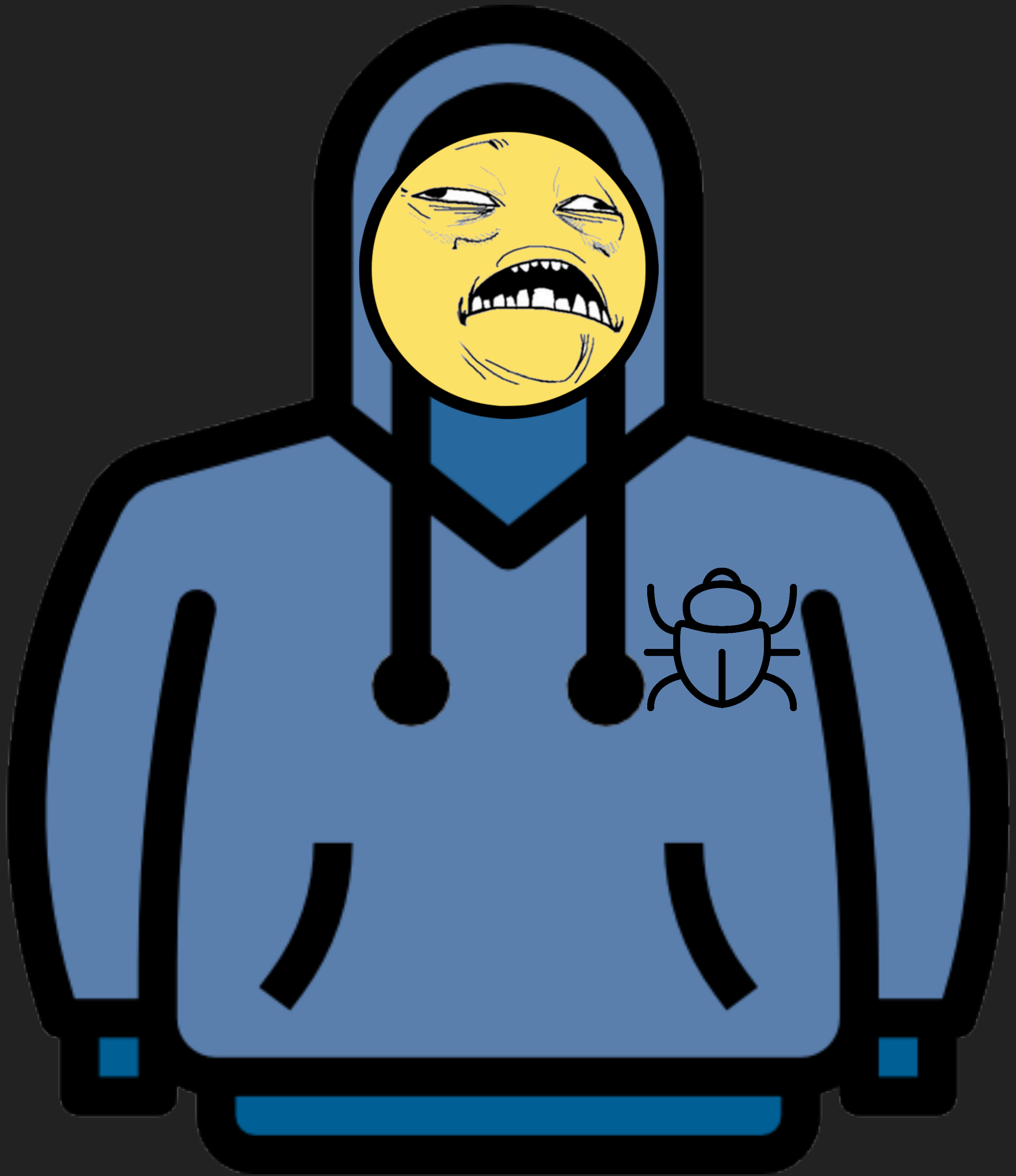
much malware

HACK IN BOAT

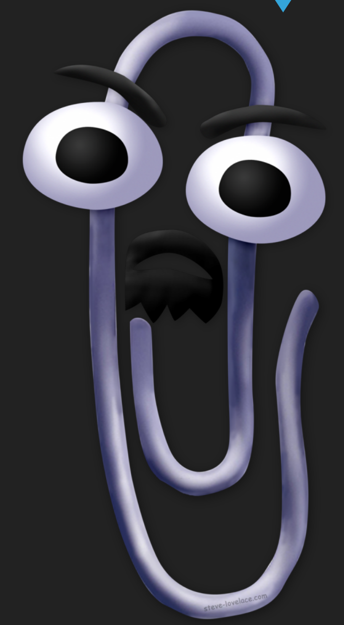
very sample

Alessandro Tanasi (@jekil)

YEAH, IT IS.



MALWARE… IS MALICIOUS SOFTWARE



CRASH COURSE

MALWARE 101

TYPES OF ANALYSIS

- **Static** analysis
  - Analyzing looking at the malware.
- **Dynamic** analysis
  - Analyzing by executing the malware
- **Memory** analysis
  - Analyzing the RAM for artifacts.

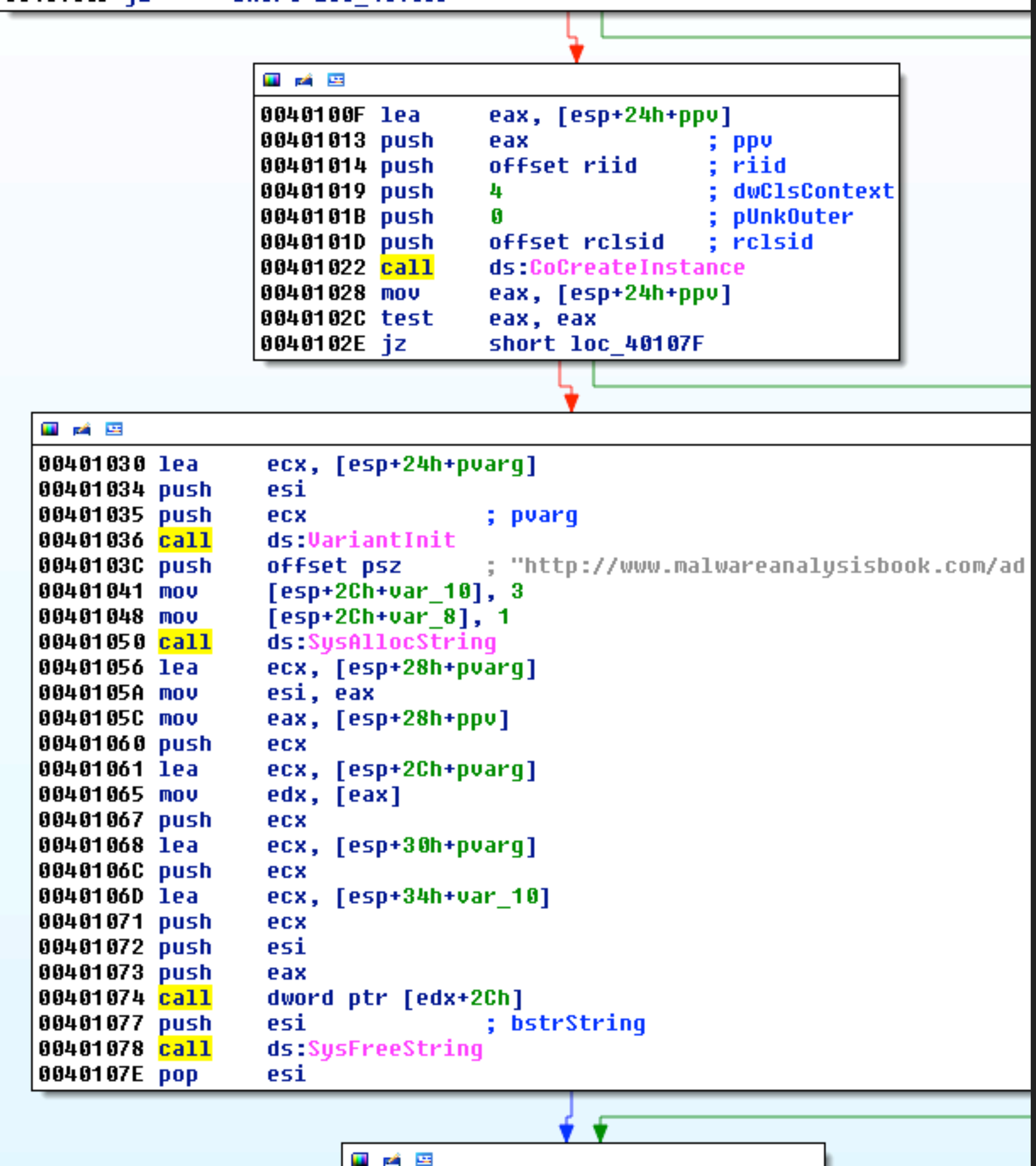
TECHNIQUES

STATIC ANALYSIS

- File type.
- Hash / fuzzy hash.
- Strings search.
- File obfuscation detection (packers).
- Imports.
- Disassembly.

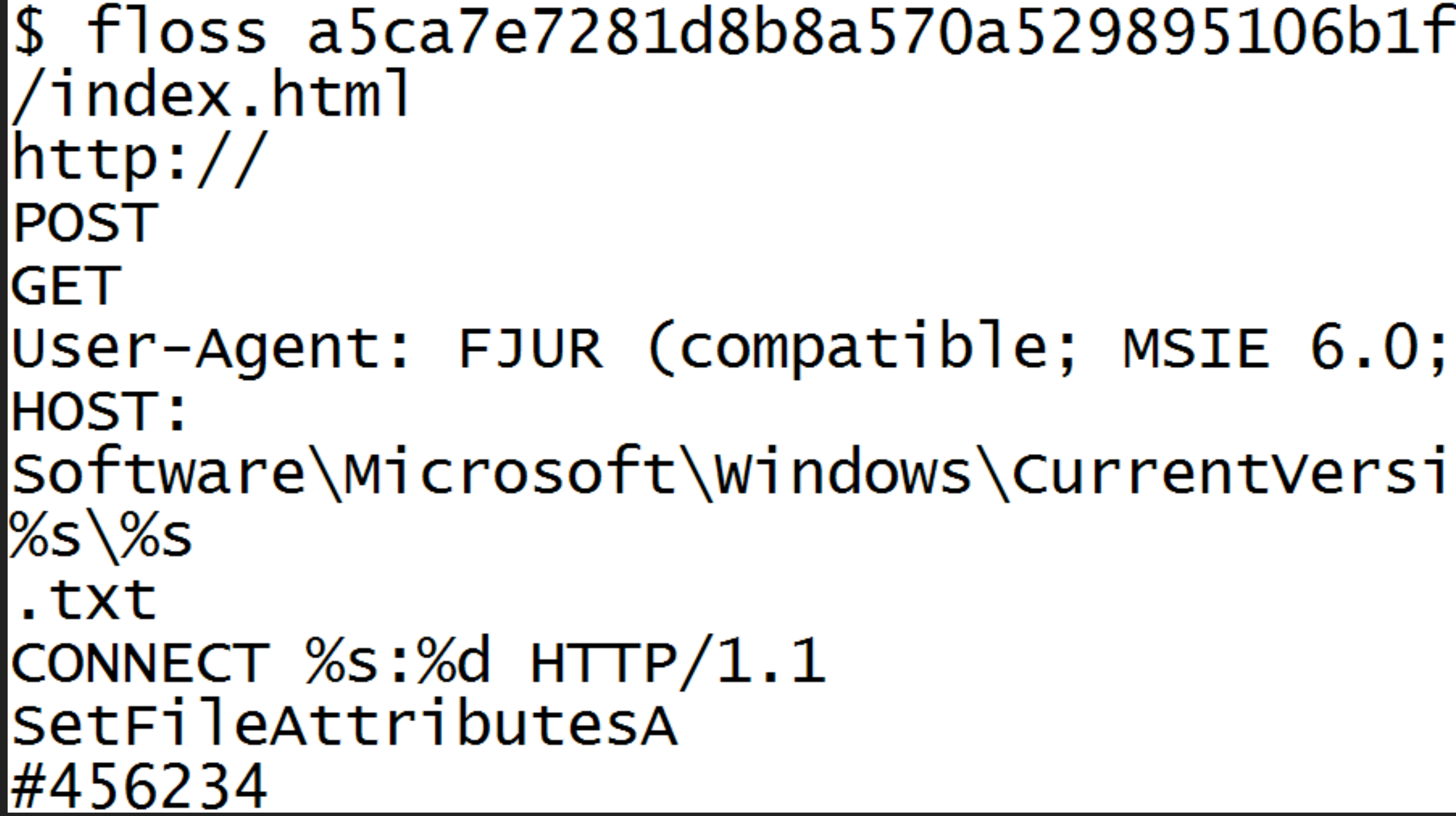
DYNAMIC ANALYSIS

- File system activity.
- Process activity.
- Network activity.
- Registry activity.
- Collect memory artifacts.
- Dropped files.
- Screenshots.

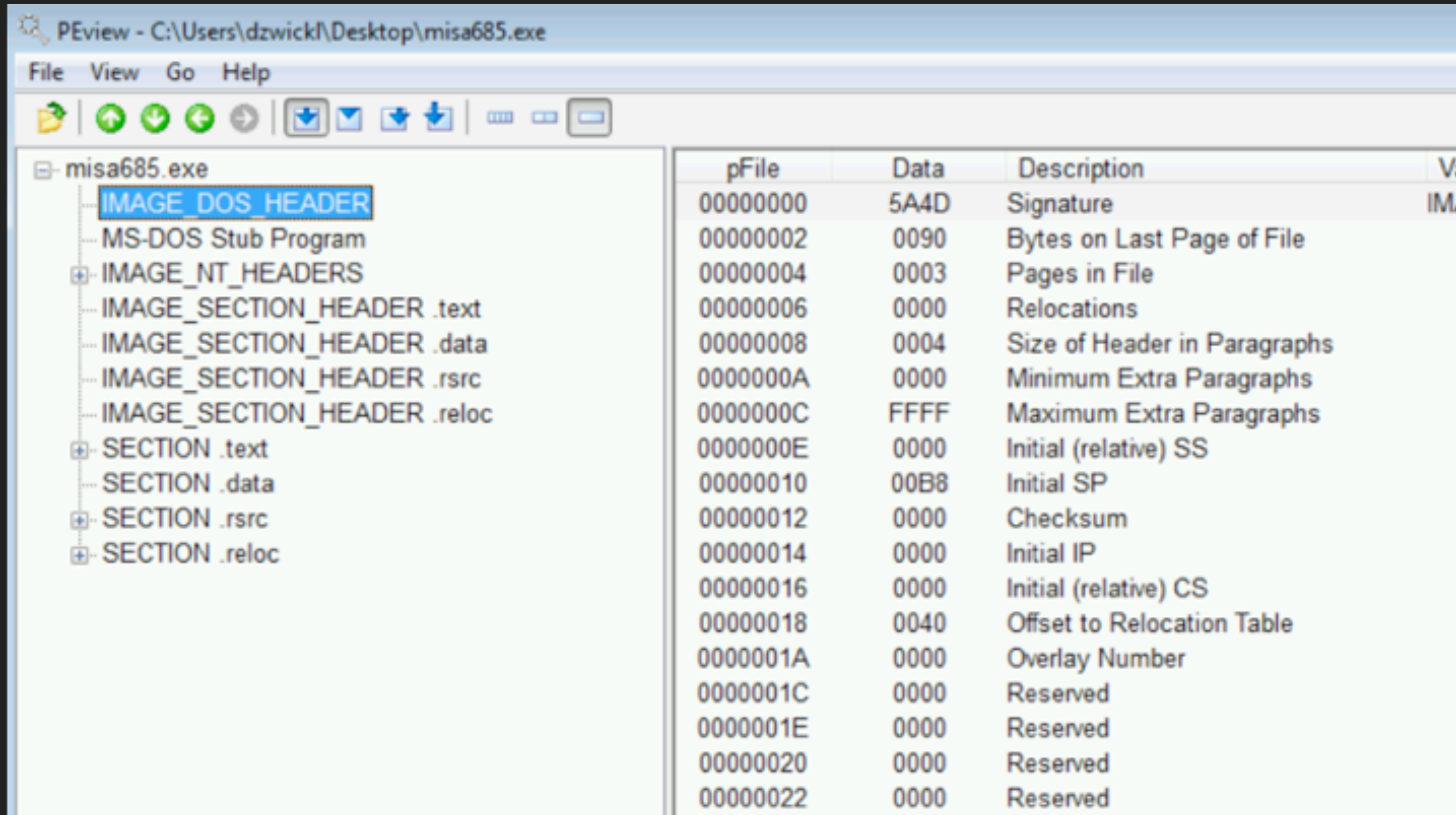


```
0040100F lea     eax, [esp+24h+ppv]
00401013 push    eax                ; ppv
00401014 push    offset riid        ; riid
00401019 push    4                  ; dwClsContext
0040101B push    0                  ; pUnkOuter
0040101D push    offset rclsid      ; rclsid
00401022 call    ds:CoCreateInstance
00401028 mov     eax, [esp+24h+ppv]
0040102C test    eax, eax
0040102E jz      short loc_40107F
```

```
00401030 lea     ecx, [esp+24h+pvarg]
00401034 push    esi
00401035 push    ecx                ; pvarg
00401036 call    ds:VariantInit
0040103C push    offset psz         ; "http://www.malwareanalysisbook.com/ad
00401041 mov     [esp+2Ch+var_10], 3
00401048 mov     [esp+2Ch+var_8], 1
00401050 call    ds:SysAllocString
00401056 lea     ecx, [esp+28h+pvarg]
0040105A mov     esi, eax
0040105C mov     eax, [esp+28h+ppv]
00401060 push    ecx
00401061 lea     ecx, [esp+2Ch+pvarg]
00401065 mov     edx, [eax]
00401067 push    ecx
00401068 lea     ecx, [esp+30h+pvarg]
0040106C push    ecx
0040106D lea     ecx, [esp+34h+var_10]
00401071 push    ecx
00401072 push    esi
00401073 push    eax
00401074 call    dword ptr [edx+2Ch]
00401077 push    esi                ; bstrString
00401078 call    ds:SysFreeString
0040107E pop     esi
```

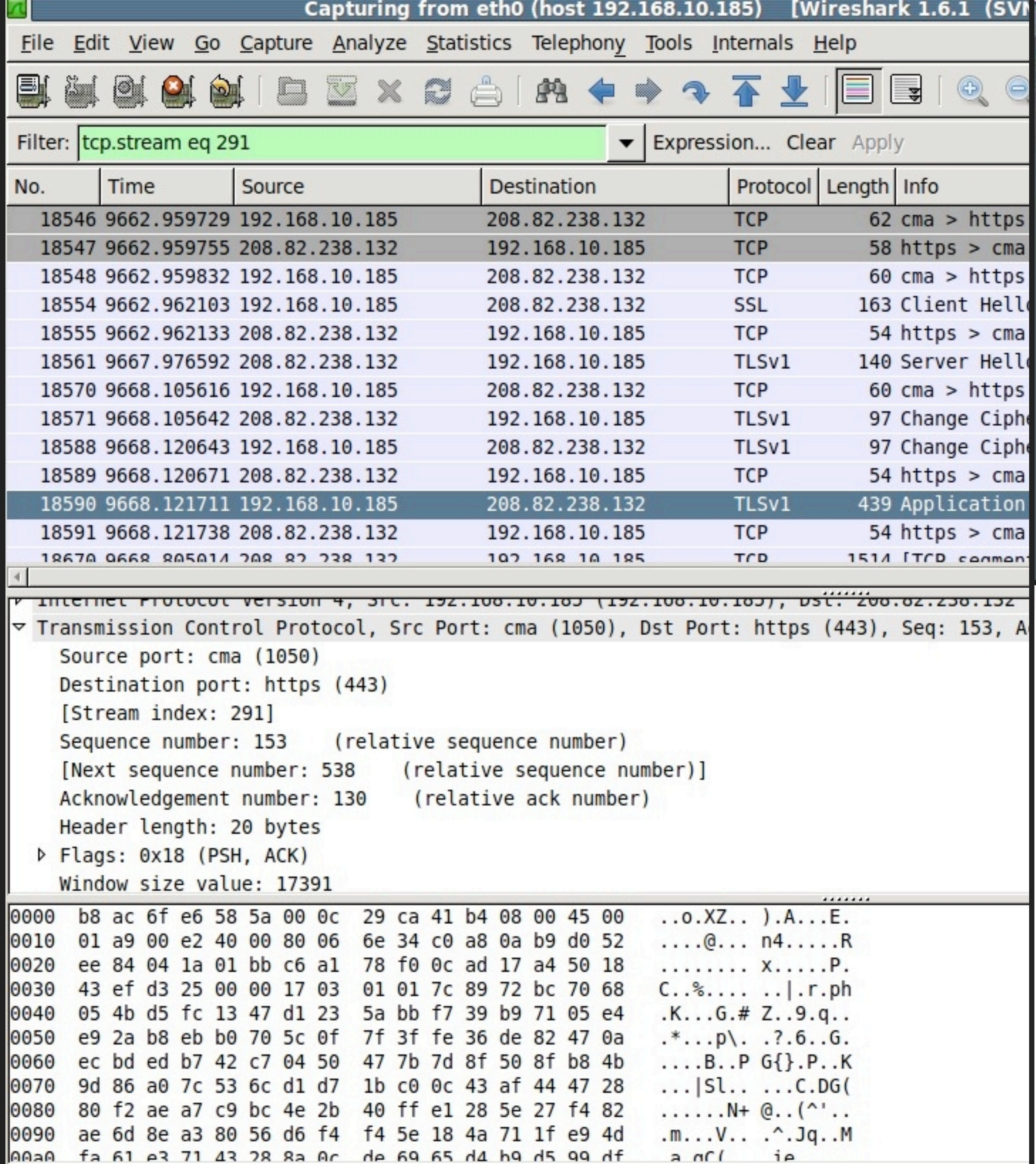


```
$ floss a5ca7e7281d8b8a570a529895106b1f
/index.html
http://
POST
GET
User-Agent: FJUR (compatible; MSIE 6.0;
HOST:
Software\Microsoft\Windows\CurrentVersi
%s\%s
.txt
CONNECT %s:%d HTTP/1.1
SetFileAttributesA
#456234
```



