b7384371a12b5877060147c5-ard-database.tdb			2020-07-22 13:49:59 GMT	2020-07-22 13:49:59 GMT	2020-0

Figure 4 /etc/machine-id and /var/lib/lightdm/.configure/pulse comparison

<sup>&</sup>lt;sup>4</sup> https://en.wikipedia.org/wiki/Fontconfig

<sup>&</sup>lt;sup>5</sup> https://linux.die.net/man/1/fc-cache

<sup>&</sup>lt;sup>6</sup> Note: The ID string presented is similar to a UUID but does not meet the exact technical requirements to be considered on. See https://www.itu.int/en/ITU-T/asn1/Pages/UUID/uuids.aspx

LightDM is a cross-platform display manager that provides the initial login and then the desktop for the Kali workstation<sup>7</sup>. LightDM is one of several choices but is currently the default installed. The pulse in the pathname refers to the Pulse Audio capability that it offers

## System.Journal

Another uniquely named file is actually a unique folder. Located at /var/log/journal/<UID> is a folder that contains the system journal. Once again, the UID found in the folder name is the same UID found in /etc/machine-id (see Figure 5). Within the folder is the system journal which records all significant events related to the system.

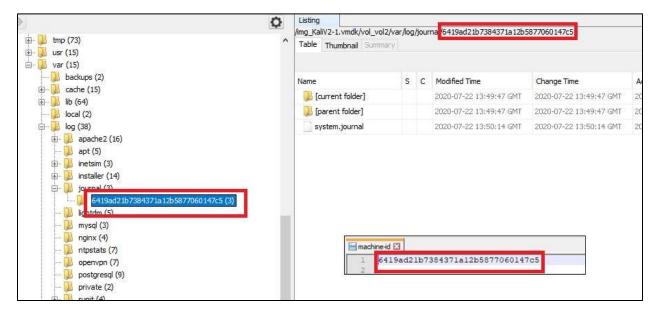


Figure 5 /etc/machine-id vs /var/log/journal/<UID> Comparison

While it is possible to delete the folder and it's contents, the folder will automatically be regenerated (with the same UID) either immediately or upon the restart of Systemd service<sup>8</sup>.

## Hashes

As noted above, each system image contained 284,996 files, each with its own MD5 hash. Of those, there were a total of 267,192 unique hashes. Of those, 7,880 hashes were repeated two or more times meaning that approximately 90% of the files were unique across the disk. Table 2 shows the 20 most repeated hashes that were found on the drive image, along with one of the files that used that hash.

<sup>&</sup>lt;sup>7</sup> https://wiki.debian.org/LightDM

<sup>&</sup>lt;sup>8</sup> https://www.freedesktop.org/software/systemd/man/systemd-journald.service.html

File Hash	Total Files	Example File
d41d8cd98f00b204e9800998ecf8427e	1386	/usr/lib/llvm-9/build/utils/lit/lit/builtin_commands/initpy
68b329da9893e34099c7d8ad5cb9c940	490	/usr/lib/python3/dist-packages/filedepot-0.5.2.egg-info/not-zip-safe
b3c40037edbaf26a9bffb1a3d4cf734e	207	/usr/lib/python3/dist-packages/OpenGL/GL/APPLE/initpy
5e1d07d82002f02a87f0f26be2d59c7b	193	/var/lib/dpkg/info/libksba8:amd64.triggers
2922a1ff6ca1e589db20b56a1b856709	122	/usr/lib/python3/dist- packages/plotly/validators/layout/updatemenu/font/initpy
1d35517f12a3c14d7ec65e84bc0dde06	106	/usr/share/help/eu/mate-calc/legal.xml
e0d0fd012f6293f533701effcc6256fe	99	/usr/lib/python3/dist-packages/plotly/graph_objs/ohlc/hoverlabel/initpy
650ba8a15be160b30bf3bd05b5e29293	93	/var/lib/dpkg/info/libvisual-0.4-0:amd64.triggers
feebc3772e647be7c2fffe255fc99cfa	79	/usr/share/help/kab/atril/legal.xml
2744d2bc4adbbf6a7ccd67d74bd9991f	76	/usr/lib/python3/dist- packages/plotly/validators/scatter3d/hoverlabel/font/initpy
93c3413b07bba9d38750255de2755431	66	/var/lib/dpkg/info/libproxy1v5:amd64.triggers
ad93072740c556aa6a8d73084aeff2ca	55	/var/lib/dpkg/info/libprotobuf23:amd64.triggers
ef758398051ffbc2baca272f62f4c6dd	53	/var/lib/dpkg/info/libi2c0:amd64.triggers
ff49aa304d48c6a7c101de3135d66052	51	/usr/lib/python3/dist-packages/faraday/utils/initpy
4d17ffa4ebca8d702245a276a1cfe2a0	48	/usr/lib/python3/dist- packages/plotly/validators/layout/xaxis/tickformatstop/initpy
3c124a19ee0e1348068465cbac8387b7	47	/usr/lib/python3/dist-packages/plotly/validators/scatter3d/stream/initpy
1bd16ddfbfdcc942da8f98f69966e6fe	44	/usr/lib/python3/dist- packages/plotly/graph_objs/choropleth/colorbar/initpy
0ec9da0a97e8e2f03542d8acfb4fcc7b	42	/usr/lib/python3/dist-packages/plotly/validators/scatter3d/hoverlabel/initpy
37802a7cc55bef61ab6453d144b186c6	39	/usr/share/icons/Flat-Remix-Blue-Dark/panel/weather-clear-night-260.svg
fcbe8b2739c9b6ffae4de75d6f462464	39	/usr/share/icons/Flat-Remix-Blue-Light/panel/weather-clear-night-260.svg

Table 2 Top 20 Repeated Hashes

It stands to reason that one of two things will be true for every file that is included on all four system images (This is excluding the 45 files that had unique names). The first possibility is that the same file will have the same hash on all four systems. If the file is being copied over from the install image or downloaded from a repository, then there is no reason it would change between images (unless that package is updated). The other possibility is that the same file will have a unique hash for each of the four images. This is likely to occur when the file is generated as part of the install instead of being copied onto the system.

Out of the 284,951 common files found on all four system images, only 281 of them did not share a common hash across all four images. This means that each installation is 99.9% the same. Of the 281 files that did not have a consistent hash, 202 of them had a unique hash on each of the drive images. For the remainder of this paper, they will be referred to as "Always Unique" files.

Many of these Always Unique files are not at all surprising. For example, 22 (9%) of the files live in /var/log. The data included in log files for two different systems is almost guaranteed to be different (at the very least the times are likely to be different) which will cause the file to produce a unique hash. As a side note, it is important to remember that even if an image is copied, the chances are that the hash of a log file will change very quickly once the system is in use again.

As I said, I expected for a file either to be the same across all four images or to be unique across all four images. When I began looking at the data though, I found 79 files that had either two or three different hashes instead of one or four as expected. This got my attention. We will call these "semi-unique" hashes. In the following sections, we'll examine each file or set of files that presents a unique or semi-unique hash.

## /boot

### Initrd.img

Initrd (initial ramdisk) files are used by the system at the initial boot. They are responsible for loading a temporary file system into memory which is then used to mount to the true root file system so booting can continue<sup>9</sup>. Because of the vast number of different types of hardware that are available for a computer, this image is stripped down to the bare essentials just to get the system to a point where it can load the much large and fully configured kernel.

The initrd.img files are created when the operating system is installed and are statically compiled to that particular system. This means that the initrd.img file is unique to the system. Each system image contained an initrd.img file at both /boot/initrd.img-5.5.0-kali2-amd64 and /boot/initrd.img-5.7.0-kali1-amd64. The two files themselves are also different from each other.

Because these files are compiled specifically to this machine, they will always present a unique signature meaning that they can be tied to a specific machine. There are indications that these files can be regenerated after the system has already been installed, but this is a process that I have not personally tried and do not know if it will even work, let alone generate a new hash for the file<sup>10</sup>.

### grub.cfg

/boot/grub/grub.cfg is a 245-line file that is generated near the end of the installation of Kali. The file contains the configuration for the Grub bootloader that runs immediately when the computer is started. It is responsible for loading and then transferring control of the system to the desired operating system's kernel<sup>11</sup>. The file is generated using the **grub-mkconfig** command.

Of the 245 lines within the file, 27 of them are unique. Each of the 27 lines that are different contain the UUID of the file system installed by Kali. This UUID is the same on all 27 lines within the config but different between each file image (see Figure 6). This UUID number can also be found in /etc/fstab as described below.

<sup>9</sup> https://wiki.debian.org/Initrd

<sup>&</sup>lt;sup>10</sup> https://linoxide.com/linux-how-to/fixing-broken-initrd-image-linux/

<sup>&</sup>lt;sup>11</sup> https://www.gnu.org/software/grub/manual/grub/grub.html

Section in which	an 2010 and 1	A littlet	1,98812	Ling D
10	limod ecti .			Lamod est2
20	wet signification in the second s	11:34		new reserve 'hold', wardowil'
	at [ alterature platform search block = av [; then	1.2.1%		10   alleahure platition search him " at  ; then
14	wards	1 Cale		search over flower offerand washington which have well as a prior affection and and
10.11	e			alar.
	search rear flaggy - fr-said - servicer almant flag area and fragmentally			search - to flowry - fr and - astrony things of the first and the first
10.010			111	file and the second sec
	The second secon			The line Lines 1.7.9 halt1-sailt0
	Lines (hort/weigers.U.T hall) model soor "http:// hold the star with most thinks a		1.00	lines /hort/willing-L.7.5 tell] many conversion and the the more confirmed at
10.00	with "headley tailing random"		1	sub- "Institut Institut and a"
	inited (hust/laited.isg-5.7.3-6alii-and04			istrid /biot/Ustrid.isg-5.7.9-Kalii-ast##
14	URLIN TROUTELLING, INC. 1 POLL - BOOM	1157		Intth Providential and State and Annual Contraction
-	managetry 'Ball MWVM prov. with three T.J. Phall? three ball three and-three	11.12		secontry fair setflings, with lines 5.5.5 Mail2-and/4" flass ball flass get flass
1 N -	Just stides			Load wides
	dataset gate			London grain
44.1	if I afgrid platform " man ); then could anit; count logics for	11/11		if I should produce a news [] then presed mater presed harping \$2
	ineed pert_neine			remod betramente
	lamod est2	11144		Linkod esti
	and stores' full constant !			ant mode with made 1
18.7.7	18 I althouse platform reach hims to ap 1; then	11104		10 7 alfeature plantness search him t ap 11 thes
19.19	stand - to the the said - for both - both - both both - both - to the share - the share - to the said	1111		search - as flaggy - frontid - sectance - hist-base base and - hist with the second
28.11	8248	11.110		*Les
	search		- 48	search
20	<b>4</b>	11114		£4
	artin 'Ensking Linow 5.5.3 'Asil: and 4.			ents (bosting hirow 5.5.8 Amil: webs
	lines (hoch/mbloarth.d. intell? and/i probabilities intell the line and from the line in the second se	11:44	100	Linux /Sect/milliour-1.5.1-sall?-asett providing assett all 125 mar anti- and all
	who "loading tabled reader"	11114		entro "Londrog minist restart"
	initial (host/initid.ing-1.1.) holl:-entry			inited /heat/inited.imp-1.5.0-Mail2-mail8
	A State of the second se			
	manuatty "mill pervalage, with those \$ 7.0 Kalls same licentroly mont" sizes hall sizes		- 18	secondary "hall swithings, with himse 5.5.5 kalls would proceery note!" - class sail - cla
	Jind tides			boat video
14.	tenned sale and the second sec	I have		Landor china and a second se
	18 T algorit platform 4 more for three lossed makes instead lengths Fi	11144		18 [ afterna plathtern - news [] they issued anis; issued impire fi-
	itemed party spatia	1114		inemid part metric
	inentia webb			Longer average
	set roors'bdi.metasi'			est costs'hui, Apdoel'
	10 ( affeature glattern search hirt + as is then	1122		if I softwaters platform search hint = et 11 then
	shards rear Daugy - Drast - savenus - stor biashd, and at - ther af rid, and at -		- 10	search - and have a farmal - searchest - him have been at - him of that, and at
1000			100	the second
	Annual rear Diverse with mail water and the state and the state and the state		-	search - and flyggy - fa-maid - ant "poor, ministin-state-stree-time-mails the far
100	G G			And a state of the
10 C C C C	ache "Scalling Linux 515.0+Balld-and64"			etter 'hosting kloss 5.5.0-64112-ant/4'
	Time /hoot/militar-5.5.3-ball2-mail4 meressoning hearth that and from itemations a		1.00	lines (book/miliner-5-5-5-teall) and a correl/(interact) will the fine mile had bat
	arts "Loading tottial randing"			
	inited (headlanised.ing-1.1.1-he112-paid)			hakted /hours/Austend.dmg=0.8.0.0000242-mm488
		11494		512 <b>%</b>

Figure 6 /boot/grub/grub.cfg Differences

Because the UUID of each file system is by definition, unique, it is tied to a specific system. Additionally, because this UUID is tied directly to the UUID of the boot partition, it is found through the disk and in various logs and cannot easily be changed.

### /etc

#### adjtime

The file /etc/adjtime tracks the amount of drift between the hardware clock of the system and the actual time. In theory, the hardware clock gains/loses the same amount of time each day. By recording the amount of draft that occurs each day, and then determining how many days have passed since that time was recorded, the system can figure out the approximate true system time.

The file consists of 3 lines (see Figure 7). The 1<sup>st</sup> line has three space-separated fields. The first field is the drift rate or the amount of drift the clock has each day. The second field contains the epoch time of the last adjustment. The final field is the last adjustment status which is always set to 0 now for backward compatibility. The 2<sup>nd</sup> line is the epoch time of the last calibration and should generally be the same as field two on the 1<sup>st</sup> line. The 3<sup>rd</sup> line is set to the time zone.

On a physical server, the amount of drift between two systems has a high likelihood of being unique, however, there is a good chance that multiple virtual machines on the same physical server will hold the same drift rate. Even though the drift rate may be the same across virtual machines though, it is highly unlikely that the time of the last adjustment will be the same, even across virtual machines<sup>12</sup>.

<sup>&</sup>lt;sup>12</sup> https://man7.org/linux/man-pages/man5/adjtime.5.html

adjtime	_8171 🖸	▲ 🔚 adjtime_7135 🔀	
1	0.000000 1595427902 0.000000	1 =0.000000 1595425706 0.000000	
2	<b>1</b> 595427902	2 📲 1595425706	
3	UTC	3 UTC	
4		4	

Figure 7 /etc/adjtime differences

While there is a high likelihood that epoch time of the last time adjustment makes /etc/adjtime unique to a particular system, the fact that this file is simple flat text and a change to any of the fields within the file will likely result in no impact to the system's operation. This means that this file is a poor indicator of system uniqueness.

#### cacerts

The file /etc/ssl/certs/java/cacerts contains all of the certificate authorities that java trusts by default on the system. This file is separate from what the system's web browser uses. An examination of the file shows that each system's copy is 150,007 bytes in length and that while there are large sections of the file that are almost identical, there are also portions with significant differences.

