From Novice to Professional

Starting a Career in Cybercrime Forensics

Andrew Moore - PGCE, FHEA, BSc, CSIR, CFIP

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 eight years
- Course leader for BSc(Hons) Digitech (Cyber, Network, Software) at ARU
- Consults for **Botprobe**, a Cambridge start-up
- Worked on and completed a range of UK & EU projects from **Cyber ASAP** and **ECTEG**
- Holds qualifications such as **CFIP**, **CSIR** and a **BSc(Hons)** in **Information Security & Forensic Computing**
- Plays guitar, football and computer games

What we will cover

- Digital Forensics and its various types such as cybercrime forensics
- Advice for getting starting in these roles
- Common soft & hard skills across these various roles
- DEMO on Prefetch files
- 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 Digital Forensics?

Advice for Getting Starting

Common Soft & Hard Skills

Demo on Prefetch Files

Home Lab Setup

Free Tools for Different Roles

List of Evidence Samples

Resources for Learning

Conclusion

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

What is Digital Forensics?

What is Digital Forensics?

- Digital forensics is the practice of **identifying, extracting** and **considering evidence** from digital media such as computer hard drives

- Digital evidence is both **fragile** and **volatile** and requires the attention of a certified specialist to ensure that materials of evidentiary value can be:
    - Effectively isolated
    - Extracted in a scientific manner
    - Will stand up to the scrutiny of a court of law

The Value to Our Society

- A report from the police-foundation states:
  - ***"The importance of digital forensics as a core capability within policing and criminal justice cannot be overstated."*** – which is true, many (potential) crimes have some form of digital evidence to be analysed (CCTV, phones, fitbits, cars etc)

  - ***"It is not easy to assess the public value delivered by digital forensics for a number of reasons***
    - ***no consolidated picture of the value generated by digital forensics***
    - ***An area of considerable change and flux, there is little academic research on the impact of digital forensic work."***

- **"Later the report states on the benefits to the public**
  - **Swifter justice through the early identification of offenders, and speedier exoneration of innocent suspects.**
  - **The prevention of potentially large numbers of future crimes by supporting the identification and conviction in court of prolific offenders.**
  - **Reductions in investigation times allowing the police to move on to other cases and solve more crimes."**

Digital Forensics Professions

- Within the area of Digital Forensics there are a selection of specific roles that could become your area of expertise:
  - **Data Recovery** – Recovering data from damaged devices (CCTV, HDD, Memory cards)
  - **E-Discovery** – Based on the EDRM (Electronical Discovery Reference Model)
  - **Mobile Forensics** – Mobile device specific such as Android or Apple phones & tablets
  - **Network/Cloud Forensics** – Network devices, internet investigations, cloud providers
  - **Malware Forensics** – Malicious software such as viruses, rootkits, trojans, worms
  - **IoT Forensics** – IoT devices such as amazon Alexa or Samsung smart things

Typical Starting Jobs For These Areas

- Most people in forensics start as an **Analyst** or **Technician**. 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** (Bedfordshire is the closest to us) (link) (iCait, CCIT, DFIT)

- 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!)

Advice for Getting Starting

Advice on Education

- Typically a technical honours degree:
  - Digital forensics & information security
  - Cyber security
  - Computer Science
  - Networking
  - Investigation studies
  - Criminology

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

- Additionally:
  - GCSEs (or equivalents) Computing + Maths
  - A levels (or equivalents) Computing + Maths

Advice Continued…

- Fundamentals are key to your success

- Start in one place and build up you knowledge before moving on (start in **windows forensics**, then move to other **operating systems** only when you have a good level of **experience**)

- Depending on the employer, you will need to pass some form of security check (baseline, SC, CTC, DV). Information is linked here: Link

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"*

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 if remote collections are not an option (can include outside of the UK)
- Manage your own time
  - (You might be involved in different cases at any given time)
- Interact with clients or law enforcement directly

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/regulations
  - (27001, 17025, ACPO)
- Not be afraid of command lines
  - (CMD, PowerShell, Terminal)
- 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 Prefetch Files

a.r.u.

What is an Artefact?

- "*Every contact **leaves a trace***."
  - Dr Edmond Locard

- Artefacts are something that have been **left behind** that could contain information of a an event/person from the **past**.
  - In digital forensics, we know these as: "**Historical Artefacts**"

- Based on these findings they could help us learn something about our future too! (or the person we are investigating)

DEMO - Prefetch

- Prefetch files are created by the windows operating system whenever an application is run from a specific location for the first time. Prefetch files are used to speed up the application start-up process.
    - (so it can start faster the next time its loaded)

- Analysis of prefetch files reveal evidence of **program execution** for a particular user or from a particular location.

- Prefetch entries may still remain even after the program has been **deleted or un-installed.**

- Location WinXP/7/8/10:
    - **C:\Windows\Prefetch**
    - If you want to learn more check out the SANS cheat sheets later on!

Demo removed due to space issues

Checkout the YouTube video for it ☺

Home Lab Setup

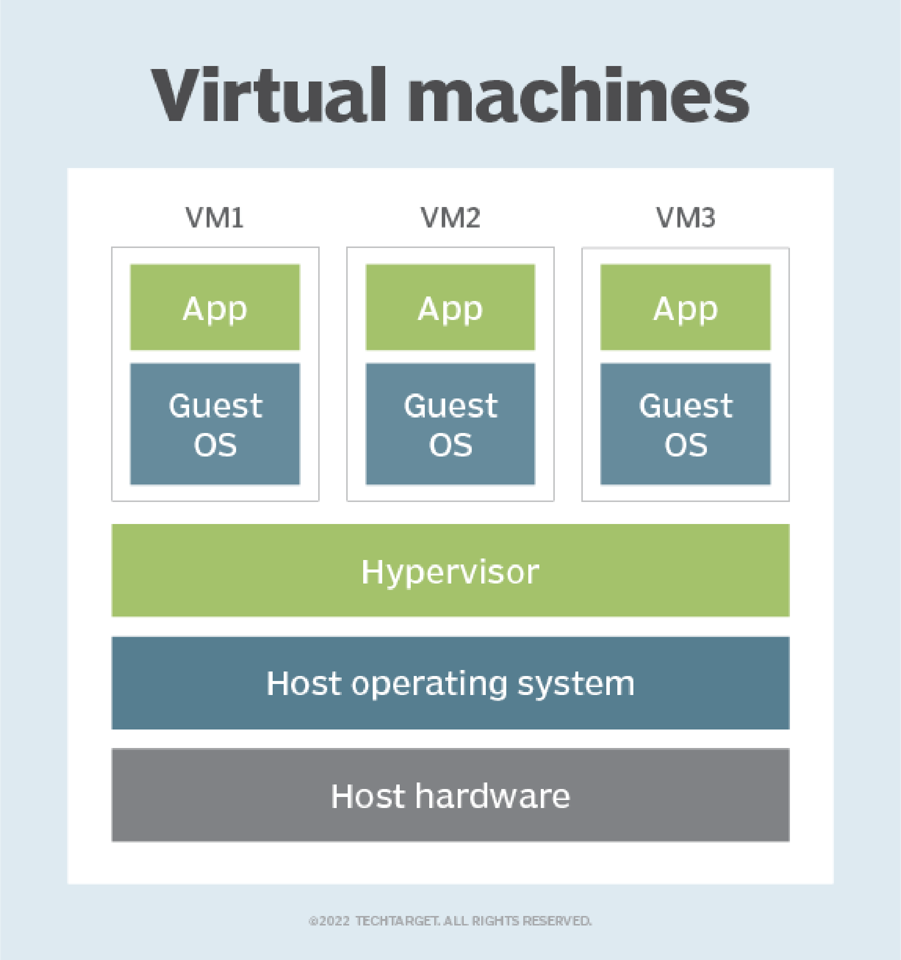
Why Build a Home Lab?