PEview - C:\Users\dzwickl\Desktop\misa685.exe

pFile	Data	Description	V
00000000	5A4D	Signature	IM
00000002	0090	Bytes on Last Page of File	
00000004	0003	Pages in File	
00000006	0000	Relocations	
00000008	0004	Size of Header in Paragraphs	
0000000A	0000	Minimum Extra Paragraphs	
0000000C	FFFF	Maximum Extra Paragraphs	
0000000E	0000	Initial (relative) SS	
00000010	00B8	Initial SP	
00000012	0000	Checksum	
00000014	0000	Initial IP	
00000016	0000	Initial (relative) CS	
00000018	0040	Offset to Relocation Table	
0000001A	0000	Overlay Number	
0000001C	0000	Reserved	
0000001E	0000	Reserved	
00000020	0000	Reserved	
00000022	0000	Reserved	

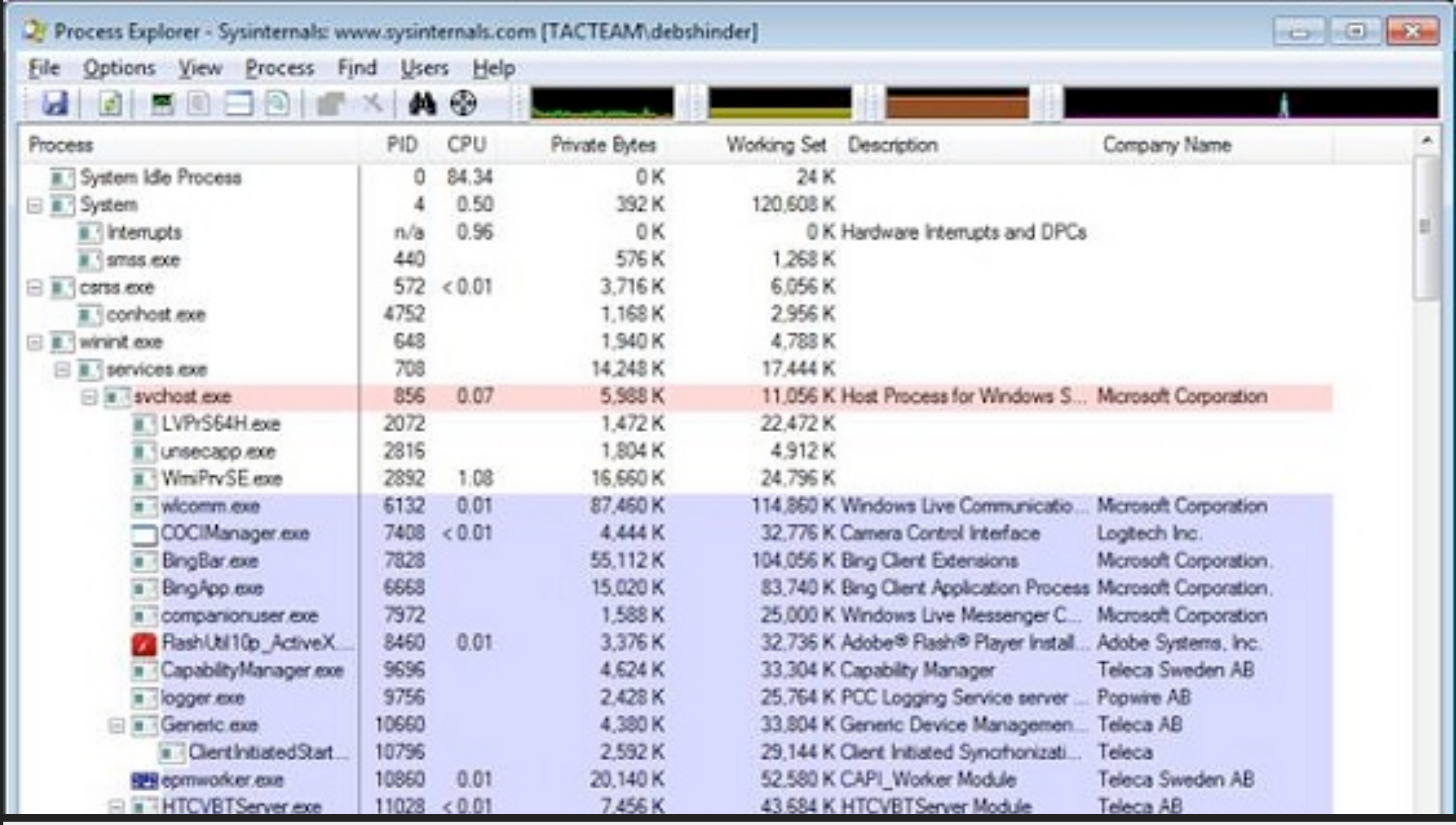

Capturing from eth0 (host 192.168.10.185) [Wireshark 1.6.1 (SVN
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply

Filter: tcp.stream eq 291

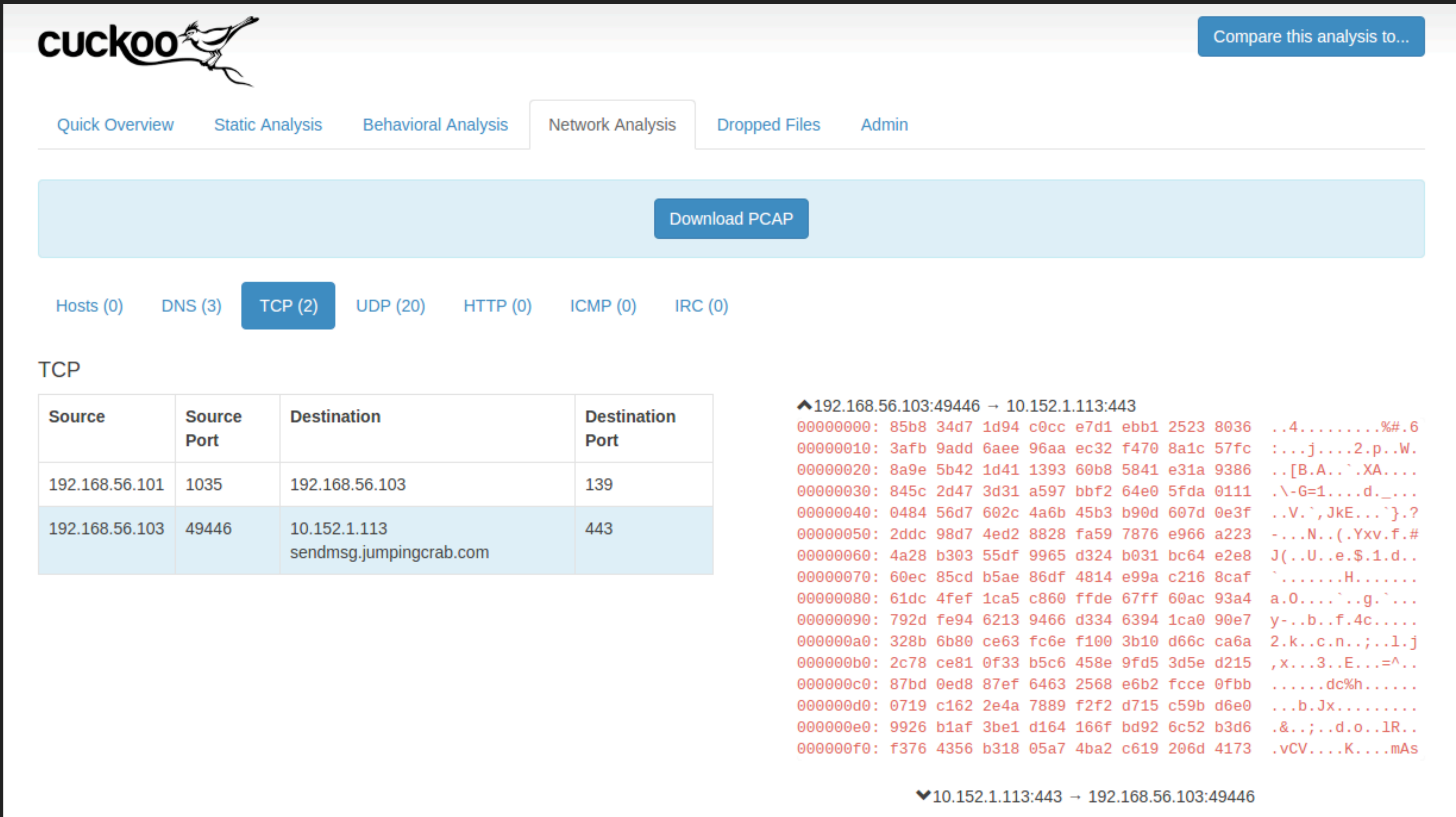
```
No.    Time         Source          Destination     Protocol Length Info
 18546 9662.959729 192.168.10.185  208.82.238.132  TCP          62 cma > https
 18547 9662.959755 208.82.238.132  192.168.10.185  TCP          58 https > cma
 18548 9662.959832 192.168.10.185  208.82.238.132  TCP          60 cma > https
 18554 9662.962103 192.168.10.185  208.82.238.132  SSL         163 Client Hell
 18555 9662.962133 208.82.238.132  192.168.10.185  TCP          54 https > cma
 18561 9667.976592 208.82.238.132  192.168.10.185  TLSv1       140 Server Hell
 18570 9668.105616 192.168.10.185  208.82.238.132  TCP          60 cma > https
 18571 9668.105642 208.82.238.132  192.168.10.185  TLSv1        97 Change Ciphe
 18588 9668.120643 192.168.10.185  208.82.238.132  TLSv1        97 Change Ciphe
 18589 9668.120671 208.82.238.132  192.168.10.185  TCP          54 https > cma
 18590 9668.121711 192.168.10.185  208.82.238.132  TLSv1       439 Application
 18591 9668.121738 208.82.238.132  192.168.10.185  TCP          54 https > cma
 18670 9668.805014 208.82.238.132  192.168.10.185  TCP        1514 [TCP segment
```

```
▷ Internet Protocol Version 4, Src: 192.168.10.185 (192.168.10.185), Dst: 208.82.238.132
▽ Transmission Control Protocol, Src Port: cma (1050), Dst Port: https (443), Seq: 153, A
    Source port: cma (1050)
    Destination port: https (443)
    [Stream index: 291]
    Sequence number: 153    (relative sequence number)
    [Next sequence number: 538    (relative sequence number)]
    Acknowledgement number: 130    (relative ack number)
    Header length: 20 bytes
  ▷ Flags: 0x18 (PSH, ACK)
    Window size value: 17391
```

```
0000  b8 ac 6f e6 58 5a 00 0c  29 ca 41 b4 08 00 45 00   ..o.XZ.. ).A...E.
0010  01 a9 00 e2 40 00 80 06  6e 34 c0 a8 0a b9 d0 52   ....@... n4.....R
0020  ee 84 04 1a 01 bb c6 a1  78 f0 0c ad 17 a4 50 18   ........ x.....P.
0030  43 ef d3 25 00 00 17 03  01 01 7c 89 72 bc 70 68   C..%.... ..|.r.ph
0040  05 4b d5 fc 13 47 d1 23  5a bb f7 39 b9 71 05 e4   .K...G.# Z..9.q..
0050  e9 2a b8 eb b0 70 5c 0f  7f 3f fe 36 de 82 47 0a   .*...p\. .?.6..G.
0060  ec bd ed b7 42 c7 04 50  47 7b 7d 8f 50 8f b8 4b   ....B..P G{}.P..K
0070  9d 86 a0 7c 53 6c d1 d7  1b c0 0c 43 af 44 47 28   ...|Sl.. ...C.DG(
0080  80 f2 ae a7 c9 bc 4e 2b  40 ff e1 28 5e 27 f4 82   ......N+ @..(^'..
0090  ae 6d 8e a3 80 56 d6 f4  f4 5e 18 4a 71 1f e9 4d   .m...V.. .^.Jq..M
00a0  fa 61 e3 71 43 28 8a 0c  de 69 65 d4 b9 d5 99 df   .a.qC(.. .ie.....
```


Process Explorer - Sysinternals: www.sysinternals.com [TACTEAM\debshinder]
File Options View Process Find Users Help

Process	PID	CPU	Private Bytes	Working Set	Description	Company Name
System Idle Process	0	84.34	0 K	24 K		
System	4	0.50	392 K	120,608 K		
Interrupts	n/a	0.96	0 K	0 K	Hardware Interrupts and DPCs	
smss.exe	440		576 K	1,268 K		
csrss.exe	572	< 0.01	3,716 K	6,056 K		
conhost.exe	4752		1,168 K	2,956 K		
wininit.exe	648		1,940 K	4,788 K		
services.exe	708		14,248 K	17,444 K		
svchost.exe	856	0.07	5,988 K	11,056 K	Host Process for Windows S...	Microsoft Corporation
LVPrS64H.exe	2072		1,472 K	22,472 K		
unsecapp.exe	2816		1,804 K	4,912 K		
WmiPrvSE.exe	2892	1.08	16,660 K	24,796 K		
wlcomm.exe	6132	0.01	87,460 K	114,860 K	Windows Live Communicatio...	Microsoft Corporation
COCIManager.exe	7408	< 0.01	4,444 K	32,776 K	Camera Control Interface	Logitech Inc.
BingBar.exe	7828		55,112 K	104,056 K	Bing Client Extensions	Microsoft Corporation.
BingApp.exe	6668		15,020 K	83,740 K	Bing Client Application Process	Microsoft Corporation.
companionuser.exe	7972		1,588 K	25,000 K	Windows Live Messenger C...	Microsoft Corporation
FlashUtil10p_ActiveX...	8460	0.01	3,376 K	32,736 K	Adobe® Flash® Player Install...	Adobe Systems, Inc.
CapabilityManager.exe	9696		4,624 K	33,304 K	Capability Manager	Teleca Sweden AB
logger.exe	9756		2,428 K	25,764 K	PCC Logging Service server ...	Popwire AB
Generic.exe	10660		4,380 K	33,804 K	Generic Device Managemen...	Teleca AB
ClientInitiatedStart...	10796		2,592 K	29,144 K	Client Initiated Synchronizati...	Teleca
epmworker.exe	10860	0.01	20,140 K	52,580 K	CAPI_Worker Module	Teleca Sweden AB
HTCVBTServer.exe	11028	< 0.01	7,456 K	43,684 K	HTCVBTServer Module	Teleca AB



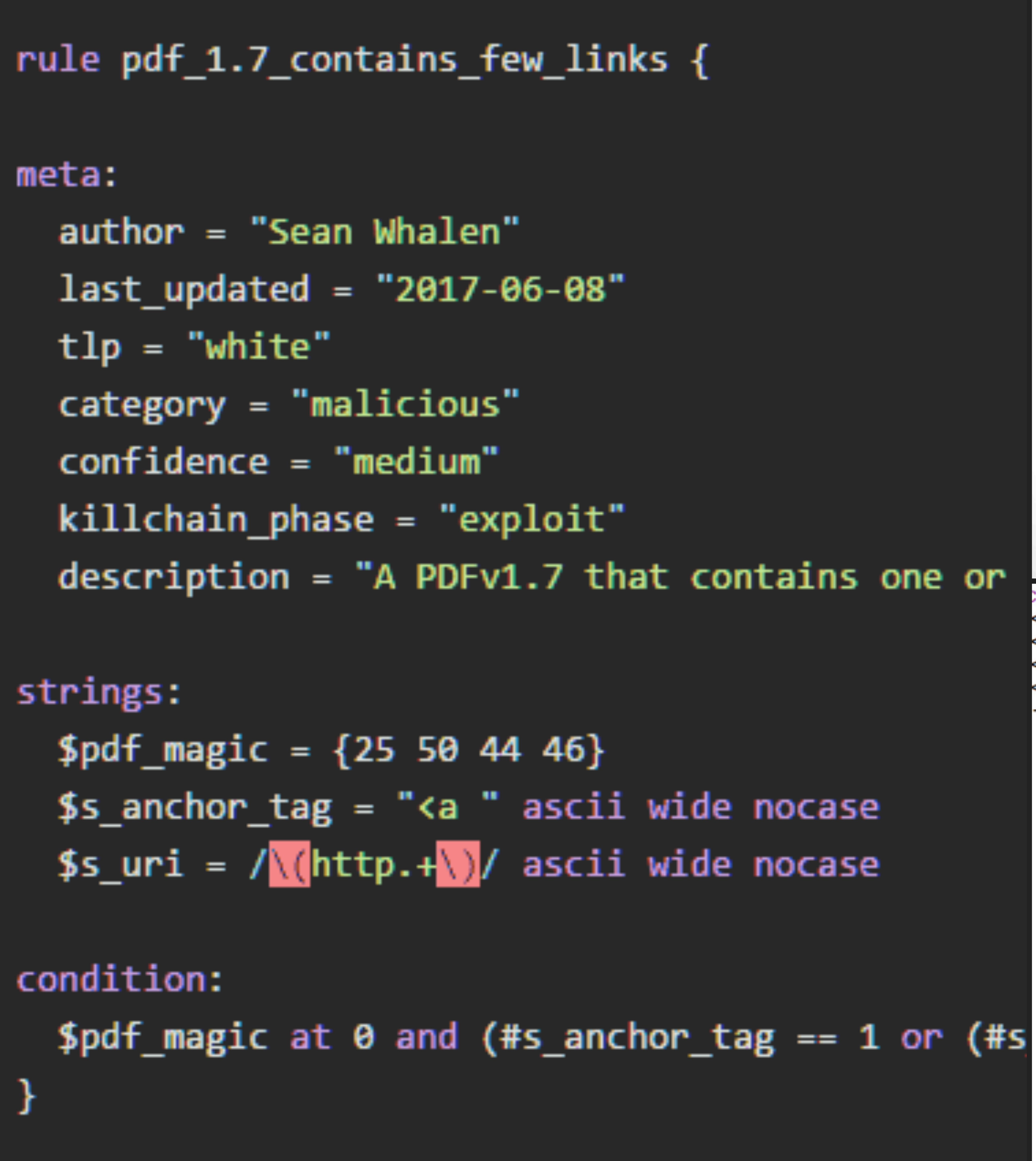
TCP

Source	Source Port	Destination	Destination Port
192.168.56.101	1035	192.168.56.103	139
192.168.56.103	49446	10.152.1.113 sendmsg.jumpingcrab.com	443

