OSDFCon 2017

# RAPID INCIDENT RESPONSE

Asif Matadar

@d1r4c

STROZ FRIEDBERG
an Aon company

# #whoami

- Director of Incident Response for Stroz Friedberg in the U.K.

- Lead complex incidents around the world:

  - Advanced Targeted Attacks
  - State Affiliated
  - Data Breaches
  - Industrial Espionage

- Over 6 years' experience working in incident response and penetration testing on infrastructure, web, and mobile applications.

- Presented at security conferences in the U.K. and the U.S.

# Rapid Incident Response

- During large-scale incident response investigations we often come across situations where we undertake repetitive tasks so that includes Triage and Memory Analysis.

- This talk will walk-through different techniques that are required to provide these results for Windows and *nix environments and the importance of Triage and Memory Analysis during an investigation. How they are vital components that are often neglected during incident response investigations.

# Rapid Incident Response

- **Agenda**
  - Collaboration
  - Live Triage Analysis
    - Windows environments
    - *nix environments
  - Memory Analysis
    - Optimise Memory Analysis

STROZ FRIEDBERG
an Aon company

# Collaboration

# Collaboration

- Large-scale incident response investigations pose many obstacles:
  - Geographical limitations
  - Time zone issues
  - Which Investigator did what/when?
    - Contemporaneous Notes
  - Status of different work streams and sharing findings
  - Client or Management pressures
  - Lack of communication between personnel
  - Operating multiple incidents

STROZ FRIEDBERG
an Aon company

# Collaboration – TheHive

- A collaborative tool called “TheHive” is a great platform that can aid Investigators:
  - You can start correlating findings in real time
  - Technical Leads can track pending tasks
  - Everyone can keep track of who is doing what
  - Create case templates
    - APT
    - Ransomware
    - Data breach
  - MISP can be fed into the platform or query other platforms like YETI, VirusTotal and DomainTools to name a few
  - TheHive4py - Python API client to send alerts and emails for further action

# Collaboration – TheHive

*<DEMO>*

https://github.com/CERT-BDF/TheHive

STROZ FRIEDBERG
an Aon company

# Collaboration – Timesketch

- Timesketch is an open source tool for collaborative forensic timeline analysis.
  - Create Timeline from JSON/CSV file
  - Create Timeline from Plaso file
  - Enable Plaso upload via HTTP
  - Create Stories for correlation purposes
  - Create comments on specific findings

