Table of Contents

Section	Title	Page
1	Introduction	3
1.1	Summary of Case and Tasking	3
1.2	Statement of Compliance	3
2	Chain of Custody	3
2.1	Suspect's Digital Devices	4
2.2	Forensic Case Examination	4
3	Audit Trail of Investigation Process	5
4	Case Report	6
4.1	Evidence Acquisition	6
4.2	Evidence Preservation	7
4.3	Evidence Analysis and Results	7
4.4	ACPO Compliance in Digital Forensics: The Case of Kroger Paul	8
5	Reflection	9
5.1	Summary of Investigation Results	9
5.2	Recent Developments and Challenges	9
6	Suspect Sites Visit on Tor Browser	10
7	Disclaimer	11

Deepfake Deception and Digital Trails: A Forensic Analysis of The Puppet Master's Machiavellian Gambit

1. Introduction

This report aims to delineate a comprehensive narrative of the digital manipulations conducted by Kroger Paul, specifically in the context of the 2024 United States elections. The evidence detailed is strictly within the bounds of digital forensics expertise.

a. Summary of Case and Tasking

Kroger Paul is accused of engineering a sophisticated cyber operation. His activities, conducted with the intent to skew public discourse and affect election outcomes, included procuring technology for deepfake creation, extracting sensitive information via Google Dorking, and deploying cyberattacks.

b. Statement of Compliance

As a forensic expert, I assert my commitment to impartiality and the accuracy of this report. The conclusions drawn are based on evidence within my professional domain, and I will update all stakeholders if subsequent evidence alters my understanding.

2. Chain of Custody: In alignment with ACPO guidelines, meticulous records were kept throughout the evidence's journey from Paul's devices to the forensic lab. Each handler's details were scrupulously logged, ensuring the evidence's journey upheld legal standards and maintaining its forensic integrity for courtroom presentation.

a. Suspect's Digital Devices:

1. Suspect's Desktop PC

- Date/Time of Custody: 08:30 am, January 05, 2024
- Location of Seizure: Artisan Heights, 3 New Wakefield St. Manchester, M15AA, United Kingdom
- Evidence Description: Digital artifacts related to deepfake creation and social media manipulation extracted from the desktop PC.
- Evidence Source: Desktop PC
- Make/model: ACER NITRO 5
- Operating System: Windows 11, Version: 23H2, OS Build: 22621.607
- Browser version: Tor Browser 13.0.5 (based on Mozilla Firefox 115.5.0)
- Software: Adobe After Effects, DeepFaceLab, Custom AI Scripts

2. Suspect's Raspberry Pi

- Date/Time of Custody: 08:30 am, January 05, 2024
- Location of Seizure: Artisan Heights, 3 New Wakefield St. Manchester, M15AA, United Kingdom
- Evidence Description: Digital artifacts with custom scripts and tools for manipulation and data analysis

- Evidence Source: Raspberry Pi
- Make/model: Raspberry Pi 2 Model B
- Operating System: Parrot OS, Version 2021.3
- Browser version: Tor Browser 13.0.5 (based on Mozilla Firefox 115.5.0)
- Software: Custom Python Scripts, Social Media Bots Management Tools

2. Forensic Case Examination:

1) **Device Identification:**
   - The forensic team meticulously captured the condition and specifications of both the desktop PC and Raspberry Pi. Every detail, from serial numbers to individual hardware components, was cataloged to establish a baseline for the investigation.

2) **Evidence Preservation:**
   - The devices were stored in signal-proof containment to protect against any potential tampering or data loss, ensuring the pristine state of the digital evidence was maintained throughout the transfer process to the forensic lab.

3) **Chain of Custody Verification:**
   - A rigorous chain of custody was maintained, with detailed logging of each evidence handler's identity and the specific time of interaction, providing a transparent evidence trail.

4) **Forensic Imaging:**
   - Forensic clones of the devices' storage were created, and their integrity was confirmed through cryptographic hashing, with all processes thoroughly recorded for procedural accuracy and reliability.

5) **Operating System Analysis:**
   - The operating systems—Windows 11 and Parrot OS—underwent a full forensic examination. Autopsy and other specialized tools were employed to extract and analyze system logs, revealing traces of deepfake software use and social media manipulation tactics.

6) **Data Recovery:**
   - Using advanced recovery software, previously deleted files crucial to the investigation, such as video editing projects and scripts for bot networks, were retrieved and analyzed for evidence of tampering or misuse.

7) **Reporting Process:**
   - The findings were compiled into exhaustive reports, systematically detailing every artifact and piece of evidence. These reports were prepared with the utmost precision, ensuring they met the standards necessary for legal proceedings and judicial review.