- 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)
- A Raspberry Pi, may also be an option if you happen to have the latest models with enough RAM
- 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
  - 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

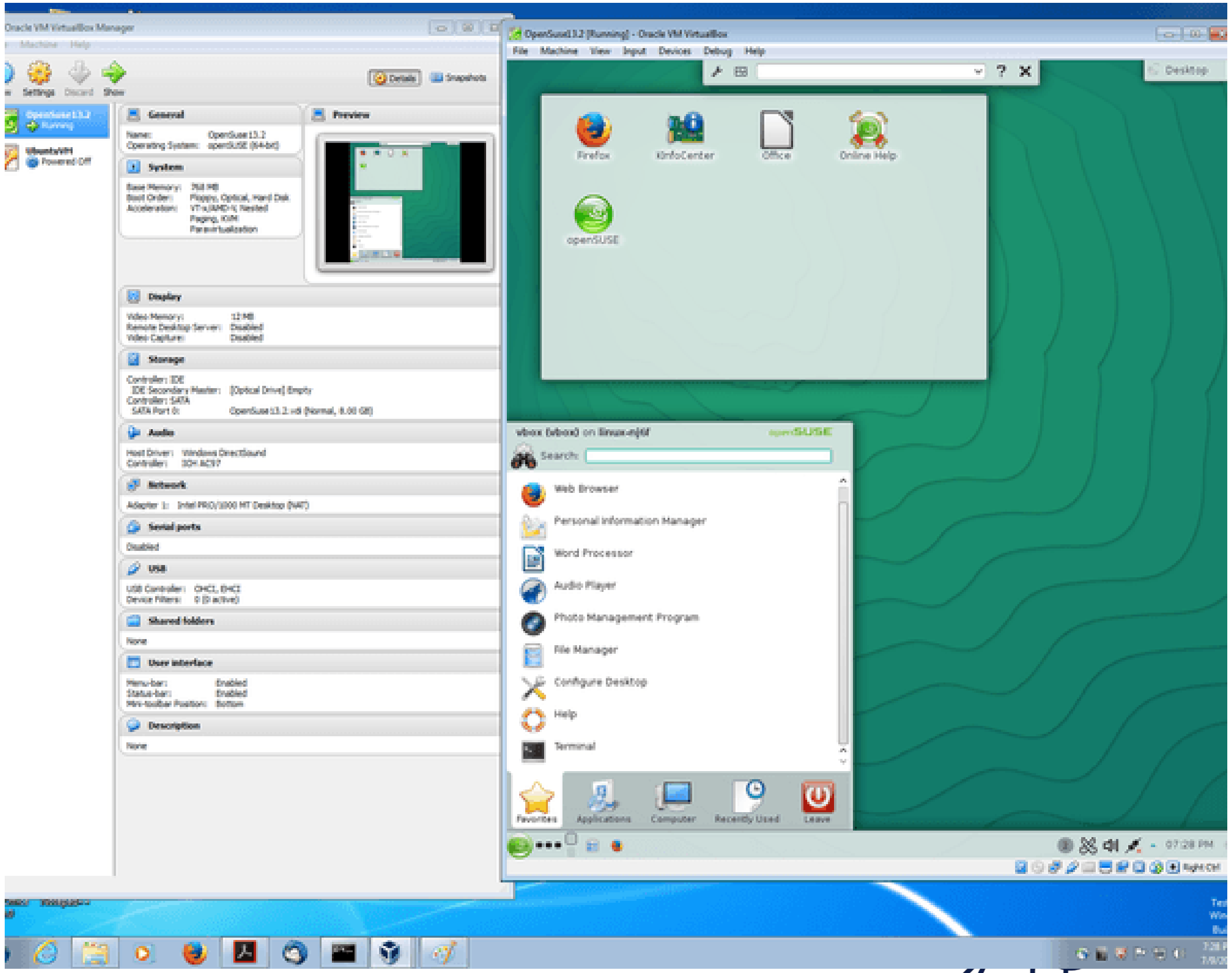


Free Tools for Different Roles

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

OpenSuse13.2 Running

UbuntuVM Powered Off

General

Name: OpenSuse 13.2
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

OpenSuse13.2 [Running] - Oracle VM VirtualBox

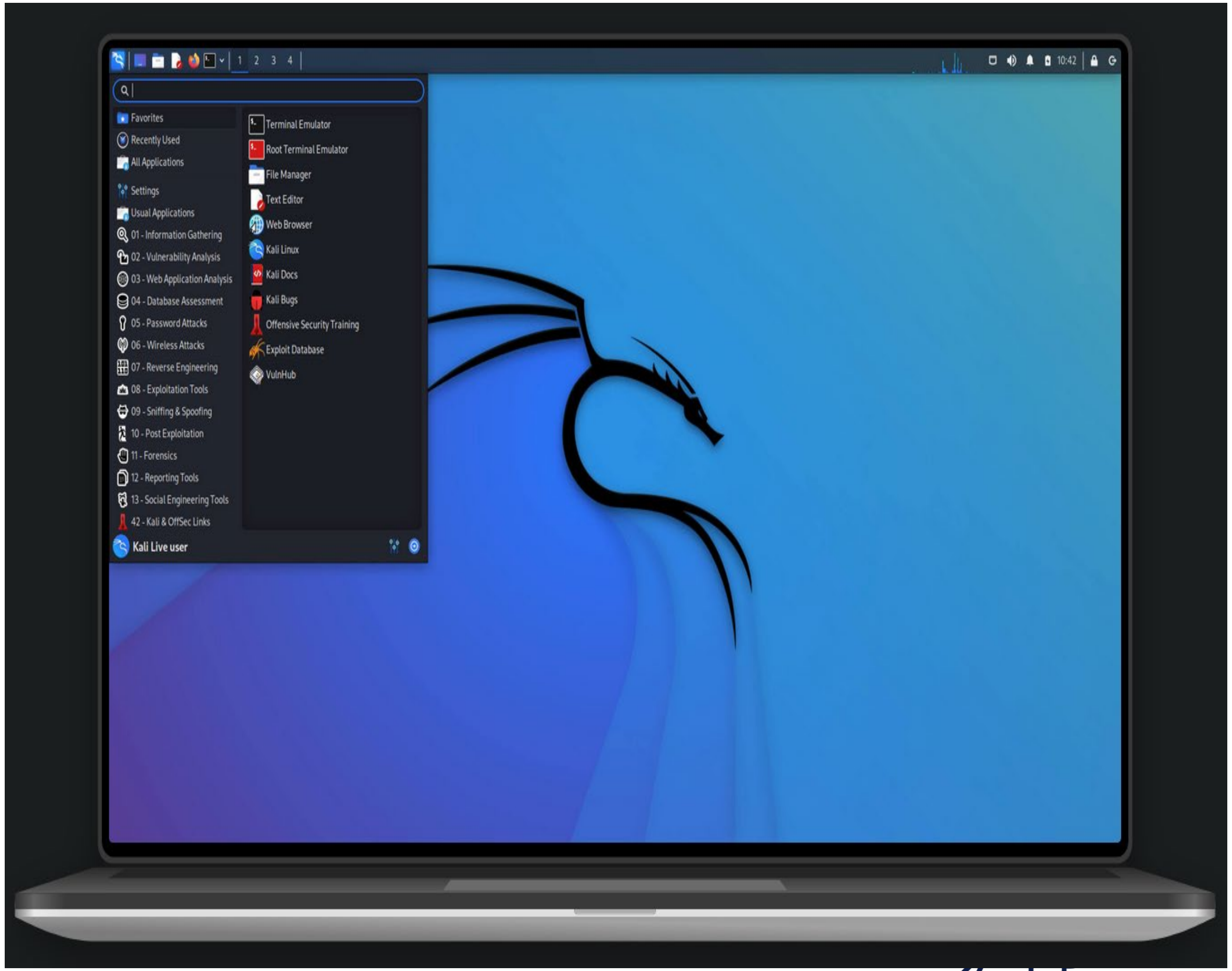
vbox (vbox) on linux-mj6f

a.r.u.