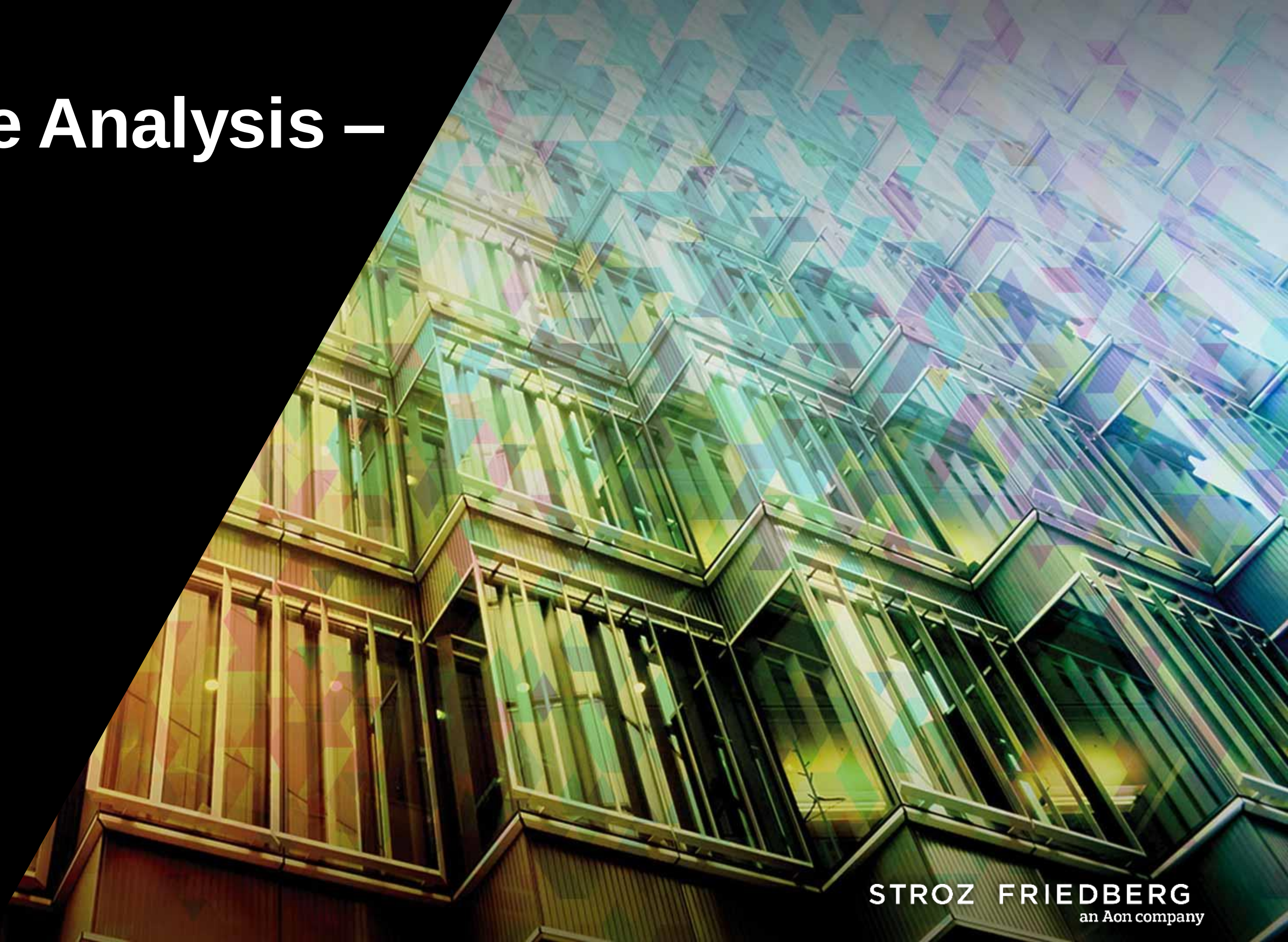
STROZ FRIEDBERG
an Aon company

# Collaboration – Timesketch

*<DEMO>*

https://github.com/google/timesketch

# Live Triage Analysis – Windows



STROZ FRIEDBERG
an Aon company

# Live Triage Analysis

- Live Triage Analysis is an essential component during incident response investigations.

- Quickly triage many systems in an efficient manner whilst looking for any Indicators of Compromise (IOC) or Tactics, Techniques and Procedures (TTP).

- Once triage analysis has taken place, one can embark on full forensic analysis if there are signs of intrusions.

# How will you deploy your tools?

- Can you utilise built-in Windows utilities to deploy your tools efficiently?
    - Modern Windows environments now have the ability to facilitate quick deployment of tools on many systems.
        - This is great from incident response perspective!
- What options are available?

STROZ FRIEDBERG
an Aon company

# How will you deploy your tools?

- **PowerShell DSC (Desired State Configuration)**
  - PowerShell DSC is a management platform in PowerShell that enables you to manage your IT and development infrastructure with configuration as code.
- **SCCM (System Centre Configuration Manager)**
  - SCCM is a software management suite provided by Microsoft that allows users to manage a large number of Windows based computers which features remote control, patch management, operating system deployment, and network protection.
- **GPO**
  - Group Policy is simply the easiest way to reach out and configure computer and user settings on networks based on Active Directory Domain Services (AD DS).
- **PowerShell and WMI**

# Live Triage Analysis – Windows

- Secure environments have restrictions in place to prevent certain services from being enabled.

