CSF lab report

Course name: COMPSCI5063 Cyber Security Fundamentals MSc - 2024-25
Group members:

Member Name + student ID	Work
Hanyi Zhang 2982164Z	Completed Lab3 experiment and report writing.
Jiaxin Cheng 2973117C	Completed Lab1 experiment and report writing.
Ziang Liu 2977952L	Completed Lab2 experiment and report writing.
Jie Zhan 2981030Z	Completed Lab2 experiment and report writing.
Wencheng Shi 2976762S	Completed Lab3 experiment and report writing.
Haokun Xie 2974555X	Completed Lab1 experiment and report writing.
Mingze Gao 2969378G	Completed Lab3 experiment and report writing.

Analysis of Sample 1

The sample1.pcap file primarily contains Spanning Tree Protocol (STP) packets. These packets are transmitted using a broadcast communication model, meaning they are sent to all devices in the network.

All the packets captured are Bridge Protocol Data Units (BPDU), which are used for STP calculations between switches to determine which paths should be blocked to prevent network loops.

These STP BPDU packets are typically sent when a switch starts up or when a network topology change occurs. They do not interfere with normal user traffic. BPDU packets are usually transmitted at 2-second intervals, which aligns with standard STP behavior. There’s no unusual or suspicious traffic was detected in this capture.

Analysis of Sample 2

The protocols in sample 2 are Ethernet and Address Resolution Protocol (ARP), which is a protocol for resolving IP addresses and MAC addresses. The communication mode is broadcast, which is used to resolve IP addresses to MAC addresses.

ARP scanning or ARP flooding may exist in the captured data. Because the time interval of each ARP protocol is very short and the number is large, multiple requests are made between 0.098 seconds and 0.110 seconds.

ARP scanning: query different IP addresses in a large number in a short period of time, explore the surviving hosts in the LAN, and find hosts with open related port numbers or services to attack.

ARP flooding: the device sends excessive ARP requests in a very short period of time. The attacker may try to overflow the ARP table of the switch, triggering network failures and affecting normal communication.

Analysis of Sample 3

The sample3.pcap file contains multiple network protocols, including Cisco Discovery Protocol (CDP), Address Resolution Protocol (ARP), Internet Protocol Version 4 (IPv4), User Datagram Protocol (UDP), Domain Name System (DNS), Internet Control Message Protocol (ICMP), and Loopback (CTP).

This capture contains loopback test traffic where all LOOP packets originate from and terminate at the same MAC address (Cisco_7c:eb:3d). These packets are transmitted at 10 second intervals and show that the Cisco device is performing routine self-diagnostic checks. The data field is filled with all zeros and the purpose of this traffic is to verify network interface functionality. The total traffic is only 17 packets (1532 bytes), so its impact on the network is negligible.

Captured CDP packets broadcast detailed device information such as hostname (gramirez-isdn.tivoli.com), IP address (172.26.112.33), hardware model (Cisco C804), and software version (Cisco IOS). While this is normal behavior for Cisco network devices, CDP broadcasts can pose a security risk as attackers could potentially use this information to identify network vulnerabilities.

In the captured DNS queries and responses, one of the devices queried picard.uthscsa.edu and successfully resolved to 129.111.30.27. No evidence of DNS spoofing or DNS tunneling was found. ICMP (ping) requests were also recorded, sent from 10.0.0.6 to 10.0.0.254, which appears to be standard network diagnostic traffic.

Lab 2

Basic information

```
Delivered-To: mariaevangelopoulou87@gmail.com
Received: by 2002:a4a:52cd:0:0:0:0:0 with SMTP id d196csp4101874oob;
        Sun, 24 Feb 2019 14:49:07 -0800 (PST)
Return-Path: <security@gla.ac.uk>
Received: from localhost (emkei.cz. [46.167.245.207])
        by mx.google.com with ESMTPS id
f77si4370373wme.16.2019.02.24.14.49.06
        for <mariaevangelopoulou87@gmail.com>
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256
bits=128/128);
        Sun, 24 Feb 2019 14:49:07 -0800 (PST)
```

Tools

We choose Visualtotal, Urlscan, and IPvoid to analysis this email.

