From Novice to Professional

Starting a Career in Malware Forensics

Andrew Moore – MSc, BSc, PGCE, FHEA, MBCS, CSIR, CMIP, CMI, CFIS, CFIP

Senior Lecturer Practitioner / Digital Forensics Consultant

Cambridge, UK

Andrew.Moore@aru.ac.uk

Speaker Bio

Andrew Moore, Anglia Ruskin University and Cybercrime Forensics Consultant

- Digital Forensics Professional - Consulted in Digital Forensics, e-Discovery & Academic roles across the last ten years
- Senior Lecturer Practitioner & Course Leader for BSc(Hons) Cyber Security & Digital Forensics @ ARU
- Consults for **ALT Digital Investigations**
- Worked on and completed a range of UK & EU projects from **Cyber ASAP** and **ECTEG**
- Holds Certifications such as **CFIP/CFIS**, **CSIR, CMIP/CMI and VCA** and
- Holds qualifications such as **MSc Cyber Security** & **BSc(Hons)** in **Information Security & Forensic Computing**
- Plays guitar, football, computer games and spoils his two naughty cats!

a.r.u.

What we will cover

- Introduction to Malware Forensics and its various roles
- Advice for getting starting in these roles
- Common soft & hard skills across these various roles
- DEMO on Sample files that are free to access
- Widely available resources to help you succeed in this career path:
  - Free tools & building a home lab
  - Evidence samples to freely analysis
  - Resources for learning

Overview

What is Malware Forensics?

Advice for Getting Starting

Common Soft & Hard Skills

Demo on Malware Samples in FLARE VM

Home Lab Setup

Free Tools for Different Roles

List of Malware Samples

Resources for Learning

Conclusion

- What is Malware forensics
- The roles
- Advice for starting
- Soft and hard skills to succeed
- Tools
- Malware samples
- Free Resources

What is Malware Forensics?

Definitions of Related Fields in Scope

- To answer, an understanding of **Digital forensics** is needed for context.
  - Digital forensics is the practice of **identifying, extracting** and **considering evidence** from digital media such as computer hard drives

- Malware forensics is the process of **investigating** and **analysing malicious software (**on those hard drives or Memory**),** known as Malware, to understand its **behaviour, purpose,** and **impact** on **computer systems or networks**

- There are many different types of Malware. Ranging from **Viruses, Worms or Trojans** etc…
- Different companies and authorities categorises these differently.
- Some as a complete new categories or as sub categories under the three above.

Typical Starting Jobs For These Areas

- Most people in Malware Forensics started as an **Analyst, Technician or Software Developer**. Though this is shown differently with many industry buzz words from job to job

- In the Police you will typically have a job in a **High-Tech Crime Unit**
  - Other non-civilian based ways include becoming a **police officer first**, then moving internally to a **computing** role or via the **military**

- **Consulting** is another direction, you can go. you may need to be a little further in you development for this type of job. (more on helping with this later!)
- Depending on the employer, you will need to pass some form of security check (baseline, SC, CTC, DV). Information is linked here: Link

Advice for Getting Starting

a.r.u.

Advice on Education

- Typically a technical honours degree:
  - Digital Forensics & Information Security
  - Cyber Security
  - Computer Science
  - Software Development
  - Networking
  - Investigation Studies
  - Criminology

May require a computing top-up depending on the structure of the degree pathways taken

- Alternatives:
  - MSc Conversion course
  - Apprenticeship program (such as TechSkills)
  - Going down the self-taught route and doing freely available or well known certifications and building an e-portfolio to evidence their learning

Advice on Education

- Understanding the difference between files “on disk” and “in memory”
- Files on the hard disk are not running, they are sleeping (in a way) and when clicked on, wake up and are loaded into memory
  - Static analysis is done on files that are not running if we have a copy of the Malware (more on this in the DEMO)

- Files that are running are in loaded into memory
  - The files on the disk can be different as files in memory can be modified after execution
  - An example would be a legit file was modified in memory and then become infected, changing its behaviour

key Performance Indicators (KPIs)

- KPIs are essential to understand when dealing with Malware as part of an investigation. These are broken down as:
  - Ports
  - Processes
  - Files
  - Startup

- Once you have an understanding of these, its only a matter of time before the Malware will show itself
- Its all about quick wins, once achieved, further analysis can be performed at a later date if the business requires it.
  - As sometimes its just, "Is the Malware gone? Yes! Okay, bye!" ☺

Advice Continued…

- You will need a **home lab** to start/continue your development. (be it **locally virtualised** or **cloud based**)
  - There is a section coming on getting start on this, so don't worry!

- This can amount to a **portfolio** that you can show/demonstrate to an employer of your current skills and interests
  - This way you are a known quantity and know what you need training wise
    - *"If they are this driven by themselves, imagine what they would be like with professional training and guidance"*

- Fundamentals are key to your success. Start in one place and build up you knowledge before moving on
  - Start in **Windows**, then move to other **operating systems** only when you have a good level of **experience**)

Common Soft & Hard Skills

Common Soft Skills

It would be ideal if you were able to:

- Work in a team
- Work by yourself
- Taking notes
  - (build a **user guide** for tasks when shown) refer to this when stuck
- Travel as infections will typically require on site work due to the possibility of further infection

- Manage your own time
  - (You might be involved in different cases at any given time)
- Interact with clients or law enforcement directly
- Have an investigative mindset (great book on this in the resource section)

Common Hard Skills

It would be ideal if you were able to:

- Have a good grasp on current legislation
  - (RIPA, PACE, CMA, GDPR)
- Have a good understanding of current ISO/guidelines
  - (27001,2 etc, 17025, ACPO 4 principles)
- Not be afraid of command lines
  - (CMD, PowerShell, Terminal) its your future!
- Understanding what an incident response plan is and when it was last tested
  - Having a known good config

- Show a good understanding of networking
  - (IP addresses, ports, protocols, OSI/TCPIP models, devices & their function on a network)
- Show good understanding of computer hardware
  - (CPU, RAM, HDD but also types of computer)
- Have an understanding of what artefacts you can gain from a popular operating system such as windows 10
  - (Prefetch, Shell bags, Jump lists, SAM)

Demo on Malware Samples in FLARE VM

DEMO

Home Lab Setup

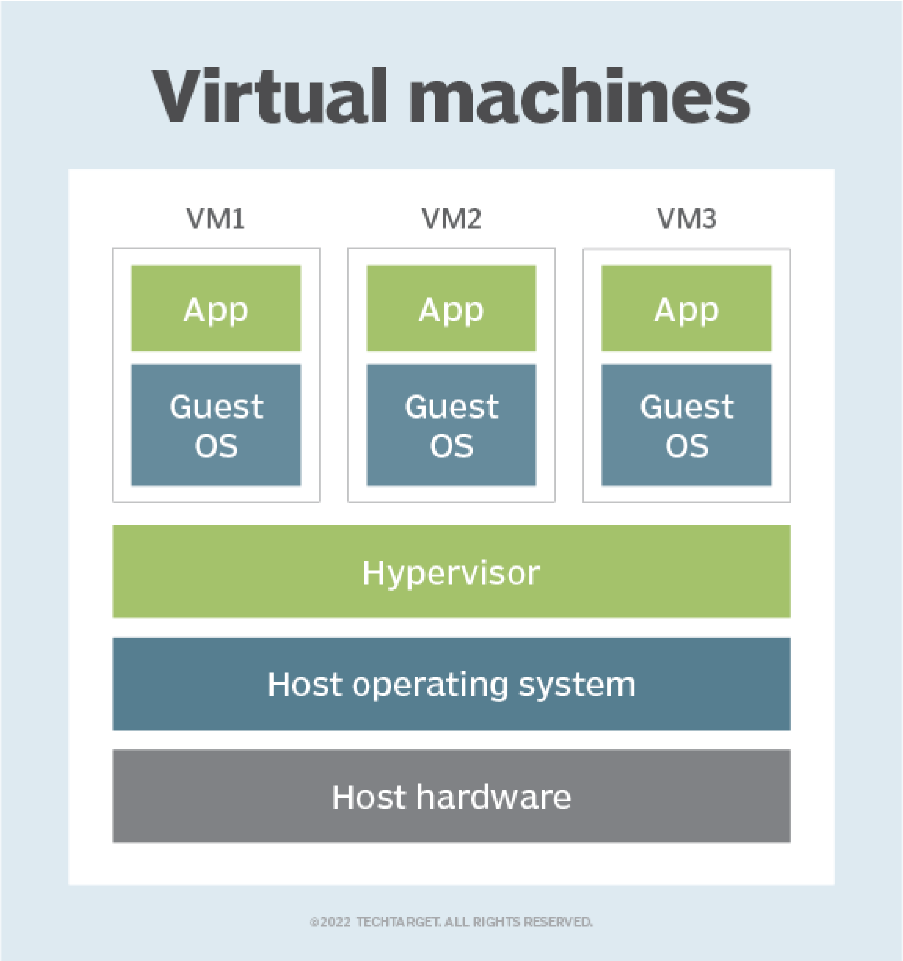
Why Build a Home Lab?

- Home labs offer you a unique chance to craft a **custom learning environment**, just for you
- The environment can be self hosted (on your PC) or in the cloud on AWS/Azure etc (though they come with large costs)
- Oracle Cloud (OCI) has a free forever tier 4 Cores/24GB RAM, 200GB storage and Linux based
- A Raspberry Pi, may also be an option if you happen to have the latest models with enough RAM or even an old workstation from eBay
- This could be a fantastic tool to build skills and show a potential employer that there is a low risk to hiring you!

