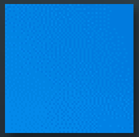
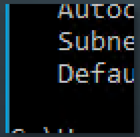
OCR'ING THE BITMAP CACHE PUZZLE

DREW LUCKENBAUGH

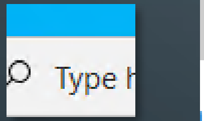
WHAT IS IT?

- Small Cached images from RDP sessions
- Helps improve bandwidth of Remote Desktop sessions



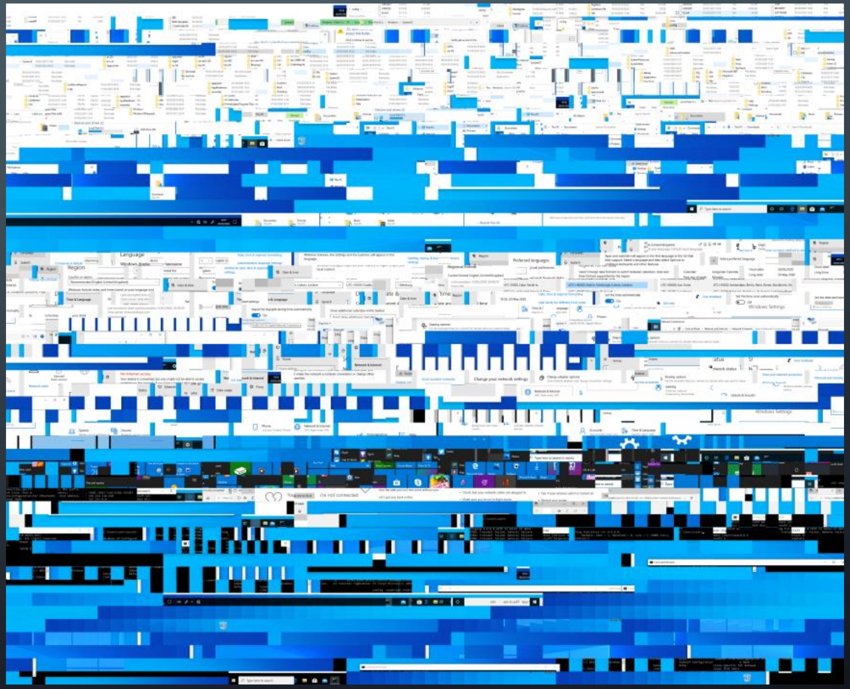


Autoc
Subne
Defau



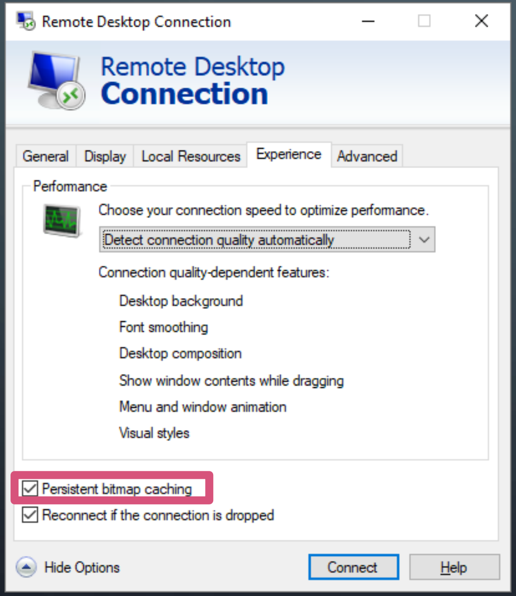
Type h

⚠ Troub
ange con



WHEN WAS IT INTRODUCED?

- First introduced in Windows XP
- Still currently in Windows under a different extension and location
  - .bmc vs .bin



Performance

Choose your connection speed to optimize performance.

Detect connection quality automatically

Connection quality-dependent features:

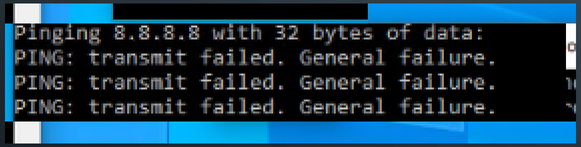
Desktop background
Font smoothing
Desktop composition
Show window contents while dragging
Menu and window animation
Visual styles

☑ Persistent bitmap caching

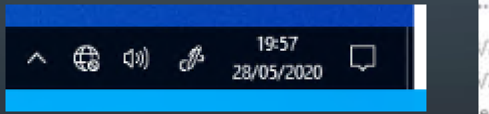
☑ Reconnect if the connection is dropped

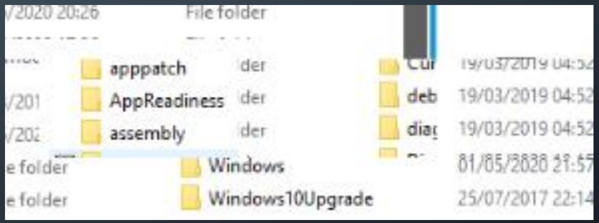
WHAT DOES IT TELL ME?

