

# Angad

Malware Detection via  
Multi-Dimensional Visualization

Ankur Tyagi (@7h3rAm)

# whoami

— — —

- Sr. Malware Research Engineer @ [Qualys](#)
- [@7h3rAm](#) on the Interweb

# Outline

---

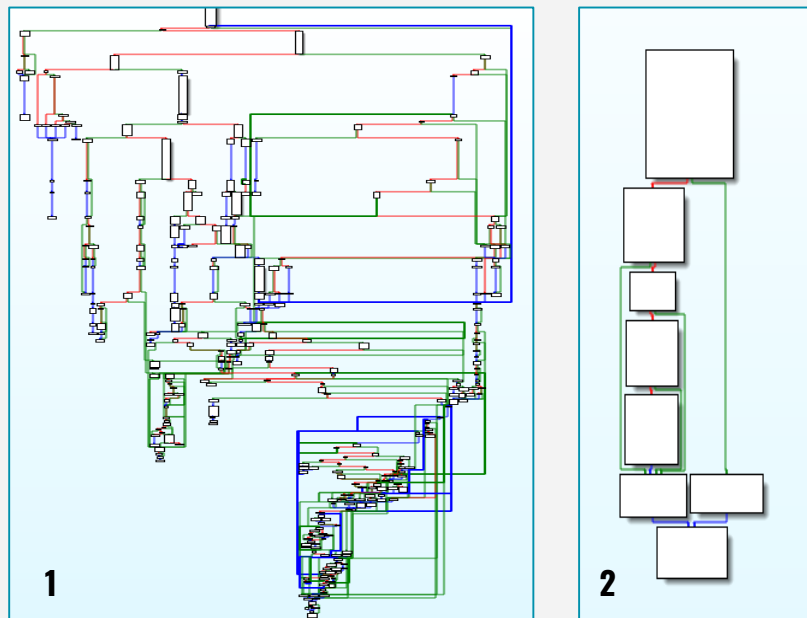
- Issues with Malware Analysis
- What is Multi-Dimensional Visualization?
- Context-aware Multi-Dimensional Visualization
- Usecases

# Issues with Malware Analysis

— — —

- Nymaim (is a trojan, downloads additional malware) CFGs
- pre deobfuscation (#1): 200+ blocks
- post deobfuscation (#2): 8 blocks

Nymaim obfuscation and cyber variant of "knock, knock, who's there?" (@Avira)



# Issues with Malware Analysis

— — —

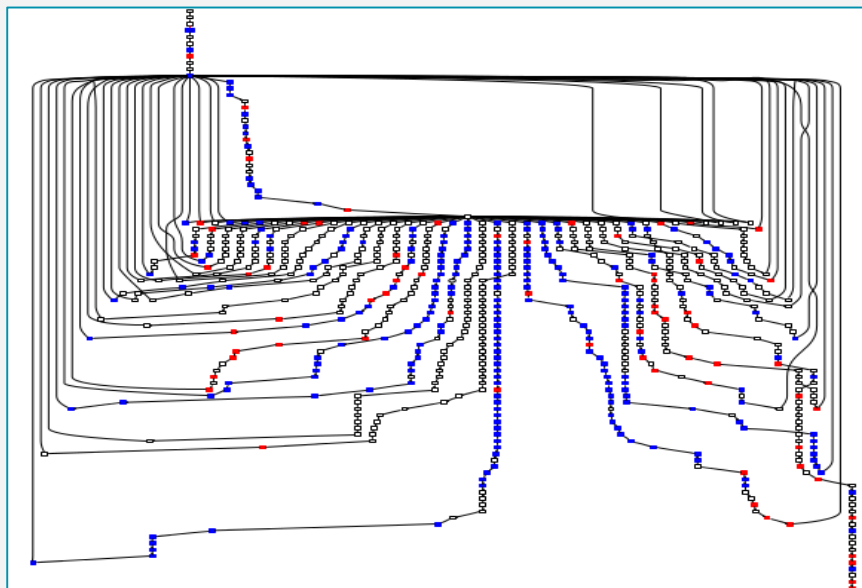
- Malware Analysis is difficult:
  - Obfuscation, anti-\* (disassembly, debugging, virtualization)
  - Volume of new unknowns is huge (250k+ unknowns daily, 90%+ clean)
- Lots of interesting proposals to solve these issues over last many years
- Vendors use proprietary (closed/IP-protected) solutions
- Enthusiasts build and use “personal” projects (difficult to gain traction)

# Issues with Malware Analysis

— — —

- Issues with current automated techniques:
  - packers/virtualizers/compressors (themida, vmpack, aspack)
  - runtime dependencies
  - trigger conditions
  - sandbox detection
  - user interaction