1-2-61	and discounter the second little bairs to a second met. (ST(ST))	1 E-Kal Transmitt of Automy Kall/1-1986 and Autom 1 Hills, Report 24-28-2021-08-39 (Incontent Rooksmall Cares
	Do HA NO DA OF DE UN OF DA CH OF DO OF DF Decoded test	and the second
		Offessin) 00 01 02 03 04 05 04 07 05 05 08 08 00 00 05 07 Devodes text
	FE ED FE EN DO DO DO DO DO DO DO TE DO DE DO DE PAPE	0000000 FE ED FE ED 00 00 00 00 00 00 00 00 11 00 00 Diplatetetetetetetetetetetetetetetetetetete
	to 14 44 41 42 44 41 42 3A 47 74 73 5F 72 4F 4Fdebianigte_roe	00000010 00 18 68 65 62 65 81 62 38 67 78 73 58 77 68 67debianigts_cos
	74 NF 72 32 28 70 48 40 00 00 01 73 76 83 82 30 5_82.pemsvem1	00000020 74 19 72 10 28 70 45 40 00 01 01 13 74 C0 55 CT 5_#2.pemev2.C
	00 00 38 00 38 00 39 00 00 00 88 80 82 09 5A 30 +.X.909"0E0	01.00.000.00 10 10 10 10 00 10 00 10 00 10 00 10 00 0
	82 01/42 00 03 00 01 07 02 10 ME 07 NP 07 5A 00	00000040 82 03 42 A0 63 03 03 03 03 10 68 47 A8 C6 84 83
	ET 20 CD 30 9A 3F 40 H2 F2 HF 30 0D 04 H9 ZA 04 q A08358600+9	010000060 RT 20 CS 10 SA 17 48 51 F2 47 80 10 04 00 24 54 9 A08758Co0**
	48 A4 #7 00 01 01 00 00 00 00 47 11 08 00 08 00 8*+001.0.	000000000 48 58 57 50 01 01 00 00 00 30 47 31 88 30 05 00 H#++++++++++++++++++++++++++++++++++
	00 00 00 00 10 10 10 10 01 01 01 00 10 00 10 55 00 .0	00000070 03 55 04 06 13 02 55 53 31 23 30 20 96 03 58 08 ,0001*00.
	0A 03 19 67 67 67 67 67 66 20 64 72 76 78 78 20doogle Truss	00000000 0A 13 19 47 6F 6F 67 6C 65 20 54 72 75 71 74 19 Stogle Trust
	53 65 72 78 69 63 65 79 20 80 40 43 31 14 55 13 Dervices LULLO,	000006660 53 65 72 76 68 63 68 73 20 %C 43 31 14 30 13 Services ILCL.G.
	08 03 35 04 03 13 08 47 54 13 20 12 67 67 74 20UWIS Boos	00000080 06 03 85 04 03 13 08 47 84 53 20 13 48 HT 74 10
	12 10 30 1F 17 10 31 16 30 36 32 10 30 30 10 R201604230000	00001050 H2 H2 30 JE 17 10 51 10 50 10 82 10 30 30 50 51 H201404220000
	BO NO BA 17 OD NE 36 NO P6 NE 32 NE 30 NE 30 D02., 94042200000	00000000 NO 30 5A 17 0D 33 24 10 36 81 52 10 30 30 50 50 007, 36083200000
	00 NA 30 TT \$1.10 30 00 06 01 88 01 06 13 02 00 10 02.0	UC000000 30 18 30 47 31 08 30 40 08 00 18 28 04 18 18 08 18 08 18 07 10 0.00000
	53 11 22 00 20 10 00 15 04 00 13 13 47 87 87 87 51 51 10	00000088 88 31 32 88 00 04 03 51 04 88 13 13 47 67 67 61 8140
	6C 01 20 14 72 73 73 74 20 13 42 73 76 00 63 05 In Trush Service	000000F0 60 63 20 54 73 75 73 74 20 53 65 75 76 64 63 65 18 Trust Service
	73 30 40 40 43 31 14 30 13 04 03 35 04 03 13 08 # LLCL.0U	00000100 78 20 40 40 40 11 14 10 12 04 08 08 08 01 18 08 # 1201.00
	47 14 53 20 52 6F 4F 14 20 12 52 10 52 10 GTS Boot R20,."6	00000110 47 54 53 20 52 47 62 74 20 02 32 50 82 01 22 30 923 Bove 820, *0
	00 06 09 05 86 49 56 FT 00 01 01 03 03 09 08 40*TRT*	**************************************
	DE 07 00 00 82 00 0A 03 62 00 01 00 CE DE 50 A0	00000110 02 OF 00 10 02 01 03 01 03 01 02 01 01 00 CE DE FD AN
	F5 30 E0 14 34 30 47 10 55 40 59 27 15 31 00 77 611.442124.524	00000140 FR 80 80 14 34 10 07 01 88 10 58 17 18 10 80 17 011.4c.,212+,12+
	CI NO 33 AA D3 CD 38 A4 93 CI EF CH FA CO 90 FN A.D*03/A*si.un.8	DODDALMO CA NO MA AN DA CO MB AN MA TA MF IN MA NO MO FA A.UMOE/HTML.ON.D
	PO DE DE DE AL DE 12 DE DE CE DE LE 20 AC EP CE ALCINEYPA 11-1E	DODDELED . BD 00 00 00 AT 01 02 07 09 00 07 07 28 MC EF CH A.R.L.MAYSA-10-LE
	76 00 16 00 DF 20 01 00 00 00 00 C4 00 1D 07 FE 10 V5.V81*.1*.1*.1*	0000110 TE 48 14 10 DF ND 01 40 30 17 CE 11 10 88 FE 11 VE."3. 14. A. 304
	TT DO 20 NO AF DI 04 NO 4F TI AO 10 04 NO 80 NO WALL AL 04 10 TA	00000100 TT BU 20 10 AF DI 04 DF 4F 75 A0 1A 34 90 BE 39 H8, ["A:10: .4"49
	68.00 98.15 TE 79 AL 16 69.15 09 13 8D 19 60 11 8L+814(#1*1980)	00000100 68 HC 85 20 70 70 AL 21 40 00 00 10 00 10 10 AL+4(V;#L+)MBD
	AD ED 36 EA 73 SC FF 53 E2 CS 7D C1 D2 CE 4A E3 .168494974E3A0E3*	DODODIAS AD ED D4 EA 78 ht PF to E2 th 70 ti 00 th 44 ht .144444014013*
	5D H5 9E H5 49 50 20 21 55 10 4E 18 90 18 30 18	00000180 8D 00 98 00 40 01 DF 01 38 00 48 15 F0 20 30 10 1.841"64081"640.
	82 SC FA BC B4 17 GA 48 EE 55 MB CE MB 48 DE 50 .004 RA' (&) AD"	00000100 BZ PU FA BU BA 17 GA 48 25 00 98 US 98 00 DE DU JONA', HA'SANAS
	CA 24 03 70 DA 71 96 01 46 44 87 30 40 50 E8 10 E 1,403.,ed=\L.e-	00000100 CA 54 03 FO DA F4 90 80 45 68 F7 50 40 80 E8 10 E 40, ed+12.4-
	AN 12 39 17 81 11 32 11 00 11 30 AD 25 11 48 11 21 49 AD2	000001E0 44 18 99 D7 B5 13 16 C1 D0 13 60 AD EE 0+ 45 78 2**** A-501881
	10 10 27 18 18 42 12 14 12 11 12 10 07 21 18 17 Mid.38., Mid.85.	HOODDIFD OF SE FT SE IF ST 42 14 12 83 CD 45 FT 53 AA 37 10-0.08., 148-83.
	47 01 AN 74 5A 11 FU 01 63 20 10 10 83 10 81 10 G7(120482()	HODDDDD 41 H1 A4 74 84 H1 F8 81 48 18 48 18 18 88 88 88 81 81(220840(+.*.V
	TT WE AR DE WE TO DE TH DF DE BE DE RE HE TE DA MERETARDALSA .O	00000210 TT 41 A2 16 95 TF C4 FE 28 29 EE 16 AV TF D4 H8+6'V40441-6 .0
	41 OF 61 40 DC 3F 8C DA K1 TO T4 DE C2 40 A1 F0 A.QK/100AptdAnja	00000220 41 UF 51 48 30 UF 80 UF 81 70 74 00 CE 49 A1 F8 #.0847004g-00Apin
	C1 10 E9 61 E2 17 88 15 80 14 04 EE 4A 48 00 50 A.4.8.40(V.1382*	00000000 CL OC ES AL ES TE ME 15 DC 74 DE EE 46 45 CC 50 A.4.4.4Uvr.1502*
	65 10 8D 3A 8D 47 08 19 9A 11 83 10 A3 D1 F8 T3 "OHMO.HA.p"601a	DODDDD40 08 10 4D 55 BD SY 08 50 9A 15 B1 00 A3 D1 FB 71 "OK840.H#.H"&OG#
	C1 17 61 00 26 50 75 13 AZ 17 52 27 00 51 08 10 AMAS(Va.#+Zc.Q	000000260 C1 ST 61 00 29 54 75 10 AE 01 88 87 00 51 09 10 ARAY(Ve.##20.0.
	75 00 40 00 00 79 78 30 D4 13 48 17 24 10 38 40 u'D4.0(ob48.+Ceb	00000280 78 88 40 80 80 F5 78 30 D4 22 48 37 28 30 E8 88 8"14.014078.+Dex
	BR ++ BL 13 33 11 32 ++ AF AD 4A FL 80 21 74 4A #DeE3q2F",20041)	00000270 85 () \$1 () 33 71 53 () AF 10 4A F1 80 E1 74 14 +DaE3q2?". (\$284:)
	AC 37 1A 12 79 10 33 10 FT 15 42 CT 33 10 39 13	00000200 AC ET IA 13 73 80 52 30 F7 11 42 C7 22 38 55 11 -47."ACO+45C";;.
	AD 10 22 CE C3 10 07 AL 20 11 35 10 87 23 52 10 ADA.* SIMA'S	00000200 AD 06 28 26 C3 76 27 AD 20 27 35 48 27 28 82 48 850.* 5280'2
	E5 10 14 12 31 CT 28 16 TE 18 A3 CT 54 10 22 37 87.210+0107744	0000000AN EN 16 16 10 04 07 08 06 7E 05 AV 07 66 55 23 NF 67.21g+SAC"V*2
	6A 10 7E 11 21 21 23 12 DP 01 3A 41 4D 11 5E 10 2E-1142344Dex[]	00000289 48 49 78 01 21 01 23 11 DF 04 88 41 40 00 18 00 18-1*#284ADMY[]
	PE 14 AD 10 MB CG TE 67 0D 14 FF 48 CE AA B4 AF A	DODDEDCH FE DO AD LC BB CO TH DT BD DI FF DE CE AA 54 AF 8 Ext
	11 51 39 18 D# FE 47 30 D# 68 11 50 42 51 18 80	00000200 11 11 11 10 00 FE DO FE W7 AD DO HE 11 10 32 94 18 50 .00'00g.0(2#.W
	DB HA BE AN CH CH OB AN 65 NH 27 NC ED CA SA CH O"INCEALSU"\ASHE	SCODEZED DS DA NA AN CO CH 25 WE SA NY 27 NC ED CA DE CH B'IWEERLOU'VARKE
	00 01 28 18 87 DO CO EE 16 70 D3 AN 90 DE 92 AD 740. 001.00:50'9	COODERFO DE 41 FE NT DE CE DE 14 FE DE AF 40 DE 42 AN "AG. DEL.GO:LP'N
	D4 ET DF 35 06 54 DE LE SD 45 D4 95 30 AA SL CE 0405.TPE "0*.I	00000300 D4 E2 DF F1 06 14 DE 25 9D 48 84 43 30 33 61 CE GE85.TDE.*04.E
	DD 1A DC 31 78 CD 4F 70 EF 81 B4 16 21 19 79 81 9.0Qs.cpe4g.1.y*	00000010 DD 1X DC 01 79 00 4F 70 E9 E9 DF 10 31 19 79 50 2.028.00685.1.94
	Ke op de 75 ee de DS AR BC op di 10 Al PY De 14 secudêdeech.A.:1907	00000020 IN NO OB TH ON TH ON AN BC NO CI IN AL IT DO NO WELLDEDWALK. 1907
1000 000 0000	AL 00 90 70 14 20 00 00 07 10 A4 00 02 00 02 00 1.49.4 400	000001330 A2 00 30 00 14 04 03 00 07 00 A4 07 02 00 01 00 1.49.0.******

Figure 8 File Comparission of /etc/ssl/certs/java/cacerts

I believe that the reason why each of these is different is that each system has several self-signed certificates that are created as part of the system install. I believe that one or more of these certificates is included within this file which causes each one to be unique.

While this file appears to be unique to a single system, it is easy enough to change this simply by creating a new certificate and then updating the file with the update-ca-trust command<sup>13</sup>. This means that this file is likely a poor indicator of system uniqueness.

#### fstab

/etc/fstab contains all of the information that the operating system needs to identify the various drive partitions and other information within the file system and mount them. Each line contains multiple fields that identify file systems connected to the system and how they are configured. The first field on each line describes the individual block device. The preferred method to identify these devices is through its UUID, which is how Kali does it by default<sup>14</sup>. There will always be at least one device listed here (the / partition) and in our tests, there was another listed (/dev/sr0) which is the CD-ROM that was used to install the system (see Figure 9). Because the UUID included within the file is by definition, supposed to be unique, this file is tied to a particular system.



#### Figure 9 /etc/fstab differences

Also within /etc/fstab is a reference to the boot partition (in some cases, this could be / partition noted above). Regardless of what the boot partition is, this same partition UUID is also referenced in /boot/grub as noted above.

Because of the multiple UUIDs within the file, /etc/fstab is unique to the system. Because these UUIDs are tied to the file system partitions they are not very easy to change. Additionally, these UUIDs appear in /boot/grub and multiple logs making this file a very good unique system indicator.

#### machine-id

Located at both /etc/machine-id and /var/lib/dbus/machine-id is a file that simply contains a 32character (128-bit) hexadecimal number that uniquely identifies this particular installation of the operating system (see Figure 10)<sup>15</sup>. This number is unique to this individual installation and does not change if the install is moved to a new physical device or if the IP address or hostname is changed<sup>16</sup>.

<sup>&</sup>lt;sup>13</sup> https://www.systutorials.com/docs/linux/man/8-update-ca-trust/

<sup>&</sup>lt;sup>14</sup> https://man7.org/linux/man-pages/man5/fstab.5.html

<sup>&</sup>lt;sup>15</sup> It is important to note that while this number is not a true UUID (by the definition) it serves the same role and is considered to be equivalent to a UUID.

<sup>&</sup>lt;sup>16</sup> https://wiki.debian.org/Machineld

⊨ machine-id_2986 🗵	machine-id_3003 🔀
1 = 772b8bc325774cf29258e487592d8a5e	1 🖶 6419ad21b7384371a12b5877060147c5
2	2

Figure 10 /etc/machine-id Comparison

The ID is randomly generated at the time of the OS installation and does not tie directly to any particular information that may be of use, although a variety of other items within the operating system make use of it to uniquely identify the system. The machine-id can be regenerated by using the following commands<sup>17</sup>:

rm -f /etc/ı	machine-id /var/lib/dbus/machine-id
dbus-uuidg	genensure=/etc/machine-id
dbus-uuidg	gen –ensure
reboot	

It is unclear what the effects are if the system-id is changed given that several files are named based on its value (see the description of LightDM above). Also, it is important to note that this file exists in both /etc/ and /var/lib/dbus/. These are separate physical files that contain the exact same content (exact hash match) but they are not a link. Because the contents of the file by definition uniquely identifies this system, the file itself can uniquely identify the system. What is currently unclear to me though is how hard it is to change the contents of the file (along with the names of the LightDM files) and what effect it would have on the system.

