VOL 4 | ISSUE 2 | MAY 2022 https://doi.org/10.46293/4n6 | ISSN: 2582-1172

INDIA'S 1ST DIGITAL FORENSICS PUBLICATION

DIGITAL FORENSICS (4N6)

4N6 4N6 4N6 4N6 4N6 4N6 4N6

MAY 2022

₹ 500/-

digital4n6journal.com /d4n6j @d4n6j @d4n6j

OUR SPONSORS & PARTNERS

DIGITAL FORENSICS (4N6)

MAY 2022 ISSUE

PARTNERS

CONFERENCE PARTNERS

OUR TEAM

OUR MENTORS

MR. R. V. SUTHAR
ADVOCATE GUJARAT HIGH COURT DY SECRETARY (RETD.) GOVERNMENT OF GUJARAT

MR. OMVEER SINGH
GCFA - DIRECTOR / SCIENTIST (RETD.)
CERT-IN AND MINISTRY OF ELECTRONICS & IT GOVERNMENT OF INDIA

EDITORIAL BOARD

Seema Khadsare - Editor-in-Chief
Rakhi R Wadhwani - Associate Editor
Amrit Chhetri - Technical Editor
Jyoti Nene - Resident Editor
Evita K-Breukel - Associate Technical Editor
Deep Shankar Yadav - Associate Technical Editor

EDITORIAL BOARD MEMBERS

Seema Khadsare - Editor-in-Chief
Rakhi R Wadhwani - Associate Editor
Amrit Chhetri - Technical Editor
Jyoti Nene - Resident Editor
Evita K-Breukel - Associate Technical Editor
Deep Shankar Yadav - Associate Technical Editor

TECHNICAL COMMITTEE

Deepak Kumar (D3)
Tanmay Dikshit
Smith Gonsalves
Yogesh Pandit
Hriday Raval

DESIGN & DEVELOPMENT COMMITTEE

Aman Agarwal
Kritharth Jhala
Rishabh Sovani

CONTENT READER

Megha Bhatt

Dear Readers of 4N6 Journal,

Welcome to the May'22 Edition of Digital 4N6! We have dedicated this edition towards celebrating International Women's Day 2022.Digital Forensics is scaling new heights. New domains in the Digital forensics' domain are gaining importance as various gadgets and technologies are being used in day-to-day life. These gadgets and technologies have become inseparable part of our individual lives.

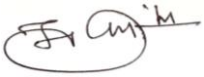
In this edition, we bring you many exciting articles topics such as cloud forensics, crypto forensics, and forensics psychology etc. This edition also covers the top 5 mistakes made by the investigator while working on the cases.We at, 4N6 publication wants to meet your expectations and needs! So do not hesitate and reach for this treasure trove of knowledge now!

As we progress in this wonderful journey, we do again seek the hones feedbacks and suggestions from the readers as we trust that this is a community effort and the publication eventually belongs to the community. We hope that you enjoy reading this issue! As always, thanks to all the authors, reviewers, to our amazing proof readers, and of course you, our readers for staying with us ☺

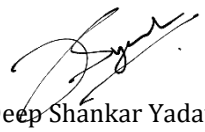
4N6 … The Investigation Begins Here…

Happy Reading Forensics works by eminent Digital Forensics Authors and Researchers!

Seema Khadsare
(Chief Editor)



Amrit Chhetri
(Sr. Associate Technical Editor)



Deep Shankar Yadav
(Associate Technical Editor)

Rakhi R Wadhwani
(Associate Editor)

4N6 INDEX
MAY'22 EDITION

https://doi.org/10.46293/4n6/2022.05.01.01

Digital 4N6 : India's First Digital Forensics (4N6) Publication

Volume : IV | Issue : II

DIGITAL 4N6 ANALYSIS

CLOUD FORENSICS

HIGHLIGHTS

This article mainly accentuates a forensic investigation performed on remotely hosted docker container. It also discusses steps followed for performing the forensic investigation and the different tools which have been used.

.

– Editorial Team, Digital Forensics (4N6)

Ajaybalaji

Ajaybalaji is currently pursuing M.Tech in the stream of Cyber Security in Amrita Vishwa Vidyapeetham, Coimbatore. He is working as Malware Researcher Intern at Mindtree. He is interested in exploring Cyber Forensics and Purple Team. He has also completed Microsoft Security, Compliance and IdentityFundamentals, Fortinet NSE 1,2 Network Security Associate, One Trust Privacy Professional certifications.

Email : cb.en.p2cys20003@cb.students.amrita.edu

Kowshik Hurshan

Kowshik Hurshan is a Cyber Security aspirant, currently pursuing his M.Tech from Amrita Vishwa Vidyapeetham, Coimbatore. At present, he is working as a Red Team Security Analyst at Fire Compass. He is interested in exploring Red Team and Cyber Forensics.

Email : cb.en.p2cys20019@cb.students.amrita.edu

► ABSTRACT

The usage of cloud technology in an organization is tremendously increasing because of its scalability, reliability, etc. So, the importance of performing forensics in a cloud environment is drastically rising and safeguarding digital evidence of particular infrastructure is the main concern. Nowadays cloud comes with a wide variety of upgrades and even new technologies within scope sprang up. Therefore, it becomes a daunting task for a forensic investigator to analyze the evidence from the cloud. A proper insight into how to use forensic tools is required to collect the related content. This paper mainly accentuates a forensic investigation performed on remotely hosted docker containers. It also discusses the steps followed for performing the forensic investigation. The paper also emphasizes the experimental findings obtained by investigation.

Keywords: Cloud Forensics, Docker Container, Evidence, Investigation, Findings.

► INTRODUCTION

The rise of cloud technology paves the way for different opportunities for optimistic usage. Attackers could be able to exploit certain areas of the cloud-like security. Cloud models need not require users to physically own infrastructure, they can access a variety of features by remote desktop. This type of computing describes a unique challenge for forensic investigators. It defines the salience of having unique forensic tools and methodologies for accumulating and inspecting digital evidence in this digital world, in some circumstances even prior to data loss and different service models, had added more challenges for forensic investigators to obtain full access and control the outspread resources of the cloud. Such developments in the computing world pave the way for the increase in cyber-crimes. The research stack is at a newfangled state in inscribing issues of digital forensics for the conventional computing world including virtual environments but these solutions may not be applied in the cloud directly. Our motivation is to perform forensic analysis of docker container

(remotely hosted), carry out the investigation, analyze logs and report the findings.

► PROPOSED SYSTEM

The first step is to do an analysis of how a third-party member gains access to a system for gathering evidence in a cloud environment and improvising skills to conduct better investigations. We will be performing log analysis (forensic technique) and how it is done within the container. The forensic analysis must be done in a cloud environment (Microsoft azure) that has already fallen victim to an attack.The first and foremost phase is information gathering to get the details of the incident and various attack methods that had been used by him. By getting gathered information, we can be able to deeply analyze and investigate containers on how the intruder(attacker) gained his access. After gaining access, how the attacker installs the program, what are the implications, research and analysis phase of this part. What attacker does in the host machine; report containing detailed findings from forensic analysis. We will be connected to a victim machine hosted on the azure platform before starting the analysis. Azure portal is a browser-based GUI to manage resources.

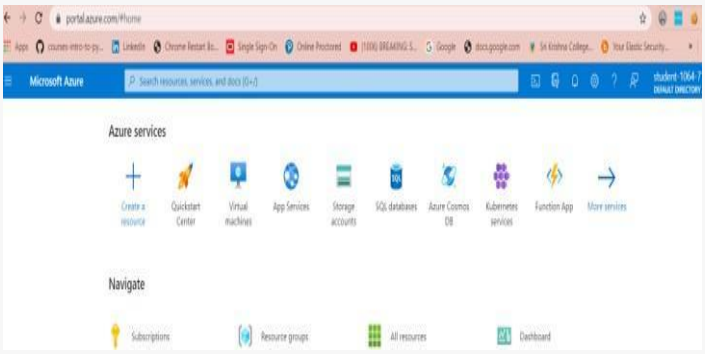


Fig. 1: Azure Portal

There are API, CLI but the portal is simple to follow. Before starting forensic analysis, we must connect RDP (Remote Desktop Protocol) enables remote connection for windows host to victim virtual machines running remote desktop service and want to go through some research to understand the system.

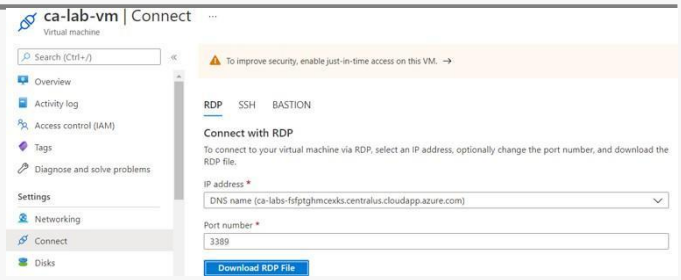


Fig. 2: Connect with RDP to analyze the victim machine

We were provided with sources of base docker containers, and one team member gave an installed source of the application. Analyze Docker container so that we need to search if there is any information on the page relevant to the vulnerability of container but the page gives info about Debian and details about the container, doesn't mention any security info, so this one will not be helpful for us to proceed.

Next, we can visit the Debian Linux Security forum [3] by going through that forum we could able to find reported vulnerabilities for Debian docker, issues in the bulletin had been resolved as of 18.09.1(solved in buster distro). So, the Debian container will be Debian Buster, whether likely that the attack source was a vulnerability in the container itself, but only security bulletin for Debian docker container fixed as Buster, where the container is running, so there will be no security vulnerabilities.

After that, we want to analyze an application that a team member had installed in a container which is DVWA (Damn Vulnerable Web Application) used to demo web vulnerabilities by providing an environment where we can exploit them. As it is a web application, the software will be outward-facing. By considering both application and container, the case is like a website that provides interfaces that are vulnerable and will be visible to the outside making somewhere a source of the attack. As an overall layer, we investigated the victim machine and narrowed down the attack source. We need to find the ID of the container and then the IP address of the container so that we can access websites hosted online.

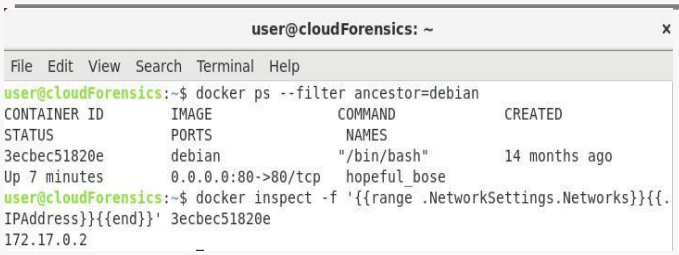


Fig. 3: Note ID and IP ADDRESS of Docker Container

Before we enter into the container need to access the application running on it by going to the IP found above followed by :80 in our web browser. The website will be presented with a login page so the team member informs that he left with default credentials as username and password is admin and password. We need to have look at the DVWA website, after a glance we can conclude that it is likely source of attack due to many vulnerabilities it presents and accessing is way easy.

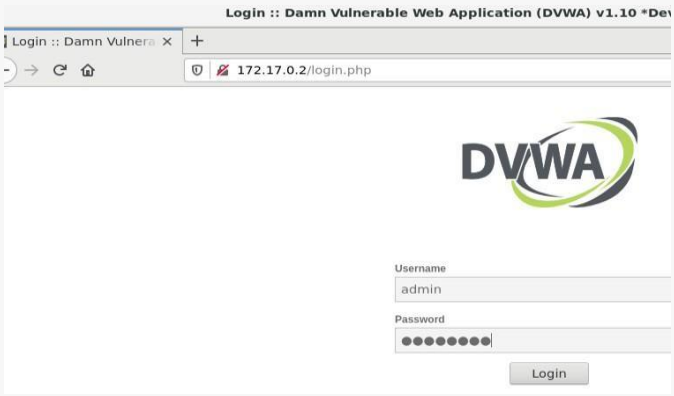


Fig. 4: Enter IP ADDRESS of Docker Container with port number 80, so we could able to view DVWA Application

Enter the terminal and use the necessary command to access the container and now we are in the container, open authorization logs. After entering the container, we could able to view the authorization log by cat /var/log/auth.log. Authorization logs are being used in digital forensics as it keeps track of all the actions done by users or systems that require authorization. This one will be very useful in an attack where the attacker has gained access to the machine, and it can be used to view how the attacker will gain access and some things that they did once they were on the platform. We can notice the auth attempt comes from a weird file.

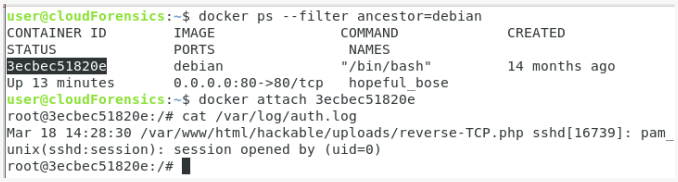


Fig. 5: Access the Container, Attach ID and open authorization log, able to notice reverse-TCP.php file(malicious).

We can visit the DVWA Application, the file came from file upload and extra information is like it will not be evident that burp suite was used by the attacker to confirm that file had been executed at least one time before it was received by the victim machine.

Fig. 6: : Malicious file will be injected in file upload option.

The attacker gained access by file uploading that triggered a reverse TCP connection to the machine, allowing him to remotely access the victim machine Command Line Interface. Till now, we analyzed container logs and were able to determine how the attacker gained access to the victim machine. After going through what the attacker did gaining access to CLI and must dig for info on which tools the attacker used, full-picture analysis to bring the full picture of the attack. We were not able to find interesting logs because the Virtual machine had no authorization restrictions, so only executing privileged commands will not generate authorization logs. There will be no authorization logs for users' actions because the Debian container doesn't have user restrictions because it is a very stripped version of Debian, so only one user account is there and no privilege occurred so nothing to generate requests of authorization by running just the commands. If the attacker hasn't cleaned the tracks, then it becomes simple to discover what he did once they were in this account. History command shows all the commands run by user unless it is cleared will be used to find what the attacker did in the account if he had not covered the track.

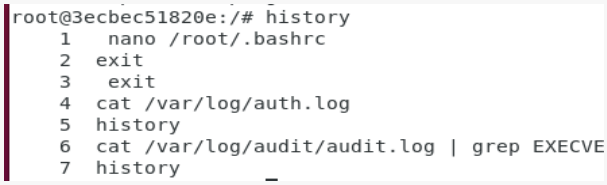


Fig. 7: History of commands ran by user

Audit log rules are set to record every command that runs, if the attacker had not caught on to this it will be simple to point out what he did. Audit logs are used most often in cloud forensics while default audit rules are useful, an additional set of rules can be set up to make audit logs track different information. In the addition to the audit rule to track “execve”, concern had made it so users’ actions are tracked in audit logs, something an attacker might not expect when track covering. Auth.log files contain lots of irrelevant logs so make use of command to get only execve type.

Fig.8: Audit logs of container

We now have logs for every command run on the machine, it would be not good to filter results further as the results are already filtered to commands run by compromised accounts so filtering further may filter away actions done by the attacker.

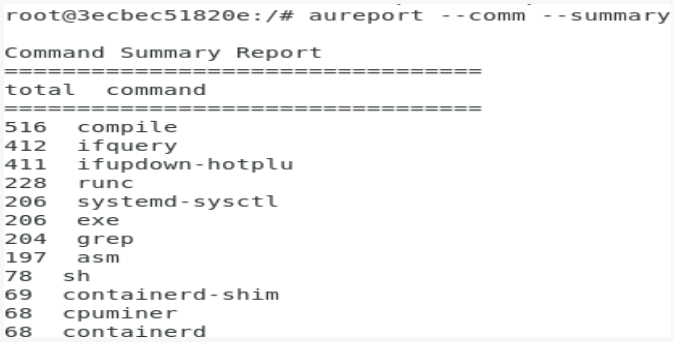


Fig.9: We can get a summary of unique commands regularly used to install programs.

The attacker had downloaded one program from GitHub(botb) and wanted to explore more to get some important information regarding the investigation and analysis part. This speaks about breakout the box that gives commands for executing exploits specific to containers. It is structured in a manner to break out of the container in the host machine. From our perspective, we can say it is dangerous because the attacker target will not only be the container but also the machine hosted. So automatically extending further analysis on the host machine is also required apart from the container. We did small research about the program that the attacker downloaded and ran on the victim machine.

Fig.10: Attacker had installed break out of box program in victim machine.

Some important artifacts (attacks) to be covered for the analysis phase will be as follows:

- The attacker used PHP file which has code for reverse-TCP Connection.
- Keeping the File Upload function in DVWA, the attacker manages to pull the file into the system.
- One of the team members left the webserver while he was not using it, and set a container firewall to allow external connections on port 80.
- Once in the system, the attacker installed a break out of box program to break out of the container to the host machine.
- The particular attack causes damage to the concern that owns the machine host and potentially to any other concerns that are hosted on the same machine.