[What Does Obfuscated Software Look Like? \(The University of Arizona\)](#)



# Issues with Malware Analysis

— — —

- We need to focus on generic signatures to reduce overhead and increase future coverage
- Note: Excessive generalization in detection methods can increase FPs
- We still need specialized detection methods for threat attribution

# Issues with Malware Analysis

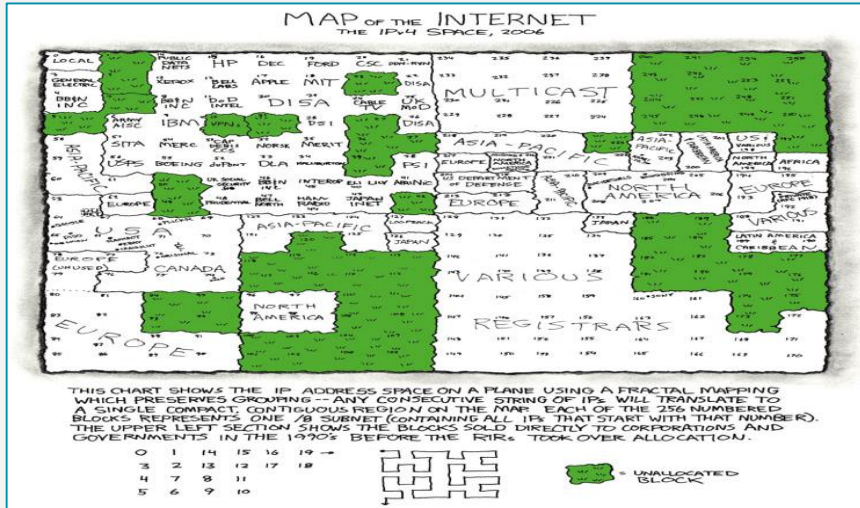
— — —

- Lots of interesting research has been done towards applying visualization techniques for malware analysis
  - [Malware Analysis Using Visualized Image Matrices \(Han et al.\)](#)
  - [Malware Images: Visualization and Automatic Classification \(Nataraj et al.\)](#)
  - [Visual Analysis of Malware Behaviour Using Treemaps and Thread Graphs \(Holz et al.\)](#)
  - [and many more ...](#)

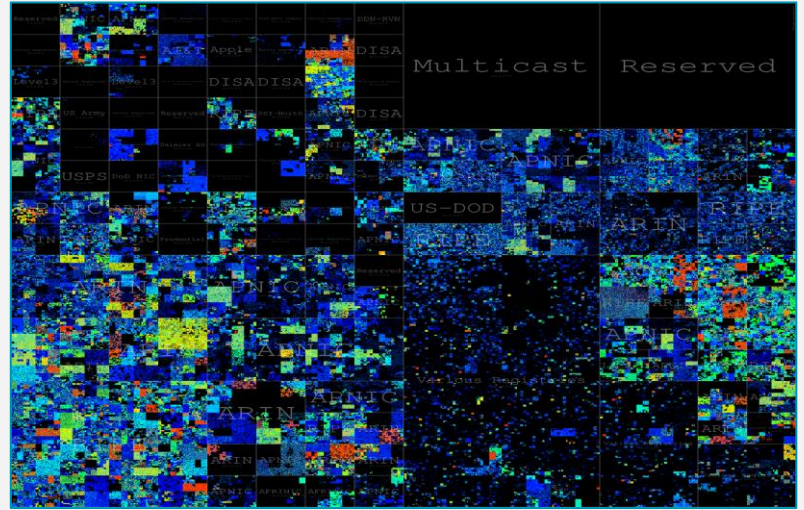




# What is Multi-Dimensional Visualization?



xkcd 195: Map of the Internet



Mapping the whole Internet with Hilbert curves (@benjojo12)