Home Lab Hardware

- Typically you will need a computer that will be able to run two operating systems at one time (Host & Guest)
    - Software details included in the next section
- Recommendations would include:
    - 4 Cores/8Threads (Slightly higher for Windows Guest VMs)
    - 16GB of RAM
    - An SSD with 500GB of storage
    - Two screens if you happen to have one (I used my TV for years)

Image taken from techtarget.com link

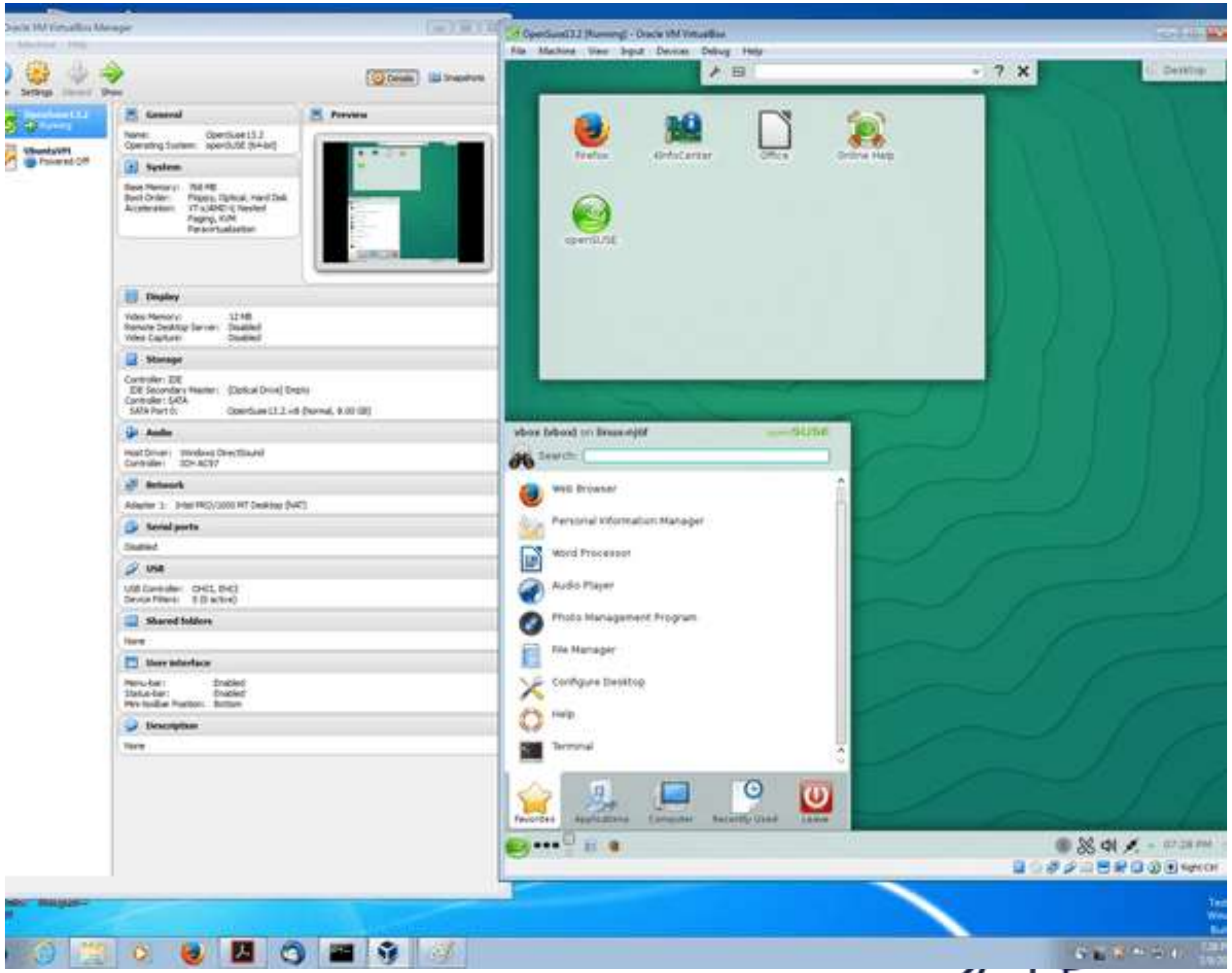


Free Tools for Different Roles

Virtual Box

- This software allows you to have an operating system, nested inside of your own current one.
- This allows you to play in a "sandbox"
- Install any tools you want
- Change specific sets such as turning of your antivirus or changing your network settings
- Allows the use of snapshots (reset button or save specifics to go back to)

Image taken from VirtualBox Link



Oracle VM VirtualBox Manager

General
Name: OpenSuse13.2
Operating System: openSUSE (64-bit)

System
Base Memory: 768 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization

Display
Video Memory: 12 MB
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: OpenSuse13.2.vdi (Normal, 8.00 GB)

Audio
Host Driver: Windows DirectSound
Controller: ICH AC97

Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT)

Serial ports
Disabled

USB
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders
None

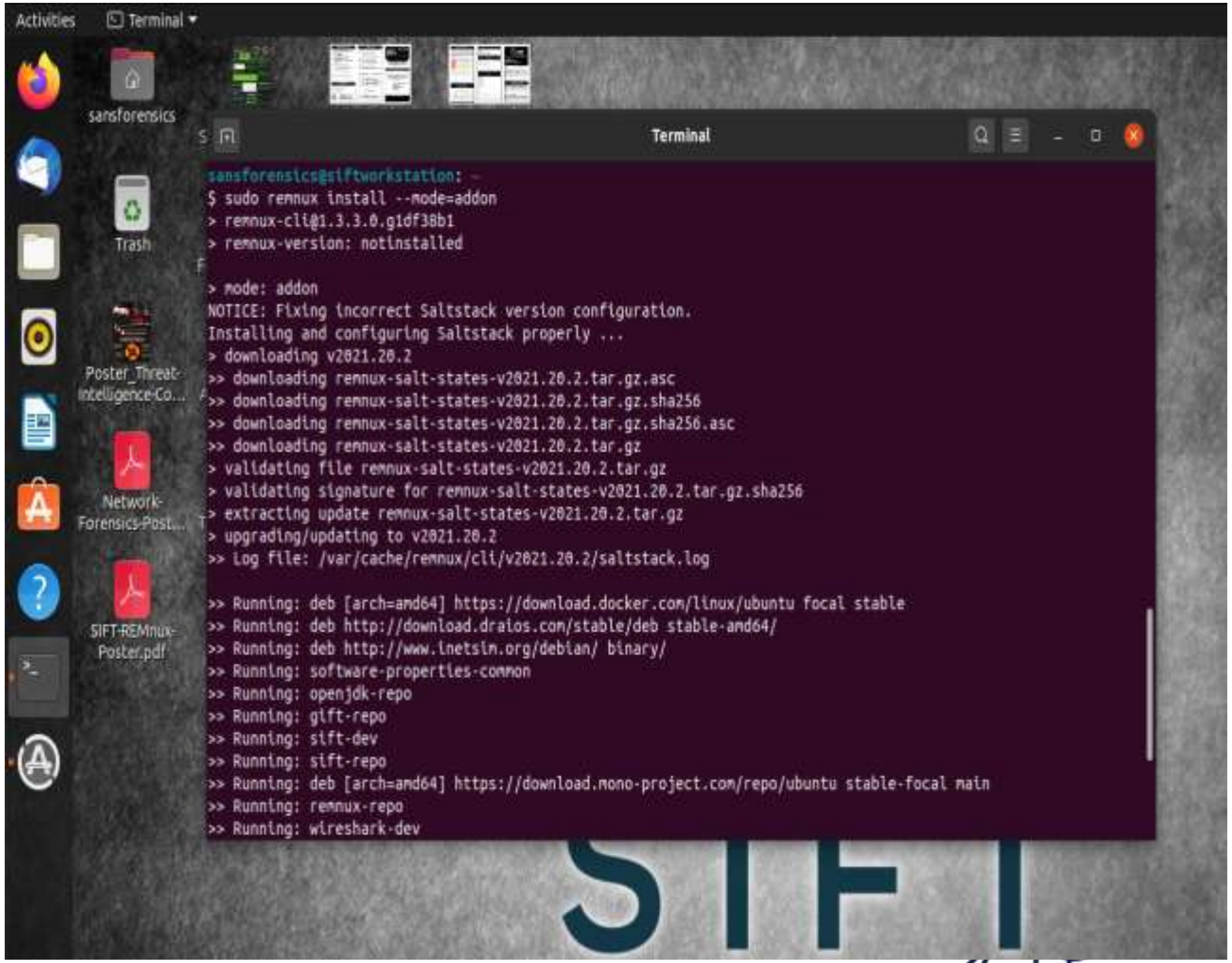
User interface
Menu-bar: Enabled
Status-bar: Enabled
Mini-toolbar Position: Bottom

Description
None

SIFT

- The SIFT Workstation is a collection of free and open-source incident response and forensic tools designed to perform detailed digital forensic examinations in a variety of settings
- SIFT demonstrates that advanced incident response capabilities and deep-dive digital forensic techniques
- Uses cutting-edge open-source tools that are freely available, frequently updated and links with REMnux (next slide)