We will figure out what the attacker did in the host machine and generate a report which breaks down what happened. Docker swarm is a docker service that allows for the management of certain types of containers and some containers only work with swarm enabled. This suggests that the attacker installed the container to be run on the host machine. While looking through authorization logs of the host machine, docker swarm create, docker swarm inits, docker service create must stand out to find exactly logs of docker. We analyzed logs in the ubuntu host and

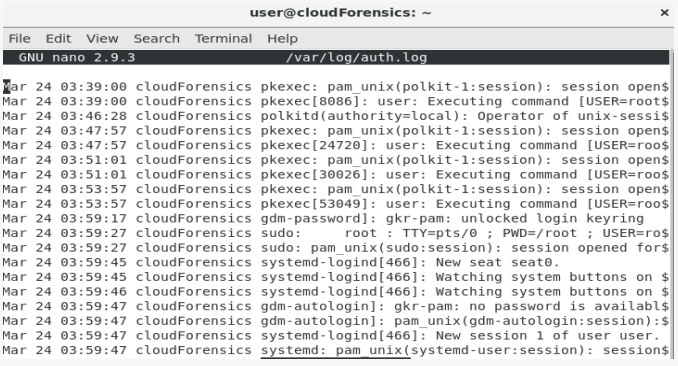


Fig.11: Authorization logs of victim machine

the attacker’s intent was to run containers on the host.
The next process is to investigate docker logs to try and identify the container since the auditd haven’t been installed on the host machine, so there are no audits to check.

Fig.12: Docker log details

In docker logs, check cpuminer and cryptonight. Logs containing the term cpuminer and cryptonight which is cryptomining algorithm indicate the intent of the attacker. This reinforces that the container is being used to steal compute-time from the cloud host for mining purposes. The other logs are network error messages which suggest that the attack is a failure as the container did not connect to the mining network.

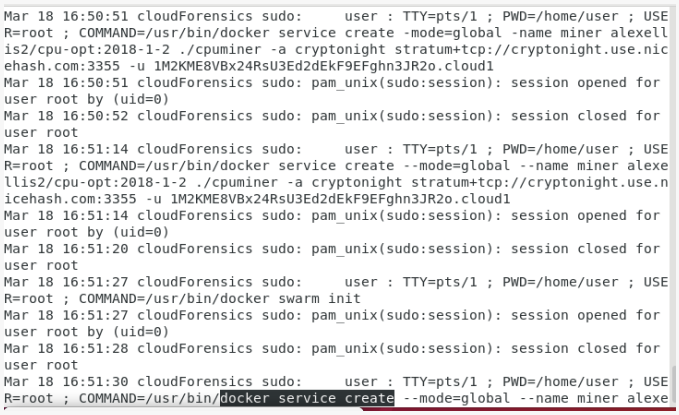


Fig.12: Docker log details

We had performed forensic analysis on the victim machine hosted on the azure platform and conducted an investigation for collecting evidences, traces, logs on how an attacker could have implemented an attack by using some strategies, tools loopholes in a container to achieve the goal and at last report findings had been provided for better understanding on how stuff did from initial to final.

► CONCLUSION

We had performed forensic analysis on the victim machine hosted on the azure platform and conducted an investigation for collecting evidences, traces, logs on how an attacker could have implemented an attack by using some strategies, tools loopholes in a container to achieve the goal and at last report findings had been provided for better understanding on how stuff did from initial to final.

► CONCLUSION

1) Sai Bharath S and Geethakumari G, "Cloud forensics: Evidence collection and preliminary analysis," 2015 IEEE International Advance Computing Conference (IACC), 2015, pp. 464-467, doi: 10.1109/IADCC.2015.7154751.

2) E. Morioka and M. S. Sharbaf, "Digital forensics research on cloud computing: An investigation of cloud forensics solutions," 2016 IEEE Symposium on Technologies for Homeland Security (HST), 2016, pp. 1-6, doi: 10.1109/THS.2016.7568909.

3) https://www.debian.org/security/2019/dsa-4521.en.html

4) Chandran, Ashwathi, and C. K. Shyamala. "Data management issues in cloud-integrated computing: A big picture." In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1-8. IEEE, 2017.

5) Srinivas, Sethuraman, Sreepriya Menon, and Kamalanathan Kandasamy. "Data-driven techniques for neutralizing authentication and integrity issues in the cloud." ARPN Journal of Engineering and Application Science 12, no. 12 (2017): 3914-3919.

DIGITAL 4N6 QUIZ

FEBRUARY'22 EDITION OF 4N6

Digital Forensics Scenarios -Based Quiz

Mr. Amrit Chhetri
Digital Forensics Analyst | Cyber Security Researcher | Security Coder | Cyber Forensics Psychologist | DFIR Researcher (Edge AI & QML)
amritchhetrib@gmail.com
https://www.linkedin.com/in/amritchhetrib

Experties :

Amrit Chhetri areas of interests and passions include Mentorships, Industrial Researches, Authoring Books and Lecturing in the fields of Cyber Security, Digital Forensics, Incident Response, Edge AI and Quantum Computing.

Credentials :

He is currently working as Cyber Security Consultant & CEI with Rosefinch (Siliguri) and engaged with My Cyber Hubs(MCH). He is also recognised an experienced Digital Forensic Instructor to LEA and Experts globally since 2014. He is also active Reviewer of Research Papers/Articles with great Journals- Elsevier(Global), GJFS, IEEE-ICRITO(AsU,India) & 4N6 (India). Known for accomplishing Reviews of 21 Research Papers in 30 Days!!

CONTEXTUAL FORENSIC SCENARIO

The Labs of ***Machine Learning Centre Of Excellence (MLCoE)*** of a well-known and award-winning Digital Forensic Start-up was attacked multiple times in the past with different Malware-based attacks. The first one was Ransomware Attack in 2021; second one was Mobile Malware, Joker in late 2021 and Advanced Persistent Attack (ATP) in early 2022. Recently, the organization had procedure Forensic Workstations and Appliances covered with Cyber Insurance and Device Insurance, both. But, the older systems were not covered by any kind of insurance.

In the context of Cyber Breaches, SOC Managers and CISO of the firm were called upon by CIO and further by the Executive Management Team to understand the breaches in detail, to strengthen the security practices further for future protection and to know the status of Investigations. Next day, SOC Manager asked his Forensic Expert, Miss. Avantika Sharma to collect maximum evidence from every corner- including Cyber Psychology facts.

NOTE: Almost all Forensic Tools, Methodologies and Steps are covered inside Articles of November and January Editions.

FORENSICS CTF-BASED QUIZZES

1. ***Quiz-1*:** Which of the following Open Source Reverse Engineering Tools, can Miss. Avantika used to analyse the .dlls accessed by the Ransomware?
    - **a. Ghidra**
    - b. SysAnalyzer
    - c. Process Explorer
    - d. OS Forensics

2. ***Quiz-2*:** To get Cyber Insurance Amount from the Insurance, the Team was asked to submit **ISO Certification** of their Labs. Which ISO Standard is applied to the Digital Forensic Lab. related to Sound Forensic Practices of Tools installed?
    a. ISO 27043
    b. ISO 27001
    c. ISO 27041
    d. ISO 12609

3. ***Quiz-3:*** During the Investigation, it is realized that one of the systems was compromised through DLL Injection using Metasploit. What Forensic Tool can she use to acquire the Memory Image that gives an open source image format?
    a. Autopsy
    b. FTK Imager
    c. Cyber Triage
    d. Magnet RAM Capture

4. ***Quiz-4:*** Miss Avantika acquired NTLM Hashes loaded into Memory by the Malware and tried to decode to get the plain-text values. Which is the best one under Sound Digital Forensic Practices?
    a. Cain And Abel
    b. Hydra
    c. Passware Kit Forensic
    d. Hashcat

5. ***Quiz-5:*** In Internal Meeting, it was pointed out that some of Credentials/Security Codes were hijacked through Brain-Mapping and proving it in the court is not easy as Forensic Systems is not well established in this domain? Which of the following Brain Imaging Techniques can be suitable in reading acceptable evidences from the suspects in this scenario?
    a. FMRI
    b. Traditional Neuro-Imaging
    c. Functional Near-Infrared Spectroscopy (fNIRS)
    d. Polygraph

https://doi.org/10.46293/4n6/2022.05.01.02
Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

DIGITAL 4N6 ANALYSIS

WHERE DID THIS CHAT COME FROM? THE 'ORIGIN PATH' CONCEPT IN BELKASOFT X

HIGHLIGHTS

This article mainly accentuates a forensic investigation performed on remotely hosted docker container. It also discusses steps followed for performing the forensic investigation and the different tools which have been used.
– Editorial Team, Digital Forensics (4N6)

Yuri Gubanov
Belkasoft Founder and CEO
yug@belkasoft.com
https://www.linkedin.com/in/yurigubanov/

Expertise:
Yuri Gubanov is a renowned digital forensics expert. He is a frequent speaker at industry-known conferences such as HTCIA, EnFuse/CEIC, FT-Day, CAC, CACP, ICDDF, and others. Yuri is the Founder and CEO of Belkasoft, the manufacturer of digital forensic software empowering police departments in more than 130 countries. With years of experience in the digital forensics and security domain, Yuri led forensic training courses for multiple law enforcement departments in several countries.

► ABSTRACT

The The 'push button forensics' is a sarcastic term for the job DFIR specialists perform when they use DFIR tools, which extract various useful data out of the box, alleviating the manual extraction of many different types of artifacts. While there is room for sarcasm, the automatic extraction of artifacts is not necessarily evil. Given the volume of data which modern devices can store, an investigator or examiner cannot efficiently analyze everything manually. This means some reasonable level of automation is a 'must have'.

The problem that arises is when this automation is used blindly without challenging the obtained results and without cross-checking them with other tools' output, or by manual examination. This may lead to a situation when one's results are challenged later—by a counterparty.

It is worth mentioning that some digital forensic tools on the market provoke using the tools blindly. Such tools work as a black box and give results without explanations of how the artifacts were obtained. No surprise, that conclusions based on such results will not withstand in court if challenged by a knowledgeable counterparty. A question as simple as: 'How was this deleted chat restored by "Software A"?', could appear extremely difficult to answer, if "Software A" is a black box for you.

In this article, we will review a healthier approach to the automatic extraction of artifacts for a digital forensic or an incident response case.

► THE ORIGIN PATH CONCEPT WITHIN BELKASOFT X EXPLAINED

'Origin path' is a property that every artifact has in Belkasoft X; Belkasoft's flagship product for a computer, mobile and cloud forensics. This property aids the examiner by allowing them to understand where an artifact came from. Every chat, URL, document, picture, registry key, email, etc., have this property.

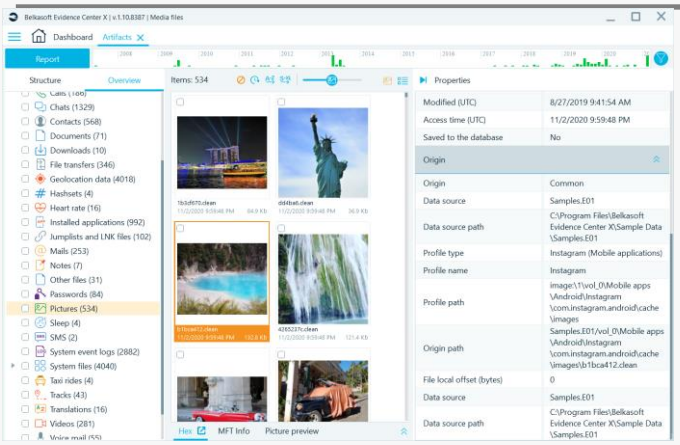


Fig.1: Properties pane

While simple artifacts such as a document parsed from an existing file, will likely not cause any issues, the following situations may bring some difficulties:

- Deleted chat or URL. How can you prove that they existed? Can you show where they were recovered from? Can you repeat this manually?
- Embedded picture. Where did this picture come from?
- Email attachment. Which email was it attached to?
- Any carved artifacts

To illustrate how Belkasoft X's Origin path can help, let us review the first situation: a chat recovered from the Skype application. Here is an example of an Origin path, that a Skype chat can have:

```
'image.e01//C:\Users\Smith\AppData\Roaming\Skype\smith48\main.db//Messages\Freelist'
```

You can see that this chat originated from an image 'image.e01'. This is the first part of the Origin path, and it always ends with a double slash.The path to a profile, which is the second part of the Origin path value,

is `'C:\Users\Smith\AppData\Roaming\Skype\smith48\main.db'`. This is where the Skype data is stored for this particular profile (smith48).

Finally, after the second double slash, we can see the table name, as well as a special area inside the table, is mentioned too. This particular chat was extracted from the 'freelist' area from the Messages table inside the SQLite database 'main.db' (main Skype database file).

Note: you can learn more on freelists, write-ahead logs and SQLite journal files at https://belkasoft.com/sqlite-analysis

Now you have all the knowledge of where to find the artifact manually if needed. Well, almost all.

Next to the Origin path, you will also see an offset inside the file (for artifacts recovered in a file) or an offset from the beginning of a partition (for carved artifacts). With this information, you will be able to accurately explain where an artifact originated from, and also how to manually validate the product interpretation of raw data by using a built-in Hex viewer or a third-party tool.

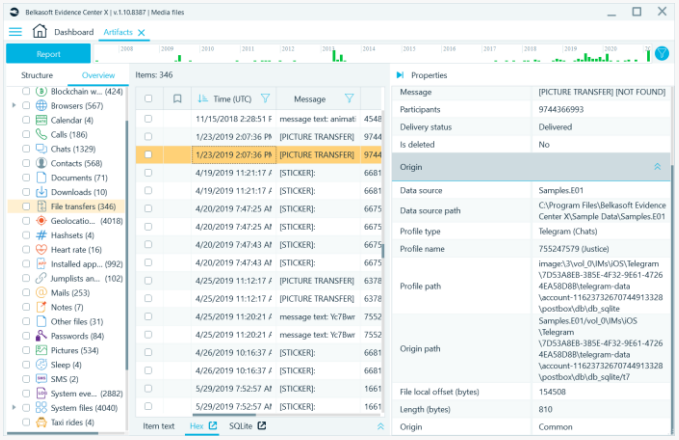


Fig.2: File local offset on the Properties pane

► REVIEWING ARTIFACTS ON A DATABASE AND AT THE RAW BYTE LEVEL

One of the benefits of using Belkasoft X as your digital forensic tool of choice is that it helps you to understand how and where artifacts were extracted from, on a few different levels.

►THE INTERPRETED LEVEL

You can see artifacts such as chats, URLs, pictures, registry data and so on in the artifact list on the Artifacts window. All values are fully interpreted, including date and time stamps, decoded or decrypted texts, message directions and more. You can rely on this information, unless you have doubts or a complicated situation when you need to double-check the interpretation.

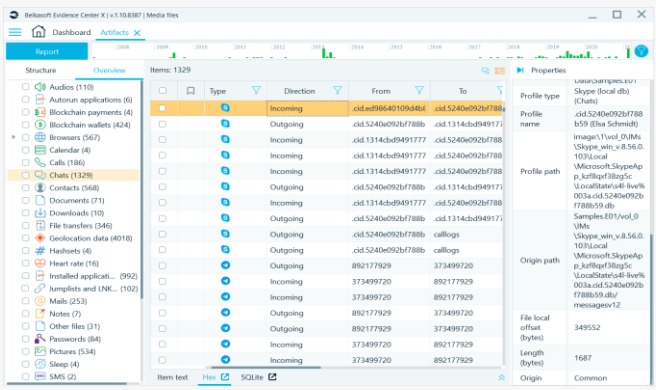


Fig.3: Chats as shown on the Artifacts window

▶ THE DATABASE LEVEL

On this level, you can see particular artifact data as it is stored logically within a database or another file, such as a plist or a registry file. For example, when you click on an artifact, which is stored inside of an SQLite database, Belkasoft X will show you a separate SQLite viewer tab below the artifact list (in the so-called 'Tools' area). This tab will conveniently show the corresponding SQLite table and row selected.

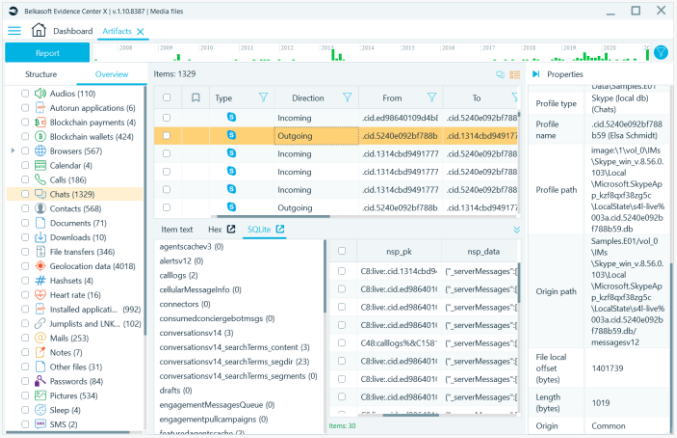


Fig.4: SQLite Viewer tab

You can click on the 'Expand' icon to open a full-size SQLite Viewer.