Imaging Software

- Kali is an opensource cyber security operating system. It can be used for penetration testing, Wi-Fi hacking or digital forensics etc
- The OS is Linux based
- This OS contains software such as:
    - Guymager, which allows imaging of computer devices
    - Range of popular Hex editors

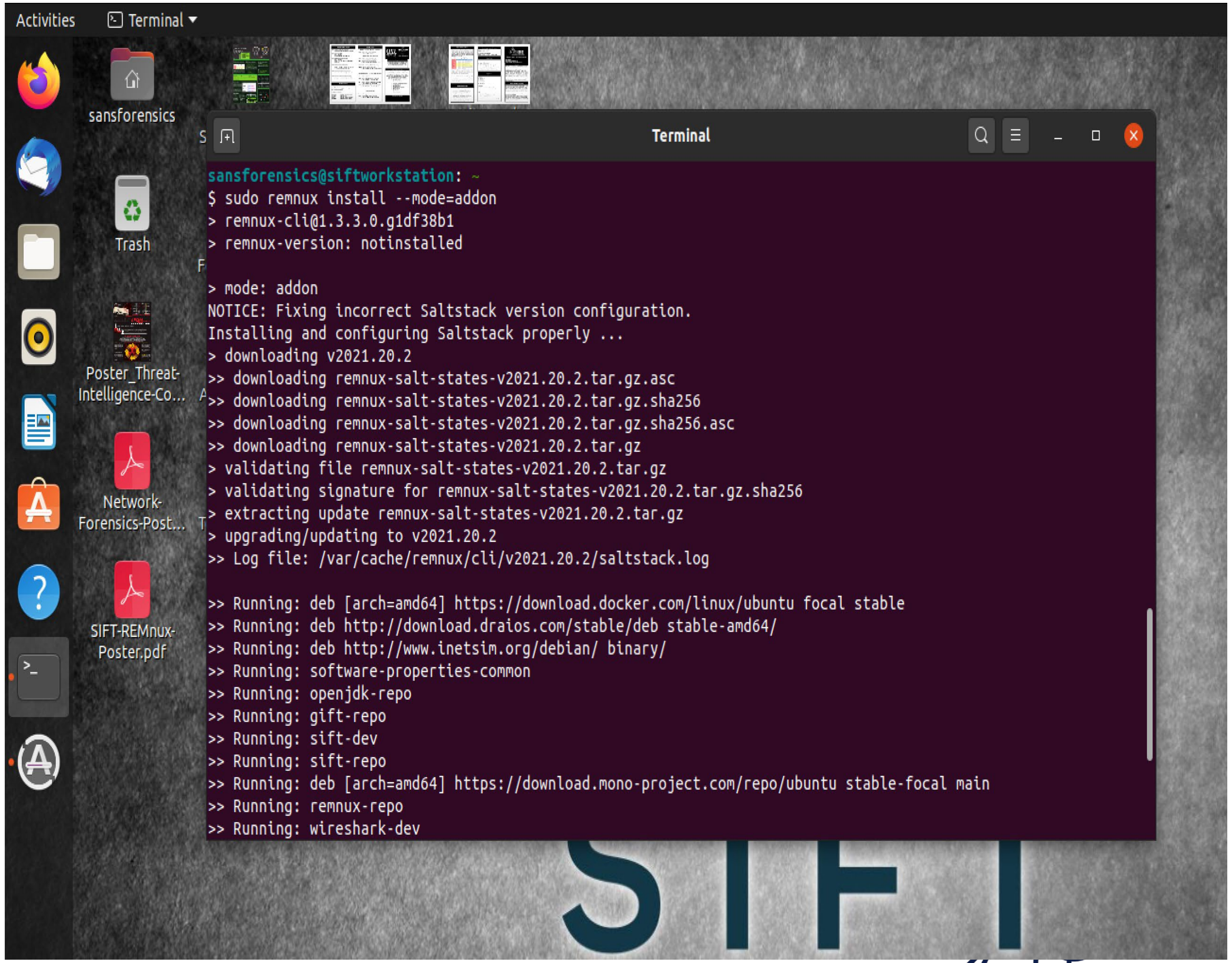
Image taken from Kali.org Link



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



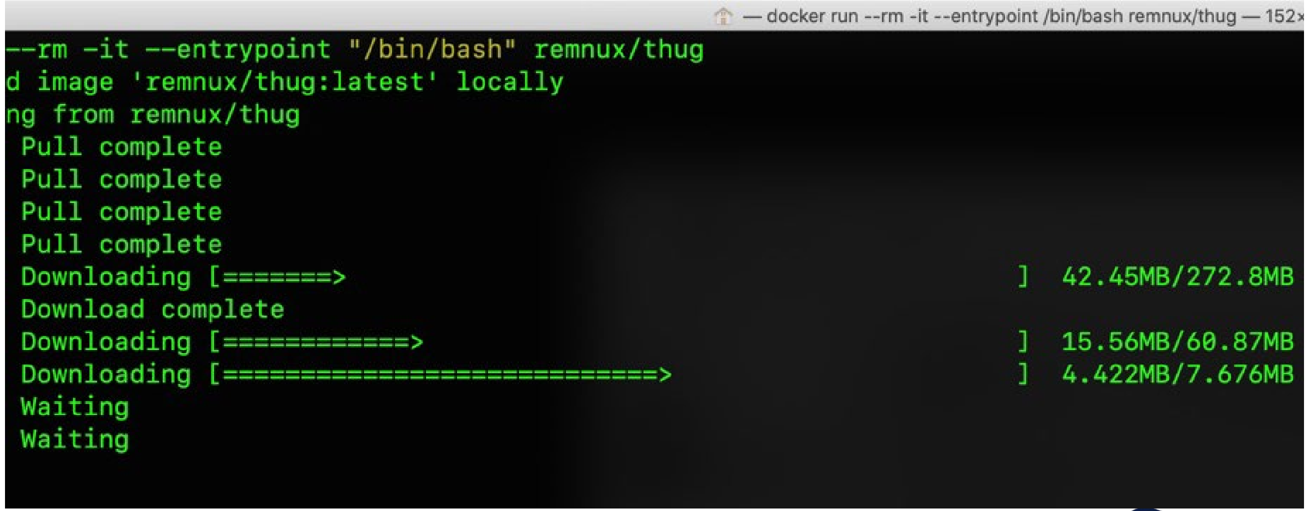
```
sansforensics@siftworkstation: ~
$ sudo remnux install --mode=addon
> remnux-cli@1.3.3.0.g1df38b1
> remnux-version: notinstalled

> 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]()

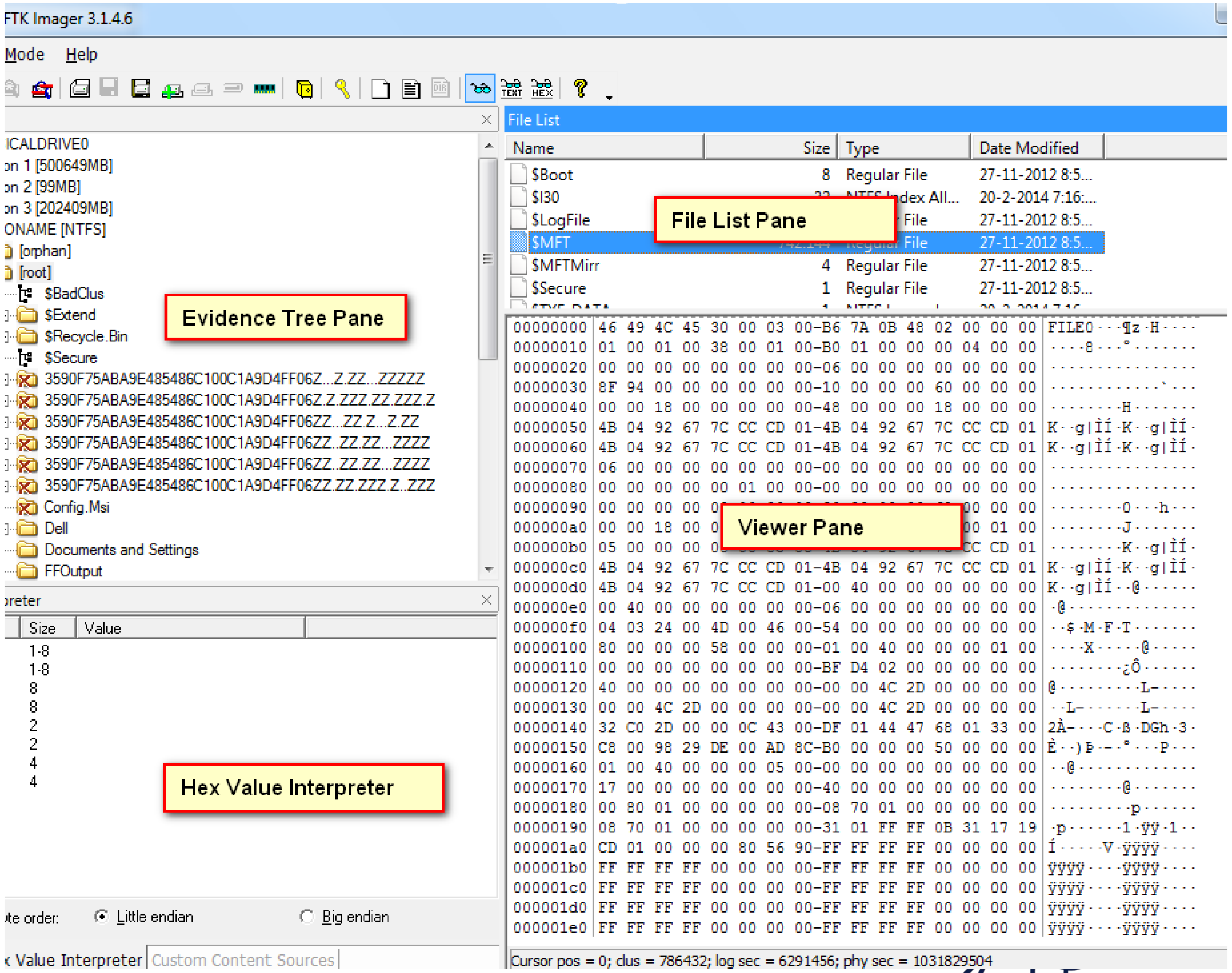

— docker run --rm -it --entrypoint /bin/bash remnux/thug — 152×

