VILNIAUS GEDIMINAS TECHNICAL UNIVERSITY

FACULTY OF FUNDAMENTAL SCIENCES

DEPARTMENT OF INFORMATION SYSTEMS

DIGITAL FORENSIC REPORT

CASE 00001

Investigator: Elbayi Asgarov

Date: 14.10.2021

Abstract

This document is submitted as the practical part of the Cyber Forensics program.

This practical is in two parts, the first of which required recovery of partitions. During this part, the investigator recovered deleted partitions using Active@ Undelete Recovery, Disk Drill, Autopsy and Hiren Boot CD (Lazasoft Data Recovery). The conclusion is that the owner of the hard drive was member of a cyber attacker's group called 'Cyber Bunny' which was distributing malware. Images with specific dates and suspected faces, encrypted archives, and other system files necessary for the investigation were recovered.

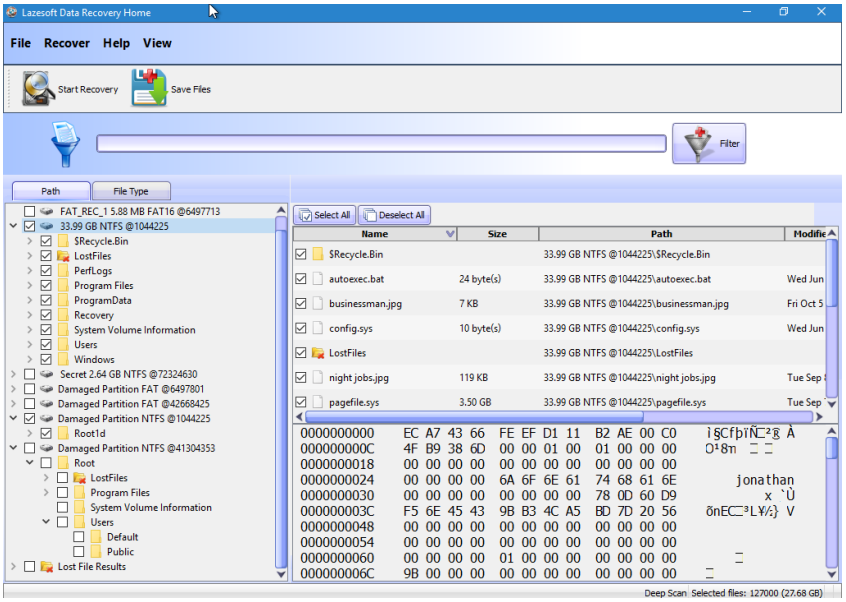
In the second part, further investigation was carried based on disk image evidence recovered from hard drive. One of the images contained some documents, videos, and archives ranging from 1993 to 2004. Nothing related to group members was found inside images.

1st Part of the Investigation

Description	Maxtor M3 HDD 1TB
Serial Number of the item	NM13RT4R

After the item was handed to forensic investigator disk image was taken from drive using FTK Imager and was mounted using Arsenal Image Mounter only for read to block alterations.

For recovery of deleted partitions, Lazasoft Data Recovery detected 3 unique partitions with data, one of them was partition with system files and all contained some secret files related to malware distribution plan and group members.



Source File	S	C	O	Name	Domain	Version	Processor Architecture	Temporary Files Directory
SYSTEM				JONATHAN		Windows_NT	x86	%SystemRoot%\TEMP
SOFTWARE								

The name of the owner is Jonathan and has association with user john and three OS accounts were on 10.09.2019:

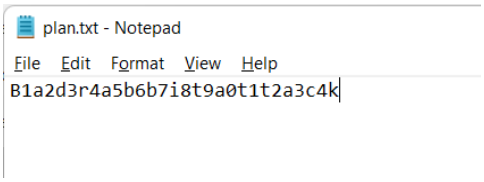
Name	Login Name	Realm Name	Creation Time
S-1-5-21-2254694460-761781497-156424663-500	Administrator		2019-09-10 10:06:20 EEST
S-1-5-21-2254694460-761781497-156424663-501	Guest		2019-09-10 10:06:20 EEST
S-1-5-21-2254694460-761781497-156424663-1000	john		2019-09-10 00:06:31 EEST

a) Partition I:

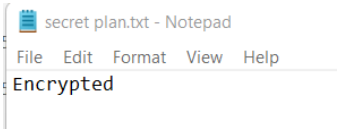
Name	Secret NTFS @72324630
Size	206 MB
Content	15 files, 6 folders

$RECYCLE.BIN	11/5/2021 3:16 AM	File folder	
LostFiles	11/5/2021 3:16 AM	File folder	
System Volume Information	11/5/2021 3:16 AM	File folder	
encase_forensic_imager__x64)_709.exe	9/13/2019 11:22 AM	Application	24,556 KB
OxyForensic_Setup.exe	9/13/2019 11:23 AM	Application	160,629 KB
plan.txt	9/9/2020 12:02 AM	Text Document	1 KB
secret plan.txt	9/13/2019 11:24 AM	Text Document	1 KB
WinHex.exe	9/13/2019 11:23 AM	Application	2,523 KB
WinHex64.exe	9/13/2019 11:23 AM	Application	3,326 KB

Name	plan.txt
Hash	26e8924a242473a8e687066955e3e933
Date created	Sep. 9, 2020, 12:01AM
Location	//SECRET/



Name	secret plan.txt
Hash	def09fa4a833717d38298eb37c861af8
Date created	Sep. 13, 2019, 11:24AM
Location	//SECRET/



In addition to these files, some forensic tool installers also were found:

WinHex.exe, OxyForensicSetup.exe, encase_forensic_imager_x64.exe

b) Partition II:

Name	Damaged Partition NTFS @1044225
Size	13.8 GB
Content	63511 files, 11026 folders

Name	businessman.jpg
Hash	a380b93d01c66e886f67be0eaaaf8ae3
Date created	Sep. 13, 2019, 01:51AM
Location	//DP NTFS @1044225/