1. VirusTotal: Detecting Known Malware and Phishing Links VirusTotal is a powerful online tool that uses multiple antivirus engines to scan URLs and email attachments, capable of detecting malware, phishing, and blacklisted domains. It checks if the

link or attachment of the email has been marked as a threat by the security database. In this lab, we use VirusTotal to analyze suspicious links to determine if it is a known phishing website. Since VirusTotal relies on existing marked threat intelligence, VirusTotal may not detect newly created phishing websites as malicious. In this case, Urlscan can be used to crawl the website and detect hidden redirects, phishing login pages, and suspicious scripts to analyze whether the email is a threat.

2. Urlscan: Analyzing URL Behavior and Detecting Phishing Tactics
   Urlscan is a web security tool that provides real-time behavioral analysis of a URL. Unlike VirusTotal, which relies on pre-existing blacklists, Urlscan actively visits the website, captures a screenshot, and tracks where the link redirects the user.
   Urlscan mainly focuses on analyzing webpage behavior and redirections. However, it does not provide information about the sender's credibility or IP reputation, meaning it cannot determine whether the email was sent from a trusted source. IPvoid can help verify the sender's authenticity by checking if the email's originating IP address is blacklisted or associated with cyber threats. Even if the URL appears safe, the sender may still be using a compromised or fraudulent mail server.
3. IPvoid: Checking Sender Reputation and Detecting Spoofing
   IPvoid allows us to check the reputation of the email sender's IP address to determine whether it has been reported for phishing, spam, or malicious activity. In our investigation, we analyzed the sender's IP (46.167.245.207) and found that it does not match the legitimate domain (security@gla.ac.uk), indicating possible email spoofing.
   IPvoid only focuses on the sender's IP reputation and does not analyze URLs or attachments for potential threats. This means even if an email originates from a compromised mail server, it does not directly tell us whether the email contains phishing links or malware. VirusTotal can scan the email's URL and attachments for malware or phishing. This ensures that even if a seemingly legitimate email passes IP verification, any embedded threats can still be detected.

Experimental steps

First open the email file (Case 01x.eml) in Foxmail to check the Email Header, paste the email header to IPvoid and use the Email Header Tracer function to get the sender's real mail server. Extract the original mail server IP address as 46.167.245.207. Use the "nslookup" command to find the corresponding IP address of security@gla.ac.uk is 130.43.187.40. These two IP addresses don't match, indicated that the sender is not trustworthy. Then check the original link it turns to http://www.digitalkingdomsecurity.com. After test it on URLscan and virustotal, the result shows that only Fortinet flagged the website as malicious, there's no anomalies in this website. It is identified as a phishing site, after the user click the link, it will turn to another website instead of the www.gla.ac.uk/security.info page.

Analysis

Identifying Sender Spoofing

The sender’s email address (security@gla.ac.uk) does not match the actual originating mail server IP (46.167.245.207), the legitimate mail server for security@gla.ac.uk should correspond to 130.43.187.40, indicating that the email was not sent from the real University of Glasgow security team, but was forged using an unauthorized mail server (emkei.cz). This confirms that it is a spoofed email sender, and the attacker is impersonating a trusted institution.

URL Redirection and Phishing Detection

The email contains a spoofed link (www.gla.ac.uk/security.info), but when hovered over, it actually redirects to http://www.digitalkingdomsecurity.com, which has nothing to do with the University of Glasgow. It redirects users to an unexpected domain, which is a common phishing tactic used to trick users into believing they are visiting a legitimate page.

Lab3

Methodology

1. Install the program and import the file

First, install the digital forensic analysis tool Autopsy. After the installation is complete, create a new case, fill in the case name, description and storage path, and ensure that the case information is consistent with the experimental objectives. Select the "Add Data Source" function, locate the downloaded image file through the file browser, and Autopsy will automatically parse the partition structure of the image. The image contains multiple logical volumes, among which the "vol_vol2" volume contains user folders and a large number of documents and image files. Autopsy will start the initial analysis, including file system parsing, metadata extraction and hash value calculation. After the analysis is completed, you can browse the file directory, timeline view and metadata summary.

2. Create a search keyword list

After the file is imported, create a new keyword list. According to the file subject in the image, enter the words related to "dog" in turn. Considering the special symbols that may exist in the file, add keywords with separators to ensure that different forms of matching are covered. After completing the list editing, save it as the built-in keyword set of Autopsy, named "Dog_Investigation". The specific list is at the end of the article.