#### resume

/etc/initramfs-tools/conf.d/resume is a 1 line file that contains the UUID for the memory image that was made when the system was placed in hibernate (see Figure 11)<sup>18</sup>. This image is saved within the swap file and has a UUID just like the file systems referenced by grub.cnf



Figure 11 /etc/initramfs-tools/conf.d/resume Differences

Because the UUID of each file system is by definition, unique, and it's included within the resume file, then this file is tied to a particular system. Unless the resume feature is used though, it is possible to remove this file along with the partition and not affect the functionality of the system.

#### server\_config.yml

The file /etc/king-phisher/server\_config.yml is part of the configuration for the King Phisher tool that is installed by Kali. What is interesting, is that out of all of the tools installed on Kali by default, this is the

<sup>&</sup>lt;sup>17</sup> https://dbus.freedesktop.org/doc/dbus-uuidgen.1.html

<sup>&</sup>lt;sup>18</sup> https://askubuntu.com/questions/292878/how-to-set-swap-in-etc-initramfs-tools-conf-d-resume-if-i-have-two-swap-partito

only file that I can find that is unique for them. King Phisher is a tool "for testing and promoting user awareness by simulating real-world phishing attacks.<sup>19</sup>"

The software makes use of the PostgresSQL database server to store the various pieces of data required for each phishing campaign. On line 67 of server\_config.yml is the username and password that King Phisher uses to access the database. The username is always "king\_phisher", but the password is 16 characters randomly generated as part of the install script (see Figure 12).



Figure 12 /etc/king-phisher/server\_config.yml Comparison

While the password generated by the install is not truly unique to the system, the fact that has 62^16 combinations makes it highly unlikely that the password will be repeated on a random machine. That being said, because this is a simple password to a database, it is very easy for a user to change making this a poor indicator of system uniqueness.

#### shadow

The encrypted passwords for all local accounts are stored in the /etc/shadow file (a backup copy of the last file is also stored in /etc/shadow-). The file consists of a line for each account (53 by default). The file is the same until you get to the user-created accounts (see Figure 13).

<sup>&</sup>lt;sup>19</sup> https://github.com/rsmusllp/king-phisher

-	_nua	Heate	_789 G
11	2005111284651519999917111	1	2005111284851819999917111
12	daemon:*:10465:0:0009017::::	121	daemon:*:120465:0:9999:7::::
	bin:*:10445:0:99999:71:1	1.11	bin:**118465:0:99999:7::::
14	#2#1*11046510:000000:7:::	1.4.	#y#1*110465:0:99999:T:::
1	aync:*(18465:0)9999917117	1.1	#y801*11846510(999991711)
	games:*:10485:0:00999:7:::	6	games:*:125465:0:99999:7::::
-	man.1*1104651019999917111	1 1	mm1/*119665:0(999991711)
	1p:*:1845:0:99999:7:::	1.1	1g:*:10465:0:99999:7:::
	mell:*/19465:0/99999/7///	1.11	mail:*:19465:0:99999:7:1:
22	mews:111445501999997111	36	news:1:10465:0:99999:7::::
	384001*11846510199999(711)	111	gucp1+110466:01959595:7/11
52	nerwy:*110445-0199999:71:1	12	promy/*:18465:0:99999:7:::
100	www-date:*118465:0:39999:7111	1.11	www-detel*118665:01999999:7111
3.8	heckup:*:10445:0:98999:Tii:	1.24	backup:*:10465:0:99999:7:::
	11#1: 128465:199999:7111	1.55	11411*110465:0199999:7111
24	10017119485.0199999.7111	380	Ltc: *:19465:0:99999:7:::
11	gnats:*118465:0:99999:7:::	24	cmate:*:10465:0:99999:7:::
28	mcbcdy14118465:0:99999:7::::	38	ncbody1+115465:0:999917111
19	apt:*:10465:0:90999:7:1:	1.16	apt:*:18468:0:99999:7:::
	#ystend-timesync:":10463:0:99998:7:1:	2.0	#1#temd-timesync:*:10463:0:99999:7:::
23	svstemd-tetwork:*i18465:0:99999:7:::	21	systemd-network: *:18465:0:89999:7:::
22	#1#temd-remolver*:10465:0:99999:Til:	22	systemd-resolve:*:10445:D:39999:T:::
22	mrsgl::110665:0:99990:7:::	21	mymgl:/:15465:0:99595:7:::
54	t##1*110445:0:99999:7::::	24	1999111194651019999917111
25	stringsvan:*:10468:0:\$9999:7:::	51	etringswan:*110465:0:99999:Trr:
24	ntp1+1194681019999917111	50	htp://119465:0/99999/7///
53	mrssacsbus:*/1046510:99999:71::	21	messacabus:*11845:0:99995:7:::
21	redsockwi1111465:0:599998:7111	28	zedaocks1/118465:019999977111
22	rwhod:*:18465:0:99999:7:::	1.24	rwhod:*110465:0:99999:7:::
11	10d1ze1*(10463:0:99997711)	21	lodine:+:15465:0:99999:7:11
	minedo:*:10465:0:09090:7:::	1.52	miredo:*:10465:0:99999:7:::
22 ·	dramasci*(10465:0199995:1711)	32	dnsmasgr*118468:0(99999;71))
11	usbmus:*:10465:0:99999:7:::	1.22	unbmum:/120405:0199999:Tott
26	tcpdump1*11046510199999917111	36	topdamp(*)10465(0(99999)7)))
35	ccpoung) *** 12446:0:99999:7:::	35	rtkit:*:10445:0:99999:7:::
52	rpcr*(10465:0/99999:7)))	36	
37	Debian-wnmp:/:114465:0:99999:Trrs	31	zpo:*118465:0:99999:7:1: Debian-snap:1:18465:0:99999:7:1:
22	stat0(*)18665(0)99999(7))) postgress:*119663(0)99999(7));	71	statd:*(18465:0:99999)7::) postores:*:18465:0:99999:7:::
÷.	ptstcpres: 1104651019999997111	1.6	
			atume14:1:19465:0:99999:7:::
45	##bd:*:13463:0:09999:7:::	1.0	##bd:*:10445:0:99999:7:::
18	sslh://18465:0/99999(7):)	12	##1h:1:10665:0:55959:7:::
63	amabi::*:10465:0:99999:7:::		ersb1:*:15465:0:99999:7:::
11	ла-срепирал 10468:0:99999:7:::	1.00	zm-opezvph:*:18465:0:99995:T:::
12	nm-openconnect:*118448:0:99999:7::::	15	na-openconnect:*:18463:0:39899:7:::
44	pulae:*:18465:0:99999:T)::	146.1	pulme:*:10465:0:90999:7:::
47	seped:*110465:0:99999:7:::	.97	##Ded:*:12460:0:99999:7:::
12	inetalm:*:10465:0:99999:7:11	142	instaim:*110465:0:00095:7:::
22	dologd:*/18445:0:99999:7:::	22	0010001*11046510:99999:7111
55	geoclue:*:18465:0:99999:Ti::	20	geoclue:*:10465:0:99999:7:::
53	lightdm:*:18443:0:99999:7:::	31	lightdm:*:10468:0:99999:7:::
82.	Ring-phisher:"110965:0:99990:7:::	-82	king-phisher:*:18665:0:09990:7::::
	Exception of the second s second second s		<pre>ptpoptAtjEx1pMx51/mpRMx7Daif10F18H5Ty070fbo82m181013</pre>
34	systemd-coredump:1*:19465::::::	2.6	wysteed-dozedump:(*:10065::::::
10	Carl Contraction Contraction Contraction	1.00	

Figure 13 /etc/shadow differences

For the case of this project, I used the username "troy" and the password "password". This created the below entry for the account in the shadow file.

troy<mark>:</mark>\$6\$jEx3yWwLY/xpRWuU\$nifiGKlhGL7yOUOfbo8ZmiNi013g18EeweqIE3M8pSVgdVcfsRLko.vDPspup 5agio4A2NHHUz9Hvg84YUD2p.<mark>:</mark>18465<mark>:0:</mark>99999:7<mark>:::</mark>

The line is a colon (:) separated string that contains several fields<sup>20</sup>.

- The 1<sup>st</sup> field is the username for the account (in this case "troy")
- The 2<sup>nd</sup> field contains the hashed password. We'll look at this one closer in a minute.
- The 3<sup>rd</sup> field indicates the number of days that have passed between Jan 1, 1970, and the last time the password was changed. In this case, the value is 18465 which means the password was set on July 22, 2020. This field is not particularly unique given the fact that all of the systems that are created on a single day (or have a password changed on that day) will all share the same value.

<sup>&</sup>lt;sup>20</sup> https://linux.die.net/man/5/shadow

- The 4<sup>th</sup> field is the minimum number of days that must pass between password changes. Here it is 0 which is the default.
- The 5<sup>th</sup> field is the max number of days that can pass before the user must change their password. Here the value is 99999 which is the default.
- The 6<sup>th</sup> field indicates the number of days before the max password age that it will warn the user to change their password.
- The 7<sup>th</sup> and 8<sup>th</sup> fields are not set by default.

Within the password field noted above is a sub dollar sign (\$) separated string<sup>21</sup>.

\$6\$jEx3yWwLY/xpRWuU\$nifiGKlhGL7yOUOfbo8ZmiNi013g18EeweqIE3M8pSVgdVcfsRLko.vDPspup5agi o4A2NHHUz9Hvg84YUD2p.

- The 1<sup>st</sup> field with a value of 6 indicates the hash that was used. A value of 6 indicates SHA512 which is the current default for Kali.
- The 2<sup>nd</sup> field indicates the salt that was used with the password. A salt is an extra piece of data (in this case randomly generated) that is appended to the password to prevent the use of rainbow tables when it comes to cracking an encrypted password. In this case, the salt value is "jEx3yWwLY/xpRWuU"
- The 3<sup>rd</sup> field is the SHA512 hashed combination of the salt and the password

The fact that the salt is 16 characters long with 64 possible choices for each character gives it  $7.9 \times 10^{28}$  combinations. This combined with the fact that virtually the only way to get the same password hash is to have the same salt and password makes it exceedingly likely that if this line matches on two systems, they have a common past.

Fortunately, the regeneration of a password will cause a new salt and in turn a new hash to be generated (even if the same password is used) and will also reset the password change date field to the current date. That makes this file a poor indicator of system uniqueness.

#### ssh\_host\_\*\_key

Within /etc/ssh/ are three pairs of private/public ssh keys that are used by the sshd process. The keys are:

- ssh\_host\_ecdsa\_key / ssh\_host\_ecdsa\_key.pub
- ssh\_host\_ed25519\_key / ssh\_host\_ed25519\_key.pub
- ssh\_host\_rsa\_key / ssh\_host\_rsa\_key.pub

The three keys are referenced in /etc/ssh/sshd\_config and are used to authenticate the ssh server itself to clients. These are the keys (the public keys) that are stored in the known\_hosts files of clients. These keys are transmitted across the internet.

Because these are ssh keys, they are unique to the system, but they can be easily regenerated by using the following commands<sup>22</sup>:

<sup>&</sup>lt;sup>21</sup> https://linux.die.net/man/3/crypt

<sup>&</sup>lt;sup>22</sup> https://www.cyberciti.biz/faq/howto-regenerate-openssh-host-keys/

rm -f /etc/ssh\_host\_\*
dpkg-reconfigure openssh-serve
systemctl restart ssh

#### ssl\_cert\_snakeoil

When a web server starts to run HTTPS, there has to be a certificate there to support it. Generally, the preferred method is to get a signed certificate from a recognized certificate authority so that a web browser will accept it without a problem. When that doesn't happen though, a self-signed certificate can be used.

/etc/ssl/certs/ssl-cert-snakeoil.pem and /etc/ssl/private/ssl-cert-snakeoil.key is a self-signed certificate pair that is generated at the time of installation<sup>23</sup>. This certificate is used for SSL web sessions if another certificate hasn't been explicitly designated.