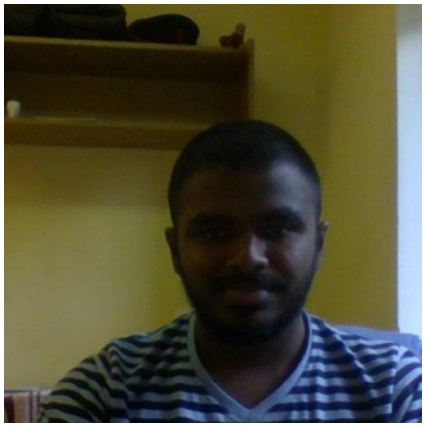
Name	night jobs.jpg
Hash	217697d481900729d21e89d2771bfe59
Date created	Sep. 9, 2020, 12:09AM
Location	//DP NTFS @1044225/

Name	Billion Dollars.jpg
Hash	4c519b1fd390fa0ac4bc015f2b92c6c3
Date created	Sep. 13, 2019, 01:49AM
Location	//DP NTFS @1044225/Users/

Name	control center.jpg
Hash	18286e7889e49577e7d58747897a26bf
Date created	Sep. 9, 2020, 12:08AM
Location	//DP NTFS @1044225/Users/

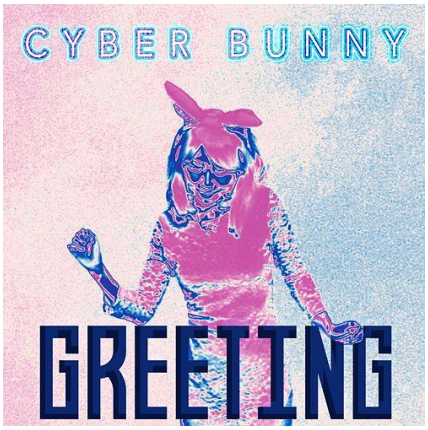
Name	armour.jpg
Hash	94fa6e3e37fd2c7ecd9a12dea1b97e33
Date created	Sep. 9, 2020, 12:07AM
Location	//DP NTFS @1044225/Users/john/Documents/

Name	lady.jpg
Hash	bef950d6ddfe4243a5879e52b15d0692
Date created	Sep. 13, 2019, 01:48AM
Location	//DP NTFS @1044225/Users/john/Documents/



Name	marine.jpg
Hash	9fc18962383ba3b8bf85ac28f30d69b7
Date created	Sep. 13, 2019, 01:49AM
Location	//DP NTFS @1044225/Users/john/Downloads/

Name	Cyberchase_Logo_April_2014.png
Hash	97c1f07a5998e49c382665ad4e5aa10d
Date created	Sep. 8, 2021, 12:08AM
Location	//DP NTFS @1044225/Users/john/Downloads/



Name	defacement.jpg
Hash	c525646dc5a027aba501eae14701cbe1
Date created	Sep. 9, 2020, 12:07AM
Location	//DP NTFS @1044225/Users/john/Music/

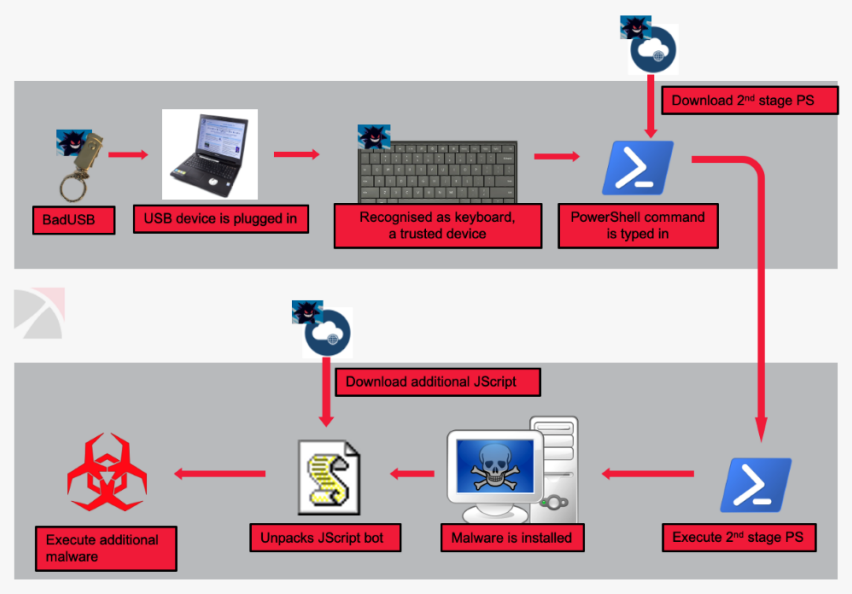
Name	DJ Coins.jpg
Hash	f78258902d6c5791208a00abb392b5c9
Date created	Sep. 13, 2019, 01:50AM
Location	//DP NTFS @1044225/Users/john/Music/

Name	present.jpeg
Hash	26ed3b1750d31cb60b17c85fc200a0c0
Date created	Sep. 9, 2020, 12:10AM
Location	//DP NTFS @1044225/Users/john/Pictures/

EXIF metadata shows that this was captured using Canon EOS 1000D:

present.jpeg			4	2017-12-24 17:34:30 EET	Canon EOS 1000D	Canon

Name	present.jpeg
Hash	30e6de838db8d7b9c0a8391cd1ab2b87
Date created	Sep. 8, 2021, 12:05AM
Location	//DP NTFS @1044225/Users/john/Pictures/



Name	badusb-attack.png
Hash	46219ac82504cbea035f49eab3705504
Date created	Sep. 8, 2021, 12:05AM
Location	//DP NTFS @1044225/Users/john/Pictures/

Name	badrabbit.png
Hash	68ab94e5c836f1d99e9bf7d8a51fc71a
Date created	Sep. 8, 2021, 12:11AM
Location	//DP NTFS @1044225/Users/john/Videos/

Name	ransom index.jpg
Hash	910a52e546811a7f493164bf38c1d1c1
Date created	Sep. 9, 2020, 12:10AM
Location	//DP NTFS @1044225/PerfLogs/Admin/

Inside `/Users/john/Favorites/` directory a few link files and bookmarks (Autopsy) were found which are also related to group's malware with already known attack vectors and intentions.