Image taken from sans.org Link

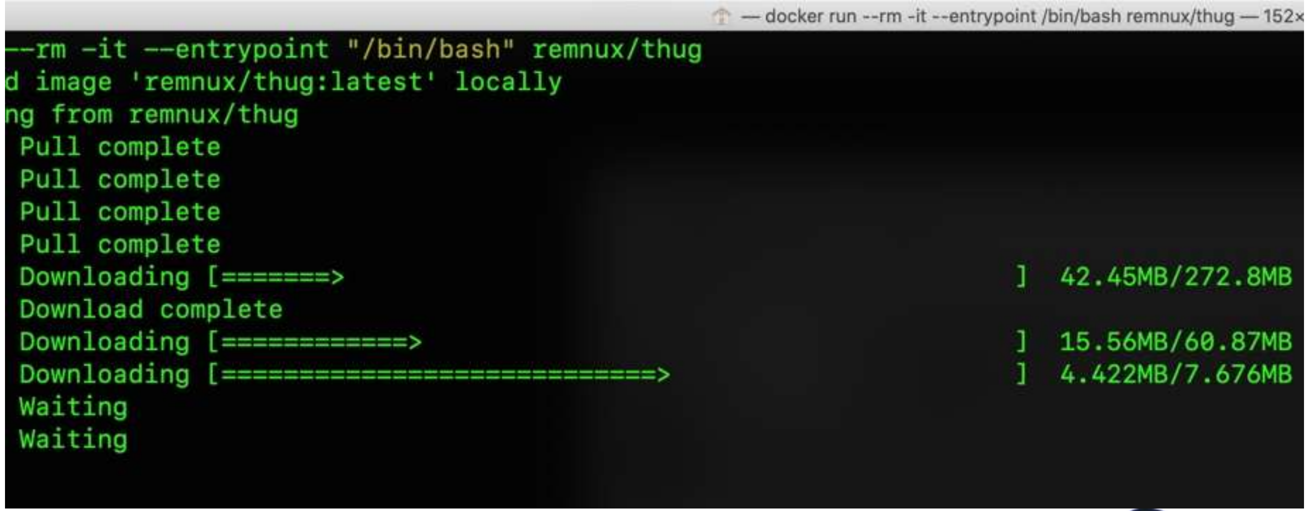


```
sansforensics@siftworkstation: ~
$ sudo remnux install --mode=addon
> remnux-cli@1.3.3.0.g1df38b1
> remnux-version: notinstalled

> mode: addon
NOTICE: Fixing incorrect Saltstack version configuration.
Installing and configuring Saltstack properly ...
> downloading v2021.20.2
>> downloading remnux-salt-states-v2021.20.2.tar.gz.asc
>> downloading remnux-salt-states-v2021.20.2.tar.gz.sha256
>> downloading remnux-salt-states-v2021.20.2.tar.gz.sha256.asc
>> downloading remnux-salt-states-v2021.20.2.tar.gz
> validating file remnux-salt-states-v2021.20.2.tar.gz
> validating signature for remnux-salt-states-v2021.20.2.tar.gz.sha256
> extracting update remnux-salt-states-v2021.20.2.tar.gz
> upgrading/updating to v2021.20.2
>> log file: /var/cache/remnux/cli/v2021.20.2/saltstack.log

>> Running: deb [arch=amd64] https://download.docker.com/linux/ubuntu focal stable
>> Running: deb http://download.draios.com/stable/deb stable-amd64/
>> Running: deb http://www.inetsim.org/debian/ binary/
>> Running: software-properties-common
>> Running: openjdk-repo
>> Running: gift-repo
>> Running: sift-dev
>> Running: sift-repo
>> Running: deb [arch=amd64] https://download.mono-project.com/repo/ubuntu stable-focal main
>> Running: remnux-repo
>> Running: wireshark-dev
```

REMnux

- REMnux is a Linux toolkit for reverse-engineering and analysing malicious software.
- REMnux provides a curated collection of free tools created by the community.
- Analysts can use it to investigate malware without having to find, install, and configure the tools.

Images taken from REMnux [Link]


— docker run --rm -it --entrypoint /bin/bash remnux/thug — 152×

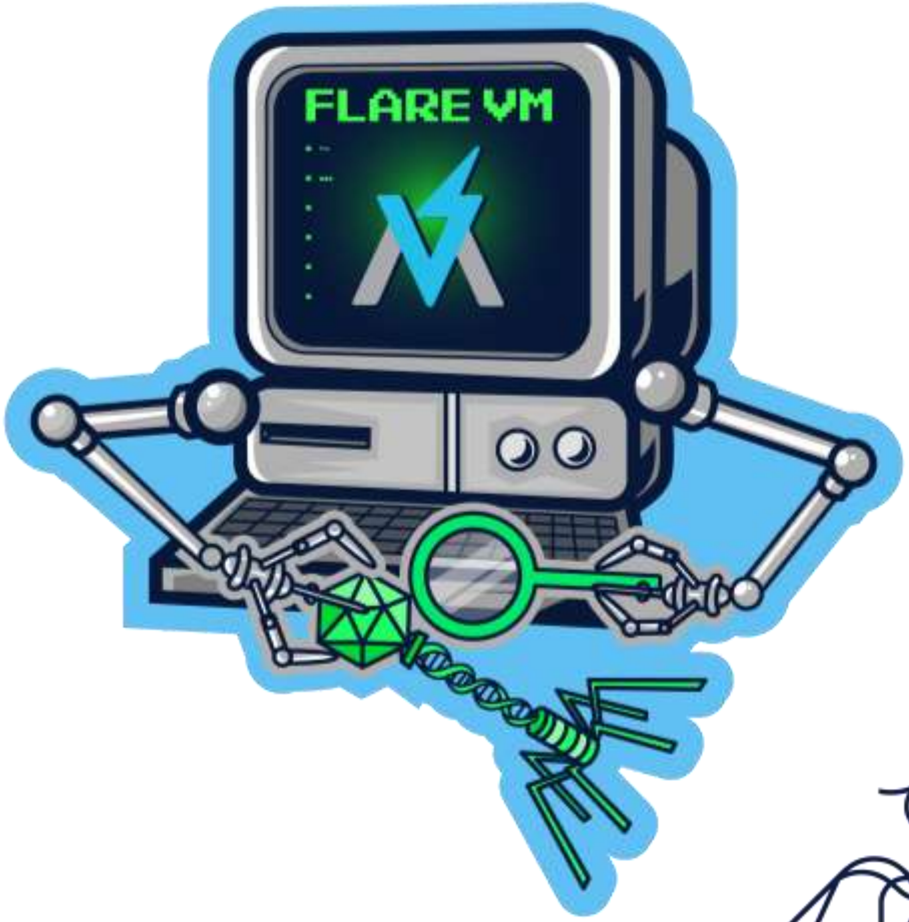
```
--rm -it --entrypoint "/bin/bash" remnux/thug
d image 'remnux/thug:latest' locally
ng from remnux/thug
 Pull complete
 Pull complete
 Pull complete
 Pull complete
 Downloading [=======>                                                   ]  42.45MB/272.8MB
 Download complete
 Downloading [============>                                              ]  15.56MB/60.87MB
 Downloading [============================>                              ]  4.422MB/7.676MB
 Waiting
 Waiting
```

FLARE VM

- FLARE is a collection of software installations scripts for Windows systems that allows you to easily setup and maintain a reverse engineering environment on a virtual machine

- Needs a specific version of Windows 10 (via Microsoft online for free but will need a licence to use past 30 days)
- Covers hundreds of tools mostly preconfigured or ready to be go

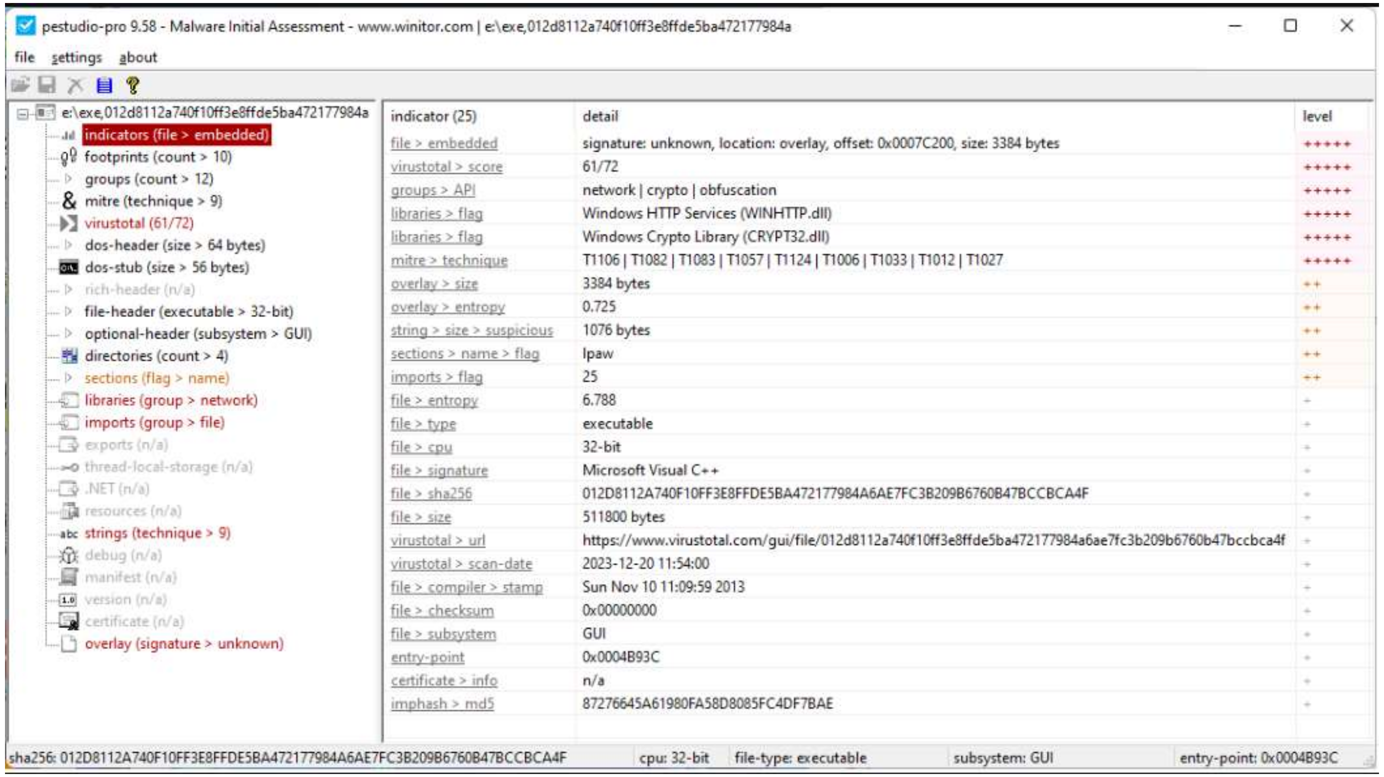
Image taken from GitHub/Mandiant
Link



PEStudio

- PEStudio is great of the static analysis of an executable file
- Its free for personal use and also comes included in FLARE
- Great for quick wins with resources for its results easily findable

Image taken from Winitor Link


pestudio-pro 9.58 - Malware Initial Assessment - www.winitor.com | e:\exe,012d8112a740f10ff3e8ffde5ba472177984a
file
settings
about