3. Analyze based on search results

Return to the main case interface, select "Perform keyword search", load the created "Dog_Investigation" list, enable deep scan mode, and set the search scope to the entire image file system. After starting the search, Autopsy will traverse all file contents, metadata, and disk free areas. After the search is completed, the results are presented in a paged list, and each record contains the file path, keyword hit location, and context fragments. For example, the preview of "3103_dogs.pdf" shows "testing to prove «dog« parentage", while "management.pdf" matches "«Dog« culls" and "regulatory framework for «dog breeding«".

Keyword List

Exact Match

dog, dogs, puppy, puppies, canine, k9, pet dog, stray dog, dog meat, dog breeding, Tibetan Mastiff, Husky, Golden Retriever, Pitbull, dog fighting, illegal breeding, dog trafficking, dog chip, dog vaccine, dog abuse, dog theft, dog farm, dog dealer, dog slaughter, dog medication, xylazine, rabies vaccine, microchip ID, illegal breeding

Substring Match

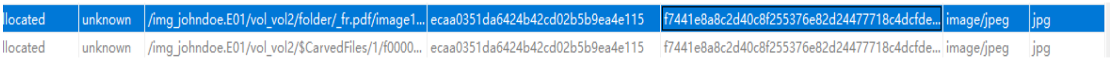
d*g, d0g, d0gs, dog*list*, dog*.jpg, dog*.pdf, dog*.xlsx, dog*, puppy*, canine*, fight*, abuse*, farm*, dealer*, transaction*, slaughter*, k9*

Regular Expression

("dog" OR "dogs"), ("puppy" OR "puppies"), ("canine" OR "k9"), dog*fight, (illegal OR unlicensed) AND dog, dog AND (abuse OR trafficking)

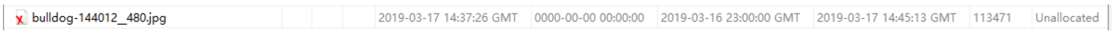
Finding and Analysis

Through in-depth detection of the target system files, it was found that there was a set of identical image files in the repository, and binary data comparison confirmed that their hash values were exactly the same.



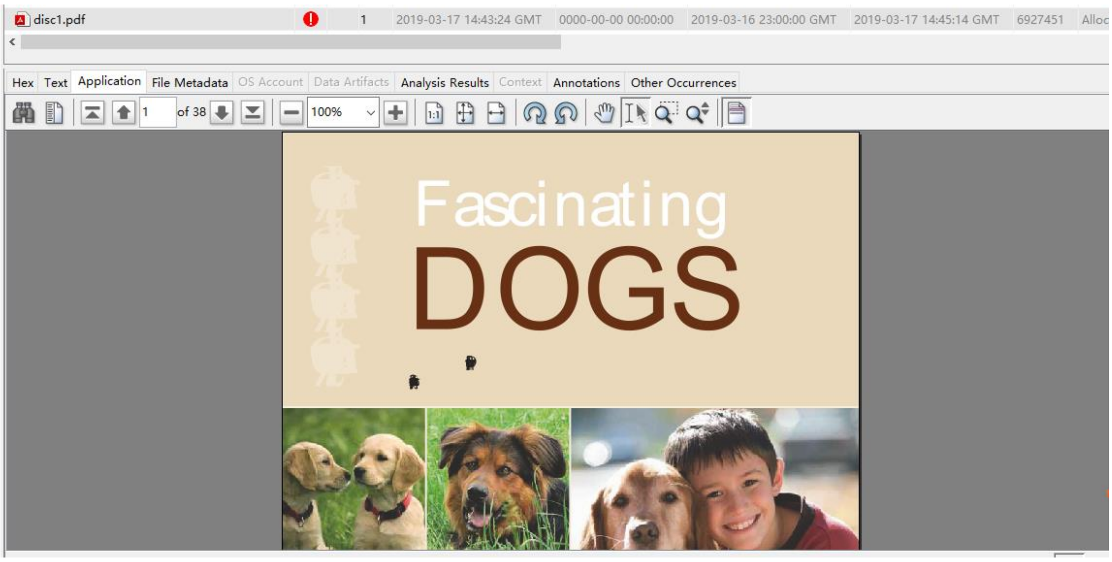
llocated	unknown	/img_johndoe.E01/vol_vol2/folder/_fr.pdf/image1...	ecaa0351da6424b42cd02b5b9ea4e115	f7441e8a8c2d40c8f255376e82d24477718c4dcfde...	image/jpeg	jpg
llocated	unknown	/img_johndoe.E01/vol_vol2/$CarvedFiles/1/f0000...	ecaa0351da6424b42cd02b5b9ea4e115	f7441e8a8c2d40c8f255376e82d24477718c4dcfde...	image/jpeg	jpg