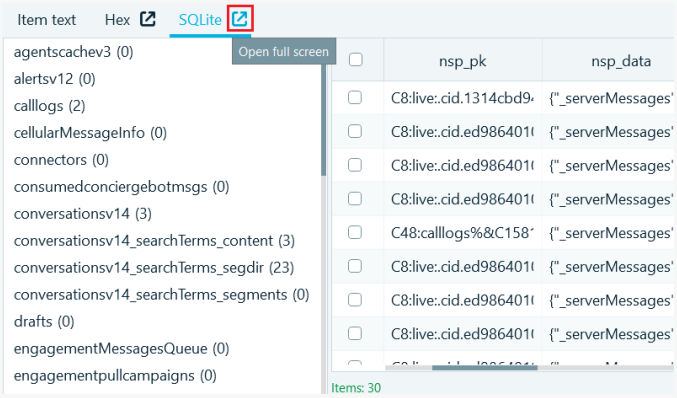


Fig.5: Full screen button to open SQLite Viewer

At the database level, you may expect to see certain types of data that are not interpreted. Particularly, date and time stamps may be in Unix format, while texts can be in ASCII, not UTF. Belkasoft's SQLite Viewer allows for changing the format of the date and time for integer columns and encoding for text columns.

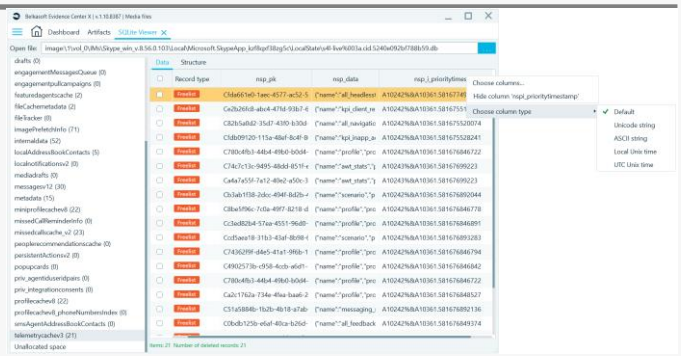


Fig.6: You can choose the date and time format

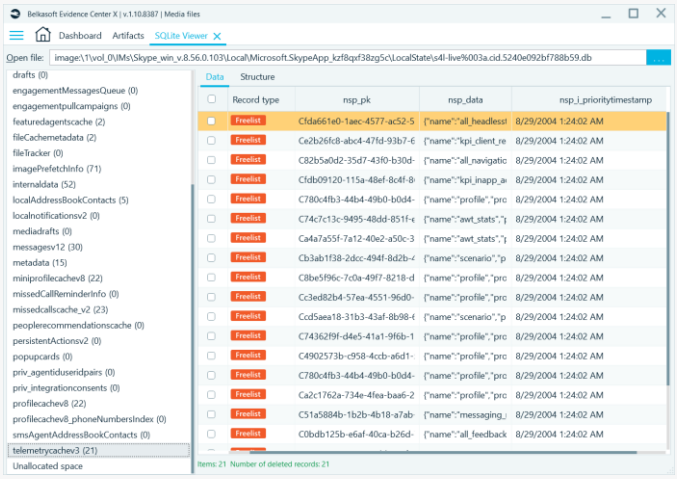


Fig.7: Time stamp converted to UTC Unix time

▶ THE RAW BYTE LEVEL

On this level, you can see particular artifact data as it is stored on the hard drive or other media. Every artifact has its own offset and length, which enables you to review its original binary data. Belkasoft's Hex Viewer tab shown in the Tools region of Belkasoft X, conveniently shows a selected artifact's raw bytes. It highlights the entire portion of bytes that belong to the artifact, which enables you to copy these bytes and interpret them manually or by using any other third-party tool.

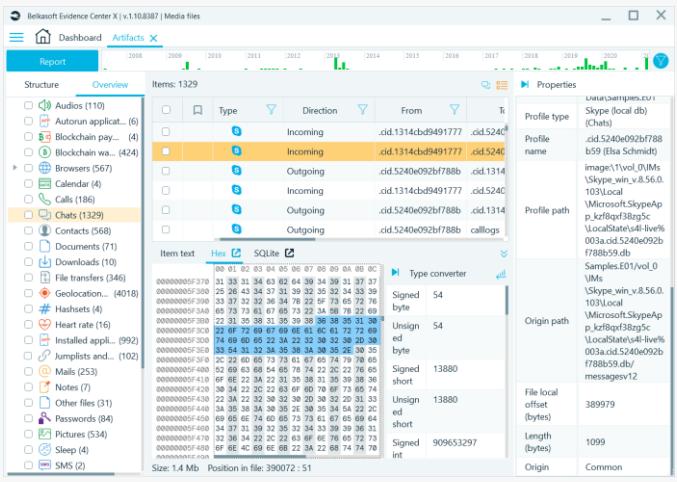
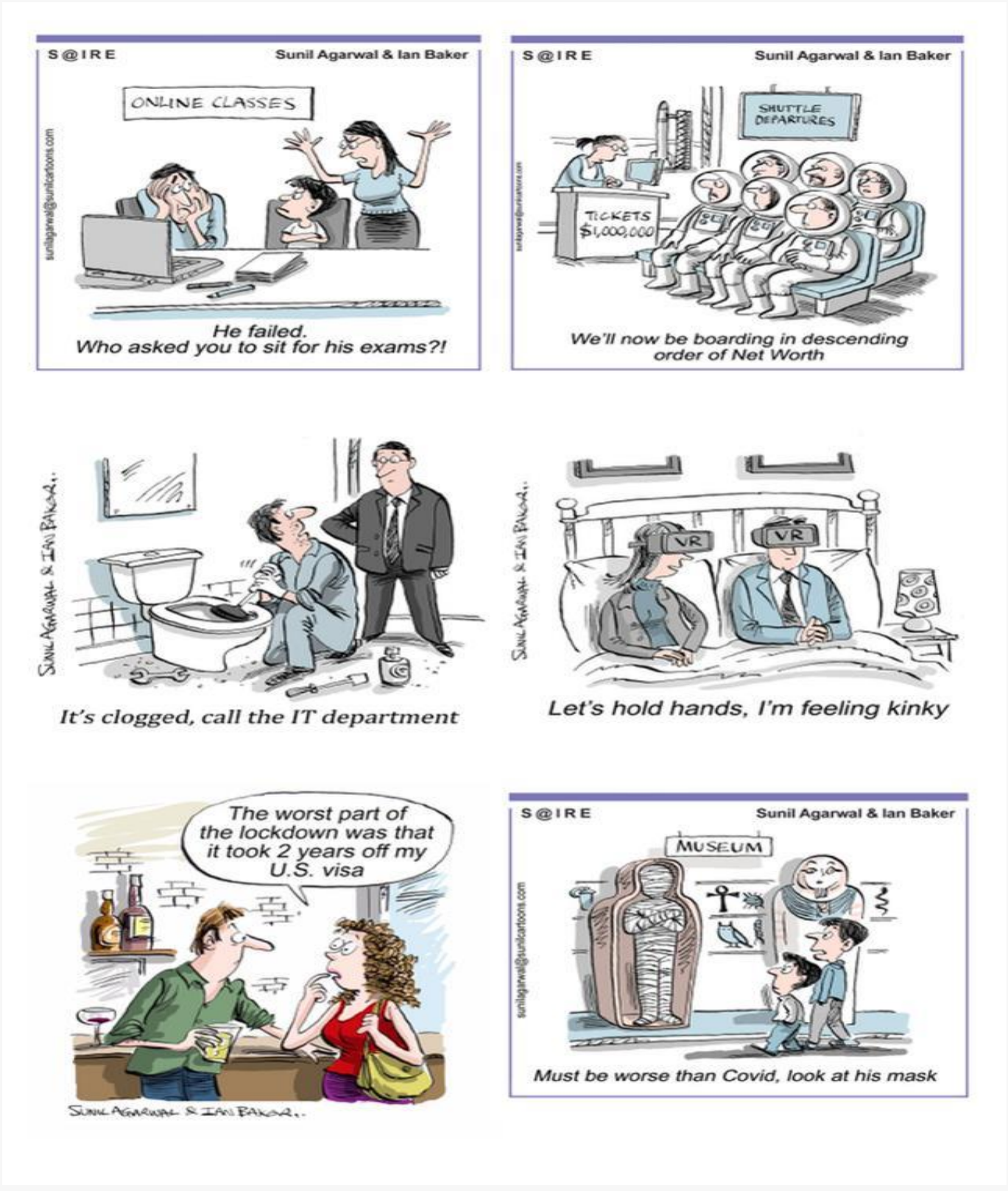


Fig.8: Hex Viewer tab

Just like with the SQLite tab, you can open a full-size Hex Viewer by clicking on the ‘Expand’ icon.

▶ CONCLUSION

As a digital forensic investigator or an incident responder, you must be ready to answer the question of 'How did your tool obtain a particular artifact?'. To assist with answering this question, Belkasoft introduced the Origin path property within the Belkasoft X product. Using this property, you can give exhaustive replies to such questions.



https://doi.org/10.46293/4n6/2022.05.01.03

Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

DIGITAL 4N6 ANALYSIS

OSINT FOR CRYPTOCURRENCY FORENSICS

HIGHLIGHTS

This article mainly accentuates a forensic investigation performed on remotely hosted docker container. It also discusses steps followed for performing the forensic investigation and the different tools which have been used.

– Editorial Team, Digital Forensics (4N6)

Pillai Anjali AnilKumar

Pillai Anjali AnilKumar is pursuing her M.Tech in Cyber Security at Amrita Vishwa Vidyapeetham, Coimbatore, India. She is working as a Cyber Security intern at Philips Innovation Campus, Bengaluru. Her areas of interest include network security and cyber forensics.

Email : cb.en.p2cys20023@cb.students.amrita.edu

Anirudh Srinivas Balaji

Anirudh Srinivas Balaji is pursuing his M.Tech in Cyber Security at Amrita Vishwa Vidyapeetham, Coimbatore, India. He is working as a Graduate Intern in the Netwitness(SIEM) Engineering Team at RSA Security. He is passionate about red teaming, SecOps and cyber forensics.

Email : cb.en.p2cys20006@cb.students.amrita.edu

► ABSTRACT

OSINT commonly known as Open-Source Intelligence involves gathering publicly available data from the internet to support reconnaissance. Most cyber threat intelligence specialists expand that term to include information aimed at the general public. Due to the sudden surge of cryptocurrencies in today's world, there are lots of scams happening around it. However, to carry out cryptocurrency forensics there are no proper guidelines, frameworks and open-source tools. Our work aims to create a standardized open-source framework to analyze a given Transaction ID/Wallet ID of any cryptocurrency.

► INTRODUCTION TO BLOCKCHAIN TECHNOLOGY

A blockchain is a decentralized ledger of transactions that is emulated and shared across the various peers in the network. Every block stores the number of transactions that took place and whenever a new transaction is being carried out, a record of that transaction is incorporated into each peer's ledger

[1]. Figure 1, illustrates the Distributed Ledger Technology (DLT), which relates to a decentralized platform controlled by different parties. Blockchain incorporates DLT in which transactions are saved in a hash format. If one block in the chain had been changed, it would be clearly evident that it was tampered.

As blocks are added to the blockchain, the security of the ledger increases greatly which indeed makes bitcoin and Ethereum grow further.

Countries have produced a wide range of DLT applications in order to improve the governmental services to the general public. Government agencies are incorporating this technology to optimize the management and control of consumer data in both public and private sectors.

Because of its successful implementation in cryptocurrencies, blockchain is famous across the globe [2].

► CRYPTOCURRENCY MINING AND ITS PROBLEMS

Bitcoin was created in 2008 by Satoshi Nakamoto as a cryptocurrency derived from blockchain technology. The Bitcoin ecosystem envisaged by Nakamoto is made up of a network of users who communicate with one another over the Internet using the open-source bitcoin protocol. Bitcoin's use becomes highly appealing because of its approximately zero transaction costs for larger transactions, lack of traceability, and potential anonymity. Because of the devolution of blockchain, cryptocurrency's influence has grown in recent years. Although Bitcoin and Ethereum are popular, there are more than five thousand different cryptocurrencies being used.

Mining refers to the process in which group of computers generate and distribute new bitcoins while also validating new transactions. Nodes or mining rigs validate the blockchain transactions for a particular cryptocurrency coin in exchange for a mining payout is known as cryptocurrency mining. Miners compete to prove their computational work in exchange for a block reward in cryptocurrency mining. After a sequence of transactions for a certain cryptocurrency, the blockchain's P2P network sees a block with accompanying cryptographic hash functions holding transaction data. Competing pools of nodes employ their high-performance computing capabilities to solve a hard mathematical problem and validate the block's integrity [3]. There are various types based on storage, connectivity and node type. Client-based wallets - installed as an application on the system (eg. Bitcoin Core); Web-based wallet - accessed on the web browser (eg. Brave); In-browser wallet - which comes as a plugin (eg. Metamask); Hardware wallet - an isolated way of storing the private key (eg. Trezor); finally, the traditional paper wallet, nothing but writing our private key in a paper and keeping it secure.

The mining party secures the blockchain addition and earns the mining reward for allocating the pool after successfully demonstrating the block's validity.

However, the most frequently mentioned disadvantage of cryptocurrency mining is the amount of energy consumed while mining cryptocurrency, as well as the hardware costs. We've seen that the crypto market is occasionally rife with scams and frauds, which can cause instability in the future.

► INTRODUCTION TO OSINT

OSINT is mainly used by law enforcement agencies and business intelligence groups to gather insights into criminals. It is useful for analysts who are using non-sensitive intelligence to answer categorized, unstructured, or private information requirements throughout all the intelligence areas.

From Figure 2, OSINT sources can be classified into a variety of information flow categories [4]:

- Media - From all across the globe, comprising print newspapers, magazines, radio, and television.

- Internet - Online periodicals, blogs, discussion forums, citizen media (such as mobile phone videos and user-generated material), YouTube, and other social media websites (such as Facebook, Twitter, Instagram, and so on). Because of its timeliness and accessibility, this source also beats a plethora of other sources.

- Public government data - Data from the government, budgets, hearings, telephone directories, press events, websites, and speeches are all available. Regardless of the fact that this source is from an official statement, it is accessible online and may be used freely.

- Professional and academic publications - Information from conferences, seminars, dissertations, as well as professional and academic journals.

- Commercial data - Databases, commercial imaging, financial and industrial assessments.

- Grey literature - Technical reports, preprints, patents and some unpublished works.

Manual research and checking up on the target subjects, including non-technical sources such as an organization's financial report, revenue filings, related news stories, and information on its web pages, YouTube and similar services, are mainly used.

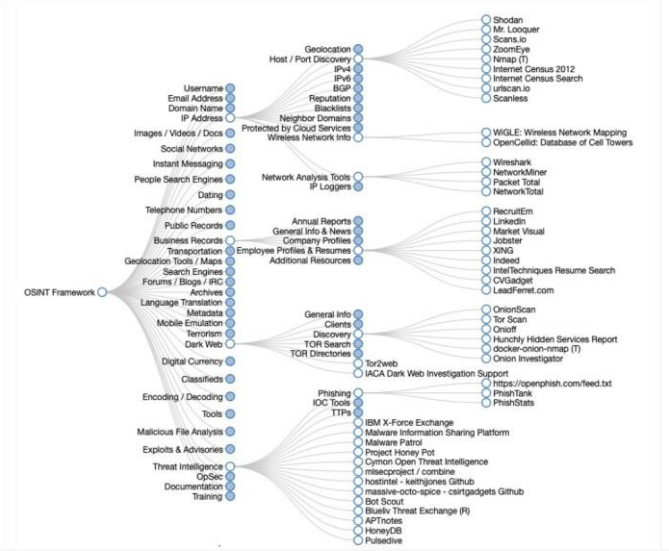


Fig. 1: OSINT FRAMEWORK

► NEED FOR OSINT IN CRYPTOCURRENCY FORENSICS:

The most fundamental framework of any forensic investigation consists of identifying a target, searching for information about them, identifying the target's associates, and then searching for information about them. Cryptocurrencies were a natural fit for our inquiry. Due to an increasing reliance on cryptographic protection and a decentralised P2P system, cryptocurrency has become the preferred means of exchange for cybercriminals and those seeking to avoid the restrictions of traditional banking. Money ownership is tacitly pseudonymous, while its flow is publicly accessible and perceptible.

Additional open-source intelligence tools, such as OSINT-SPY, Maltego, Recon-NG, theHarvester, FOCA and so on, can be used as part of investigations to uncover linked emails, locations, social media sources and other pertinent information.