- e:\exe,012d8112a740f10ff3e8ffde5ba472177984a
  - indicators (file > embedded)
  - footprints (count > 10)
  - groups (count > 12)
  - mitre (technique > 9)
  - virustotal (61/72)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 56 bytes)
  - rich-header (n/a)
  - file-header (executable > 32-bit)
  - optional-header (subsystem > GUI)
  - directories (count > 4)
  - sections (flag > name)
  - libraries (group > network)
  - imports (group > file)
  - exports (n/a)
  - thread-local-storage (n/a)
  - .NET (n/a)
  - resources (n/a)
  - strings (technique > 9)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (signature > unknown)

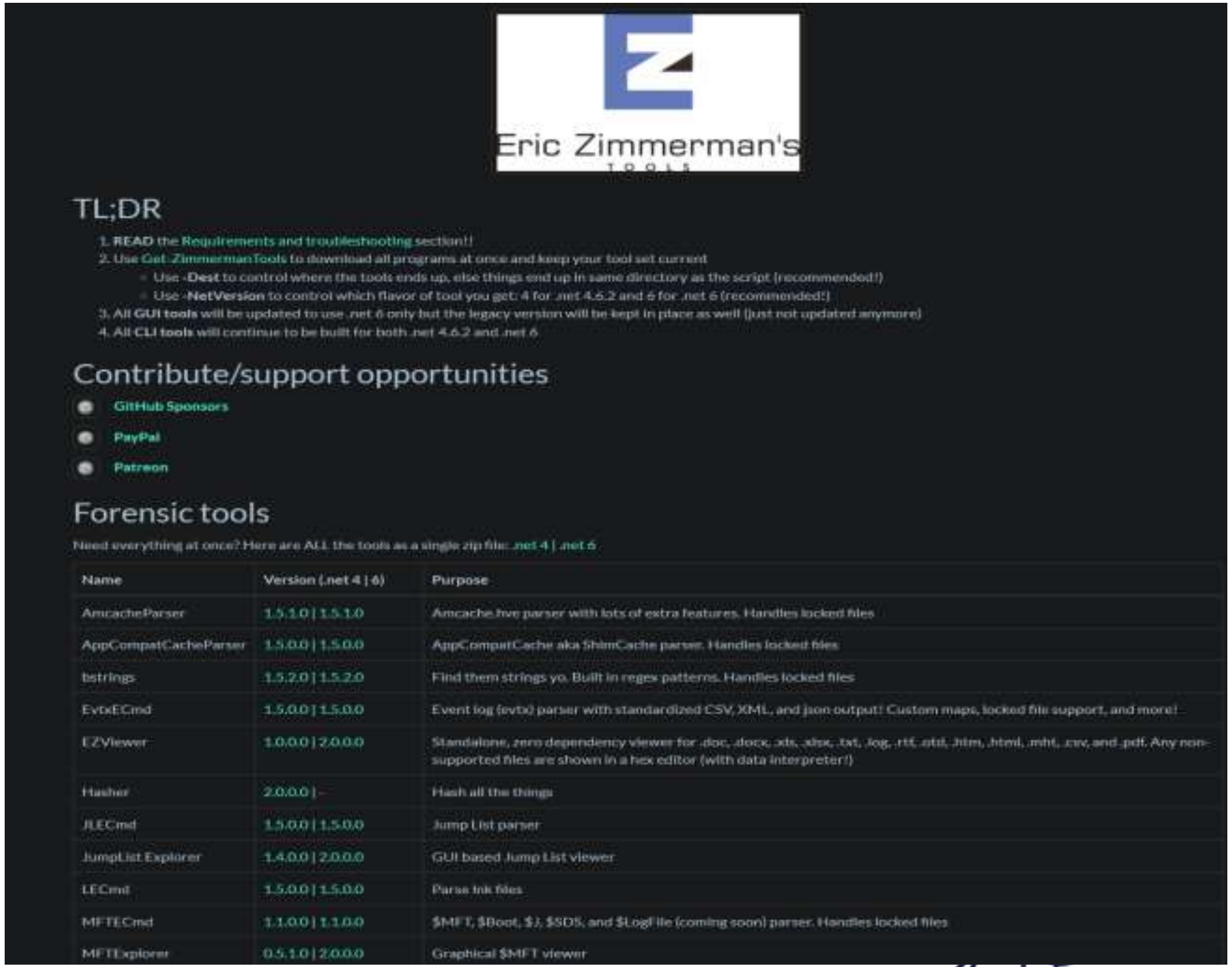
indicator (25)	detail	level
file > embedded	signature: unknown, location: overlay, offset: 0x0007C200, size: 3384 bytes	+++++
virustotal > score	61/72	+++++
groups > API	network | crypto | obfuscation	+++++
libraries > flag	Windows HTTP Services (WINHTTP.dll)	+++++
libraries > flag	Windows Crypto Library (CRYPT32.dll)	+++++
mitre > technique	T1106 | T1082 | T1083 | T1057 | T1124 | T1006 | T1033 | T1012 | T1027	+++++
overlay > size	3384 bytes	++
overlay > entropy	0.725	++
string > size > suspicious	1076 bytes	++
sections > name > flag	Ipaw	++
imports > flag	25	++
file > entropy	6.788	+
file > type	executable	+
file > cpu	32-bit	+
file > signature	Microsoft Visual C++	+
file > sha256	012D8112A740F10FF3E8FFDE5BA472177984A6AE7FC3B209B6760B47BCCBCA4F	+
file > size	511800 bytes	+
virustotal > url	https://www.virustotal.com/gui/file/012d8112a740f10ff3e8ffde5ba472177984a6ae7fc3b209b6760b47bccbca4f	+
virustotal > scan-date	2023-12-20 11:54:00	+
file > compiler > stamp	Sun Nov 10 11:09:59 2013	+
file > checksum	0x00000000	+
file > subsystem	GUI	+
entry-point	0x0004B93C	+
certificate > info	n/a	+
imphash > md5	87276645A61980FA58D8085FC4DF7BAE	+

sha256: 012D8112A740F10FF3E8FFDE5BA472177984A6AE7FC3B209B6760B47BCCBCA4F cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0004B93C

Zimmerman Tools

- Eric Zimmerman, is a forensics specialist who has created many tools to help us in our daily job
- The site contains many tools (including the Prefetch parser to show previously ran programs on Windows!)
- Can be downloaded using a script and are "mostly" command line based with some GUI tools

Image taken from ericzimmerman.github.io Link



Eric Zimmerman's TOOLS

TL;DR

1. **READ** the Requirements and troubleshooting section!!
2. Use Get-ZimmermanTools to download all programs at once and keep your tool set current
    - Use -**Dest** to control where the tools ends up, else things end up in same directory as the script (recommended!)
    - Use -**NetVersion** to control which flavor of tool you get: 4 for .net 4.6.2 and 6 for .net 6 (recommended!)
3. All **GUI tools** will be updated to use .net 6 only but the legacy version will be kept in place as well (just not updated anymore)
4. All **CLI tools** will continue to be built for both .net 4.6.2 and .net 6

Contribute/support opportunities

- GitHub Sponsors
- PayPal
- Patreon

Forensic tools

Need everything at once? Here are ALL the tools as a single zip file: .net 4 | .net 6

Name	Version (.net 4 | 6)	Purpose
AmcacheParser	1.5.1.0 | 1.5.1.0	Amcache.hve parser with lots of extra features. Handles locked files
AppCompatCacheParser	1.5.0.0 | 1.5.0.0	AppCompatCache aka ShimCache parser. Handles locked files
bstrings	1.5.2.0 | 1.5.2.0	Find them strings yo. Built in regex patterns. Handles locked files
EvtxECmd	1.5.0.0 | 1.5.0.0	Event log (evtx) parser with standardized CSV, XML, and json output! Custom maps, locked file support, and more!
EZViewer	1.0.0.0 | 2.0.0.0	Standalone, zero dependency viewer for .doc, .docx, .xls, .xlsx, .txt, .log, .rtf, .otd, .htm, .html, .mht, .csv, and .pdf. Any non-supported files are shown in a hex editor (with data interpreter!)
Hasher	2.0.0.0 | -	Hash all the things
JLECmd	1.5.0.0 | 1.5.0.0	Jump List parser
JumpList Explorer	1.4.0.0 | 2.0.0.0	GUI based Jump List viewer
LECmd	1.5.0.0 | 1.5.0.0	Parse lnk files
MFTECmd	1.1.0.0 | 1.1.0.0	$MFT, $Boot, $J, $SDS, and $LogFile (coming soon) parser. Handles locked files
MFTExplorer	0.5.1.0 | 2.0.0.0	Graphical $MFT viewer

