Grant Thornton

An instinct for growth™

24 HOURS DIGITAL FORENSICS ANALYSIS

The power of Rapid Response, Forensic Analytics & Visualization

Christos Makedonas

Partner | Technology Risk Services Leader

Grant Thornton (Cyprus) Cybersecurity Ltd.

Our story: 24 HRs Digital Forensic Analysis

- Based on industry research conducted during the years, the need for a forensic tool that will be revealing any indicators of misconduct (such as Data Leakage, IP theft etc.) has been acknowledged.

- Consequently, computer forensics insights, support and guidance has been provided to Panagiotis Krommydakis, who primarily developed the proposed tool as part of his Master's Thesis (supervised by Dr. Eliana Stavrou from UCLan University Cyprus and myself) that we call **"24 HOURS DIGITAL FORENSICS ANALYSIS TOOL"** (available also on GitHub: https://github.com/krommydakis/24HoursForensicsAnalysisTool)

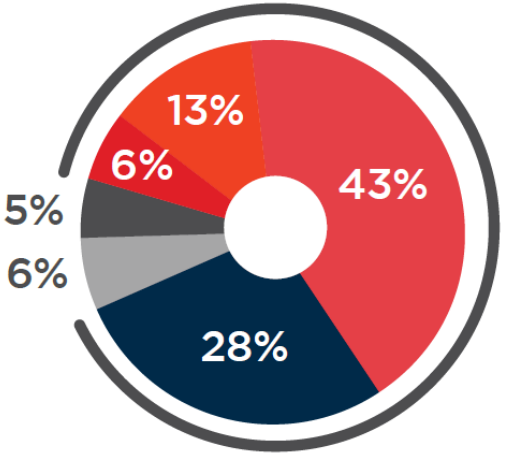
Panagiotis Krommydakis

Panagiotis Krommydakis works as a freelance Principal Information Security Consultant / Senior Penetration Tester for the last 5 years. More specifically, he is employed as an external consultant by private sector companies mainly European and Governmental organizations on the implementation of information security solutions under the auspices of IT management programs. He also performs penetration testing as well as vulnerability assessments against web applications, smartphones (mobile apps) and IT infrastructure (network infrastructure). Finally, he deals with providing services related to the establishment and proper operation of Secure SDLC to companies and organizations with software development departments. He has more than 20 years of experience as an IT professional and has worked on international projects in more than 20 countries with on-site presence, and in more than 40 countries remotely. He has previously worked for 15 years in distinguished Software Development Houses (Softcom-Int, SIEMENS SIS and SIEMENS DI&P).

He holds an MSc. in Cybersecurity from the UCLAN University in Cyprus and a BSc. In Information Technology from the Hellenic American University. He has also studied Physics at the National and Kapodistrian University of Athens.

He holds the following active professional certifications: CISSP, CISM, CISA, CRISC, CSSLP, C | EH, COBIT 5 (F), IT / IL v3 (F), ISO / IEC 27001 Lead Auditor / Auditor, SOTP.

Insider threat

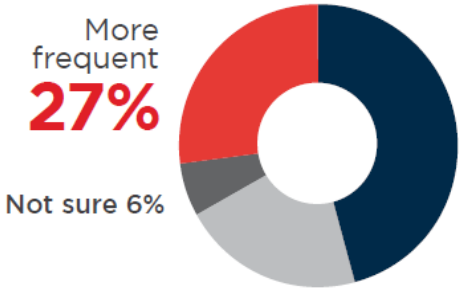


90%
feel vulnerable
to insider threats

- Extremely vulnerable
- Very vulnerable
- Moderately vulnerable
- Slightly vulnerable
- Not at all vulnerable
- Cannot disclose/not sure

Cybersecurity Insiders, 2018

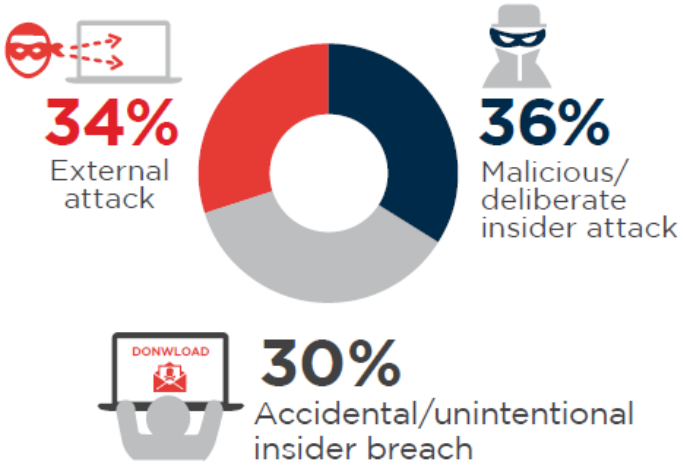
Have insider attacks against your organization become more or less frequent over the last 12 months?



Grant Thornton | An instinct for growth™

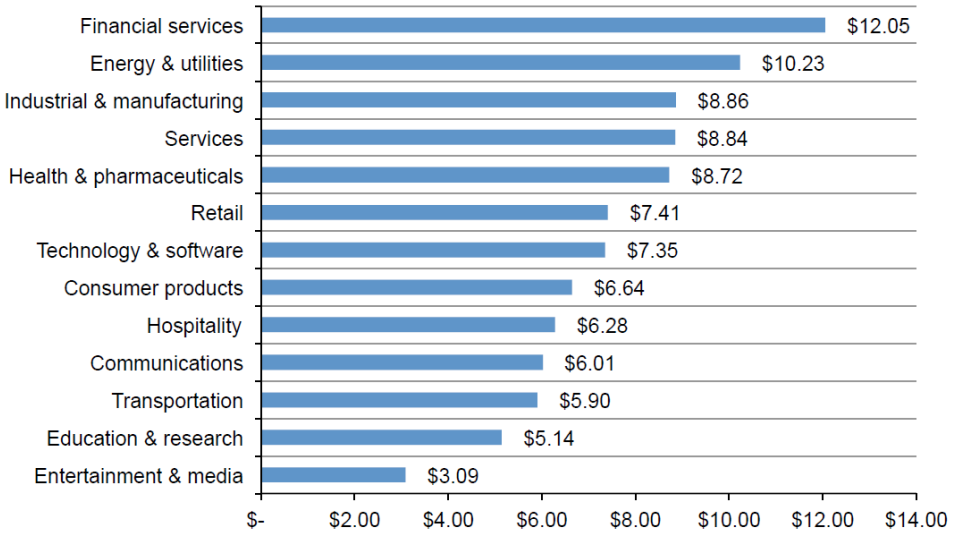
Insider threat (cont'd)

What threat do you consider most LIKELY to happen to your organisation?



Internal incident cost per sector

All types of insider incidents increase year by year (Ponemon Institute, 2018)



Grant Thornton | An instinct for growth™

Leaving employees & data leakage

In today's dynamic business environment and the emerging digital age, we are observers of crises, cyber-attacks, employee misconduct and various types of financial crimes.

Usually when an employee is about to leave his/her company there is a risk to the organization of having data leakage of personal and other intellectual property information. In addition, there may be employee productivity issues or other examples of misconduct.