►PROBLEM STATEMENT

As we saw earlier, there is still a huge research gap that exists in the blockchain technology and cryptocurrency market due to the underlying flaws and since cryptocurrencies are decentralized, attackers tend to use them in an illegal way as well. One such example is the “U.S capitol attack” in 2020 that was carried out right after Donald trump lost his election. One of his supporters named Nick Fuentes obtained 13.5 BTC, which was apparently worth $250,000 at the period of the transfer, making him the highest beneficiary of the donation as an outcome of this attack. The extremist sponsor bankrolled his donation wallet with the cryptocurrency from a French swap, which he transferred to the donation wallet into a third-party wallet which we name the "Extremist Legacy Wallet [5].”

Due to many such crimes happening across the world with the illegal usage of cryptocurrencies, there is a need amongst cyber forensic investigators to focus more on cryptocurrency forensics which enables them to use OSINT to trace and hunt down the attackers who are doing organized crime activities [7].

► LITERATURE SURVEY

Figure 3 illustrates the workflow of blockchain technology, which has become one of the most popular technologies deployed in various sectors as applications by a variety of developed businesses and organisations. The main reason for this popularity is security, because distributed ledger technology stores multiple redundant and identical copies of the same ledger globally, and if one of the accounts is compromised, many others exist as backups that can provide breached data or funds in the compromised account. The use of strict cryptographic methodologies to prevent data alteration or modification attracts the deployment of blockchain technology in various sectors.

As previously stated, companies rely on blockchain technologies for data security and reliability. Cryptocurrency mining is a significant source of revenue for cryptocurrency miners, as well as owners and third parties who participate in the blockchain market with their individual systems. According to Trend Micro's research, there are more than 700 cryptocurrencies in the market that are based on blockchain technology. Attackers use Open-Source Intelligence (OSINT) techniques to gather information about the vulnerabilities of miners, users, and exchanges, as well as a variety of attacks to mint illegal money [6]. Because bitcoin mining is so popular, attackers have focused on developing new attack vectors that target bitcoin miners and bitcoin-related transactions. Blockchain transactions can be processed using digital wallets created by parities. These digital wallets use a "multi-signature" security mechanism, which is an authorization framework for digital currency exchange. A transaction must be signed by another user before it can be added to the blockchain using multi-signature.

By exploiting a vulnerability in multi-signature wallets, attackers targeted Ethereum cryptocurrency and stole 153,000 ether tokens (worth $32.6 million USD).

Because all of these attacks were caused by a lack of network or an improper configuration, researchers developed a variety of network-based technologies and they are still focusing on a variety of aspects to resolve security-related issues in order to secure the communication environment. The proposed mechanisms and models provided a variety of solutions for various types of communication infrastructures as well as protection against various types of vulnerabilities from various perspectives such as link encryption, end-to-end encryption, and message encryption.

Cryptocurrency miners have grown in popularity as the demand for and price of cryptocurrencies such as Bitcoin and Ethereum has increased. Bitcoin mining, also known as cryptocurrency mining, is the process of coordinating transactions in a network of computers, with miners earning a profit based on the cost of mining, which is increasing in terms of a cryptocurrency over time. When a blockchain participant wants to conduct a transaction, the proposed transaction is generated using a specific consensus (Proof of Work, Proof of Stake, and so on) and distributed to the network of nodes for validation. The verified transaction is combined with other transactions to form a new data block for the ledger.

In blockchain technology, transactions are recorded in each block, and these blocks are identified by hash codes. To be added to the blockchain, a block must be validated, which is done by the participating users known as "miners."

OSINT is an important intelligence technology that derives intelligence from publicly available information sources. Global media, web blogs, academic papers, Wikipedia, YouTube, social media (Twitter, Facebook, Instagram), government reports, satellite images, and all other information available to the public on the Internet are examples of these sources. The Internet is the primary source of information for OSINT, with estimates ranging from 4.4 zettabytes (ZB) in 2013 to 44ZB by 2020[9].

The Internet serves as a conduit for accessing information sources, and also the rapid growth of this volumetric data demands the use of unique discovery, search, and retrieval techniques to precisely examine this data.

Because of the humongous amount of data and information available on the Internet, attackers can collect information to understand operating principles, architecture, features and communication infrastructure, revealing the system's vulnerabilities. With today's OSINT tools, criminals can organise more sophisticated attacks.

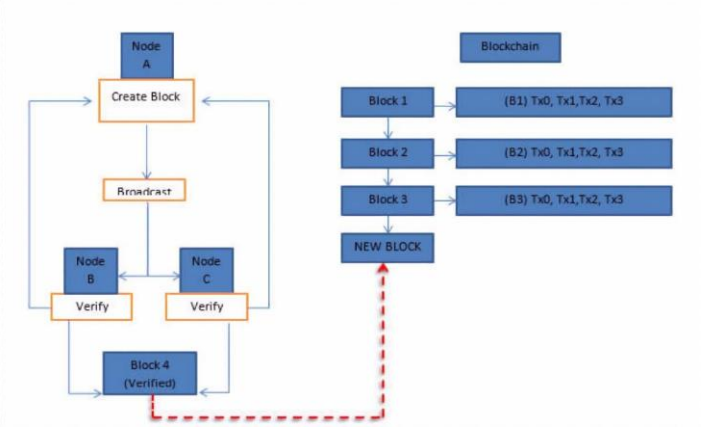


Figure 2: Blockchain Workflow

The "Antminer S9," one of the most popular bitcoin miners, is chosen for testing purposes. The AntMiner configuration page allows an attacker to alter the miner's configuration. This miner's characteristics are depicted below:

- The miner's hardware runs a "Lighttpd/1.4.32 web server, with SSH ports for remote communication. There is an exploit for "Lighthttpd 1.4.31 but it does not allow remote access to the server because the exploit has been patched in the newly released version [8].
- "Digest Authentication" is used on the AntMiner configuration page. The Digest authentication method is an "agreed-upon" authentication method. The web server negotiates the credentials with the client's web browser using this method.
- This authentication method employs MD5 cryptographic hashing in conjunction with nonce values to prevent replay attacks.
- Another type of miner proposed for Ethereum mining is the Ethereum-Claymore miner. The new dork proposed exposing the list of available miners using

OSINT techniques. There are many cryptocurrency miners on the Internet, and their IP addresses are exposed to the public via the OSINT technique with the help of specific queries and dorks. Once you know the IP address of the miner server, you can use the Claymore Remote Manager API to manage it remotely. The miner's configuration file can be modified by transferring remote JSON packages.

OSINT is used by existing paid tools such as Bitcoin Ant miner and Ethereum Claymore to gather critical information about miners, such as exposing the target's vulnerabilities. With this information, attackers can exploit a vulnerability in the miner's configuration file to obtain sensitive information from it.

► RESEARCH GAP

- Tools such as Bitcoin Ant miner and Ethereum claymore are paid tools and not all agencies/individuals will be able to afford them to carry out their forensic investigation.
- There are no proper guidelines and frameworks to perform cryptocurrency forensics.

► PROPOSED SYSTEM

We took a python tool named OSINT-SPY as our base tool that performs a recon on the email addresses/domain addresses/IP addresses/organizations to collect some important information about the target which could be used as a lead for the investigation.

It is used by Information security researchers, Penetration testers and cyber-crime investigators to know more information about the targets. It works by integrating the following API keys such as Email Hunter, Shodan, Clearbit, Full Account and Virus Total [10].

As shown in figure 3, with OSINT-SPY as the base tool, we developed two python-based tools in which the first one automates the process of gathering transaction details, domain links, email addresses by giving user input as the date and the other one takes wallet ID as input and gathers the tweets related to the bitcoin addresses.

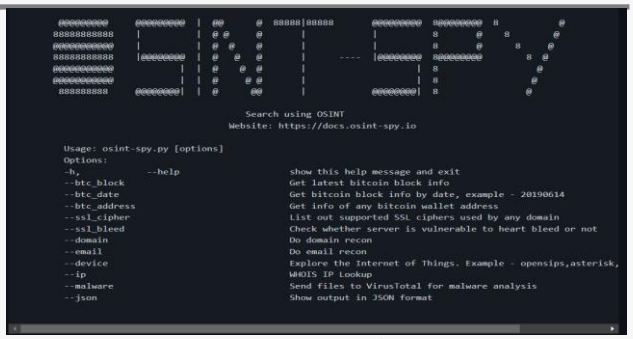


Figure 3: OSINT-SPY flags

To find the owner and the persons behind a particular mining website, we developed a bash tool that performs NMAP scan on all the collected domains and performs Whois lookup on all the collected domains. The first python tool named bitcoin OSINT scanner takes user input as the date and fetches information such as nonce, hash, previous block hash, next block hash, pool name, pool links and more.

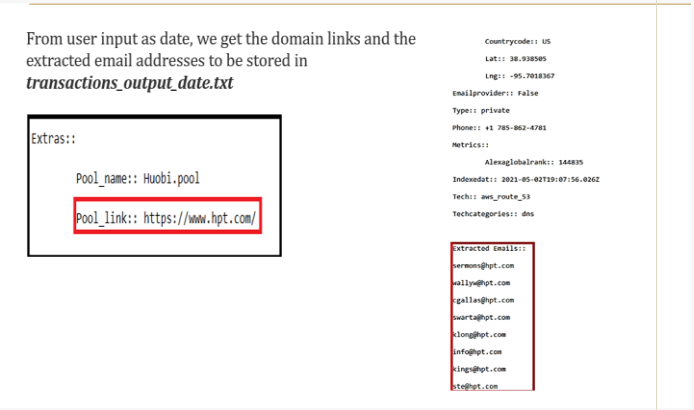


Figure 4: : Bitcoin OSINT Scanner

Once we get the pool links which are nothing but the URLs of the miners, we scrape only the pool links and perform recon to obtain the company's information such as location, social media handles and funding information of the company. From the collected chunks of these details, we scrape only the email addresses corresponding to the organizations and save them in a separate file text file. From the email recon flag, it identifies the personal details with the respective emails and stores them in separate text files. The outputs of this tool are shown in figure 5 and figure 6.

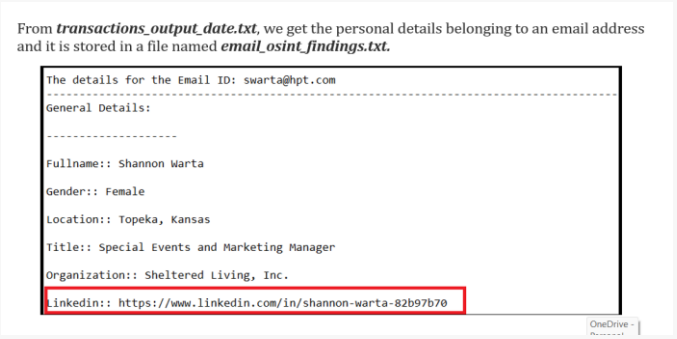


Figure 5: Email OSINT findings

Forensic investigators can run this tool continuously in a VPS (Virtual Private Server) to check on a miner that they suspect to be looting illegal money and identify the transactions and the persons involved in the act. The bitcoin OSINT SM tweet tool shown in figure 6, takes user input as Bitcoin wallet ID and fetches tweets related to the given address ID in the form of an URL which can be used to find or suspect a person behind a transaction that has been carried out. The outputs are logged into a separate text file.

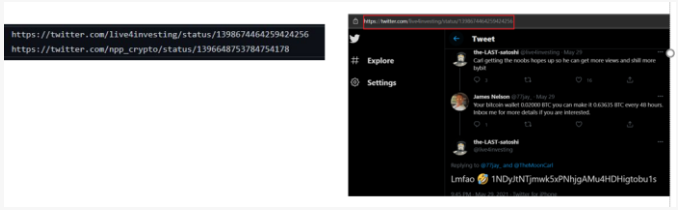


Figure 6: Bitcoin OSINT SM tweet tool

The bash tool which is shown in figure 7, named bitcoin OSINT scanner also takes user input as the date and collects all the URLs with the help of user input and removes all the duplicate links. It performs a NMAP scan on all the URLs to identify if there are any open ports and other services running on the target that helps forensic investigators to try and exploit to gather some sensitive information on the target. Finally, it also performs Whois lookup on all the URLs and identifies who owns the particular domain which can be helpful in identifying the administrator or owner of a particular mining website. The results can be seen in figure 8 below.

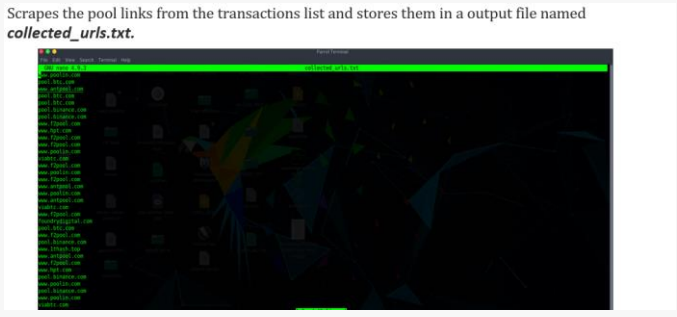


Figure 7: : Bitcoin OSINT scanner

Figure 8: : NMAP scan and whois lookup on all the filtered URLs(miners).

► CONCLUSION

With RBI envisioning to roll out digital currencies in 2023, cryptocurrency demand across a hugely populated country like India will tend to increase day by day and black-hat hackers will definitely have an eye on luring people to cryptocurrency scams, thereby increasing the need for cyber forensic investigators to carry out cryptocurrency forensics for tracing out the criminals who are responsible for minting illegal cryptocurrencies.

► REFERENCES

[1] Ramaguru R., Sindhu M., Sethumadhavan M. (2019) Blockchain for the Internet of Vehicles. In: Singh M., Gupta P., Tyagi V., Flusser J., Ören T., Kashyap R. (eds) Advances in Computing and Data Sciences. ICACDS 2019. Communications in Computer and Information Science, Vol. 1045. pp. 412-423. Springer, Singapore.

[2] DLT - https://phemex.com/academy/what-is-distributed-ledger-technology-dlt (Last Accessed On: Jan 2022)

[3] Minu M, Ramaguru R. நம்Chain: Crypto Wallets: (2020) Comprehensive View. Retrieved from https://namchain.blogspot.com/p/crypto-wallets.html

[4] Portswigger – How is OSINT used –

https://portswigger.net/daily-swig/osint-what-is-open-source-intelligence-and-how-is-it-used - (Last Accessed On: Jan 2022)

[5] Capitol riot attack - https://blog.chainalysis.com/reports/capitol-riot-bitcoin-donation-alt-right-domestic-extremism/ - (Last Accessed On: Jan 2022)

[6] Kalpakis, G., Tsikrika, T., Cunningham, N., Iliou, C., Vrochidis, S., Middleton, J., & Kompatsiaris, I. (2016). OSINT and the Dark Web. In Open-Source Intelligence Investigation (pp. 111-132). Springer, Cham.

[7] Tziakouris, G. (2018). Cryptocurrencies—a forensic challenge or opportunity for law enforcement? Interpol perspective. IEEE Security & Privacy, 16(4), 92-94.

[8] Sari, A., & Kilic, S. (2017). Exploiting cryptocurrency miners with osint techniques. Transactions on Networks and Communications, 5(6), 62.

[9] OSINT - https://www.sentinelone.com/cybersecurity-101/open-source-intelligence-osint/ (Last Accessed On: Jan 2022)

[10] OSINT-SPY TOOL - https://github.com/SharadKumar97/OSINT-SPY (Last Accessed On: June 2021

https://doi.org/10.46293/4n6/2022.05.01.04

Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

INFORMATION SECURITY

A PRIMER ON DCSYNC ATTACK AND DETECTION

HIGHLIGHTS

In this research article the author has shared different methods for the DCSync attack and it's detections. the article covers different system configurations and policies required to detect and response to the attacks..

– Editorial Team, Digital Forensics (4N6)

Chirag Salva

Chirag Savla is an information security professional whose areas of interest include penetration testing, red teaming, azure, active directory security, and post-exploitation research. He has over 7+ years of experience in information security. Chirag likes to research new attack methodologies and create open-source tools that can be used during the red team assessments. He has worked extensively on Azure, Active Directory attacks, defense, and bypassing detection mechanisms. He is the author of multiple Open-Source tools such as Process Injection, Callidus, etc. He has spoken at multiple conferences and local meetups.

► INTRODUCTION

Active directory is a backbone of almost all the organizations. It helps the IT team to manage the systems, users, policies etc, centrally across the complete network. Since it is an integral part of the organization, it opens multiple opportunities for the attackers to leverage the features of the active directory and abuse them with malicious intent. We will look at one such feature known as Active Directory Replication in this post. In this post, we will look at a few approaches that we can use to detect the DCSync attack and gain understand about the attack. DCSync attack and detection are already explained by Sean Metcalf & Will Schroeder in their blog post.