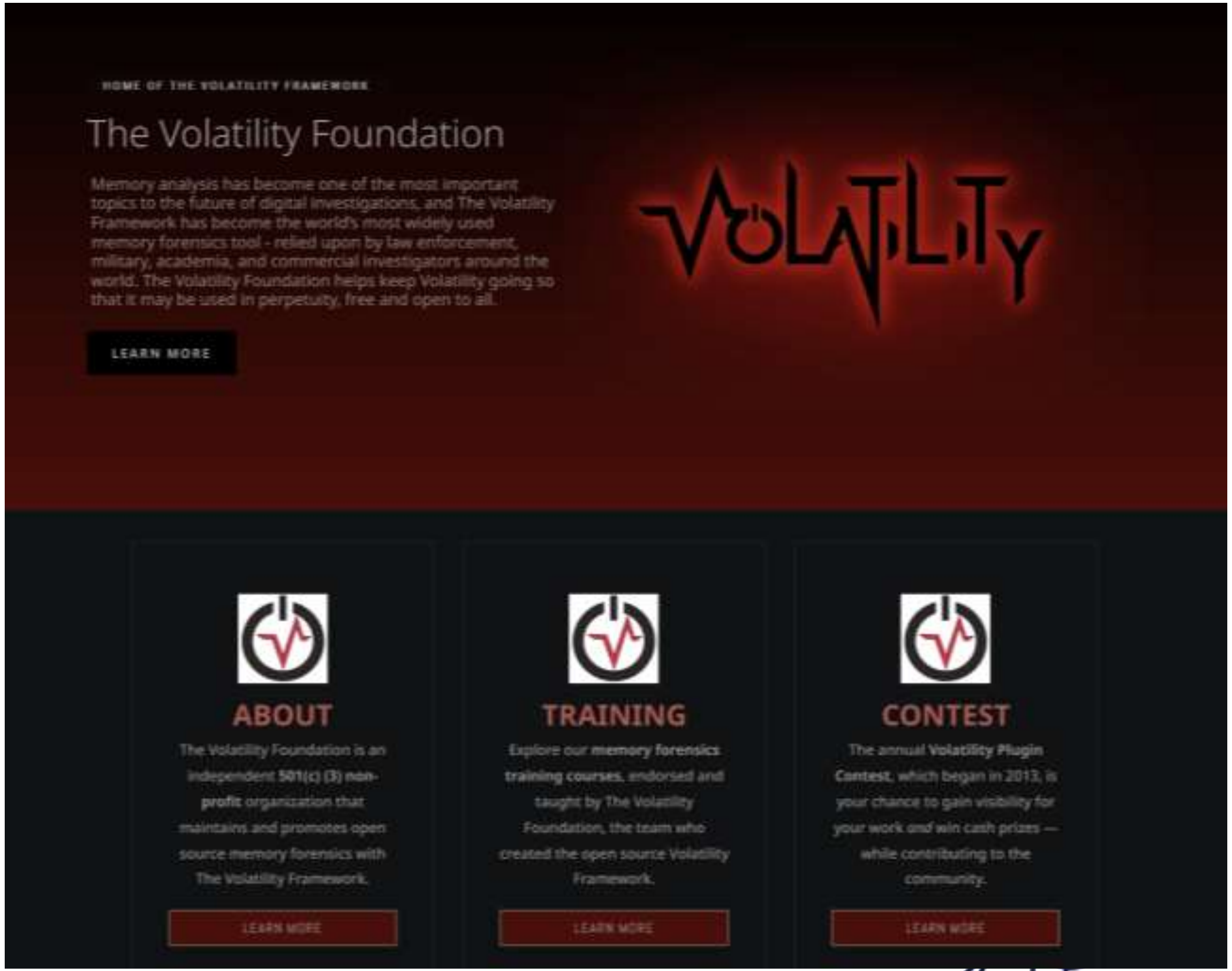
Volatility

- Volatility is a program that allows capture and analysis of computer memory (RAM)

- Very powerful in Forensic/Malware investigations

- Free for personal use and used as a plugin for many well known forensic software

Image taken from Vol Foundation Link



HOME OF THE VOLATILITY FRAMEWORK

The Volatility Foundation

Memory analysis has become one of the most important topics to the future of digital investigations, and The Volatility Framework has become the world's most widely used memory forensics tool - relied upon by law enforcement, military, academia, and commercial investigators around the world. The Volatility Foundation helps keep Volatility going so that it may be used in perpetuity, free and open to all.

ABOUT

The Volatility Foundation is an independent **501(c) (3) non-profit** organization that maintains and promotes open source memory forensics with The Volatility Framework.

TRAINING

Explore our **memory forensics training courses**, endorsed and taught by The Volatility Foundation, the team who created the open source Volatility Framework.

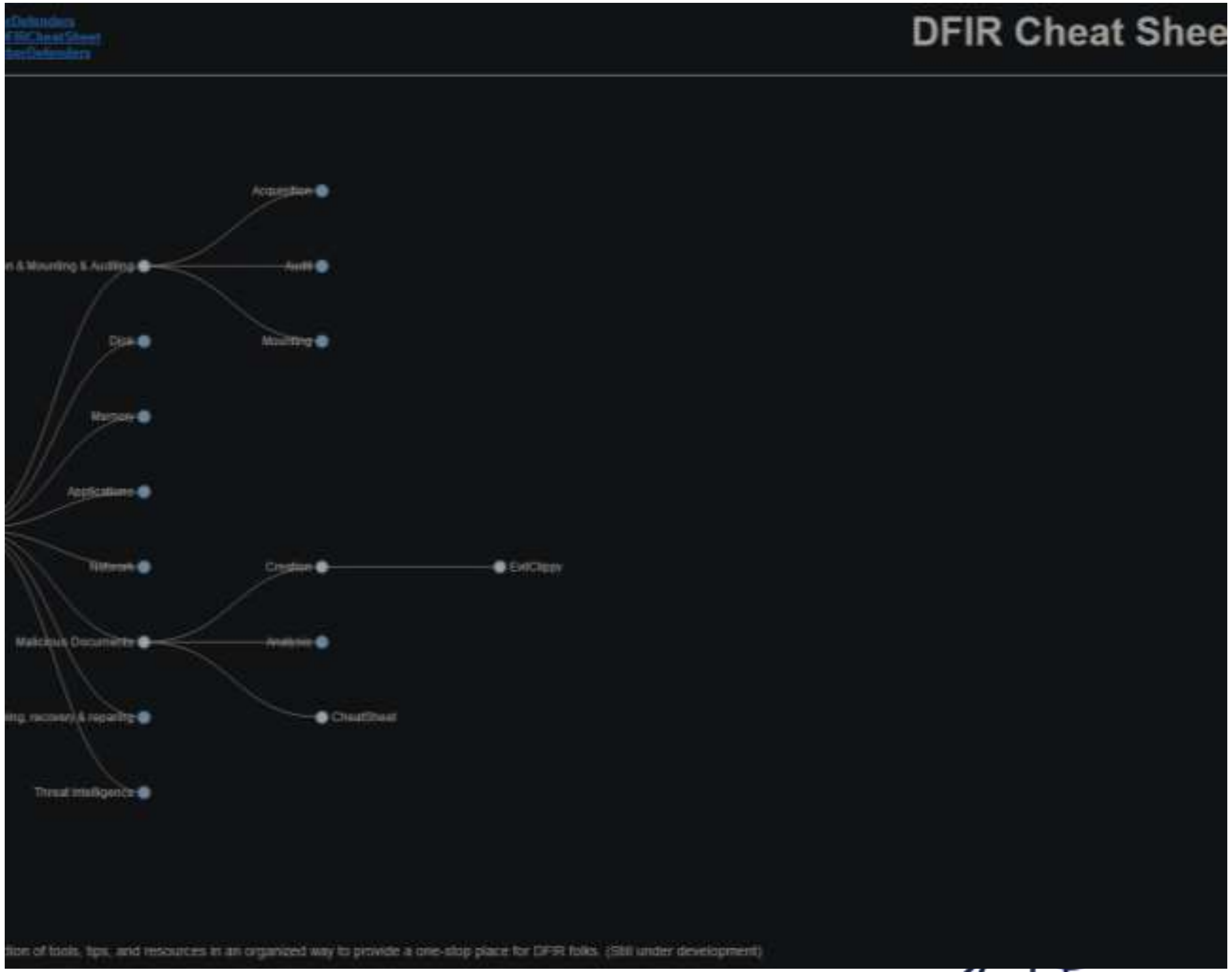
CONTEST

The annual **Volatility Plugin Contest**, which began in 2013, is your chance to gain visibility for your work and win cash prizes — while contributing to the community.

DFIR Training Tools

- Great collection of tools that allow different types of investigation or creation of evidence
- In this case EvilClippy is selected, which creates Malware infected PDFs.
- This can then be used as testing against firewall/IDS/IPS rules for example

Image taken from GitHub Link



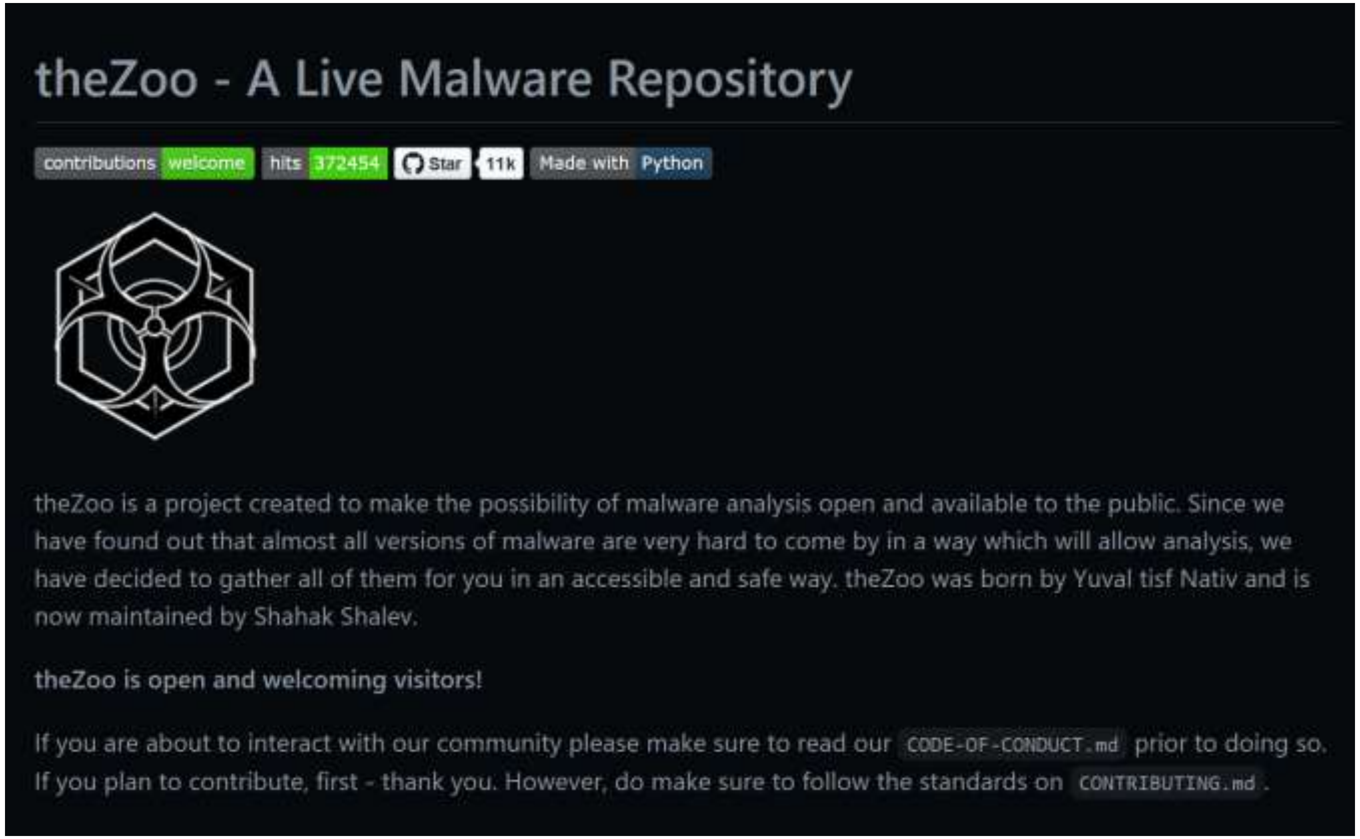
tion of tools, tips, and resources in an organized way to provide a one-stop place for DFIR folks. (Still under development)