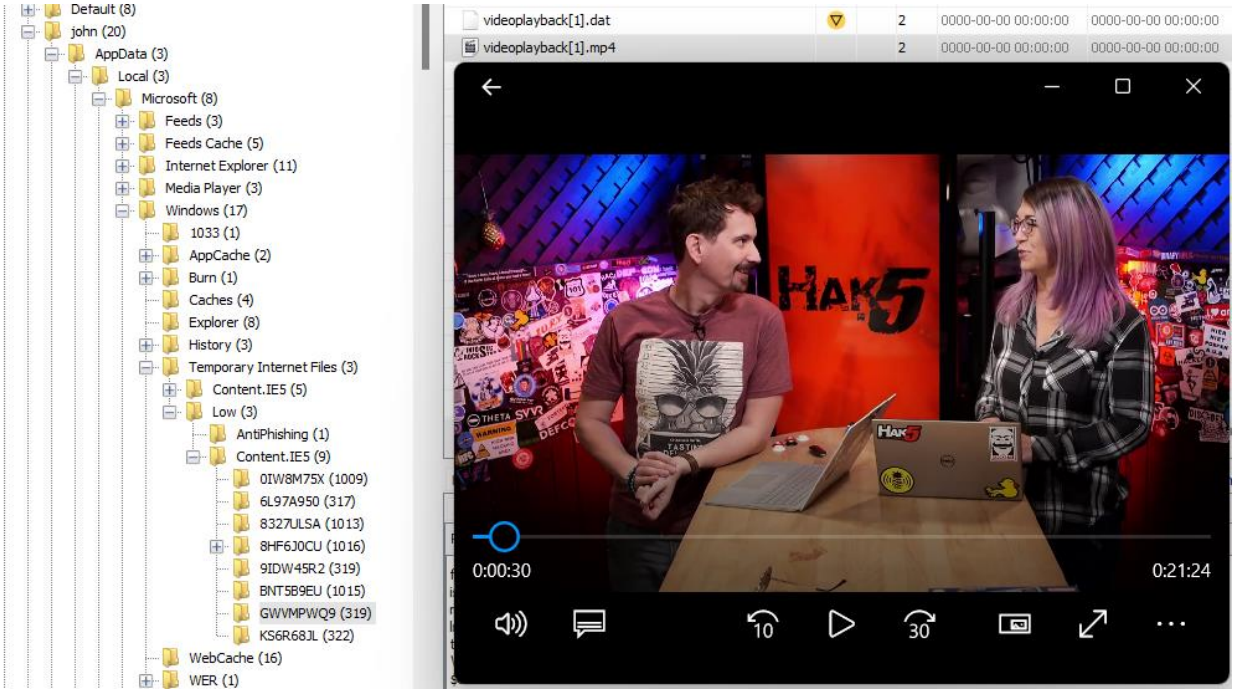
Bad Rabbit – What you need to know about this ransomware and its prevention?

February 14, 2019 | By admin ★★★★★ *(6 votes, 5.00 / 5*

Ransomware is a malicious software, that secretly downloads on to a computer and warns the user to delete or revoke access to their data. When the hacker has full control of the computer or network, they demand a ransom normally through cryptocurrency to restore the access to the files.

Of late, the ransomware attacks are increasing drastically, with this the enterprise data has become more vulnerable to cybercriminals in recent years. Thereby, it is important to have an antivirus program installed on computers, systems, and corporate network to evade all types of cyber-attacks. Bad Rabbit is one of

Inside temporary internet files directory, this video is also stored in cache:



Rare BadUSB attack detected in the wild against US hospitality provider

Hackers use snail-mail to send target company an envelope with a malware-laced USB thumb drive.

By Catalin Cimpanu for Zero Day | March 26, 2020 | Topic: Security

A US hospitality provider has recently been the target of an incredibly rare BadUSB attack, ZDNet has learned from cyber-security firm Trustwave.

The attack happened after the company received an envelope containing a fake BestBuy gift card, along with a USB thumb drive.

The receiving company was told to plug the USB thumb drive into a computer to access a list of items the gift card could be used for.

RELATED

Online safety and end-to-end encryption can co-exist, says data protection watchdog. But how?
Security

Microsoft just expanded its malware protection for Linux servers
Security

Get patching: Cisco warns of these critical product vulnerabilities
Security

Cyberchase

From Wikipedia, the free encyclopedia

This article is about the educational children's television series. For other uses, see Cyberchase (disambiguation).

Cyberchase is an animated children's television series on PBS Kids. The series focuses around three children from Earth: Jackie, Matt, and Inez. They were brought into Cyberspace, a digital universe, in order to protect the world from the villain Hacker.[4] These kids are able to prevent Hacker from taking over Cyberspace by means of problem-solving skills in conjunction with basic math, environmental science, and wellness. In Cyberspace, they meet Digit, a "cybird" who helps them on their missions.[5]

Cyberchase was created by Thirteen and debuted on January 21, 2002. In 2010, after the season eight finale, *Cyberchase* went on hiatus, but it returned in 2013 for a ninth season,[6] followed by a tenth season in 2015.[7] The eleventh season premiered on October 23, 2017,[8] and the twelfth season premiered on April 19, 2019.

A thirteenth season has been confirmed, October 19, 2020. Though it is unknown when it will be released.[9]

Contents [hide]