After checking the timeline, we found that this group of images had significant metadata anomalies, the file creation time (2019-03-17 23:37:26) was later than the last modification time (2019-03-17 23:45:13). This time inversion phenomenon violates the basic file management logic of the operating system. After further expanding the scope of investigation, 19 additional abnormal files of the same type were found, all of which showed the characteristic that the creation time lagged behind the modification time, which was suspected to be traces of human tampering with file attributes.



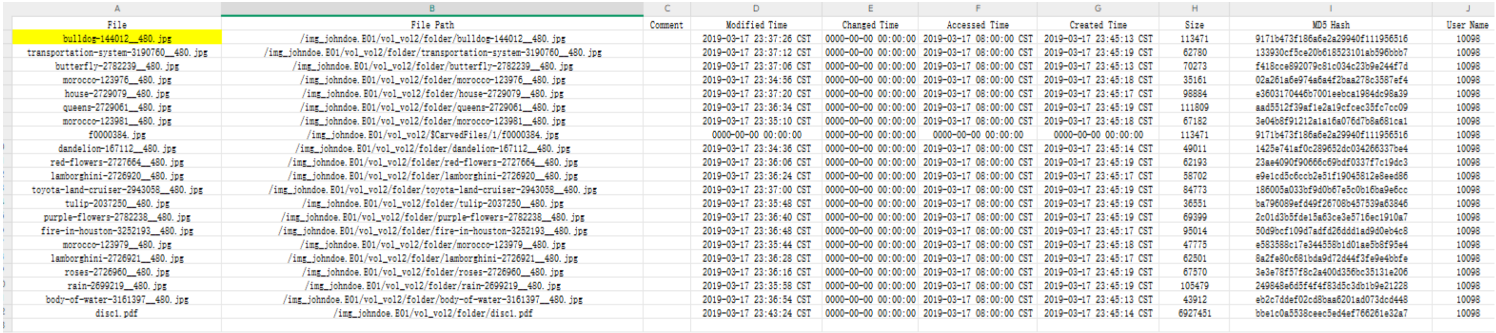
bulldog-144012_480.jpg			2019-03-17 14:37:26 GMT	0000-00-00 00:00:00	2019-03-16 23:00:00 GMT	2019-03-17 14:45:13 GMT	113471	Unallocated

An encrypted file disc1.pdf marked as "bad_item.enc" was found in the core directory. Its pseudo-password "pup" was successfully cracked through password cracking, and a PDF document with the theme of fantastic dogs was obtained after decryption. After content analysis, the document format is complete and the data is logically self-consistent, and no traces of steganography or abnormal code injection were detected.



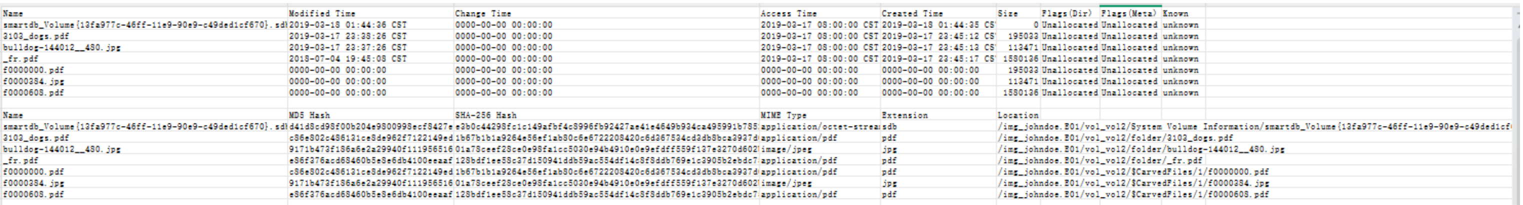
disc1.pdf 1 2019-03-17 14:43:24 GMT 0000-00-00 00:00:00 2019-03-16 23:00:00 GMT 2019-03-17 14:45:14 GMT 6927451 Alloc