hvojn@tocalhost - (Desitsion/Reports/Harly2-FH-94), Report DF-28-2020-06-30-21/santeest/Bawkreani	Physical Society (Sector) (Sec
troyBlocalhowi Bookmark)# openesi wi05 -text -mout -in esi-pert-enskenil_5883.p	th (troy@localbost Bookmark]5 openaal x000 -text -noost -is asi-cert-adakeoil
	(certificate)
Deter	Dattar
Vernioni 3 4002)	Version: 2 (0x2)
Serial Number:	Berlal Mumbers
lprediblyddrogi0g:70:52:17;61:4Free:dcrec:fl:g2:86:g7;2d:um	23:32:40:04:64:64:04:47:98:21:67:24:04:4a:68:68:68:68:68:68:68:68:68:68:68:68:68:
Signature Algorithm: shall-fwithSSAEnoryptics	Signature Algorithm: shall With SAIncryption.
Insur: CD-Mail	Issuer: CP-Wall
Validity	Validity
Not Before: 243 22 13:42:47 2030 GMT	Not Before: Jul 22 14:20:05 2020 GMT
Not After : Jul 20 13:82:47 2030 [MT	Not After : Jul 30 14:20:05 2030 GMT
5/10/Sect1 (3P+kw11)	Subject: CH+kali
Subject Public Key Infol	Subject Public Key Info:
Public Rey Algorithm: reaEncryption-	Fublic Ney Algorithms rasEncryption
EwD11d-Ney( (2048.011)	Public-Enyr (2048 bit)
Hpdmlmm:	Boduliser
0010210030124413415415112(40)00102122(40)001	00:00:ma:0f:00:17:6d:5a:50:70:Ra:15:2b:d7:51:
	Hatd015er0drim:7fied;bl:uTre2:bb:63:30(ab:ff)
d0:T1:36:4c:16:2c:f0:5b:25:c0:31:b3:aT:cf:cd;	30148(09)h3(bf)6f)fe(b6(f)8b)49(09)70(71)42)
4(c) #1 (db) 121 (721 (7c) (c4) #6 (dd) 27 (60) (54) (65 (c2) #5)	c3:12:43:64:30:09:3e:3e:04:63:69:c9:16:f0:29:
bciect3a11a19550a;c616117d1691ca13710510917f1	UE108:78:30:41:98:3E:07:28:00:9E(Dd)42:15:62)
144:#3:20;2#:0e:#3:00:#e:#3:00:fo:c0:#0:00:#7:30:cod:e3:5e:	49:00136(#1:4a/501a5136;50:6e(00/30)64(44/21)
49148/38/00Tc07/29/38/00L90/08/09/68/68/66/06/00/28/	TT:\$1:bb:Ue:85:\$1:93:74:c8:Hareerod:17:#T:ee:
66:2a:29:0c:e2:c0:bd:31:2c:7b:nd:cf:47:d4:90:	faib7iafi70;61;60;81;55;77;c6;01;de;b3;00;f0;
	bw:57:11:0a:Yf:55:06:c9:38:79:73:00:1b:Do:4a:
2. 教授主要的主要的文明委员名常见教育学校主要的主要的工具的工作的工作的工作的工作的主义	Be:ec:55:9d:63:10:0d:f1:20:57:1d:fc:93:77:80:
.ad:04:09:00:00:00:00:00:00:00:00:00:00:00:00:	49/c4/e0/65/76/09/e6/99/d6/80/90/37/d6/c0/
41110年19412110日10年10年10日10日10日10日110日10日10日10日10日1	mid:c5:6D:GardfreD:b7:1f:6D:Se:41:7d:60ffe:20:
b01000100128+100100510017016217016217010010010101000	25:72;bo;b5;85;df;b5;c4;e5;45;f5;10;0;03;d0;
be:30:90:TE:Oc:Te:eT:DE:cl:PO:20:3d:ac:eG:Ge:	6d:d0:10:00:30:7a:37:7d:6b:05:e0:0d:Na:e7:30:
d9106(79)00(99)11(00(90)96(60)00(90)10(100)	mSchar63ra5te0:d2:4arfdrcfrb4ra3t57r09:3Erdat
£7:cc:11110:46:24:3d:a1:63:60:aa:3d:01:7e:6e:	ee1711%e1803883f21091361281371271403001e21471
2012e:1912a:32:45:09:57:66:da:30:00:40:00:00:	7f:53:8e:40:29:25:86:40:190:109:78:54:40:190:0f;
Exponent: 65537 (0x100D1)	Exponent: 67637 (0x10001)
3309v3 mstemsions)	X509v3 extensions:
X10993 Basic Constraints:	MS09v3 Basic Constraints:
CA: TALSE	CAIFALSE
350997 Subject Alternative Same:	X109v3 Subject Alternative Heme:
DHE: kali	1001 ( in 11,
Signature Algorithm: sheINEWithRSAEmeryptics	Signature Algorithmi shalisWithRAAEscryption
4#+6D()00167:00(#1:07/01:00:00(90:00)(0:00)(0:00)	Te:#BisT:D::D::D::20:00:70:70:00:00:27:00:00:27:00:00:27:00:
7#12d:fc:0f:011#2:15:77:40:#7:b0:27:ff:a2:00:0#:0f:df:	351e4(00)97(c5:06(4+1e6)50(ee)0e(0)39(50(35:04)129)8E(
71:f4:d6:B1:70:ae:53:2e:16:f9:ff:8e:mar10:b5:ec:fe:f1:	Ex:03:01:E4:04:73:x7:c2:xc:77:00:32:x0:03:38:05:3x:50:
derükräcr?fre?:b0rdar6c136:121ef173:59:bei44:bb103:0ei	\$x:2f:a0;f0:x7:b0:67:b0:62:10:ga:70:f8:(4x:95:d6:26:94:10:5x)
7min8:73:20:2a:80:24:00:a4:20:64:b0:d4:34:60:60:24:9a: 39:28:ea:32:49:34:52:40:04:32:22:b0:5e:30:07:00:4a:ec:	06/08/ad:9d:20/00/4fr30/For07/18/27/00/eTr85/14/4#134)
#0166:9b13e;35:b0:f5:13:b0:f3:47:90:15:f2:b6:7b:f4:66:	f4:dd:34:db:45:95:30:00:ee:99:7b:b9:81:c5:00:74:5c:3a:
08:cl:wf:c5:40:l1:61:ef:b4:6c:7b:21:65:55:d6:6d:6a:a2:	25:07(32:67)75:86:ee:00(76:00(82)17:62(E6:98:51)1e:1e)
29/d0143/51/ff/70/fer04/00/60/66/f3/0f/09/ad/01/f0/9e/	d4:43:2e:03:25:f6:79:69:fe:79:94:d0:d0:b9:99:b0:ef:d2:
ididi.20:79:ff:00:c9:b3:22:97:eb:db:70:7d:ab:e5:	ds:01:ff:e9:66:30:d6:2e:e7:30:b6:96:40:bc:4e:3a:bailar
b6:5e:00:55:w0:b2:60:54:w5:41:66:E3:w3:00:34:70:37:18:	#314511D:40158:661#31e613#1e#17did#1371#018d359152133:
0412718913E14213E14213E14810810813913619617E1001E41811301	63:751d0:7eial:06:40:d2:02:27:22:0f:aeie2:07:b2:07:44:
#3:a7:fe:d4:Wa:Se:Sb:ba:we:a4:6a:70:b0:H2:D4:bf:a0:Bc:	w1:e2:ad:15:e5:d0:ea:b1:b3:d0:9f:20:15:f2:ab:cf:59:72:
cf:bore0(01(00)3*(0b;ef)23(3b;f*:43(f2)01(f*:43(85)14)	Rai02(H1)cd1aa170(57(c4)cde(c3)cda190(14)c3)\$31£7(£0)31.
de (Betedia)	<pre>%c:d5:07:07:00:dc:60:24:e7:cc:b5:c0:cf:e6:e5:7e:a7:45:</pre>
	32:00105103
rb98localhest Bookmark[]	[troy@incalhest Bockmark]5

Figure 14 /etc/ssl/certs/ssl-cert-snakeoil.pem comparrision

An examination of the keys shows that while the Issuer CN is always kali (based on the system name given at install), everything else is completely different. The validity dates are from the time that the system was originally imaged, until 10 years later.

<sup>&</sup>lt;sup>23</sup> https://wiki.debian.org/Self-Signed\_Certificate

The snakeoil SSL certificate can be regenerated with the following command:

make-ssl-cert generate-default-snakeoil --force-overwrite

The serial number, modulus, and signatures are always different between each system which makes this file a unique identifier to the system. While there is a risk of this artifact being viewable by the outside world if it was served up as the SSL server certificate when someone tried to browse to it, this would only occur if a web server was installed and it was configured to point to this specific certificate which makes the chances of it being externally visible significantly smaller. While the certificate itself is easy enough to regenerate, the fact that it is unlikely to be noticed in the first place makes it a moderate indicator of system uniqueness.

### Wired Connection 1

The file /etc/NetworkManager/system-connections/Wired connection 1 is a file generated by the network-manager to uniquely identify the physical network interface. It is important to note that if additional interfaces are added to the system (wired or wireless) that additional files will be generated<sup>24</sup>.

This file contains information about the physical interface itself and is not directly tied to the system's MAC or IP addresses. Each file is 14 lines long and the only difference is the UUID for the interface located on line 4 (see Figure 15).

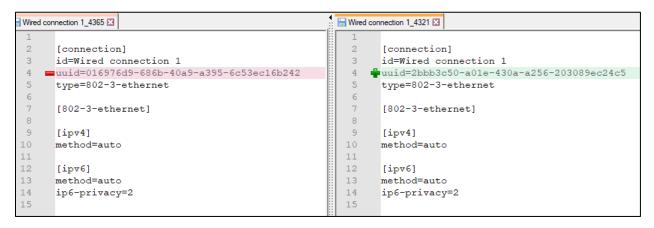


Figure 15 /etc/NetworkManager/system-connections/Wired connection 1 differences

The UUID within the file is also contained within /var/lib/NetworkManager and appears in multiple logs. The UUID allows the file to uniquely identify a system but the ID can be changed with minimal effort making this file a poor indicator of uniqueness.

#### /usr

.uuid

Scattered throughout multiple folders within /usr/share is a file simply called .uuid. The vast majority of these are located within folders related to fonts (33/39) but a few others appear in other folders. Within each file is simply a single UUID and nothing else. When completing a search of the system for each of the UUIDs though, it ties back to one of the uniquely named files found in

<sup>&</sup>lt;sup>24</sup> https://wiki.archlinux.org/index.php/NetworkManager

/var/cache/fontconfig/ (see Font Config above). This indicates to the system what cache file it can find information about the fonts within that folder.

Name	Location									
.uuid	/img_KaliW2-1.vmdk/vol_vol2/usr/share/fonts/truetype/dejavu/.uuid									
📑 mlocate.db	/img_KaliV2-1.vmdk/vol_vol2/var/lib/mlocate/mlocate.db									
564a544d-a92e-4a43-9a50-5d35b8306f57-le64.cache-7	/img_KaliV2-1.vmdk/vol_vol2/var/cache/fontconfig/564a544d-a92e-4a43-9a50-5d35b8306f57-le64.cache-7									
Hex Text Application File Metadata Context Results Annotat	ions Other Occurrences									
Strings Indexed Text Translation										
Page: 1 of 1 Page 🔄 🎐 Matches on page: 1 of 1 Match	← → 100% Ø   Reset									
.uuid 564a544d-a92e-4a43-9a50-5d35b8306f57										

Figure 16 /usr/share/.uuid and /var/carche/fontconfig correlation

As I indicated before, the fact that a UUID is present makes this file unique to this particular system but it can also be regenerated simply by deleting the file and the fc-cache -f command making this a poor indicator of system uniqueness.

#### classes.jsa

Beginning in Java 5.0 the Class Data Sharing feature was provided. The feature was designed to reduce loading time by loading up all frequently used classes once and then mapping the memory structure into a single file. Once this was done, every time java was loaded it would simply reload the memory structure that had already been established<sup>25</sup>.

These memory structures are stored in a file called classes.jsa. In Kali, these files exist in two places, /usr/lib/jvm/java-11-openjdk-amd64/lib/server/classes.jsa and /usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64/server/classes.jsa

While the classes that get loaded are the same from system to system, because the jsa file is generated on the system and not as part of the downloaded package, it is unique to the system itself however it looks like the file can easily be regenerated on the system.

#### pyc files

Out of the 79 semi-unique files, 71 of them were .pyc files, mostly located within various cache directories in /usr/lib/python3. If you're not familiar with what a .pyc is, it is just a compiled version of a python file. This is done to speed up the execution of a python file that is frequently used and is done transparently to the user. My first thought is that maybe I got unlucky and perhaps there was an update to one of the source files between the few hours when I started to make images 1 and image 4. But then I noticed that if that was the case, I should find a .py file somewhere where the hash also changed. That wasn't the case. The other thing that I found was that there were cases where images 1 and 3 would have one hash and 2 and 4 would have a new (but same) hash. Again, if a source file had changed, I would expect all of the images that were made after that change to have the same change.

After doing some research, it turns out that this isn't completely unusual. For reasons that I don't completely understand, it's not unusual for a .pyc file to compile with either the same hash or a new

<sup>&</sup>lt;sup>25</sup> http://sekhar4j.blogspot.com/2014/11/what-is-class-data-sharing.html

hash. The really interesting part is that this will occur even if you recompile on the same system multiple times, let alone a different system. It's just kind of a crapshoot.

I decided to dig into a couple of these .pyc files just to see what the difference was. The first file that I looked at was /usr/lib/python3.8/\_\_pycache\_\_/\_pyio.cpython-38.pyc. The file is 74,079 bytes long but between the four images I captured, presented two separate hashes. An examination of the file reveals a total of 14 bytes that are different and 11 of those bytes are actually just a group of 5 bytes and 6 bytes) where the locations were swapped (see Figure 17).

00000200	64 10 65 17 63 10 5A 10 65 10 6A 10 AU 11 65 10	60e'f.23e.53 (e3	00000240 64 10 65 27 83 01 85 11 65 11 65 11 60 11 65 11 60e'f.23e.53 (e5
00000270	A1 01 01 00 47 00 65 01 66 33 86 00 66 32 65 03	i6.d1d1d1e.	00000170 A1 81 01 00 47 00 64 31 64 32 54 00 64 31 65 03 15.did1d2e.
000000300	43. 10 53 13 53 13 47 10 64 33 44 39 24 10 64 39	145.250.433409	00000200 6A 30 85.02 5A 35 67 00 64 33 64 30 84 00 64 34 547.250.850404
000000290	45 10 55 10 58 00 47 00 64 15 48 10 54 10 64 10	#3f.16G.d5d#d0	000000290 65 81 83 83 83 56 47 00 64 18 64 36 84 88 64 18 64 38 ±34.268.05d6d6
00000280	65 18 85 13 68 17 66 02 53 00 25 55 TA 25 6A 10	eif.17(1.1,)8s).8	000002A0 45 04 02 03 5A 37 44 02 53 00 29 00 7A 28 0A 20 eff.I7d.S.) 6g).F
000000380	79 78 48 47 48 30 49 40 70 40 48 40 48 48 74 41	ython implements	00000280 79 34 68 47 68 30 68 67 70 00 65 65 65 74 61 ython implements
00000200	74 48 47 42 20 47 46 20 74 48 42 20 48 47 20 48	tion of the ic m	00000200 74 60 6E 62 20 67 64 20 74 68 65 10 69 67 20 60 tion of the io m
00000200	67 00 75 00 65 20 08 29 00 00 00 00 45 29 01 1W	odule#	00000220
00000280	100 41 40 40 48 48 48 14 14 46 18 40 47 48 48 48 48	Allooste_look>,	Silcate Lock 10 25 H3 65 17 18 18 18 19 20 19 18 10 0310000
00000289	00 10 00 25 06 43 79 47 77 69 62 78 05 77 69 62	Retracted with	000002F0 00 00 00 04 05 TT 48 55 23 22 28 04 43 TH 4T TT
80000380	13 12 29 01 DA 07 73 85 74 80 88 84 82 20 08 DA	U. (setmode) .U	90000000 5 1 29 00 DA 07 73 60 74 6D 6F 64 65 29 94 DA 10
	of at	. All 0.8888 B	00000310 U7 17 17 17 41 40 40 17 17 18 10 13 41 45 48 48 17 10 . 411 U.SEEK 3
80000320	45 1+ 16 (0 52 45 45 10 57 4) 55 17 16 (0 52 4)	RIU.SEEM_CORD_SE	00000320 45 14 DA 00 53 45 48 48 57 47 58 57 DA 08 58 40 ETU.SEEN CUBU.SE
80000330	45 48 57 45 42 44 29 51 08 00 28 29 02 00 00	EIL EHDe	000000330 45 48 5F 45 4E 48 EF 11 00 00 00 EF 02 00 50 00 ER END4
00000340	DA 119 53 15 45 15 5F 11 4F 10 48 19 20 22 00 00	U.SEEK BOLEL	00000240 DA DA S3 45 45 40 SF 40 4F 4C 45 60 00 20 D0 50 D.SEEM BOLEL
100000350	33. 10 67 65 74 74 68 74 61 50 75 65 66 65 68 75	I.gettotalsefoou	00000350 SR 10 67 05 76 76 65 78 61 60 72 65 66 61 65 75 2.gestotalrefrom
00000340	42 74 DA 01 72 29 FF FF FF FF 54 63 08 00 00	atd.c#91997c	00000360 68 14 DA 01 72 E5 PF FF FF 54 63 05 08 D0 08 ms0.zegypyTe
00000370	00 00 00 00 00 00 00 00 16 00 00 00 00 00 00 00	**************	00000370 00 00 00 00 00 00 00 14 00 00 00 00 00 00 00
00000300	43 00 00 00 73 24 03 00 00 74 00 70 00 74 01 05		00000380 43 00 00 00 73 36 03 00 00 74 00 70 00 74 01 03 Cs
	03 73 34 74 02 A0 03 70 00 AJ 03 70 00 74 00 70		00000590 02 75 16 74 02 A0 03 70 00 AL 01 70 00 70 00 70 .a.tt.:
00000340	00 TH 04 TH 05 TH 01 HE 03 13 62 TE 36 TH 04 HH	.t.t.t.f.f.#0t.d	00000380 00 74 04 74 05 74 01 44 03 03 02 73 00 74 06 44 states.f.f.sot.d.
00000588	82 37 00 14 00 83 01 87 03 18 00 37 03 54 04 85	1 4 V L L A T	2000003885 0X 30 00 14 00 23 04 27 03 34 05 27 03 34 04 23 4 4 + 1 + 4

Figure 17 Byte Comparison of /usr/lib/python3.8/\_\_pycache\_\_/\_pyio.cpython-38.pyc

A look at another file (/usr/lib/python3/dist-packages/IPython/core/\_\_pycache\_\_/application.cpython-38.pyc) which actually had 3 variations in hashes. In this case, we see something very similar starting at hex offset 0x4E0. In this case the file is 14,126 bytes and depending on which two version you are comparing there are only 7 or 9 bytes different between the two versions (see Table 3).