Remediation and threat mitigation

Insider threat mitigation efforts rely usually on the following five (5) categories of tools or capabilities:

1. User Activity Monitoring (UAM)
2. Data Loss or Leakage Prevention (DLP)
3. Security Information and Event Management (SIEM)
4. Analytics, and
5. **Digital Forensics**

Grant Thornton | An instinct for growth™

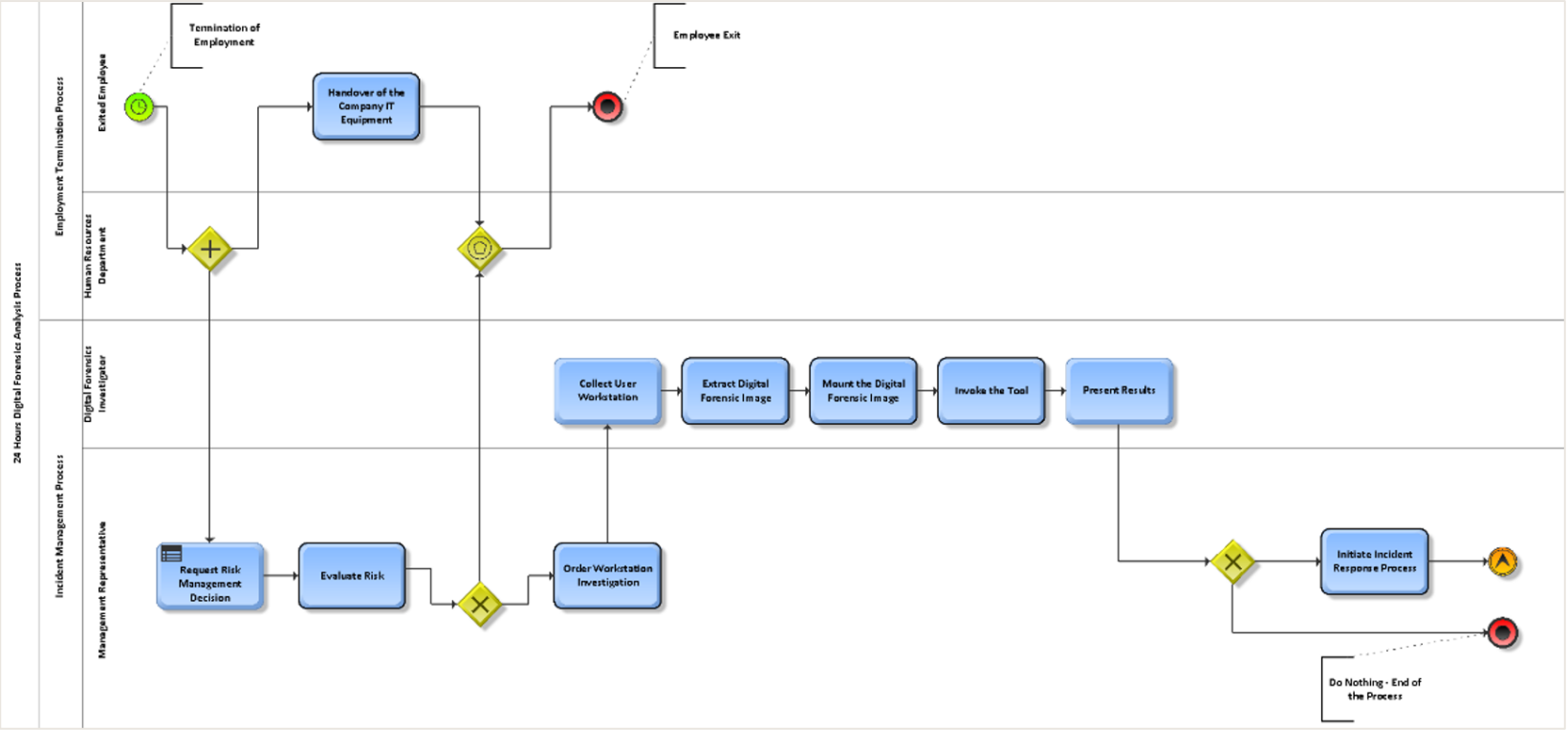
Rule: Digital Forensics Lab based investigation

- Do not make other assumptions / don't be confused with:
  - Cyber Incident response
  - Forensic triage
  - Indicators of Compromise (IOC)
  - Network Forensics
  - Investigating server logs / proxy / firewall / DLP
  - Etc.
- Do not take for granted anything (technological advancements)

Why Rapid Response - Project Scope

- Management in Crisis and Panic Attack alert!
- During an investigation there are many expectations from the management towards Digital Forensics Investigators so as to provide answers to questions like who? when? how? where? what?
- Being able to provide key answers within the first 24 hours of an investigation can assist the organization or even the investigation team to go to different directions or perform a more in-depth investigation
- What about GDPR and reporting “without undue delay” / 72hrs DPA notification?

Proposed methodology & Building a hypothesis



Grant Thornton | An instinct for growth™

Methodology: Applicable Threat Scenarios

Identify potential risks and build hypothesis for potential malicious scenarios or minimal productivity

- Classified (or sensitive) Data Exfiltration
- Classified (or sensitive) Data Alteration
- Classified (or sensitive) Data Destruction
- Install an Advanced Persistent Threat (APT)
- Plant a Logic Bomb
- Use of stolen credentials
- Limited Productivity
- Use of Anti-forensics tools or Techniques

Building hypothesis - Malicious Activities

1. Workstation access outside business hours
2. Workstation access outside working days
3. Copy data into a USB key
4. Copy data to a non-company cloud share
5. Send data to a non-business mail account
6. Copy data through a remote connection (i.e. Team Viewer)
7. Install and activate unauthorised bind shell to the workstation
8. Install and activate unauthorised reverse shell to the workstation
9. Install unauthorised products such as for remote connection (i.e. team viewer) to the workstation
10. Delete company information assets (i.e. source code)
11. Alter the integrity of company information assets
12. Install malware on the workstation
13. Install virtualization software on the workstation
14. Turn off the runtime protections of the workstation
15. Deletion of workstation log files
16. Access network shares with different account
17. Attempts to access network shares on different workstations
18. Access “black-listed” internet sites
19. Use of browser incognito mode
20. Taking screenshot
21. Print document
22. Modify Task Scheduler (or Create a new task i.e. for the logic bomb)
23. Access gray (limited productivity attack) listed internet sites
24. Access Proxy and Filter Avoidance internet sites (anti forensics)
25. Screensaver duration/occurrences during business hours

Windows 10 Artifacts

Just a few:

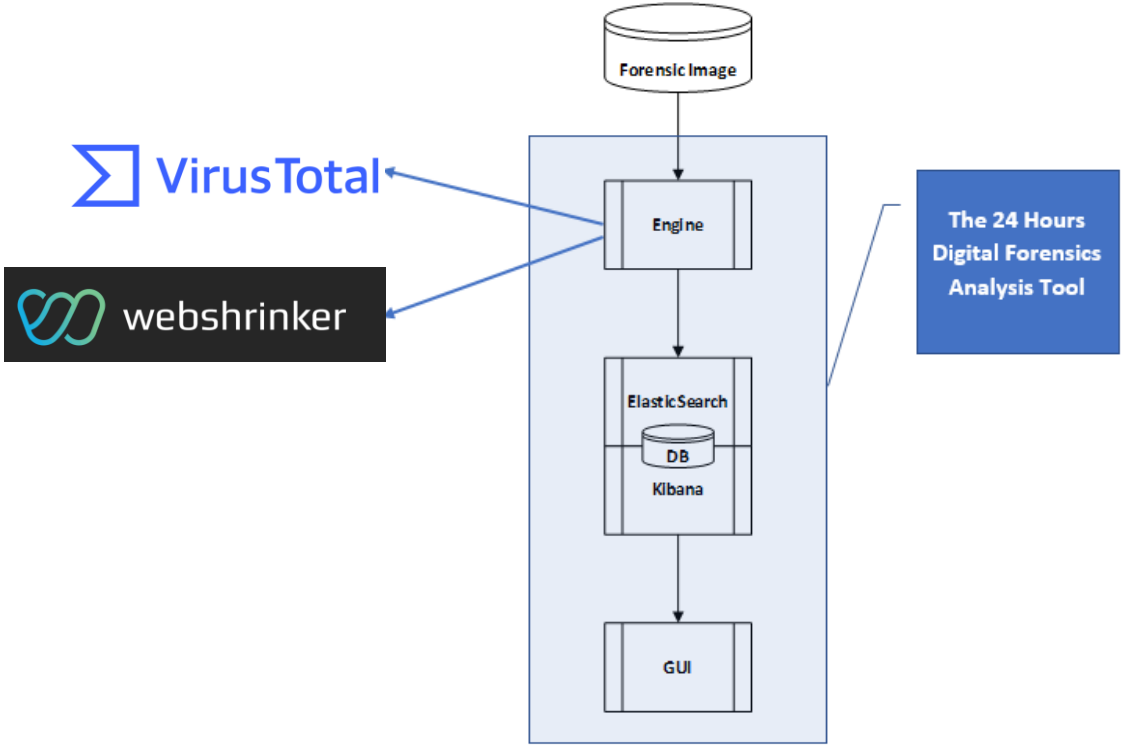
Evidence of	Artifact	Artifact Description	Artifact Location
File Download	Open or Save MRU	Key to trace files that have been opened or saved within a Windows shell dialog box (applicable to web browsers and common applications). The "*" subkey is used for files of any extension	NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSavePIDIMRU
	Email Attachments	MS Outlook data files, of the latest application version, are stored in OST and PST format. Email attachments are encoded with MIME (Base64) format.	%USERPROFILE%\AppData\Local\Microsoft\Outlook
	Skype History	Skype history is activated by default and keeps a log of a) chat sessions and b) files transferred	C:\%USERPROFILE%\AppData\Roaming\Skype\<skype-name>
	Browser Artifacts	Information is recorded per local account along with the frequency each site has been visited. Browser history will list the links for the files that were opened from the visited web sites (via download to the local filesystem).	Internet Explorer • IE8-9: %USERPROFILE%\AppData\Roaming\Microsoft\Windows\IEDownloadHistory\index.dat • IE10-11: %USERPROFILE%\AppData\Local\Microsoft\Windows\WebCache\WebCacheV*.dat Firefox • v3-25: %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\downloads.sqlite • v26+: %userprofile%\AppData\Roaming\Mozilla\Firefox\Profiles\<random text>.default\places.sqlite Table:moz_annos Chrome: %USERPROFILE%\AppData\Local\Google\Chrome\User Data\Default\History

Grant Thornton | An instinct for growth™

Windows 10 Artifacts (cont'd)

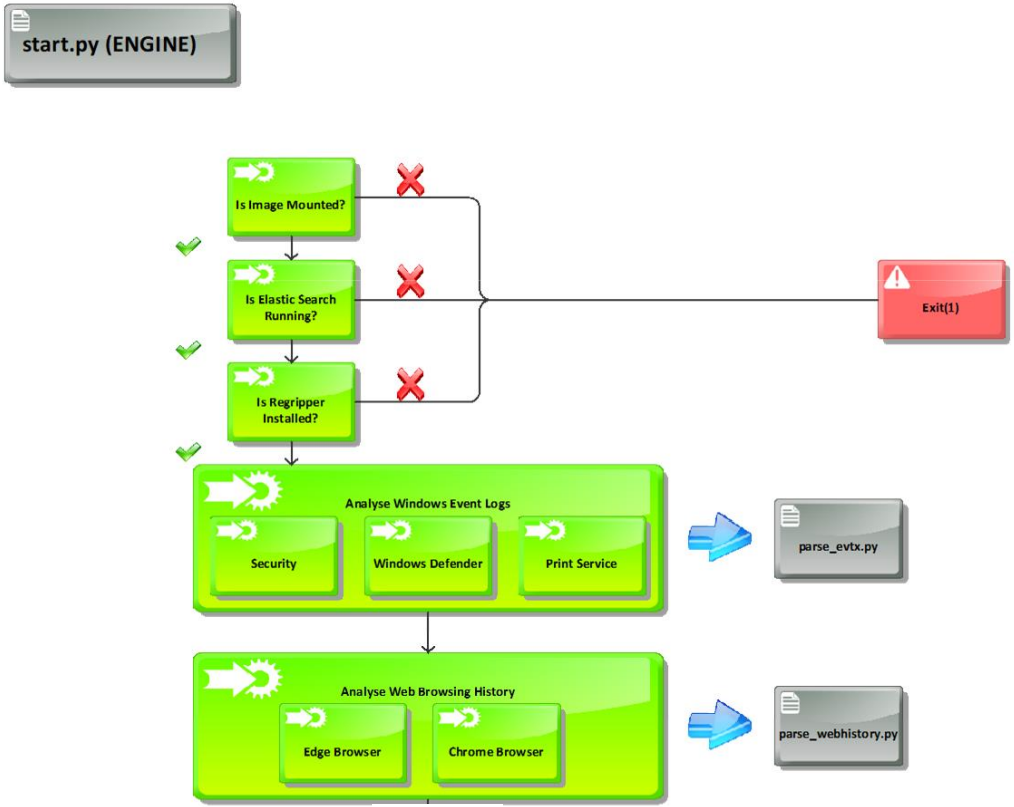
Evidence of	Artifact	Artifact Description	Artifact Location
Program Execution	UserAssist	GUI-based programs launched from the desktop are tracked by the Windows launcher as follows (ROT-13 encoding): a) CEBFF5CD (Executable File) b) F4E57C4B (Shortcut)	NTUSER.DAT HIVE: NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\ {GUID}\Count
	Windows 10 Timeline	Win10 keep track, in an SQLite db, tracesregarding all the recently used applications and files in the form of a "timeline". (to access it one should hit the "WIN+TAB" keys combination)	C:\Users\<profile>\AppData\Local\ConnectedDevices Platform\L.<profile>\ActivitiesCache.db
	RecentApps	Launching of a GUI Program is tracked by the RecentApps key. Each GUID refers to a different application that has been recently executed. Following records are stored: • AppID = Name of Application • LastAccessTime = Last execution time in UTC • LaunchCount = Number of times executed	NTUSER.DAT\Software\Microsoft\Windows\Current Version\Search\RecentApps
	Shimcache	Windows Application Compatibility Database keeps track of any compatibility issues along with the executable file name, file size, last modified time. Useful to identify is specific malware has been executed on the system	SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
	Jump Lists	Used to provide fast and easy access, through the associated application (AppID), to recently accessed media files and performed tasks. Following tracks are stored: Creation Time, Last time of execution, Modification Time	C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations
	Amcache.hve	ProgramDataUpdater uses this registry file to store data during a process creation.	C:\Windows\AppCompat\Programs\Amcache.hve