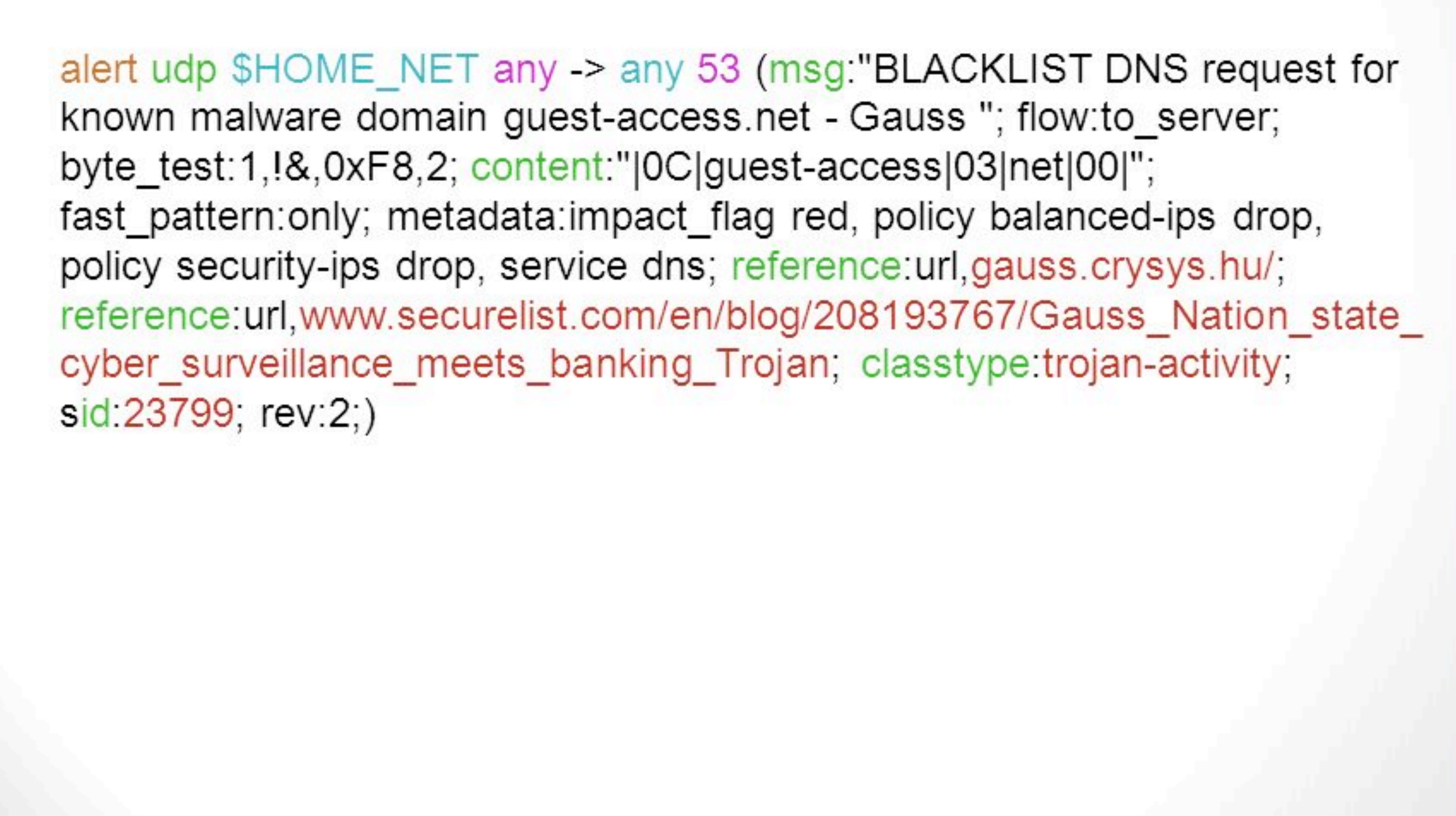
^192.168.56.103:49446 → 10.152.1.113:443

```
00000000: 85b8 34d7 1d94 c0cc e7d1 ebb1 2523 8036  ..4.........%#.6
00000010: 3afb 9add 6aee 96aa ec32 f470 8a1c 57fc  :...j....2.p..W.
00000020: 8a9e 5b42 1d41 1393 60b8 5841 e31a 9386  ..[B.A..`.XA....
00000030: 845c 2d47 3d31 a597 bbf2 64e0 5fda 0111  .\-G=1....d._...
00000040: 0484 56d7 602c 4a6b 45b3 b90d 607d 0e3f  ..V.`,JkE...`}.?
00000050: 2ddc 98d7 4ed2 8828 fa59 7876 e966 a223  -...N..(.Yxv.f.#
00000060: 4a28 b303 55df 9965 d324 b031 bc64 e2e8  J(..U..e.$.1.d..
00000070: 60ec 85cd b5ae 86df 4814 e99a c216 8caf  `.......H.......
00000080: 61dc 4fef 1ca5 c860 ffde 67ff 60ac 93a4  a.O....`..g.`...
00000090: 792d fe94 6213 9466 d334 6394 1ca0 90e7  y-..b..f.4c.....
000000a0: 328b 6b80 ce63 fc6e f100 3b10 d66c ca6a  2.k..c.n..;..l.j
000000b0: 2c78 ce81 0f33 b5c6 458e 9fd5 3d5e d215  ,x...3..E...=^..
000000c0: 87bd 0ed8 87ef 6463 2568 e6b2 fcce 0fbb  ......dc%h......
000000d0: 0719 c162 2e4a 7889 f2f2 d715 c59b d6e0  ...b.Jx.........
000000e0: 9926 b1af 3be1 d164 166f bd92 6c52 b3d6  .&..;..d.o..lR..
000000f0: f376 4356 b318 05a7 4ba2 c619 206d 4173  .vCV....K....mAs
```

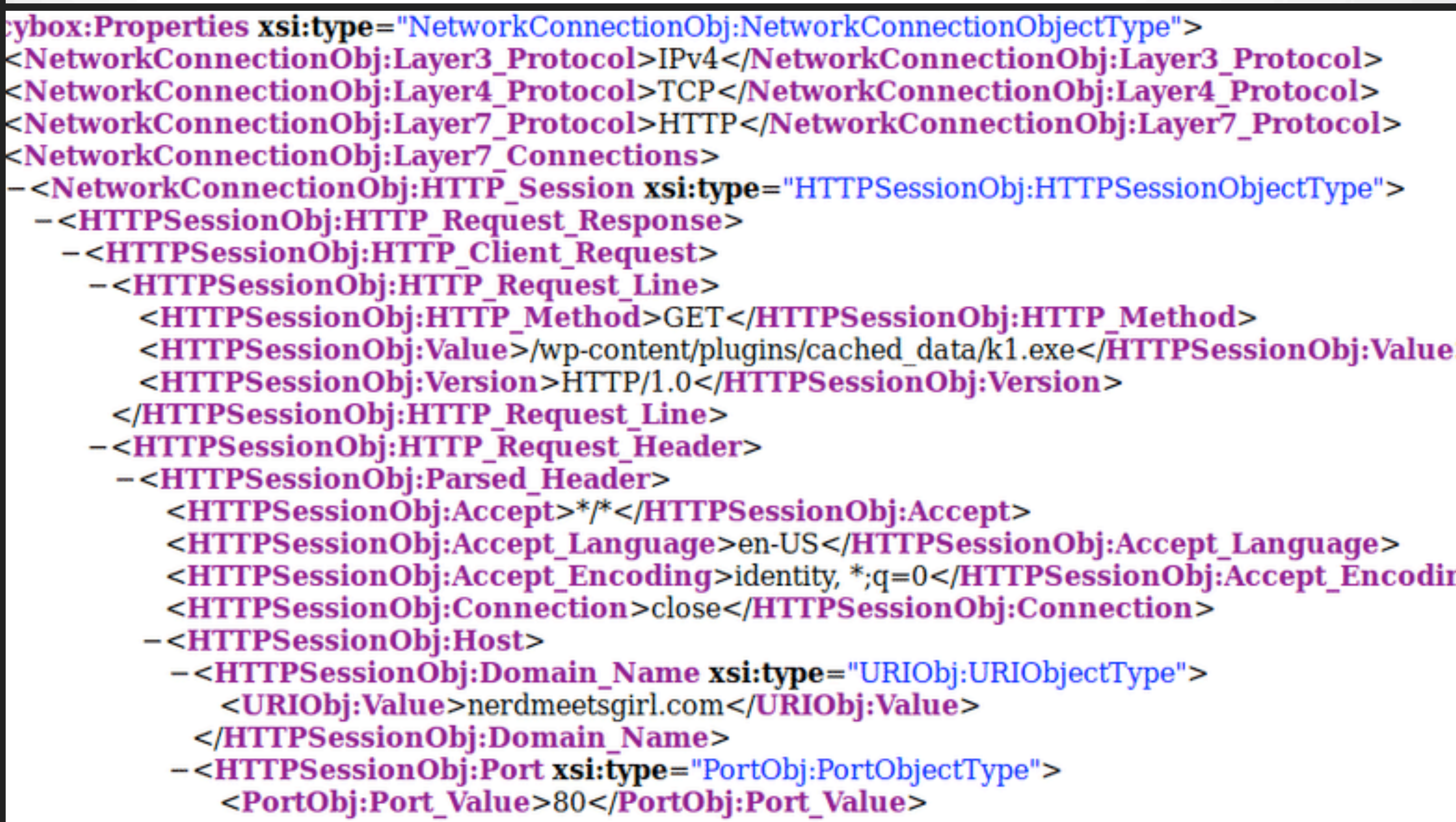
⌄10.152.1.113:443 → 192.168.56.103:49446



```
rule pdf_1.7_contains_few_links {

meta:
  author = "Sean Whalen"
  last_updated = "2017-06-08"
  tlp = "white"
  category = "malicious"
  confidence = "medium"
  killchain_phase = "exploit"
  description = "A PDFv1.7 that contains one or

strings:
  $pdf_magic = {25 50 44 46}
  $s_anchor_tag = "<a " ascii wide nocase
  $s_uri = /\(http.+\)/ ascii wide nocase

condition:
  $pdf_magic at 0 and (#s_anchor_tag == 1 or (#s
}
```

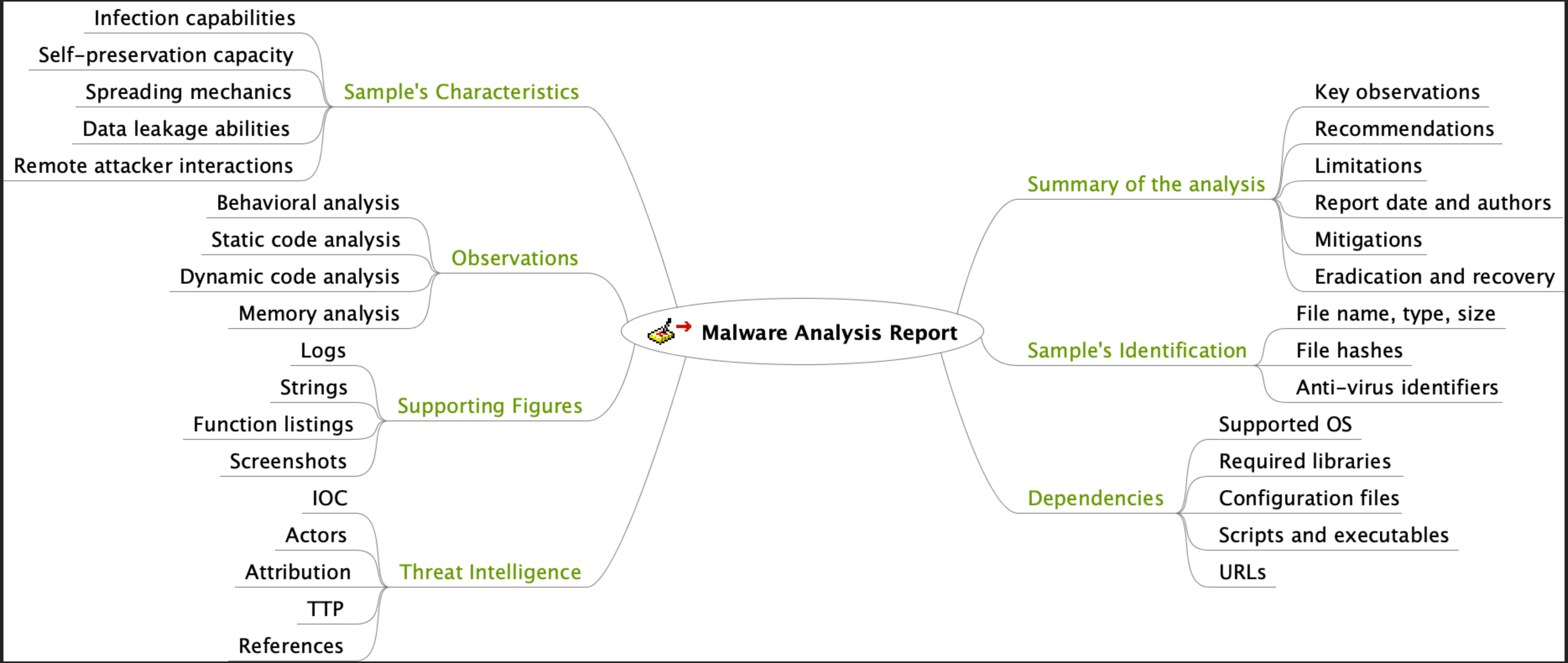


```
alert udp $HOME_NET any -> any 53 (msg:"BLACKLIST DNS request for
known malware domain guest-access.net - Gauss "; flow:to_server;
byte_test:1,!&,0xF8,2; content:"|0C|guest-access|03|net|00|";
fast_pattern:only; metadata:impact_flag red, policy balanced-ips drop,
policy security-ips drop, service dns; reference:url,gauss.crysys.hu/;
reference:url,www.securelist.com/en/blog/208193767/Gauss_Nation_state_
cyber_surveillance_meets_banking_Trojan; classtype:trojan-activity;
sid:23799; rev:2;)
```



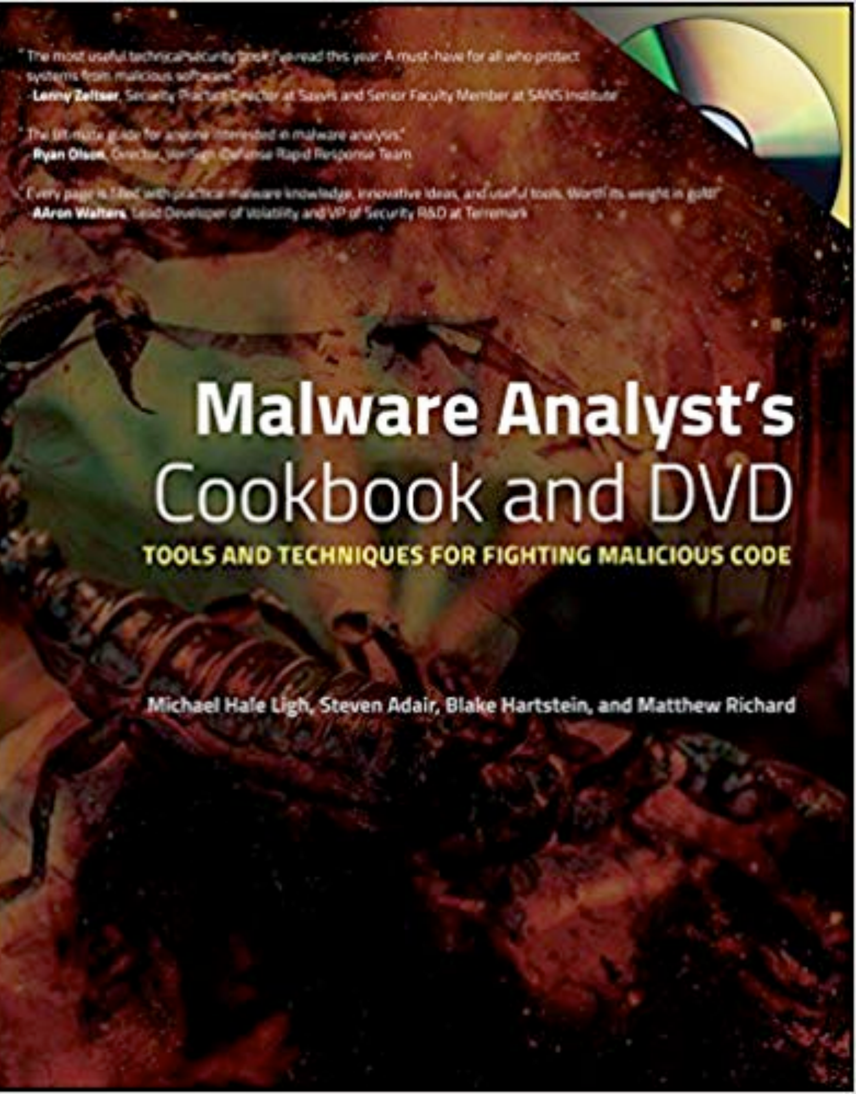
```
:ybox:Properties xsi:type="NetworkConnectionObj:NetworkConnectionObjectType">
<NetworkConnectionObj:Layer3_Protocol>IPv4</NetworkConnectionObj:Layer3_Protocol>
<NetworkConnectionObj:Layer4_Protocol>TCP</NetworkConnectionObj:Layer4_Protocol>
<NetworkConnectionObj:Layer7_Protocol>HTTP</NetworkConnectionObj:Layer7_Protocol>
<NetworkConnectionObj:Layer7_Connections>
-<NetworkConnectionObj:HTTP_Session xsi:type="HTTPSessionObj:HTTPSessionObjectType">
  -<HTTPSessionObj:HTTP_Request_Response>
    -<HTTPSessionObj:HTTP_Client_Request>
      -<HTTPSessionObj:HTTP_Request_Line>
          <HTTPSessionObj:HTTP_Method>GET</HTTPSessionObj:HTTP_Method>
          <HTTPSessionObj:Value>/wp-content/plugins/cached_data/k1.exe</HTTPSessionObj:Value
          <HTTPSessionObj:Version>HTTP/1.0</HTTPSessionObj:Version>
        </HTTPSessionObj:HTTP_Request_Line>
      -<HTTPSessionObj:HTTP_Request_Header>
        -<HTTPSessionObj:Parsed_Header>
            <HTTPSessionObj:Accept>*/*</HTTPSessionObj:Accept>
            <HTTPSessionObj:Accept_Language>en-US</HTTPSessionObj:Accept_Language>
            <HTTPSessionObj:Accept_Encoding>identity, *;q=0</HTTPSessionObj:Accept_Encodin
            <HTTPSessionObj:Connection>close</HTTPSessionObj:Connection>
          -<HTTPSessionObj:Host>
            -<HTTPSessionObj:Domain_Name xsi:type="URIObj:URIObjectType">
                <URIObj:Value>nerdmeetsgirl.com</URIObj:Value>
              </HTTPSessionObj:Domain_Name>
            -<HTTPSessionObj:Port xsi:type="PortObj:PortObjectType">
                <PortObj:Port_Value>80</PortObj:Port_Value>
```