- Depending on the environment you are in, you can leverage a number of methods to commence Live Triage Analysis:

  - PowerShell

  - WinRM

  - WMI

# Live Triage Analysis – CyLR

- The CyLR tool collects forensic artefacts from hosts with NTFS file systems quickly, securely and minimizes impact to the host.
  - Collected artefacts are stored in memory for optimisation
  - Windows API are not used for collecting the artefacts
  - Option to send triage data to server over SFTP tunnel for Host Analysis

# Live Triage Analysis – CyLR

*<DEMO>*

https://github.com/rough007/CyLR

STROZ FRIEDBERG
an Aon company

# Other notable projects

- PSHunt is a PowerShell Threat Hunting Module designed to scan remote endpoints* for indicators of compromise or survey them for more comprehensive information related to state of those systems (active processes, autostarts, configurations, and/or logs).

https://github.com/Infocyte/PSHunt

- Live Response Collection is an automated tool that collects volatile data from Windows, OSX, and *nix based operating systems.

https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip

STROZ FRIEDBERG
an Aon company

# Other notable projects

- Kansa is a modular incident response framework in PowerShell.

https://github.com/davehull/Kansa

- PowerForensics provides an all inclusive framework for hard drive forensic analysis.

https://github.com/Invoke-IR/PowerForensics

- PSRecon gathers data from a remote Windows host using PowerShell (v2 or later), organizes the data into folders, hashes all extracted data, sent to the security team for review.

https://github.com/gfoss/PSRecon

# Agentless PowerShell project

- NOAH is an agentless open source Incident Response framework based on PowerShell, called "No Agent Hunting" (NOAH).

```
C:\> .\NOAH.ps1 -Processor -Memory -InstalledPrograms -Netstat -AMCache -Prefetch
-EnableHash -HuntDescription “Triage Analysis - DESKTOP-3C0HA7E"
```

https://github.com/giMini/NOAH

# WMI projects

- CimSweep is an ICIM/WMI-based tools that enables the ability to perform incident response and hunting operations remotely across all versions of Windows.