- Provides snippets of visual information that can help confirm activity observed in other artifacts
  - Programs open during RDP sessions
  - Date / timestamps
  - Files and folders accessed / viewed
- Can provide a small window into the perspective of the attacker



```
Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

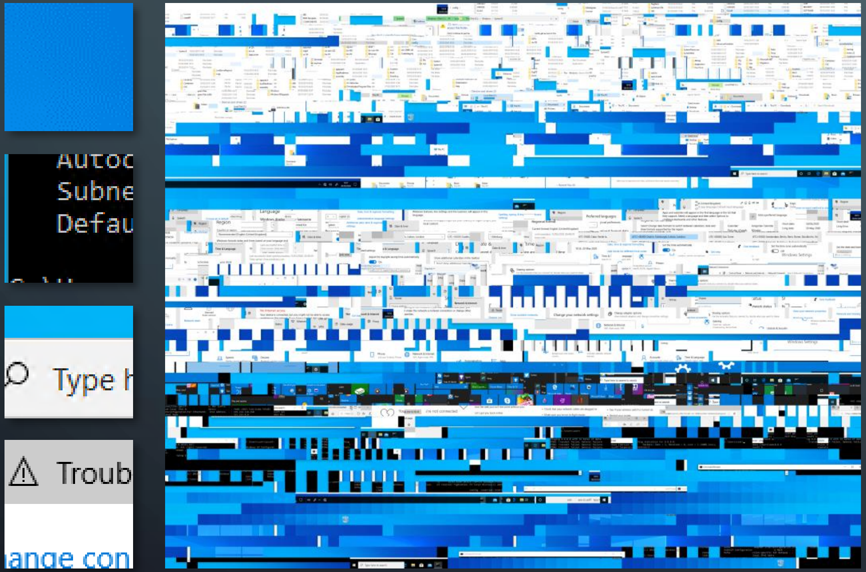


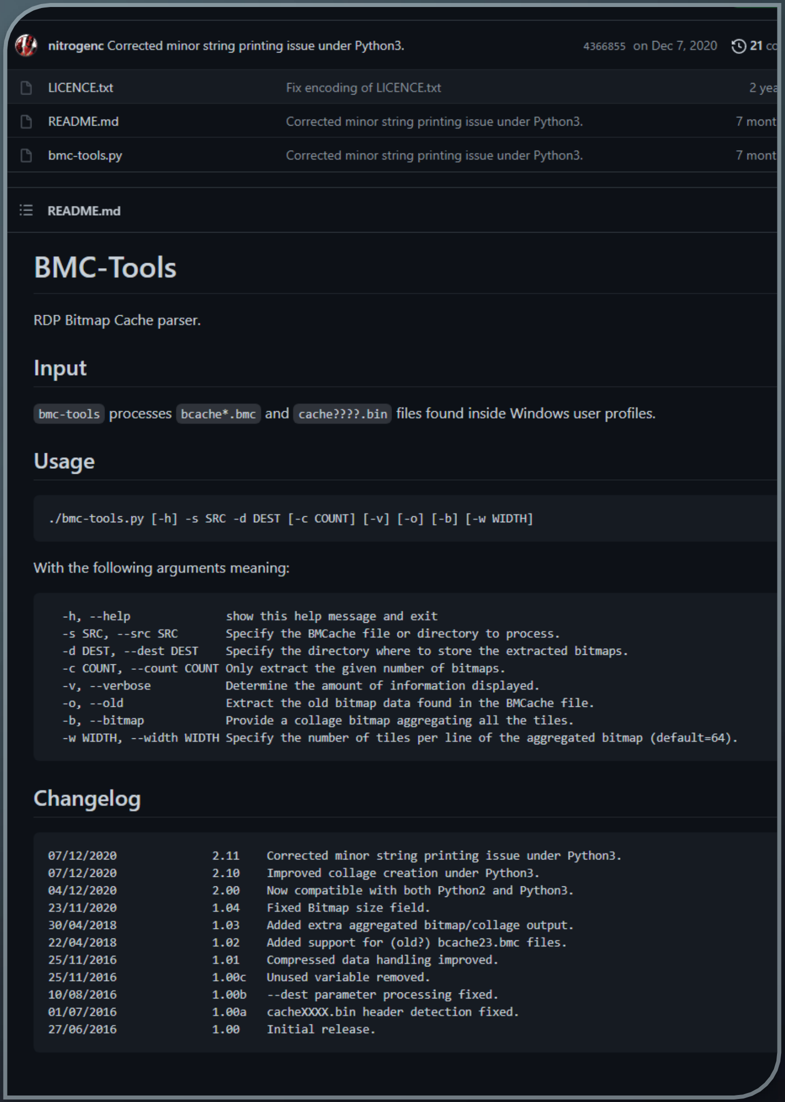


For more information on the Bitmap Cache artifact, please check out:
https://www.allthingsdfir.com/do-you-even-bitmap-cache-bro/
https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpegdi/2bf92588-42bd-4527-8b3e-b90c56e292d2

HOW DO I PARSE IT?

- ANSSI - BMC-tools
    - A python script that allows you to parse either .bmc or .bin files and even puts them all into a final collage





nitrogenc Corrected minor string printing issue under Python3. 4366855 on Dec 7, 2020 21 co

LICENCE.txt	Fix encoding of LICENCE.txt	2 yea
README.md	Corrected minor string printing issue under Python3.	7 mont
bmc-tools.py	Corrected minor string printing issue under Python3.	7 mont

README.md

BMC-Tools

RDP Bitmap Cache parser.

Input

`bmc-tools` processes `bcache*.bmc` and `cache????.bin` files found inside Windows user profiles.

Usage

```
./bmc-tools.py [-h] -s SRC -d DEST [-c COUNT] [-v] [-o] [-b] [-w WIDTH]
```

With the following arguments meaning:

```
  -h, --help            show this help message and exit
  -s SRC, --src SRC     Specify the BMCache file or directory to process.
  -d DEST, --dest DEST  Specify the directory where to store the extracted bitmaps.
  -c COUNT, --count COUNT Only extract the given number of bitmaps.
  -v, --verbose         Determine the amount of information displayed.
  -o, --old             Extract the old bitmap data found in the BMCache file.
  -b, --bitmap          Provide a collage bitmap aggregating all the tiles.
  -w WIDTH, --width WIDTH Specify the number of tiles per line of the aggregated bitmap (default=64).
```

Changelog