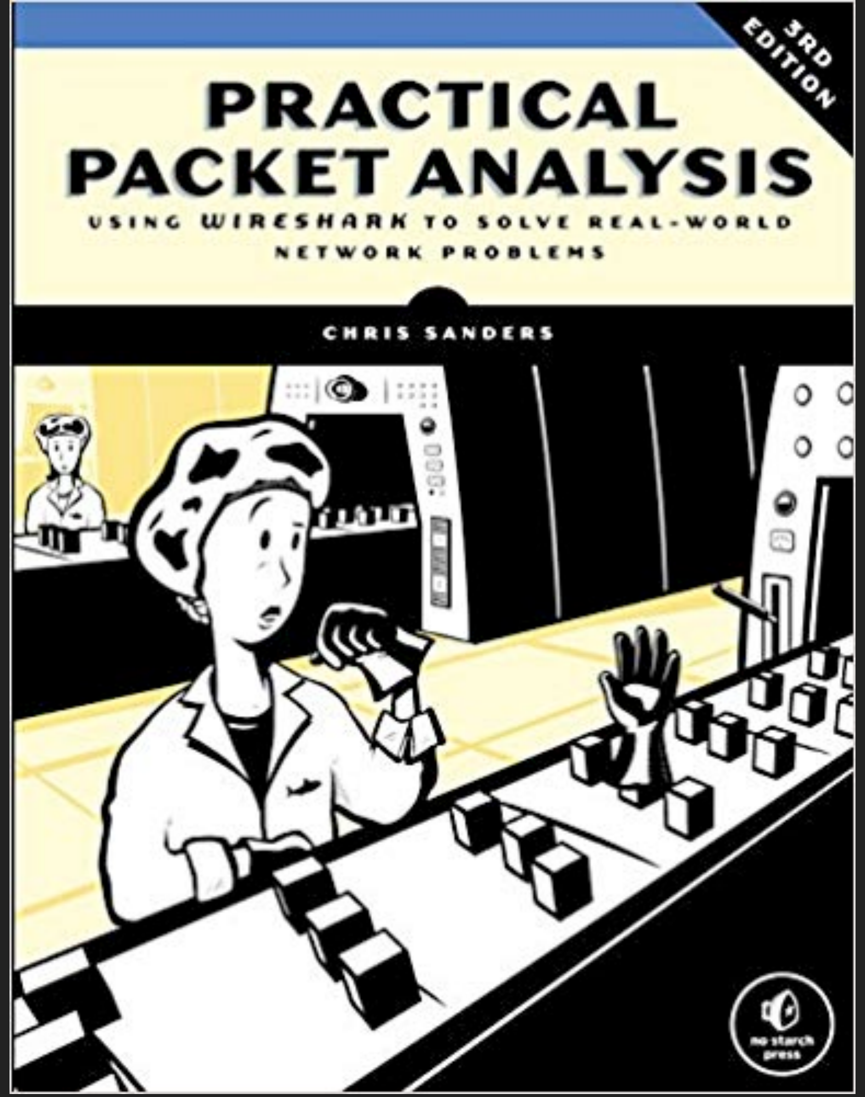
REPORT & INTEL

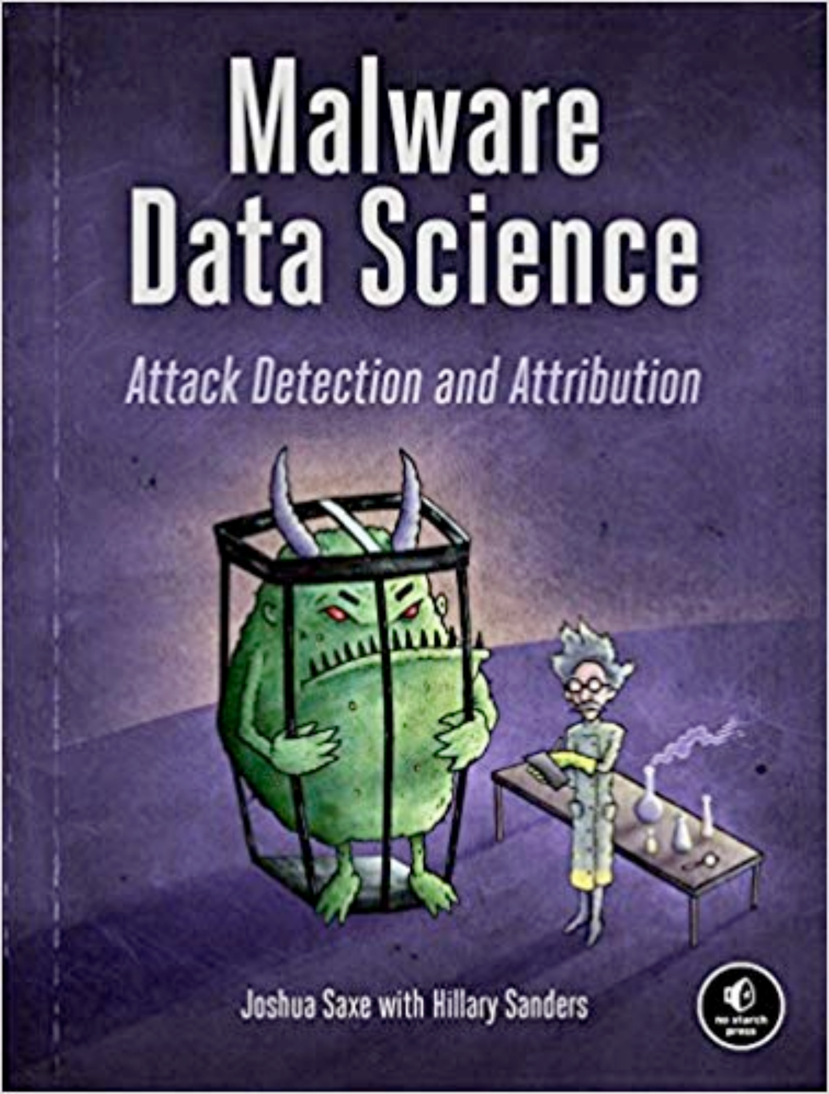


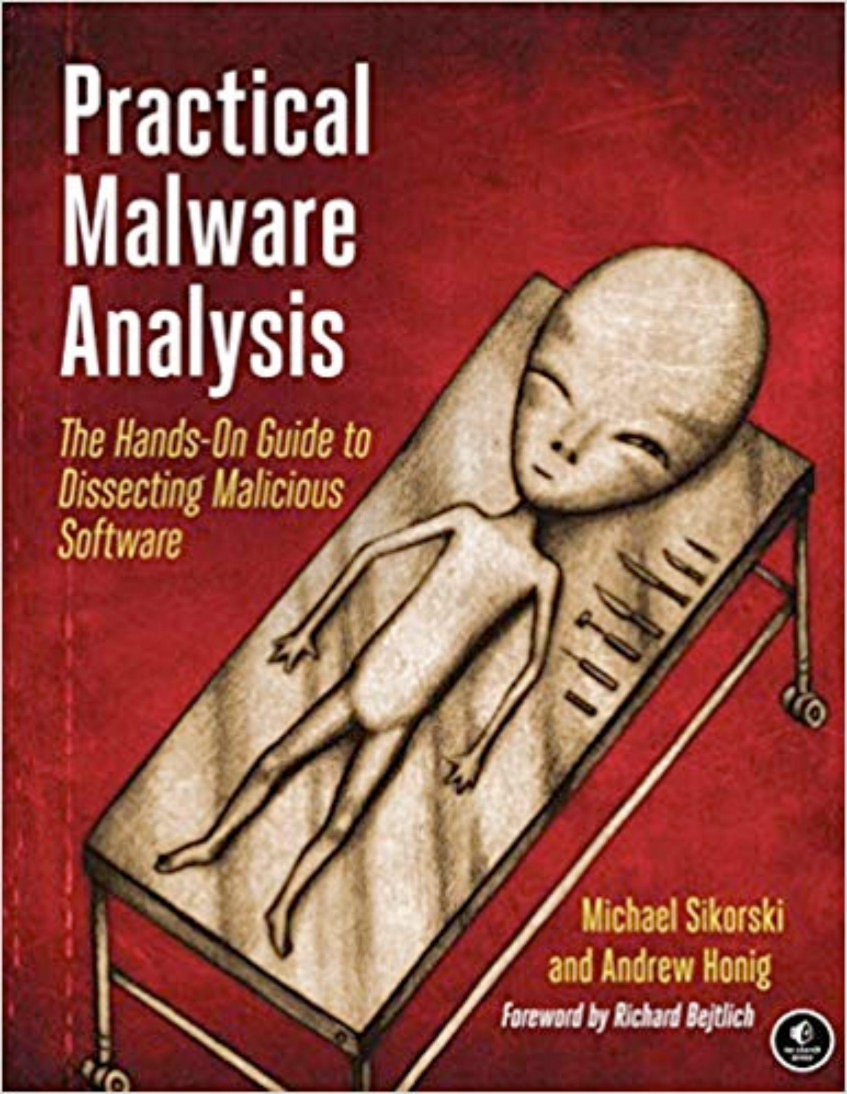
Malware Analysis Report

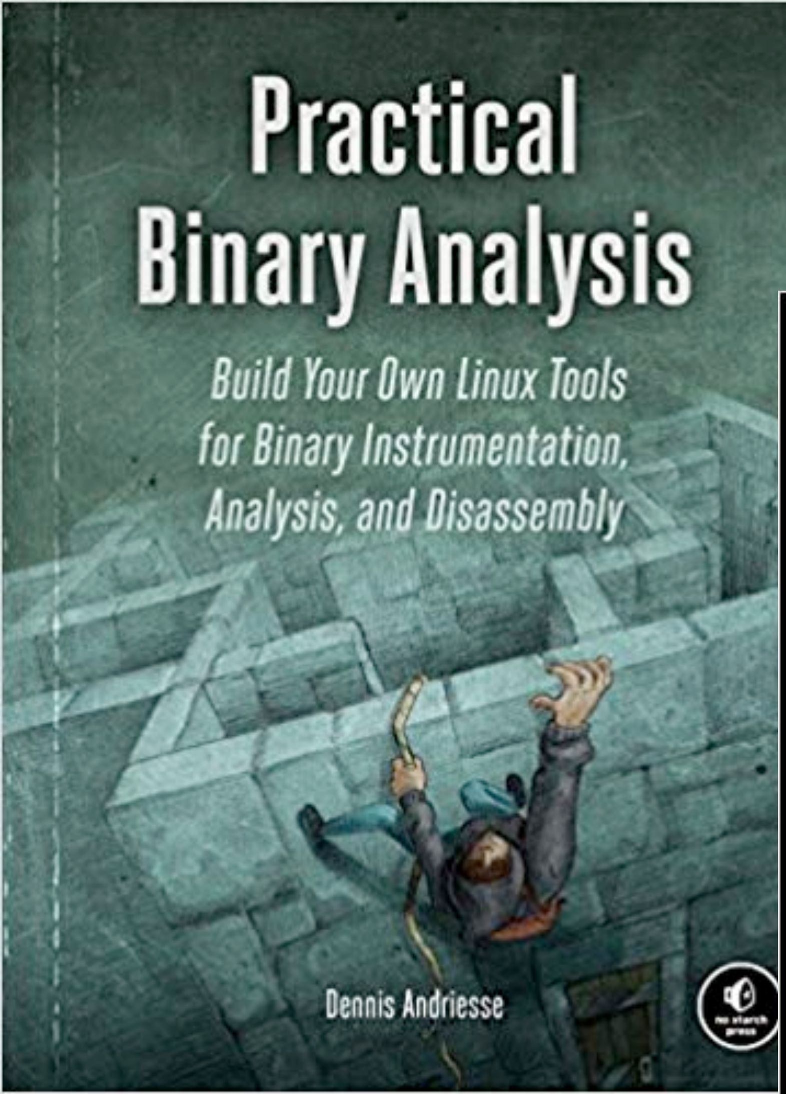
- Sample's Characteristics
  - Infection capabilities
  - Self-preservation capacity
  - Spreading mechanics
  - Data leakage abilities
  - Remote attacker interactions
- Observations
  - Behavioral analysis
  - Static code analysis
  - Dynamic code analysis
  - Memory analysis
- Supporting Figures
  - Logs
  - Strings
  - Function listings
  - Screenshots
- Threat Intelligence
  - IOC
  - Actors
  - Attribution
  - TTP
  - References
- Summary of the analysis
  - Key observations
  - Recommendations
  - Limitations
  - Report date and authors
  - Mitigations
  - Eradication and recovery
- Sample's Identification
  - File name, type, size
  - File hashes
  - Anti-virus identifiers
- Dependencies
  - Supported OS
  - Required libraries
  - Configuration files
  - Scripts and executables
  - URLs

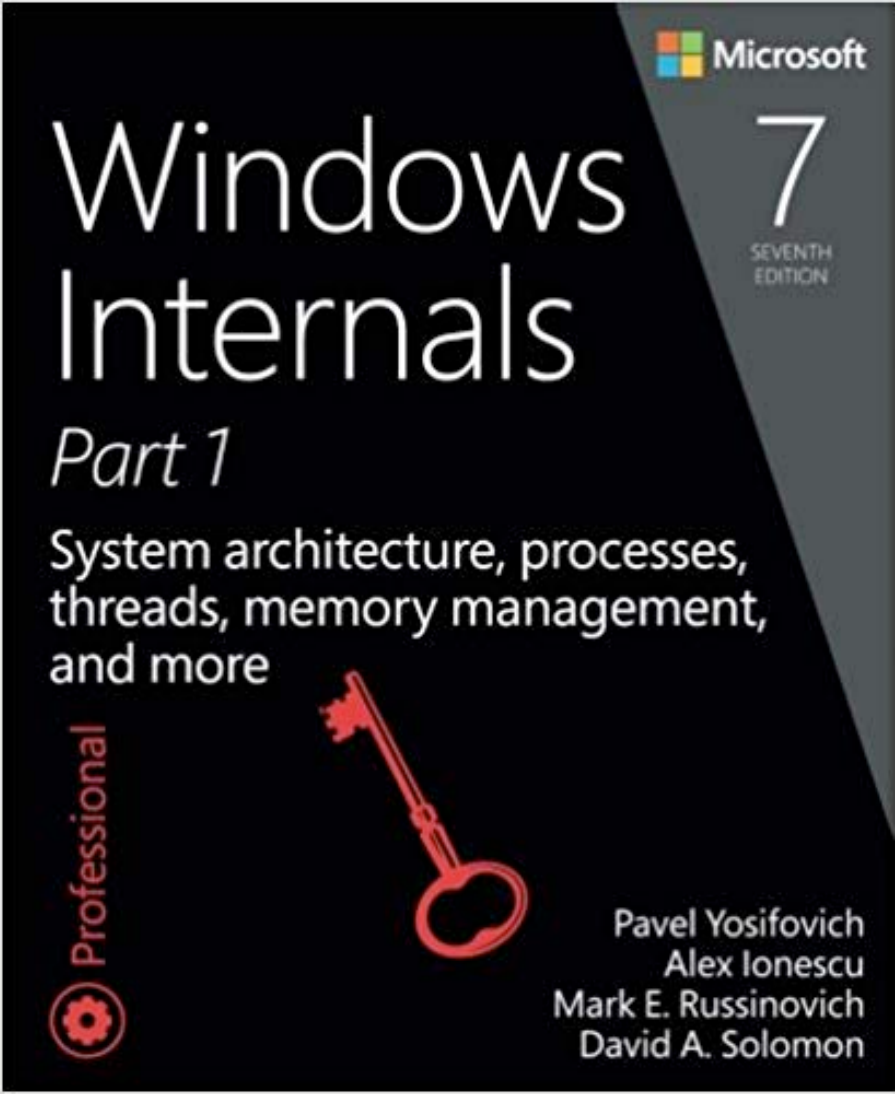

"The most useful technical security book I've read this year. A must-have for all who protect systems from malicious software."
-Lenny Zeltser, Security Practice Director at Savvis and Senior Faculty Member at SANS Institute
"The ultimate guide for anyone interested in malware analysis."
Ryan Olson, Director, VeriSign iDefense Rapid Response Team
"Every page is filled with practical malware knowledge, innovative ideas, and useful tools. Worth its weight in gold!"
AAron Walters, Lead Developer of Volatility and VP of Security R&D at Terremark
Malware Analyst's
Cookbook and DVD
TOOLS AND TECHNIQUES FOR FIGHTING MALICIOUS CODE
Michael Hale Ligh, Steven Adair, Blake Hartstein, and Matthew Richard


3RD EDITION
PRACTICAL
PACKET ANALYSIS
USING WIRESHARK TO SOLVE REAL-WORLD NETWORK PROBLEMS
CHRIS SANDERS

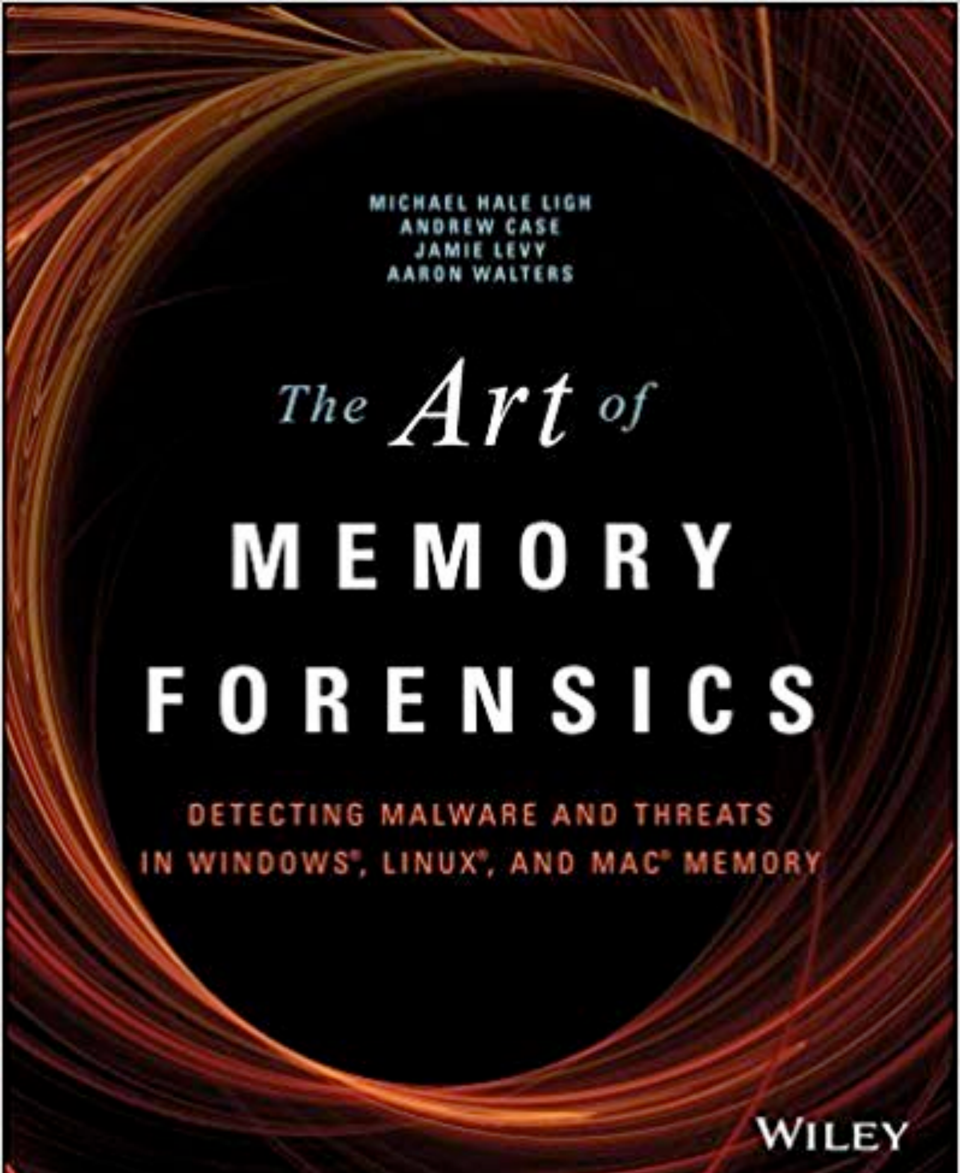

Malware
Data Science
Attack Detection and Attribution
Joshua Saxe with Hillary Sanders

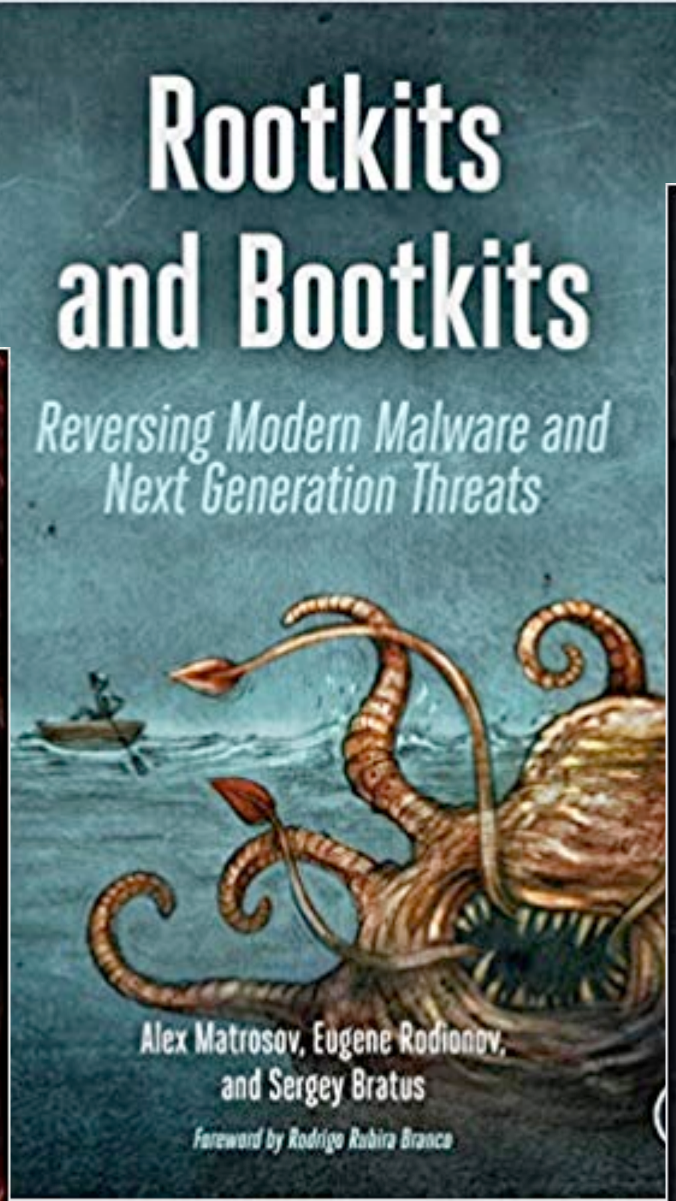

Practical
Malware
Analysis
The Hands-On Guide to
Dissecting Malicious
Software
Michael Sikorski
and Andrew Honig
Foreword by Richard Bejtlich