List of Malware Samples

The Zoo Repo

- The Zoo Repo is on GitHub and contains thousands of Malware samples to test in your safe environment
- Free of charge with instructions on how to download the samples
- Covers Linux, Mac, Android and Windows etc…

Image taken from GitHub [Link]



theZoo - A Live Malware Repository

theZoo is a project created to make the possibility of malware analysis open and available to the public. Since we have found out that almost all versions of malware are very hard to come by in a way which will allow analysis, we have decided to gather all of them for you in an accessible and safe way. theZoo was born by Yuval tisf Nativ and is now maintained by Shahak Shalev.

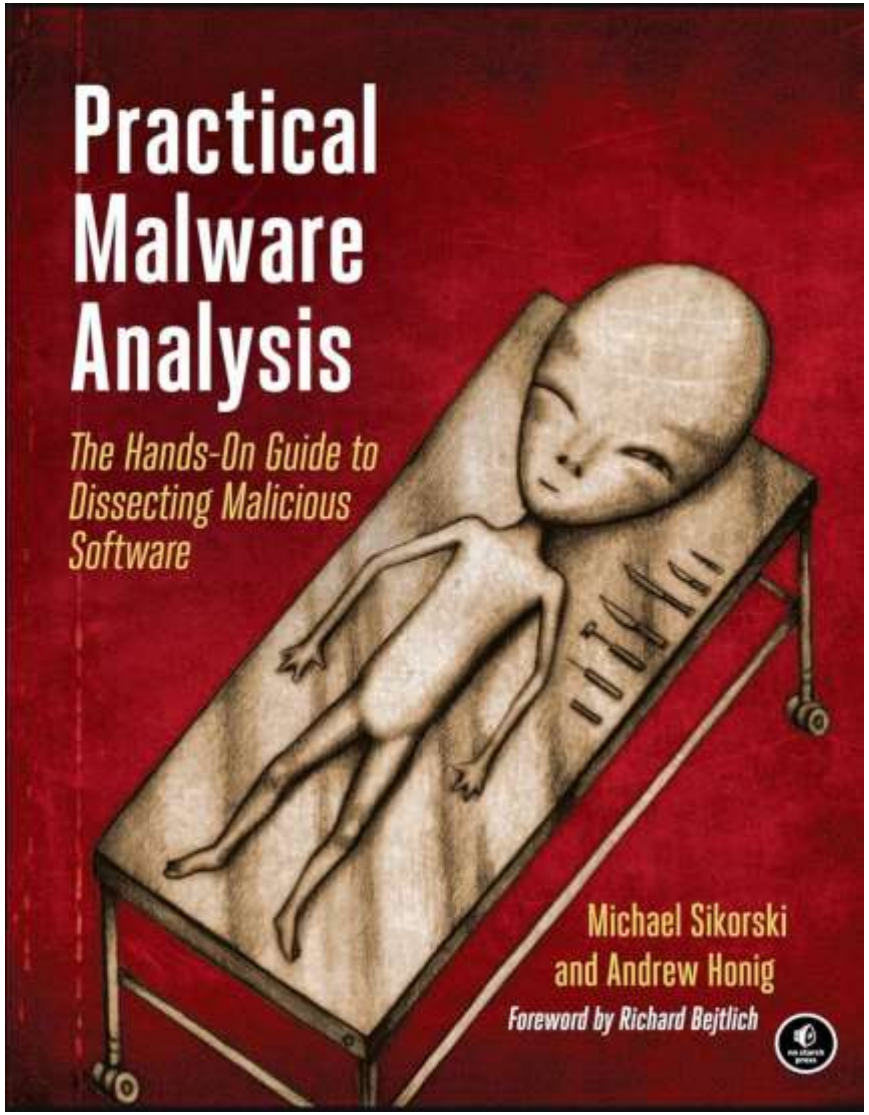
theZoo is open and welcoming visitors!

If you are about to interact with our community please make sure to read our `CODE-OF-CONDUCT.md` prior to doing so. If you plan to contribute, first - thank you. However, do make sure to follow the standards on `CONTRIBUTING.md`.

Practical Malware Analysis

- This is a resource as well as a Malware samples
- The book can be bought online but also found in a university library or possibly a public library at request
- Covers many aspects of XP based Malware (a good starting point) which can then later be built upon

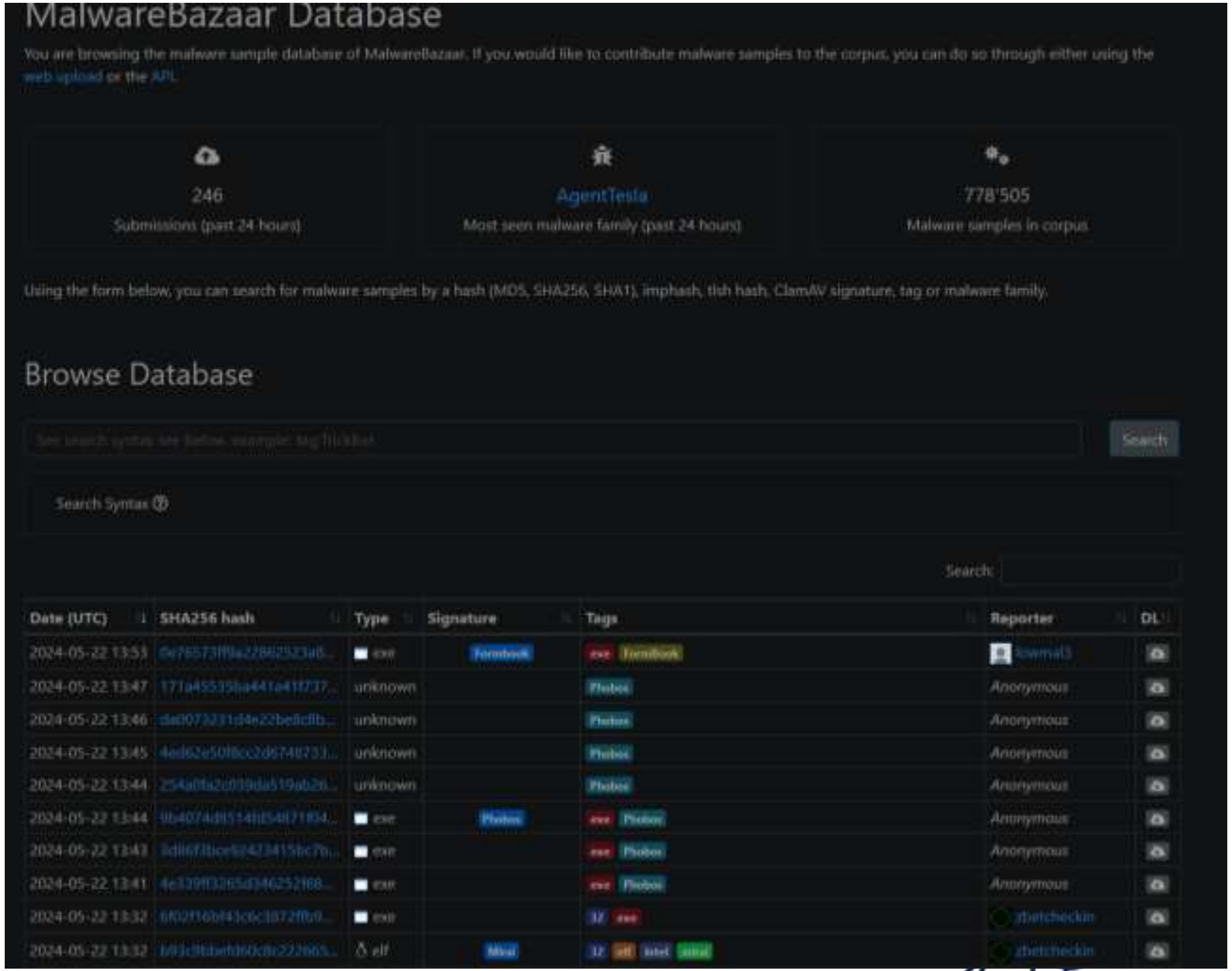
Link to the resource


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

Malware Bazaar

- A great place to find up to date and recent examples of Malware files
- Many are categorised, making it easy to search for samples to test

Image taken from Link



MalwareBazaar Database

You are browsing the malware sample database of MalwareBazaar. If you would like to contribute malware samples to the corpus, you can do so through either using the web upload or the API.

246
Submissions (past 24 hours)

AgentTesla
Most seen malware family (past 24 hours)

778'505
Malware samples in corpus

Using the form below, you can search for malware samples by a hash (MD5, SHA256, SHA1), imphash, tlsh hash, ClamAV signature, tag or malware family.