- IPv4:  $2^{32} \approx 4+$  billion addresses

# What is Multi-Dimensional Visualization?

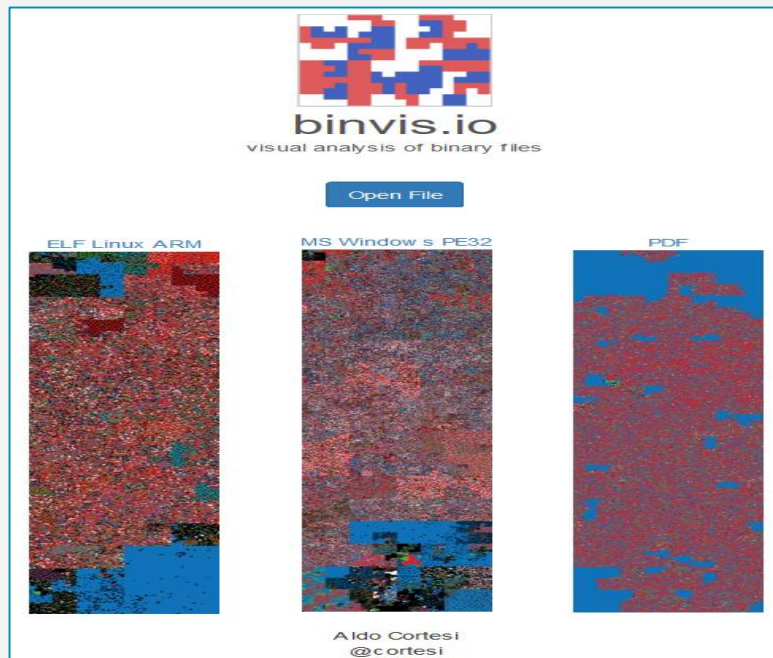
— — —

- Important characteristics:
  - Clustering (locality preserving in 2D)
  - Spatial indexing
- Can be indexed and matched against unknown input for clustering and classification
- Can be used as a visual hash (contrast with cryptographic hashes)

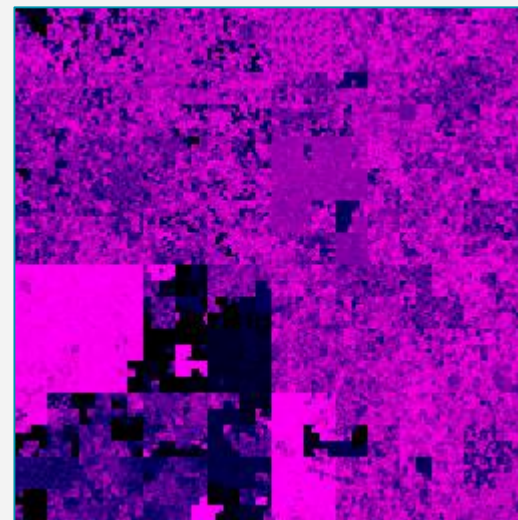
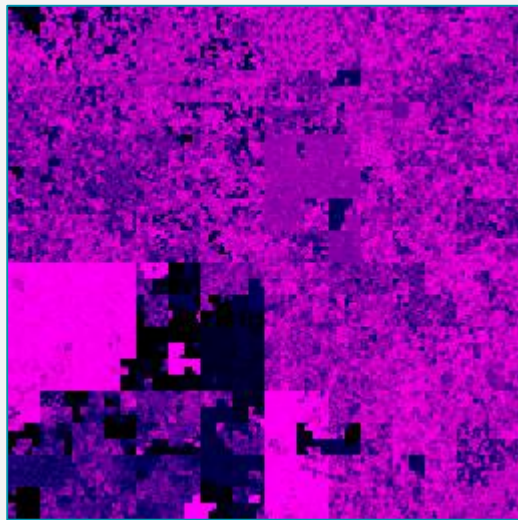
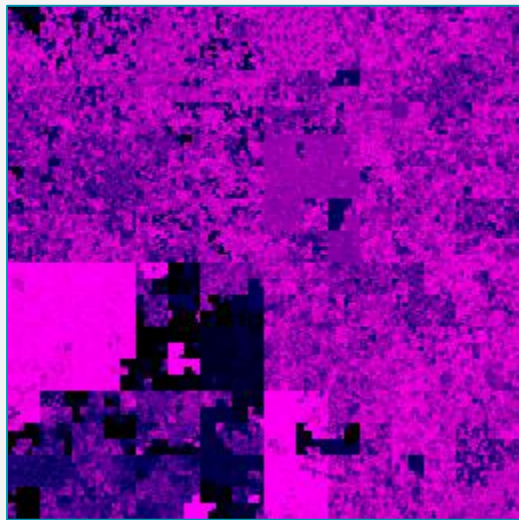
# What is Multi-Dimensional Visualization?