24hrs Digital Forensics Analysis Tool



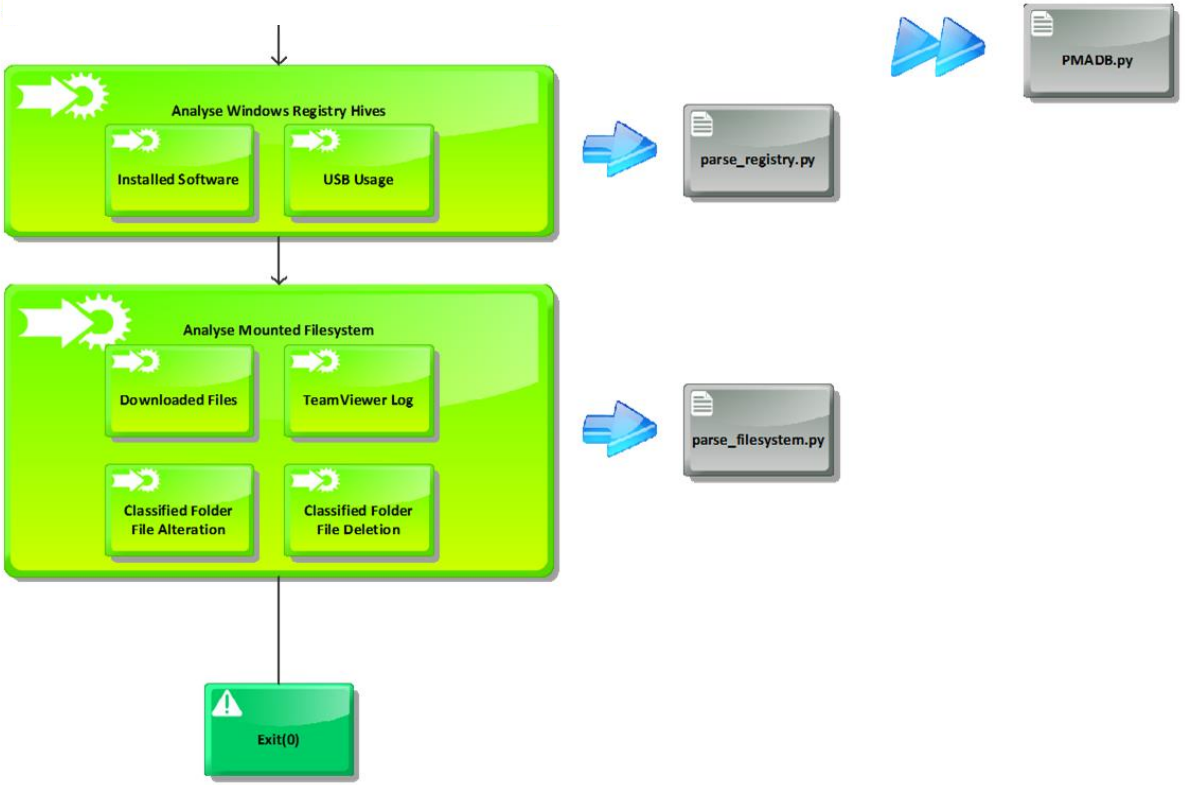
Grant Thornton | An instinct for growth™

Engine



Grant Thornton | An instinct for growth™

Engine (cont'd)



Grant Thornton | An instinct for growth™

Digital Forensicator & Investigation Steps

She/he is responsible for the overall configuration and administration of the tool. More particularly she/he is assigned with the following responsibilities:

- Prepare the Digital Forensic Image from the workstation of the exited employee
- Mount the aforementioned image on the tool's Virtual Machine for further analysis
- Configure the parameters of the tool's engine
- Trigger the analysis by the tool
- Present the analysis results to the upper management, via the graphical interface, and support them to interpret the results

24hr Forensics

24hrs Forensics - Mozilla Firefox

24hrs Forensics

localhost

Most Visited 24hrs Forensics Tool Kibana

24hrs Forensics

Welcome to 24hts forensics Tool.

Once you fill in correctly Settings you can run "python start.py".

After it successfully executes and collects all the artifacts into your ElasticSearch you can visit Report

24hrs Forensics - Settings - Mozilla Firefox

24hrs Forensics - Settings

localhost/settings

Most Visited 24hrs Forensics Tool Kibana

24hrs Forensics - Settings

Image Path	/mnt/theimage/
Suspected User	user
Classified Data Folder	Desktop/CompanyData
ElasticSearch host name	localhost
ElasticSearch port	9200
RegRipper Path	/root/tools/RegRipper2.8/rip.pl
VirusTotal API key	e85fa18951bf4a357af530eda8c77dcd4b21f04bc0bef09bef85063d53bb210b
WebShrinker API key	UNjoa9Ha35Sg8QrNnL6c
WebShrinker API secret	nitxn6xGD52Ei4gT45V4

Modify!