```
07/12/2020          2.11    Corrected minor string printing issue under Python3.
07/12/2020          2.10    Improved collage creation under Python3.
04/12/2020          2.00    Now compatible with both Python2 and Python3.
23/11/2020          1.04    Fixed Bitmap size field.
30/04/2018          1.03    Added extra aggregated bitmap/collage output.
22/04/2018          1.02    Added support for (old?) bcache23.bmc files.
25/11/2016          1.01    Compressed data handling improved.
25/11/2016          1.00c   Unused variable removed.
10/08/2016          1.00b   --dest parameter processing fixed.
01/07/2016          1.00a   cacheXXXX.bin header detection fixed.
27/06/2016          1.00    Initial release.
```

CAN I ORGANIZE THESE IMAGES?

SIMPLE IMAGE EDITING

Ps Adobe Photoshop

W Microsoft Word

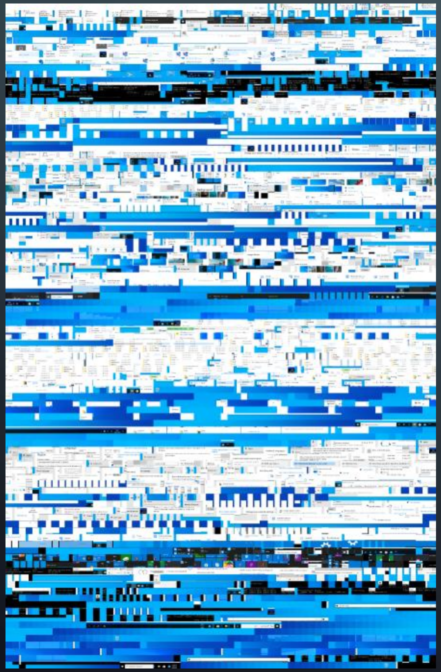
MORE COMPLEX TOOLS

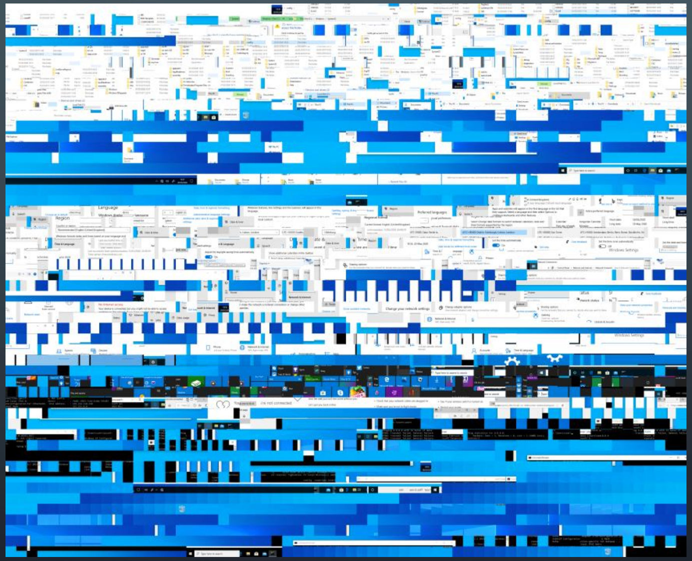
- BriMor Labs - RDPieces
  - https://github.com/brimorlabs/rdpieces
- BSI Bund - RdpCacheStitcher
  - https://github.com/BSI-Bund/RdpCacheStitcher

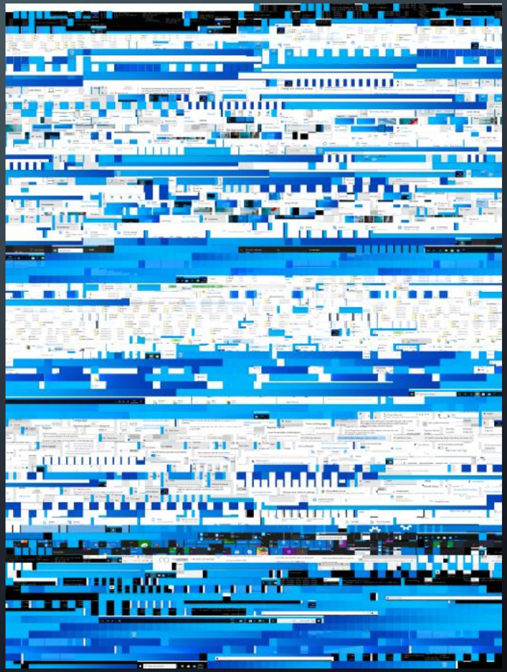
WHY OPTICAL CHARACTER RECOGNITION (OCR)?

SCENARIO

- Imagine a host with multiple 100MB BMC .bin files on it
- Job is to analyze each collage for any information that could help confirm evidence observed in other artifacts





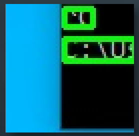


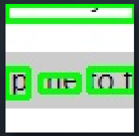
SCENARIO CONT.

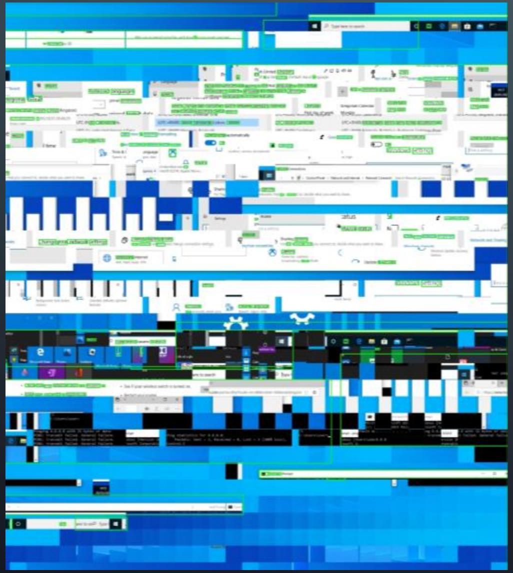
- Where do you start?
- How do you keep track of the information you are finding?
  - Screenshots, notes?
- Are you only looking for IOCs or is it broader than that?
- Only have the source host?
- Do you have an accurate inventory of the hosts / Ips?

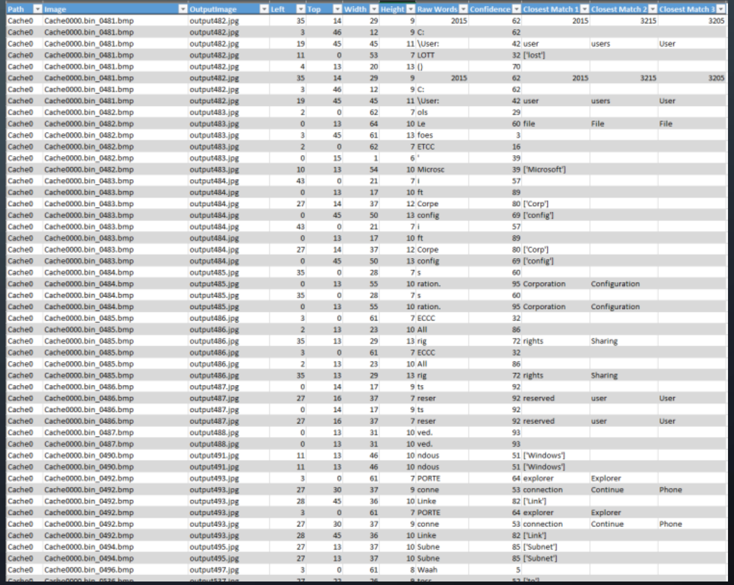
OCR-BITMAP-CACHE

- A new tool to quickly triage these bitmap images
  - Utilizes Tesseract OCR to analyze images
  - Matches a custom wordlist to words found in the images
  - Outputs a CSV of the words it identified
  - Outputs a folder of images with highlights around the words it identified





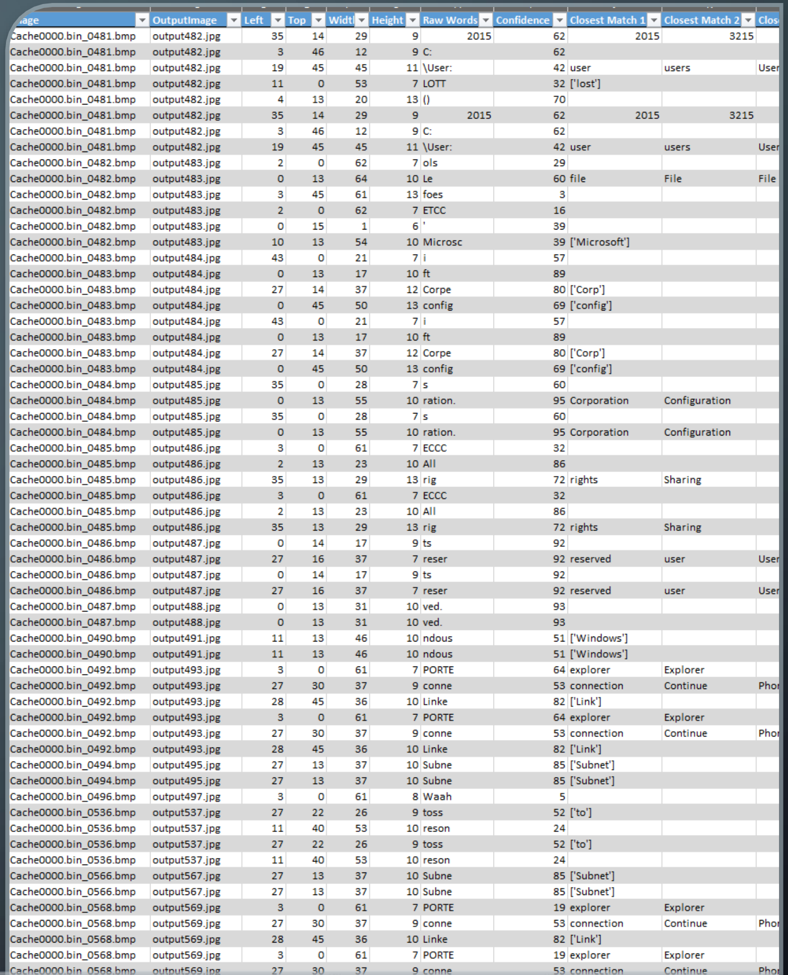




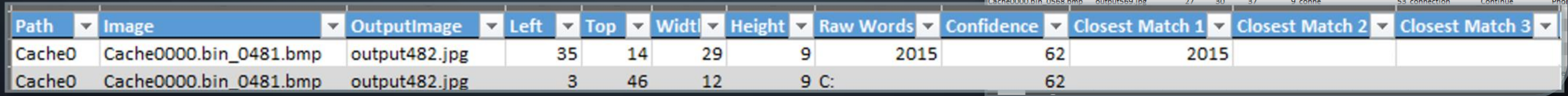
Path	Image	OutputImage	Left	Top	Width	Height	Raw Words	Confidence	Closest Match 1	Closest Match 2	Closest Match 3
Cache0	Cache0000.bin_0481.bmp	output482.jpg	35	14	29	9	2015	62	2015	3215	3205
Cache0	Cache0000.bin_0481.bmp	output482.jpg	3	46	12	9	C:	62			
Cache0	Cache0000.bin_0481.bmp	output482.jpg	19	45	45	11	\User:	42	user	users	User
Cache0	Cache0000.bin_0481.bmp	output482.jpg	11	0	53	7	LOTT	32	['lost']		
Cache0	Cache0000.bin_0481.bmp	output482.jpg	4	13	20	13	()	70			
Cache0	Cache0000.bin_0481.bmp	output482.jpg	35	14	29	9	2015	62	2015	3215	3205
Cache0	Cache0000.bin_0481.bmp	output482.jpg	3	46	12	9	C:	62			
Cache0	Cache0000.bin_0481.bmp	output482.jpg	19	45	45	11	\User:	42	user	users	User
Cache0	Cache0000.bin_0482.bmp	output483.jpg	2	0	62	7	ols	29			
Cache0	Cache0000.bin_0482.bmp	output483.jpg	0	13	64	10	Le	60	file	File	File
Cache0	Cache0000.bin_0482.bmp	output483.jpg	3	45	61	13	foes	3			
Cache0	Cache0000.bin_0482.bmp	output483.jpg	2	0	62	7	ETCC	16			
Cache0	Cache0000.bin_0482.bmp	output483.jpg	0	15	1	6	'	39			
Cache0	Cache0000.bin_0482.bmp	output483.jpg	10	13	54	10	Microsc	39	['Microsoft']		
Cache0	Cache0000.bin_0483.bmp	output484.jpg	43	0	21	7	i	57			
Cache0	Cache0000.bin_0483.bmp	output484.jpg	0	13	17	10	ft	89			
Cache0	Cache0000.bin_0483.bmp	output484.jpg	27	14	37	12	Corpe	80	['Corp']		
Cache0	Cache0000.bin_0483.bmp	output484.jpg	0	45	50	13	config	69	['config']		
Cache0	Cache0000.bin_0483.bmp	output484.jpg	43	0	21	7	i	57			
Cache0	Cache0000.bin_0483.bmp	output484.jpg	0	13	17	10	ft	89			
Cache0	Cache0000.bin_0483.bmp	output484.jpg	27	14	37	12	Corpe	80	['Corp']		
Cache0	Cache0000.bin_0483.bmp	output484.jpg	0	45	50	13	config	69	['config']		