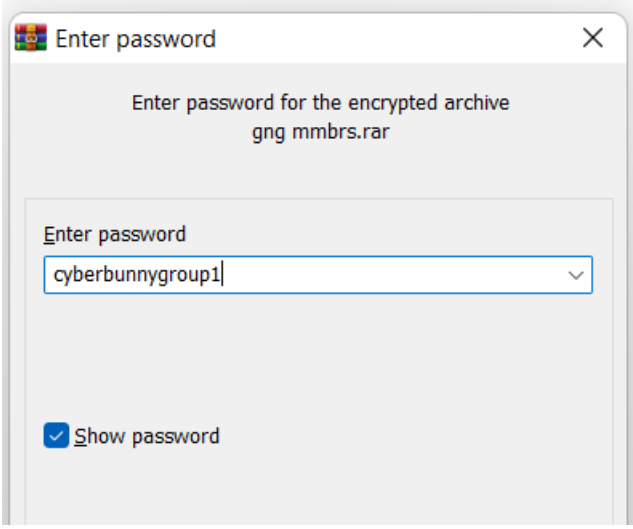
Cyberchase

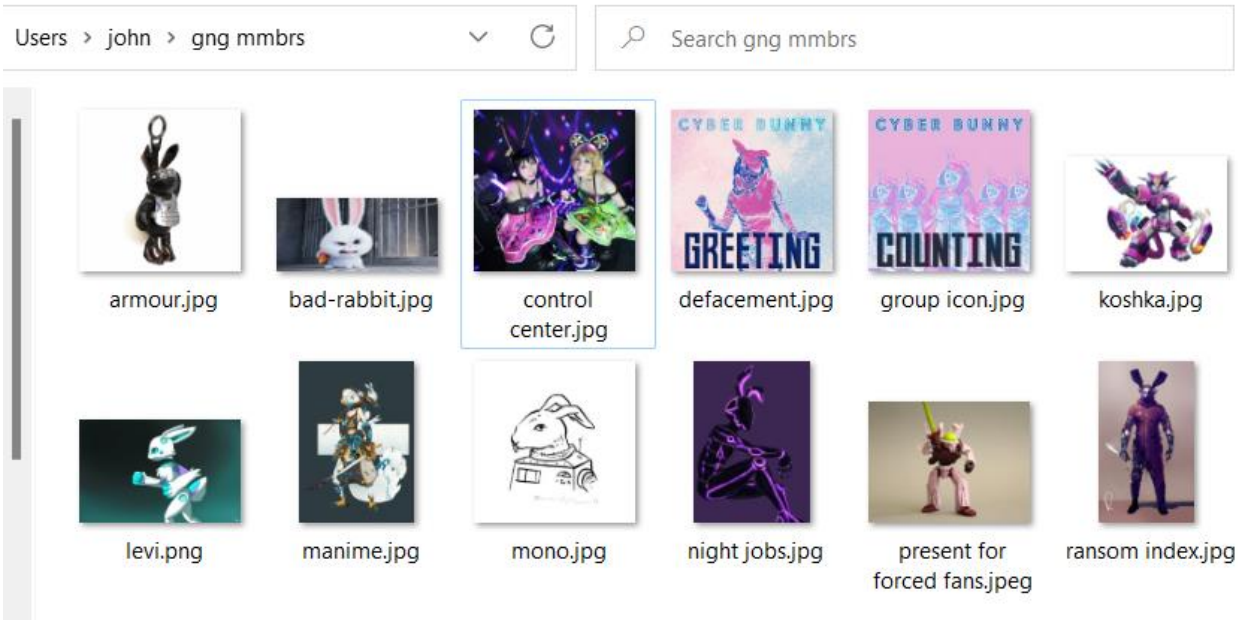
From left to right: Matt, Jackie and Inez

Source File	S	C	O	URL	Title
Bad Rabbit How to Prevent Bad Rabbit Ransomware Attacks.url			3	https://antivirus.comodo.com/blog/comodo-news/bad-rabb…	Bad Rabbit How to Prevent Bad Rabbit Ransomware Attac…
Bash Bunny Phishing Attack With Hamsters - Hak5 2306 [Cyber Security Education] - YouTube.url			3	https://www.youtube.com/watch?v=TYR2a2XoK3A	Bash Bunny Phishing Attack With Hamsters - Hak5 2306 [C…
Cyberchase - Wikipedia.url			3	https://en.wikipedia.org/wiki/Cyberchase	Cyberchase - Wikipedia.url
Suggested Sites.url			3	https://ieonline.microsoft.com/#ieslice	Suggested Sites.url
Web Slice Gallery.url			3	http://go.microsoft.com/fwlink/?LinkId=121315	Web Slice Gallery.url
GobiernoUSA.gov.url			3	http://go.microsoft.com/fwlink/?LinkId=129792	GobiernoUSA.gov.url
USA.gov.url			3	http://go.microsoft.com/fwlink/?LinkId=129791	USA.gov.url
PancakeBunny Attacked With Massive $200M Flash Loan Exploit - BeInCrypto.url			3	https://beincrypto.com/pancakebunny-attacked-massive-2…	PancakeBunny Attacked With Massive $200M Flash Loan E…
Rare BadUSB attack detected in the wild against US hospitality provider ZDNet.url			3	https://www.zdnet.com/article/rare-badusb-attack-detect…	Rare BadUSB attack detected in the wild against US hospit…

Name	gng mmbrs.rar
Hash	9f9569d7e94a494900550d286a7887fd
Date created	Sep. 9, 2020, 12:09AM
Location	//DP NTFS @1044225/Users/john/

The password of one of the archives was found via dictionary attack with 1 million passwords. This archive contains images of group members:





control center.jpg	18286e7889e49577e7d58747897a26bf
defacement.jpg	c525646dc5a027aba501eae14701cbe1
bad-rabbit.jpg	53a2eebce5f7d8d7dd084aa5cc3f81db
group icon.jpg	e4bee83c08490285c0197f3ad8d6c953
koshka.jpg	4e510938d55e1d53142a208cf359ac36
levi.png	1be661d877a0807aa284f0712cc92445
manime.jpg	f12a7d00c90b43e7c2ded42de6ce35b4
mono.jpg	b51e035cdffd365bffebb1d0f9fd822b
night jobs.jpg	217697d481900729d21e89d2771bfe59
present for forced fans.jpeg	26ed3b1750d31cb60b17c85fc200a0c0
ransom index.jpg	910a52e546811a7f493164bf38c1d1c1
armour.jpg	94fa6e3e37fd2c7ecd9a12dea1b97e33

didi image

Name	didi
Hash	0069813c892a462f88dc6d376624f7d9
Date created	Sep. 13, 2019, 01:54AM
Location	//DP NTFS @1044225/Users/
Size	61.9 MB

1.dd

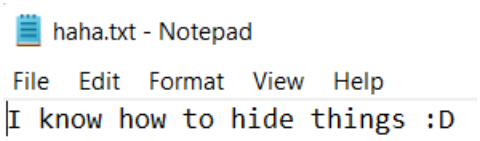
Name	1.dd
Hash	4aeb06ecd361777242ab78735d51ace6
Date created	Sep. 13, 2019, 01:55AM
Location	//DP NTFS @1044225/Windows/Help
Size	5.87 MB

2.dd

Name	2.dd
Hash	6cbd2c5248fa7030d699eb6cde051623

Date created	Sep. 13, 2019, 01:55AM
Location	//DP NTFS @1044225/Users/john/Documents/
Size	123 MB

In the directory where 2.dd file was found haha.txt file also was there with following content:



Name	haha.txt
Hash	064982681a6ba553b8af7a66220261ad
Date created	Sep. 9, 2020, 12:18AM
Location	//DP NTFS @1044225/Users/john/Documents/

In Autopsy lnk files shows recently accessed files (We can see that some files from attached E drive were opened):

Source File	S	C	O	Path	Date Accessed	Data Source
archive pass.lnk				E:\office\1\pics pack\archive pass.txt	0000-00-00 00:00:00	LogicalFileSet1
badrabbit.png.lnk				C:\Users\john\Videos\badrabbit.png	0000-00-00 00:00:00	LogicalFileSet1
badusb-attack.png.lnk				C:\Users\john\Pictures\badusb-attack.png	0000-00-00 00:00:00	LogicalFileSet1
badusb-letter.jpg.lnk				C:\Users\john\Pictures\badusb-letter.jpg	0000-00-00 00:00:00	LogicalFileSet1
Cyberchase_Logo_April_2014.png.lnk				C:\Users\john\Pictures\Cyberchase_Logo_April_2014.png	0000-00-00 00:00:00	LogicalFileSet1
haha.txt.lnk				C:\Users\john\Documents\haha.txt	0000-00-00 00:00:00	LogicalFileSet1
pics pack.lnk				E:\office\1\pics pack	0000-00-00 00:00:00	LogicalFileSet1
Pictures.lnk				C:\Users\john\AppData\Roaming\Microsoft\Windows\Librar...	0000-00-00 00:00:00	LogicalFileSet1
plan.txt.lnk				E:\plan.txt	0000-00-00 00:00:00	LogicalFileSet1
secret plan.lnk				E:\secret plan.txt	0000-00-00 00:00:00	LogicalFileSet1
Secret _E).lnk				E:\	0000-00-00 00:00:00	LogicalFileSet1
System and Security.lnk				No preferred path found	0000-00-00 00:00:00	LogicalFileSet1
Videos.lnk				C:\Users\john\AppData\Roaming\Microsoft\Windows\Librar...	0000-00-00 00:00:00	LogicalFileSet1
NTUSER.DAT				C:\Windows\system32\compmgmt.msc		LogicalFileSet1

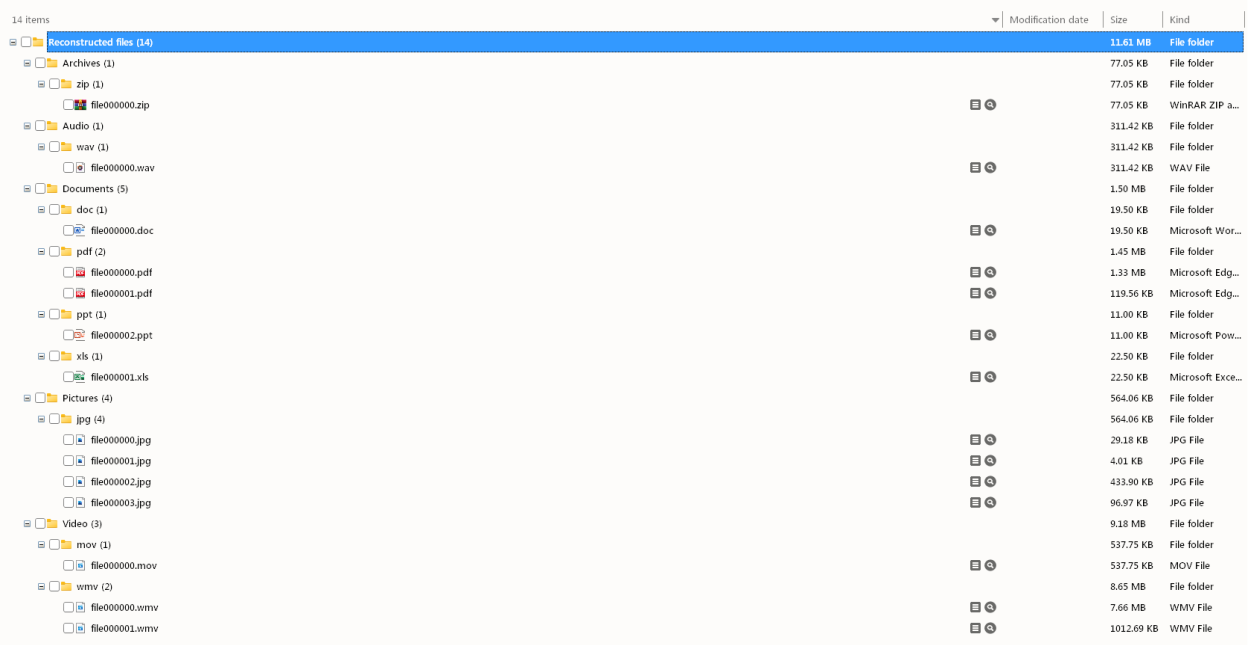
2nd part

3 dd images were analyzed using Disk Drill 2.0 (because newer versions didn't discover any files) and disk images were mounted via Arsenal Image Mounter. Inside one (didi) of them some files were found.

No system files were found, following artifacts were found.

a) file000000.pdf was published in 1994 by IEEE. And references used for this article also were before this date.
b) file000001.pdf was made in 2000.
c) Word 2003 was supported by OS.
d) ppt file was created on Microsoft PowerPoint 97-2003 format.
e) EXIF metadata of video file(file000000.wmv) was analyzed and revealed that it was captured 27.04.2002.
f) file000001.wmv on 28.02.2004.