3. Audit Trail of Investigation Process

Step No.	Date	Action/Event	Comment/Location	Responsible Party
1	05/01/24 :09:00:00	Arrest of Suspect (Kroger Paul)	Suspect detained based on digital forensics evidence. Location: Artisan Heights, 3 New Wakefield st. Manchester, M15AA	Law Enforcement Agency
2	05/01/22 :01:16:46	Seizure of Desktop PC and Raspberry Pi	High-end Desktop PC and Raspberry Pi seized from suspect's residence. Devices contain evidence of deepfake software, scripts, and digital artifacts related to deepfake creation and social media manipulation. **Evidence Source**: Desktop PC, Raspberry Pi **Make/Model**: ACER NITRO 5,, Raspberry Pi 2 Model B **Operating System**: Windows 11, Parrot OS Data was securely transferred to an encrypted **Amazon S3 bucket** with strict access controls, **multi-factor authentication**, and logging to maintain evidence integrity and a clear audit trail.	Law Enforcement Agency
3	05/01/22 :01:23:02	Transfer to Forensic Lab	Devices and accompanying digital media transferred to the forensic lab for analysis.	Law Enforcement Agency
4	05/01/22 :01:32:36	Initial Forensic Assessment	Preliminary assessment of the seized devices conducted.	Forensic Lab Team
5	05/01/22 :01:47:55	Disk Imaging	The desktop PC and Raspberry Pi were powered off upon seizure to maintain the integrity of potential evidence. Forensic imaging was conducted using a live version of FTK Imager to avoid any data alteration. The images captured were then securely hashed to ensure data integrity before analysis: ● Desktop PC Image: img_DesktopPC_LEA2024KP001.001 ○ MD5 - d387ad2551ccba2d4bc205f88582c498 ○ SHA 1 HASH - 9a1fd71883d5de4ac8efe0c343adbae6bd365413 ● Raspberry Pi Image: img_RaspberryPi_LEA2024KP002.001 ○ MD5 HASH - 24eeb2845cbfda238b78fa165c21607d ○ SHA 1 HASH - 4578a184e2170744a6a10dd8265309a3b5accfd3 No bad blocks were reported during the imaging process, indicating a healthy state of the storage media.	Digital Forensic Analyst
6	05/01/22 :06:48:12	Upload to Secure	Forensic images uploaded to Amazon S3 with encryption, and access logs activated.	Digital Forensic Analyst

		Cloud Storage		
7	05/01/22 :06:58:26	Detailed Evidence Analysis	Analysis of disk images for digital artifacts related to deepfake creation and social media manipulation.	Digital Forensic Analyst
8	05/01/22	Drafting of Preliminary Findings	Initial report compiled, summarizing key digital evidence and analysis.	Forensic Investigation Team
9	05/01/22	Review of Findings	Conducted a thorough internal review to validate the preliminary findings.	Forensic Investigation Team
12	05/01/22	Final Analysis and Reporting	Developed a final comprehensive report, encapsulating the forensic investigation's outcomes.	Digital Forensic Analyst
13	05/01/22	Submission of Final Report	Delivered the final report to law enforcement and legal teams.	Forensic Investigation Team

4. Case Report

4.1. Evidence Acquisition

In the initial phase of our digital forensic investigation, the collection of electronic evidence from Kroger Paul's desktop PC and Raspberry Pi was paramount. The process was carried out using a suite of advanced forensic tools chosen for their precision and reliability within the forensics community. Autopsy (4.21) facilitated a granular analysis of the devices, extracting pivotal data including browsing history, file access records, and detailed communication logs. Concurrently, FTK Imager (Version 4.7.1.2) ensured the creation of comprehensive forensic images, capturing the full spectrum of digital evidence, both apparent and concealed. In the interest of maintaining the evidence's integrity during transfer and subsequent storage, Amazon S3's secure and encrypted services were employed. The actions taken from the initial device seizure to the final evidence storage were meticulously documented, with every procedural step recorded to ensure a transparent and verifiable audit trail. This initial stage laid the groundwork for a robust investigation, with each action taken to collect evidence carried out using write-blocked devices, upholding the pristine state of the digital evidence.

Figure 1 in the Evidence Acquisition section depicts the systematic process of gathering and securing digital evidence against Kroger Paul. It outlines the journey of forensic data from initial capture to secure storage, emphasizing crucial steps such as secure storage in S3, encryption via KMS, oversight with CloudTrail, automation using Lambda, and IAM for stringent access control.