The Configuration Settings of the Tool

24hr Forensics - Tool Invocation

Sample of Activities

```
File  Edit  View  Search  Terminal  Help
root@kali:~# cd Desktop/24HoursForensicsAnalysisTool/
root@kali:~/Desktop/24HoursForensicsAnalysisTool# ls
24hrsForensics.py  config.ini  parse_evtx.py        parse_registry.py    PMADB.py     README.md  requirements.txt  tools
app                forms.py    parse_filesystem.py   parse_webhistory.py  __pycache__  report.py  start.py          venv
root@kali:~/Desktop/24HoursForensicsAnalysisTool# source venv/bin/activate
(venv) root@kali:~/Desktop/24HoursForensicsAnalysisTool# python start.py
Image mounted at: /mnt/theimage/
Using ElasticSearch instance: localhost:9200
Dropping potentially_malicious_actions index.
Created index: potentially_malicious_actions
Dropping url index.
Created index: url
Company Data in: Desktop/CompanyData
RegRipper tool version: Rip v.2.8_20190128


Obtaining Windows Logs from evtx files ... Be patient. This may take a while ..
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
```

```
root@kali: ~/Desktop/24HoursForensicsAnalysisTool
File  Edit  View  Search  Terminal  Help
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................Finished processing Event logs in 181 seconds.

Checking Edge web browsing history...
............ done in 15 seconds.

Checking Chrome web browsing history...
1  of  117 2019-03-20 09:06:09 Business https://www.google.com/search?q=how+to+disable+windows+defender&oq=how+to+disable+&aqs=chrome.1.69i57j0l5
2  of  117 2019-03-20 09:07:20 Business https://www.windowscentral.com/how-permanently-disable-windows-defender-windows-10
3  of  117 2019-03-20 11:10:59 Information Technology https://www.google.com/search?q=download+teamviewer&oq=download+team&aqs=chrome.0.0j69i57j0
4  of  117 2019-03-20 11:11:06 Information Technology https://www.teamviewer.com/nl/download/old-versions.aspx
5  of  117 2019-03-20 11:14:56 Electronic Mail Provider https://mail.google.com/mail/?tab=rm
.6  of  117 2019-03-20 11:14:56 Electronic Mail Provider https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=ht
=2&emr=1&osid=1#
.7  of  117 2019-03-20 11:14:56 Electronic Mail Provider https://mail.google.com/intl/nl/mail/help/about.html#
.8  of  117 2019-03-20 11:14:56 Business https://www.google.com/intl/nl/mail/help/about.html#
9  of  117 2019-03-20 11:14:56 Business https://www.google.com/intl/nl/gmail/about/#
10  of  117 2019-03-20 11:15:10 Electronic Mail Provider https://accounts.google.com/AccountChooser?service=mail&continue=https://mail.google.co
.11  of  117 2019-03-20 11:15:10 Uncategorized https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service
.12  of  117 2019-03-20 11:15:11 Uncategorized https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service
.13  of  117 2019-03-20 11:15:12 Business https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&servi
14  of  117 2019-03-20 11:15:18 Business https://accounts.google.com/signin/v2/sl/pwd?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=m
1&navigationDirection=forward
15  of  117 2019-03-20 11:15:28 Uncategorized https://accounts.google.com/CheckCookie?hl=nl&checkedDomains=youtube&checkConnection=youtube%3A95%
2Fmail.google.com%2Fmail%2F&gidl=EgIIAA
.16  of  117 2019-03-20 11:15:29 Electronic Mail Provider https://mail.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Fmail.google
oDVmspXELiYraiAYu_9Q6tAi8U7Ins0HqXwqa7Sb-b29Vl52mul11WhTaqXSmt0yheIAI7CoEZnscSuJ4YY1tpUo8LZgr
.17  of  117 2019-03-20 11:15:29 Electronic Mail Provider https://mail.google.com/mail/
.18  of  117 2019-03-20 11:15:29 Electronic Mail Provider https://mail.google.com/mail/u/0/
.19  of  117 2019-03-20 11:15:35 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox
.20  of  117 2019-03-20 11:31:23 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox/FMfcgxwBWKQxDfjSwMpXvZrZckprHnWN
.21  of  117 2019-03-20 11:31:37 Uncategorized https://www.google.com/url?q=https://www.dropbox.com/l/AABAV98wFfbc5v1dy7l8xYB5Qwvn7zHl-Z0&source
.22  of  117 2019-03-20 11:31:37 Business https://www.dropbox.com/l/AABAV98wFfbc5v1dy7l8xYB5Qwvn7zHl-Z0
23  of  117 2019-03-20 11:31:37 Business https://www.dropbox.com/login_notification/this_was_me?oref=e&request_id=2c7cdaf88160b5330e335ca49fad6f
24  of  117 2019-03-20 11:31:54 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox
.25  of  117 2019-03-20 11:32:16 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox?compose=new
.26  of  117 2019-03-20 11:32:26 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox?compose=DmwnWrRmVpVMMHcmHVdDmsspVxtwPHMpbhmpqb
.27  of  117 2019-03-20 11:33:09 Electronic Mail Provider https://mail.google.com/mail/u/0/#inbox
.28  of  117 2019-03-20 11:34:37 Media Sharing https://www.google.com/search?q=dropbox+login&oq=Dropbox+login&aqs=chrome.0.0j69i60l3j0l2.7363j0j
.29  of  117 2019-03-20 11:34:40 Business https://www.dropbox.com/en_GB/login
30  of  117 2019-03-20 11:35:28 Business https://www.dropbox.com/
```

Event Logs, Browsing History etc.

Grant Thornton | An instinct for growth™

24hr Forensics - Tool Invocation (Cont'd)

root@kali: ~/Desktop/24HoursForensicsAnalysisTool

File Edit View Search Terminal Help

```
...
Analyzing downloaded files...
15 files will be scanned.
* Sending 10_Anti-Forensics_2.ppt to VirusTotal:
  14:Scan request successfully queued, come back later for the report
 Scan finished, information embedded
 Clean :)
* Sending desktop.ini to VirusTotal:
  13:Scan request successfully queued, come back later for the report
 Scan finished, information embedded
 Clean :)
* Sending eicar.com to VirusTotal:
  12:Scan request successfully queued, come back later for the report
* Sending eicar.com.txt to VirusTotal:
  11:Scan request successfully queued, come back later for the report
* Sending eicarcom2.zip to VirusTotal:
  10:Scan request successfully queued, come back later for the report
* Sending eicar_com.zip to VirusTotal:
  9:Scan request successfully queued, come back later for the report
* Sending malicious (2).zip to VirusTotal:
  8:Scan request successfully queued, come back later for the report
* Sending malicious.zip to VirusTotal:
  7:Scan request successfully queued, come back later for the report
* Sending TeamViewer_Setup.exe to VirusTotal:
  6:Scan request successfully queued, come back later for the report
 Scan finished, information embedded
 Clean :)
* Sending jsp-reverse.jsp to VirusTotal:
  3:Scan request successfully queued, come back later for the report
 Scan finished, information embedded
 24 positives!
{'MicroWorld-eScan': 'Backdoor.Small.DT', 'FireEye': 'Backdoor.Small.DT', 'McAfee': 'JSP/BackDoor.gen', 'ESET-NOD32': 'a variant of Generik.GSWTSKI', 'TrendMicro-HouseCall': 'HKTL_NETCAT', 'Avast': 'Java:JspShel
l-A [Trj]', 'BitDefender': 'Backdoor.Small.DT', 'Tencent': 'Html.Win32.Script.500628', 'Ad-Aware': 'Backdoor.Small.DT', 'Comodo': 'Malware@#w6czo3q2qy51', 'TrendMicro': 'HKTL_NETCAT', 'McAfee-GW-Edition': 'JSP/B
ackDoor.gen', 'Emsisoft': 'Backdoor.Small.DT (B)', 'Fortinet': 'Riskware/Generik.GSWTSKI!tr', 'Arcabit': 'Backdoor.Small.DT', 'AegisLab': 'Trojan.Script.Small.4!c', 'Microsoft': 'Backdoor:ASP/Aspy', 'AhnLab-V3':
 'Script/Backdoor', 'ALYac': 'Backdoor.Small.DT', 'MAX': 'malware (ai score=100)', 'Ikarus': 'Trojan.SuspectCRC', 'GData': 'Backdoor.Small.DT', 'AVG': 'Java:JspShell-A [Trj]', 'Qihoo-360': 'virus.js.qexvmc.1'}
.* Sending shell.aspx to VirusTotal:
  2:Scan request successfully queued, come back later for the report
* Sending jsp-reverse.jsp to VirusTotal:
  1:Scan request successfully queued, come back later for the report
* Sending shell.aspx to VirusTotal:
  0:Scan request successfully queued, come back later for the report
... done in 72 seconds.
TeamViewer log not present.
..Scanning of image (/mnt/theimage/) finished in 305 seconds.
Please launch GUI to see result analysis.
(venv) root@kali:~/Desktop/24HoursForensicsAnalysisTool#
```