---

- Let's discuss how to use Hilbert curves to visualize malware structure and APIs
- [Aldo Cortesi \(@cortesi\)](#) has posted about this in depth on his [blog](#)
- Check out his project [binvis.io](#) for more details

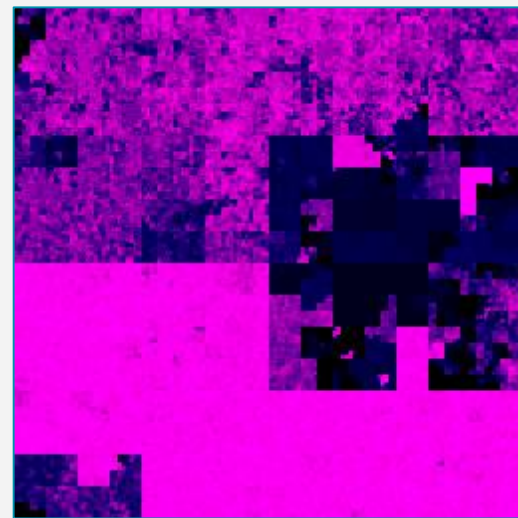
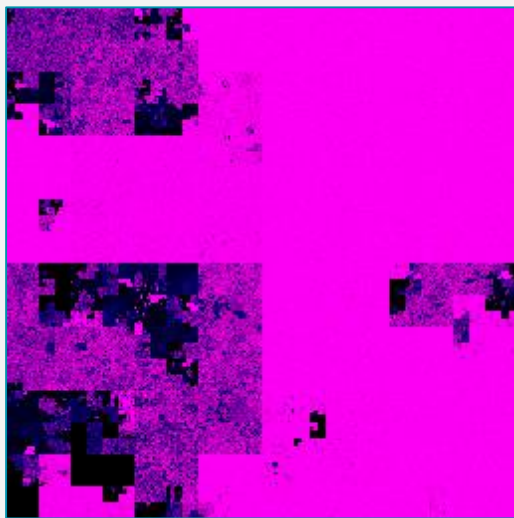
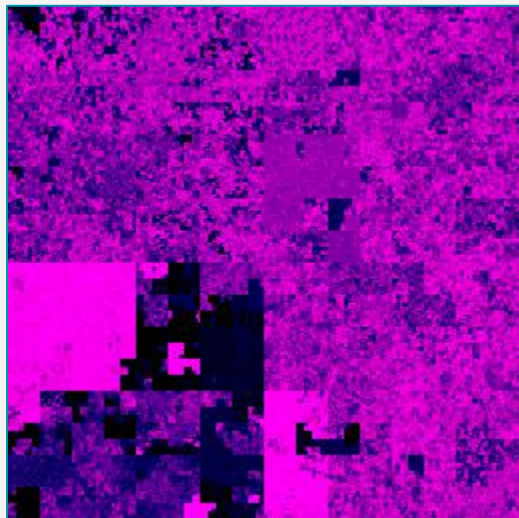


# What is Multi-Dimensional Visualization?



- Hilbert curves created using [scurve](#) library from [@cortesi](#)
- All files have unique hashes but (structurally) similar Hilbert curve representations

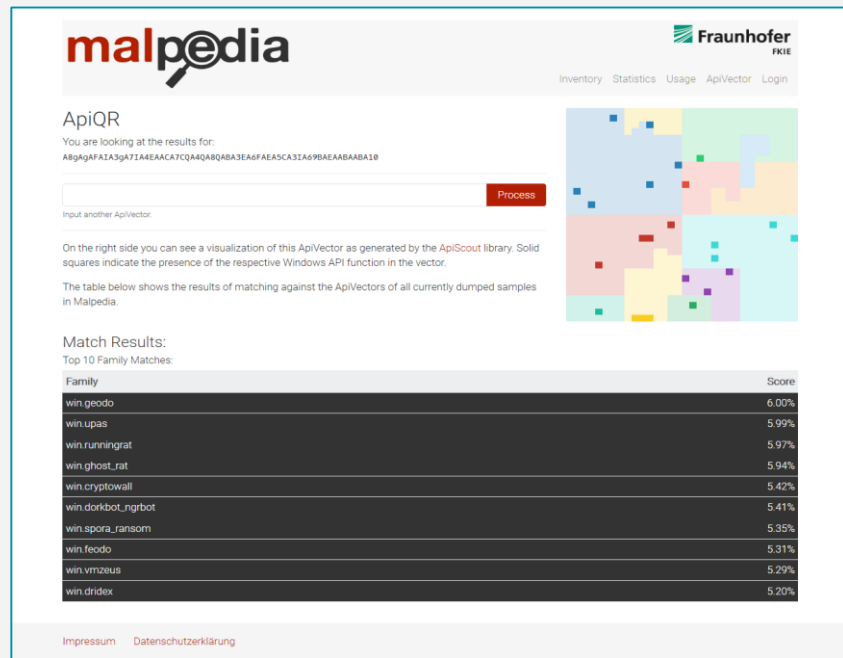
# What is Multi-Dimensional Visualization?