► ABOUT ACTIVE DIRECTORY REPLICATION

Domain Controllers (DC) are the pillars of Active Directory (AD) environments. Organizations often have multiple Domain Controllers for their Active Directory as a backup or they have different Domain Controllers for each location so that the authentication and other policies can be made available locally on the site location. Now as there are multiple Domain Controllers in the organization every Domain Controller must be aware of every change made in the environment. These changes are synced with each Domain Controller via Microsoft Directory Replication Service Remote Protocol (MS-DRSR). AD uses several counters and tables to ensure that every DC has the most current information for each attribute and object and to prevent any endless replication loops. AD uses naming contexts (NCs), also known as directory partitions, to segment replication. Every forest has a minimum of three NCs: the domain NC, the configuration NC, and the schema NC. AD also supports special NCs, often known as application partitions or non-domain naming contexts (NDNCs). DNS uses NDNCs (e.g., DomainDnsZones, ForestDnsZones). Each NC or NDNC replicates independently of one another.

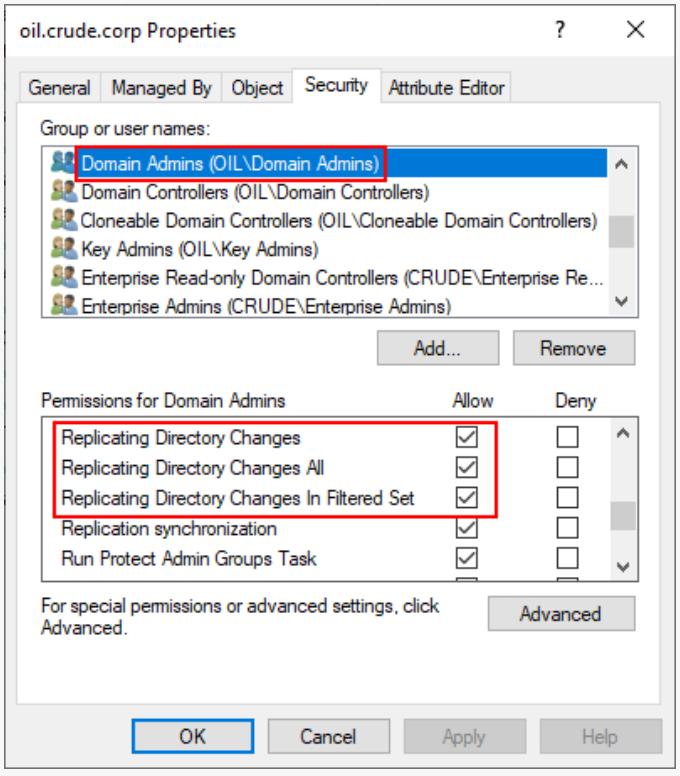
ABOUT DCSYNC ATTACK

DCSync is a technique used to extract credentials from the Domain Controllers. In this, we mimic a Domain Controller and leverage the (MS-DRSR) protocol and request for replication using GetNCChanges function. In response to this, the Domain Controller will return the replication data that includes password hashes. This technique was added to the Mimikatz tool in August 2015 by Benjamin Delpy and Vincent Le Toux. To perform the DCSync attack we need the following rights on the Domain Object:

1) Replicating Directory Changes (DS-Replication-Get-Changes)

2) Replicating Directory Changes All (DS-Replication-Get-Changes-All)

3) Replicating Directory Changes In Filtered Set (DS-Replication-Get-Changes-In-Filtered-Set) (this one isn't always needed but we can add it just in case).Generally, members of Administrators, Domain Admins, or Enterprise Admins as well as Domain Controller computer accounts by default have the above rights.



DCSYNC ATTACK SCENARIO

We will look at 2 Scenarios in this article:

Note: There can be many more scenarios that you can think of to perform a DCSync attack.

1) We assume that we have a User account hash that is a member of Domain Admins group

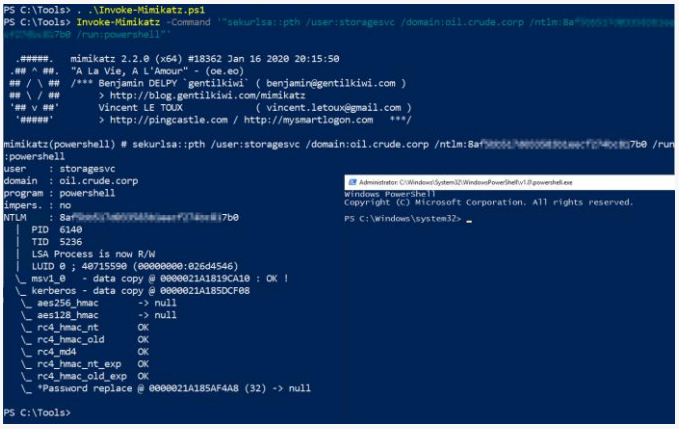
2) We assume that we have User credentials that have WriteDACL rights on the Domain Object

1) First Scenario

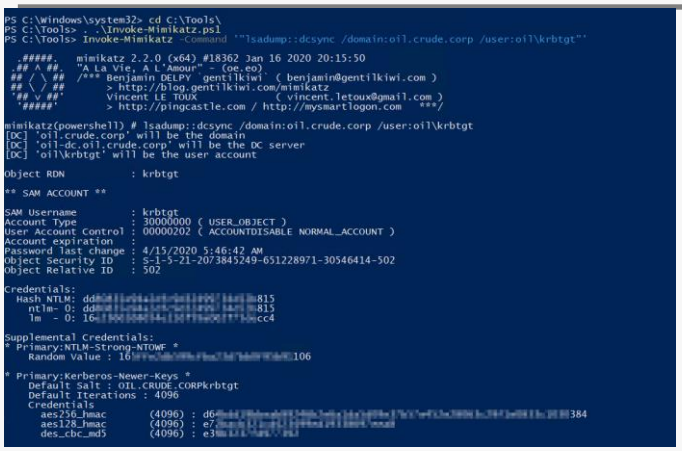
So, let's assume that we have already compromised the user account that is a member of the Domain Admins group. In our Lab, we have a user named storagesvc that is a member of the Domain Admins group as we can see in the below screenshot.

```
PS C:\Windows\system32> net group "Domain Admins" /dom
The request will be processed at a domain controller for domain oil.crude.corp.

Group name     Domain Admins
Comment        Designated administrators of the domain

Members

-------------------------------------------------------------------------------
Administrator            storagesvc
The command completed successfully.

PS C:\Windows\system32>
```

So, we can now perform the OverPass-The-Hash attack using the Invoke-Mimikatz PowerShell script and start a new PowerShell console with the privileges of the storagesvc use



In the New PowerShell console, we can load the Invoke-Mimikatz PowerShell script and perform the DCSync attack.

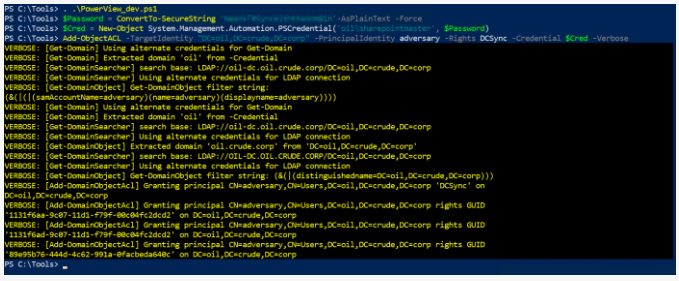


As we can see in the above screenshot, we were able to perform a DCSync attack successfully and retrieve the KRBTGT account hash.

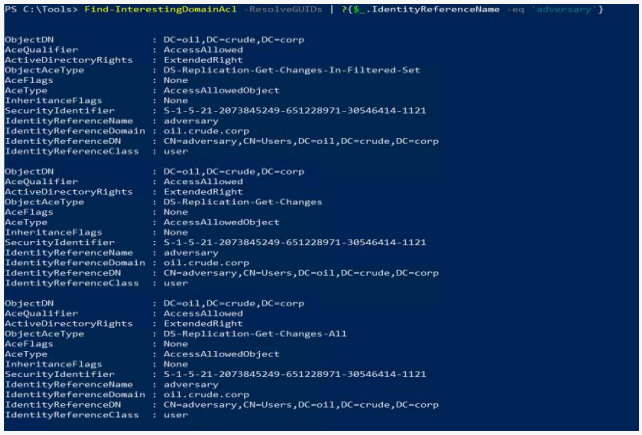
2) Second Scenario

So, let's assume that we have already found the clear text credential of the user that has WriteDACL privileges on the Domain Object. In our Lab, we have a user named sharepointmaster that has WriteDACL rights on the Domain Object as we can see in the below screenshot.We will leverage the PowerView script to grant the DCSync rights to another user(adversary) that we own.

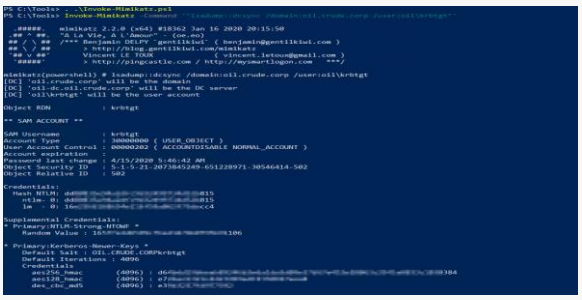
Note:- We can also grant DCSync rights to sharepointmaster users.



We will enumerate and confirm if the adversary user has DCSync rights.



As we can see in the above screenshot, we were able to grant the DCSync rights to the adversary user successfully. Now, we will load the Invoke-Mimikatz PowerShell script and perform the DCSync attack.



As we can see in the above screenshot we were able to perform a DCSync attack successfully and retrieve the KRBTGT account hash.

Note: There are other tools that can also perform DCSync attacks such as Impacket Library & DSInternals etc.

►DETECTION

To detect the OverPass-The-Hash attack, ACL based attacks & DCSync attack we need to enable a few logs on the Domain Controller before emulating the attack.

In our Lab, we have already enabled those logs. But you can follow the below-mentioned steps to enable the logs in your environment. We have also deployed the Sysmon in our lab for additional logging. You can also deploy Sysmon with Sysmon Modular config in your environment.

To Capture the Logon Events, we need to enable the "Audit Logon" logs. Follow the below steps to enable the Logs:

1) Login to Domain Controller

2) Open Group Policy Management Console

3) Expand the Domain Object

4) Expand the Group Policy Objects

5) Right-click on the Default Domain Policy and click on Edit (The policy that is applied to all the domain computers. It may differ in your environment)

6) Follow the below path to enable Audit Logon events.

Computer Configuration --> Windows Settings --> Security Settings --> Advanced Audit Policy Configuration --> Audit Policies --> Logon/Logoff --> Audit Logon

7) Select "Configure the following audit events:" Checkbox
8) Select Success & Failure Checkbox

To Capture the Directory Service Access Events, we need to enable the "Audit Directory Service Access" logs. Follow the below steps to enable the Logs:

1) Login to Domain Controller
2) Open Group Policy Management Console
3) Expand the Domain Object
4) Expand the Group Policy Objects
5) Right click on the Default Domain Policy and click on Edit (The policy that is applied to all the domain computers. It may differ in your environment)
6) Follow the below path to enable Audit Logon events. Computer Configuration --> Windows Settings --> Security Settings --> Advanced Audit Policy Configuration --> Audit Policies --> DS Access --> Audit Directory Service Access
7) Select "Configure the following audit events:", "Success" & "Failure" Checkbox

To Capture the Directory Service Change Events, we need to enable the "Audit Directory Service Changes" logs. Follow the below steps to enable the Logs.

1) Login to Domain Controller
2) Open Group Policy Management Console
3) Expand the Domain Object
4) Expand the Group Policy Objects
5) Right-click on the Default Domain Policy and click on Edit (The policy that is applied to all the domain computers. It may differ in your environment)
6) Follow the below path to enable Audit Logon events. Computer Configuration --> Windows Settings --> Security Settings --> Advanced Audit Policy Configuration --> Audit Policies --> DS Access --> Audit Directory Service Changes
7) Select "Configure the following audit events:", "Success" & "Failure" Checkbox After we published the blog @TactiKoolSec highlighted us that 4662 event won't be generated if the DCSync attack is performed by Computer Accounts.

Later @4ndr3w6S shared a tweet from @cnotin where @cnotin & @exploitph discussed this behaviour and mentioned that we need to add additional SACLs on the Domain Object for detecting DCSync attacks performed by Computer Accounts and Domain Controllers.

To add the Domain Computers SACL on the Domain Object. Follow the below steps:

1) Login to Domain Controller
2) Open Active Directory Users and Computers Console.
3) Right-click on the Domain Object and click on Properties.
4) Click on the Security" tab in the Properties dialog box and then click on the Advanced button.
5) Click on the Auditing" tab in the Advanced Security Settings dialog box and click on Add button.
6) Click on "Select a principal" and enter "Domain Computers" in the text box and click on "Check Names" button and then click on the "OK" button.
7) Select "Success" from the drop-down list of "Type".
8) Select "This object only" from the drop-down list of "Applies to".
9) Select "All extended rights" checkbox and click on "OK" button.
10) Click on the "Apply" button and then click on "OK" button.

To add the Domain Controllers SACL on the Domain Object. Follow the below steps:

1) Login to Domain Controller
2) Open Active Directory Users and Computers Console.
3) Right-click on the Domain Object and click on Properties.

4) Click on the Security" tab in the Properties dialog box and then click on the Advanced button.

5) Click on the Auditing" tab in the Advanced Security Settings dialog box and click on Add button.

6) Click on "Select a principal" and enter "Domain Controllers" in the text box and click on the "Check Names" button and then click on the "OK" button.

7) Select "Success" from the drop-down list of "Type".

8) Select "This object only" from the drop-down list of "Applies to".

9) Select "All extended rights" checkbox and click on "OK" button.

10) Click on the "Apply" button and then click on the "OK" button.

Note about false positive: Some false positive DCSync alerts will be generated when we add the SACL for Domain Controllers on Domain Object. Since the Domain Controllers regularly sync data between themselves. Other applications would also generate false-positive DCSync alerts like Azure AD Connect or any AD Backup Solution.

In our lab, we are using HELK setup to parse and query the logs and winlogbeat to push the logs from the individual systems to the HELK instance.

Detect OverPass-The-Hash Now let's run the below query to detect the Logon event that is generated while performing OverPass-The-Hash attack

```
event_id:4624 and logon_type : 9 and logon_process_name : seclogo
```

In the above query, we are searching for Event ID 4624 logs that contains logon_type 9 and logon_process_name seclogo.

Event ID 4624 - This event is generated when a logon session is created.

Logon Type 9 - A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity but uses different credentials for other network connections.

When we perform the OverPass-The-Hash attack a Logon Type is 9.

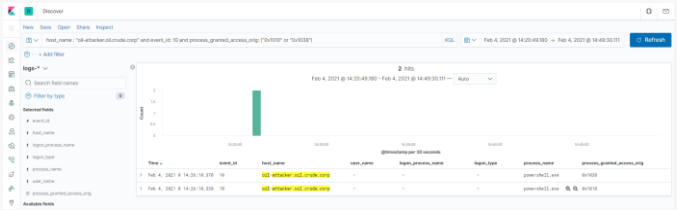
Logon Process - The name of the trusted logon process that was used for the logon. When we perform the OverPass-The-Hash attack a Logon Process with the name is "seclogo".

```
event_original_message
An account was successfully logged on.

Subject:
        Security ID:            S-1-5-21-2073845249-651228971-30546414-1121
        Account Name:           adversary
        Account Domain:         OIL
        Logon ID:               0x61904

Logon Information:
        Logon Type:             9
        Restricted Admin Mode:  -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
        Security ID:            S-1-5-21-2073845249-651228971-30546414-1121
        Account Name:           adversary
        Account Domain:         OIL
        Logon ID:               0x2604546
        Linked Logon ID:        0x0
        Network Account Name:   storagesvc
        Network Account Domain: oil.crude.corp
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Process Information:
        Process ID:             0x304
        Process Name:           C:\Windows\System32\svchost.exe

Network Information:
        Workstation Name:       -
        Source Network Address: ::1
        Source Port:            0

Detailed Authentication Information:
        Logon Process:          seclogo
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
```

While performing the OverPass-The-Hash attack Mimikatz tries to access the LSASS process. Run the below query to detect if the LSASS process is accessed with certain privileges that are common while running Mimikatz on the machine to extract the credentials or perform an OverPass-The-Hash attack.

```
host_name : "oil-attacker.oil.crude.corp" and event_id: 10 and process_granted_access_orig: ("0x1010" or "0x1038")
```

In the above query, we are searching for Event ID 10 logs on "oil-attacker" machine that has granted certain access to the LSASS process. We can look for process-specific access rights here.