Cache0	Cache0000.bin_0484.bmp	output485.jpg	35	0	28	7	s	60			
Cache0	Cache0000.bin_0484.bmp	output485.jpg	0	13	55	10	ration.	95	Corporation	Configuration	
Cache0	Cache0000.bin_0484.bmp	output485.jpg	35	0	28	7	s	60			
Cache0	Cache0000.bin_0484.bmp	output485.jpg	0	13	55	10	ration.	95	Corporation	Configuration	
Cache0	Cache0000.bin_0485.bmp	output486.jpg	3	0	61	7	ECCC	32			
Cache0	Cache0000.bin_0485.bmp	output486.jpg	2	13	23	10	All	86			
Cache0	Cache0000.bin_0485.bmp	output486.jpg	35	13	29	13	rig	72	rights	Sharing	
Cache0	Cache0000.bin_0485.bmp	output486.jpg	3	0	61	7	ECCC	32			
Cache0	Cache0000.bin_0485.bmp	output486.jpg	2	13	23	10	All	86			
Cache0	Cache0000.bin_0485.bmp	output486.jpg	35	13	29	13	rig	72	rights	Sharing	
Cache0	Cache0000.bin_0486.bmp	output487.jpg	0	14	17	9	ts	92			
Cache0	Cache0000.bin_0486.bmp	output487.jpg	27	16	37	7	reser	92	reserved	user	User
Cache0	Cache0000.bin_0486.bmp	output487.jpg	0	14	17	9	ts	92			
Cache0	Cache0000.bin_0486.bmp	output487.jpg	27	16	37	7	reser	92	reserved	user	User
Cache0	Cache0000.bin_0487.bmp	output488.jpg	0	13	31	10	ved.	93			
Cache0	Cache0000.bin_0487.bmp	output488.jpg	0	13	31	10	ved.	93			
Cache0	Cache0000.bin_0490.bmp	output491.jpg	11	13	46	10	ndous	51	['Windows']		
Cache0	Cache0000.bin_0490.bmp	output491.jpg	11	13	46	10	ndous	51	['Windows']		
Cache0	Cache0000.bin_0492.bmp	output493.jpg	3	0	61	7	PORTE	64	explorer	Explorer	
Cache0	Cache0000.bin_0492.bmp	output493.jpg	27	30	37	9	conne	53	connection	Continue	Phone
Cache0	Cache0000.bin_0492.bmp	output493.jpg	28	45	36	10	Linke	82	['Link']		
Cache0	Cache0000.bin_0492.bmp	output493.jpg	3	0	61	7	PORTE	64	explorer	Explorer	
Cache0	Cache0000.bin_0492.bmp	output493.jpg	27	30	37	9	conne	53	connection	Continue	Phone
Cache0	Cache0000.bin_0492.bmp	output493.jpg	28	45	36	10	Linke	82	['Link']		
Cache0	Cache0000.bin_0494.bmp	output495.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0	Cache0000.bin_0494.bmp	output495.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0	Cache0000.bin_0496.bmp	output497.jpg	3	0	61	8	Waah	5			
Cache0	Cache0000.bin_0536.bmp	output537.jpg	27	22	36	8	tocr	53	['to']		

OCR-BITMAP-CACHE CSV OUTPUT

- Path to the original image
- Name of the highlighted output image
- Output size and location of the words located in the highlighted image
- Characters identified by the OCR
- Confidence of the characters identified
- Top three closest matches to the characters from the custom wordlist



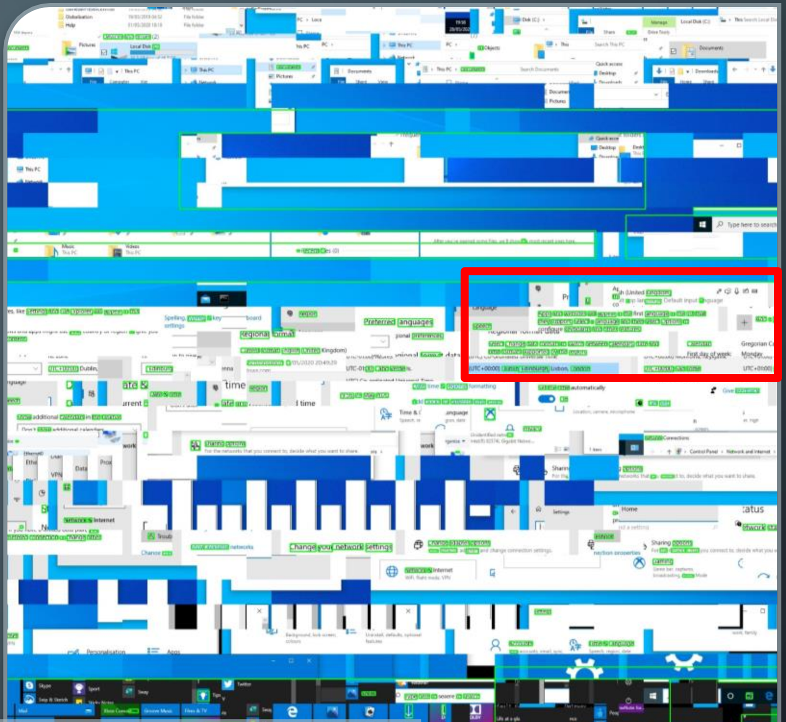
age	OutputImage	Left	Top	Widtl	Height	Raw Words	Confidence	Closest Match 1	Closest Match 2	Clos
Cache0000.bin_0481.bmp	output482.jpg	35	14	29	9	2015	62	2015	3215	
Cache0000.bin_0481.bmp	output482.jpg	3	46	12	9	C:	62			
Cache0000.bin_0481.bmp	output482.jpg	19	45	45	11	\User:	42	user	users	User
Cache0000.bin_0481.bmp	output482.jpg	11	0	53	7	LOTT	32	['lost']		
Cache0000.bin_0481.bmp	output482.jpg	4	13	20	13	()	70			
Cache0000.bin_0481.bmp	output482.jpg	35	14	29	9	2015	62	2015	3215	
Cache0000.bin_0481.bmp	output482.jpg	3	46	12	9	C:	62			
Cache0000.bin_0481.bmp	output482.jpg	19	45	45	11	\User:	42	user	users	User
Cache0000.bin_0482.bmp	output483.jpg	2	0	62	7	ols	29			
Cache0000.bin_0482.bmp	output483.jpg	0	13	64	10	Le	60	file	File	File
Cache0000.bin_0482.bmp	output483.jpg	3	45	61	13	foes	3			
Cache0000.bin_0482.bmp	output483.jpg	2	0	62	7	ETCC	16			
Cache0000.bin_0482.bmp	output483.jpg	0	15	1	6	'	39			
Cache0000.bin_0482.bmp	output483.jpg	10	13	54	10	Microsc	39	['Microsoft']		
Cache0000.bin_0483.bmp	output484.jpg	43	0	21	7	i	57			
Cache0000.bin_0483.bmp	output484.jpg	0	13	17	10	ft	89			
Cache0000.bin_0483.bmp	output484.jpg	27	14	37	12	Corpe	80	['Corp']		
Cache0000.bin_0483.bmp	output484.jpg	0	45	50	13	config	69	['config']		
Cache0000.bin_0483.bmp	output484.jpg	43	0	21	7	i	57			
Cache0000.bin_0483.bmp	output484.jpg	0	13	17	10	ft	89			