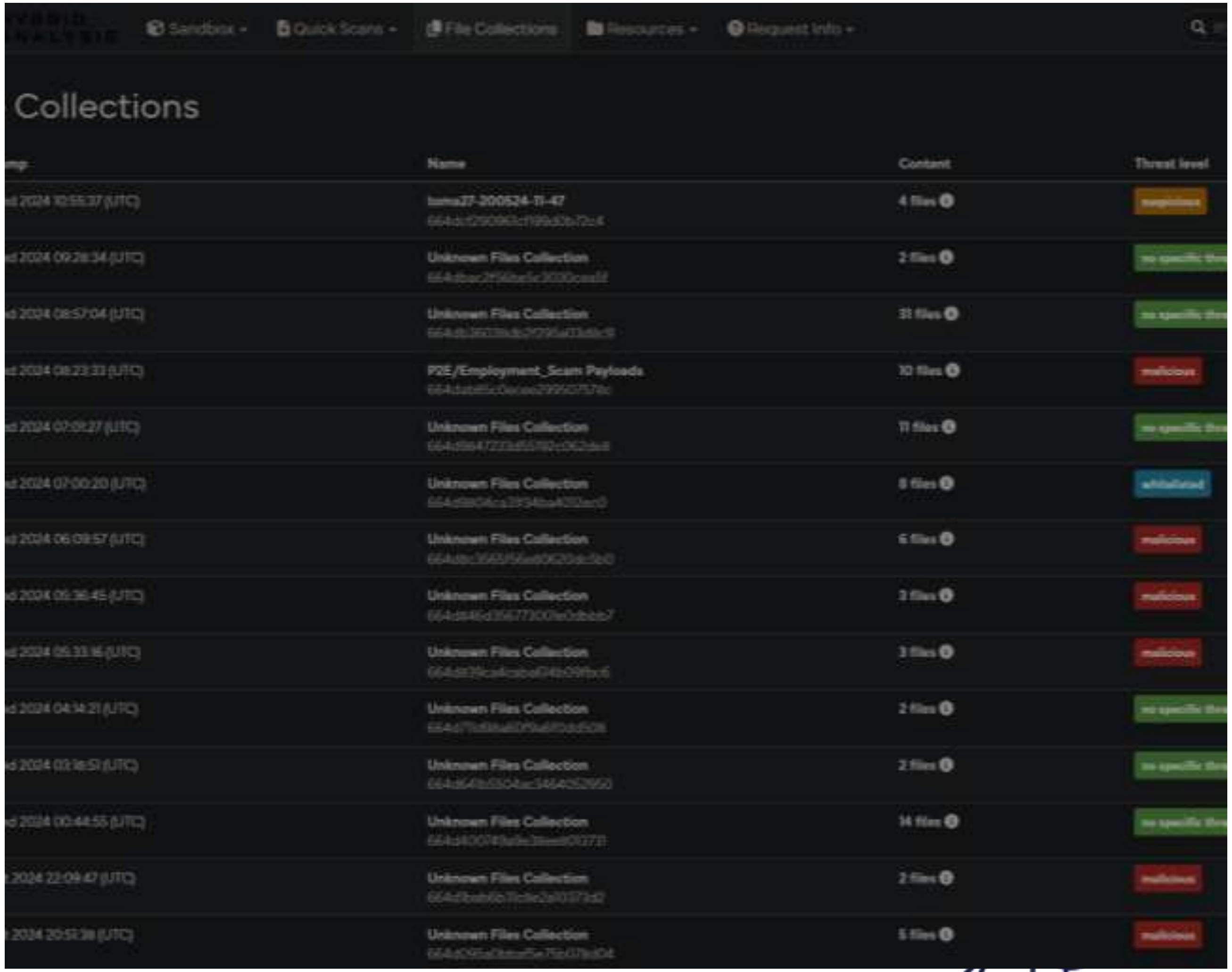
Browse Database

Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2024-05-22 13:53	0e76573ff9a22862523a6...	exe	Formbook	exe Formbook	lowmal3	
2024-05-22 13:47	171a45535ba441a41f737...	unknown		Phobos	Anonymous	
2024-05-22 13:46	da0073231d4e22be8c8b...	unknown		Phobos	Anonymous	
2024-05-22 13:45	4ed62e50f8cc2d5748733...	unknown		Phobos	Anonymous	
2024-05-22 13:44	254a0fa2c039da519ab26...	unknown		Phobos	Anonymous	
2024-05-22 13:44	9b4074d8514fd54f71f04...	exe	Phobos	exe Phobos	Anonymous	
2024-05-22 13:43	3d8f3bce92423415bc7b...	exe		exe Phobos	Anonymous	
2024-05-22 13:41	4e339f3265d346252f68...	exe		exe Phobos	Anonymous	
2024-05-22 13:32	6f02f16bf43c6c3872ff0...	exe		32 exe	zbetcheckin	
2024-05-22 13:32	b93c9bbefd60c8c222665...	elf	Mirai	32 elf intel mirai	zbetcheckin	

Hybrid Analysis

- Like Malware Bazaar, another resource for finding an updated collection of Malware for free
- This website will require an account to download samples, which is verified using a profile on your company website for example

Image taken from Link



Collections

mp	Name	Content	Threat level
d 2024 10:55:37 (UTC)	luma27-200524-11-47 [illegible]	4 files	suspicious
d 2024 09:28:34 (UTC)	Unknown Files Collection [illegible]	2 files	no specific thre
d 2024 08:57:04 (UTC)	Unknown Files Collection [illegible]	31 files	no specific thre
d 2024 08:23:33 (UTC)	P2E/Employment_Scam Payloads [illegible]	10 files	malicious
d 2024 07:01:27 (UTC)	Unknown Files Collection [illegible]	11 files	no specific thre
d 2024 07:00:20 (UTC)	Unknown Files Collection [illegible]	8 files	whitelisted
d 2024 06:09:57 (UTC)	Unknown Files Collection [illegible]	6 files	malicious
d 2024 05:36:45 (UTC)	Unknown Files Collection [illegible]	3 files	malicious
d 2024 05:33:16 (UTC)	Unknown Files Collection [illegible]	3 files	malicious
d 2024 04:14:21 (UTC)	Unknown Files Collection [illegible]	2 files	no specific thre
d 2024 03:18:51 (UTC)	Unknown Files Collection [illegible]	2 files	no specific thre
d 2024 00:44:55 (UTC)	Unknown Files Collection [illegible]	14 files	no specific thre
2024 22:09:47 (UTC)	Unknown Files Collection [illegible]	2 files	malicious
2024 20:51:38 (UTC)	Unknown Files Collection [illegible]	5 files	malicious

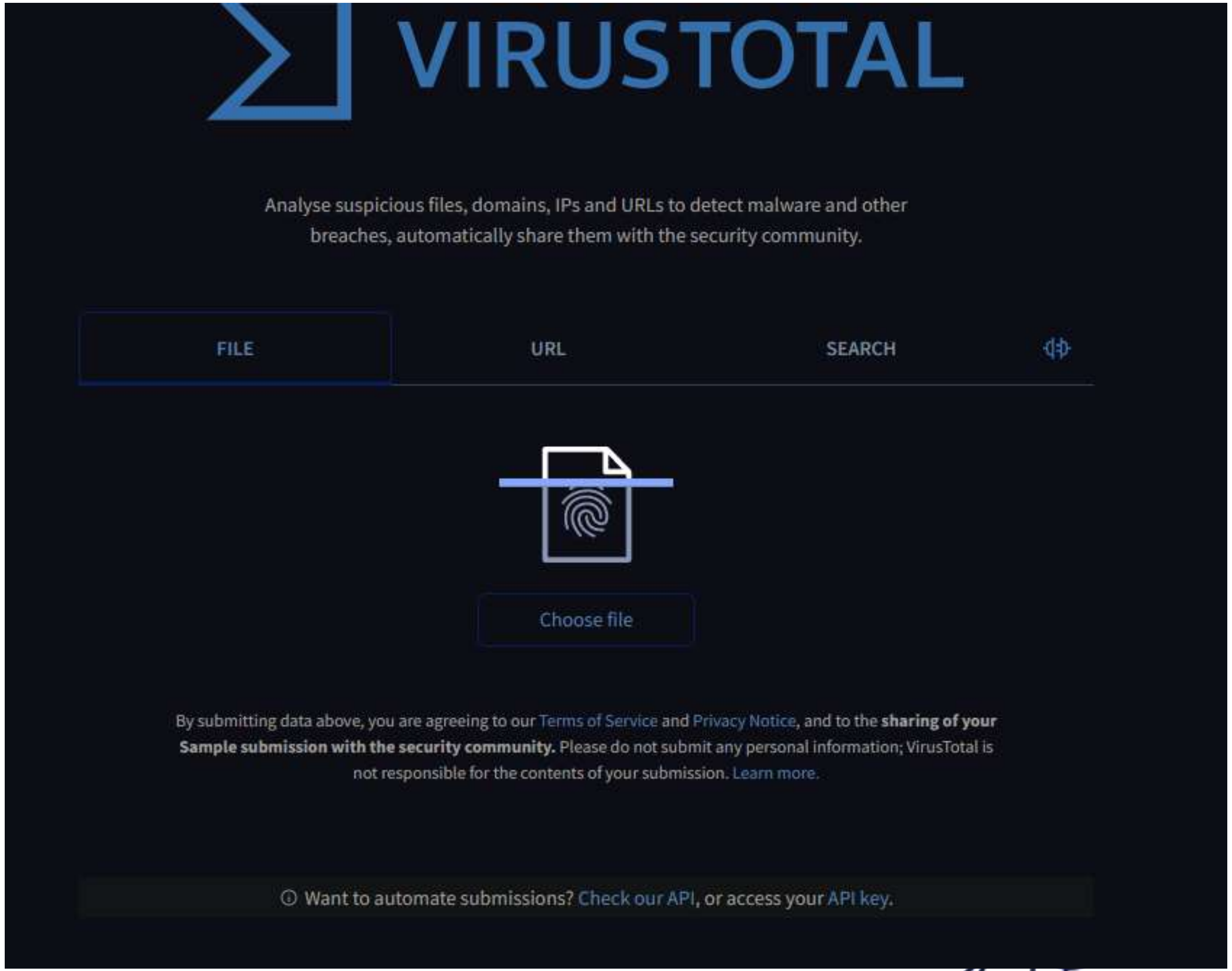
Resources for Learning

Virus Total

- Great places to see if a sample that you have came across has been already analysed by someone.
  - (why do the work twice right?)