4E0	4E1	4E2	4E3	4E4	4E5	4E6	4E7	4E8	4E9	4EA	4EB	4EC	4ED	4EE	4EF
00	DA	01	31	DA	04	74	72	75	65	54	3E	02	00	00	00
00	DA	01	31	DA	04	74	72	75	65	54	3E	02	00	00	00
00	DA	04	74	72	75	65	DA	01	31	54	3E	02	00	00	00
5E0	5E1	5E2	5E3	5E4	5E5	5E6	5E7	5E8	5E9	5EA	5EB	5EC	5ED	5EE	5EF
DA	01	30	DA	05	66	61	6C	73	65	46	7A	8E	55	6E	73
DA	05	66	61	6C	73	65	DA	01	30	46	7A	8E	55	6E	73
DA	01	30	DA	05	66	61	6C	73	65	46	7A	8E	55	6E	73

 Table 3 Byte Comparison of /usr/lib/python3/dist-packages/IPython/core/\_\_pycache\_\_/application.cpython-38.pyc

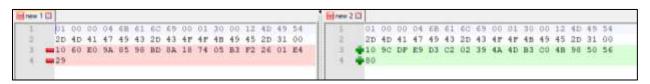
Because of this known situation, I don't believe that having a unique or non-unique hash with .pyc files is indicative one way or another of a particular system. That being said, .pyc files are frequently recompiled by python as different modules are used by the system. Additionally, they can be completely deleted from the system and they will be regenerated as required<sup>26</sup>.

<sup>&</sup>lt;sup>26</sup> https://indianpythonista.wordpress.com/2018/01/05/demystifying-pyc-files/

### /var

### .Xauthority

LightDM allows for the use of cookies for authentication. Each system stores it's cookie at /var/lib/lightdm/.Xauthority. Each file is 49 bytes, and the first 32 bytes are the same.



#### Figure 18 /var/lib/lightdm/.Xauthority differences

Because there are only 17 bytes of entropy in each file, it means that there are only 131 thousand possible combinations. This means that it will repeat itself rather frequently and should not be used to uniquely identify the system even though in our case it had a unique hash each time.

#### aux-cache

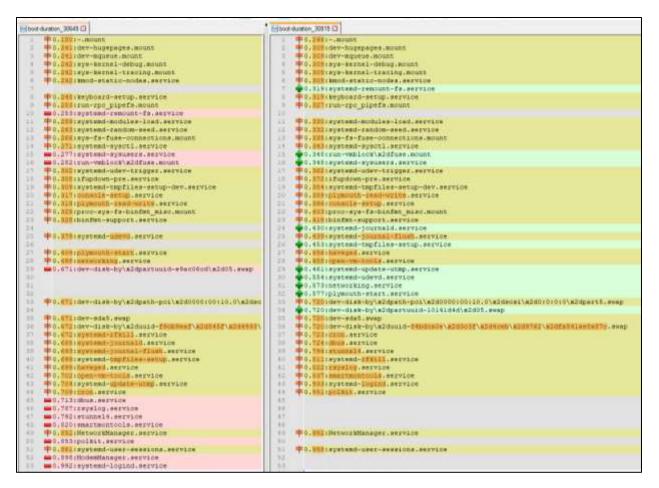
Located at /var/cache/ldconfig/aux-cache is the shared library links and cache file. It is designed to speed up the loading of some libraries, and also allows the dynamic linker to call libraries by their soname<sup>27</sup>. While the same libraries are cached in each installation, because the cache is compiled at run time, they are all different at the hash level. The file can be regenerated by deleting it and then running ldconfig. This cache file can be used to uniquely identify a system but the ease with which it can be regenerated makes it a poor indicator of system uniqueness.

#### boot\_duration

Located at /var/lib/plymouth/ is a file called boot-duration. Plymouth is the program that shows the splash screen when the system first boots up. While each version of the file is similar, there are differences. First, certain events seem to be missing from some versions as opposed to others. Second, the numbers within each event are also generally different. The one thing within the file that does make it unique is the UUID for the swap partition found on line 36 in the images below. This UUID is located within fstab as well as several log files which makes it unique to the system. While this particular instance of the UUID could be changed relatively easily, it would prove significantly harder to change it in its other locations making this a good indicator of system uniqueness.

<sup>27</sup> 

https://lists.fedoraproject.org/archives/list/devel@lists.fedoraproject.org/thread/DVBZI2UJRHI5GVMJXIQNLHK4T UFS5ZM2/



#### cookie

/var/lib/lightdm/.config/pulse/cookie is part of the lightdm display manager that is standard for Kali 1604 and below<sup>28</sup>. The cookie file is used to uniquely identify the system. Because of that, it is of course unique to the system and can be used to identify an individual system.

#### default\_cert.pem

Inetsim is a software suite that can simulate common Internet services within a lab<sup>29</sup>. It comes ready to run many pre-configured services to include an HTTPS server. When run, the certificate located at /var/lib/inetsim/certs/default\_cert.pem and key located at /var/lib/inetsim/certs/default\_key.pem serves as the SSL certificate for the webserver. Like the /etc/ssl/certs/ssl-cert-snakeoil.pem file, this is a valid SSL certificate. Instead of having a subject CN of kali, it now has a more fully populated subject record that includes an Organization of INetSim, Organization Unit of Development, and a CN of inetsim.org. This key is also valid for 10 years. Also like the snake\_oil certificate, the rest of the certificate is unique to this particular installation of the operating system.

<sup>&</sup>lt;sup>28</sup> https://wiki.ubuntu.com/LightDM

<sup>&</sup>lt;sup>29</sup> https://www.aldeid.com/wiki/INetSim

Inet by its design is supposed to be used within a lab environment only. While the certificate is technically viewable from the outside if it is served, the chances of this happening accidentally are very low.

Freedbicathout - Deskop/Experts/Fakt/2 (1978), https://doi.ab.2019/01/19.25/content/Experiment	🚽 🚽 bayddiaddiad - Deithy Reputst Kalif - 1 HDA, Reput 0+ 31-702-58-43-25 (anters Bakmark)
troyglocalhost Bookmark(S openee) #500 -text -noout -in default_cert_II310.pen	(Aroy@incalhost Boomsark]\$ opensal a505 steat shoot sin default cert 51164.pen
Ternificate:	Certificate)
Datal	
Version: 3 (Us2)	Version: 3 (0s2)
Derial Number: STroe:Wdred:4br0a:Beib6:31:HE:49:ed:65:67:Eb:19:73:bE:94:51	Secial Summer:
Signature Algorithm; shalWithRSAEncryption	c2:50:53:54:46:c5:c5:64:5+:17:c5:56:55:c#:5#;c7:5#:56:55
Issue: 0-INetSim, CD-Sevelopment, CD-inetsim.ory	Signature Algorithm: stalWithES&Encryption
Validity	Tesuer: O-INerlin, CO-Development, CN-inersis.org
Not Before: Jul 22 13:46:10 2030 SHT	Validity
Not After 1 Jul 20 18:46:10 2000 DMT	Not Hefore: Jul 22 19:13:12 2020 HMT
Subject: O-INetZim, CO-Development, CD-Instain.org	Nos After ( Jul 20 14:21:12 2030 UMT
Subject Public Hey Info:	Subject: O-THetSis, OD-Development, CH-inetaim.crg Subject Fublic Key Info:
Public Ney Algorithm: rmsIncryptics	Public Ney Algorithm: realboryptics
Public-Rey: (2040 bit)	Public-Sey) (2000 hit)
Modulast	Hodding:
001rbb135rea14012a16b10314a17a1821661391ff1321	00/00/32/00/30/09/00/20/10/99/00/00/00/00/
b3:91-14:64:00:09:99:96:05:08:be:30:00:50:	EdicaldF:Saib4:Goib5:#F:Finb:T4:Fi:29:0f:b0:
54、米市196130130130146、7月170146、半月153330333533344441	54(b4)(b)(0)(0)(0)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)(2)
12146:57:43:26:46:74:57:10:86:44:48:10:15:cb:	00:47:70:00:47:90:46:20:00:47:10:20:04:0d:32:
edidord5ro1:04.04r3ar8e1d1rd8r07130r14r34r01r	7di21:06:55:66:00:02:80:33:51:61:67:56:40:00:30:
0410011D:301e0:0::0frc1:33:94:4e167:13:66:b0:	9dilmibdiae:07:91:c0:07:03:46:e6:le:ff:31:
\$0:95101179:0211415917417810#1571501801681081	d017715410713712312e12517110014a1971501501501
31:ce:#3:a2:56:15:62:F3:46:5e:#3:55:e1:95:cb:	lf:25:da:e7:4b:25:25:ec:0b:a5:3c:ee:52:b7:73:
H1:34:a6/b4:a3:d4:f2:00:a7:80:13:6f:bf:a8:b9:	67/0016810e19e12e1001d81261301231081d81d81
N3:70:81:321:41:42:13:85:27:56:48:10:85:20:45: 17:25:10:44:95:26:47:262:35:11:64:44:74:40:63:	d8119:4c:97:00:37:99:43:21:dd:88:65:13:24:72:
ED:76:e6:52:54:93:db:8c:65:73:E0:ac:4c:4tb6:	4615619E102(00)20(20(20)20)171b6190(70(69)
b7/BeraelDer20r8b:6f:fai27/70:16/Ber62recrc7/	05:5c:77:c6:d0:07:ed:00:b2:9e:42:45:02:03:
#2:77:ce:38:fir#2:ab:00:77:56:05:a6:60:	01:70:60182:27:73:8e:±9:00:42:44:00:96:96:00:07:
Bd:70:36:ef:#0:1a:f1:3#:70:0f:96:#6:#f:94:76:	43:11:12:ef:14:5d:00:00:4d:01:00:ff:37:5b:4f:
c2:d9:le:14:De:05:7a:05:abrad:77:31:d1:08:54:	<pre>49:991b0:60:00:00:00:00:00:00:00:00:00:00:00:00</pre>
hothbil5:47:04:c0:h9:c6:Sethfie4:43:0a:20:d5:	29-30-001-00-00110-00-00100-00100-00-00-00-0
52:35	43:15
Exponent: 45537 (0x10001)	Esponent1 85887 (0x10001)
R50593 extensions:	X009v1 Stansions:
Xidevi Hubject Wey Identifier:	X508v0 Subject Sey Identifier:
F5/90/93/6E/SF(22/74/4C/1E)SF(44)4B/FE/E5/AC/SC/4F/9F/C5/CF	C5:FF:02:20:15:C2:40:19:59:45:E9:3C:12:0F:82:C1:08:F3:C9:F2
KSG9v3 Authority Ney Identifier:	X505v3 Authority Hev Identifiers
Regin(%) 80(93)8E(3F123)74(4C)1E(3F)44(40)TE(E5)AC(3C)4F10F(C3)C6	keyid:C5:FF:01:2D;15:C2:8D:19:59:45;K9:3C:12:DF:K2:C2:6H:F3:C9:F2
X109vJ Basic Constanints; colling) ChrTHOE	X503v3 Basic Constraints: critical
Signature Algorithm: shalWithESAEncevicine	CRATERUE Description of the second s
<pre>chi5d:6e:Rordl:BerBf:0f:df:60:40:56:b0:80:80:20:</pre>	Signature Algorithm: smalWithREAEncryption
Seind: 78:66:00:25:09:06:00:75:00:00:05:05:05:05:05:05:	<pre>.mb:of)ae:04:dEinf:W9:Dd:nd:T1:2d:ed:9e:e0:42:88:86;</pre>
Of:farla:e7:00:b0:10:95:a0:90:04:ab:09:20:al:bd:b6:2b:	00:99:8w:02:01:94:30:f2:d1:f3:d1:a5:37:d7:fw:96:90:46:
#4:6b:24:31:45:50:02:40:44:42:42:42:29:50:04:06:02:02:	<pre>wbr4frim(hd)e0(00191;00(00100;00(00100100;00(00100;00))) 00007cd0;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(00100;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(000;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00(00;00;</pre>
30:de:m4:le:Td:b5:l6:85:69:1f:79:90:53:c8:85:2b)79:bc:	20160145:90(20(2)(2)(20(2)(2))0(2e(4)(a+9e(6)(8)(24(2)(2)(2))
98:0e:19:ae:0e:12:94:11:02:11:02:20:42:61:ef:al:00:50:	14:08:ef1e2:me:32:20:ef:26:fd:1a:65:40:16:56:5d:96:fl:me:
hj:d5:3d:Verd2:7b:93:d2:37;her92:e0:91:46:c6arcb:61:9b:adu	Jer67/Jar13/Doub4/f8/D0/Jf/of/e6/Der46/Lf/30/48/Dor47/
691671601671661721971631691551991391201201661701701061	wirffrür:f2:bd:34:19:Gw:Cw:46:9e:0f:c6:21:fw:dw:db:6c:
m315er951eer49:24129116157:001311091m4:cm:20:47:08:7701	5E1501301271871811501051211801401001031861001851061701
Ebib5:dd:ff:fm:04:74:0biacis0:am:00:25:f4:33:40:57:45:	36:10:ff:f0:57:54:3e:02:57:2b:2e:51:5b:23:d0:44:bb:36:
5a:94:8a:02:43:90:15:f3:f3:0c:Sb:b9:fb:34:7d:13:73:d7:	08:08:89:91:155:08:86:85:26:80:49:08:1ac08:02:121a9:2e:
07101r0b;76100115:02:72:25:00:00:90:00:31:01:01:01:10:	b7:00:47;a2:44:51:cd:71:11:a3:12:20:01:2c:74:b3:db:4d:
64:d3:06:5e:00:4e:70:3e:e8:64:77:34:3b:e3:be:df:37:00:	
G#150:32:111:27138:00:00:00:06:52:85:03:00:06:52:81:52:61:	UT:7e:#3:16:76:2d:#5:db:75:00:96:56:6c:75:8d:13:29:#a:
ad:13:29:42 (troy@localhost Boommark)#	
	troy@localhost Bookmar& C

Figure 19 /var/lib/inetsim/certs/default\_cert.pem comparison

#### Index.db

Located in /var/cache/man/ are 30 additional directories with cache files for the various man files in each language. Within each directory is a file called index.db which is the cache. The cache is populated by the program mandb<sup>30</sup> and can manually be regenerated on demand. Out of the 79 semi-unique files previously identified, 7 of them belong to the index.db files for various languages.

An examination of the files shows a significant difference between two copies of the same file, but there are still plenty of instances where the same copy is found. For right now, I have no idea why it only affected these 7 languages (vs the other 23) and why some files are the same and others are different. Again, because of this, I don't believe that index.db files for the man files are indicative of a particular system.

<sup>&</sup>lt;sup>30</sup> https://man7.org/linux/man-pages/man8/mandb.8.html

### kali-amd64

The folder /var/lib/initramfs-tools/ contains two files, 5.5.0-kali2-amd64 and 5.7.0-kali1-amd64. While I can't figure out exactly what these files are for, initramfs-tools is used to create an initramfs for the kernel headers. These images are loaded up into memory at boot time to allow the rest of the file system to load<sup>31</sup>.

Both files contain unique hashes in all four instances and can be used to uniquely identify a system.

#### mlocate.db

The file /var/lib/mlocate/mlocate.db contains the database that is generated for use with the locate command. It contains among other things, a list of all of the files found on the disk. The reason why the database is different is because of the 45 uniquely named files noted at the start of this paper (see Figure 20). The mlocate.db is continuously changed as files are added/removed from the system. The file can be manually updated through the use of the dbupdate command. This file is not a good indicator of a unique system.