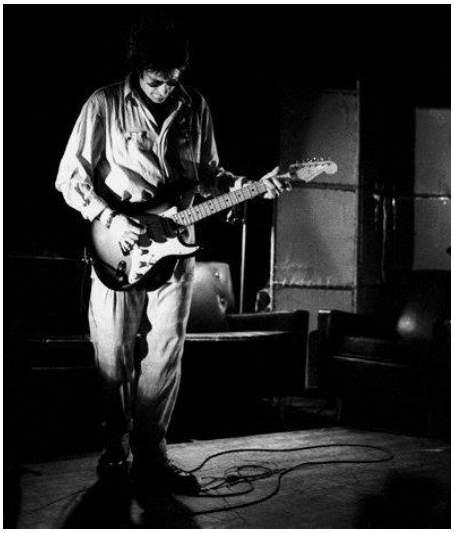
Name	didi
Content	13 Files
Size	11.6 MB



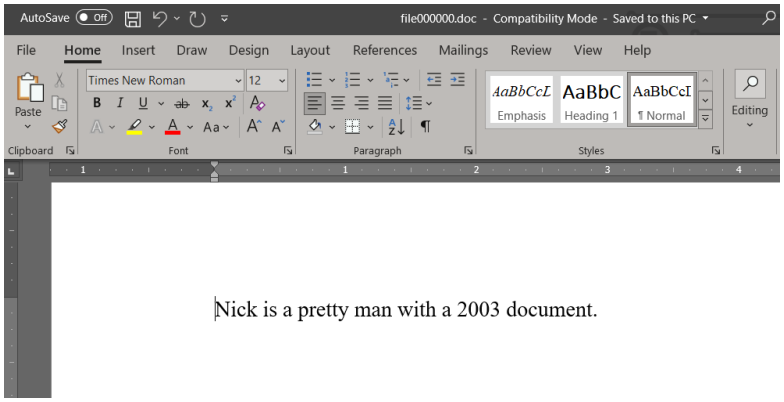
Name	file000003.jpg
Hash	d83428b8742a075b57b0dc424cd297c4

Name	file000001.jpg
Hash	81070c30e857bddcd269ac133929191f

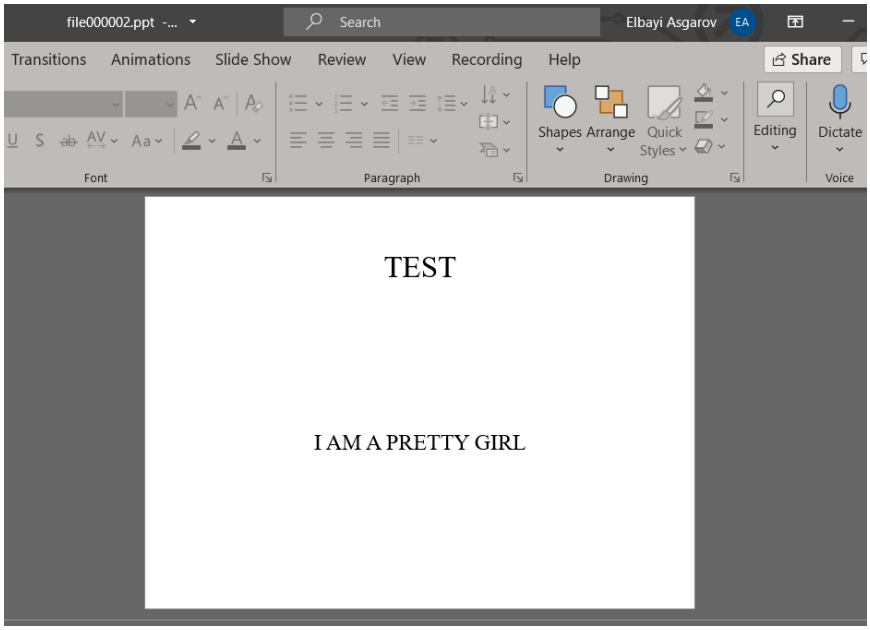
Name	file000002.jpg
Hash	6c9859e5121ff54d5d6298f65f0bf3b3



Name	file000000.jpg
Hash	37a49f97ed279832cd4f7bd002c826a2



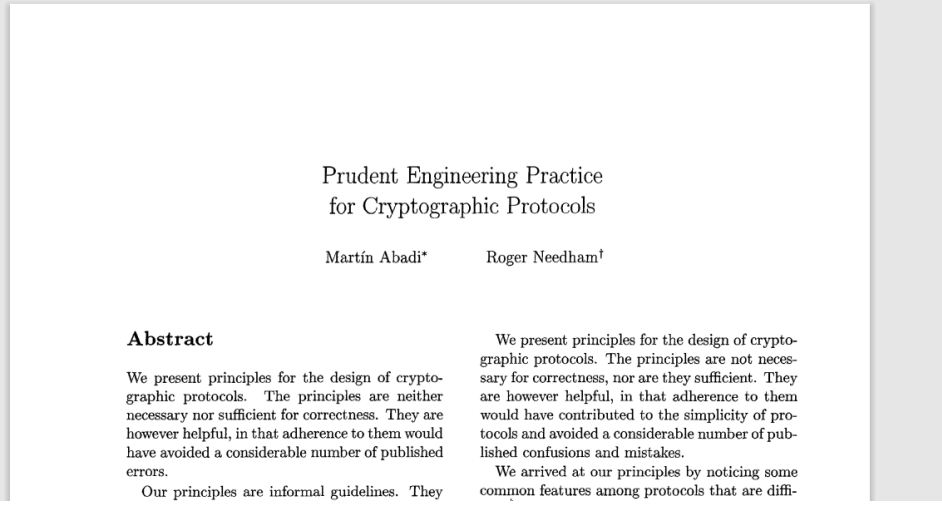
Name	file000000.doc
Hash	e72f388b36f9370f19696b164c308482



Name	file000002.ppt
Hash	d35c3334619fe05fda99cb029e92dc18

	A	B	C	D	E	F	G	H	I
1	SUMMARY OUTPUT								
2									
3	*Regression Statistics*								
4	Multiple R	0.809303							
5	R Square	0.654972							
6	Adjusted R	0.611844							
7	Standard E	1.139371							
8	Observatio	10							
9									
10	ANOVA								
11		*df*	*SS*	*MS*	*F*	*ignificance F*			
12	Regressio	1	19.71466	19.71466	15.18653	0.004564			
13	Residual	8	10.38534	1.298167					
14	Total	9	30.1						
15									
16		*Coefficients*	*tandard Err*	*t Stat*	*P-value*	*Lower 95%*	*Upper 95%*	*ower 95.0%*	*pper 95.0%*
17	Intercept	-20.4342	7.894879	-2.58829	0.032199	-38.6398	-2.22858	-38.6398	-2.22858
18	Height (in)	0.430451	0.110457	3.89699	0.004564	0.175736	0.685166	0.175736	0.685166
19									
20									
21									
22	RESIDUAL OUTPUT								
23									
24	*bservatio*	*icted Shoe*	*Residuals*						
25	1	11.84962	0.150376						
26	2	11.41917	-0.41917						
27	3	9.697368	0.302632						