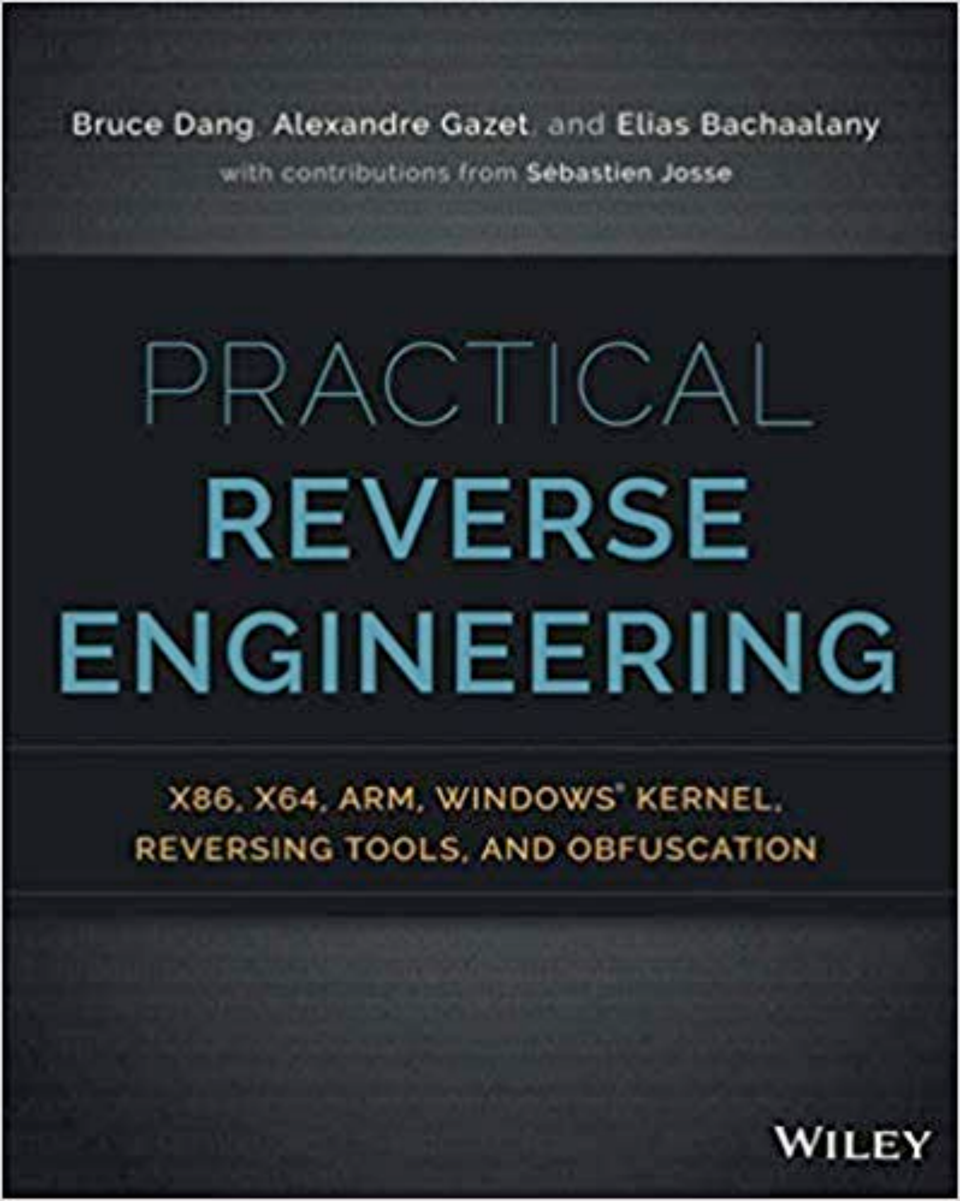

Practical
Binary Analysis
Build Your Own Linux Tools
for Binary Instrumentation,
Analysis, and Disassembly
Dennis Andriesse

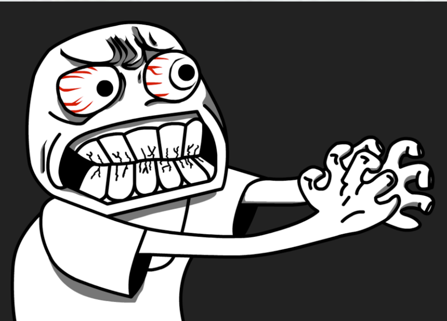

Microsoft
Windows
Internals
7
SEVENTH EDITION
Part 1
System architecture, processes,
threads, memory management,
and more
Professional
Pavel Yosifovich
Alex Ionescu
Mark E. Russinovich
David A. Solomon

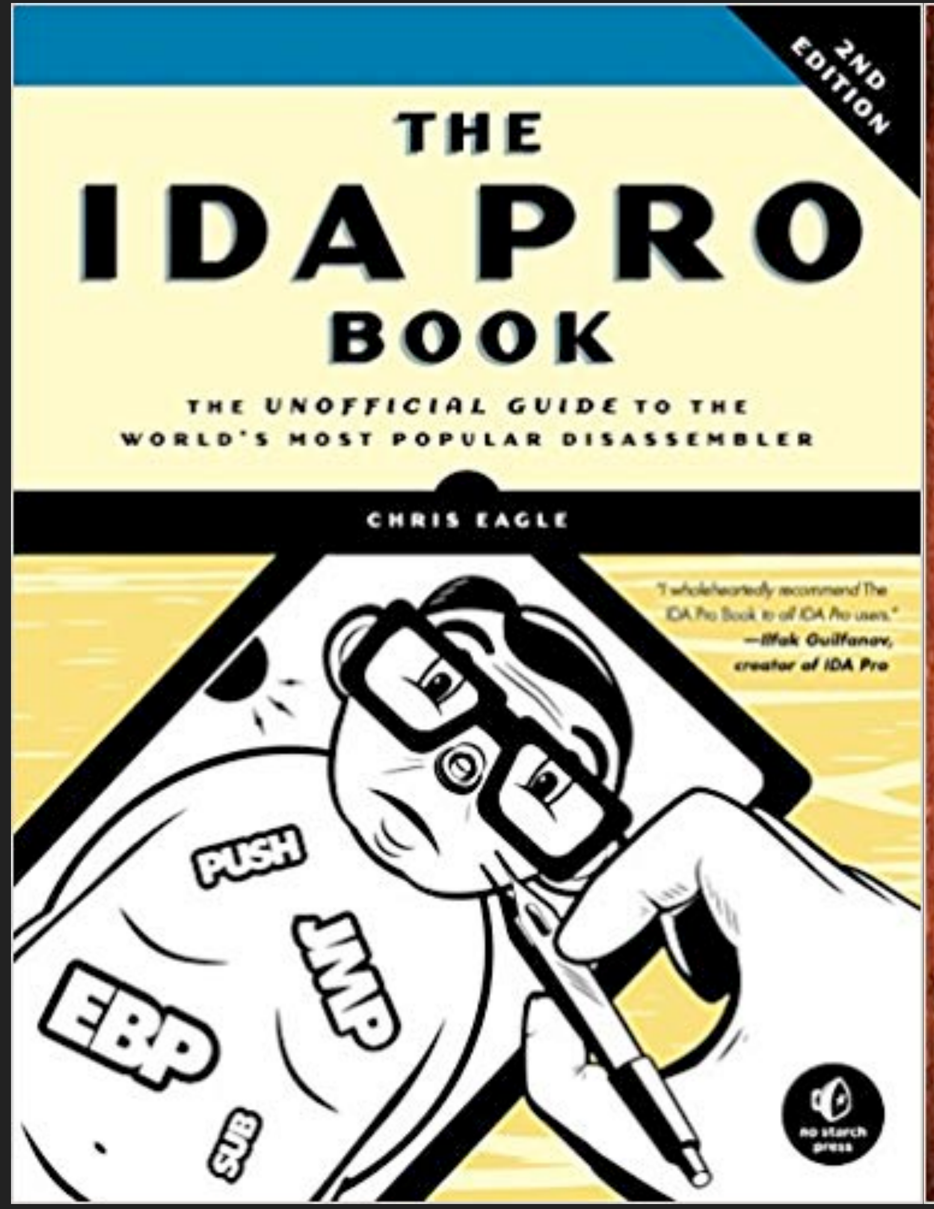
REAL DIGITAL
FORENSICS
Computer Security
and Incident Response
Hands-on practice with real forensics data
KEITH J. J
RICHARD BEJT
CURTIS W.

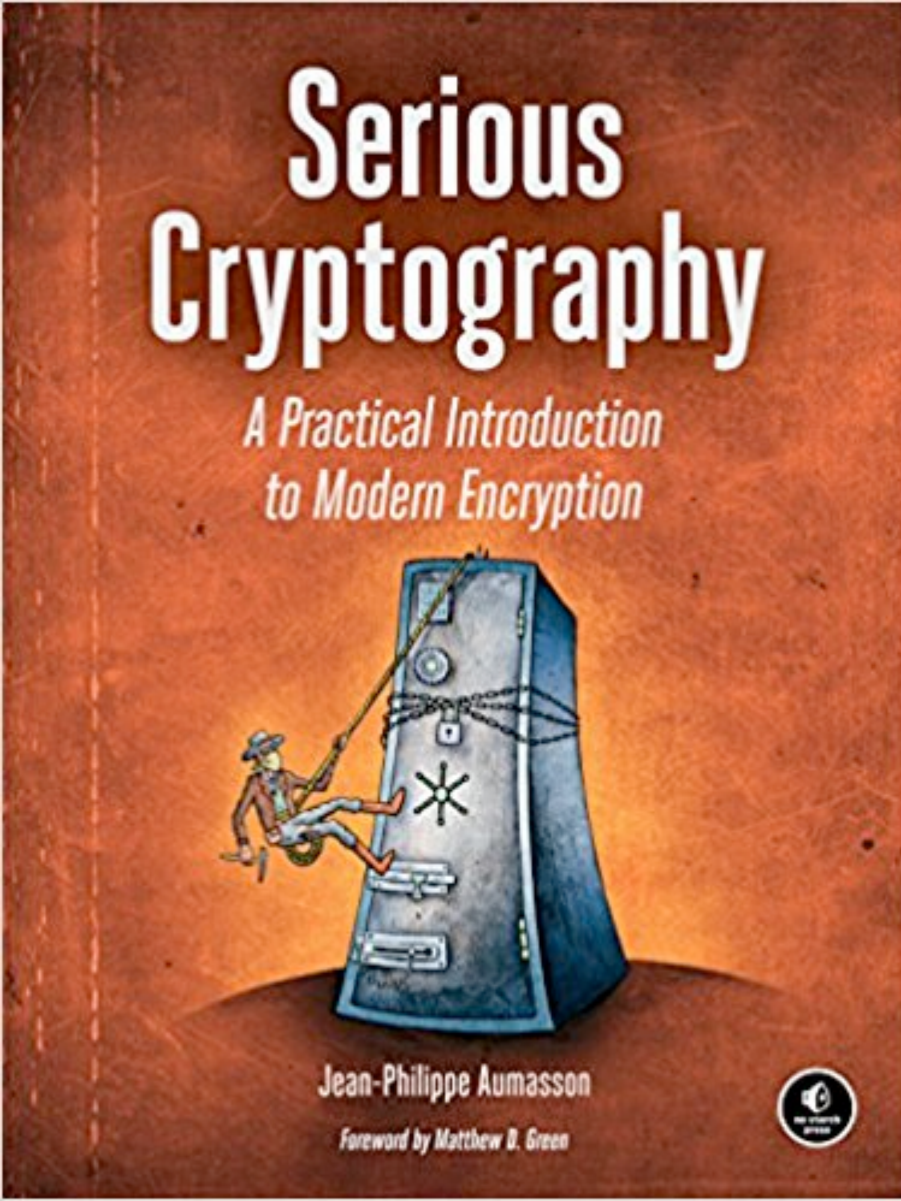

MICHAEL HALE LIGH
ANDREW CASE
JAMIE LEVY
AARON WALTERS
The Art of
MEMORY
FORENSICS
DETECTING MALWARE AND THREATS
IN WINDOWS®, LINUX®, AND MAC® MEMORY
WILEY


Rootkits
and Bootkits
Reversing Modern Malware and
Next Generation Threats
Alex Matrosov, Eugene Rodionov,
and Sergey Bratus
Foreword by Rodrigo Rubira Branco


Bruce Dang, Alexandre Gazet, and Elias Bachaalany
with contributions from Sébastien Josse
PRACTICAL
REVERSE
ENGINEERING
X86, X64, ARM, WINDOWS® KERNEL,
REVERSING TOOLS, AND OBFUSCATION
WILEY




2ND EDITION
THE
IDA PRO
BOOK
THE UNOFFICIAL GUIDE TO THE WORLD'S MOST POPULAR DISASSEMBLER
CHRIS EAGLE
"I wholeheartedly recommend The IDA Pro Book to all IDA Pro users."
—Ilfak Guilfanov, creator of IDA Pro
PUSH
JMP
EBP
SUB


Serious
Cryptography
A Practical Introduction
to Modern Encryption
Jean-Philippe Aumasson
Foreword by Matthew D. Green

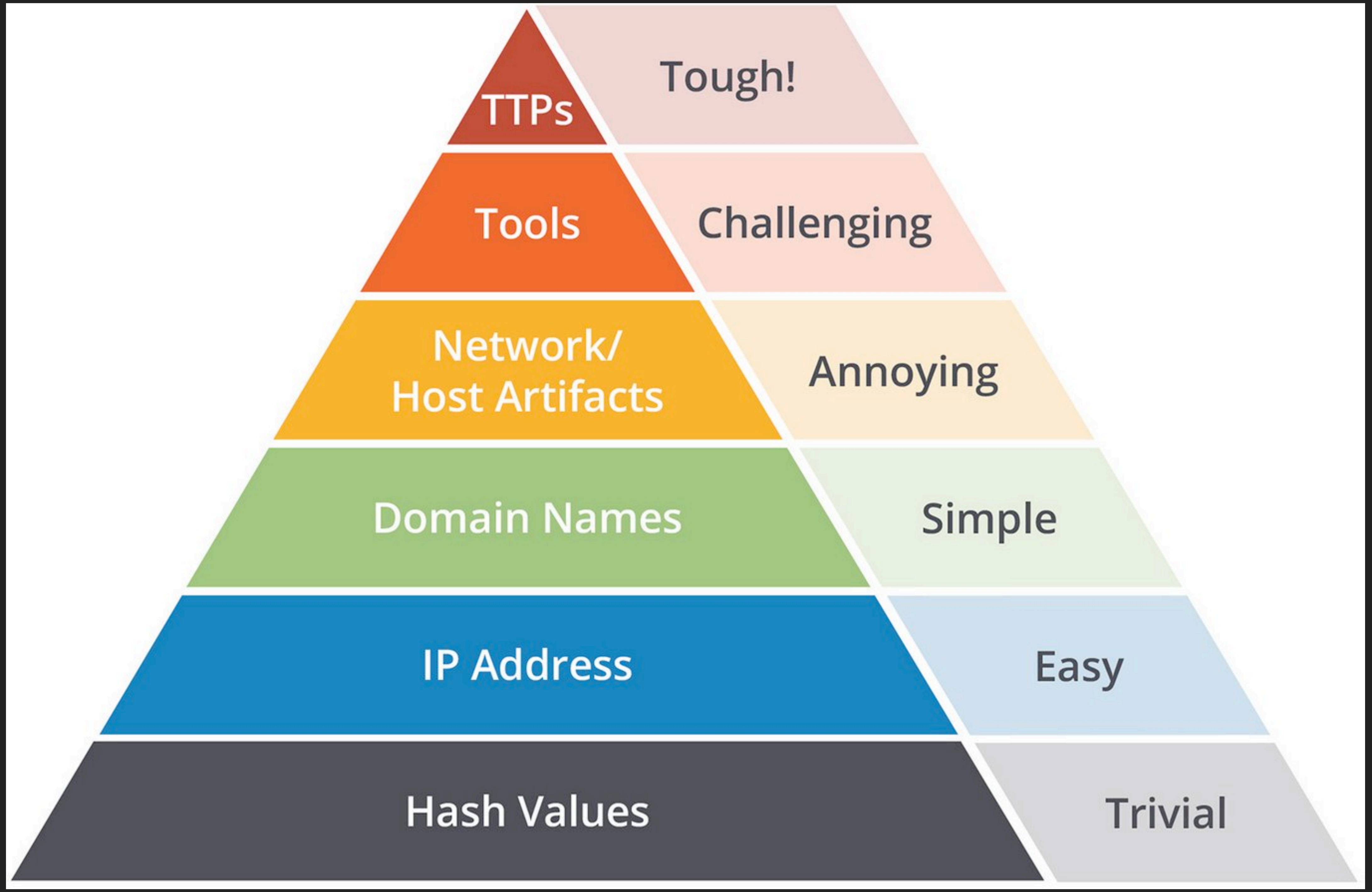
TRACKING ADVERSARIES

THREAT HUNTING

THREAT INTEL GOALS

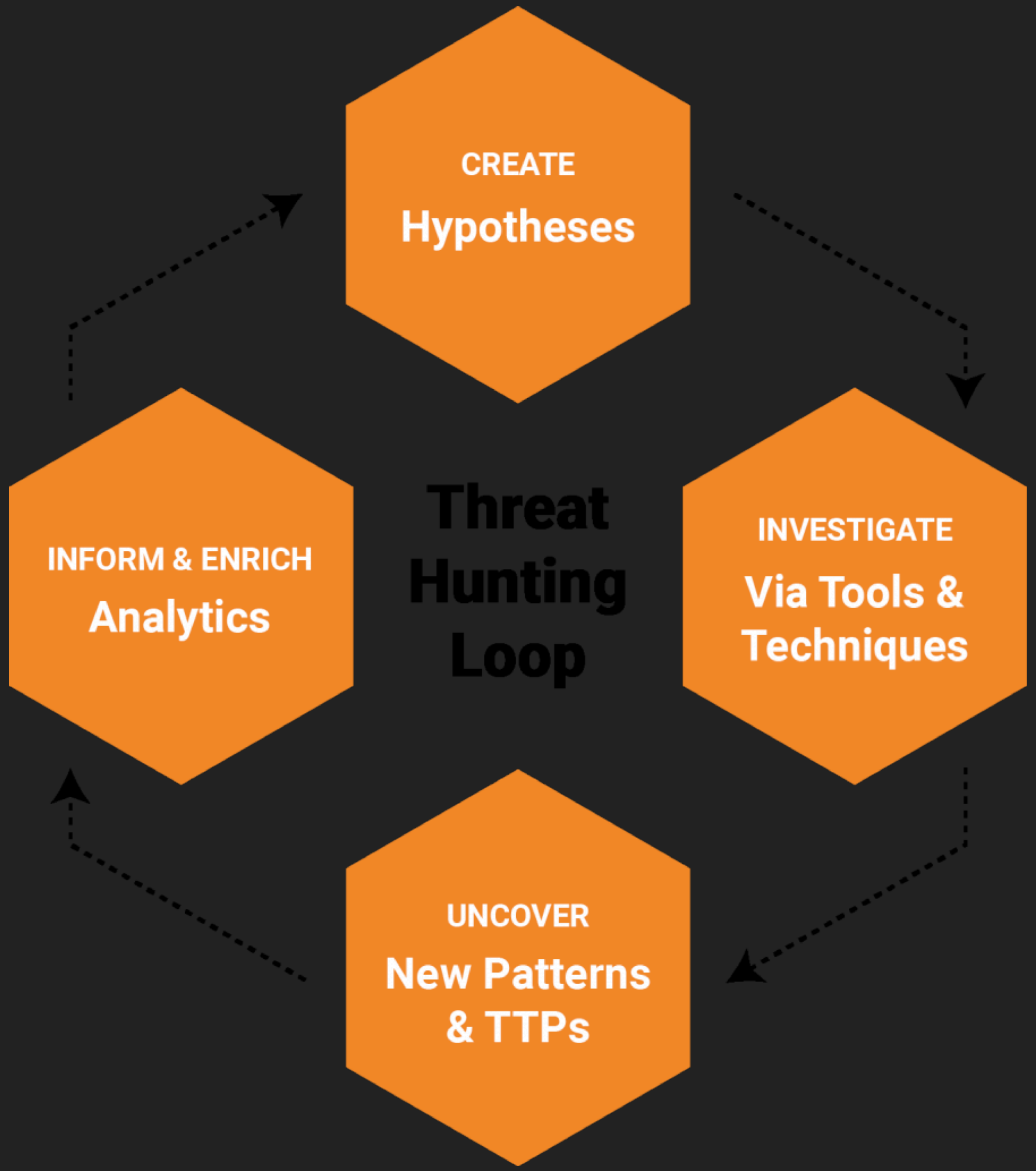
- **Who** is behind the action.
- What are their **goals**.
- Where is the **infrastructure**.
- When do they **operate**.
- **Why** are they conducting the operation.
- How do we **thwart** their activities.