Name	Location	Modified Time
2c53115d-7f38-4bfc-9172-71687740e27d-e64,cache-7	/img_KaliV2-1.vmdk/vol_vol2/var/cache/fontconfig/2c5311	2020-07-22 13:47:30 0
2c53115d-7f38-4bfc-9172-71687740e27d-e64.cache-7-slack	/img_KaliV2-1.vmdk/vol_vol2/var/cache/fontconfig/2c5311	2020-07-22 13:47:30 0
uuid 📃	/img_KaliV2-1.vmdk/vol_vol2/usr/share/fonts/X11/Type1/	2020-07-22 13:47:28 (
mlocate.db	/img_KaliV2-1.vmdk/vol_vol2/var/lib/mlocate/mlocate.db	2020-07-22 13:47:34 0
,uuid.NEW	/img_KaliV2-1.vmdk/vol_vol2/usr/share/fonts/X11/Type1/	2020-07-22 13:47:28 0
<		
Page: 221 of 229 Page Address of page: 1 of 1 Ma 136f21f7-d779-44fe-94bd-9acca931261b-1e64.cache- 19471168-b12b-4cfe-b66d-78fa53b13167-1e64.cache- 1bd710f5-632e-46c7-aac0-ccbe00c423dc-1e64.cache- 1e7ae182-406c-4bec-ab4d-2d0c2bb24054-1e64.cache- 26927276-cf88-4d8e-b66b-5697d2ba5bb5-1e64.cache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664.eache- 2655b202-602e-4664	-7 -7 -7 -7 -7 -7	
2c53115d-7f38-4bfc-9172-71687740e27d le64.cache-		
2ef35129-5b00-4bcd-8bcf-b1bf54d629cb-le64.cache-		
34aff380-48fd-44b1-9b1d-071c52895e13-1e64.cache-		
564a544d-a92e-4a43-9a50-5d35b8306f57-le64 cache-		

Figure 20 Uniquely named files located within mlocate.db

## MySQL files

Of the 202 files across the images that always had a unique file hash, 60 of them were located within /var/lib/mysql/mysql as either .frm or .myi files. A .frm file is a table definition file. What is interesting with the .frm files is that the table definitions on each image should match since they are defined the same (columns, etc.). However in the case of column\_stats.frm, and others there are only a small

<sup>&</sup>lt;sup>31</sup> https://wiki.debian.org/initramfs-tools

number (11 in that case) of bytes that are different. An examination of the file format shows that these hex offsets should not actually in use so I'm not entirely sure why they are different<sup>32</sup>.

The .myi files are the index files for each of the corresponding tables. As with the .frm files, the differences between versions of the same file are minor (only 5 bytes for columns\_priv.myi for example) that makes them a poor indicator of a unique system.

#### pubring.kbx

/var/lib/lightdm/.gnupg/pubring.kbx contains the keyring of public keys that that LightDM recognizes. By default, it doesn't include any keys which means that the keyrings should all have the same hash. But for some reason, they all have a unique hash. The file itself is 32 bytes long and they are the same except for two bytes that are repeated once.

While each file had a different hash here, the fact that there are only two bytes that change means that there are only 65,536 possible combinations so there is a high likelihood that they are repeated. This file should not be relied on to uniquely identify a system.



Figure 21 /var/lib/lightdm/.gnupg/pubring.kbx comparison

#### questions.dat

Located at /var/log/installer/cdebconf/questions.dat, I expected this file to be unique across all images. Instead, though, I got one hash for two images and another hash for the other two images. Questions.dat is a file that is generated when the initial Kali install is occurring. It records the values that are assigned to various variables. The file doesn't contain any date or timestamps, so the chances of getting an exact duplicate (assuming you follow the same build instructions) are significantly higher.

When I examined the files, it took a while, but I finally figured out what the difference was:

Name: tasksel/first

Template: tasksel/first

Value: Desktop environment [selecting this item has no effect], … Xfce (Kali's default desktop environment), Collection of tools [selecting this item has no effect], … top10 -- the 10 most popular tools, … default -- recommended tools (available in the live system) Variables:

CHOICES = Desktop environment [selecting this item has no effect], ... Xfce (Kali's default desktop environment), ... GNOME, ... KDE Plasma, Collection of tools [selecting this item has no effect], ... top10 -- the 10 most popular tools, ... default -- recommended tools (available in the live system), ... large -default selection plus additional tools

CHOICES\_C = desktop, desktop-xfce, desktop-gnome, desktop-kde, meta, meta-top10, meta-default, meta-large

<sup>&</sup>lt;sup>32</sup> https://dev.mysql.com/doc/internals/en/frm-file-format.html

Name: tasksel/first Template: tasksel/first Value: Desktop environment [selecting this item has no effect], ... Xfce (Kali's default desktop environment), Collection of tools [selecting this item has no effect], ... top10 -- the 10 most popular tools, ... default -- recommended tools (available in the live system) Variables: CHOICES\_C = desktop, desktop-xfce, desktop-gnome, desktop-kde, meta, meta-top10, meta-default, meta-large CHOICES = Desktop environment [selecting this item has no effect], ... Xfce (Kali's default desktop environment), ... GNOME, ... KDE Plasma, Collection of tools [selecting this item has no effect], ... and effect], ... top10 -- the 10 most popular tools, ... default -- recommended tools (available in the live system), ... large -default selection plus additional tools

The last and 2<sup>nd</sup> to last lines contain the same information, but the order is reversed. That is the only difference in a 4k line log file. When I built the images, I did the same steps each time, but for some reason this log entry is different and I'm not entirely sure why. And the fact that it is the same on two of the systems and has the same difference on the other two systems makes it a little unusual. I suspect that there are likely two processes that are going on in parallel and that some of the time the first process finishes first and generates its log entry while other times the second one will complete first.

#### random-seed

Operating systems make extensive use of various cryptographic functions. For them to operate securely, they must be fed with random numbers. In Linux, random numbers are provided through the /dev/random interface. For this interface to produce truly random numbers though it, must wait for enough entropy to be collected. Unfortunately in the case of booting the system, this can be a lengthy process. To prevent a slow-down, an initial entropy value is saved to disk before shutdown. This value is saved at /var/lib/random-seed<sup>33</sup>. The file is a 4,096-bit file that contains a dump of entropy from the system at shutdown. While it doesn't meet the requirements for true cryptographic use, it is sufficiently random to provide the systemd process what it needs at boot to generate UUIDs and other functions.

While this file is unique to the system, the fact that it has a fairly short lifetime between changes (each system shutdown/reboot) makes it a very poor indicator of system uniqueness.

<sup>&</sup>lt;sup>33</sup> https://systemd.io/RANDOM\_SEEDS/

E:\Kali Experi	ment	v2\/	\uto	psy∖l	KaliV	2-2\	Repo	rts\K	aliV2	2-2 H	ITML	Rep	ort 0	9-28	-2020	0-06-4	43-25\content\Bookmark\ra
Offset(h)	00	01	02	03	04	05	06	07	08	09	ΟA	0B	0C	0D	0E	OF	Decoded text
00000000	65	B3	52	7F	D4	DE	AB	2A	44	DA	41	FE	F4	EA	7C	22	e³R.ÔÞ«*DÚAþôê "
00000010	D6	84	2F	ΕO	AD	F9	46	4D	0C	96	2C	96	25	89	49	30	Ö"/à.ùFM,-%‰I0
00000020	8C	9B	11	D4	1F	F4	C7	BF	86	AD	8A	C4	5A	14	1C	25	Œ>.Ô.ôÇ¿†.ŠÄZ%
00000030	18	71	ЗF	53	34	A5	05	E6	89	95	1F	30	AA	9F	C7	92	.q?S4¥.払.0°ŸÇ′
00000040	CF	4F	94	71	47	7A	3C	0D	E2	CD	25	71	Α6	F4	<b>E1</b>	88	ÏO″qGz<.âÍ%q¦ôá^
00000050	99	59	DE	83	EA	C0	37	BC	EA	ΕO	50	EA	0A	5E	FO	BB	™YÞfêÀ74êàPê.^ð»
00000060	2C	D2	36	В4	5D	C1	84	D2	AE	В0	17	52	0C	CB	AB	25	,Ò6′]Á"Ò⊗°.R.Ë«%
00000070	21	8C	74	4D	<b>B1</b>	E4	73	OF	6A	0C	C0	64	43	ЗB	22	A0	!ŒtM±äs.j.ÀdC;"
08000000	A3	C6	AF	1E	67	BB	DC	91	19	4D	10	C0	97	1B	92	22	£Æg»Ü`.M.À—.′"
00000090	F1	DO	19	25	9E	22	C6	В9	39	87	8C	6A	82	CA	15	4D	ñÐ.%ž"ƹ9‡Œj,Ê.M
000000A0	75	BA	49	4E	79	41	F4	A5	C2	0F	<b>A</b> 7	94	<b>A1</b>	F9	6B	23	u°INyAô¥Â.§″;ùk#
000000B0	4C	82	25	4C	6C	C3	8B	63	49	E3	FB	ЗF	4B	03	Β6	5A	L,%LlÃ <ciãû?k.¶z< td=""></ciãû?k.¶z<>
000000000	76	30	AD	1D	D5	BC	28	9D	8F	93	5D	AC	<b>A</b> 7	22	64	73	v0Õ¼("]¬§"ds
000000D0	1B	7F	0A	FO	4F	EB	7F	5A	88	54	0D	AC	5C	2B	09	89	ðOë.Z^T.¬\+.‰
000000E0	08	E0	8A	49	47	37	AЗ	82	<b>A</b> 7	55	A0	17	EC	26	18	68	.àŠIG7£,§U .ì&.h
000000F0	4C	5B	9C	7F	48	F5	7D	26	C5	CE	23	F7	51	2E	69	1B	L[œ.Hõ}&ÅÎ#÷Q.i.
00000100	C1	C6	FO	65	17	94	ЗD	BC	69	CE	07	5A	5D	4B	93	AF	ÁÆðe.″≕₄iÎ.Z]K"
00000110	3D	92	8A	4D	41	AA	В9	9C	EB	0C	03	СВ	7A	55	AD	4D	=′ŠMAª¹œëËzU.M
00000120	37	4C	5E	05	C9	A3	1D	F7	Α4	EC	67	4F	8E	24	7B	B6	7L^.É£.÷¤ìgOŽ\${¶
00000130	8A	8D	7A	AA	59	0F	ЗA	43	C1	51	DA	13	87	3C	51	44	Š.zªY.:CÁQÚ.‡ <qd< td=""></qd<>
00000140	Α7	2B	A6	8F	6A	E1	37	48	FF	75	B1	30	6A	D2	B1	C5	§+¦.já7Hÿu±0jÒ±Å
00000150	8E	32	BA	BC	CE	EB	E9	91	B8	CA	4C	FB	24	76	BD	12	Ž2°¥iÎëé∖,ÊLû\$v⊁.
00000160	E3	FC	<b>A</b> 5	E5	27	59	DO	E5	D8	B3	16	92	57	06	1E	B2	ãü¥å'YÐ娳.′₩≗
00000170	67	F9	D3	5D	E3	00	67	8F	8D	EE	07	11	D4	5C	1C	ED	gùÓ]ã.gîÔ∖.í
00000180	Α6	A4	05	9C	FO	99	87	0A	6A	27	F1	6F	65	24	5A	43	¦¤.œð™‡.j'ñoe\$ZC
00000190	59	BA	DD	F2	44	70	10	0A	<b>A</b> 8	91	4A	FD	73	E7	C4	6C	Y°ÝòDp¨'JýsçÄl
000001A0	BF	C8	19	82	6D	16	61	F8	72	14	4A	7C	7B	31	05	53	¿È.,m.aør.J {1.S
000001B0	F3	46	56	EF	0F	ЗF	D9	DA	09	21	CD	12	96	DD	54	96	óFVï.?ÙÚ.!ÍÝT-
000001C0	DE	F6	E7	B2	09	E9	99	5F	<b>A</b> 5	C4	ЗA	AA	81	D3	49	DA	Þöç°.é™ ¥Ä:ª.ÓIÚ
000001D0	A5	F6	C3	Α9	96	78	08	64	В9	D3	8B	44	00	D7	41	5A	¥öé-x.d²Ó <d.×az< td=""></d.×az<>
000001E0	AC	<b>A</b> 5	B8	AA	D3	77	32	09	88	AO	53	EE	9D	9E	7F	42	⊣¥,ªÓw2.^ Sî.ž.B
000001F0	06	83	B2	83	F4	22	E3	9A	9A	5E	9A	11	E9	BC	7F	44	.f°fô"ãšš^š.é4.D

Figure 22 /var/lib/systemd/random-seed

#### timestamps

When a user uses the Network Manager Connection Editor in the GUI, one item presented to them is the last time that a particular network connection was used. This information is found in the file /var/lib/NetworkManager/timestamps (see Figure 23). The file consists of a single line for each network interface on the system. The line contains the UUID for the connection (see the analysis of file /etc/NetworkManager/system-connections/Wired connection 1 above) and the epoch time of when that connection was last active.



Figure 23 /var/lin/NetworkManager/timestamps differences

While the timestamp does not help in the identification of a system (although can help with the building of a timeline in traditional forensics), the fact that the file contains the same UUID as is used in /etc/NetworkManager/system-connections/Wired connection 1 means that this file can uniquely identify a particular system.

## Conclusion

In conclusion, the Kali is a fairly complicated, and poorly documented operating system. While the vast majority of it is common to every installation, there are 226 files that are unique to every installation of it (excluding log files). While many of these files are very easy to replace without affecting the system, there are 13 that appear to be extremely difficult to modify without either affecting the operation of the system, or removing all artificats that would indicate that they had been purposely changed.

While it appears that all of these files would require access to the system itself (likely root level), they do present a vulnerability to the complete anonamyzation of a system. In the end, if true annomization of the system is a requirement, the operating system should be installed fresh each time it is used.