```
--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
```

FTK Imager

- This software allows you to copy all addressable data from a device that is connected to your computer
- It will then put this data into an evidence file (such as E01), so it is stored safely
- This can then safely be searched for potentially relevant data

Image taken from eForeniscs Link



ICALDRIVE0
on 1 [500649MB]
on 2 [99MB]
on 3 [202409MB]
ONAME [NTFS]
[orphan]
[root]
$BadClus
$Extend
$Recycle.Bin
$Secure
3590F75ABA9E485486C100C1A9D4FF06Z...Z.ZZ...ZZZZZ
3590F75ABA9E485486C100C1A9D4FF06Z.Z.ZZZ.ZZ.ZZZ.Z
3590F75ABA9E485486C100C1A9D4FF06ZZ...ZZ.Z...Z.ZZ
3590F75ABA9E485486C100C1A9D4FF06ZZ...ZZ.ZZ...ZZZZ
3590F75ABA9E485486C100C1A9D4FF06ZZ...ZZ.ZZ...ZZZZ
3590F75ABA9E485486C100C1A9D4FF06ZZ.ZZ.ZZZ.Z..ZZZ
Config.Msi
Dell
Documents and Settings
FFOutput

Name	Size	Type	Date Modified
$Boot	8	Regular File	27-11-2012 8:5...
$I30	32	NTFS Index All...	20-2-2014 7:16:...
$LogFile		File	27-11-2012 8:5...
$MFT	742.144	Regular File	27-11-2012 8:5...
$MFTMirr	4	Regular File	27-11-2012 8:5...
$Secure	1	Regular File	27-11-2012 8:5...

Size	Value
1-8	
1-8	
8	
8	
2	
2	
4	
4	

te order: ● Little endian ○ Big endian

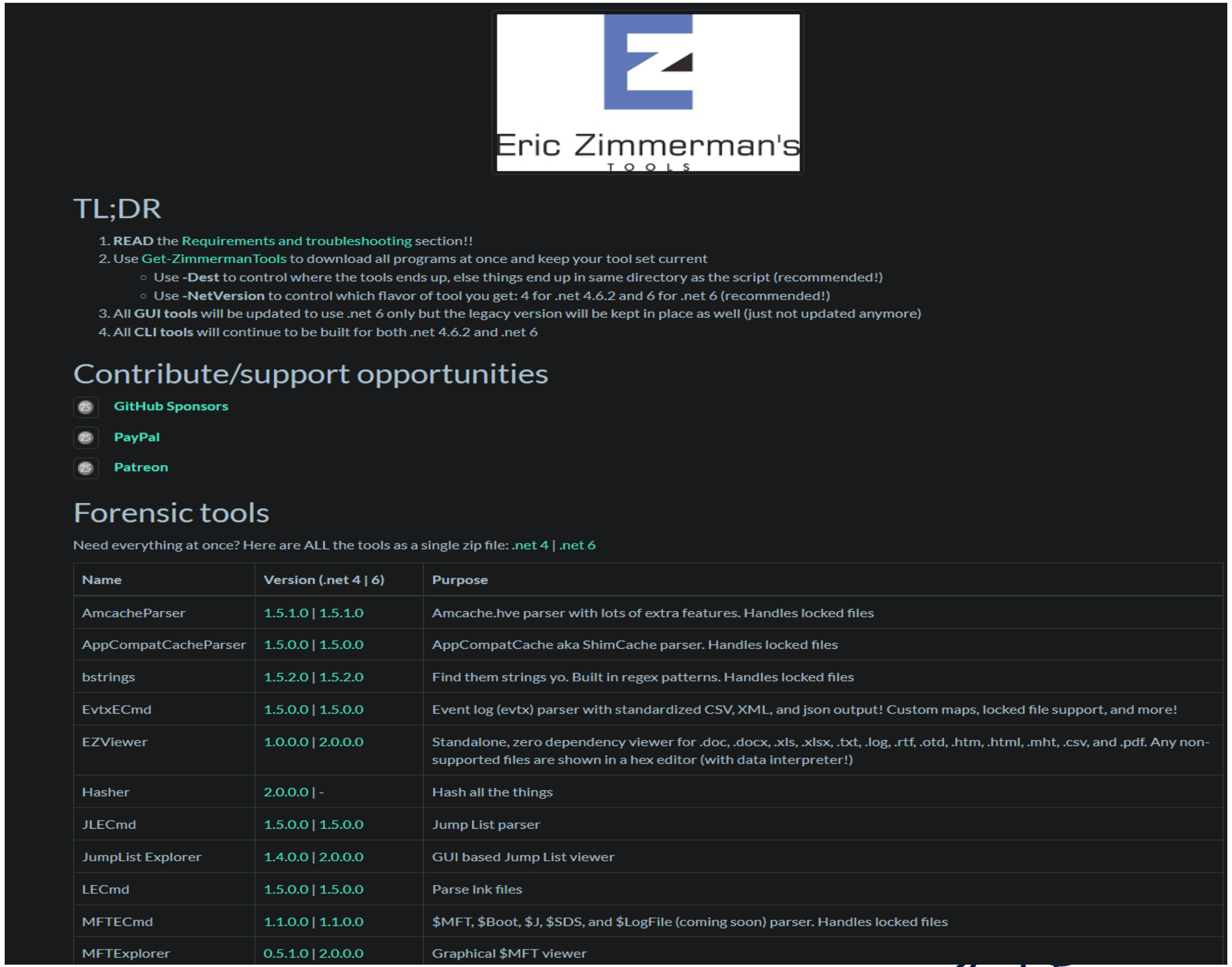
```
00000000 46 49 4C 45 30 00 03 00-B6 7A 0B 48 02 00 00 00 FILE0···¶z·H····
00000010 01 00 01 00 38 00 01 00-B0 01 00 00 00 04 00 00 ····8···°·······
00000020 00 00 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ················
00000030 8F 94 00 00 00 00 00 00-10 00 00 00 60 00 00 00 ············`···
00000040 00 00 18 00 00 00 00 00-48 00 00 00 18 00 00 00 ········H·······
00000050 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000060 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
00000070 06 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00000080 00 00 00 00 00 01 00 00-00 00 00 00 00 00 00 00 ················
00000090 00 00 00 00 0                          00 00 00 ········0···h···
000000a0 00 00 18 00 0                          00 01 00 ········J·······
000000b0 05 00 00 00 0                          CC CD 01 ········K··g|ÌÍ·
000000c0 4B 04 92 67 7C CC CD 01-4B 04 92 67 7C CC CD 01 K··g|ÌÍ·K··g|ÌÍ·
000000d0 4B 04 92 67 7C CC CD 01-00 40 00 00 00 00 00 00 K··g|ÌÍ··@······
000000e0 00 40 00 00 00 00 00 00-06 00 00 00 00 00 00 00 ·@··············