Cache0000.bin_0483.bmp	output484.jpg	27	14	37	12	Corpe	80	['Corp']		
Cache0000.bin_0483.bmp	output484.jpg	0	45	50	13	config	69	['config']		
Cache0000.bin_0484.bmp	output485.jpg	35	0	28	7	s	60			
Cache0000.bin_0484.bmp	output485.jpg	0	13	55	10	ration.	95	Corporation	Configuration	
Cache0000.bin_0484.bmp	output485.jpg	35	0	28	7	s	60			
Cache0000.bin_0484.bmp	output485.jpg	0	13	55	10	ration.	95	Corporation	Configuration	
Cache0000.bin_0485.bmp	output486.jpg	3	0	61	7	ECCC	32			
Cache0000.bin_0485.bmp	output486.jpg	2	13	23	10	All	86			
Cache0000.bin_0485.bmp	output486.jpg	35	13	29	13	rig	72	rights	Sharing	
Cache0000.bin_0485.bmp	output486.jpg	3	0	61	7	ECCC	32			
Cache0000.bin_0485.bmp	output486.jpg	2	13	23	10	All	86			
Cache0000.bin_0485.bmp	output486.jpg	35	13	29	13	rig	72	rights	Sharing	
Cache0000.bin_0486.bmp	output487.jpg	0	14	17	9	ts	92			
Cache0000.bin_0486.bmp	output487.jpg	27	16	37	7	reser	92	reserved	user	User
Cache0000.bin_0486.bmp	output487.jpg	0	14	17	9	ts	92			
Cache0000.bin_0486.bmp	output487.jpg	27	16	37	7	reser	92	reserved	user	User
Cache0000.bin_0487.bmp	output488.jpg	0	13	31	10	ved.	93			
Cache0000.bin_0487.bmp	output488.jpg	0	13	31	10	ved.	93			
Cache0000.bin_0490.bmp	output491.jpg	11	13	46	10	ndous	51	['Windows']		
Cache0000.bin_0490.bmp	output491.jpg	11	13	46	10	ndous	51	['Windows']		
Cache0000.bin_0492.bmp	output493.jpg	3	0	61	7	PORTE	64	explorer	Explorer	
Cache0000.bin_0492.bmp	output493.jpg	27	30	37	9	conne	53	connection	Continue	Phor
Cache0000.bin_0492.bmp	output493.jpg	28	45	36	10	Linke	82	['Link']		
Cache0000.bin_0492.bmp	output493.jpg	3	0	61	7	PORTE	64	explorer	Explorer	
Cache0000.bin_0492.bmp	output493.jpg	27	30	37	9	conne	53	connection	Continue	Phor
Cache0000.bin_0492.bmp	output493.jpg	28	45	36	10	Linke	82	['Link']		
Cache0000.bin_0494.bmp	output495.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0000.bin_0494.bmp	output495.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0000.bin_0496.bmp	output497.jpg	3	0	61	8	Waah	5			
Cache0000.bin_0536.bmp	output537.jpg	27	22	26	9	toss	52	['to']		
Cache0000.bin_0536.bmp	output537.jpg	11	40	53	10	reson	24			
Cache0000.bin_0536.bmp	output537.jpg	27	22	26	9	toss	52	['to']		
Cache0000.bin_0536.bmp	output537.jpg	11	40	53	10	reson	24			
Cache0000.bin_0566.bmp	output567.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0000.bin_0566.bmp	output567.jpg	27	13	37	10	Subne	85	['Subnet']		
Cache0000.bin_0568.bmp	output569.jpg	3	0	61	7	PORTE	19	explorer	Explorer	
Cache0000.bin_0568.bmp	output569.jpg	27	30	37	9	conne	53	connection	Continue	Phor
Cache0000.bin_0568.bmp	output569.jpg	28	45	36	10	Linke	82	['Link']		
Cache0000.bin_0568.bmp	output569.jpg	3	0	61	7	PORTE	19	explorer	Explorer	
Cache0000.bin_0568.bmp	output569.jpg	27	30	37	9	conne	53	connection	Continue	Phor

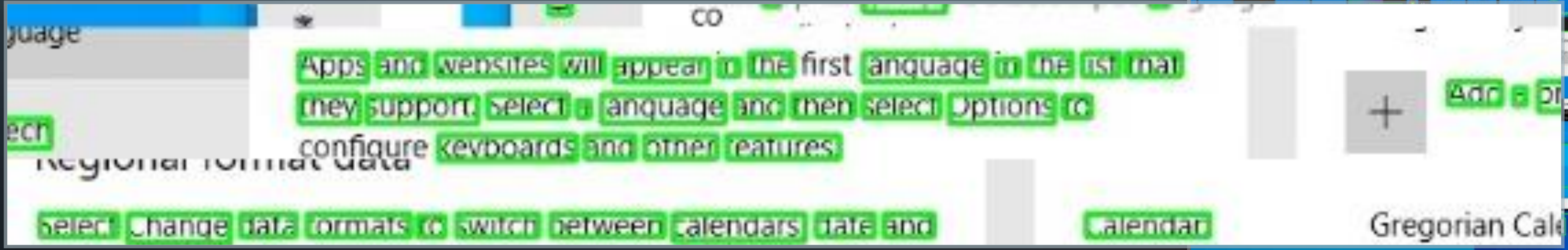


Path	Image	OutputImage	Left	Top	Widtl	Height	Raw Words	Confidence	Closest Match 1	Closest Match 2	Closest Match 3
Cache0	Cache0000.bin_0481.bmp	output482.jpg	35	14	29	9	2015	62	2015		
Cache0	Cache0000.bin_0481.bmp	output482.jpg	3	46	12	9	C:	62			

OCR-BITMAP-CACHE HIGHLIGHTED IMAGE OUTPUT

- Highlights the characters the OCR identifies and creates a new image with these highlights
- Saves these images into a directory specified by the “-d” destination flag





Apps and websites will appear in the first language in the list that they support. Select a language and then select Options to configure keyboards and other features.

Regional format data

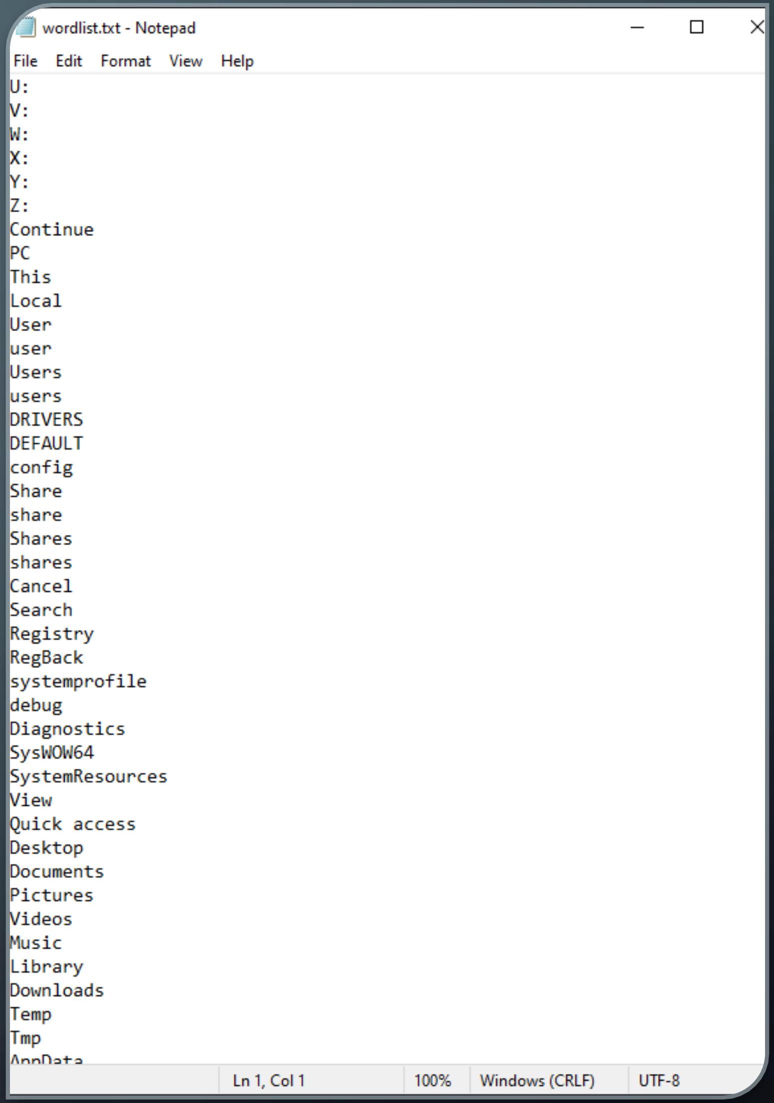
Select Change data formats to switch between calendars, date and

Calendar

Gregorian Cale

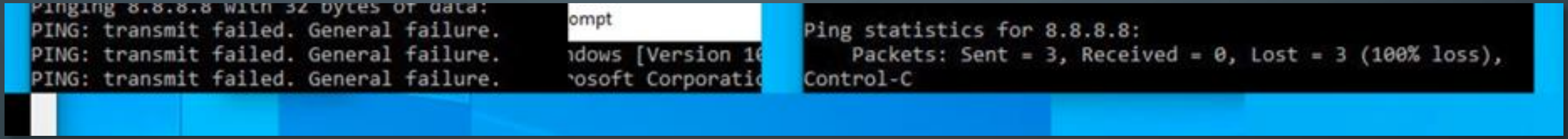
OCR-BITMAP-CACHE WORDLIST INPUT

- Allows for wordlist customization
- Can tailor the wordlist to match IOCs, users, IPs and more that are observed in the incident