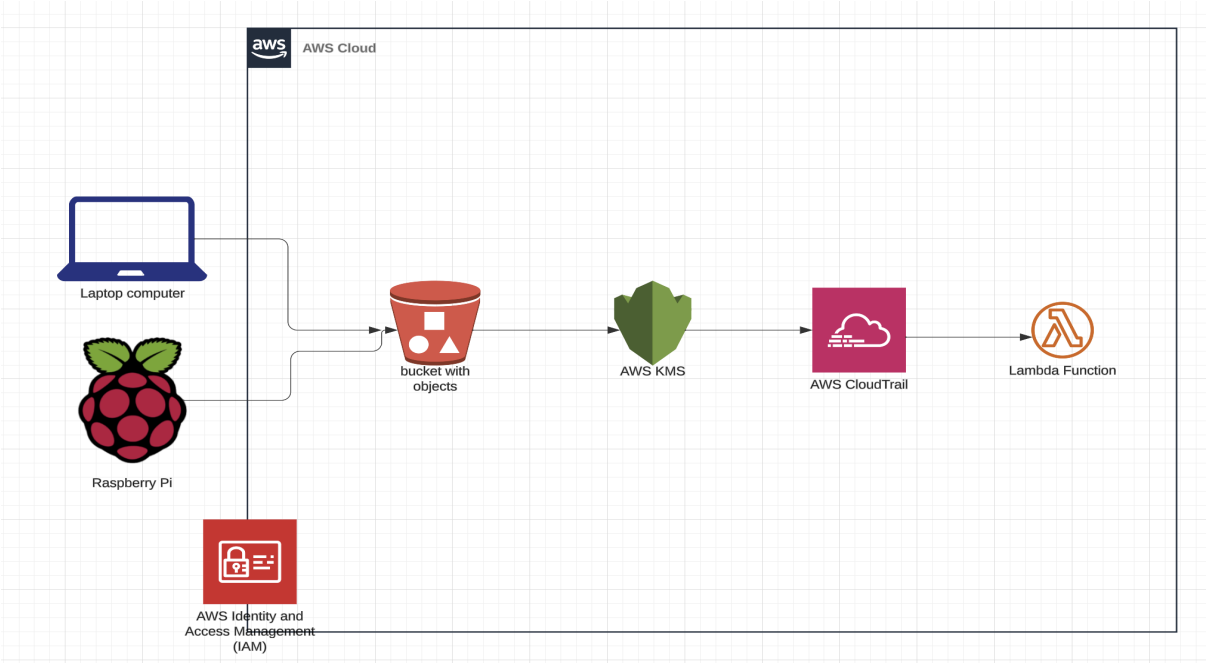


Fig.1 Evidence Acquisition and transfer process

4.2 Evidence Preservation

Following acquisition, the preservation of the forensic integrity of the data was our next critical step. This involved a scrupulous approach to maintaining data and metadata integrity during the imaging process. Attributes such as file creation, modification times, and last access timestamps were carefully preserved to uphold the evidentiary value of the data. Hash verification methods, including MD5, SHA1, and SHA-256, were systematically applied to confirm the collected evidence's integrity. This not only fortified the evidence against potential contamination but also against any unintended alterations during both local storage and cloud-based uploads. Our preservation process incorporated post-analysis checks with rigorous standards to prevent evidence modification, ensuring that the original state of the evidence was immutably conserved.

4.3 Evidence Analysis and results

The depth of analysis performed on the forensically duplicated evidence was exhaustive and methodical. Utilizing tools acclaimed for their capability to discern and analyze artificial media and digital communication patterns, we probed the depths of Kroger Paul’s deepfake production and network manipulations. This meticulous examination, performed on exact duplicates of the original evidence, assured that our analysis was both comprehensive and forensically sound without compromising the physical evidence's integrity. The conclusions drawn from our extensive analysis provided irrefutable evidence of Paul's engagement in creating and disseminating deepfake content aimed at political disruption. The confidence in these conclusions is anchored in the detailed digital evidence and robust analysis methodology. A timeline of events/actions was established, painting a chronological picture of Paul’s cyber manipulation tactics, leading to recommendations for enhanced security measures and legal proceedings. Our investigation’s thorough nature not only brought to light the suspect’s sophisticated maneuvers but also demonstrated the forensic team's methodical and

unbiased approach in ensuring an accurate representation of the events that culminated in Paul's apprehension.

4.4. ACPO Compliance in Digital Forensics: The Case of Kroger Paul

In my capacity as a digital forensic investigator, I hereby confirm the adherence to the Association of Chief Police Officers (ACPO) guidelines throughout our investigation into the activities of Kroger Paul. The investigative procedures were carefully designed and executed to maintain the integrity of the evidence and uphold the principles of digital forensics:

- Preservation of Evidence: We ensured no alteration of the original state of digital evidence was made, consistent with the ACPO 'Principle of No Change'.
- Comprehensive Audit Trail: From the initial acquisition of the suspect's devices to the detailed analysis phases, every action was documented. This included the seizure, imaging, analysis, and reporting. All procedures were logged with precise timestamps, actions, and outcomes for transparency and accountability.
- Data Integrity and Security: The integrity of the evidence was upheld using cryptographic hashes. Security measures for evidence storage and access were stringent, employing methods such as secure cloud transfers and restricted access controls to prevent unauthorized data tampering.
- Legally Compliant Investigation: Our methods and analysis, especially those regarding the use of sensitive tools and techniques, remained within the legal framework and respected privacy rights and boundaries.