000000f0 04 03 24 00 4D 00 46 00-54 00 00 00 00 00 00 00 ··$·M·F·T·······
00000100 80 00 00 00 58 00 00 00-01 00 40 00 00 00 01 00 ····X·····@·····
00000110 00 00 00 00 00 00 00 00-BF D4 02 00 00 00 00 00 ········¿Ô······
00000120 40 00 00 00 00 00 00 00-00 00 4C 2D 00 00 00 00 @·········L-····
00000130 00 00 4C 2D 00 00 00 00-00 00 4C 2D 00 00 00 00 ··L-······L-····
00000140 32 C0 2D 00 00 0C 43 00-DF 01 44 47 68 01 33 00 2À-···C·ß·DGh·3·
00000150 C8 00 98 29 DE 00 AD 8C-B0 00 00 00 50 00 00 00 È··)Þ·-·°···P···
00000160 01 00 40 00 00 00 05 00-00 00 00 00 00 00 00 00 ··@·············
00000170 17 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ········@·······
00000180 00 80 01 00 00 00 00 00-08 70 01 00 00 00 00 00 ·········p······
00000190 08 70 01 00 00 00 00 00-31 01 FF FF 0B 31 17 19 ·p······1·ÿÿ·1··
000001a0 CD 01 00 00 00 80 56 90-FF FF FF FF 00 00 00 00 Í·····V·ÿÿÿÿ····
000001b0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001c0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001d0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
000001e0 FF FF FF FF 00 00 00 00-FF FF FF FF 00 00 00 00 ÿÿÿÿ····ÿÿÿÿ····
```

Cursor pos = 0; clus = 786432; log sec = 6291456; phy sec = 1031829504

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 which was in the demo)
- 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

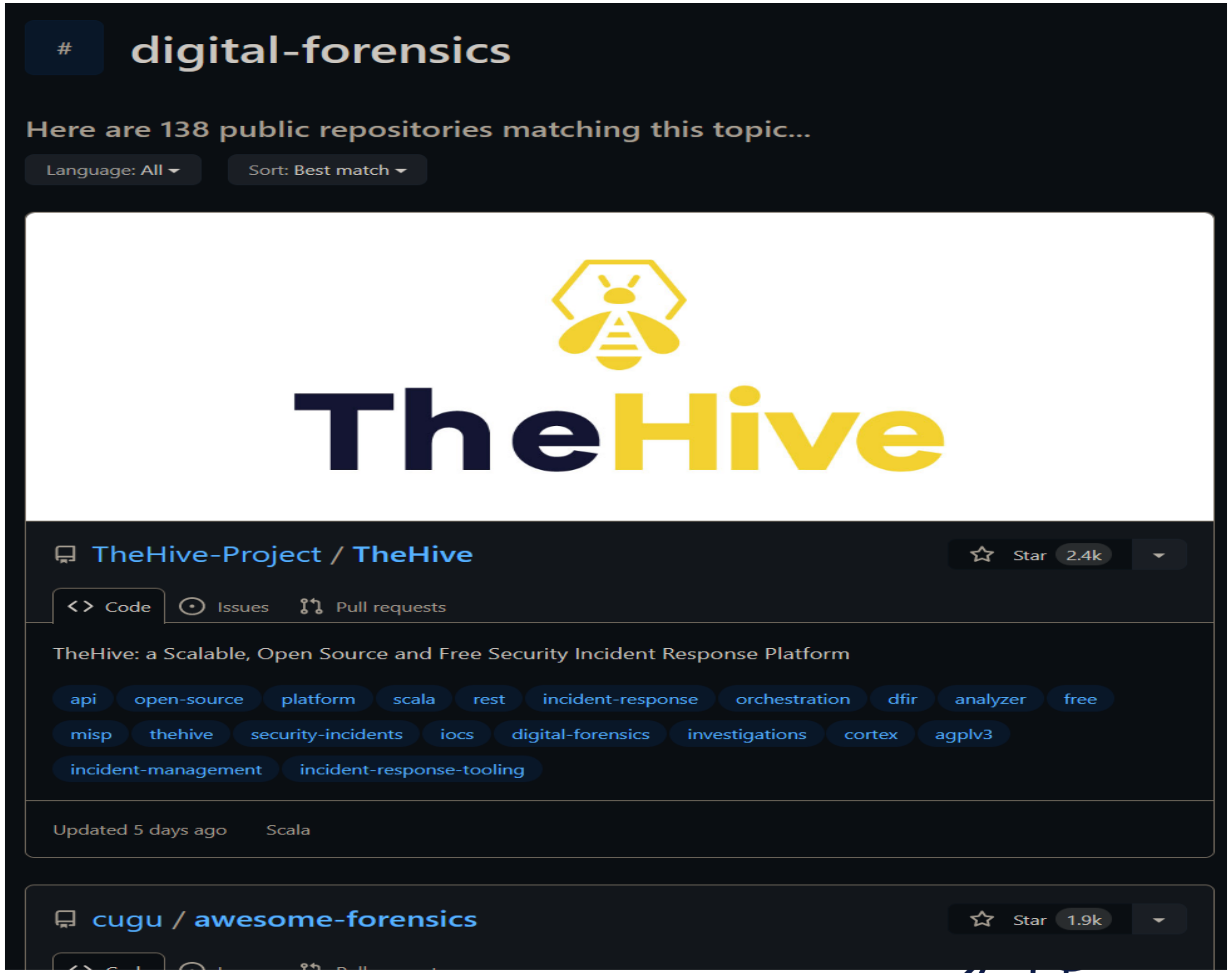
Need everything at once? Here are ALL the tools as a single zip file: .net 4 | .net 6

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

GitHub Tools

- GitHub is a place where you can download software from various creators around the world
- There is a specific section that covers digital forensics and incident response
- Currently has 138 repositories of data to check out!

Image taken from GitHub Link



digital-forensics

Here are 138 public repositories matching this topic...

TheHive-Project / TheHive

TheHive: a Scalable, Open Source and Free Security Incident Response Platform

Updated 5 days ago Scala

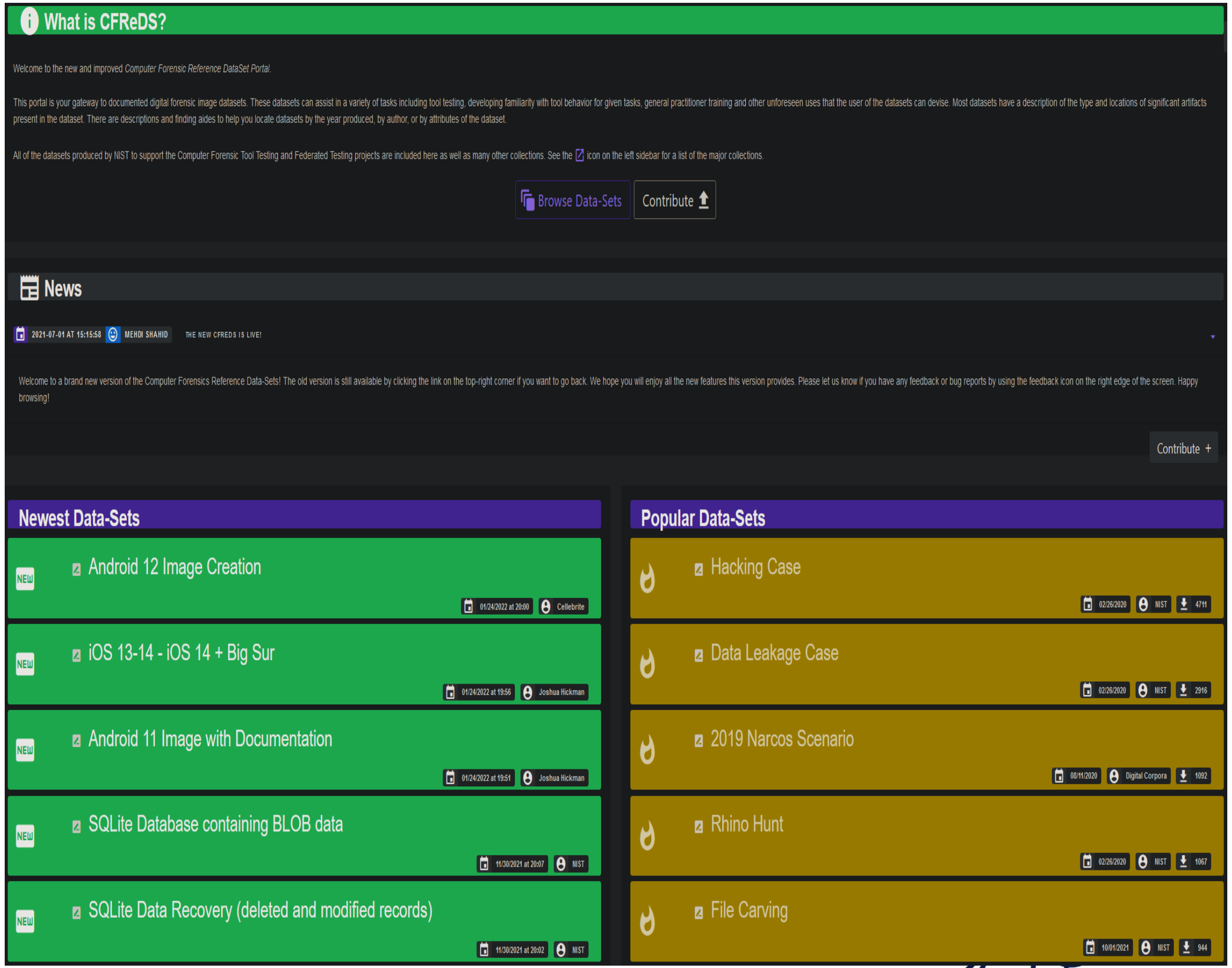
cugu / awesome-forensics

List of Evidence Samples

NIST Computer Forensic Reference DataSet Portal

- This portal is your gateway to documented digital forensic image datasets.
- These datasets can assist in a variety of tasks including tool testing, developing familiarity with tool behaviour for given tasks and general practitioner training