- Difficult to identify offsets for prominent structures
- Unable to retain shape for similar content at different offsets

# Context-aware Multi-Dimensional Visualization

- [Daniel Plohmann](#) has used Hilbert curve to visualize [import APIs](#)
- Check out the [Malpedia](#) service to see how imported APIs from PE files are used to create a visual hash ([ApiQR](#))



**malpedia** Fraunhofer  
PKIE

Inventory Statistics Usage ApiVector Login

### ApiQR

You are looking at the results for:  
A8gAgFA1A3gkT1A4EAAC7CQ4Q8Q8A3EA6FAEASC31A69BAEABABA1B

Input another ApiVector.

On the right side you can see a visualization of this ApiVector as generated by the ApiScout library. Solid squares indicate the presence of the respective Windows API function in the vector.

The table below shows the results of matching against the ApiVectors of all currently dumped samples in Malpedia.

#### Match Results:

Top 10 Family Matches:

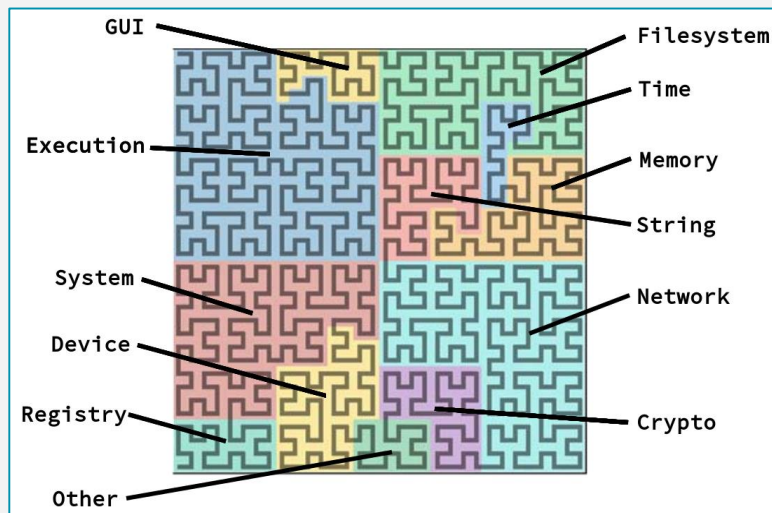
Family	Score
win.geodo	6.00%
win.upas	5.99%
win.runningrat	5.97%
win.ghost_rat	5.94%
win.cryptowall	5.42%
win.dorkbot_ngrbot	5.41%
win.spora_ransom	5.35%
win.feodo	5.31%
win.vmzeus	5.29%
win.dridex	5.20%

[Impressum](#) [Datenschutzerklärung](#)

# Context-aware Multi-Dimensional Visualization

---

- Use file-format specific context to create Hilbert curves
- For PE files, visualize:
  - Import APIs from IAT
  - System Calls from behavior report



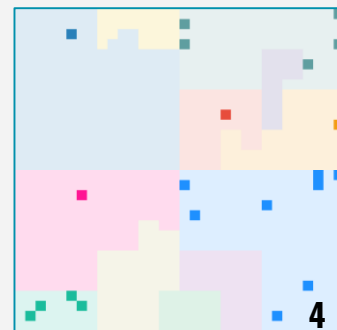
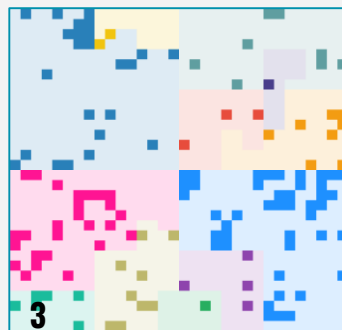
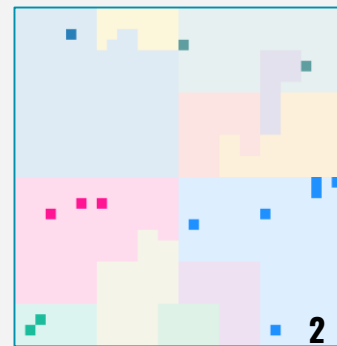
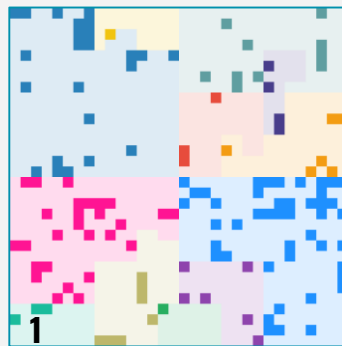
[ByteAtlas: ApiQR representation: Hilbert curve for our 1024 bit ApiVector with the semantic categories](#)