Expand your search and iterate, until no more information are available.



HUNTING

- Threat research.
  - Search for **other samples**.
  - Different **TTP**.
  - Another **infrastructure**.
- Understand attackers TTP over time.
- Get the big picture of a **campaign** or **actor**.
- Attribution?

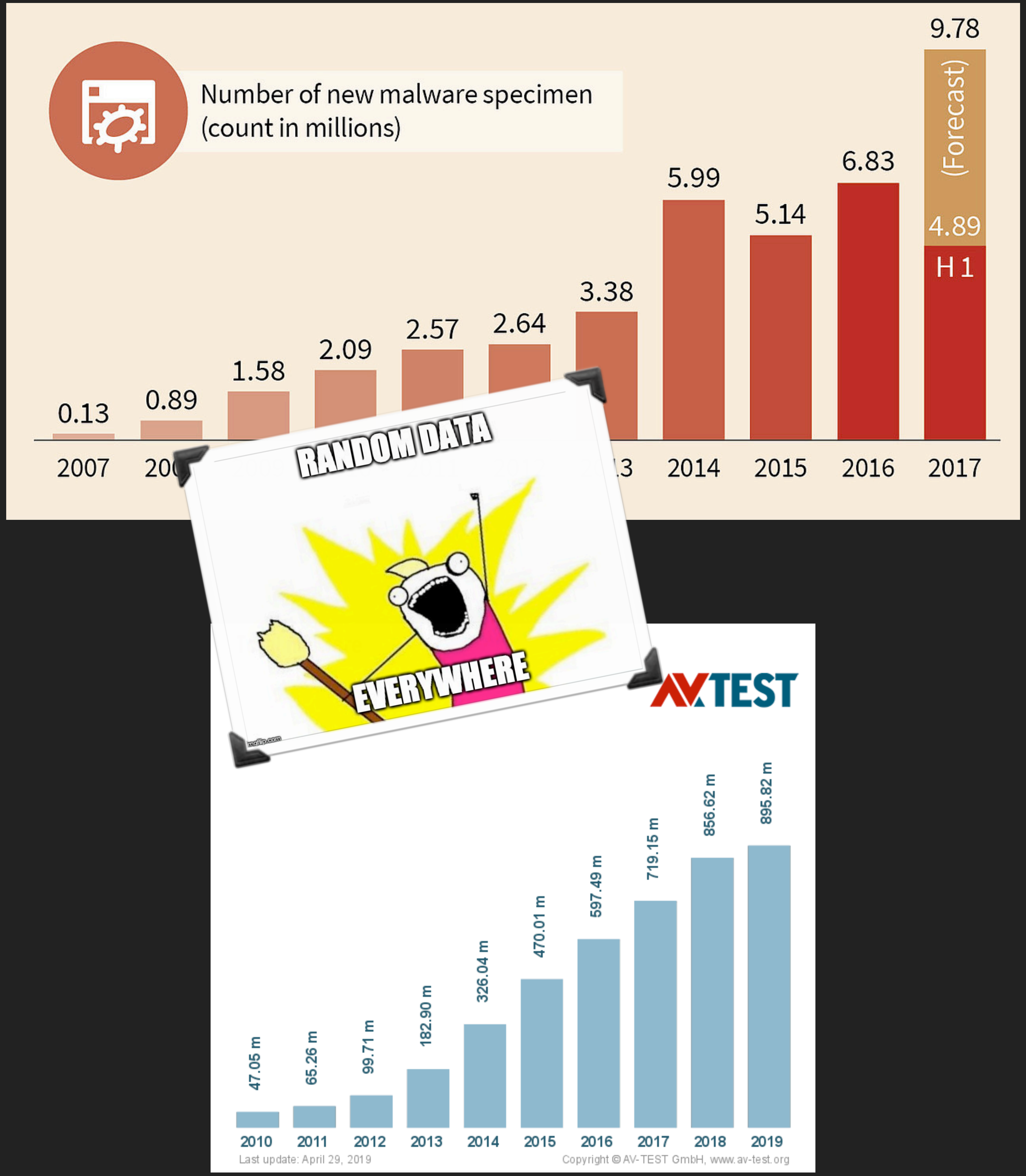


CYBER SCENARIO

ARMS RACE

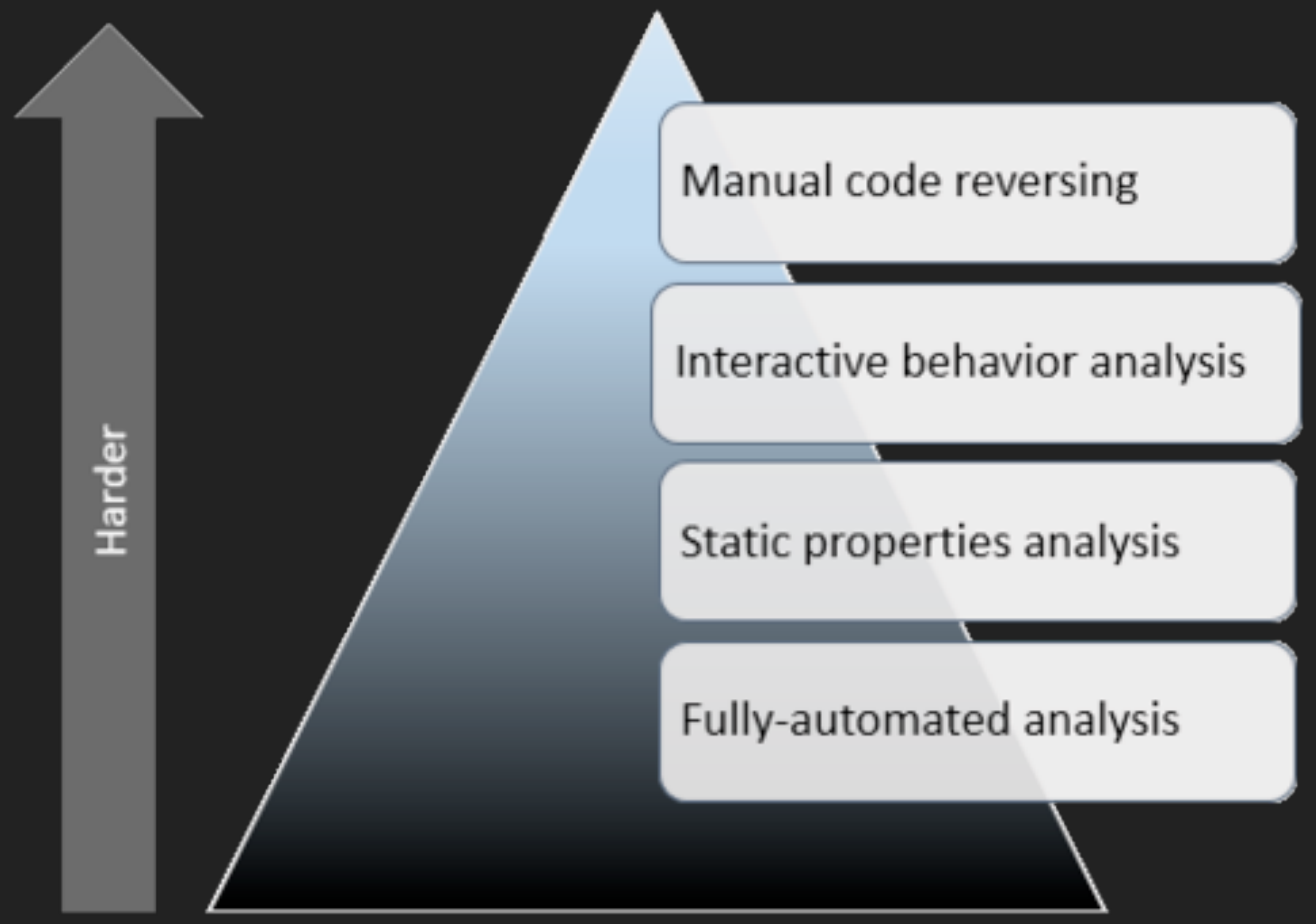
BACK TO REALITY

- The adversaries **produce** more and more malware.
- More than we can possible analyze.
- We have to operate in the **open** while they operate in secret.
- Actors are criminal organisations or nation state.



HUMANS DON'T SCALE

- How long does it take to **reverse engineer** a sample?
- How long does it take to create a **signature**?
- How long does it take to create efficient **IOCs**?
- Some analysis tasks can be automated.
- You still need humans at some point (i.e. hunting, TTP, connecting dots)



ACTUAL STATE OF MALWARE ANALYSIS

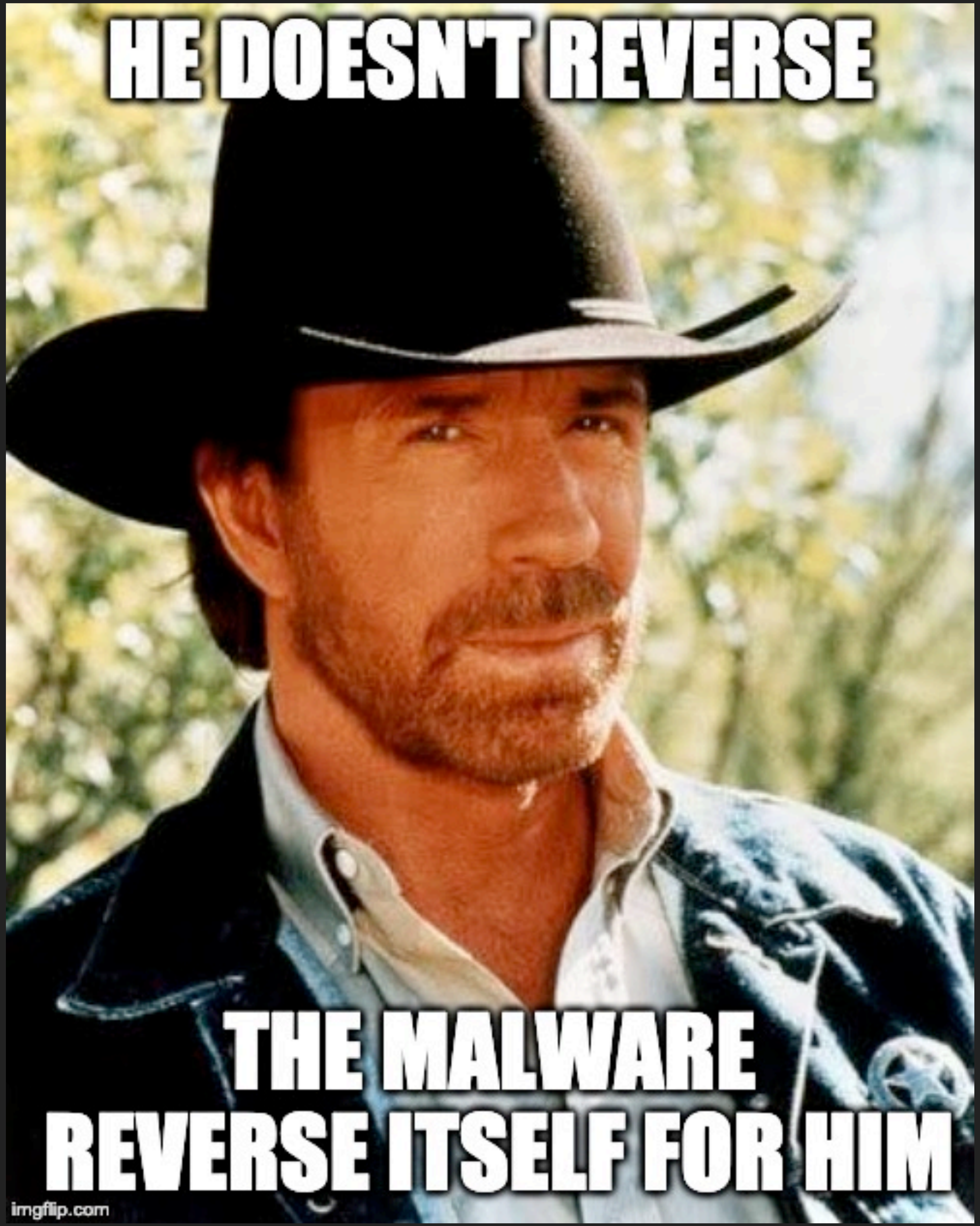
EVERYTHING IS FINE

WHAT IF…

- You daily receive over 100k samples.
- You are asked to spot the relevant one.
- You shall automate almost all tasks.

… SO …

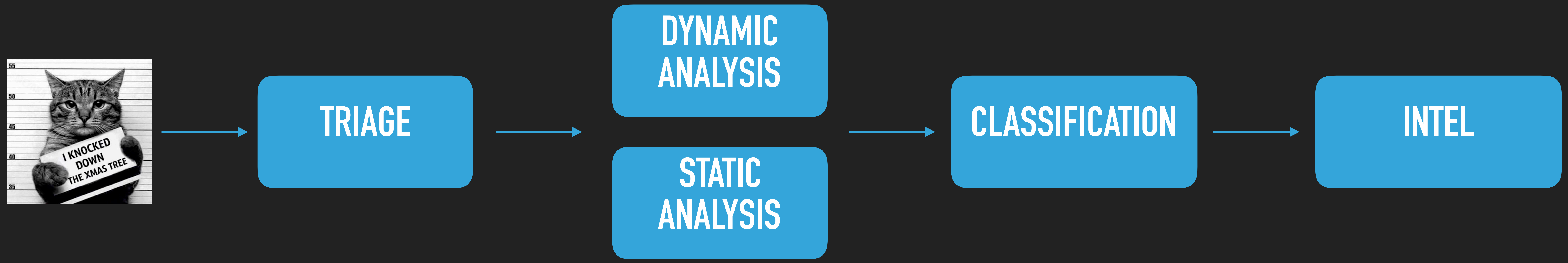
- How to store and index TB of data?
- How to run the analysis?
- How much horse power?



DESIGNING IS THE KEY

THINKING

ANALYSIS STEPS



TRIAGE

DYNAMIC ANALYSIS

STATIC ANALYSIS

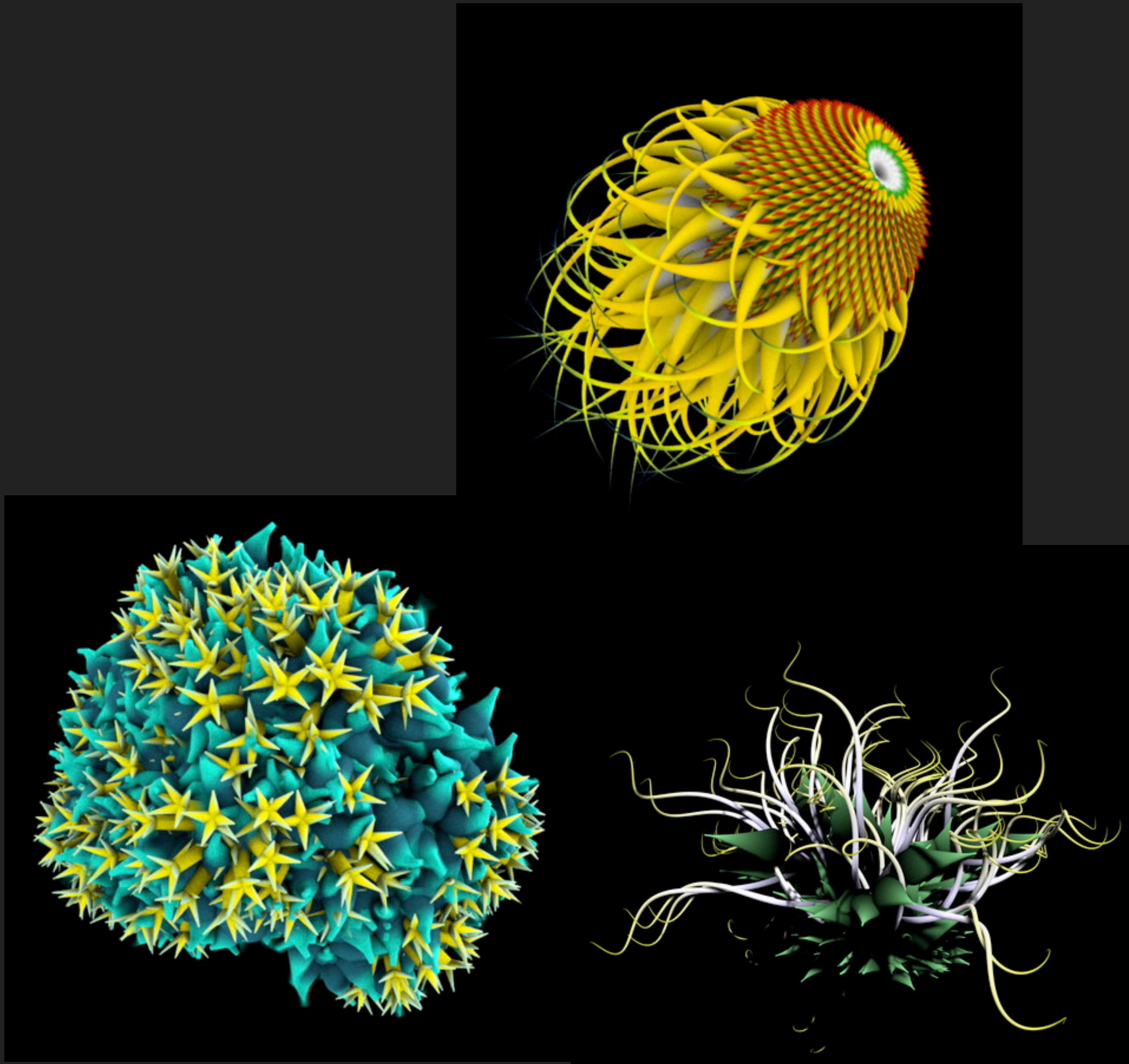
CLASSIFICATION

INTEL

- A good design is the **key** for your infrastructure success.
- You should start writing down your **workflow**.