- Most datasets have a description of the type and locations of significant artifacts present in the dataset.
- There are descriptions and finding aides to help you locate datasets by the year produced, by author, or by attributes of the dataset.

Image taken from nist.gov Link



What is CFReDS?

Welcome to the new and improved *Computer Forensic Reference DataSet Portal*.

This portal is your gateway to documented digital forensic image datasets. These datasets can assist in a variety of tasks including tool testing, developing familiarity with tool behavior for given tasks, general practitioner training and other unforeseen uses that the user of the datasets can devise. Most datasets have a description of the type and locations of significant artifacts present in the dataset. There are descriptions and finding aides to help you locate datasets by the year produced, by author, or by attributes of the dataset.

All of the datasets produced by NIST to support the Computer Forensic Tool Testing and Federated Testing projects are included here as well as many other collections. See the icon on the left sidebar for a list of the major collections.

News

2021-07-01 AT 15:15:58 MEHDI SHAHID THE NEW CFREDS IS LIVE!

Welcome to a brand new version of the Computer Forensics Reference Data-Sets! The old version is still available by clicking the link on the top-right corner if you want to go back. We hope you will enjoy all the new features this version provides. Please let us know if you have any feedback or bug reports by using the feedback icon on the right edge of the screen. Happy browsing!

Newest Data-Sets

- NEW Android 12 Image Creation — 01/24/2022 at 20:00 — Cellebrite
- NEW iOS 13-14 - iOS 14 + Big Sur — 01/24/2022 at 19:56 — Joshua Hickman
- NEW Android 11 Image with Documentation — 01/24/2022 at 19:51 — Joshua Hickman
- NEW SQLite Database containing BLOB data — 11/30/2021 at 20:07 — NIST
- NEW SQLite Data Recovery (deleted and modified records) — 11/30/2021 at 20:02 — NIST

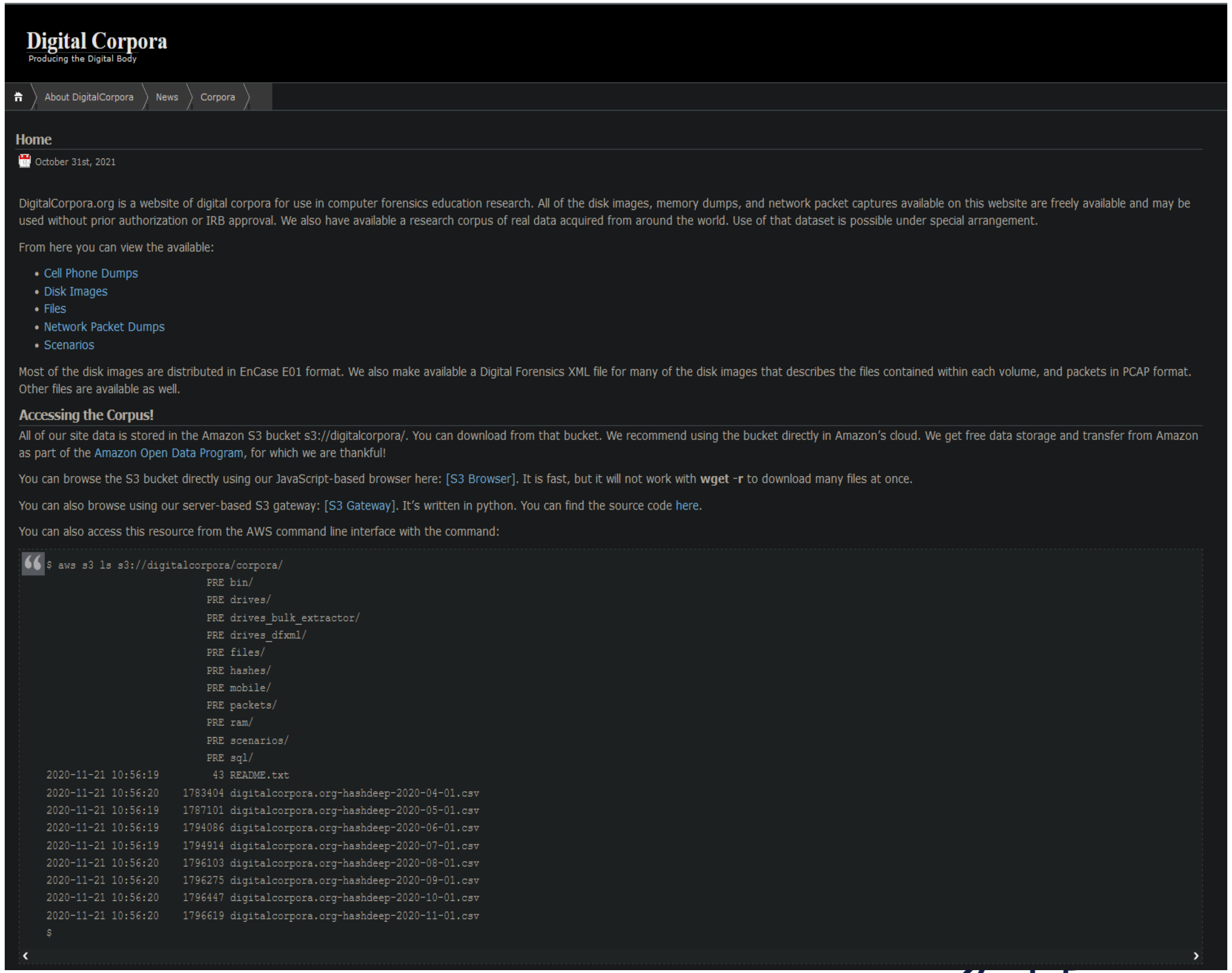
Popular Data-Sets

- Hacking Case — 02/26/2020 — NIST — 4711
- Data Leakage Case — 02/26/2020 — NIST — 2916
- 2019 Narcos Scenario — 08/11/2020 — Digital Corpora — 1092
- Rhino Hunt — 02/26/2020 — NIST — 1067
- File Carving — 10/01/2021 — NIST — 944