# Context-aware Multi-Dimensional Visualization

---

- APIs from IAT and behavior report:
  - APIs are extracted from IAT and sandbox execution report
  - Names are normalized (eg: `RegOpenKey <- RegOpenKeyExW`)
  - A 32x32 bit vector (1024 cells) is created and mapped on Hilbert curve
  - A sliding window scheme is used to create animated Hilbert curve from extracted APIs



# Usecase: #1 APT33

```
(env) ~/toolbox/misc/angad [master L] ✓
02:54 $ python angad.py -i input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/

Angad (v0.1) - Ankur Tyagi (@7h3rAm)

[byteview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.vlr:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
curvenap: hilbert
curvetype: square
curvecolor: entropy
mode: fileview (396973 bytes)
[1/1] /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.square.entropy.png

[latview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.vlr:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
importsvector: /home/ankur/toolbox/misc/angad/data/winapi1024v1.txt
cvector: ._t._f_p_?_,#fNks*kWnzKIQJMQEACLJAAgA3SAWggAgABA4sA5gACIA5gA3EA3MA9gA5QA7gA6kA30EA30
importapis: 137
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.iv.png

[behaviorview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.behavior.json:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
importsvector: /home/ankur/toolbox/misc/angad/data/winapi1024v1.txt
cvector: LAoARA10CA10gA6IA8IA6CA82IA31EA6
behaviorapis: 14
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.bv.png

[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 130aa7bd89aa4b68f1561d33bd0068ad96abc0cd78c74cdc3eb89cf19076916 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)
[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 285aa5fe83503fee229bb4a1ab861427933c7ab047f63472543f75d8872735a9 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)
[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 28cb4114ee5615e9fa039c913d41db660c089b206565d25a4342eeaf71d9b7f9 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)

[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 130aa7bd89aa4b68f1561d33bd0068ad96abc0cd78c74cdc3eb89cf19076916 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)
[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 285aa5fe83503fee229bb4a1ab861427933c7ab047f63472543f75d8872735a9 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)
[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 28cb4114ee5615e9fa039c913d41db660c089b206565d25a4342eeaf71d9b7f9 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)

[+] saved /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/report.html
[+] saved /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/summary.json
```

# Usecase: #1 APT33

## Angad (v0.1): apt33

apt, apt33

# SHA256

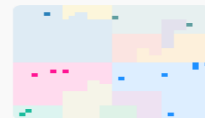
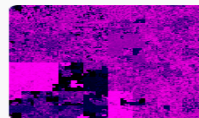
ByteView

IATView

BehaviorView

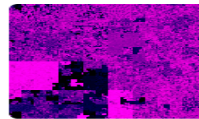
1. 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d

Packer: NA



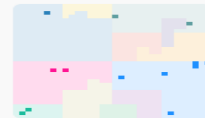
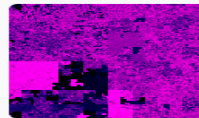
2. 130aa7bd89aa4b68f1561d33bbd0068ad96abc0cd78c74cdc3eb89cf19076916

Packer: NA



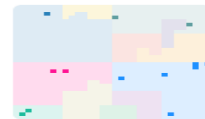
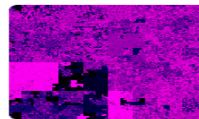
3. 285aa5fe83503fee229bb4a1ab861427933c7ab047f63472543f75d8872735a9