MODERN TECH

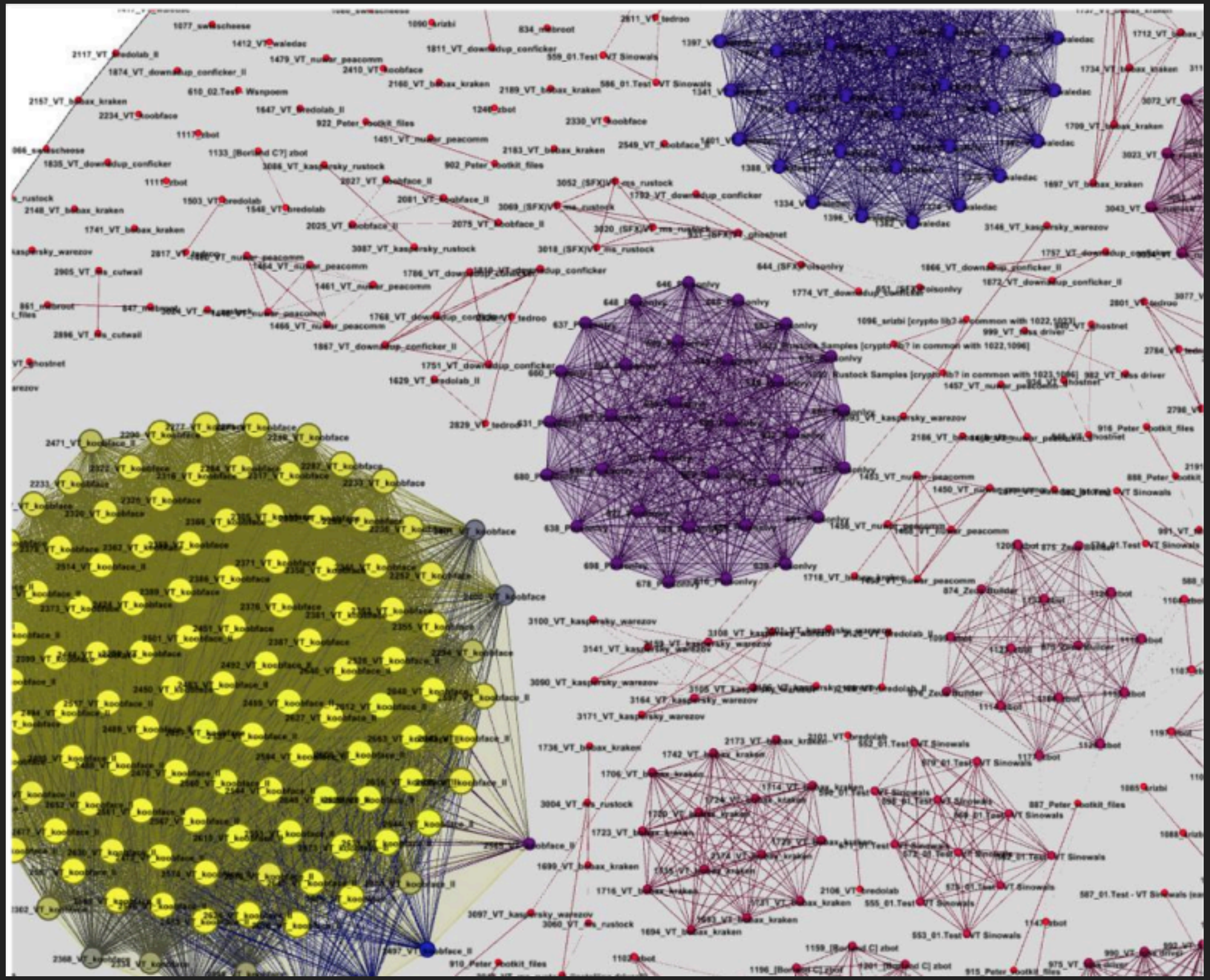
- We are in the age of Big Data.
- Machine Learning to make better informed analytic decisions.
- Modern graphical representation.



http://sq.ro/malwarez.htm

SIMILAR SAMPLES

- Malware clustered into **families**.
- Triage samples of the same malware.
- **Similarity** detection
  - Common code could be implemented with a different syntax



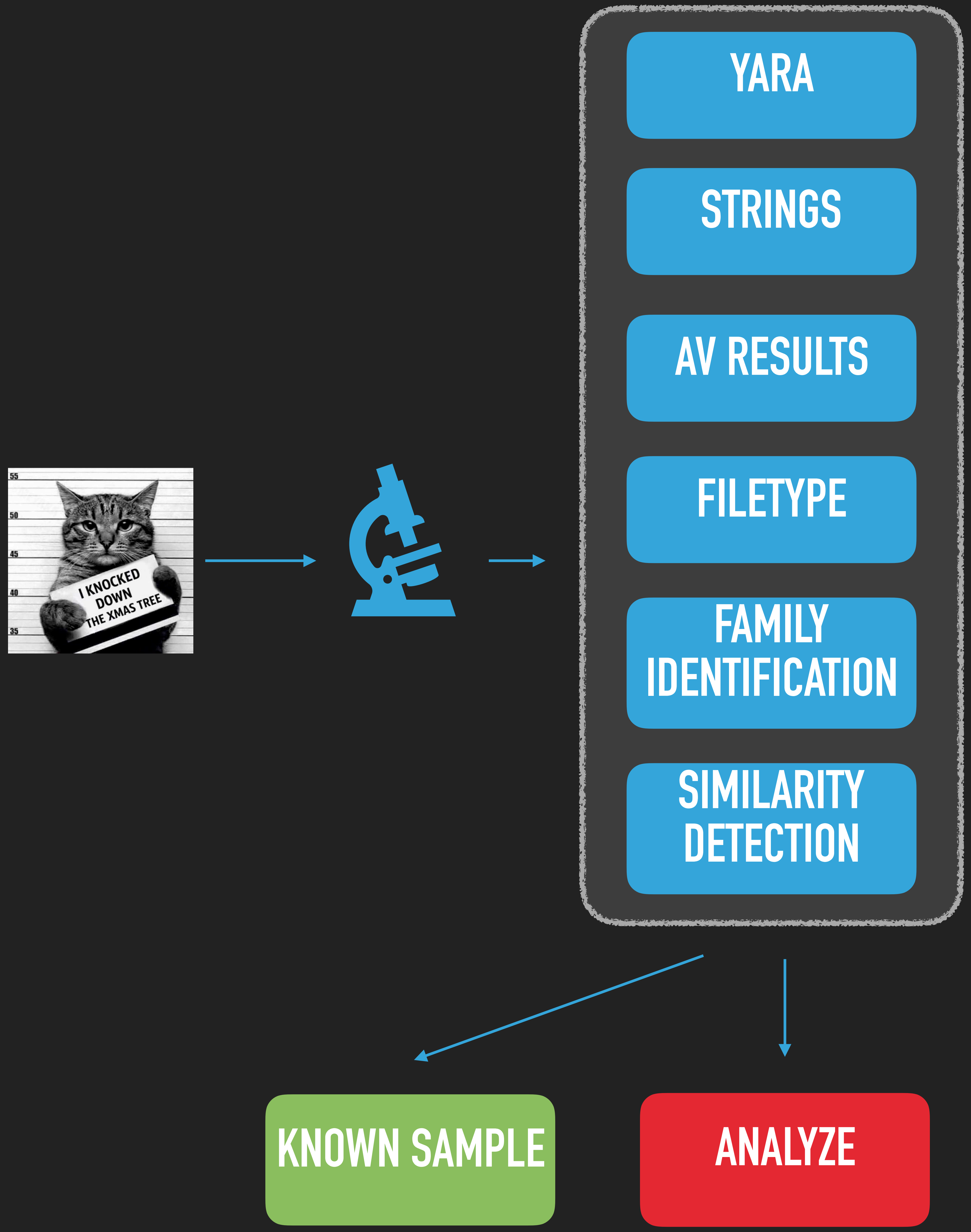
DESIGNING IS THE KEY

COMPONENTS

A GOOD TRIAGE CAN SAVE YOU TIME

SAMPLE TRIAGE

- Prioritise (or skip) analysis.
- Runs some quick tasks to determine:
  - If the sample has been analyzed.
  - If the sample is from a known family.
  - If the sample has some similarities.
- Comes before time consuming tasks.



YARA

STRINGS

AV RESULTS

FILETYPE

FAMILY IDENTIFICATION

SIMILARITY DETECTION

KNOWN SAMPLE

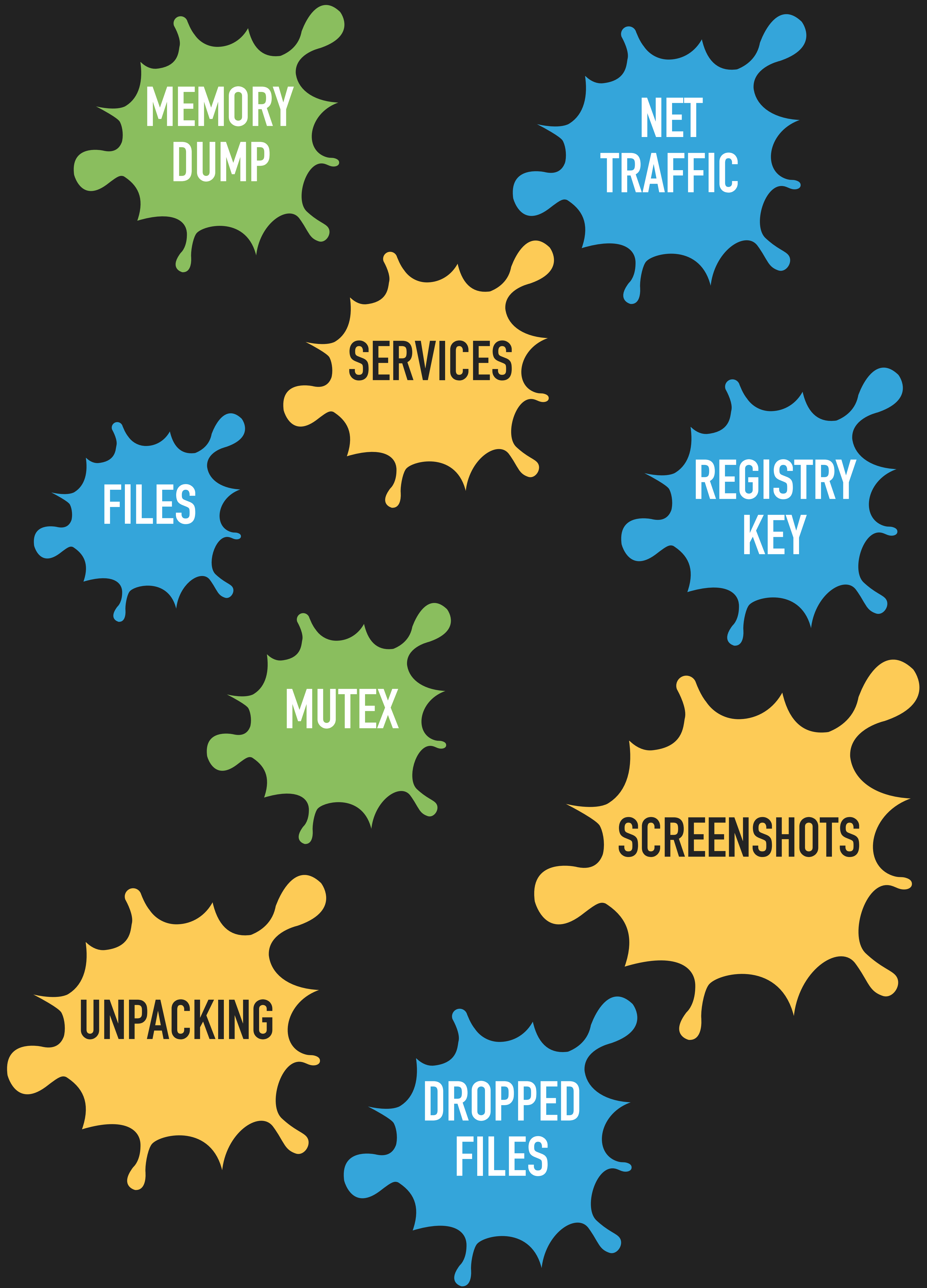
ANALYZE

STORAGE

- **Flat files** on distributed file system.
- RDBMS, only for temporary / local data.
- **NoSQL** datastore
  - MongoDB, Cassandra, Hadoop
- **Indexes**
  - Lucene, Elasticsearch
- **Cache**
  - Redis, memcached

MALWARE PROCESSING

- Malware execution in **safe** environment.
- Think about your **network** usage.
- Multiple execution, results comparison.
- Collect and store only information you need.
- Using an hypervisor with low overhead could save kittens.



MEMORY DUMP

NET TRAFFIC

SERVICES

FILES

REGISTRY KEY

MUTEX

SCREENSHOTS

UNPACKING

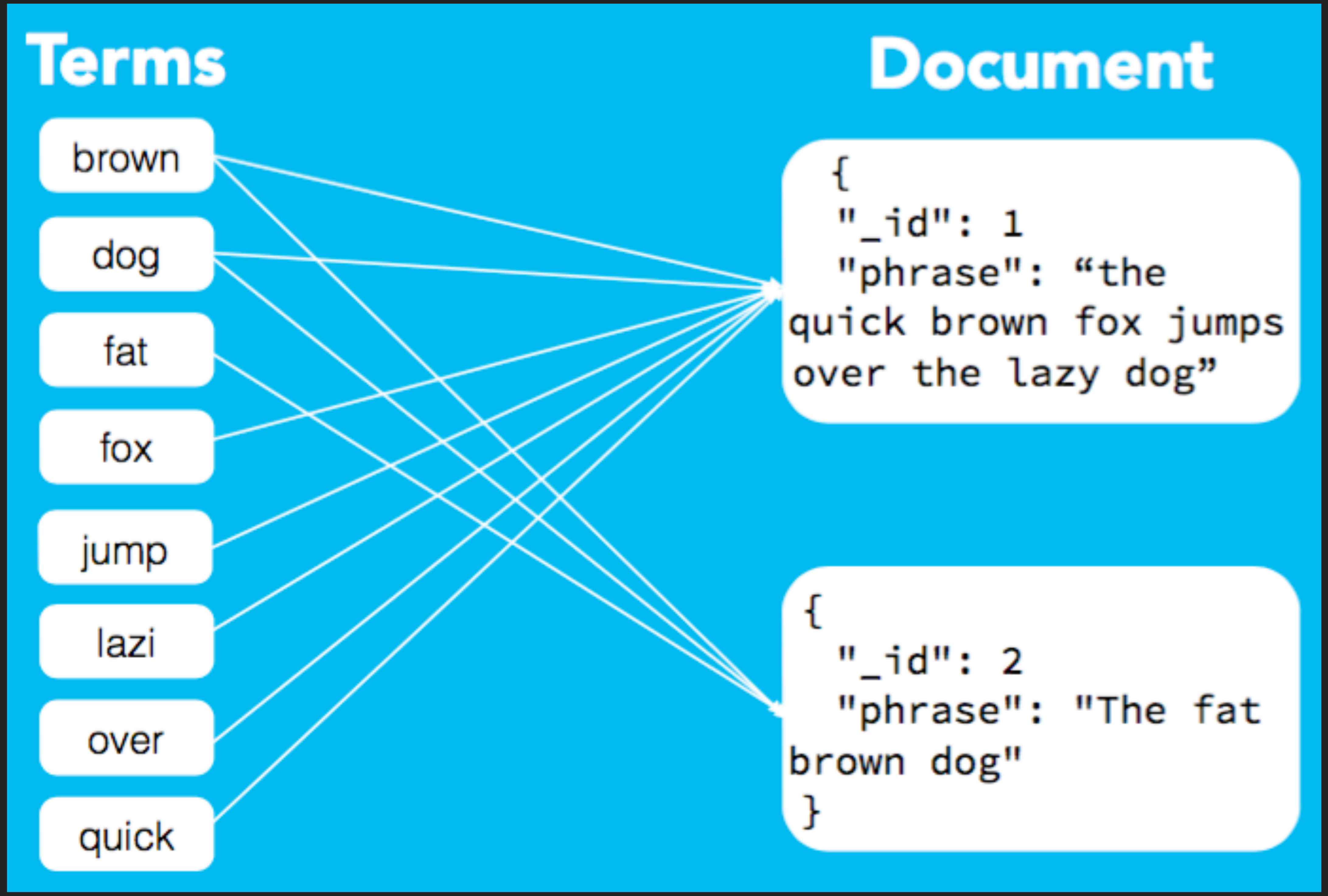
DROPPED FILES

ANALYTICS ENGINE

- A middleware you have to develop
- Workers management
- Map reduce tasks
- Machine learning engine
- Distributed tools
  - Apache Spark
  - Apache Pig

SEARCH SYSTEM

- Traditional RDBMS may not be sufficient.
- Handle **variety** of data structures.
- Hadoop or other NoSQL may be better.
- Index just what you really **need** to search.
- **Limit** result query set.



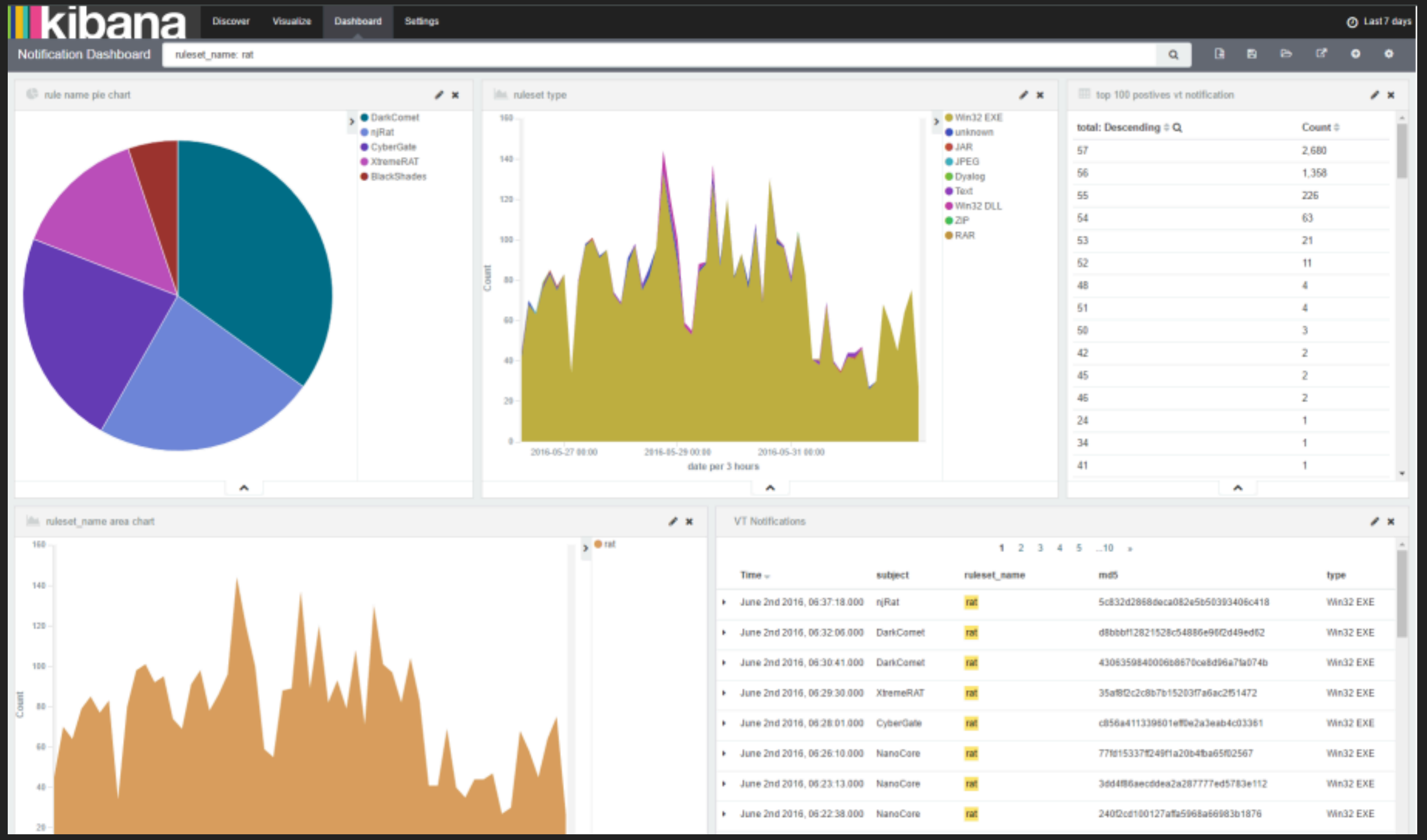
```
{
 "_id": 1
 "phrase": “the
quick brown fox jumps
over the lazy dog”
```

```
{
 "_id": 2
 "phrase": "The fat
brown dog"
}
```

CONSIDER USE CASE IN DESIGN

USER ACCESS

- API
- Batch processing
- Application
  - Custom web interface
  - Kibana
  - Infrastructure monitoring (zabbix & co.)