```
U:
V:
W:
X:
Y:
Z:
Continue
PC
This
Local
User
user
Users
users
DRIVERS
DEFAULT
config
Share
share
Shares
shares
Cancel
Search
Registry
RegBack
systemprofile
debug
Diagnostics
SysWOW64
SystemResources
View
Quick access
Desktop
Documents
Pictures
Videos
Music
Library
Downloads
Temp
Tmp
AppData
```

EXAMPLE – INPUT IMAGE



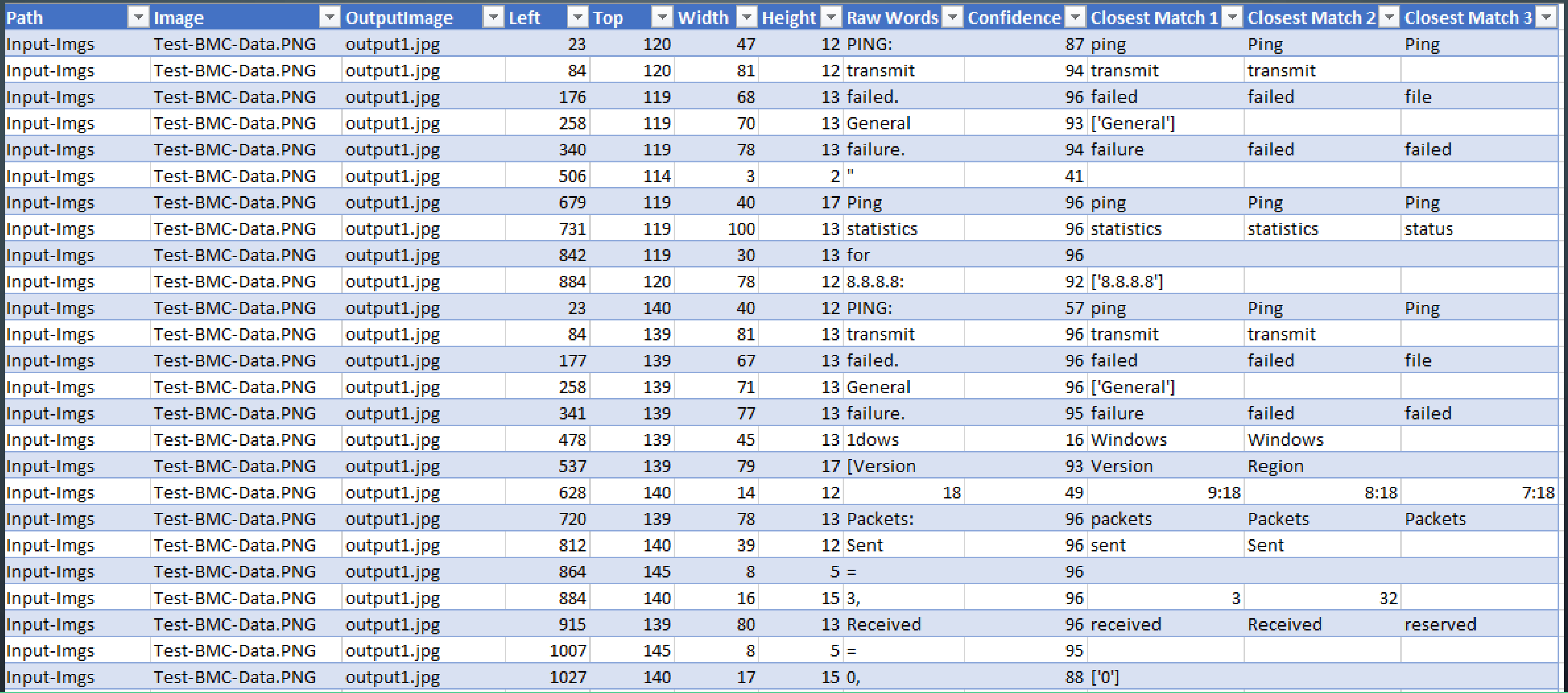
```
Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
```