By strictly following these guidelines, we ensure that our findings are legally sound and that the investigation's integrity is beyond reproach. Our commitment to the ACPO standards reinforces the credibility of our results and conclusions in the case against Kroger Paul.

PART 2 - REFLECTION

5. Summary of Investigation Results:

The investigation into Kroger Paul's actions revealed a concerted effort to influence the political Our investigation into Kroger Paul's digital conduct culminated in a detailed compilation of evidence that underscores a strategic attempt to influence electoral outcomes. Key findings include:

- Procurement and utilization of sophisticated hardware for generating deepfake media.
- Active engagement in information gathering and exploitation targeting political adversaries.
- Execution of cyber operations that manipulated social media discourse.
- Financial maneuvers designed to obfuscate the origin and flow of funds supporting these activities.

The evidence, meticulously documented in the audit trail, substantiates the allegations against Paul, painting a comprehensive picture of his cyber endeavors.

5.1 Recent Developments and Challenges:

The field of digital forensics is encountering unprecedented challenges, many of which were manifested in the case of Kroger Paul:

- Advanced anonymization tools that complicate the tracing of illicit online activities.
- Sophisticated deepfake technologies that pose new types of threats to public trust.
- Rise in the use of cryptocurrencies, presenting hurdles in financial tracing.
- Increasing sophistication in cyberattacks, particularly related to social media platforms.

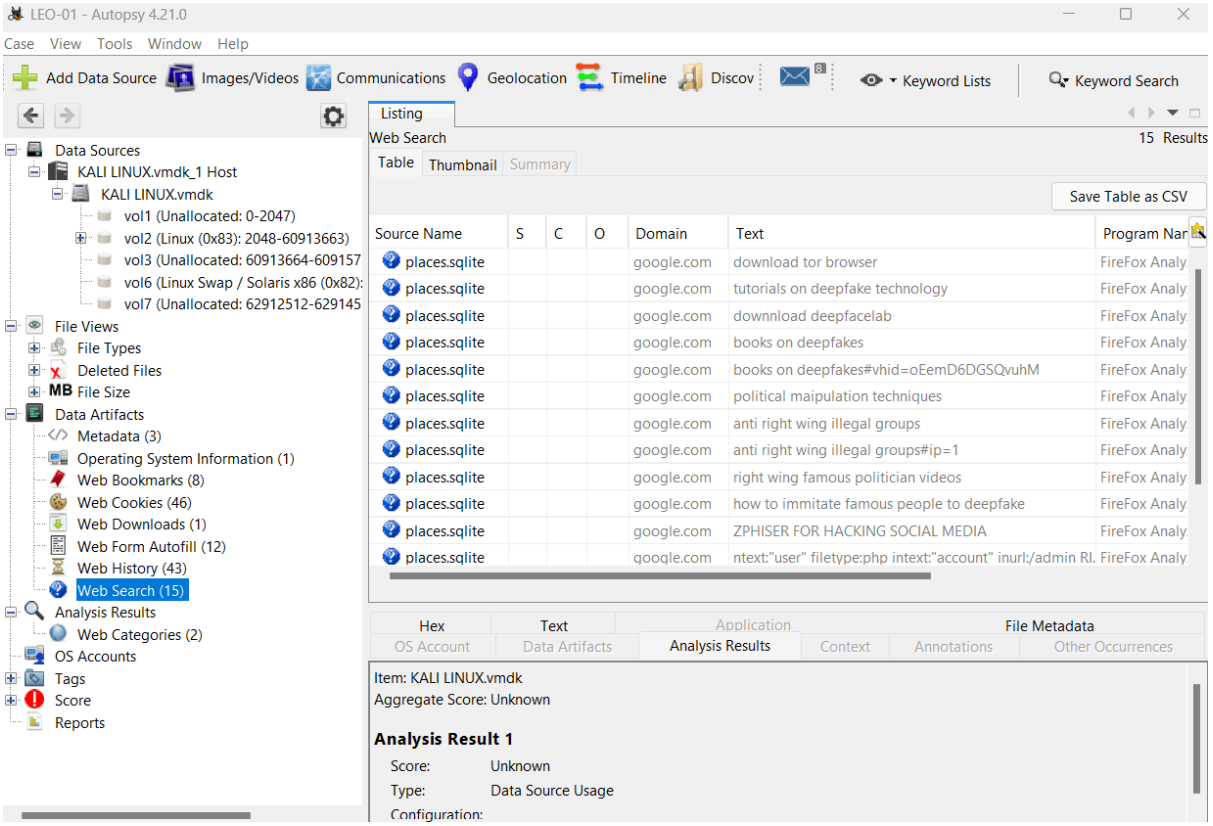
Such developments underscore the necessity for continual advancement in forensic techniques and a proactive approach to emerging cyber threats.