Evidence List



File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size	MD5 Hash	User Name
bulldog-144012__480.jpg	/img_johndoe.E01/vol_vol2/folder/bulldog-144012__480.jpg		2019-03-17 23:37:26 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:13 CST	113471	9171b473f186a6e2a29940f111956516	10098
transportation-system-3190760__480.jpg	/img_johndoe.E01/vol_vol2/folder/transportation-system-3190760__480.jpg		2019-03-17 23:37:12 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	62780	133930cf5ce20b618523101ab596bbb7	10098
butterfly-2782239__480.jpg	/img_johndoe.E01/vol_vol2/folder/butterfly-2782239__480.jpg		2019-03-17 23:37:06 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:13 CST	70273	f418cce892079c81c034c23b9e244f7d	10098
morocco-123976__480.jpg	/img_johndoe.E01/vol_vol2/folder/morocco-123976__480.jpg		2019-03-17 23:34:56 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:18 CST	35161	02a261a6e974a6a4f2baa278c3587ef4	10098
house-2729079__480.jpg	/img_johndoe.E01/vol_vol2/folder/house-2729079__480.jpg		2019-03-17 23:37:20 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:17 CST	98884	e3603170446b7001eebca1984dc98a39	10098
queens-2729061__480.jpg	/img_johndoe.E01/vol_vol2/folder/queens-2729061__480.jpg		2019-03-17 23:36:34 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	111809	aad5512f39af1e2a19cfcec35fc7cc09	10098
morocco-123981__480.jpg	/img_johndoe.E01/vol_vol2/folder/morocco-123981__480.jpg		2019-03-17 23:35:10 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:18 CST	67182	3e04b8f91212a1a16a076d7b8a681ca1	10098
f0000384.jpg	/img_johndoe.E01/vol_vol2/$CarvedFiles/1/f0000384.jpg		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	113471	9171b473f186a6e2a29940f111956516	10098
dandelion-167112__480.jpg	/img_johndoe.E01/vol_vol2/folder/dandelion-167112__480.jpg		2019-03-17 23:34:36 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:14 CST	49011	1425e741af0c289652dc034266337be4	10098
red-flowers-2727664__480.jpg	/img_johndoe.E01/vol_vol2/folder/red-flowers-2727664__480.jpg		2019-03-17 23:36:06 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	62193	23ae4090f90666c69bdf0337f7c19dc3	10098
lamborghini-2726920__480.jpg	/img_johndoe.E01/vol_vol2/folder/lamborghini-2726920__480.jpg		2019-03-17 23:36:24 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:17 CST	58702	e9e1cd5c6ccb2e51f19045812e8eed86	10098
toyota-land-cruiser-2943058__480.jpg	/img_johndoe.E01/vol_vol2/folder/toyota-land-cruiser-2943058__480.jpg		2019-03-17 23:37:00 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	84773	186005a033bf9d0b67e5c0b16ba9e6cc	10098
tulip-2037250__480.jpg	/img_johndoe.E01/vol_vol2/folder/tulip-2037250__480.jpg		2019-03-17 23:35:48 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	36551	ba796089efd49f26708b457539a63846	10098
purple-flowers-2782238__480.jpg	/img_johndoe.E01/vol_vol2/folder/purple-flowers-2782238__480.jpg		2019-03-17 23:36:40 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	69399	2c01d3b5fde15a63ce3e5716ec1910a7	10098
fire-in-houston-3252193__480.jpg	/img_johndoe.E01/vol_vol2/folder/fire-in-houston-3252193__480.jpg		2019-03-17 23:36:48 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:17 CST	95014	50d9bcf109d7adfd26ddd1ad9d0eb4c8	10098
morocco-123979__480.jpg	/img_johndoe.E01/vol_vol2/folder/morocco-123979__480.jpg		2019-03-17 23:35:44 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:18 CST	47775	e583588c17e344558b1d01ae5b8f95e4	10098
lamborghini-2726921__480.jpg	/img_johndoe.E01/vol_vol2/folder/lamborghini-2726921__480.jpg		2019-03-17 23:36:28 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:17 CST	62501	8a2fe80c681bda9d72d44f3fe9e4bbfe	10098
roses-2726960__480.jpg	/img_johndoe.E01/vol_vol2/folder/roses-2726960__480.jpg		2019-03-17 23:36:16 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	67570	3e3e78f57f8c2a400d356bc35131e206	10098
rain-2699219__480.jpg	/img_johndoe.E01/vol_vol2/folder/rain-2699219__480.jpg		2019-03-17 23:35:58 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:19 CST	105479	249848e6d5f4f4f83d5c3db1b9e21228	10098
body-of-water-3161397__480.jpg	/img_johndoe.E01/vol_vol2/folder/body-of-water-3161397__480.jpg		2019-03-17 23:36:54 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:13 CST	43912	eb2c7ddef02cd8baa6201ad073dcd448	10098
disc1.pdf	/img_johndoe.E01/vol_vol2/folder/disc1.pdf		2019-03-17 23:43:24 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:14 CST	6927451	bbe1c0a5538ceec5ed4ef766261e32a7	10098