```
ompt
ndows [Version 1
rosoft Corporati
```

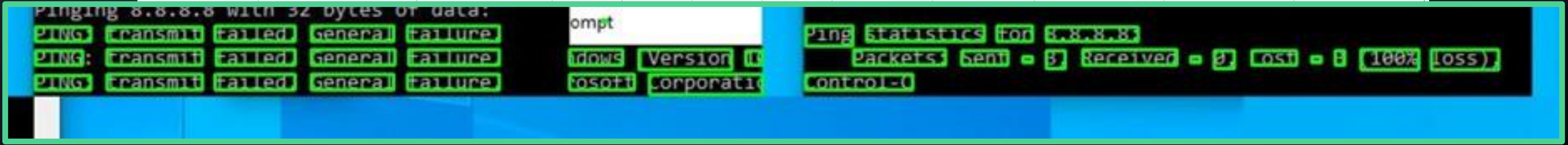
```
Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
```

./ocr.py [-h] [-c MIN_CONF] -s SOURCE -d DEST -o CSV -w WORDLIST

EXAMPLE – OUTPUT



Path	Image	OutputImage	Left	Top	Width	Height	Raw Words	Confidence	Closest Match 1	Closest Match 2	Closest Match 3
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	23	120	47	12	PING:	87	ping	Ping	Ping
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	84	120	81	12	transmit	94	transmit	transmit	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	176	119	68	13	failed.	96	failed	failed	file
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	258	119	70	13	General	93	['General']		
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	340	119	78	13	failure.	94	failure	failed	failed
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	506	114	3	2	"	41			
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	679	119	40	17	Ping	96	ping	Ping	Ping
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	731	119	100	13	statistics	96	statistics	statistics	status
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	842	119	30	13	for	96			
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	884	120	78	12	8.8.8.8:	92	['8.8.8.8']		
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	23	140	40	12	PING:	57	ping	Ping	Ping
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	84	139	81	13	transmit	96	transmit	transmit	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	177	139	67	13	failed.	96	failed	failed	file
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	258	139	71	13	General	96	['General']		
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	341	139	77	13	failure.	95	failure	failed	failed
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	478	139	45	13	1dows	16	Windows	Windows	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	537	139	79	17	[Version	93	Version	Region	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	628	140	14	12	18	49	9:18	8:18	7:18
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	720	139	78	13	Packets:	96	packets	Packets	Packets
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	812	140	39	12	Sent	96	sent	Sent	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	864	145	8	5	=	96			
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	884	140	16	15	3,	96	3	32	
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	915	139	80	13	Received	96	received	Received	reserved
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	1007	145	8	5	=	95			
Input-Imgs	Test-BMC-Data.PNG	output1.jpg	1027	140	17	15	0,	88	['0']		