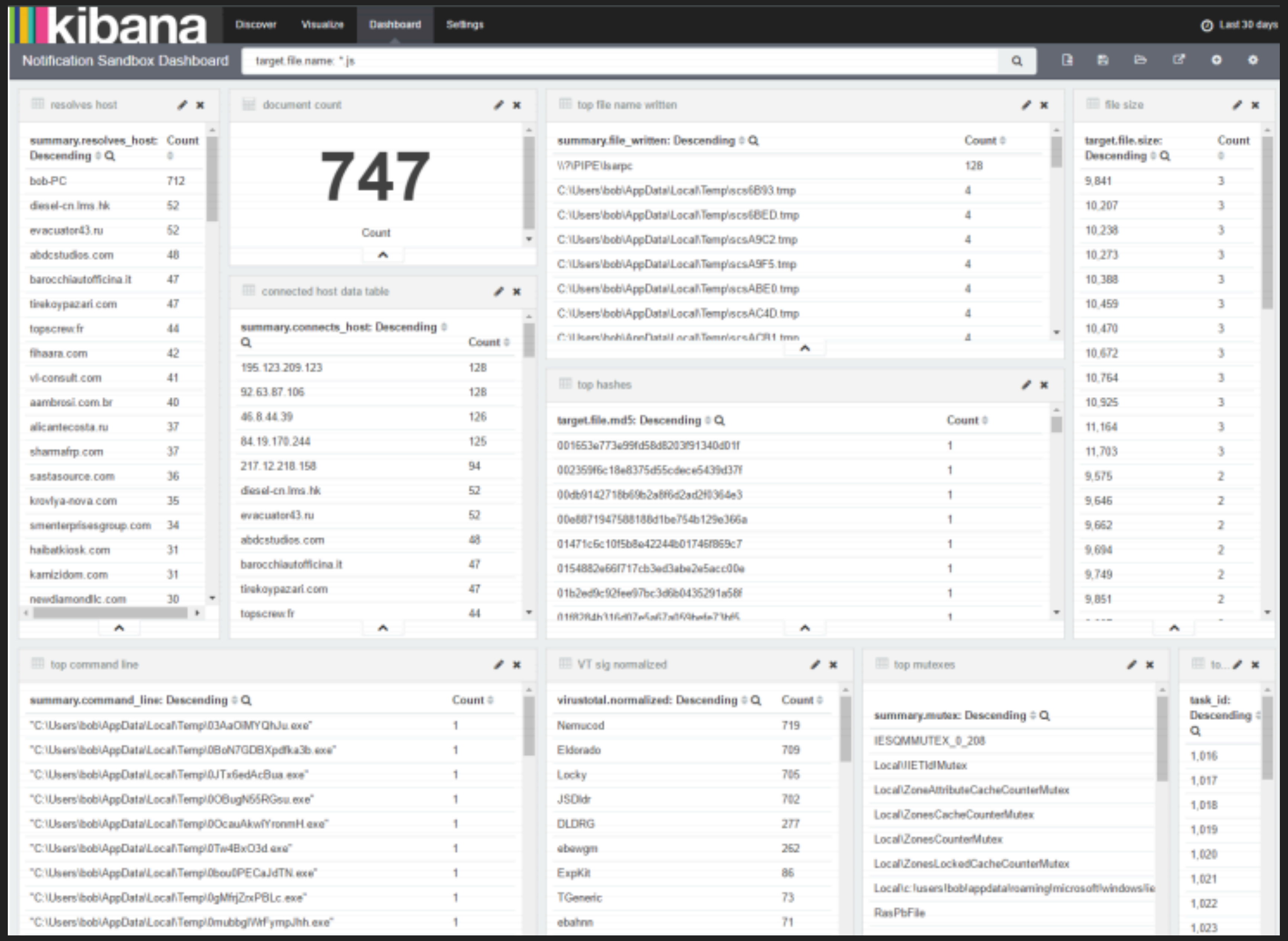
top 100 postives vt notification

total: Descending	Count
57	2,680
56	1,358
55	226
54	63
53	21
52	11
48	4
51	4
50	3
42	2
45	2
46	2
24	1
34	1
41	1

VT Notifications

1 2 3 4 5 ...10 »

Time	subject	ruleset_name	md5	type
June 2nd 2016, 06:37:18.000	njRat	rat	5c832d2868deca082e5b50393406c418	Win32 EXE
June 2nd 2016, 06:32:06.000	DarkComet	rat	d8bbbf12821528c54886e98f2d49ed62	Win32 EXE
June 2nd 2016, 06:30:41.000	DarkComet	rat	4306359840006b8670ce8d96a71a074b	Win32 EXE
June 2nd 2016, 06:29:30.000	XtremeRAT	rat	35af8f2c2c8b7b15203f7a6ac2f51472	Win32 EXE
June 2nd 2016, 06:28:01.000	CyberGate	rat	c856a411339601eff0e2a3eab4c03361	Win32 EXE
June 2nd 2016, 06:26:10.000	NanoCore	rat	77fd15337ff249f1a20b4fba65f02567	Win32 EXE
June 2nd 2016, 06:23:13.000	NanoCore	rat	3dd4f86aecddea2a287777ed5783e112	Win32 EXE
June 2nd 2016, 06:22:38.000	NanoCore	rat	240f2cd100127affa5968a66983b1876	Win32 EXE



resolves host

summary.resolves_host: Descending	Count
bob-PC	712
diesel-cn.lms.hk	52
evacuator43.ru	52
abdcstudios.com	48
barocchiautofficina.it	47
tirekoypazari.com	47
topscrew.fr	44
fihaara.com	42
vl-consult.com	41
aambrosi.com.br	40
alicantecosta.ru	37
sharmafrp.com	37
sastasource.com	36
krovlya-nova.com	35
smenterprisesgroup.com	34
haibatkiosk.com	31
kamizidom.com	31
newdiamondllc.com	30

document count

747

Count

connected host data table

summary.connects_host: Descending	Count
195.123.209.123	128
92.63.87.106	128
46.8.44.39	126
84.19.170.244	125
217.12.218.158	94
diesel-cn.lms.hk	52
evacuator43.ru	52
abdcstudios.com	48
barocchiautofficina.it	47
tirekoypazari.com	47
topscrew.fr	44

top file name written

summary.file_written: Descending	Count
\\?\PIPE\lsarpc	128
C:\Users\bob\AppData\Local\Temp\scs6B93.tmp	4
C:\Users\bob\AppData\Local\Temp\scs6BED.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9C2.tmp	4
C:\Users\bob\AppData\Local\Temp\scsA9F5.tmp	4
C:\Users\bob\AppData\Local\Temp\scsABE0.tmp	4
C:\Users\bob\AppData\Local\Temp\scsAC4D.tmp	4
C:\Users\bob\AppData\Local\Temp\scsACB1.tmp	4

top hashes

target.file.md5: Descending	Count
001653e773e99fd58d8203f91340d01f	1
002359f6c18e8375d55cdece5439d37f	1
00db9142718b69b2a8f6d2ad2f0364e3	1
00e8871947588188d1be754b129e366a	1
01471c6c10f5b8e42244b01746f869c7	1
0154882e66f717cb3ed3abe2e5acc00e	1
01b2ed9c92fee97bc3d6b0435291a58f	1
[illegible]	1

file size

target.file.size: Descending	Count
9,841	3
10,207	3
10,238	3
10,273	3
10,388	3
10,459	3
10,470	3
10,672	3
10,764	3
10,925	3
11,164	3
11,703	3
9,575	2
9,646	2
9,662	2
9,694	2
9,749	2
9,851	2

top command line

summary.command_line: Descending	Count
"C:\Users\bob\AppData\Local\Temp\03AaOiMYQhJu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0BoN7GDBXpdfka3b.exe"	1
"C:\Users\bob\AppData\Local\Temp\0JTx6edAcBua.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OBugN55RGsu.exe"	1
"C:\Users\bob\AppData\Local\Temp\0OcauAkwfYronmH.exe"	1
"C:\Users\bob\AppData\Local\Temp\0Tw4BxO3d.exe"	1
"C:\Users\bob\AppData\Local\Temp\0bou0PECaJdTN.exe"	1
"C:\Users\bob\AppData\Local\Temp\0gMfrjZrxPBLc.exe"	1
"C:\Users\bob\AppData\Local\Temp\0mubbgIWrFympJhh.exe"	1

VT sig normalized

virustotal.normalized: Descending	Count
Nemucod	719
Eldorado	709
Locky	705
JSDldr	702
DLDRG	277
ebewgm	262
ExpKit	86
TGeneric	73
ebahnn	71

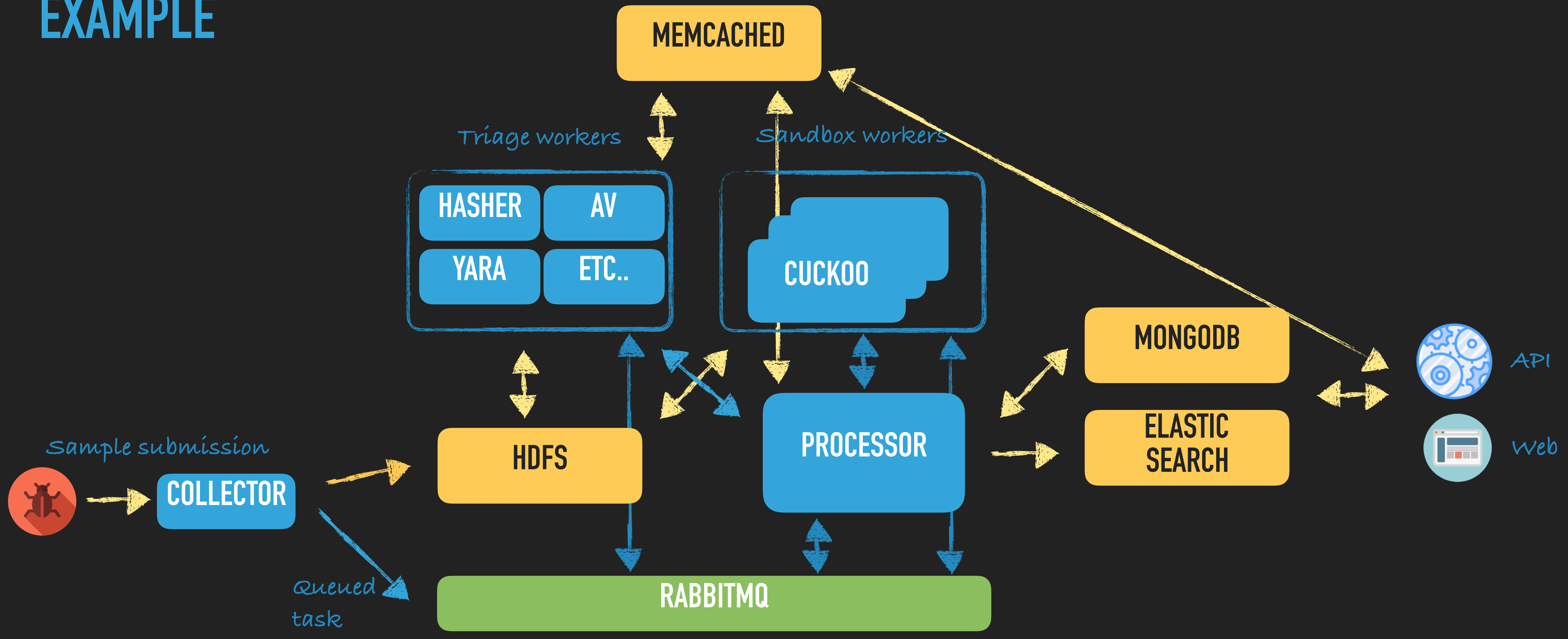
top mutexes

summary.mutex: Descending
IESQMMUTEX_0_208
Local\!IETld!Mutex
Local\ZoneAttributeCacheCounterMutex
Local\ZonesCacheCounterMutex
Local\ZonesCounterMutex
Local\ZonesLockedCacheCounterMutex
Local\c:!users!bob!appdata!roaming!microsoft!windows!ie
RasPbFile

to...

task_id: Descending
1,016
1,017
1,018
1,019
1,020
1,021
1,022
1,023

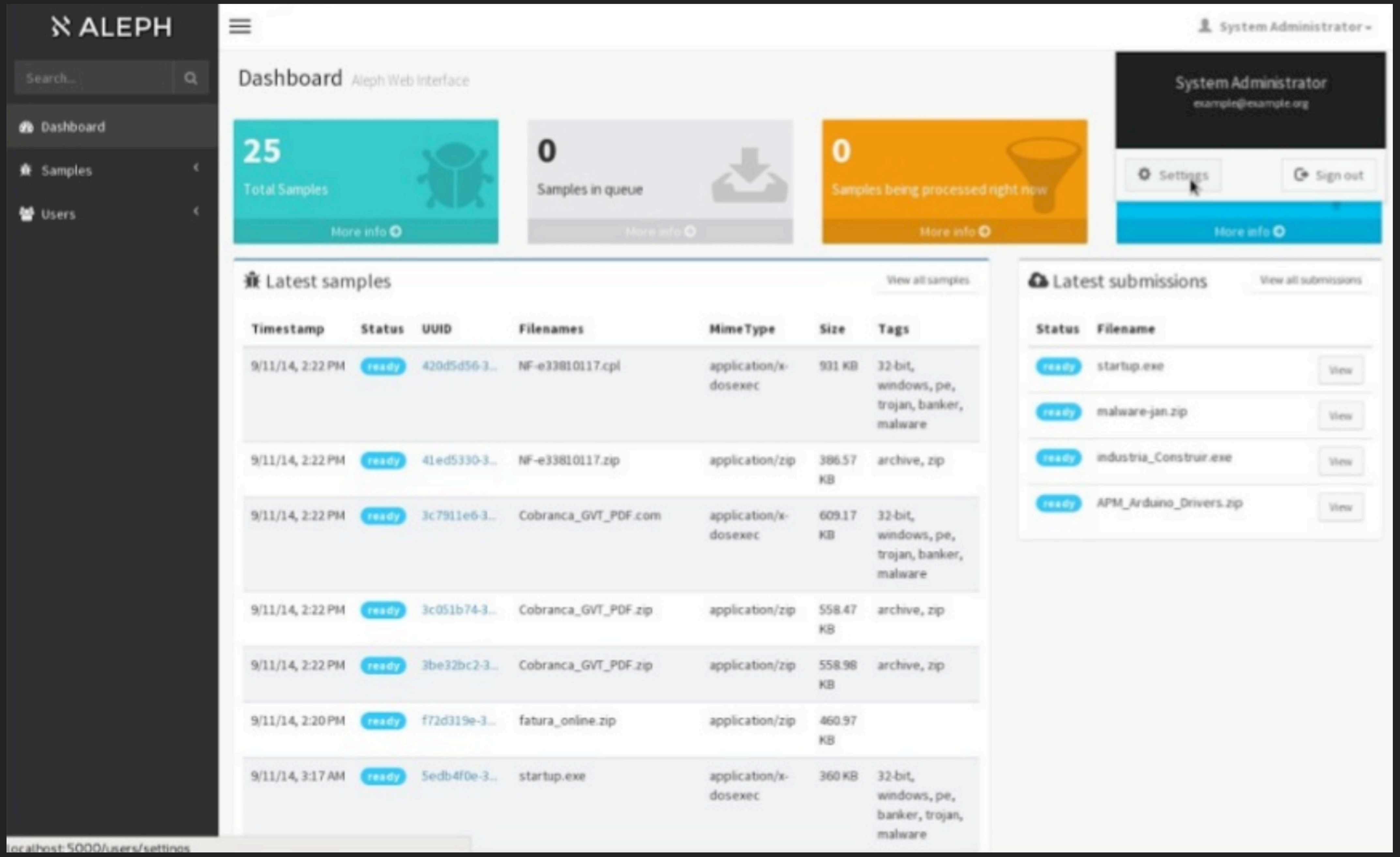
EXAMPLE


MEMCACHED
Triage workers
Sandbox workers
HASHER
AV
YARA
ETC..
CUCKOO
MONGODB
ELASTIC SEARCH
API
Web
Sample submission
COLLECTOR
HDFS
PROCESSOR
Queued task
RABBITMQ

YOU HAVE TO PUT YOUR GLUE

TOOLS

- Most real infrastructure are closed / secret
  - Public malware sandboxes
- Some open projects are just a starting point / PoC:
  - BinaryPig https://github.com/endgameinc/binarypig
  - Aleph https://github.com/merces/aleph
  - FAME https://certsocietegenerale.github.io/fame/
  - StoQ https://stoq.punchcyber.com/
  - MalwareHouse https://github.com/sroberts/malwarehouse
  - IRMA https://github.com/quarkslab/irma
  - Polichombr https://github.com/ANSSI-FR/polichombr



25 Total Samples

0 Samples in queue

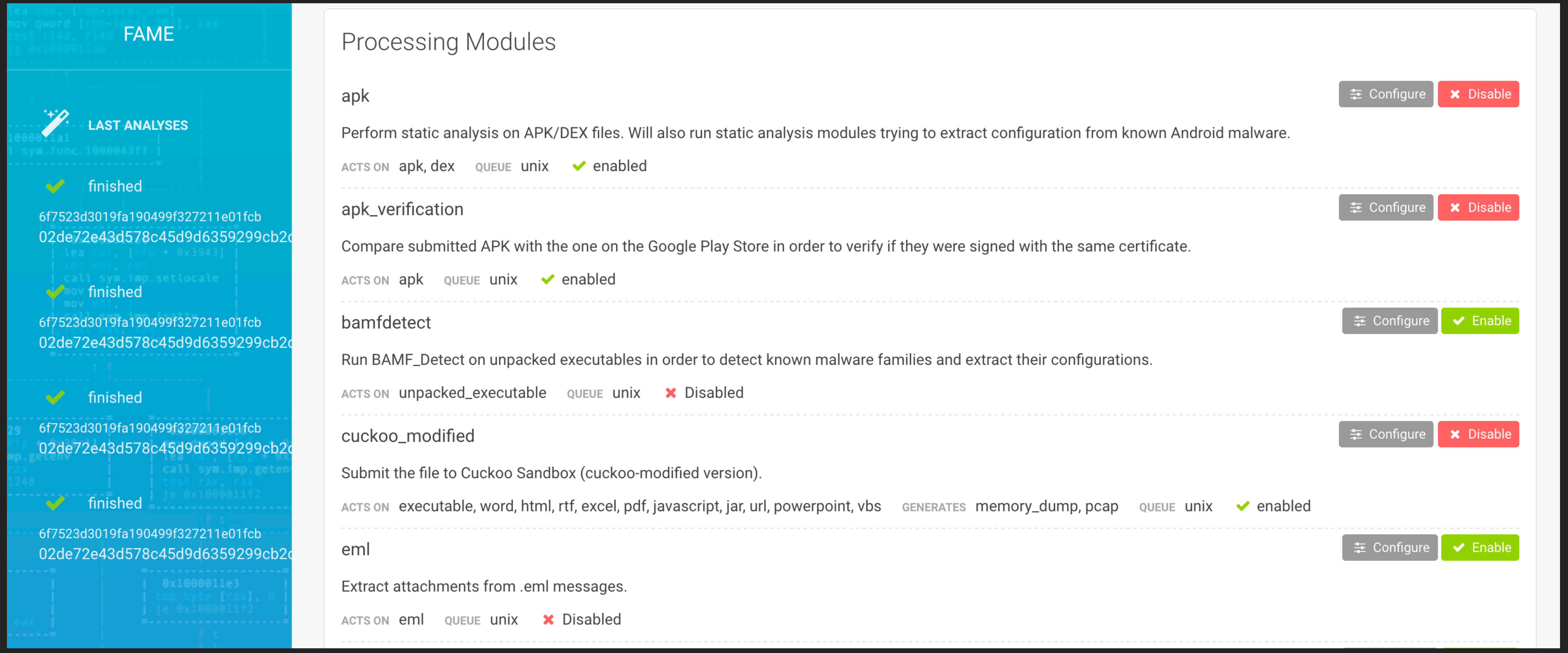
0 Samples being processed right now

Latest samples

Timestamp	Status	UUID	Filenames	MimeType	Size	Tags
9/11/14, 2:22 PM	ready	420d5d56-3...	NF-e33810117.cpl	application/x-dosexec	931 KB	32-bit, windows, pe, trojan, banker, malware
9/11/14, 2:22 PM	ready	41ed5330-3...	NF-e33810117.zip	application/zip	386.57 KB	archive, zip
9/11/14, 2:22 PM	ready	3c7911e6-3...	Cobranca_GVT_PDF.com	application/x-dosexec	609.17 KB	32-bit, windows, pe, trojan, banker, malware
9/11/14, 2:22 PM	ready	3c051b74-3...	Cobranca_GVT_PDF.zip	application/zip	558.47 KB	archive, zip
9/11/14, 2:22 PM	ready	3be32bc2-3...	Cobranca_GVT_PDF.zip	application/zip	558.98 KB	archive, zip
9/11/14, 2:20 PM	ready	f72d319e-3...	fatura_online.zip	application/zip	460.97 KB	
9/11/14, 3:17 AM	ready	5edb4f0e-3...	startup.exe	application/x-dosexec	360 KB	32-bit, windows, pe, banker, trojan, malware

Latest submissions

Status	Filename
ready	startup.exe
ready	malware-jan.zip
ready	industria_Construir.exe
ready	APM_Arduino_Drivers.zip



✓ finished
6f7523d3019fa190499f327211e01fcb
02de72e43d578c45d9d6359299cb2c

✓ finished
6f7523d3019fa190499f327211e01fcb
02de72e43d578c45d9d6359299cb2c

✓ finished
6f7523d3019fa190499f327211e01fcb
02de72e43d578c45d9d6359299cb2c

✓ finished
6f7523d3019fa190499f327211e01fcb
02de72e43d578c45d9d6359299cb2c

Processing Modules

apk

Perform static analysis on APK/DEX files. Will also run static analysis modules trying to extract configuration from known Android malware.

ACTS ON apk, dex QUEUE unix ✓ enabled

apk_verification

Compare submitted APK with the one on the Google Play Store in order to verify if they were signed with the same certificate.

ACTS ON apk QUEUE unix ✓ enabled

bamfdetect

Run BAMF_Detect on unpacked executables in order to detect known malware families and extract their configurations.

ACTS ON unpacked_executable QUEUE unix ✗ Disabled

cuckoo_modified

Submit the file to Cuckoo Sandbox (cuckoo-modified version).

ACTS ON executable, word, html, rtf, excel, pdf, javascript, jar, url, powerpoint, vbs GENERATES memory_dump, pcap QUEUE unix ✓ enabled

eml

Extract attachments from .eml messages.

ACTS ON eml QUEUE unix ✗ Disabled

QUESTIONS ?

No kittens were harmed in the production of this slideshow.

SLIDES

https://go.jekil.sexy/hackinboat19

@jekil

alessandro@tanasi.it ✉

https://jekil.sexy