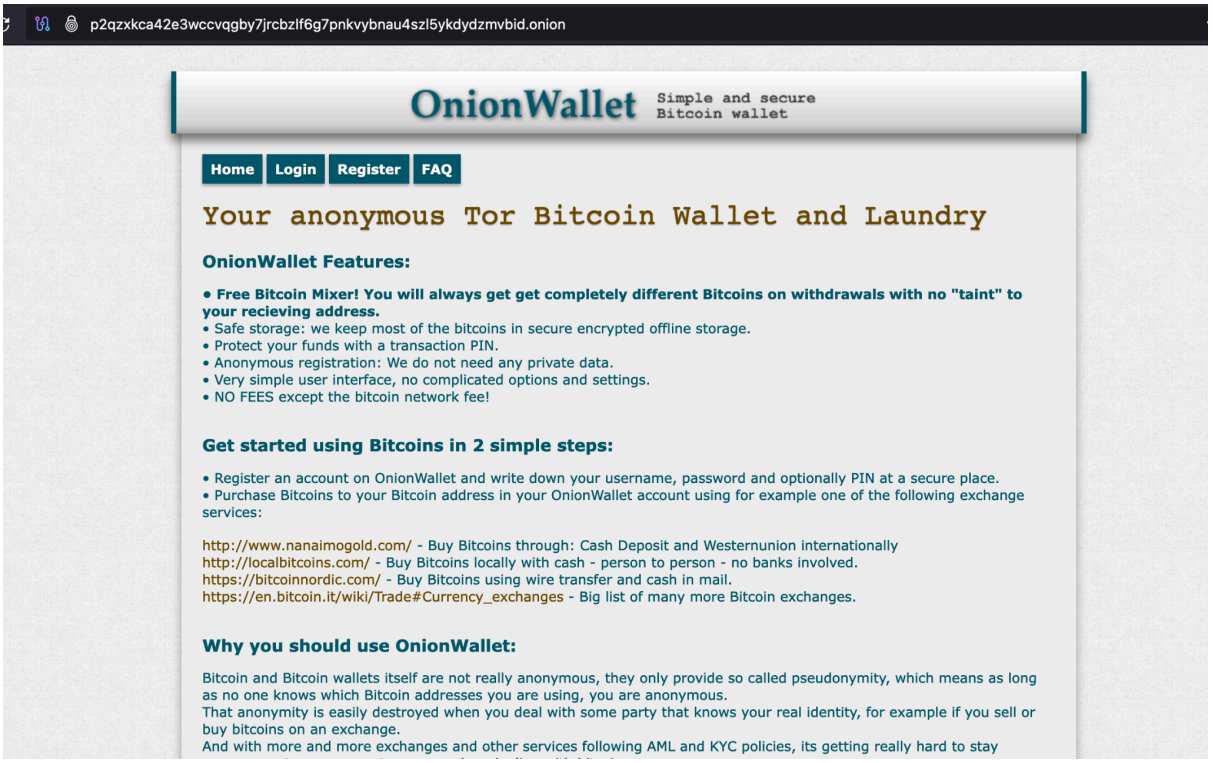
5.2 Browsing related memory artifacts from Windows 10.

Sr	Websites	Suspected Activities	Evidence Found from Browser Profile
1	Darknet Hardware Forums	Bulk purchasing of NVIDIA 4080 TI graphics cards for deepfake production	# Bulk Order Invoices # Secure Messaging with Vendors
2	Encrypted Communication Platforms	Setting up anonymous communication channels using temporary emails and numbers	# Encrypted Email Setup # Burner Phone Usage Patterns
3	Deepfake Software Repositories	Acquiring and testing various deepfake generation tools	# Software Downloads # Testing Logs