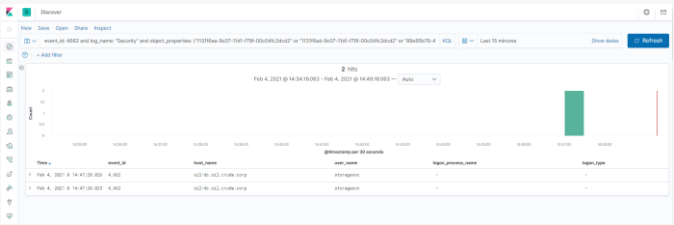
This attack can also be detected via ATA as an "Unusual protocol implementation"

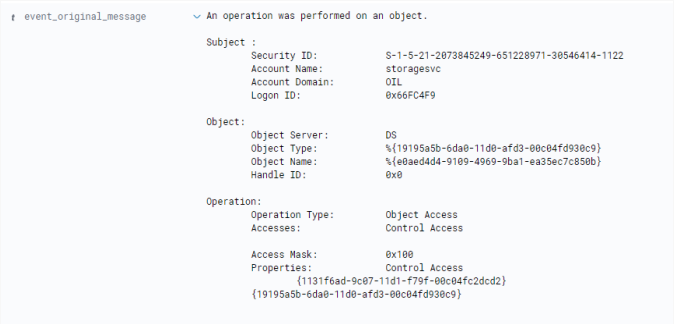
Detect DCSync

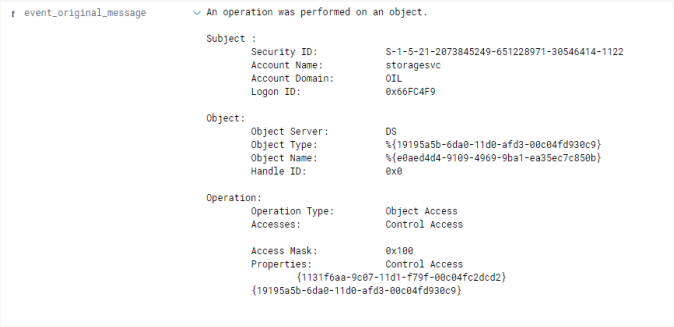
We can run the below query to identify if a DCSync attack was performed.

```
event_id: 4662 and log_name: "Security" and object_properties: ("1131f6aa-9c07-11d1-f79f-00c04fc2dcd2" or "1131f6ad-9c07-11d1-f79f-00c04fc2dcd2" or "89e95b76-444d-4c62-991a-0facbeda640c")
```

The GUIDs mentioned in the above queries are the GUIDs of the Replication rights needed to perform the DCSync attack.

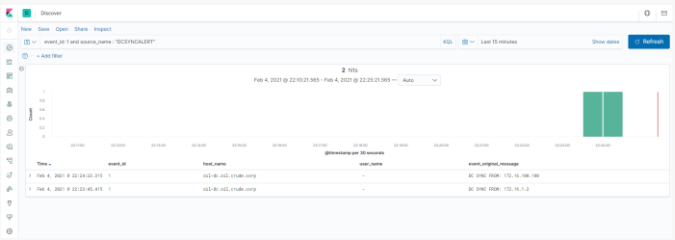




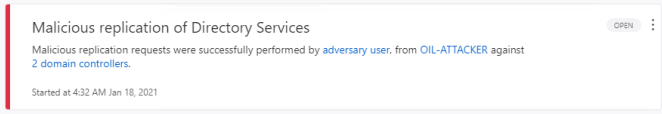


We can also leverage network traffic to detect DCSync attacks. There is a tool DCSYNCMonitor that needs to be installed on the Domain Controller to monitor for the Network Traffic. This tool triggers an alert when there is any Replication performed over the network. This can trigger false positive alerts when a Genuine Domain Controller requests a replication. Hence it is recommended to use DCSYNCMonitor tool with a configuration file where we specify the IP address of the Domain Controllers in the network to avoid false-positive alerts. We can run the below query to identify the alert triggered by DCSYNCMonitor tool.

event_id: 1 and source_name : "DCSYNCALERT"



In the above screenshot, we can see a false positive alert for 172.16.1.2 IP address as it is a valid Domain Controller. This is to highlight the importance of the config file while using DCSYNCMonitor tool.This attack can also be detected via ATA as "Malicious replication of Directory Services".

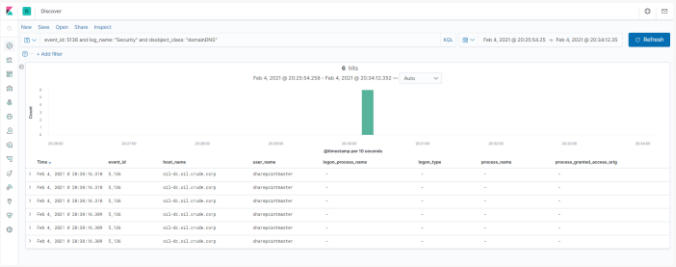


Detect ACL Modification

We can run the below query to identify the ACL modification where we granted the adversary user the DCSync rights.

```
event_id: 5136 and log_name: "Security" and dsobject_class: "domainDNS"
```

There are multiple events that are generated while modifying the ACLs.The event log count will always be in even numbers as there are always 2 events for a single ACL modification. The same can be verified by filtering using the "Correlation ID". One event is "Value Deleted"(ACL deleted / removed) and the second is "Value Added" (ACL Added / Modified).



We can also Convert the "nTSecurityDescriptor" value using "ConvertFrom-SddlString" PowerShell command to get more detail about what changes are done.

Notes:- This command can't retrieve the value of the DCSync rights, we will always see the value as "WriteAttributes" and we need to run this command from the Domain Joined machine.

▶RECOMMENDATION

It is recommended to audit risky ACL-based misconfiguration regularly as those could lead to compromise of the complete domain environment.

▶REFERENCE

1) https://adsecurity.org/?p=1729
2) https://www.harmj0y.net/blog/redteaming/abusing-active-directory-permissions-with-powerview/
3) https://www.harmj0y.net/blog/redteaming/mimikatz-and-dcsync-and-extrasids-oh-my/
4) https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync
https://gist.github.com/gentilkiwi/dcc132457408cf11ad2061340dcb53c2
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc772673(v=ws.10)

https://doi.org/10.46293/4n6/2022.05.01.05
Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

DIGITAL 4N6 VENDOR REVIEWS

WHY BELKASOFT SHOULD BE YOUR TOOL OF CHOICE FOR MOBILE FORENSICS

HIGHLIGHTS

This is the first Article inside the newly introduced Column, Digital Forensics Vendor Reviews and we are very happy to start with the first of 4N6 in the Year 2022. Here our Digital Forensics Researchers and Team will focus on nurturing and mentoring Digital Forensic Startups and other Institutes to innovate features to fill the gaps and to present their product services to Forensics Experts, LEA and other Institutions through our matured and expert readers from Academia, Research Institutions (such as IIT, RRU, NFSU, NFSL, etc.) and LEA Officers/Institutes..

– **Editorial Team, Digital Forensics (4N6)**

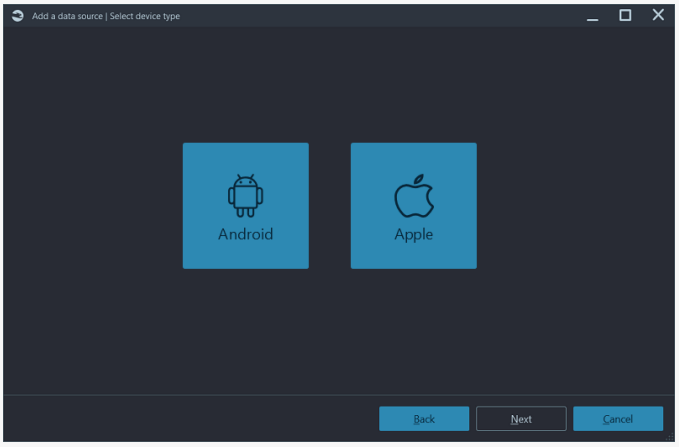
Yuri Gubanov
Belkasoft Founder and CEO
yug@belkasoft.com
https://www.linkedin.com/in/yurigubanov/

Expertise:
Yuri Gubanov is a renowned digital forensics expert. He is a frequent speaker at industry-known conferences such as HTCIA, EnFuse/CEIC, FT-Day, CAC, CACP, ICDDF, and others. Yuri is the Founder and CEO of Belkasoft, the manufacturer of digital forensic software empowering police departments in more than 130 countries. With years of experience in the digital forensics and security domain, Yuri led forensic training courses for multiple law enforcement departments in several countries.

► INTRODUCTION

Established more than 10 years ago, Belkasoft was mostly famous for its computer forensics tools. However, within the last few years, many DFIR professionals began to choose Belkasoft products specifically for our mobile acquisition and analysis functionality. Belkasoft, along with Cellebrite, was one of the two first companies in the world which supported the Checkm8-based full file system iOS acquisition on a Windows platform—while most competitors were 6 to 12 months behind with this feature. This was just one of the reasons for the rising popularity of Belkasoft as a mobile forensic tool.

In this article, we will describe the mobile forensics support that Belkasoft offers and why Belkasoft products should be your tools of choice for working with mobile devices, whether in a digital forensic investigation or an incident response case.



► Belkasoft X

Belkasoft X (Belkasoft Evidence Centre X) is a flagship tool by Belkasoft for computer, mobile and cloud forensics. It can help you to acquire and analyse a wide range of mobile devices, run various analytical tasks, perform case-wide searches, bookmark

artefacts, and create reports. A free trial of this tool is available at https://belkasoft.com/trial.

► Belkasoft R

Belkasoft R (Belkasoft Remote Acquisition) is a tool for forensically sound remote acquisitions of various types of devices, as well as partial images, including selected artifacts only (e.g. for compliance or eDiscovery needs). This product has a unique capability that allows for the acquisition of mobile devices remotely. A free trial of this tool is available at https://belkasoft.com/trial.

► OVERVIEW OF BELKASOFT'S SUPPORT FOR MOBILE FORENSICS

One of the first steps—and the most important one—of working with a mobile device is data acquisition. If there is no data acquired, there is nothing to analyse. Belkasoft has sound support for the acquisition of modern smart devices, including phones, tablets and even IoT devices.

Belkasoft X supports multiple types of acquisitions for both of the most wide-spread platforms: iOS-based and Android-based devices. There is also support for Microsoft (Windows) phones, but since they are no longer produced, we will not review this support.

Both iOS and Android devices have their own peculiarities when it comes to data acquisition. There is a standard backup mechanism for both: iTunes for iOS and ADB for Android; Also, AFC and MTP/PTP protocols allow for media files extraction. Both iTunes and ADB are very limited in the volume of information available. And of course, most data can now be acquired with methods, which are not approved by device manufacturers, such as rooting, jailbreaks, exploits and so on. Many of these methods are device, or chipset-specific. This is why it is important to have multiple types of acquisitions available to you. With that being said, it is important to start with less intrusive methods, just to be on the safe side.

One of the great features within Belkasoft X, is that it allows you to start with the least intrusive and safest methods and continue with more comprehensive (but riskier) ones.

► iOS ACQUISITION SUPPORT

For iOS, Belkasoft X supports the iTunes backup acquisition, including an interesting feature of using lockdown files to avoid unlocking the device in case a passcode is unknown. You can acquire media files with the Apple File Conduit (AFC) protocol.

Figure Labelling is not done (Applicable for all figures)

More interestingly, a full file system and even the keychain (password built-in storage) can be acquired with the help of more sophisticated methods such as a jailbroken iPhone/iPad acquisition, Checkm8-based acquisition and even our agent-based acquisition. To clarify, either our Checkm8, or agent-based acquisition is a jailbreak, so they are much more forensically sound ways to acquire data—since in many countries, it is legally impossible to perform a jailbreak on evidence.

Our Agent-based acquisition is just another one of Belkasoft X's benefits, recognized by many customers. There are not many tools on the market that offer the same feature. It is a great complementary feature to Checkm8, since Checkm8 is limited in iOS device models (iOS devices with A5-A11 Chipsets), while agent-based acquisition works even on the latest iPhones, and the supported iOS range is huge, starting with an iOS as old as version 10.

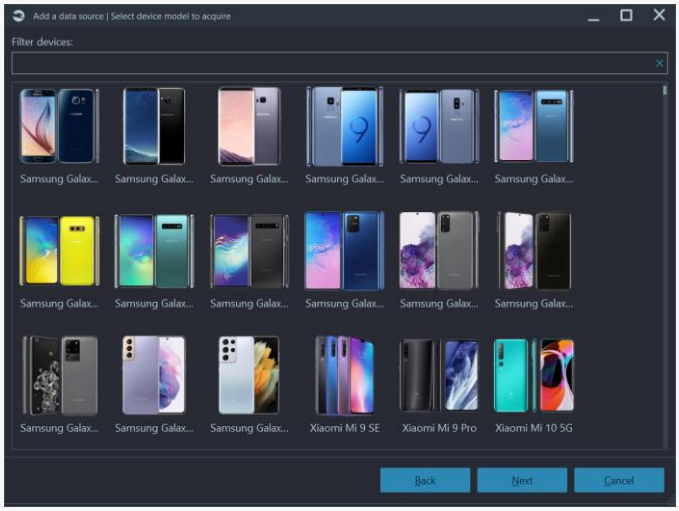
Speaking of Checkm8, Belkasoft X is adding something extra on top of the competition. For example, it can lift the so-called USB Restricted Mode—a mode, which disables data transfer via a Lightning cable in one hour after the latest unlock.

There are more types of iOS acquisition such as crash log extraction, which, though limited, may give you some useful info such as the latest IP addresses involved in your investigation.

To learn more about the iOS acquisition with Belkasoft X, please watch our webinars available at https://belkasoft.com/webinar. Recorded webinars can be found on the Previous webinars tab, including Locked iPhone investigations, Bypassing iPhone USB Restricted Mode and others.

► ANDROID ACQUISITION SUPPORT

For Androids, Belkasoft supports standard ADB backup creation and multiple types of acquisitions, based on ADB. One interesting method is our APK downgrade acquisition, which replaces an original application file (e.g., WhatsApp) with an older version. Such older versions can then be used with ADB backup creation and include much more data into our backup. Of course, at the end, the original app version is restored.



Another ADB-based method of Android acquisition by Belkasoft X, is automated screen capturing. This is possibly the safest way to extract data from a device, so you may consider starting every case or acquisition with this method—before you try a riskier method.

Belkasoft X supports various Android acquisition methods, specific for particular vendors or chipsets. Among the supported methods, you will find Spreadtrum devices, MTK (MediaTek) and Qualcomm. For MTK, the product gives you as many as three different methods of acquisition, including two types of agent-based extraction and Qualcomm devices are supported via the EDL (Emergency Download) mode.

The product can also acquire rooted devices and analyse TWRP extractions. It supports analysis of JTAG images and chip-off dumps and can perfectly ingest third-party images, including forensic product images and proprietary vendor image files. For example, you can analyze HiSuite backups—as well as Xiaomi images—with the help of Belkasoft X.

To learn more on Android acquisitions within Belkasoft X, please watch our webinars available at https://belkasoft.com/webinar. Recorded webinars can be found on the previous webinars tab, including Android phones investigation: data extraction and analysis with Belkasoft X and others.

► CLOUD FORENSICS

Though cloud forensics is very much different from mobile forensics, performing these acquisitions can complement or corroborate data obtained from a mobile device. Since this is not the topic of this particular article, we will give two examples of useful functions in Belkasoft X, which can play a role in your mobile investigations:

- WhatsApp downloading (with or without a QR code). WhatsApp extraction is a challenging task, so every additional method you have available is priceless
- iCloud downloading. If you cannot obtain an iPhone acquisition, iCloud can be your source of data, backed up from that device to the Apple-hosted storage

Both options (as well as many others) are available within Belkasoft X, when you add a cloud-based data source to your case.

► MOBILE APPLICATION ANALYSIS

You have now successfully imaged a device. Congratulations! Now you have to analyze the image contents.

There are millions of applications available for modern smartphone users and any automation of their analysis is indispensable to avoid growing case logs. Belkasoft supports more than 1500 types and versions of the most popular applications, including WhatsApp, Signal, Telegram, Instagram, TikTok, Viber, Tinder, Pinterest and many others.