Digital Corpora

- DigitalCorpora.org is a website for use in computer forensics education research
- All of the disk images, memory dumps, and network packet captures on this website are freely available
- They also have a research corpus of real data acquired from around the world. Use of that dataset is possible under special arrangement

Image taken from digitalcopora.org
Link



Home

October 31st, 2021

DigitalCorpora.org is a website of digital corpora for use in computer forensics education research. All of the disk images, memory dumps, and network packet captures available on this website are freely available and may be used without prior authorization or IRB approval. We also have available a research corpus of real data acquired from around the world. Use of that dataset is possible under special arrangement.

From here you can view the available:

- Cell Phone Dumps
- Disk Images
- Files
- Network Packet Dumps
- Scenarios

Most of the disk images are distributed in EnCase E01 format. We also make available a Digital Forensics XML file for many of the disk images that describes the files contained within each volume, and packets in PCAP format. Other files are available as well.

Accessing the Corpus!

All of our site data is stored in the Amazon S3 bucket s3://digitalcorpora/. You can download from that bucket. We recommend using the bucket directly in Amazon's cloud. We get free data storage and transfer from Amazon as part of the Amazon Open Data Program, for which we are thankful!

You can browse the S3 bucket directly using our JavaScript-based browser here: [S3 Browser]. It is fast, but it will not work with **wget -r** to download many files at once.

You can also browse using our server-based S3 gateway: [S3 Gateway]. It's written in python. You can find the source code here.

You can also access this resource from the AWS command line interface with the command:

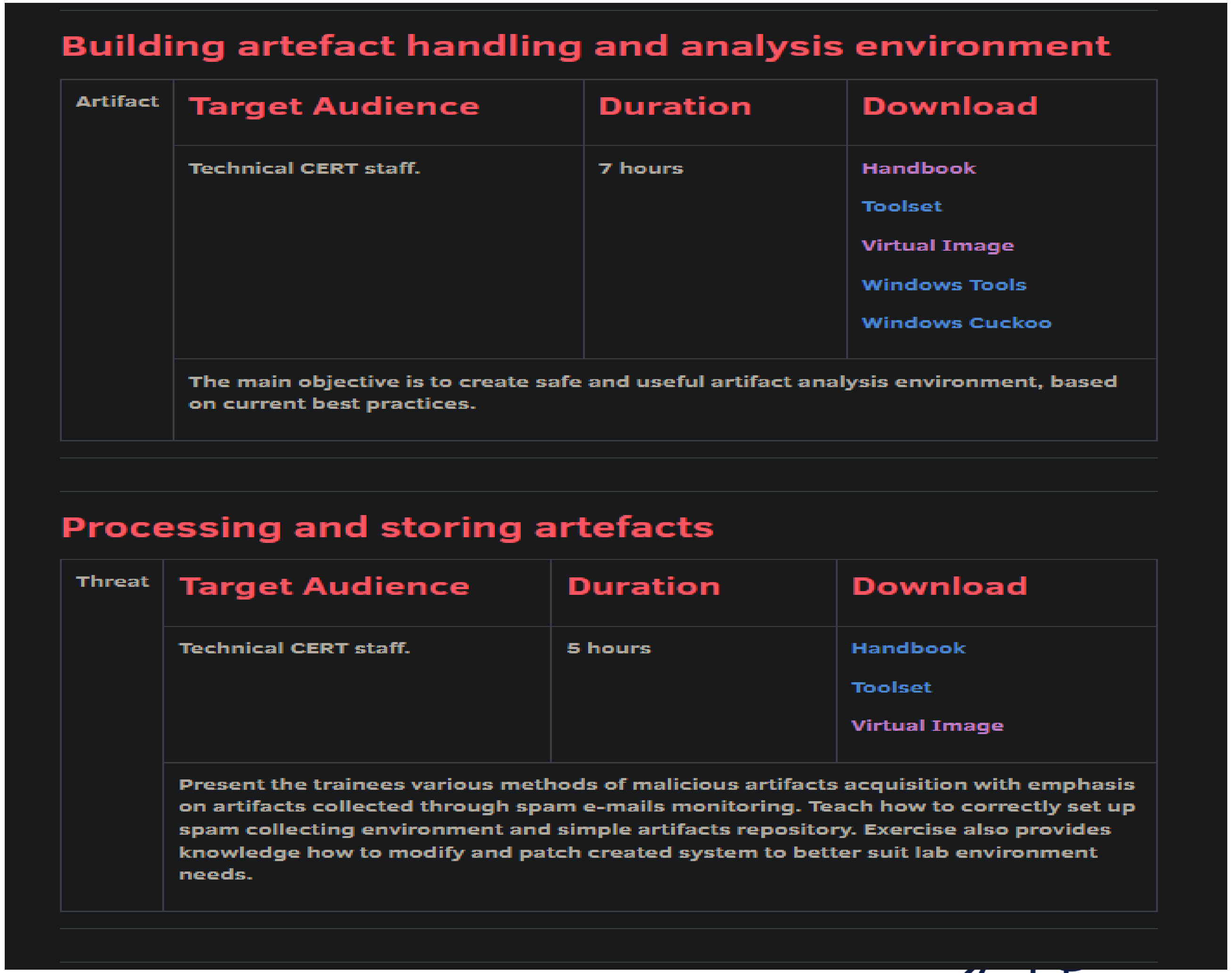
```
$ aws s3 ls s3://digitalcorpora/corpora/
                           PRE bin/
                           PRE drives/
                           PRE drives_bulk_extractor/
                           PRE drives_dfxml/
                           PRE files/
                           PRE hashes/
                           PRE mobile/
                           PRE packets/