4	Political Data Aggregators	Employing OSINT tools for in-depth profiling of political adversaries	# Data Mining Activities # Downloaded Dossiers
5	Media Archives	Archiving extensive video footage of opposition party politicians for algorithm training	# Video Metadata # Archival Timestamps
6	Scripting and Automation Hubs	Downloading and customizing scripts for automating social media influence	# Script Customization Logs # Automation Sequences
7	Secure Email Services (ProtonMail)	Orchestrating misinformation campaigns and covert communications	# Campaign Emails # Strategy Communication Logs
8	Crypto-Anonymity Networks	Masking financial transactions linked to extortion and MMU Liberal Party funding	# Anonymized Transactions # Crypto-Transfer Trails
9	Electoral Databases	Exploring vulnerabilities in digital voting infrastructures	# Access Logs # Exploitation Attempts
10	Social Media Platforms	Disseminating deepfake content and orchestrating social media takeovers	# Posted Content # Account Control Evidence

```
177629e0 76 65 64 41 6E 61 6C 79-73 65 73 45 4E 53 5F 31 vedAnalysesENS_1
177629f0 35 41 6E 61 6C 79 73 69-73 4D 61 6E 61 67 65 72 5AnalysisManager
17762a00 49 53 32 5F 4A 45 45 31-31 49 6E 76 61 6C 69 64 IS2_JEE11Invalid
17762a10 61 74 6F 72 45 4A 45 45-44 30 45 76 00 2E 72 65 atorEJEED0Ev..re
17762a20 6C 61 2E 74 65 78 74 2E-5F 5A 4E 34 6C 6C 76 6D la.text._ZN4llvm
17762a30 36 64 65 74 61 69 6C 31-37 41 6E 61 6C 79 73 69 6detail17Analysi
17762a40 73 50 61 73 73 4D 6F 64-65 6C 49 4E 53 5F 38 46 sPassModelINS_8F
17762a50 75 6E 63 74 69 6F 6E 45-4E 53 5F 32 33 53 63 61 unctionENS_23Sca
17762a60 6C 61 72 45 76 6F 6C 75-74 69 6F 6E 41 6E 61 6C larEvolutionAnal
17762a70 79 73 69 73 45 4E 53 5F-31 37 50 72 65 73 65 72 ysisENS_17Preser
17762a80 76 65 64 41 6E 61 6C 79-73 65 73 45 4E 53 5F 31 vedAnalysesENS_1
17762a90 35 41 6E 61 6C 79 73 69-73 4D 61 6E 61 67 65 72 5AnalysisManager
17762aa0 49 53 32 5F 4A 45 45 31-31 49 6E 76 61 6C 69 64 IS2_JEE11Invalid
17762ab0 61 74 6F 72 45 4A 45 45-33 72 75 6E 45 52 53 32 atorEJEE3runERS2
17762ac0 5F 52 53 36 5F 00 2E 72-65 6C 61 2E 74 65 78 74 _RS6_..rela.text
17762ad0 2E 5F 5A 4E 4B 34 6C 6C-76 6D 36 64 65 74 61 69 ._ZNK4llvm6detai
17762ae0 6C 31 37 41 6E 61 6C 79-73 69 73 50 61 73 73 4D l17AnalysisPassM
17762af0 6F 64 65 6C 49 4E 53 5F-38 46 75 6E 63 74 69 6F odelINS_8Functio
17762b00 6E 45 4E 53 5F 32 33 53-63 61 6C 61 72 45 76 6F nENS_23ScalarEvo
17762b10 6C 75 74 69 6F 6E 41 6E-61 6C 79 73 69 73 45 4E lutionAnalysisEN
17762b20 53 5F 31 37 50 72 65 73-65 72 76 65 64 41 6E 61 S_17PreservedAna
17762b30 6C 79 73 65 73 45 4E 53-5F 31 35 41 6E 61 6C 79 lysesENS_15Analy
17762b40 73 69 73 4D 61 6E 61 67-65 72 49 53 32 5F 4A 45 sisManagerIS2_JE
17762b50 45 31 31 49 6E 76 61 6C-69 64 61 74 6F 72 45 4A E11InvalidatorEJ
17762b60 45 45 34 6E 61 6D 65 45-76 00 2E 72 65 6C 61 2E EE4nameEv..rela.
17762b70 74 65 78 74 2E 5F 5A 4E-34 6C 6C 76 6D 36 64 65 text._ZN4llvm6de
17762b80 74 61 69 6C 31 39 41 6E-61 6C 79 73 69 73 52 65 tail19AnalysisRe
17762b90 73 75 6C 74 4D 6F 64 65-6C 49 4E 53 5F 38 46 75 sultModelINS_8Fu
17762ba0 6E 63 74 69 6F 6E 45 4E-53 5F 32 33 53 63 61 6C nctionENS_23Scal
17762bb0 61 72 45 76 6F 6C 75 74-69 6F 6E 41 6E 61 6C 79 arEvolutionAnaly
17762bc0 73 69 73 45 4E 53 5F 31-35 53 63 61 6C 61 72 45 sisENS_15ScalarE
17762bd0 76 6F 6C 75 74 69 6F 6E-45 4E 53 5F 31 37 50 72 volutionENS_17Pr
```