https://github.com/PowerShellMafia/CimSweep

STROZ FRIEDBERG
an Aon company

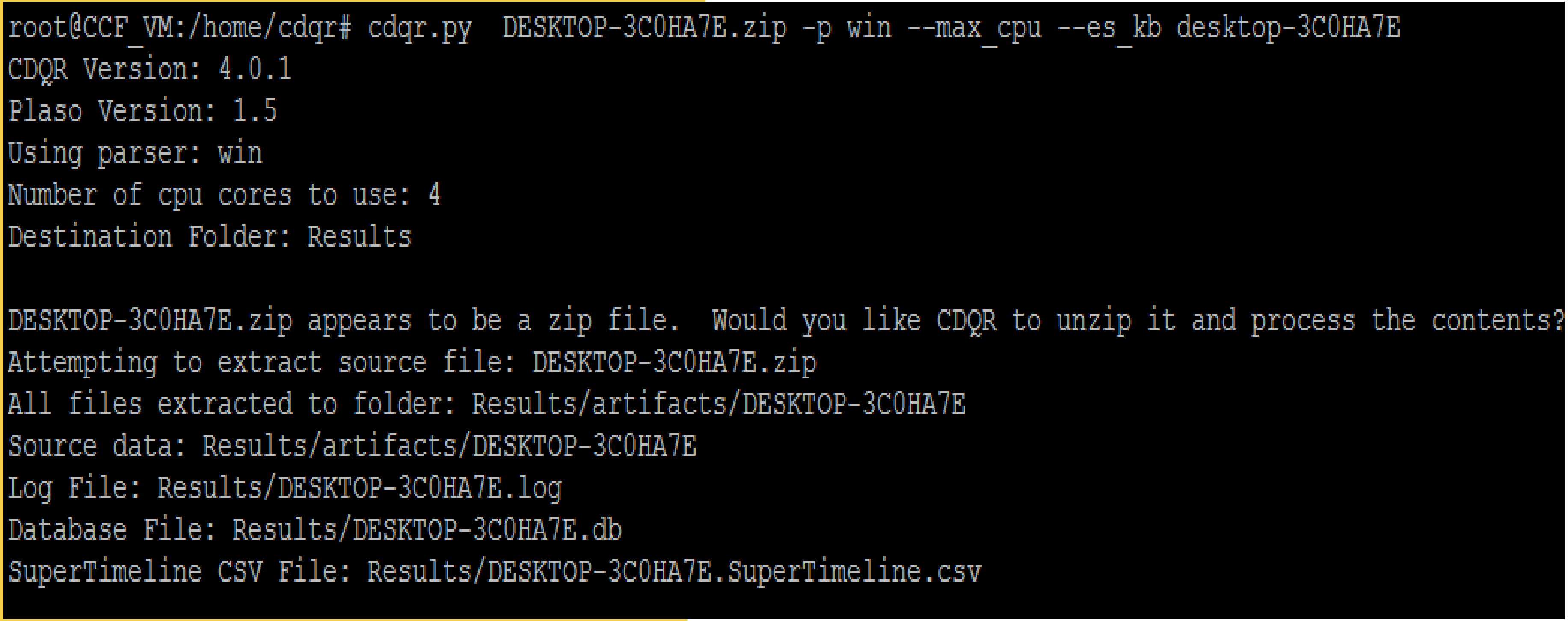
# Rapid Host Analysis – CDQR

- The Cold Disk Quick Response (CDQR) tool is a fast and easy to use forensic artefact parsing tool that works on disk images, mounted drives and extracted artefacts from Windows, Linux and macOS devices.
    - CyLR triage data can be utilised using CDQR
    - Plaso is used to parse disk images
    - Customised reports are created for Windows, Linux and macOS
    - Support for Timesketch and Kibana

https://github.com/rough007/CDQR

STROZ FRIEDBERG
an Aon company

# Rapid Host Analysis – CDQR



```
root@CCF_VM:/home/cdqr# cdqr.py  DESKTOP-3C0HA7E.zip -p win --max_cpu --es_kb desktop-3C0HA7E
CDQR Version: 4.0.1
Plaso Version: 1.5
Using parser: win
Number of cpu cores to use: 4
Destination Folder: Results

DESKTOP-3C0HA7E.zip appears to be a zip file.  Would you like CDQR to unzip it and process the contents?
Attempting to extract source file: DESKTOP-3C0HA7E.zip
All files extracted to folder: Results/artifacts/DESKTOP-3C0HA7E
Source data: Results/artifacts/DESKTOP-3C0HA7E
Log File: Results/DESKTOP-3C0HA7E.log
Database File: Results/DESKTOP-3C0HA7E.db
SuperTimeline CSV File: Results/DESKTOP-3C0HA7E.SuperTimeline.csv
```

STROZ FRIEDBERG
an Aon company

# Live Triage Analysis – *nix

# Live Triage Analysis – *nix

- Live Triage Analysis on *nix based systems is easier than most anticipate.
- SSH is the de-facto protocol to administer **MAJORITY** of *nix systems.
- On incident response investigations one can take advantage of SSH to triage systems rapidly.

STROZ FRIEDBERG
an Aon company

# *nix – SSH automation

- Run local triage scripts on *nix systems through Python or BASH:

```
# cat python_triage_script.py | ssh investigator@production.spock python -c
'''import sys;exec(sys.stdin.read())'''
```

```
# cat python_triage_script.py | ssh investigator@development.spock python -
```

```
# ssh investigator@cloud.spock "bash -s" < ./bash_triage_script.sh
```

STROZ FRIEDBERG
an Aon company

# *nix – SSH automation

- Python SSH module Paramiko is extremely useful for continuous monitoring of *nix based systems:

```
import paramiko
ssh=paramiko.SSHClient()
ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
ssh.connect('production.spock',username='investigator',password='<password_here>')
stdin,stdout,stderr = ssh.exec_command("ls -ltr /dev/shm/rootkit")
print stdout.readlines()
```

```
# python python-paramiko_triage_script.py

lrwxrwxrwx 1 webadmin 10513 25 Sep 19 15:34 /dev/shm/rootkit
```

# *nix – osquery

- osquery is an operating system instrumentation framework for Windows, OS X (macOS), Linux, and FreeBSD. The tool makes low-level operating system analytics and monitoring both performant and intuitive.
  - Queries can be fed into SIEM solution for analysis and collaboration
  - Integration with EDR products

# *nix – osquery

*<DEMO>*

https://osquery.readthedocs.io/en/stable/

STROZ FRIEDBERG
an Aon company

# *nix – Other notable projects

- Live Response Collection is an automated tool that collects volatile data from Windows, OSX, and *nix based operating systems.

https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip

- MIG: Mozilla InvestiGator allows investigators to obtain information from large numbers of systems in parallel, thus accelerating investigation of incidents and day-to-day operations security.