Name	file000001.xls
Hash	e72f388b36f9370f19696b164c308482



Prudent Engineering Practice
for Cryptographic Protocols

Martín Abadi* Roger Needham†

Abstract

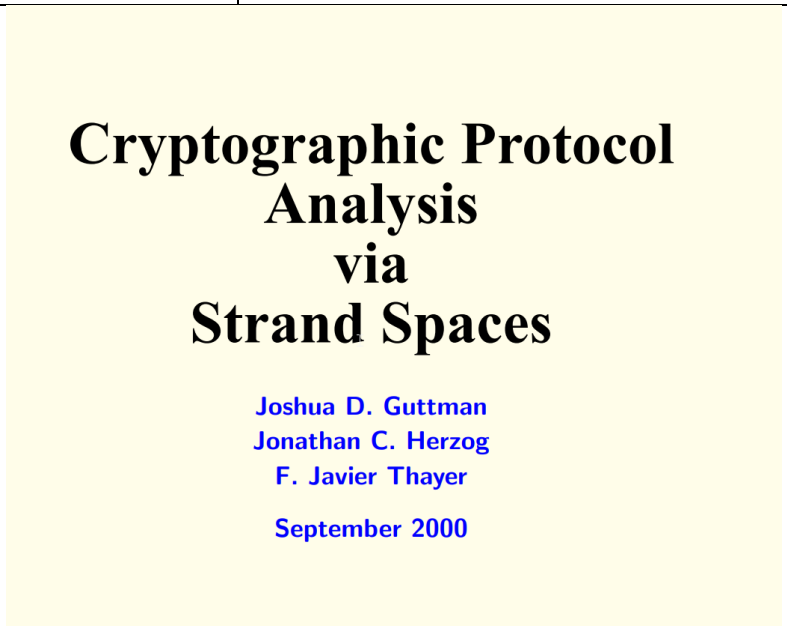
We present principles for the design of cryptographic protocols. The principles are neither necessary nor sufficient for correctness. They are however helpful, in that adherence to them would have avoided a considerable number of published errors.

Our principles are informal guidelines. They

We present principles for the design of cryptographic protocols. The principles are not necessary for correctness, nor are they sufficient. They are however helpful, in that adherence to them would have contributed to the simplicity of protocols and avoided a considerable number of published confusions and mistakes.

We arrived at our principles by noticing some common features among protocols that are diffi-