LEO-01 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discov Keyword Lists Keyword Search
Data Sources
KALI LINUX.vmdk_1 Host
KALI LINUX.vmdk
vol1 (Unallocated: 0-2047)
vol2 (Linux (0x83): 2048-60913663)
vol3 (Unallocated: 60913664-609157
vol6 (Linux Swap / Solaris x86 (0x82):
vol7 (Unallocated: 62912512-629145
File Views
File Types
Deleted Files
File Size
Data Artifacts
Metadata (3)
Operating System Information (1)
Web Bookmarks (8)
Web Cookies (46)
Web Downloads (1)
Web Form Autofill (12)
Web History (43)
Web Search (15)
Analysis Results
Web Categories (2)
OS Accounts
Tags
Score
Reports
Listing
Web Search
15 Results
Table Thumbnail Summary
Save Table as CSV
Source Name S C O Domain Text Program Nar
places.sqlite google.com download tor browser FireFox Analy
places.sqlite google.com tutorials on deepfake technology FireFox Analy
places.sqlite google.com downnload deepfacelab FireFox Analy
places.sqlite google.com books on deepfakes FireFox Analy
places.sqlite google.com books on deepfakes#vhid=oEemD6DGSQvuhM FireFox Analy
places.sqlite google.com political maipulation techniques FireFox Analy
places.sqlite google.com anti right wing illegal groups FireFox Analy
places.sqlite google.com anti right wing illegal groups#ip=1 FireFox Analy
places.sqlite google.com right wing famous politician videos FireFox Analy
places.sqlite google.com how to immitate famous people to deepfake FireFox Analy
places.sqlite google.com ZPHISER FOR HACKING SOCIAL MEDIA FireFox Analy
places.sqlite google.com ntext:"user" filetype:php intext:"account" inurl:/admin RI. FireFox Analy
Hex Text Application File Metadata
OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Item: KALI LINUX.vmdk
Aggregate Score: Unknown
Analysis Result 1
Score: Unknown
Type: Data Source Usage
Configuration:


p2qzxkca42e3wccvqgby7jrcbzlf6g7pnkvybnau4szl5ykdydzmvbid.onion
OnionWallet
Simple and secure Bitcoin wallet
Home Login Register FAQ
Your anonymous Tor Bitcoin Wallet and Laundry
OnionWallet Features:
• Free Bitcoin Mixer! You will always get get completely different Bitcoins on withdrawals with no "taint" to your recieving address.
• Safe storage: we keep most of the bitcoins in secure encrypted offline storage.
• Protect your funds with a transaction PIN.
• Anonymous registration: We do not need any private data.
• Very simple user interface, no complicated options and settings.
• NO FEES except the bitcoin network fee!
Get started using Bitcoins in 2 simple steps:
• Register an account on OnionWallet and write down your username, password and optionally PIN at a secure place.
• Purchase Bitcoins to your Bitcoin address in your OnionWallet account using for example one of the following exchange services:
http://www.nanaimogold.com/ - Buy Bitcoins through: Cash Deposit and Westernunion internationally
http://localbitcoins.com/ - Buy Bitcoins locally with cash - person to person - no banks involved.
https://bitcoinnordic.com/ - Buy Bitcoins using wire transfer and cash in mail.
https://en.bitcoin.it/wiki/Trade#Currency_exchanges - Big list of many more Bitcoin exchanges.
Why you should use OnionWallet:
Bitcoin and Bitcoin wallets itself are not really anonymous, they only provide so called pseudonymity, which means as long as no one knows which Bitcoin addresses you are using, you are anonymous.
That anonymity is easily destroyed when you deal with some party that knows your real identity, for example if you sell or buy bitcoins on an exchange.
And with more and more exchanges and other services following AML and KYC policies, its getting really hard to stay

6. Suspect sites visit on Tor Browser

	A	B	C	D	E	F	G	
1	Source Name	URL	Date Accessed	Title	Program Name	Domain	Data Source	Re
2	places.sqlite	file:///usr/share/kali-defaults/web/homepage.	2024-01-17 04:3	Kali Linux	FireFox Analyzer		KALI LINUX.vmdk	
3	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:3	download tor browser - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
4	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:36:57 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
5	places.sqlite	https://www.torproject.org/download/	2024-01-17 04:3	Tor Project | Download	FireFox Analyze	torproject.org	KALI LINUX.vmc	htt
6	places.sqlite	https://www.torproject.org/thank-you/	2024-01-17 04:3	Tor Project | Success	FireFox Analyze	torproject.org	KALI LINUX.vmc	htt
7	places.sqlite	https://dist.torproject.org/torbrowser/13.0.8/t	2024-01-17 04:3	tor-browser-linux-x86_64-13.0.8.tar.xz	FireFox Analyze	torproject.org	KALI LINUX.vmdk	
8	places.sqlite	file:///usr/share/kali-defaults/web/homepage.	2024-01-17 04:4	Kali Linux	FireFox Analyzer		KALI LINUX.vmdk	
9	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	tutorials on deepfake technology - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
10	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	downnload deepfacelab - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
11	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:47:39 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
12	places.sqlite	https://www.deepfakevfx.com/tutorials/begin	2024-01-17 04:4	Beginner Deepfake Tutorial: DeepFaceLab 2.0 - Dee	FireFox Analyze	deepfakevfx.com	KALI LINUX.vmc	htt
13	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:48:12 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
14	places.sqlite	https://github.com/iperov/DeepFaceLab	2024-01-17 04:4	GitHub - iperov/DeepFaceLab: DeepFaceLab is the l	FireFox Analyze	github.com	KALI LINUX.vmc	htt
15	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:48:22 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
16	places.sqlite	https://www.deepfakevfx.com/downloads/de	2024-01-17 04:4	DeepFaceLab - DeepfakeVFX.com	FireFox Analyze	deepfakevfx.com	KALI LINUX.vmc	htt
17	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	books on deepfakes - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
18	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	books on deepfakes - Google Search	FireFox Analyze	google.com	KALI LINUX.vmc	htt
19	places.sqlite	https://books.google.co.uk/books/about/Dee	2024-01-17 04:4	Deepfakes: The Coming Infocalypse - Nina Schick - (	FireFox Analyze	google.co.uk	KALI LINUX.vmc	htt
20	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	political manipulation techniques - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
21	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:49:36 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
22	places.sqlite	https://philarchive.org/archive/NOGMIP	2024-01-17 04:4	NOGMIPv1.pdf	FireFox Analyze	philarchive.org	KALI LINUX.vmc	htt
23	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	anti right wing illegal groups - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
24	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:5	anti right wing illegal groups - Google Search	FireFox Analyze	google.com	KALI LINUX.vmc	htt
25	places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:50:39 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	htt
26	places.sqlite	https://www.jstor.org/stable/29766959	2024-01-17 04:5	Right-Wing Politics and The Anti-Immigration Cause (	FireFox Analyze	jstor.org	KALI LINUX.vmc	htt
27	places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:5	right wing famous politician videos - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	