                           PRE ram/
                           PRE scenarios/
                           PRE sql/
2020-11-21 10:56:19         43 README.txt
2020-11-21 10:56:20    1783404 digitalcorpora.org-hashdeep-2020-04-01.csv
2020-11-21 10:56:19    1787101 digitalcorpora.org-hashdeep-2020-05-01.csv
2020-11-21 10:56:19    1794086 digitalcorpora.org-hashdeep-2020-06-01.csv
2020-11-21 10:56:19    1794914 digitalcorpora.org-hashdeep-2020-07-01.csv
2020-11-21 10:56:20    1796103 digitalcorpora.org-hashdeep-2020-08-01.csv
2020-11-21 10:56:20    1796275 digitalcorpora.org-hashdeep-2020-09-01.csv
2020-11-21 10:56:20    1796447 digitalcorpora.org-hashdeep-2020-10-01.csv
2020-11-21 10:56:20    1796619 digitalcorpora.org-hashdeep-2020-11-01.csv
$
```

Resources for Learning

ENISA

- The European union agency for cybersecurity is a great resource for learning digital forensics
- The guides show what tools, prebuild virtual images and evidence files you can use
- The time commitment is also displayed (likely higher on your first attempt)

Image taken from enisa.eu Link



Building artefact handling and analysis environment

Artifact	Target Audience	Duration	Download
	Technical CERT staff.	7 hours	Handbook Toolset Virtual Image Windows Tools Windows Cuckoo
	The main objective is to create safe and useful artifact analysis environment, based on current best practices.		

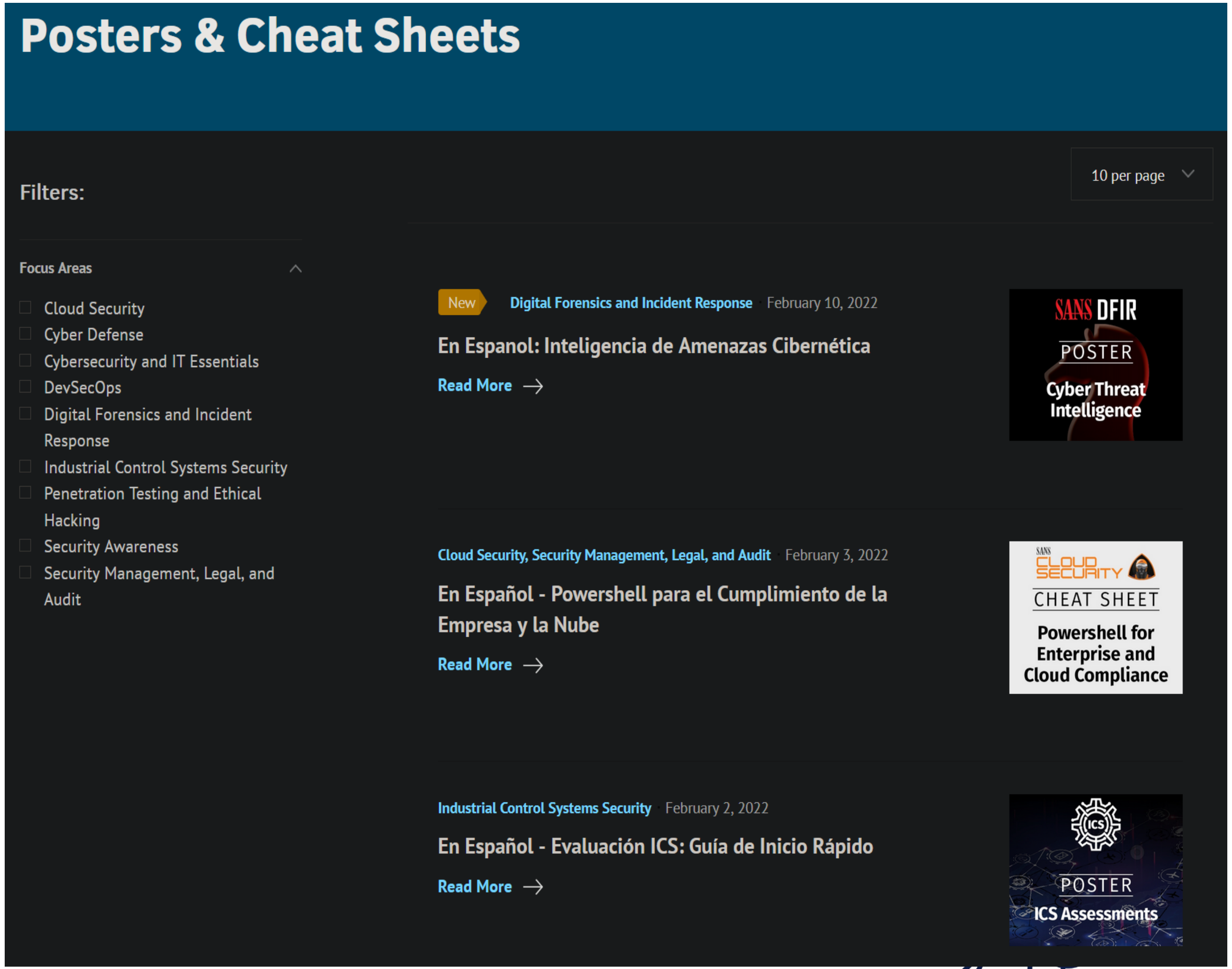
Processing and storing artefacts

Threat	Target Audience	Duration	Download
	Technical CERT staff.	5 hours	Handbook Toolset Virtual Image
	Present the trainees various methods of malicious artifacts acquisition with emphasis on artifacts collected through spam e-mails monitoring. Teach how to correctly set up spam collecting environment and simple artifacts repository. Exercise also provides knowledge how to modify and patch created system to better suit lab environment needs.		

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



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: Guía de Inicio Rápido

Read More →

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

Conclusion

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

a.r.u.

Any questions?

- **Andrew Moore - PGCE, FHEA, BSc, CSIR, CFIP**
- Lecturer Practitioner / Digital Forensics Consultant
- Cambridge, UK

- Andrew.Moore@aru.ac.uk

a.r.u.