Downloaded files Analysis – VirusTotal integration

Grant Thornton | An instinct for growth™

24hr Forensics - GUI & Analytics

24hrs Forensics - Kibana - Mozilla Firefox

24hrs Forensics - Kibana

localhost:5601/app/kibana#/dashboard/39069d60-5398-11e9-94b5-c3e1262d5987?embed=true&_g=(refreshInterval:(pause:!t,value:0),time:(from:'2019-04-13T14:14:15.797Z',mode:absolut

Most Visited | 24hrs Forensics Tool | Kibana

kibana

Discover
Visualize
Dashboard
Timelion
Canvas
Machine Learning
Infrastructure
Logs
APM
Dev Tools
Monitoring
Management
Default
Collapse

Dashboard / 24hrs Forensics

Full screen | Share | Clone | Edit | Auto-refresh | April 13th 2019, 16:14:15.797 to April 13th 2019, 16:29:15.797

Time Range

Quick | Relative | Absolute | Recent

From: 2019-03-18 00:00:00.000 (Set To Now)

To: 2019-03-29 23:59:59.999 (Set To Now)

YYYY-MM-DD HH:mm:ss.SSS

March 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

March 2019

Sun	Mon	Tue	Wed	Thu	Fri	Sat
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Go

Search... (e.g. status:200 AND extension:PHP) | Options | Refresh

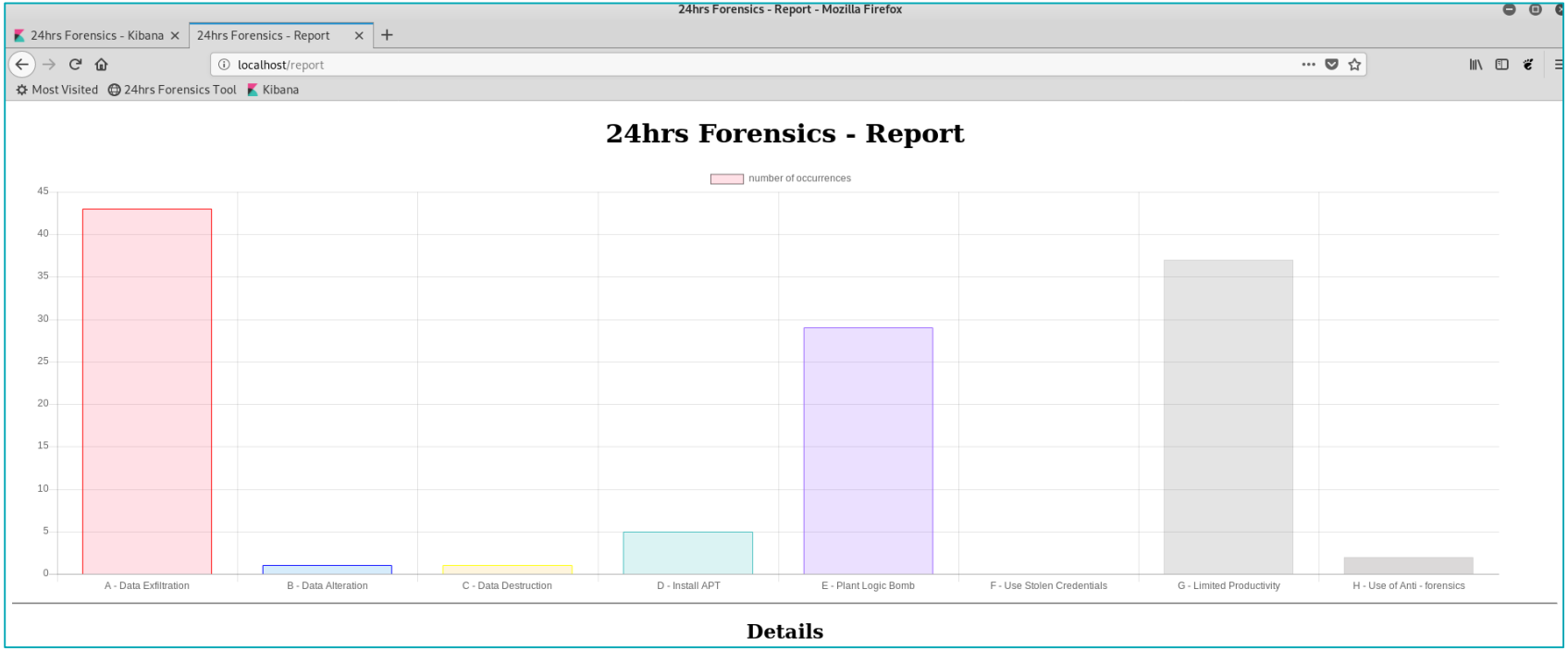
Add a filter +

Web Browsking History

1.0
0.5
Bussines Related
Private
Malicious

Grant Thornton | An instinct for growth™

24hr Forensics - GUI & Analytics (cont'd)



The Occurrences of the Identified Potential Threats

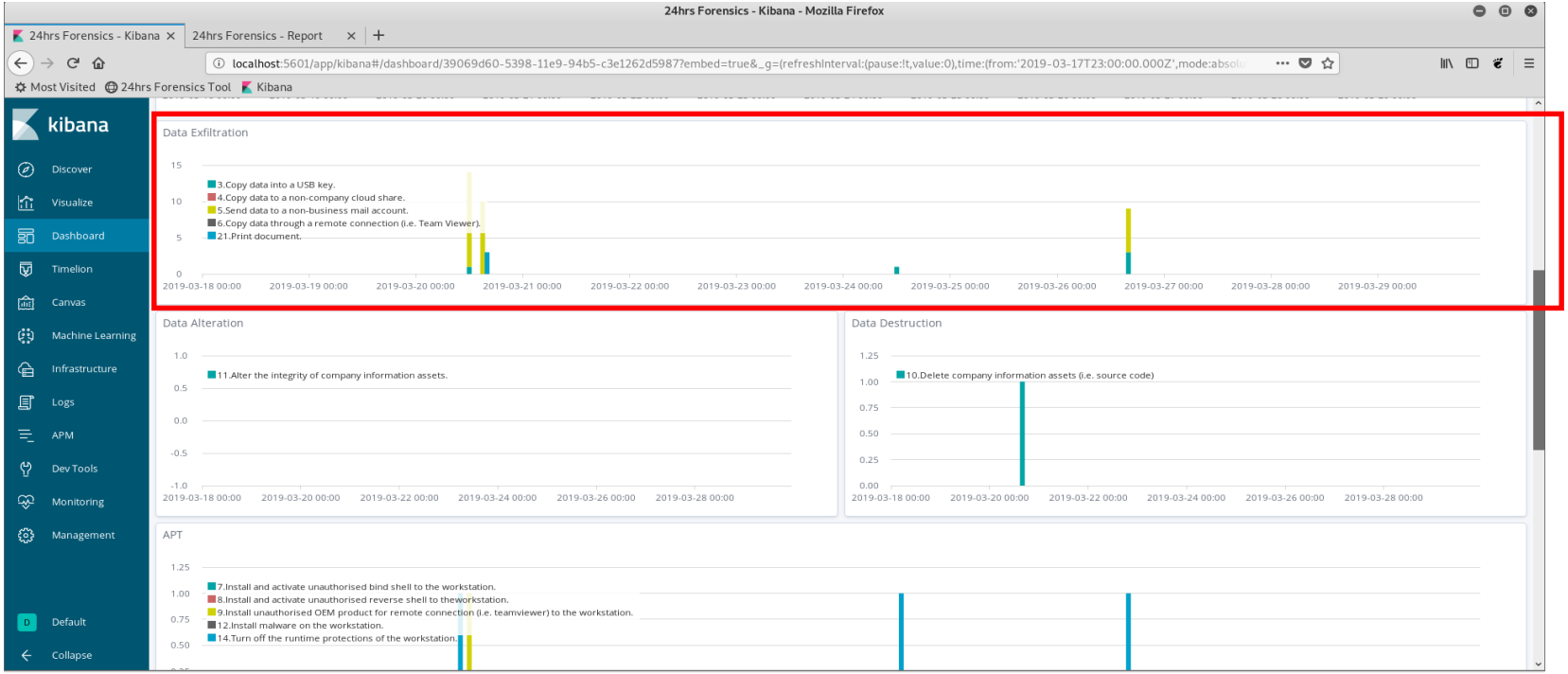
Grant Thornton | An instinct for growth™