A	B	C	D	E	F	G	
places.sqlite	https://dist.torproject.org/torbrowser/13.0.8/t	2024-01-17 04:3	tor-browser-linux-x86_64-13.0.8.tar.xz	FireFox Analyze	torproject.org	KALI LINUX.vmdk	
places.sqlite	file:///usr/share/kali-defaults/web/homepage.	2024-01-17 04:4	Kali Linux	FireFox Analyzer		KALI LINUX.vmdk	
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	tutorials on deepfake technology - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	downnload deepfacelab - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:47:39 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://www.deepfakevfx.com/tutorials/begin	2024-01-17 04:4	Beginner Deepfake Tutorial: DeepFaceLab 2.0 - Dee	FireFox Analyze	deepfakevfx.com	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:48:12 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://github.com/iperov/DeepFaceLab	2024-01-17 04:4	GitHub - iperov/DeepFaceLab: DeepFaceLab is the l	FireFox Analyze	github.com	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:48:22 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://www.deepfakevfx.com/downloads/de	2024-01-17 04:4	DeepFaceLab - DeepfakeVFX.com	FireFox Analyze	deepfakevfx.com	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	books on deepfakes - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	books on deepfakes - Google Search	FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://books.google.co.uk/books/about/Dee	2024-01-17 04:4	Deepfakes: The Coming Infocalypse - Nina Schick - (	FireFox Analyze	google.co.uk	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	political manipulation techniques - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:49:36 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://philarchive.org/archive/NOGMIP	2024-01-17 04:4	NOGMIPv1.pdf	FireFox Analyze	philarchive.org	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:4	anti right wing illegal groups - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:5	anti right wing illegal groups - Google Search	FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:50:39 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://www.jstor.org/stable/29766959	2024-01-17 04:5	Right-Wing Politics and The Anti-Immigration Cause (	FireFox Analyze	jstor.org	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:5	right wing famous politician videos - Google Search	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.youtube.com/watch?v=AF8DOS	2024-01-17 04:5	Ben Shapiro: Politics, Kanye, Trump, Biden, Hitler, E>	FireFox Analyze	youtube.com	KALI LINUX.vmdk	
places.sqlite	https://www.youtube.com/watch?v=AF8DOS	2024-01-17 04:5	Ben Shapiro: Politics, Kanye, Trump, Biden, Hitler, E>	FireFox Analyze	youtube.com	KALI LINUX.vmc	http
places.sqlite	https://www.youtube.com/watch?v=AF8DOS	2024-01-17 04:5	Ben Shapiro: Politics, Kanye, Trump, Biden, Hitler, E>	FireFox Analyze	youtube.com	KALI LINUX.vmc	http
places.sqlite	https://www.google.com/search?client=firefc	2024-01-17 04:5	how to immitate famous people to deepfake - Google	FireFox Analyze	google.com	KALI LINUX.vmdk	
places.sqlite	https://www.google.com/url?sa=t&rct=j&q=&	2024-01-17 04:52:14 GMT		FireFox Analyze	google.com	KALI LINUX.vmc	http
places.sqlite	https://thenextweb.com/news/celebrity-voice	2024-01-17 04:5	This spooky deepfake AI mimics dozens of celebs an	FireFox Analyze	thenextweb.com	KALI LINUX.vmc	http

Report Presented by:
Deep Nandre
Digital Forensic Investigator
05/01/2024

Disclaimer: This report reflects the findings and conclusions based on evidence and data collected up to 05/01/2024. It is contingent upon the information and resources available at the time and may be revised should further evidence or investigative developments come to light.

ONEDRIVE LINK FOR EVIDENCE: Digital Forensics Evidence file