Unallocated file



Name	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
smartdb_Volume{13fa977c-46ff-11e9-90e9-c49ded1cf670}.sd	2019-03-18 01:44:36 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-18 01:44:35 CS	0	Unallocated	Unallocated	unknown
3103_dogs.pdf	2019-03-17 23:38:26 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:12 CS	195033	Unallocated	Unallocated	unknown
bulldog-144012__480.jpg	2019-03-17 23:37:26 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:13 CS	113471	Unallocated	Unallocated	unknown
_fr.pdf	2018-07-04 19:45:08 CST	0000-00-00 00:00:00	2019-03-17 08:00:00 CST	2019-03-17 23:45:17 CS	1580136	Unallocated	Unallocated	unknown
f0000000.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	195033	Unallocated	Unallocated	unknown
f0000384.jpg	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	113471	Unallocated	Unallocated	unknown
f0000608.pdf	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	1580136	Unallocated	Unallocated	unknown

Name	MD5 Hash	SHA-256 Hash	MIME Type	Extension	Location
smartdb_Volume{13fa977c-46ff-11e9-90e9-c49ded1cf670}.sd	d41d8cd98f00b204e9800998ecf8427e	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b785	application/octet-strea	sdb	/img_johndoe.E01/vol_vol2/System Volume Information/smartdb_Volume{13fa977c-46ff-11e9-90e9-c49ded1cf
3103_dogs.pdf	c86e802c486131ce8de962f7122149ed	1b67b1b1a9264e56ef1ab80c6e672220842 0c6d367534cd3db8bca3937d	application/pdf	pdf	/img_johndoe.E01/vol_vol2/folder/3103_dogs.pdf
bulldog-144012__480.jpg	9171b473f186a6e2a29940f111956516	01a78ceef28ce0e98fa1cc5030e94b4910e0e9efdff559f137e3270d602	image/jpeg	jpg	/img_johndoe.E01/vol_vol2/folder/bulldog-144012__480.jpg
_fr.pdf	e86f376acd68460b5e8e6db4100eeaaf	128bdf1ee58c37d150941ddb59ac554df14c8f8ddb769e1c3905b2ebdc7	application/pdf	pdf	/img_johndoe.E01/vol_vol2/folder/_fr.pdf
f0000000.pdf	c86e802c486131ce8de962f7122149ed	1b67b1b1a9264e56ef1ab80c6e672220842 0c6d367534cd3db8bca3937d	application/pdf	pdf	/img_johndoe.E01/vol_vol2/$CarvedFiles/1/f0000000.pdf
f0000384.jpg	9171b473f186a6e2a29940f111956516	01a78ceef28ce0e98fa1cc5030e94b4910e0e9efdff559f137e3270d602	image/jpeg	jpg	/img_johndoe.E01/vol_vol2/$CarvedFiles/1/f0000384.jpg
f0000608.pdf	e86f376acd68460b5e8e6db4100eeaaf	128bdf1ee58c37d150941ddb59ac554df14c8f8ddb769e1c3905b2ebdc7	application/pdf	pdf	/img_johndoe.E01/vol_vol2/$CarvedFiles/1/f0000608.pdf