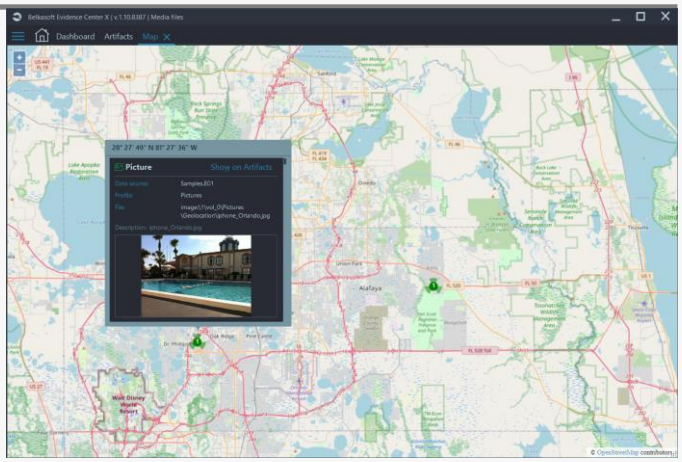
While most of these apps store data in an SQLite database (this analysis is another story), it is not as easy as opening your favourite database browser to extract all the data. First, a standard freeware tool such as DB Browser for SQLite (and even most forensic tools!) will not recover deleted data

located in freelists, or data from WAL (Write Ahead Logs) and journal files, as well as SQLite unallocated. Second, many apps use robust encryption to prevent an examiner from opening their databases without a decryption key.

Belkasoft X can decrypt and decode multiple versions of WhatsApp—and it is not necessary to have the phone rooted! You can use our APK downgrade method to extract the decryption key. iOS Signal messenger is another tough nut that Belkasoft X can crack once you have made a full file system extraction and captured the keychain (or if you have it from a third-party extraction). Wickr Me is supported for both iOS and Android platforms (as well as for computer operating systems).

In the user interface, Belkasoft X conveniently lays out various mobile (and other) artifacts, including audios, chats, documents, pictures and videos, geolocation data, cryptocurrency wallets and transactions, and data from fitness trackers, sleep data, heart rate, etc.

Unlike the competition, which often allows you to have just one device in a case, you can add as many devices—whether mobile or computer—to your case. This helps you to obtain a 'birds-eye view' via our Connection Graph—which will show how different people from your case or from different devices, were communicating. Whether it was via chats, SMS, voicemail, or calls and email. Finally, you can make connections between your added datasets and no matter the type of device, a feature not supported by competition. This can be tough and time-consuming manual work otherwise, to correlate data from a mobile device of one user with a laptop of another user, since you will have to work in two different software products, not necessarily talking to each other or supporting each other's formats.

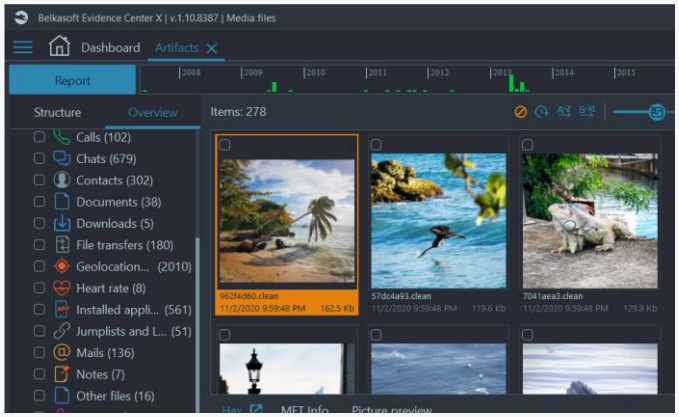


Reviewing geolocation data, such as photos made on a mobile device, with Belkasoft X's built-in Maps

►BENEFITS OF BELKASOFT'S SOLUTIONS FOR MOBILE FORENSICS

There are multiple reasons why Belkasoft is considered to be a tool of choice by a growing number of prominent digital forensic experts and incident responders. Among them are:

- A solid support of mobile device acquisition, including sophisticated methods such as Checkm8 and Agent-based acquisition
- Wide range of supported device models
- Forensically sound remote acquisition of mobile devices
- A huge number of mobile applications and artifacts supported out of the box by Belkasoft X
- Very affordable price: much less than any mobile forensic software by competitors

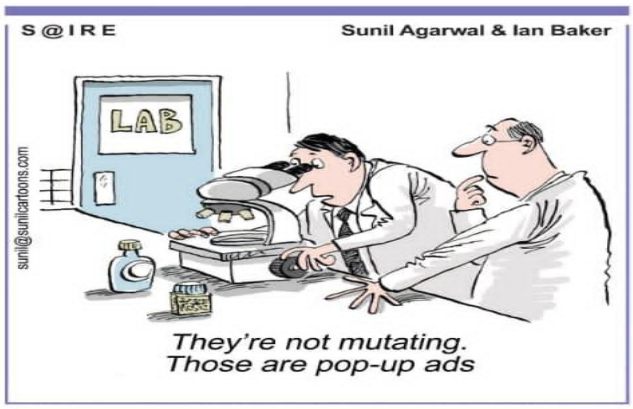


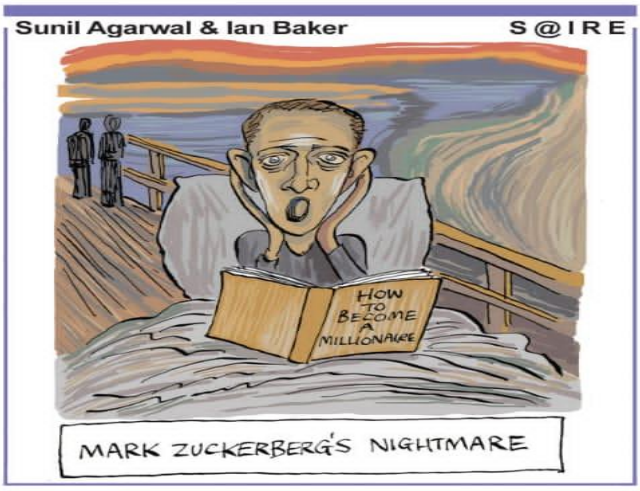
▶ READY TO TEST BELKASOFT?

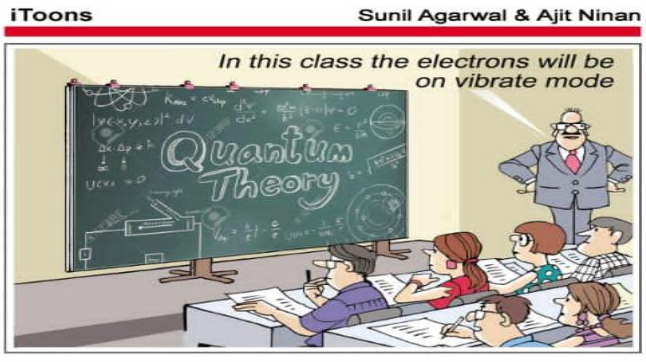
If this article convinced you to try Belkasoft tools, you can download them from https://belkasoft.com/trial. The Belkasoft X installation contains sample images with both computer and mobile data.

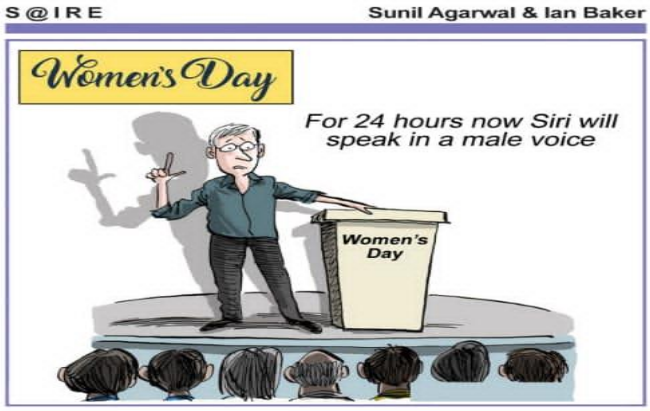
Do you need a more sophisticated image to try? Solve our BelkaCTF number 2 ('Drugdealer case'), devoted to an Android investigation. You will see the power of Belkasoft X for yourself: even the most difficult tasks can be solved with this tool in a matter of minutes.

If you do not have the time to dedicate to a full CTF, try to catch some of our short BelkaTalk videos where we answer difficult questions from across the community, some focused mainly in mobile forensics.



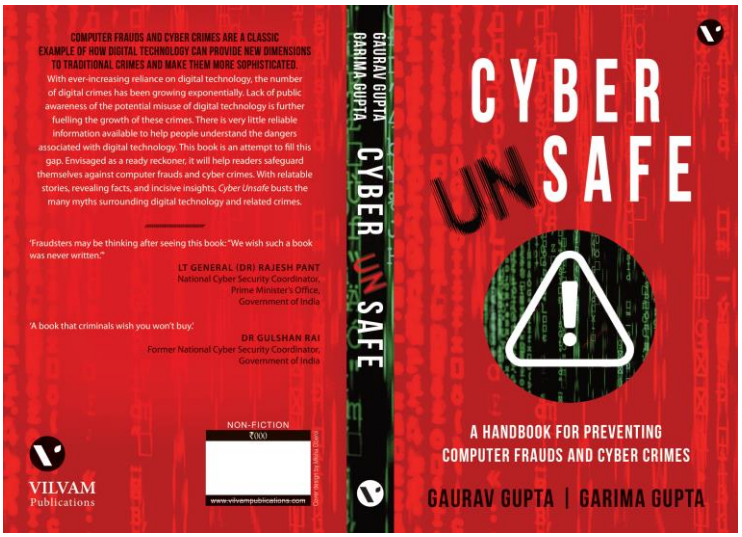






Cyber Reviews of Cyber Unsafe of Dr. Gaurav Gupta & Garima Gupta

'A book that criminals wish you won't buy' is perfect anecdote explain the purpose of book. The purpose of this book is to analyze computer fraud and cyber crime issues from the perspective of a common man and to unmask the myths of computer frauds and cyber crimes, with a hope to reduce the exploitation of the common man by criminals. The book can be searched on amazon with its name "Cyber Unsafe" and it available at https://www.amazon.in/UNSAFE-HANDBOOK-PREVENTING-COMPUTER-FRAUDS/dp/8195422918/ref=sr_1_1?dchild=1&keywords=cyber+unsafe&qid=1634016894&sr=8-1



In this book, brother sister duo of Dr. Garima Gupta and Dr Gaurav Gupta has used relatable real-world incidents and stories to demonstrate the risks associated with digital technology. Further, easy-to-implement, mostly nontechnical, methods have been identified for technology users to help them safeguard against prevailing computer frauds and cyber crimes.

The book has been envisaged as a ready reckoner for anyone who uses digital technology. This book will provide a completely new perspective on technology-related frauds and help readers become aware and responsible citizens in cyber space.

This is a must read book people of all age groups including youngsters and senior citizens as they the preferred target of cyber criminals. Book contains sixty two probable myths which most of technology users may have and highlights how criminals exploit human emotions to carry outfrauds and cyber crimes. We highly recommend this book.

https://doi.org/10.46293/4n6/2022.05.01.06

Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

DIGITAL 4N6 CASE STUDIES

DELETED CHAT CASE STUDY

HIGHLIGHTS

This is a Case Study on WhatsApp Chat Data and History Recovery and Carving. Here, Author tried to present his insights on how Forensic Analysis of Business Communication keeps untruthful allegations in Corporate Politics and Tactical Planning inside the organization. This Case study highlights ways of saving your own employment and reputations through Forensic Psychology point of view!

– Editorial Team, Digital Forensics (4N6)

Mr. Nikhil Mahadeshwar
Cyber Security Evangelist and Tech Futurist
webmaster.nikhilm@gmail.com

Mr. Nikhil Mahadeshwar is a renowned cybersecurity expert and technology-based innovator with more than a decade of experience in the web industry. He is a Digital Forensics Investigator and Consultant for various law enforcement and private investigative agencies. He is 'A certified Security Analyst,' 'Computer Hacking Forensics Investigator,' 'ISO 27001:2013 Information Security Management Systems Lead Auditor', and 'Certified Threat Intelligence Analyst.' He has also trained more than 40,000 people on cyber awareness & lectures to entrepreneurs, school & college students, police officials, corporates, etc. He has been awarded as the youngest entrepreneur and was presented as the youngest researcher at the National conference on social media responsibility.

► THE DELETED CHAT CASE STUDY

Cybersecurity as a domain is proving to be a lifesaver in various professional and personal aspects today. Cybersecurity offers a range of detective and preventive measures that undeniably protect firms and individuals from Cyber Breaches. However, in many such Incidents, cybersecurity companies enabled troubleshooting Cybercrime Cases!

Skynet Softest came across one such client under dire duress due to malpractices within an organization that threatened to cost the client their job and reputation.

► THE INCIDENT REPORT

A client (Mr. X) came to us under severe emotional stress because of the fear of losing his job. His employer was a call centre firm, a multinational firm with a respectable name in the industry. The employees within the organization were often encouraged to collect five-star feedback from their clients. While this was a common practice within the industry, above was an illegal one. The employees were often encouraged and coerced by their managers and team leads to get good ratings, which would impact the overall team performance. These conversations happened in the client's office group chat on his Apple iPhone; those chats history was now deleted.

The glitch in this system came to light during a recent Audit, wherein this malpractice came to light, and the client's job was at stake and risk. As a result, the client reached out to us to recover these confidential chats to not lose his job and prove with absolute certainty that he was acting under the instructions of his superiors and managers!

► THE BACKGROUND WORK

Our A-team was put in place to identify and recover the chats as per the client's requirements. However, ample historical data came to light, and manually or systematically filtering the necessary data would be a tediously time-consuming process.

Our team took further assistance from the client and narrowed down the search window. We also gathered the telephone numbers of the suspected managers and tried to cross-check the

data with them. The client gave us a time window of December 2019 to September 2020, which significantly simplified the search, although not a short one.

Upon repetitive help from the client, such as looking for keywords – including 'feedback ', survey' and more made finding significantly easier. This was aimed to help our team streamline the search and get the required results.

▶ THE RESULTS

Upon carefully searching the graphical interface and using CLI commands, we minutely went through the necessary data and timeline. They proved to be highly supportive and in alignment with the claims made by the client. To cross-check and validate the said data, the first-level information is shared virtually via shared screens with the client. Upon first-level validation, the second level of physical validation was arranged. The client carefully rechecked our process, data collection and the proof collected. With final verification, our team of cybersecurity experts and Digital Forensic Experts generated the final report along with the necessary authorizations.

The entire process was well-documented and followed the necessary standard operating procedures as required, aiming to receive an International Quality Certificate in the future!

▶ THE CONCLUSION

Skynet Softtech was successfully able to troubleshoot a client requirement. This included tactfully extracting chats from the highly secure iPhone model. However, without timely intervention, the action would likely cost them their job at a top-level MNC, putting them through financial, emotional and reputational duress. This would also have long-term repercussions on the client's credibility and career.

At Skynet Softtech, our team of highly trained, experienced, skilled and certified professionals are here to successfully help clients in their cybersecurity and Data Carving requirements.

https://doi.org/10.46293/4n6/2022.05.01.07

Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

CYBER FORENSIC PSYCHOLOGY

OVERVIEW OF FORENSIC PSYCHOLOGY

HIGHLIGHTS

This article aims to give a generic overview of Forensic Psychology, studies around the discipline and ? Author has also empathized on differentiating Forensic Science with General psychology and different paths to acquire skills needed for Forensic Psychologist. This also expands to Forensic Specialists with deep interests on Forensic Hypnotism, Cognitive Behavioural Therapy and Forensic Psychologists in Narco-Analysis Tests.

– Editorial Team, Digital Forensics (4N6)

Pranjal Vyas

Pranjal Vyas have excellence in Resource Curation, Pursuing Master's in Clinical Psychology from School Of Psychology Gujarat University , Ahmedabad

Twitter: @vyaspranjal33

► WHY FORENSIC PSYCHOLOGY

Forensic Psychology is the cross-section between the study of psychology and the justice systems. This specifically includes understanding expert witness's testimony and specific content areas of concern (e.g. ability to stand in trial, child custody and visitation, or workplace discrimination and also in Motivational Speech), as well as fundamental legal principles with relevant judicial considerations. For Example, in the United States, the definition of insanity in criminal trials varies from state to state) so as to properly interact with judges, lawyers, and other legal professionals. Another, important aspect of Forensic Psychology is the ability to testify as an expert witness in a courtroom, improving the legal language of the court to make psychological findings, providing information to legal personnel in a way that can be understood, during Court Trials of Crime Crimes or in conjunction with other areas – including Forensic Physics, Forensic Medicines/Chemistry, etc.Skynet Softest came across one such client under dire duress due to malpractices within an organization that threatened to cost the client their job and reputation.

The word forensic originates from the Latin word 'forensics,' which means "the forum" or the court system of Ancient Rome. Christopher Cronin, an Forensic Writer defined it as "A field that combines the practice of psychology and the law. Those who work in this field utilize psychological expertise as it applies to the justice system The application of clinical specialties to legal institutions and people who come into contact with the law" [1]

► HISTORY OF FORENSIC PSYCHOLOGY

James McKeen Cattell is recognized by most as the first Psychologist to combine the law and psychology in his research titled History of Forensic Psychology, 2013; Parrott, 1997) [2] .In fact, in 1895, the experimental psychologist Cattell wrote: " As a last example of the usefulness of measurements of the accuracy of observation and memory I may refer to its application in courts of justice. The probable accuracy of a witness could be measured and his testimony weighted accordingly … The testimony could be collected independently, and be given to experts who could affirm for example that the chances are 19 to 1 that the homicide was committed by the defendant, as referred from pages 65–66.