- Allows you to upload a sample also if you want it to be scanned against well known Anti-Virus programs

Image taken from Virus Total Link



Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

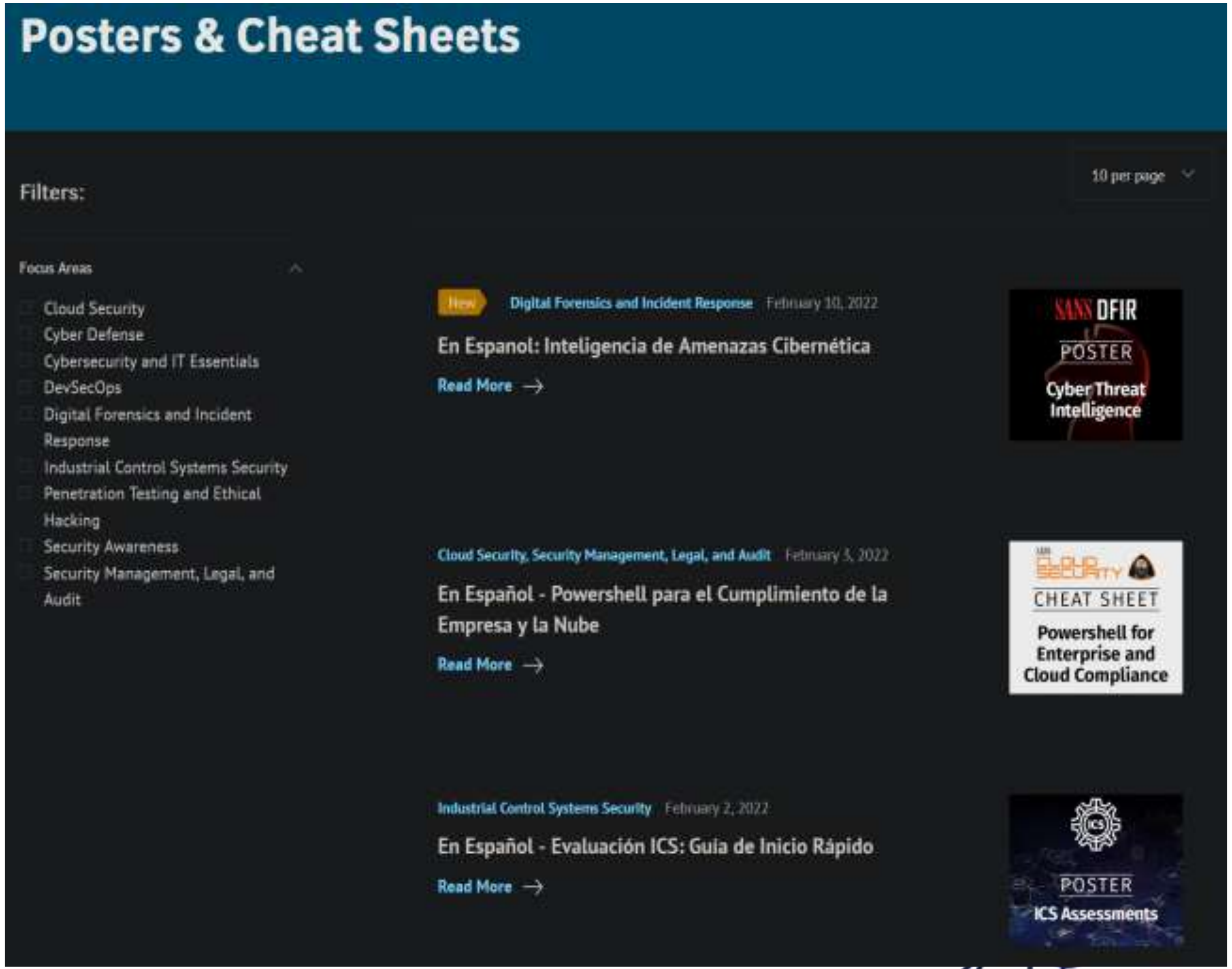
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, or access your API key.

SANs

- SANs have many posters and cheat sheets to help anyone from a beginner to an expert in all things digital forensics & incident response to malware
- The posters and cheat sheets are free, you just need to sign up

Image taken from SANs.org Link
Malware specific Poster Link



Posters & Cheat Sheets

Filters:

10 per page

Focus Areas

□ Cloud Security
□ Cyber Defense
□ Cybersecurity and IT Essentials
□ DevSecOps
□ Digital Forensics and Incident Response
□ Industrial Control Systems Security
□ Penetration Testing and Ethical Hacking
□ Security Awareness
□ Security Management, Legal, and Audit

New Digital Forensics and Incident Response February 10, 2022

En Espanol: Inteligencia de Amenazas Cibernética

Read More →

Cloud Security, Security Management, Legal, and Audit February 3, 2022

En Español - Powershell para el Cumplimiento de la Empresa y la Nube

Read More →

Industrial Control Systems Security February 2, 2022

En Español - Evaluación ICS: Guia de Inicio Rápido

Read More →

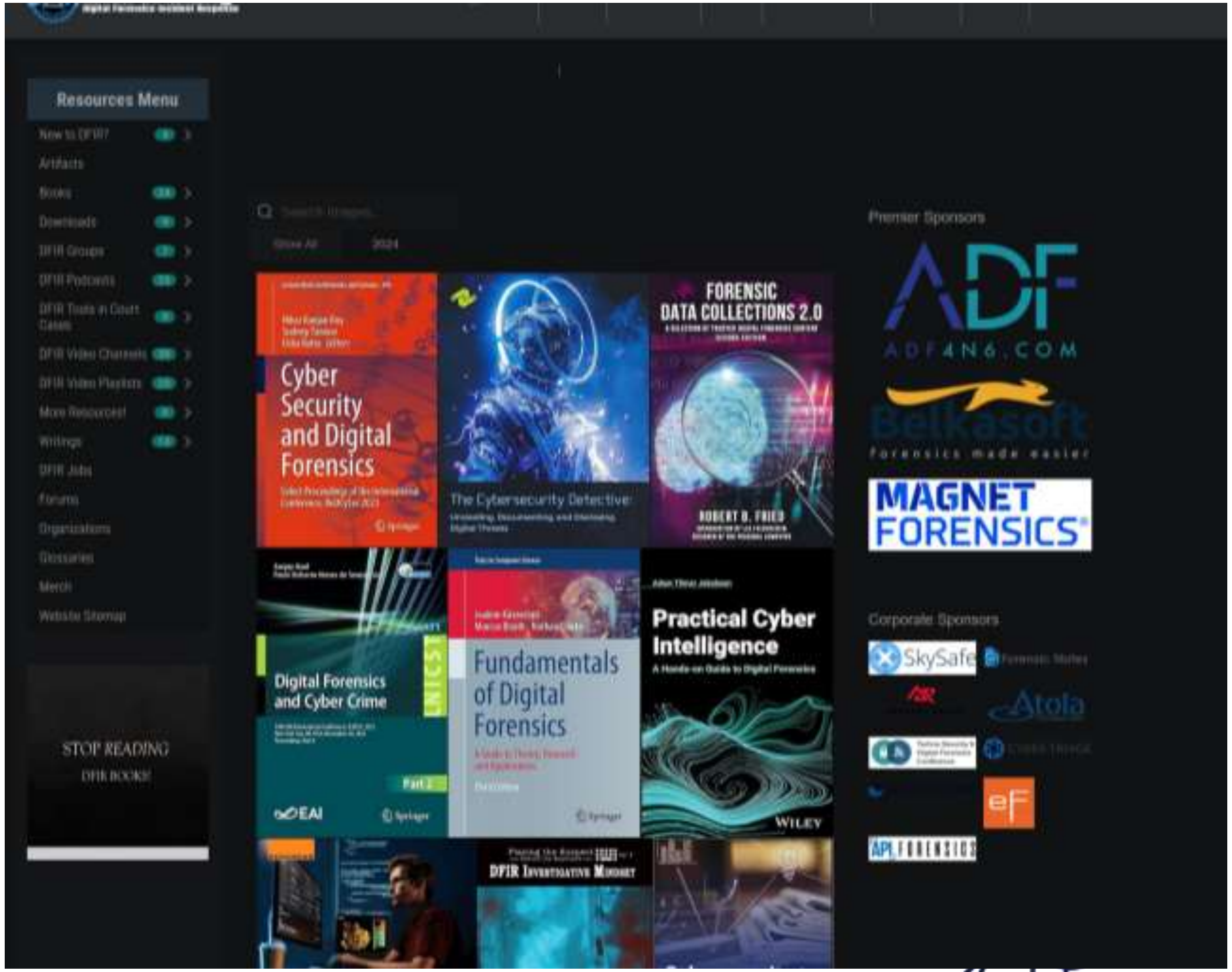
SANS DFIR
POSTER
Cyber Threat Intelligence
CLOUD SECURITY
CHEAT SHEET
Powershell for Enterprise and Cloud Compliance
ICS
POSTER
ICS Assessments

DFIR Training Collection

- DFIR Training (Digital Forensics & Incident Response) is a collection of resource such as books, evidence, podcasts and tools

- Very well known Forensic resource as well as developed books on investigator Mindset, which is a fantastic read!

Image taken from [Link]()



Conclusion

- What is Malware forensics
- The roles
- Advice for starting
- Soft and hard skills to succeed
- Tools
- Malware samples
- Free Resources

Any questions?

- Andrew Moore – MSc, BSc, PGCE, FHEA, MBCS, CSIR, CMIP, CMI, CFIS, CFIP
- Senior Lecturer Practitioner / Digital Forensics Consultant
- Cambridge, UK

- Andrew.Moore@aru.ac.uk

a.r.u.

bcs The Chartered Institute for IT