24hr Forensics - GUI & Analytics (cont'd)

Analysis Results on Web Browsing History

Grant Thornton | An instinct for growth™

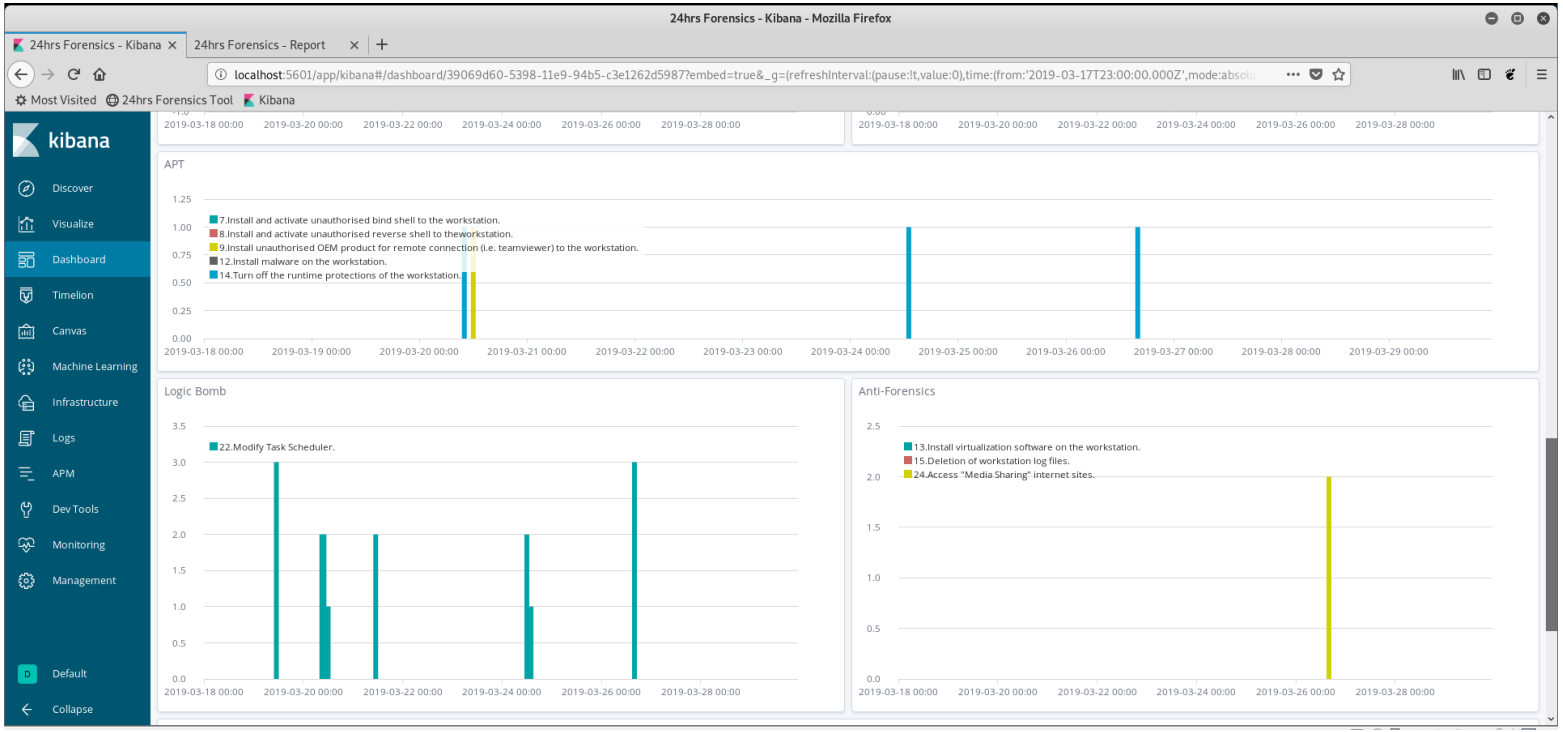
24hr Forensics - GUI & Analytics (cont'd)