Name	file000000.pdf
Hash	e026ec863410725ba1f5765a1874800d

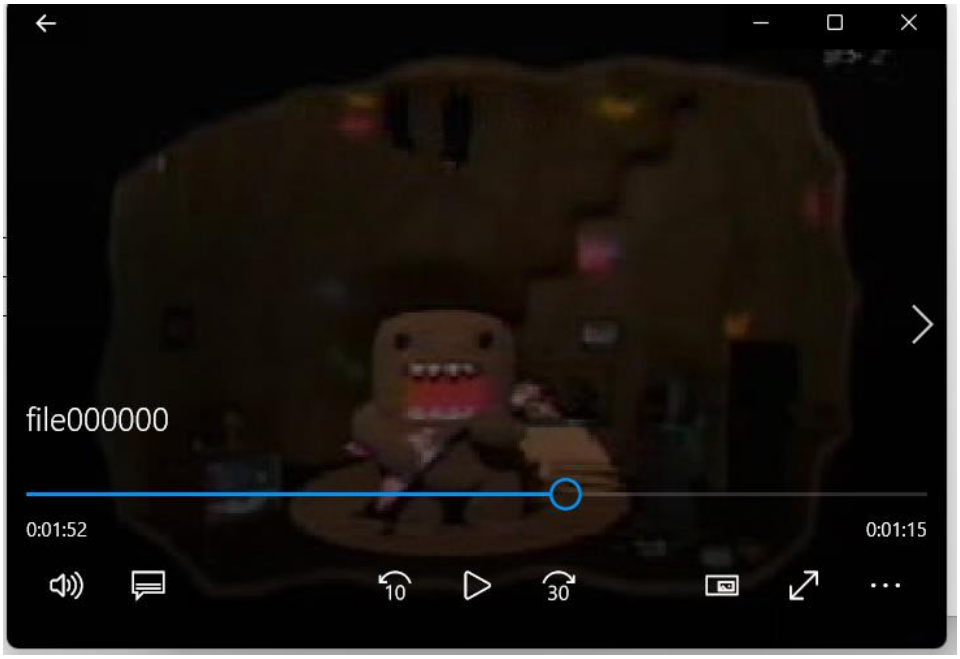


Cryptographic Protocol Analysis via Strand Spaces

Joshua D. Guttman
Jonathan C. Herzog
F. Javier Thayer

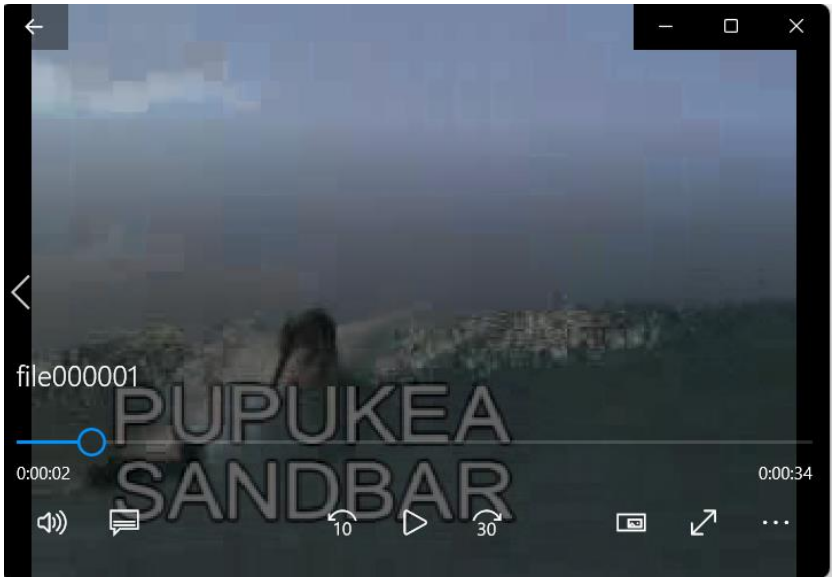
September 2000

Name	file000001.pdf
Hash	5b3e806e8c9c06a475cd45bf821af709



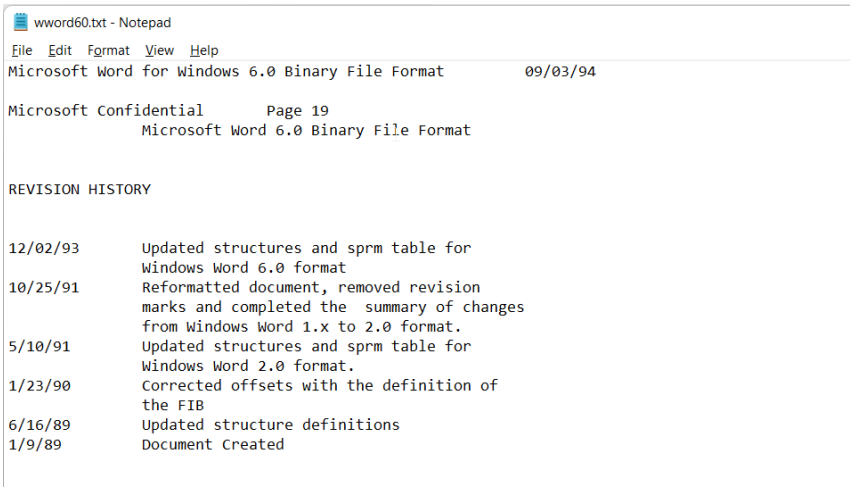
File Name	file000000.wmv
File Size	7.7 MiB
File Type	WMV
File Type Extension	wmv
Mime Type	video/x-ms-wmv
File Id	136CAA76-C5EA-4167-9853-DAD29251CD78
File Length	8037267
Creation Date	2002:04:27 00:51:37Z
Data Packets	1832
Duration	0:03:10
Send Duration	0:03:07
Preroll	3100
Flags	2
Min Packet Size	4386
Max Packet Size	4386
Max Bitrate	351 kbps
Audio Codec Id	Windows Media Audio V2 V7 V8 V9 / DivX audio (WMA) / Alex AC3 Audio
Audio Channels	1
Audio Sample Rate	22050

Name	file000000.wmv
Hash	63c0c6986cf0a446cb54b0ac65a921a5
Video length	03:07
Size	7.66 MB



File Name	file000001.wmv
File Size	1013 KiB
File Type	WMV
File Type Extension	wmv
Mime Type	video/x-ms-wmv
Title	Untitled
Copyright	©
File Id	00000000-0000-0000-0000-000000000000
File Length	1036994
Creation Date	2004:02:28 09:23:50Z
Data Packets	716
Duration	0:00:40
Send Duration	0:00:37
Preroll	3000
Flags	2
Min Packet Size	1444
Max Packet Size	1444
Max Bitrate	235 kbps
Wmadrc Peak Reference	32767
Wmadrc Average Reference	9073
Audio Codec Name	Windows Media Audio 9
Audio Codec Description	32 kbps, 32 kHz, stereo (A/V) 1-pass CBR
Video Codec Name	Windows Media Video V7
Audio Codec Id	Windows Media Audio V2 V7 V8 V9 / DivX audio (WMA) / Alex AC3 Audio

Name	file000001.wmv
Hash	ff085d0c4d0e0fdc8f3427db68e26266
Video length	00:36
Size	0.98 MB

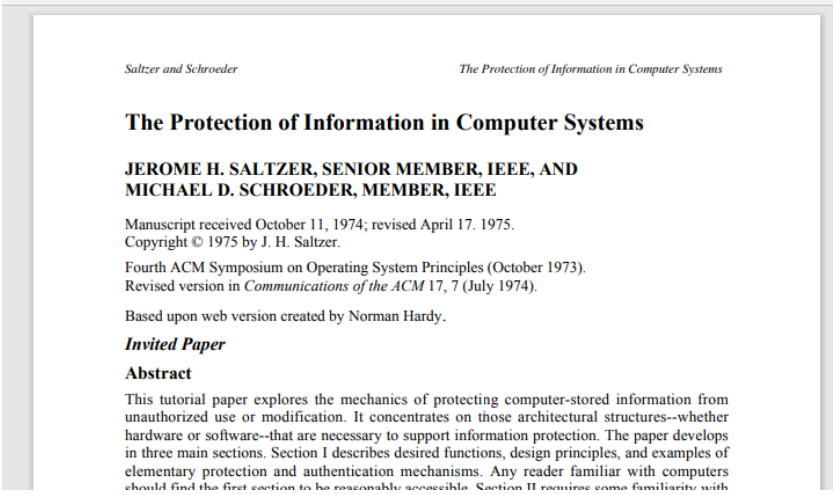

wword60.txt - Notepad

File Edit Format View Help

```
Microsoft Word for Windows 6.0 Binary File Format         09/03/94

Microsoft Confidential       Page 19
              Microsoft Word 6.0 Binary File Format


REVISION HISTORY


12/02/93       Updated structures and sprm table for
               Windows Word 6.0 format
10/25/91       Reformatted document, removed revision
               marks and completed the  summary of changes
               from Windows Word 1.x to 2.0 format.
5/10/91        Updated structures and sprm table for
               Windows Word 2.0 format.
1/23/90        Corrected offsets with the definition of
               the FIB
6/16/89        Updated structure definitions
1/9/89         Document Created
```

Name	wword60.txt
Hash	65ae3e29afbfa403d245a6fc4e7d8ccc
Modified date	June 7, 1998, 9:28 PM

Contents of 2.dd:



Saltzer and Schroeder *The Protection of Information in Computer Systems*

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND MICHAEL D. SCHROEDER, MEMBER, IEEE

Manuscript received October 11, 1974; revised April 17. 1975.

Fourth ACM Symposium on Operating System Principles (October 1973).
Revised version in *Communications of the ACM* 17, 7 (July 1974).

Based upon web version created by Norman Hardy.

Invited Paper

Abstract

This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with

Name	f0005646.pdf
Hash	2d4831f8a0c70844a126d961fca3792b

Name	f0005162.bmp
Hash	05111b496f0f094504998a1ba6172cae

Name	f0005628.jpg
Hash	937846adb96773ee25fcb34821230976