Packer: NA



4. 28cb4114ee5615e9fa039c913d41db660c089b206565d25a4342eeaf71d9b7f9

Packer: NA



@7h3rAm

# Usecase: #2 Dorv

```
(env) ~/toolbox/misc/angad [master L] ✓
02:54 $ python angad.py -i input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/

Angad (v0.1) - Ankur Tyagi (@7h3rAm)

[byteview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.vlr:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
curvenap: hilbert
curvetype: square
curvecolor: entropy
mode: fileview (396973 bytes)
[1/1] /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.square.entropy.png

[latview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.vlr:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
importsvector: /home/ankur/toolbox/misc/angad/data/winapi1024v1.txt
cvector: ._t._f_p_?_,#fNks*kWnzKIQJMQEACLJAAgA3SAAwggAgABA4sA5gACIA5gA3EA3MA9gA5QA7gA6kA30EA30
importapis: 137
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.iv.png

[behaviorview] visualizing input/apt33/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.behavior.json:
reportsdir: /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d
importsvector: /home/ankur/toolbox/misc/angad/data/winapi1024v1.txt
cvector: LAoARA10CA10gA6IA8IA6CA82IA31EA6
behaviorapis: 14
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d.bv.png

[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 130aa7bd89aa4b68f1561d33bd0068ad96abc0cd78c74cdc3eb89cf19076916 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)
[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 285aa5fe83503fee229bb4a1ab861427933c7ab047f63472543f75d8872735a9 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)
[cluster] [imports] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 28cb4114ee5615e9fa039c913d41db660c089b206565d25a4342eeaf71d9b7f9 (0FCBDA96CF1D462CB79CC6DA3958CA2F: 100.00%)

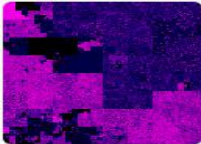

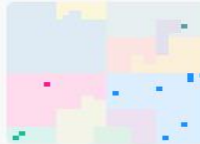
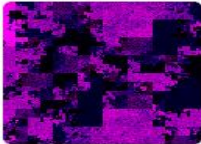

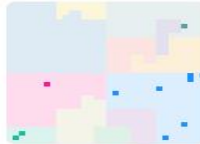
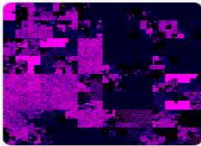

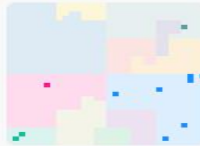
[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 130aa7bd89aa4b68f1561d33bd0068ad96abc0cd78c74cdc3eb89cf19076916 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)
[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 285aa5fe83503fee229bb4a1ab861427933c7ab047f63472543f75d8872735a9 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)
[cluster] [behavior] 0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d == 28cb4114ee5615e9fa039c913d41db660c089b206565d25a4342eeaf71d9b7f9 (0373ECA10E294FD7BD02B249D4E2BC1C: 91.80%)

[+] saved /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/report.html
[+] saved /home/ankur/toolbox/misc/angad/reports/0f80b73706df263d337c4da52aad67c3699d1deea00aafe78e604d61a54c649d/summary.json
```

# Usecase: #2 Dorv

Angad (v0.1): dorv

trojan

#	SHA256	ByteView	IATView	BehaviorView
1.	<a href="#">0275acf5332c354ccda0a3daea804005e42219c4500edd23ddc7091d277d0434</a> <b>Packer:</b> UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser			
2.	<a href="#">038f68c4afa8213c38fc861f6e854a2d9ef636f3f3ab86003721f2af61e1fcd7</a> <b>Packer:</b> UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser			
3.	<a href="#">03fc48e75f754ad29e4420ebfdf2ec87ce5c59cf6f2fce0b7e4daedd19a31ff6</a> <b>Packer:</b> UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser			

# Usecase: #2 Dorv

## Angad (v0.1): dorv

trojan

#	SHA256	ByteView	IATView	BehaviorView
3.	<b>03fc48e75f754ad29e4420ebfdf2ec87ce5c59cf6f2fce0b7e4daedd19a31ff6</b> <b>Packer:</b> UPX 2.90 [LZMA] -> Markus Oberhumer, Laszlo Molnar & John Reiser			
4.	<b>02f136ec7a39f40c26973f36e0209401a8f0343aec6b743164f2e621d45fb7aa</b> <b>Packer:</b> PECompact 2.xx --> BitSum Technologies			
5.	<b>03ddace7f36bc9c57e679237b2c5f0fc31f3763bc467bcfebce7132717b69faa</b> <b>Packer:</b> PECompact 2.xx --> BitSum Technologies			
6.	<b>03fd30ac12245f5d135d596dca97800893507df8aac973b8c01f02a637d99519</b> <b>Packer:</b> PECompact 2.xx --> BitSum Technologies			