```
Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.     ompt                Ping statistics for 8.8.8.8:
PING: transmit failed. General failure.     idows  Version  (       Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
PING: transmit failed. General failure.     rosoft  Corporati    Control-C
```

OCR-BITMAP-CACHE GITHUB PAGE

https://github.com/DFIR-Drew/OCR-Bitmap-Cache

WHAT'S NEXT?

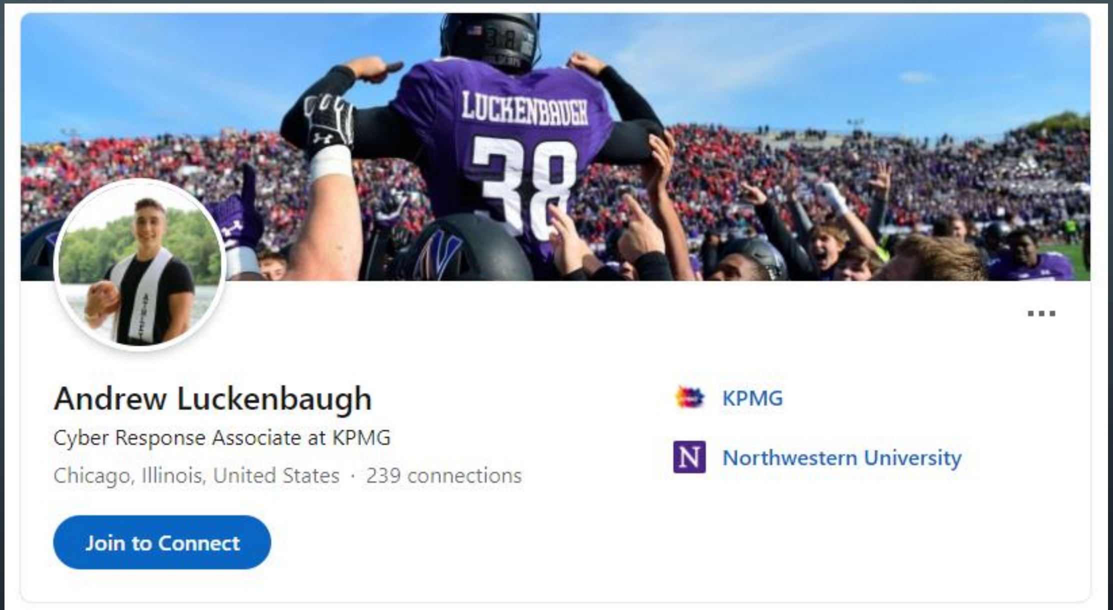
- Multiple ways to improve the accuracy / reliability of the OCR
  - Image quality / image pre-processing
  - Currently, take original, grayscale, and inverse grayscale images
- Piecing together larger sections first could improve accuracy
- Tailoring the wordlist to match IOCs, users, IPs, etc. that match the incident
- OCR'ing collections of images, not just BMC images

KEY TAKEAWAYS

- Bitmap Cache can be a very important artifact
  - Provides context of what activity may have occurred
- OCR-Bitmap-Cache aims to simplify the triaging of an artifact that already has great tools to go with it

THANK YOU

- Feel free to connect with me!
  - https://bit.ly/3z3RcOm



Andrew Luckenbaugh

Cyber Response Associate at KPMG

Chicago, Illinois, United States · 239 connections