# **Appendix 1: Always Unique Hashes**

Path
/boot/grub/grub.cfg
/boot/initrd.img-5.5.0-kali2-amd64
/boot/initrd.img-5.7.0-kali1-amd64
/etc/adjtime
/etc/fstab
/etc/initramfs-tools/conf.d/resume
/etc/king-phisher/server_config.yml
/etc/machine-id
/etc/NetworkManager/system-connections/Wired connection 1
/etc/shadow
/etc/shadow-
/etc/ssh/ssh_host_ecdsa_key
/etc/ssh/ssh_host_ecdsa_key.pub
/etc/ssh/ssh_host_ed25519_key
/etc/ssh/ssh_host_ed25519_key.pub
/etc/ssh/ssh_host_rsa_key
/etc/ssh/ssh_host_rsa_key.pub
/etc/ssl/certs/java/cacerts
/etc/ssl/certs/ssl-cert-snakeoil.pem
/etc/ssl/private/ssl-cert-snakeoil.key
/usr/lib/jvm/java-11-openjdk-amd64/lib/server/classes.jsa
/usr/lib/jvm/java-8-openjdk-amd64/jre/lib/amd64/server/classes.jsa
/usr/lib/python3.8/pycache/_markupbase.cpython-38.pyc
/usr/lib/python3.8/pycache/ftplib.cpython-38.pyc
/usr/lib/python3.8/pycache/hashlib.cpython-38.pyc
/usr/lib/python3.8/pycache/pydoc.cpython-38.pyc
/usr/lib/python3.8/pycache/rlcompleter.cpython-38.pyc
/usr/lib/python3.8/asyncio/pycache/maincpython-38.pyc
/usr/lib/python3/dist-packages/django/db/pycache/utils.cpython-38.pyc
/usr/lib/python3/dist-packages/django/test/pycache/signals.cpython-38.pyc
/usr/lib/python3/dist-packages/flask/pycache/helpers.cpython-38.pyc
/usr/lib/python3/dist-packages/gevent/pycache/_socket3.cpython-38.pyc
/usr/lib/python3/dist-packages/gpg/pycache/core.cpython-38.pyc
/usr/lib/python3/dist-packages/hupper/pycache/worker.cpython-38.pyc
/usr/lib/python3/dist-packages/IPython/core/pycache/inputsplitter.cpython-38.pyc
/usr/lib/python3/dist-packages/IPython/core/pycache/inputtransformer2.cpython-38.pyc
/usr/lib/python3/dist-packages/matplotlib/pycache/dates.cpython-38.pyc
/usr/lib/python3/dist-packages/mitmproxy/net/http/pycache/request.cpython-38.pyc
/usr/lib/python3/dist-packages/nbformat/v4/pycache/convert.cpython-38.pyc

/usr/lib/python3/dist-packages/packaging/\_\_pycache\_\_/tags.cpython-38.pyc

/usr/lib/python3/dist-packages/pandas/core/\_\_pycache\_\_/resample.cpython-38.pyc

/usr/lib/python3/dist-packages/pandas/tests/indexes/datetimes/\_\_pycache\_\_/test\_tools.cpython-38.pyc

/usr/lib/python3/dist-packages/pandas/tests/indexes/interval/\_\_pycache\_\_/test\_interval.cpython-38.pyc

/usr/lib/python3/dist-packages/scipy/\_lib/\_\_pycache\_\_/\_numpy\_compat.cpython-38.pyc

/usr/lib/python3/dist-packages/scipy/spatial/tests/\_\_pycache\_\_/test\_distance.cpython-38.pyc

/usr/lib/python3/dist-packages/wapitiCore/net/\_\_pycache\_\_/swf.cpython-38.pyc

/usr/local/share/fonts/.uuid

/usr/share/fonts/.uuid

/usr/share/fonts/cMap/.uuid

/usr/share/fonts/cmap/.uuid

/usr/share/fonts/opentype/.uuid

/usr/share/fonts/opentype/cantarell/.uuid

/usr/share/fonts/opentype/font-awesome/.uuid

/usr/share/fonts/opentype/roboto/.uuid

/usr/share/fonts/opentype/roboto/slab/.uuid

/usr/share/fonts/opentype/urw-base35/.uuid

/usr/share/fonts/truetype/.uuid

/usr/share/fonts/truetype/dejavu/.uuid

/usr/share/fonts/truetype/droid/.uuid

/usr/share/fonts/truetype/firacode/.uuid

/usr/share/fonts/truetype/font-awesome/.uuid

/usr/share/fonts/truetype/hack/.uuid

/usr/share/fonts/truetype/lato/.uuid

/usr/share/fonts/truetype/liberation/.uuid

/usr/share/fonts/truetype/lyx/.uuid

/usr/share/fonts/truetype/noto/.uuid

/usr/share/fonts/truetype/quicksand/.uuid

/usr/share/fonts/truetype/ttf-bitstream-vera/.uuid

/usr/share/fonts/type1/.uuid

/usr/share/fonts/type1/urw-base35/.uuid

/usr/share/fonts/X11/.uuid

/usr/share/fonts/X11/100dpi/.uuid

/usr/share/fonts/X11/75dpi/.uuid

/usr/share/fonts/X11/encodings/.uuid

/usr/share/fonts/X11/encodings/large/.uuid

/usr/share/fonts/X11/misc/.uuid

/usr/share/fonts/X11/Type1/.uuid

/usr/share/fonts/X11/util/.uuid

/usr/share/javascript/mathjax/fonts/HTML-CSS/TeX/otf/.uuid

/usr/share/poppler/cMap/Adobe-CNS1/.uuid         /usr/share/poppler/cMap/Adobe-GB1/.uuid         /usr/share/poppler/cMap/Adobe-Agan1/.uuid         /usr/share/poppler/cMap/Adobe-Japan1/.uuid         /usr/share/poppler/cMap/Adobe-Agan1/.uuid         /usr/share/poppler/cMap/Adobe-Agan1/.uuid         /usr/share/poppler/cMap/Adobe-Korea1/.uuid         /var/cache/man/cs/index.db         /var/cache/man/ds/index.db         /var/cache/man/ds/index.db         /var/cache/man/ld/index.db         /var/cache/man/nlu/index.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/nl/index.db         /var/cache/man/nl/i	/usr/share/pgcli/pgcli/packages/pycache/sqlcompletion.cpython-38.pyc
/usr/share/poppler/cMap/Adobe-3pan1/.uuid         /usr/share/poppler/cMap/Adobe-Japan2/.uuid         /usr/share/poppler/cMap/Adobe-Japan2/.uuid         /usr/share/poppler/cMap/Adobe-Japan2/.uuid         /usr/share/poppler/cMap/Adobe-Japan2/.uuid         /var/cache/man/cs/index.db         /var/cache/man/cs/index.db         /var/cache/man/ds/index.db         /var/cache/man/ds/index.db         /var/cache/man/ds/index.db         /var/cache/man/les/index.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/pl/mdex.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/lib/intestim/certs/default_cert.pem         /var/lib/intestim/certs/default_exp.pem         /var/lib/intestim/certs/default_exp.pem         /var/lib/intramfs-tools/5.5.0-kail2-amd64	
/usr/share/poppler/cMap/Adobe-Japan1/.uuid /usr/share/poppler/cMap/Adobe-Japan2/.uuid /usr/share/poppler/cMap/Adobe-Korea1/.uuid /var/cache/man/ds/index.db /var/cache/man/ds/index.db /var/cache/man/ds/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/jn/index.db /var/cache/man/jn/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/js/index.db /var/cache/man/js/index.db /var/cache/man/js/index.db /var/cache/man/js/index.db /var/cache/man/js/index.db /var/cache/man/js/index.db /var/ib/jnitsim/certs/default_cert.pem /var/lib/intsim/certs/default_cert.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/certs/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/intsim/setas/default_key.pem /var/lib/	
/usr/share/poppler/cMap/Adobe-Japan2/.uuid /usr/share/poppler/cMap/Adobe-Korea1/.uuid /var/cache/man/cs/index.db /var/cache/man/ds/index.db /var/cache/man/ds/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/index.db /var/cache/man/index.db /var/cache/man/index.db /var/cache/man/index.db /var/cache/man/index.db /var/cache/man/ja/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/ib/intesim/certs/default_cert.pem /var/lib/intesim/certs/default_key.pem /var/lib/intramfs-tools/5.5.0-kali1-amd64 /var/lib/intramfs-tools/5.5.0-kali1-amd64 /var/lib/lightdm/.comfig/pulse/cookie /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/mysql/aria_log.control /var/lib/mysql/aria_log.control /var/lib/mysql/aria_log.control /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.frm	
/usr/share/poppler/cMap/Adobe-Korea1/.uuid /var/cache/man/cs/index.db /var/cache/man/da/index.db /var/cache/man/da/index.db /var/cache/man/da/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/it/index.db /var/cache/man/it/index.db /var/cache/man/it/index.db /var/cache/man/it/index.db /var/cache/man/it/index.db /var/cache/man/it/index.db /var/cache/man/ja/index.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/plindex.db /var/cache/man/sv/index.db /var/cache/man/sv/index.db /var/ib/intestim/certs/default_cert.pem /var/lib/intestim/certs/default_key.pem /var/lib/intestim/certs/default_key.pem /var/lib/intestim/certs/default_key.pem /var/lib/intestim/certs/default_amd64 /var/lib/liptdm/.config/pulse/cookie /var/lib/liptdm/.config/pulse/cookie /var/lib/liptdm/.xauthority /var/lib/liptdm/.xauthority /var/lib/liptdm/.xauthority /var/lib/liptdm/.xauthority /var/lib/liptdm/.xauthority /var/lib/liptdm/.xauthority /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db /var/lib/mysql/micate.db	
/var/cache/man/cs/index.db /var/cache/man/cs/index.db /var/cache/man/de/index.db /var/cache/man/de/index.db /var/cache/man/index.db /var/cache/man/inf/index.db /var/cache/man/index.db /var/cache/man/index.db /var/cache/man/in/index.db /var/cache/man/in/index.db /var/cache/man/in/index.db /var/cache/man/nl/index.db /var/cache/man/nl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl/index.db /var/cache/man/pl_BR/index.db /var/cache/man/zh_CN/index.db /var/cache/man/zh_CN/index.db /var/cache/man/zh_CN/index.db /var/cache/man/zh_CN/index.db /var/cache/man/zh_CN/index.db /var/lib/jolus/machine-id /var/lib/jintesim/certs/default_cert.pem /var/lib/jintesim/certs/default_cert.pem /var/lib/jintesim/certs/default_cert.pem /var/lib/jintesim/certs/default_amd64 /var/lib/jintesim/certs/default_ev.pem /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ev.pem /var/lib/jintesim/certs/default_cookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/certs/default_ceookie /var/lib/jintesim/ceookie /var/lib/jintesim/ceookie /var/	
/var/cache/man/da/index.db /var/cache/man/de/index.db /var/cache/man/fr/index.db /var/cache/man/fr/index.db /var/cache/man/lit/index.db /var/cache/man/lit/index.db /var/cache/man/lit/index.db /var/cache/man/pt/index.db /var/cache/man/pt/index.db /var/cache/man/pt/index.db /var/cache/man/pt/index.db /var/cache/man/pt/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/cache/man/ru/index.db /var/lib/inetsim/certs/default_cert.pem /var/lib/inetsim/certs/default_key.pem /var/lib/inetsim/certs/default_key.pem /var/lib/initramfs-tools/5.5.0-kali2-amd64 /var/lib/lightdm/.config/pulse/cookie /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/lightdm/.xauthority /var/lib/lightdmata /var/lib/lightdata /var/lib/mysql/raia_log_control /var/lib/mysql/aria_log_folom_stats.frm /var/lib/mysql/colum_stats.frm /var/lib/mysql/colums_priv.frm /var/lib/mysql/mysql/colums_priv.frm	
/var/cache/man/de/index.db         /var/cache/man/ls/index.db         /var/cache/man/tn/index.db         /var/cache/man/in/index.db         /var/cache/man/in/index.db         /var/cache/man/in/index.db         /var/cache/man/in/index.db         /var/cache/man/nl/index.db         /var/cache/man/zh_ER/index.db         /var/lib/dus/machine-id         /var/lib/lib/dus/machine-id         /var/lib/lib/lib/lib/lib/lib/lib/li	/var/cache/man/cs/index.db
/var/cache/man/lex.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/ln/index.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/lindex.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_BR/index.db         /var/cache/man/pl_DN/index.db         /var/cache/man/pl_DN/index.db         /var/cache/man/sviindex.db         /var/lib/lub/sightam/cache/ma/sci.db         /var/lib/lub/sightam/cache/ma/sci.db         /var/lib/lib/lib/lib/lib/lib/lib/lib/lib/lib	/var/cache/man/da/index.db
/var/cache/man/fr/index.db         /var/cache/man/index.db         /var/cache/man/it/index.db         /var/cache/man/it/index.db         /var/cache/man/ja/index.db         /var/cache/man/ja/index.db         /var/cache/man/p1/index.db         /var/cache/man/p1/index.db         /var/cache/man/p1/index.db         /var/cache/man/p1/index.db         /var/cache/man/p1/index.db         /var/cache/man/p1_BR/index.db         /var/cache/man/ru/index.db         /var/cache/man/ru/index.db         /var/cache/man/sv/index.db         /var/lib/lib/lib/lib/lib/lib/lib/lib/lib/lib	/var/cache/man/de/index.db
/var/cache/man/hu/index.db         /var/cache/man/it/index.db         /var/cache/man/ja/index.db         /var/cache/man/ja/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pt/index.db         /var/cache/man/pt/index.db         /var/cache/man/pt/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/ru/index.db         /var/cache/man/zh_CN/index.db         /var/cache/man/zh_CN/index.db         /var/lib/dbus/machine-id         /var/lib/inetsim/certs/default_cert.pem         /var/lib/initramfs-tools/5.5.0-kali2-amd64         /var/lib/initramfs-tools/5.5.0-kali2-amd64         /var/lib/inghtdm/.config/pulse/cookie         /var/lib/lightdm/.gnupg/pubring.kbx         /var/lib/lightdm/.suthority         /var/lib/lightdm/.suthority         /var/lib/lightdm/.suthority         /var/lib/lightdm/_sol_ooo00001         /var/lib/mysql/aria_log_control         /var/lib/mysql/aria_log_control         /var/lib/mysql/jata1         /var/lib/mysql/mysql/colum_stats.frm         /var/lib/mysql/mysql/colum_stats.frm         /var/lib/mysql/mysql/colum_stats.frm         /var/lib/mysql/mysql/colums_priv.frm	/var/cache/man/es/index.db
/var/cache/man/index.db         /var/cache/man/ija/index.db         /var/cache/man/ja/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pt/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/sv/index.db         /var/cache/man/sv/index.db         /var/cache/man/sv/index.db         /var/lib/dbus/machine-id         /var/lib/dbus/machine-id         /var/lib/inetsim/certs/default_cert.pem         /var/lib/initramfs-tools/5.5.0-kali2-amd64         /var/lib/lightdm/.config/pulse/cookie         /var/lib/lightdm/.config/pulse/cookie         /var/lib/lightdm/.gnupg/pubring.kbx         /var/lib/lightdm/.sauthority         /var/lib/lightdm/.sauthority         /var/lib/lightdm/.sauthority         /var/lib/lightdmi_sal_og_control         /var/lib/mysql/aria_log_control         /var/lib/mysql/lodata1         /var/lib/mysql/mysql/column_stats.frm         /var/lib/mysql/mysql/column_stats.MYI         /var/lib/mysql/mysql/columns_priv.frm	/var/cache/man/fr/index.db
/var/cache/man/li/index.db         /var/cache/man/li/index.db         /var/cache/man/pl/index.db         /var/cache/man/pl/index.db         /var/cache/man/pt/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/pt_BR/index.db         /var/cache/man/ru/index.db         /var/cache/man/ru/index.db         /var/cache/man/sv/index.db         /var/cache/man/zh_CN/index.db         /var/lib/dbus/machine-id         /var/lib/dbus/machine-id         /var/lib/inetsim/certs/default_cert.pem         /var/lib/intramfs-tools/5.5.0-kali2-amd64         /var/lib/initramfs-tools/5.7.0-kali1-amd64         /var/lib/lightdm/.config/pulse/cookie         /var/lib/lightdm/.gnupg/pubring.kbx         /var/lib/lightdm/.sauthority         /var/lib/lightdm/.sauthority         /var/lib/lightdm/sauthority         /var/lib/mysql/aria_log_control         /var/lib/mysql/aria_log_control         /var/lib/mysql/ib_logfile0         /var/lib/mysql/ib_logfile0         /var/lib/mysql/mysql/column_stats.frm         /var/lib/mysql/mysql/column_stats.MYI         /var/lib/mysql/mysql/columns_priv.frm	/var/cache/man/hu/index.db
/var/cache/man/ja/index.db/var/cache/man/ja/index.db/var/cache/man/pl/index.db/var/cache/man/pt/index.db/var/cache/man/pt_BR/index.db/var/cache/man/pt_BR/index.db/var/cache/man/pt_BR/index.db/var/cache/man/pt_BR/index.db/var/cache/man/sv/index.db/var/cache/man/zh_CN/index.db/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.5.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/mysql/aria_log_0000001/var/lib/mysql/aria_log_control/var/lib/mysql/ib/data1/var/lib/mysql/column_stats.frm/var/lib/mysql/column_stats.MYI/var/lib/mysql/columns_priv.frm	/var/cache/man/index.db
/var/cache/man/nl/index.db/var/cache/man/pl/index.db/var/cache/man/pt/index.db/var/cache/man/pt_BR/index.db/var/cache/man/ru/index.db/var/cache/man/ru/index.db/var/cache/man/ru/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/lib/dbus/machine-id/var/lib/intetsim/certs/default_cert.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.xauthority/var/lib/lightdm/.xauthority/var/lib/msql/aria_log_control/var/lib/msql/aria_log_control/var/lib/msql/ib_logfile0/var/lib/msql/msql/column_stats.frm/var/lib/msql/msql/column_stats.MYI/var/lib/msql/msql/columns_priv.frm/var/lib/msql/msql/columns_priv.frm	
/var/cache/man/pl/index.db/var/cache/man/pt/index.db/var/cache/man/pt_BR/index.db/var/cache/man/ru/index.db/var/cache/man/sv/index.db/var/cache/man/zh_CN/index.db/var/cache/man/zh_CN/index.db/var/cib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.squpg/pubring.kbx/var/lib/mlocate/mlocate.db/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log_control/var/lib/mysql/ibdata1/var/lib/mysql/column_stats.frm/var/lib/mysql/column_stats.MYI/var/lib/mysql/column_priv.MYI	/var/cache/man/ja/index.db
/var/cache/man/pt/index.db/var/cache/man/pt_BR/index.db/var/cache/man/ru/index.db/var/cache/man/sv/index.db/var/cache/man/zh_CN/index.db/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lib/ithdm/.config/pulse/cookie/var/lib/inghtdm/.config/pulse/cookie/var/lib/inghtdm/.xauthority/var/lib/imysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/ib/ata1/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.frm	/var/cache/man/nl/index.db
/var/cache/man/pt_BR/index.db/var/cache/man/ru/index.db/var/cache/man/sv/index.db/var/cache/man/sv/index.db/var/lib/dbus/machine-id/var/lib/intesim/certs/default_cert.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.xauthority/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log.control/var/lib/mysql/idata1/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/colums_priv.MYI	/var/cache/man/pl/index.db
/var/cache/man/ru/index.db/var/cache/man/sv/index.db/var/cache/man/zh_CN/index.db/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/inetsim/certs/default_key.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/mocate/mlocate.db/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/ibdata1/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/columns_priv.frm/var/lib/mysql/mysql/columns_priv.frm	/var/cache/man/pt/index.db
/var/cache/man/sv/index.db/var/cache/man/zh_CN/index.db/var/lib/dbus/machine-id/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/inetsim/certs/default_key.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.control/var/lib/mysql/aria_log_control/var/lib/mysql/ib_logfile0/var/lib/mysql/column_stats.frm/var/lib/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.MYI	/var/cache/man/pt_BR/index.db
/var/cache/man/zh_CN/index.db/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/inetsim/certs/default_key.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.snupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/iblata1/var/lib/mysql/column_stats.frm/var/lib/mysql/column_stats.MYI/var/lib/mysql/column_priv.frm/var/lib/mysql/mysql/column_priv.MYI	/var/cache/man/ru/index.db
/var/lib/dbus/machine-id/var/lib/inetsim/certs/default_cert.pem/var/lib/inetsim/certs/default_key.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log_control/var/lib/mysql/ib_logfile0/var/lib/mysql/jbdata1/var/lib/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.frm/var/lib/mysql/mysql/columns_priv.MYI	/var/cache/man/sv/index.db
/var/lib/inetsim/certs/default_cert.pem/var/lib/inetsim/certs/default_key.pem/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/iblata1/var/lib/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.frm/var/lib/mysql/mysql/columns_priv.MYI	/var/cache/man/zh_CN/index.db
/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/lip/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/aria_log_control/var/lib/mysql/ib_logfile0/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/column_priv.frm/var/lib/mysql/mysql/column_priv.MYI	/var/lib/dbus/machine-id
/var/lib/initramfs-tools/5.5.0-kali2-amd64/var/lib/lip/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.xauthority/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log_0000001/var/lib/mysql/aria_log_control/var/lib/mysql/b_logfile0/var/lib/mysql/ib_ata1/var/lib/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/column_priv.frm/var/lib/mysql/mysql/column_priv.frm	/var/lib/inetsim/certs/default_cert.pem
/var/lib/initramfs-tools/5.7.0-kali1-amd64/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log_control/var/lib/mysql/ib_logfile0/var/lib/mysql/ibdata1/var/lib/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.frm	/var/lib/inetsim/certs/default_key.pem
/var/lib/lightdm/.config/pulse/cookie/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.00000001/var/lib/mysql/aria_log_control/var/lib/mysql/b_logfile0/var/lib/mysql/ibdata1/var/lib/mysql/mysql/column_stats.frm/var/lib/mysql/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.frm/var/lib/mysql/mysql/columns_priv.MYI	/var/lib/initramfs-tools/5.5.0-kali2-amd64
/var/lib/lightdm/.gnupg/pubring.kbx/var/lib/lightdm/.Xauthority/var/lib/mlocate/mlocate.db/var/lib/mysql/aria_log.0000001/var/lib/mysql/aria_log_control/var/lib/mysql/ib_logfile0/var/lib/mysql/ibdata1/var/lib/mysql/column_stats.frm/var/lib/mysql/column_stats.MYI/var/lib/mysql/mysql/columns_priv.frm/var/lib/mysql/mysql/columns_priv.frm	/var/lib/initramfs-tools/5.7.0-kali1-amd64
/var/lib/lightdm/.Xauthority /var/lib/mlocate/mlocate.db /var/lib/mysql/aria_log.00000001 /var/lib/mysql/aria_log_control /var/lib/mysql/ib_logfile0 /var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/lightdm/.config/pulse/cookie
/var/lib/mlocate/mlocate.db /var/lib/mysql/aria_log.00000001 /var/lib/mysql/aria_log_control /var/lib/mysql/ib_logfile0 /var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/lightdm/.gnupg/pubring.kbx
/var/lib/mysql/aria_log.00000001 /var/lib/mysql/aria_log_control /var/lib/mysql/ib_logfile0 /var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/lightdm/.Xauthority
/var/lib/mysql/aria_log_control /var/lib/mysql/ib_logfile0 /var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mlocate/mlocate.db
/var/lib/mysql/ib_logfile0 /var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/aria_log.0000001
/var/lib/mysql/ibdata1 /var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/aria_log_control
/var/lib/mysql/mysql/column_stats.frm /var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/ib_logfile0
/var/lib/mysql/mysql/column_stats.MYI /var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/ibdata1
/var/lib/mysql/mysql/columns_priv.frm /var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/mysql/column_stats.frm
/var/lib/mysql/mysql/columns_priv.MYI	/var/lib/mysql/mysql/column_stats.MYI
	/var/lib/mysql/mysql/columns_priv.frm
/var/lib/mysql/mysql/db.frm	/var/lib/mysql/mysql/columns_priv.MYI
	/var/lib/mysql/mysql/db.frm