@7h3rAm

# Usecase: #3 Mooqkel

```
(env) ~/toolbox/misc/angad [master L1]
$ python angad.py -i input/mooqkel/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/

Angad (v0.1) - Ankur Tyagi (@7h3rAm)

[byteview] visualizing input/mooqkel/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.v:ir
reportsdir: /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5
curvemap: hilbert
curvetype: square
curvecolor: entropy
mode: fileview (2786304 bytes)
[1/1] /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.square.entropy.png

[latview] visualizing input/mooqkel/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.v:lr
reportsdir: /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5
importsvector: /home/ankur/toolbox/misc/angad/data/winnapi1024v1.txt
cvector: \_f\._f_p_._,IeekeGUgACACXCCABAI4Y43W3WA3MAABAIAIIEAABACEABA3EAABASCA7QAQA2BAAGAQAI4EA21CAAGAS
importapis: 136
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.lv.png

[behaviorview] visualizing input/mooqkel/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.behavior.json
reportsdir: /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5
importsvector: /home/ankur/toolbox/misc/angad/data/winnapi1024v1.txt
cvector: LAGARAEACA17IA8IAAIQQACASCAIAI512A3Q3A3IA3IEGAS
behaviorapis: 21
exported defaultvector as png /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5.bv.png

[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 043dee2920046475ca4909e340e4ab31712064ae792f570b8dca19600770c78 (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0a45ee3c3d12af3571d80bd4cd60f37801b416044e411786aa5ab343836702e1 (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0f3da39c086901edde02cda6680cb94c1f6f6870377e0058810ab1584f023b (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0fcd603b6e8d04d31562244a7ab105d3453ac91e7524540def7184c030b3a2c4 (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 11187d65cee9f2a0431fc55b0f1be093d8042fd5ebfb6e7270b86d519534a8b (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
[cluster] [imports] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 1f01db65cc1b969e8736935b50c8ef743a8ad302636cabbf85ffaebd62212f (09B049C5A91A4AE1BFF3C14835CD9787: 100.00%)
















[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 01d09cd684edfae388e23743f98e278812d5b01abf74131fe03515db5ab7b8add (0373ECA10E294FD7B02B249D4E28C1: 95.74%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 098649bd64541c6bee0821a5a42837263fea15035d94213f338a5db141ec6c6 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 09b412001ceab6f0b4aac4bc4b0f9add539ef47be23ee967ea26636907f92 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0a45ee3c3d12af3571d80bd4cd60f37801b416044e411786aa5ab343836702e1 (0373ECA10E294FD7B02B249D4E28C1: 93.48%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0b75826fa1bc1f5df5f3decc2e605eb407a29172e7b2abeb872c2e97f40508b (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0bb2c48485123c9ba75ac21537b7b424ea2f5030538ca8929ab84404a8147e5 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 9cf70e9dad938772bde99190ab92c589cdf8ee189b430ef47c76ea34a52aba37 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0ee3f274f96cc5ff9f1595001946eecd36aa523b20fd79a7a871a66caa351a13 (0373ECA10E294FD7B02B249D4E28C1: 95.74%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 05fddfff65967fe368fcc4541257894A5edc2982f3292ba6878f459659ff7c (0373ECA10E294FD7B02B249D4E28C1: 95.74%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0fc72014c954097af936cdcc99e14f6de7236ca44be7e04bbd4ef49ea0b9043 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 0fcd603b6e8d04d31562244a7ab105d3453ac91e7524540def7184c030b3a2c4 (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 11187d65cee9f2a0431fc55b0f1be093d8042fd5ebfb6e7270b86d519534a8b (0373ECA10E294FD7B02B249D4E28C1: 100.00%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 18dc39a641ce25208a1d0bc310bc3c4e81dcf956a8d7644ba19f8548d8317 (0373ECA10E294FD7B02B249D4E28C1: 93.48%)
[cluster] [behavior] 01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5 -- 1f01db65cc1b969e8736935b50c8ef743a8ad302636cabbf85ffaebd62212f (0373ECA10E294FD7B02B249D4E28C1: 93.48%)

[+] saved /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/report.html
[+] saved /home/ankur/toolbox/misc/angad/reports/01b6ffc35fea26d6486226faca1ec371d535fc72b9fa13c9a3a2706b8dd1af5/summary.json
```

# Usecase: #3 Mooqkel

## Angad (v0.1): mooqkel

trojan, rat

#	SHA256	ByteView	IATView	BehaviorView
1.	<b>01b6ffc35fea26d6486226facaa1ec371d535fc72b9fa13c9a3a2706b8dd1af5</b> Packer: UPX_LZMA, UPX			
2.	<b>043dee2920046a75ce4909e340e4ab31712064ae792f570b8dca169600770c78</b> Packer: UPX_LZMA, UPX			
3.	<b>0a45ee3c3d12af3571d80bd4cd60f37801b416044e411786aa5ab343836702e1</b> Packer: UPX_LZMA, UPX			
4.	<b>01d09cd684edfae388e23743f98e27881d2b501abf7413f1e0351db5ab7b8add</b> Packer: UPX			
5.	<b>098649ebd5451c6bee0821a5a42837263feac15035d94213f338a5db141ec6c6</b> Packer: UPX			



@7h3rAm



# Ending Notes / Q&A

— — —

- <https://github.com/7h3rAm/angad/>



- [@7h3rAm](#) 

- **Thanks:**

- Aldo Cortesi: [@cortesi](#)
- Daniel Plohmann: [@push\\_pnx](#)
- xkcd :)