Analysis Results on Potential Data Exfiltration Attempts

Grant Thornton | An instinct for growth™

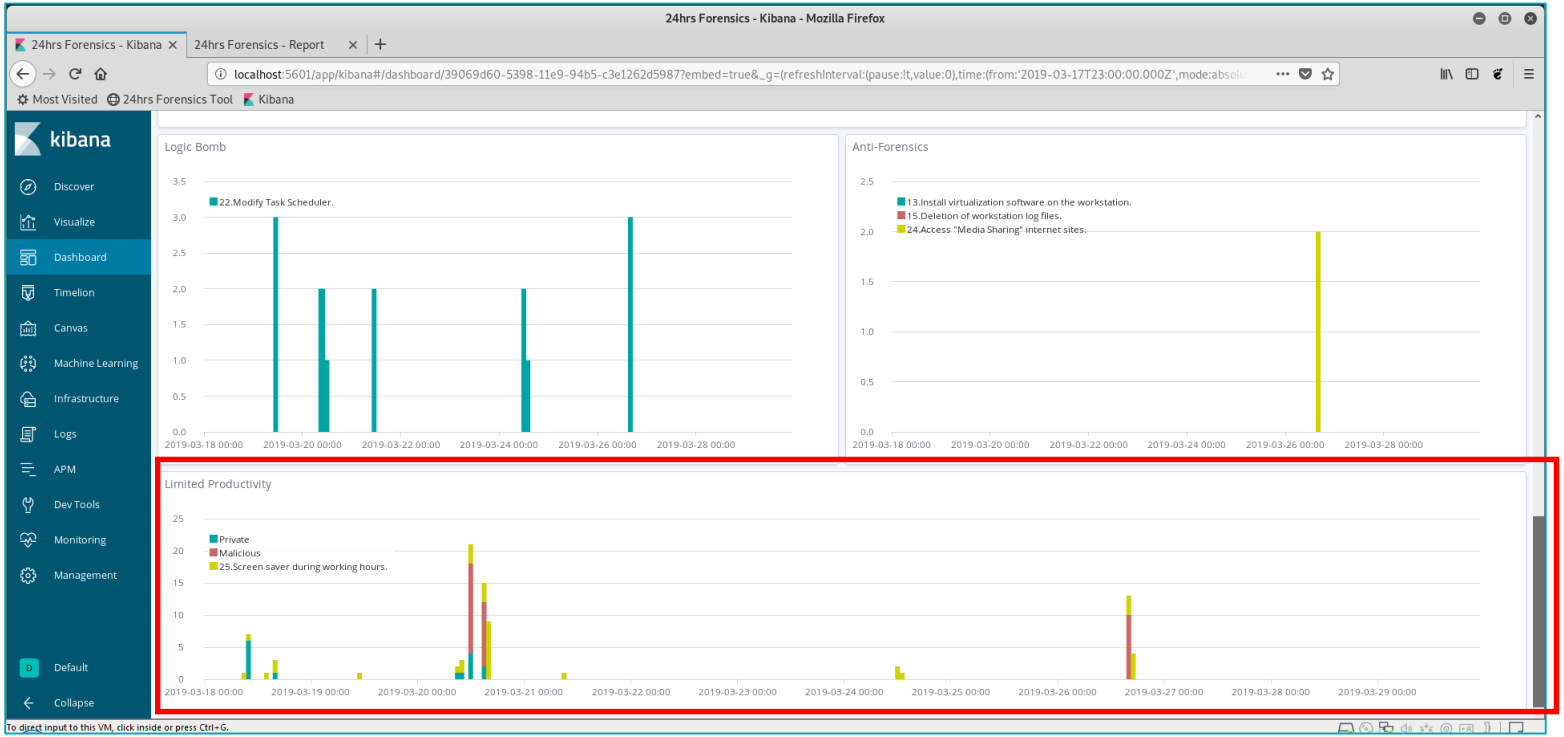
24hr Forensics - GUI & Analytics (cont'd)



Analysis Results on Potential APT Attempts - Bomb Activation Attempts & Anti-forensics

Grant Thornton | An instinct for growth™

24hr Forensics - GUI & Analytics (cont'd)



Analysis Results on Potential Limited Productivity

Grant Thornton | An instinct for growth™

Areas for improvement

- Redesign the solution so as to perform real-time (and not static) acquisition of the artefacts
- Eliminate design flaws
- Enrich the detectable threat scenarios by taking into consideration alternative attack vectors for the various malicious actions
- Strengthen the threat identification capabilities, using supervised or reinforcement learning algorithms of machine learning
- Enrich the data visualization capabilities of the tool (i.e. by using Canvas features in Kibana).
- Support different vendor and versions of Operating Systems

Support this tool

Why GitHub? Enterprise Explore Marketplace Pricing Search / Sign in Sign up

krommydakis / 24HoursForensicsAnalysisTool

Watch 2 Star 1 Fork 0

Code Issues 0 Pull requests 0 Projects 0 Security Insights

Dismiss

Join GitHub today

GitHub is home to over 40 million developers working together to host and review code, manage projects, and build software together.

Sign up

This project was created in the context of the Master thesis in the MSc Cybersecurity course at UCLan Cyprus, under the co-supervision of Mr. Christos Makedonas, President of ISACA Cyprus Chapter (with GitHub ID: cyberfpro), and Dr Eliana Stavrou, Course Leader MSc Cybersecurity. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND. AL...

5 commits 1 branch 0 releases 1 contributor

Branch: master New pull request Find File Clone or download

krommydakis Update README.md Latest commit 4126f82 on 9 Apr

app	Add files via upload	6 months ago
tools	Update run_GUI.sh	6 months ago
24hrsForensics.py	Add files via upload	6 months ago
PMADB.py	Add files via upload	6 months ago
README.md	Update README.md	6 months ago
config.ini	Add files via upload	6 months ago
forms.py	Add files via upload	6 months ago
parse_evtx.py	Add files via upload	6 months ago
parse_filesystem.py	Add files via upload	6 months ago

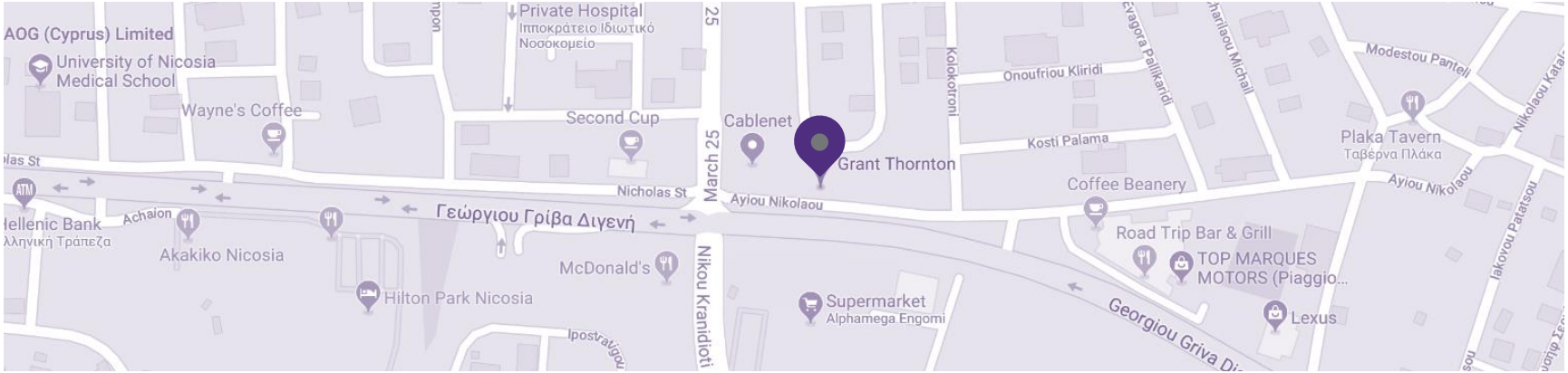
GitHub

https://github.com/krommydakis/24HoursForensicsAnalysisTool

Grant Thornton | An instinct for growth™

Thank you.

Stay in touch



Nicosia, Headquarters

+357 22600000

trs@cy.gt.com

41-49 Agiou Nicolaou Street
Nimeli Court, Block C, 2408, Engomi
P.O.Box 23907
1687 Nicosia
Cyprus

linkedin.com/company/**grantthorntoncy**

facebook.com/**grantthorntoncyprus**

twitter.com/**grantthorntoncy**

Grant Thornton | An instinct for growth™

Grant Thornton

An instinct for growth™

grantthornton.com.cy