/var/lib/mysql/mysql/db.MYI /var/lib/mysql/mysql/event.frm /var/lib/mysql/mysql/event.MYI
/var/lib/mysql/mysql/event.MYI
/var/lib/mysql/mysql/func.frm
/var/lib/mysql/mysql/func.MYI
/var/lib/mysql/mysql/general_log.frm
/var/lib/mysql/mysql/general_log.nm /var/lib/mysql/mysql/gtid_slave_pos.frm
/var/lib/mysql/mysql/belp_category.frm
/var/lib/mysql/mysql/help_category.MYI
/var/lib/mysql/mysql/help_keyword.frm
/var/lib/mysql/mysql/help_keyword.MYI
/var/lib/mysql/mysql/help_relation.frm
/var/lib/mysql/mysql/help_relation.MYI
/var/lib/mysql/mysql/help_topic.frm
/var/lib/mysql/mysql/help_topic.MYI
/var/lib/mysql/mysql/host.frm
/var/lib/mysql/mysql/host.MYI
/var/lib/mysql/mysql/index_stats.frm
/var/lib/mysql/mysql/index_stats.MYI
/var/lib/mysql/mysql/innodb_index_stats.frm
/var/lib/mysql/mysql/innodb_index_stats.ibd
/var/lib/mysql/mysql/innodb_table_stats.frm
/var/lib/mysql/mysql/innodb_table_stats.ibd
/var/lib/mysql/mysql/plugin.frm
/var/lib/mysql/mysql/plugin.MYI
/var/lib/mysql/mysql/proc.frm
/var/lib/mysql/mysql/proc.MYD
/var/lib/mysql/mysql/proc.MYI
/var/lib/mysql/mysql/procs_priv.frm
/var/lib/mysql/mysql/procs_priv.MYI
/var/lib/mysql/mysql/proxies_priv.frm
/var/lib/mysql/mysql/proxies_priv.MYD
/var/lib/mysql/mysql/proxies_priv.MYI
/var/lib/mysql/mysql/roles_mapping.frm
/var/lib/mysql/mysql/roles_mapping.MYI
/var/lib/mysql/mysql/servers.frm
/var/lib/mysql/mysql/servers.MYI
/var/lib/mysql/mysql/slow_log.frm
/var/lib/mysql/mysql/table_stats.frm
/var/lib/mysql/mysql/table_stats.MYI
/var/lib/mysql/mysql/tables_priv.frm

/var/lib/mysql/mysql/tables\_priv.MYI

/var/lib/mysql/mysql/time\_zone.frm

/var/lib/mysql/mysql/time\_zone.MYI

/var/lib/mysql/mysql/time\_zone\_leap\_second.frm

/var/lib/mysql/mysql/time\_zone\_leap\_second.MYI

/var/lib/mysql/mysql/time\_zone\_name.frm

/var/lib/mysql/mysql/time\_zone\_name.MYI

/var/lib/mysql/mysql/time\_zone\_transition.frm

/var/lib/mysql/mysql/time\_zone\_transition.MYI

/var/lib/mysql/mysql/time\_zone\_transition\_type.frm

/var/lib/mysql/mysql/time\_zone\_transition\_type.MYI

/var/lib/mysql/mysql/transaction\_registry.frm

/var/lib/mysql/mysql/user.frm

/var/lib/mysql/mysql/user.MYI

/var/lib/NetworkManager/timestamps

/var/lib/plymouth/boot-duration

/var/lib/postgresql/12/main/global/pg\_control

/var/lib/systemd/random-seed

Table 4 Always Unique Hash Listing

# **Appendix 2: Uniquely Named Files**

Path	
var/lib/NetworkManager/internal-016976d9-686b-40a9-a395-6c53ec16b242-eth0.l	ease
var/cache/fontconfig/02d4f520-a997-4d93-9fff-6082379a324e-le64.cache-7	
var/cache/fontconfig/c0b0467c-cc0f-4844-9c8a-27e4ffbc4834-le64.cache-7	
var/cache/fontconfig/a5e62240-c06e-4786-a111-1d916b98e579-le64.cache-7	
var/cache/fontconfig/26927276-cfe8-4d8e-b66b-5697d2ba5bb5-le64.cache-7	
var/cache/fontconfig/7231c049-01f8-4488-ac0c-b0e5c4b59ecd-le64.cache-7	
var/cache/fontconfig/f04028cc-8cf2-4a79-9217-ccb09ab5f7f5-le64.cache-7	
var/cache/fontconfig/ac2ede34-3e40-4594-9f86-03729fd892cc-le64.cache-7	
var/cache/fontconfig/564a544d-a92e-4a43-9a50-5d35b8306f57-le64.cache-7	
var/cache/fontconfig/2955b303-602c-46f4-8e44-4378d47f8400-le64.cache-7	
var/cache/fontconfig/90833a27-c08d-4e82-94df-92d24ecebbe2-le64.cache-7	
var/cache/fontconfig/586e1327-7f72-4fad-b160-c8cc02421c48-le64.cache-7	
var/cache/fontconfig/c4fa06ad-f49f-4925-a331-caffb2d66b77-le64.cache-7	
var/cache/fontconfig/136f21f7-d779-44fe-94bd-9acca931261b-le64.cache-7	
var/cache/fontconfig/0a0e8bb7-3085-40c3-8c39-e823b0f05d36-le64.cache-7	
var/cache/fontconfig/05d9d9df-8b2b-4c25-91da-3e240196b756-le64.cache-7	
var/cache/fontconfig/bda66590-93bf-4994-a514-50b9e2ec119f-le64.cache-7	
var/cache/fontconfig/1e7ae182-406c-4bec-ab4d-2d0c2bb24054-le64.cache-7	
var/cache/fontconfig/da91ae14-4828-40aa-a41a-a78c9d0a88b5-le64.cache-7	
var/cache/fontconfig/d802e684-a3fd-4627-ac3c-8582bb44db61-le64.cache-7	
var/cache/fontconfig/2ef35129-5b00-4bcd-8bcf-b1bf54d629cb-le64.cache-7	
var/cache/fontconfig/19471168-b12b-4cfe-b66d-78fa53b13167-le64.cache-7	
var/cache/fontconfig/82323306-e521-49b2-885f-e57265725cf3-le64.cache-7	
var/cache/fontconfig/2c53115d-7f38-4bfc-9172-71687740e27d-le64.cache-7	
var/cache/fontconfig/594ec2e8-d50e-45d2-b381-c21880502f86-le64.cache-7	
var/cache/fontconfig/d26e4990-f173-4e6f-8e64-a5375eb79e29-le64.cache-7	
var/cache/fontconfig/d46ee887-955a-4e71-84b1-70fcb6868152-le64.cache-7	
var/cache/fontconfig/57934f48-9bfa-45c1-bb8f-66c726d0a2b6-le64.cache-7	
var/cache/fontconfig/9cf6e8b1-bfcc-4fb9-800c-c080822c6433-le64.cache-7	
var/cache/fontconfig/ed6ec1d1-1752-496b-87c3-b9b1cc507b10-le64.cache-7	
var/cache/fontconfig/e55bbb24-eeb9-4478-a0b4-d0a88a3aceb3-le64.cache-7	
var/cache/fontconfig/a437f435-1eb7-44d5-be3d-dc6bce27adfa-le64.cache-7	
var/cache/fontconfig/761618bc-ca18-497b-ab10-b24955b0250d-le64.cache-7	
var/cache/fontconfig/1bd710f5-632e-46c7-aac0-ccbe00c423dc-le64.cache-7	
var/cache/fontconfig/34aff380-48fd-44b1-9b1d-071c52895e13-le64.cache-7	
var/cache/fontconfig/a1214b3a-75c4-4241-ad6f-692e75b8c09f-le64.cache-7	
var/cache/fontconfig/d3646869-ec44-4f6f-8a94-fa0b5b5937fc-le64.cache-7	
var/cache/fontconfig/da8b9f6d-322b-4513-8434-ac674e86cd94-le64.cache-7	
var/cache/fontconfig/5d74a0ea-6c03-47df-a268-8df6d3645fff-le64.cache-7	

/var/lib/lightdm/.config/pulse/6419ad21b7384371a12b5877060147c5-device-volumes.tdb

/var/lib/lightdm/.config/pulse/6419ad21b7384371a12b5877060147c5-default-sink

/var/lib/lightdm/.config/pulse/6419ad21b7384371a12b5877060147c5-default-source

/var/lib/lightdm/.config/pulse/6419ad21b7384371a12b5877060147c5-stream-volumes.tdb

/var/log/journal/6419ad21b7384371a12b5877060147c5/system.journal

Table 5 Uniquely Named Files