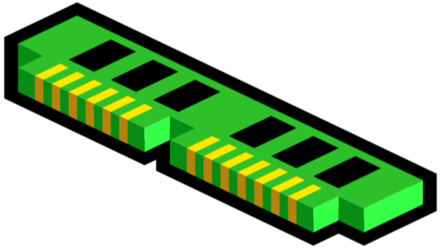
https://github.com/mozilla/mig

# Memory Analysis

STROZ FRIEDBERG
an Aon company

# Memory Analysis

- Memory Analysis is a vital component during incident response investigations, especially when dealing with advanced threat actors.
- Extraction of artefacts can provide unique visibility into running systems.
- During large-scale incident response investigations Memory Analysis can provide a level of insight that is quite unique and unparalleled.



STROZ FRIEDBERG
an Aon company

# Optimise Memory Analysis

- Optimisation during Memory Analysis is important, especially when dealing with large amounts of memory dumps.

- A number of techniques can be used to undertake that work within Volatility:

```
# cat volatilityrc
[DEFAULT]
LOCATION=file:///memdump.mem
PROFILE=Win7SP0x64
KDBG=0x80644be
DTB=0x00319000
```

# Optimise Memory Analysis

- Memory Analysis can be taken further if you utilise:
  - SSD
  - RAMDisk

```
# mount -t tmpfs -o size=12g tmpfs /dev/shm
```

  - Linux or macOS environments for optimum results when using Volatility

# Optimise Memory Analysis

- **BASH for loop**
  - BASH for loops are quite often used by Investigators during analysis but if you want results in a quick manner then it’s not feasible and inefficient.
  - Iterate one variable after another takes too long.

- **Parallel GNU**
  - Executing jobs in parallel using one or more computers.
  - Specify how many CPUs to use or the amount of jobs to run depending on CPU cores.
  - **‘pexec’** is another option that has similar capabilities to parallel GNU.
  - **‘xargs’** does support number of jobs but does not support how many CPU cores to run.

STROZ FRIEDBERG
an Aon company

# Optimise Memory Analysis Experiments

- Environment was running on ESXi Kali Virtual Machine:
  - 12GB RAM
  - 8 CPUs
  - Volatility version 2.6

- Experiments were conducted on:
  - SSD USBv3
  - RAMDisk

- Experiments ran 40 volatility plugins to quickly triage memory dumps for the relevant RAM sizes:
  - 1GB
  - 2GB
  - 4GB

- Compromised Windows 10 client:
  - Empire - PowerShell Reverse Shell
  - PowerSploit - Obfuscated Invoke-Mimikatz
  - PSReflect - Registry Persistence

# Optimise Memory Analysis Experiments

- Experiments were ran using 40 Volatility plugins to quickly triage memory dumps:
  - Processes and DLLs
  - Kernel Memory and Objects
  - Network sockets
  - Registry
  - Miscellaneous

STROZ FRIEDBERG
an Aon company

# Optimise Memory Analysis Experiments

- The following methods were used to undertake the analysis:

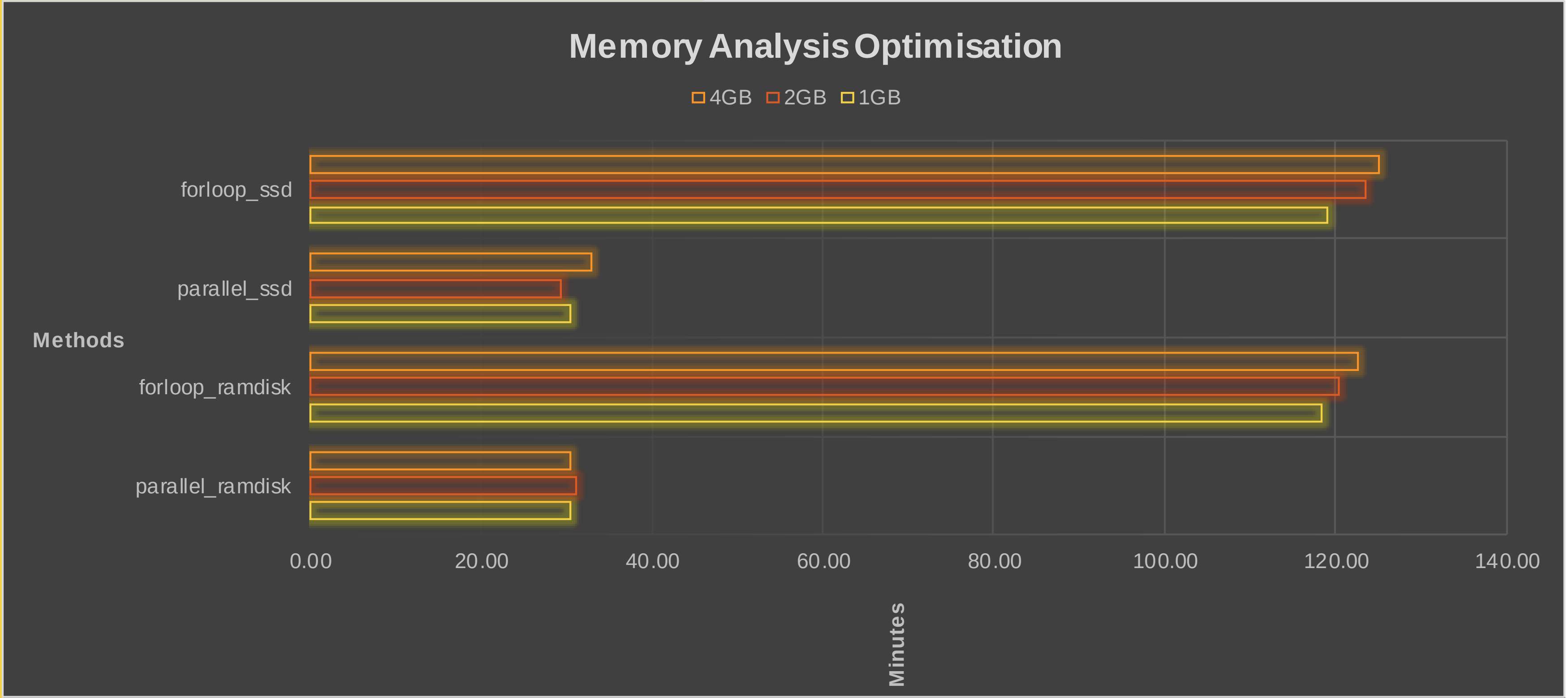
BASH for loop

```
# for i in `cat volatility_forloop_list.txt`; do vol.py $i > $i.txt; done
```

Parallel GNU

```
# parallel -a volatility_parallel_list.txt --use-cpus-instead-of-cores --colsep ' ' vol.py
{pslist} {psscan} {netscan} {consoles} {…} {…} {…} '>' {.}
```

# Optimise Memory Analysis Results



STROZ FRIEDBERG
an Aon company

# Optimise Memory Analysis Observations

- Parallel GNU:
  - 30 minutes and 67 seconds on average when running on RAMDisk

- BASH for loop:
  - 120 minutes and 49 seconds on average when running on RAMDisk

- 4 times faster to run parallel GNU compared to BASH for loop on RAMDisk or SSD

- Imagine, if you had 10 or even 100 memory dumps???

STROZ FRIEDBERG
an Aon company

# Optimise Memory Analysis Observations

- Parallel GNU is highly effective when undertaking Memory Analysis of large amounts of memory dumps.

- Complementing RAMDisk with Parallel GNU can provide rapid results.

- Utilising Volatility Unified Output can be useful when ingesting data into a SIEM for collaboration:

  - JSON
  - sqlite
  - html
  - text

**BUT**

- Large memory dump sizes can be problematic if you have limited RAM resources when undergoing analysis on RAMDisk.

# Conclusion

- Effective collaboration is vital during large-scale incident response investigations.
- Various methods can be used to Triage Windows environments depending on the environment you are in.
- Triaging *nix systems using a variety of techniques is possible.
- Optimising Memory Analysis is essential when dealing with large amounts of memory dumps.

STROZ FRIEDBERG
an Aon company

# Thank you!

- To all the project authors mentioned in this talk for making their tools FOSS!

???

STROZ FRIEDBERG
an Aon company

https://uk.linkedin.com/in/asif-matadar

@d1r4c