Cattell experimented with the accuracy of the memories of 56 junior psychology students at Columbia University to arrive at this groundbreaking idea. Previously and in contradiction, researchers were of the opinion that "useful applications of the material sciences have no parallel in the case of the mental sciences", written by Cattell. Cattell posed a series of both academic and practical questions testing the memories and powers of observation of these 56 students. From their responses, he inferred those individual recollections, when compared and contrasted, were more reliable and valid than were group responses after collaboration. He applied his theory to jury deliberations and concluded that in court, the "independently formed verdict of three jurors if concordant would probably have more validity than the unanimous verdict of 12 jurors in consultation", at page 76. Unfortunately, his tests were not considered reliable, and James Cattell terminated these experiments (Parrott, 1997).

The fact remains, however, that there does not seem to be an earlier researcher or theorist who addressed the usefulness of psychology, or "mental science" as Cattell called it, in the courtroom. Hugo Munsterberg has been referred to as the "father of forensic psychology" due to the publication of his book, On the Witness Stand: Essays on Psychology and Crime (1908), but his work followed Cattell's by at least 12 years (Huss, 2009).

Interestingly, and possibly as the stimulus for further research discussed earlier, both Cattell and Munsterberg studied under Wilhelm Wundt, the "father of experimental psychology," in Leipzig, Germany, before returning to the United States to assume their respective university positions (Boring, 1950). Cattell, born in the United States, left to study under Wundt, who had opened the first psychology laboratory in Leipzig, Germany, sometime between 1875 and 1879 (Boring, 1950; Harper, 1950). Munsterberg, younger than Cattell by 3 years and born in Germany, was also Wundt's student. The students received their doctorates from Wundt 1 year APArt, and both returned to the United States to take prestigious positions at major universities. One can only conjecture how Wilhelm Wundt's mentorship influenced his famous students' interest in what we now call forensic psychology.

► PSYCHOLOGY ASSOCIATION

The American Psychological Association officially recognized Forensic Psychology as a special area in 2001 and now let's look at their workplace where forensic psychology is different Forensic psychology is defined as the intersection of psychology and law, but this definition may change as forensic psychologists can play many roles.In many cases, people who work in forensic psychology are not necessarily "forensic psychologists." These individuals may be clinical psychologists, school psychologists, neurologists or lawyers, or counsellors who lend their mental expertise to providing evidence, analysis or recommendations in legal or criminal cases.

Psychologists working in applied forensic psychology settings can provide many services where there is too much to fully explain. In general, Correctional Psychologists may attend inmates' mental health needs, including screening, psychological assessment, personal therapy, group therapy, anger management, crisis management, court-ordered evaluations, or daily inpatient rounds. They may consult with prison staff, inmate advocates, attorneys, and court systems on a variety of mental health-related issues or recommendations. Psychologists who work directly with lawyers can provide psychological assessment, personality assessment, mitigating factors assessment, sexual offender assessment, capacity evaluation, and recommendations for parental custody or visitation.

Psychologists working in police departments often provide services such as counselling or crisis management to department employees. Also, Forensic Psychologists remain present in Narco-Analysis Tests of Investigations related to Cyber Terrorism or Cyber Warfare and other bigger Cyber Tech related attacks. Psychologists working in forensic psychology research or academic domain can teach or research psychology and law on any topic that interacts. The field is unlimited. To name a few popular areas: criminal profiling, criminal trends, effective mental health treatment for offenders, effective treatment of drug abusers, methods for jury selection, divorce effectiveness, custody, separation, child visitation etc.

► WHAT DISTINGUISHES FORENSIC PSYCHOLOGY WITH OTHERS?

The functions of a forensic psychologist are very limited in terms of scope and duration. The forensic psychologist is asked to perform a very specific task in each individual case, determining whether the accused is mentally competent to deal with the allegations.

Unlike the usual clinical setting where a client voluntarily seeks help or evaluation, a forensic psychologist usually deals with clients who do not have spontaneity. This can make assessment, diagnosis and treatment more difficult as some clients deliberately block aid efforts.

► FORENSIC PSYCHOLOGY IS NOT FORENSICS?

Forensic psychology isn't forensics, which is the application of science in legal investigations, such as the chemistry of poisons, the physics of bullets, determining the time of death or how a person was killed. In other words, all the aspects of the Crime Scene Investigation featuring in so many TV/Movies/Web shows. The examination of the scene of a crime and the exploration of the forensic evidence that can be drawn from the crime is sometimes useful to a forensic psychologist, for example in challenging an offender's claim in therapy.

► EDUCATION AND TRAINING

Masters/MPhil and PhD Programs Offered by National Forensic Science University and Rashtriya Raksha University. If you are interested in becoming a forensic psychologist, you should take courses that add value to your skills

topics such as:

- Criminal Psychology
- Social Behaviour
- Abnormal behaviour
- Cognitive psychology
- Perception
- Drugs and psychopharmacology
- Law
- Criminal justice

► CONCLUSION

Forensic Psychology can be an exciting and challenging career choice, Skills that you might need if you choose to pursue a career in this field include The ability to maintain objectivity, Critical Thinking, Strong Communication, Attention to details & Compassion

► REFERENCES/BIBLIOGRAPHY

[1], Christopher Cronin (2009). Forensic Psychology: An Applied Approach

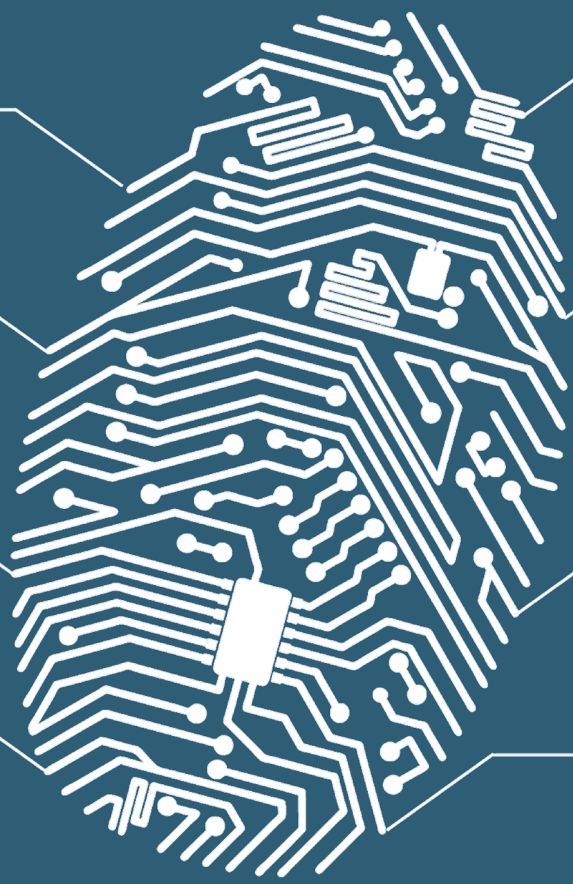
[2], Nietzel, Michael (1986). Psychological Consultation in the Courtroom. New York: Pergamon Press

[3] History of Forensic Psychology, 2013; Parrott, 1997 https://www.verywellmind.com/an-overview-of-forensic-psychology-2794901

[4] https://www.apa.org/ed/precollege/psn/2013/09/forensic-psychology

[5]https://www.psychologytoday.com/us/blog/take-all-prisoners/201006/what-is-forensic-psychology PhD Gomberg, Linda, JD (2018). Forensic Psychology 101

SEMPERSOL
CONSULTANCY



Digital investigations

Incidence response

Forensic readiness

Consulting

Forensic Lab setups

Forensic trainings

Insider threat analysis

Cyber crime investigations support

BRIGHT MINDS

BIG IDEAS

SEMPERSOL CONSULTANCY PVT. LTD.
15-G, Vinayak Complex, Opp. Maa Satiya,
Ayad Road, Udaipur (Raj.) India (313001)
E-Mail: boonlia@sempersol.in
Mob: +91-995-0996-022

https://doi.org/10.46293/4n6/2022.05.01.08

Digital 4N6 : India's First Digital Forensics (4N6) Publication Volume : IV | Issue : II

CYBER FORENSIC PSYCHOLOGY

FOMO: SOCIAL MEDIA IMPACTS IN DIGITAL WORLD

HIGHLIGHTS

This is an unique and high-value Research Paper on Cyber Psychology and contains great finds and explanations useful in Forensic Psychology. Author has tried explaining FOMO (Fear of Missing Out) with definitions of key terms and statistics. Well placed points on Causes, Symptoms and impacts of FOMO has made them truly valuable and useful in Clinical Practices too.

– Editorial Team, Digital Forensics (4N6)

Mr. Yugal Pathak
Digital Forensic Researcher, SysTools Group
Email : yugalpathak2012@gmail.com, cyberyuvi4u@gmail.com

Expertise:

Mr. Yugal Pathak is Cyber Security Researcher and he completed his Digital Forensic Internship at Cyber Forensics Lab, CERT-IN. He has experience of working with UP 100 Police, Developer for Creative Flakes Communications and other organizations and. He currently volunteers with many organizations including Kaspersky Cybermate, United Nation Peace Volunteer, Cyber Peace Foundation, eProtect Foundation, Udaan Foundation and local police.

► ABSTRACT

In this digital world social media has become an essential part of our lives. FOMO (Fear of Missing Out) is an emerging psychological disorder that has become a vital problem of today's social world. Advance technology and today's social media made our social and communicative experiences far better than older times. It provides us the unique way to be socially engaged with one another's life. But on the other hand it also encourages FOMO. Yes, social media has a big role in encouraging this social anxiety. Social media now helps most people to remain in contact with their social and professional network constantly. It may lead to compulsive checking for status updates and thinking that others might be having a great time.

Based on survey results and focus-group data collected from college and corporate employees, participants used social media primarily for purposeful communication among themselves, in addition to connecting back home. Although the construct of FOMO was present in the study, it took on a different role where participants tried to create FOMO in others as opposed to experiencing it themselves. This study provides valuable information for faculty and staff members interested in understanding impacts of social media on students, as well as adding value to the current research on FOMO and its implication on college undergraduates.

Keywords: Social Media, Fear of Missing Out (FOMO), Neuroticism, Fomo Quiz.

► INTRODUCTION: FEAR OF MISSING OUT, OR FOMO

Fomo is "a pervasive apprehension that others might be having rewarding experiences from which one is absent". This social anxiety is characterized by "a desire to stay continually connected with what others are doing".In other words, FOMO perpetuates the fear of having made the wrong decision on how to spend time since "you can imagine how things could be different than what they really happen to be" causing you anxiety, fear , anger to regret yourself of missing those good moments.

As a consequence, FOMO is perceived to have negative influences on people's psychological health and well-being

because it could contribute to people's negative mood and depressed feelings.

► TYPES OF FOMO

- Social Media generated Fomo
- Corporate Life caused Fomo
- College Life caused Fomo
- Physical and Social factors generated Fomo
- Relations and personal disturbances related Fomo

► SYMPTOMS OF FOMO

- Impulsive behaviour and anxiety to check social apps while driving
- Perceived low social rank which can cause anxiety and inferiority complex
- High chances of depression, withdrawal
- Social Insecurity and feelings of social phobia
- Irrational thinking and Irritability
- Difficult interpersonal skills with family and friends with disturbed sleep patterns due to long hours spent online
- Obsessive compulsive behaviour

Extraversion as defined is when an individual whose attention and interests are directed wholly on what is outside the self. This tells that individuals that are extroverts are very comfortable socially. It explains the sense that there is a link between extroversion and higher and more frequent social media use. They think of the media as a platform that will explore them socially and their social presence and connections with others.

Next is Neuroticism which is a category of neurotic individuals alludes to an emotional instability. This has been proven to correlate to social media use and internet addiction. They are more likely to be drawn towards social media apps such as Facebook and Twitter as an attempt to validate them through their peer's approval.

Anxiety, defined as a state of mind in which one is concerned about difficult situations or threats. Traditional literature suggests that anxious people are likely to suffer from multiple disorders. Anxious users are more engaged on social media in order to relieve their anxious state, by trying to find a sense of belonging on social media and looking for attention and many many more to list.

► REAL LIFE EXAMPLES OF FOMO

- People get angry when Wi-Fi suddenly stops working or responding
- People stress when their near and dear ones don't interact with them.
- We start listening songs or fiddling screens when in anger to get relief
- We don't sleep overnight for chatting
- We never miss out virtual webinars and get involved in them knowing its virtual too
- People annoyed on missing TV shows or movies or Social Media Lives

► AN EXAMPLE OF FOMO

Option 1: Customers were shown the fully loaded version of the car. They said the price was too expensive, so the dealer took away options in an effort to reduce the price and make customers comfortable.

Option 2: Customers now saw the base price of the car. Then the dealer asked them to select which options they wanted, slowly increasing the price.

Result: Results show that people, who spent more money, were less satisfied, in the first condition. The theory is that people experience FOMO and are reluctant to give up what they felt they already had this creates the problem.

So, next time to make a big purchase, start by looking at the cheaper models and then move up. Don't ever expose yourself to FOMO by looking at the high end options first.

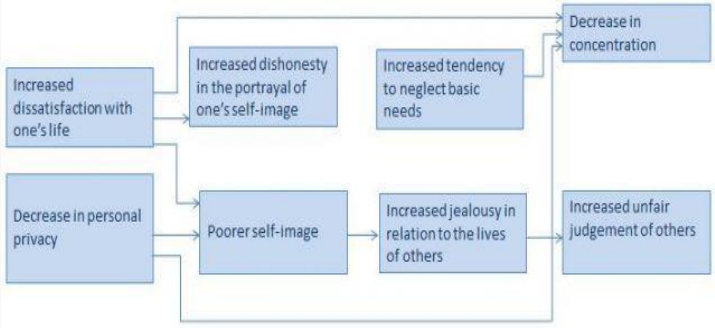
Causes of FOMO

- Our continuously being aware about how some of the people whom we are connected with, are doing so well in their Job, Business, Profession, Marital Life, Relationship, Money, name fame through their social media posting
- FOMO comes from unhappiness and dissatisfaction or rejection
- Trolling regularly on social media and platforms.
- Jealousy in relationships due to misunderstandings in social media.

- Non-acceptance by peers or friends
- Professional workload and misunderstandings or differences
- Increasing Number of Professional Tools = Increasing Level of Stress i.e. fiddling on Office, Web Pages etc. cause mental stress.

Consequences and effects

- FOMO distorts our deep desires and dreams.
- We will always, inevitably, miss out on something.
- FOMO turns our lives into one long bucket list.



Medical and Clinical findings on FOMO:

Psychologists link FOMO to dopamine seeking behaviours associated with gambling and other addictive habits. Like winning the jackpot, it is that unpredictability of getting a "hit" — in the form of a shocking post or juicy email — that produces the dopamine to keep us coming back for more.

- Constant urge to stay updated
- Impulsive behaviour to check social apps while driving
- Withdrawal in absence of networking
- Perceived low social rank which can cause
- Anxiety and inferiority complex
- High chances of depression, withdrawal
- Social insecurity and feelings of social phobia
- Irrational thinking and Irritability
- Difficult interpersonal skills with family and friends with disturbed sleep patterns due to long hours spent online
- Maintaining low profile
- Obsessive compulsive behaviour

► MEASURING AND ANALYSING FOMO

1.Based on past researches and work:

While FOMO is not an entirely new concept, there are seemingly limited means for measuring it. As previously noted, JWT Intelligence (2012) administered a survey to assess the prevalence of FOMO. In their study, they first asked respondents how well they could identify with the fear of missing out without providing respondents with any definition of the fear of missing out.

Pryzbylski et al. (2013) conducted a series of studies, the first of which focused on the development of a scale to measure FOMO. In addition, a later study used a modified version of the Przybylski et al. (2013) to explore the extent to which people check their mobile phones out of a fear of missing out. The resulting "C-FOMO" scale was used to investigate whether FOMO is a motivator for regular mobile phone checking (Haeto, 2013).

The current research focuses on scale development using foundational items, namely psychological components, which have been associated with FOMO in previous writings: inadequacy, anxiety, irritability, and self-esteem.Essentially, someone higher in feelings of inadequacy, higher in feelings of anxiety, higher in feelings of irritability,and lower in self-esteem is envisioned to have a higher fear of missing out.

Fear of Missing Out Scale: FoMOs

Przybylski, Murayama, DeHann, & Gladwell (2013)

Participant Instructions

Below is a collection of statements about your everyday experience. Using the scale provided please indicate how true each statement is of your general experiences. Please answer according to what really reflects your experiences rather than what you think your experiences should be. Please treat each item separately from every other item.

Response Anchors

Not at all true of me	1
Slightly true of me	2
Moderately true of me	3
Very true of me	4
Extremely true of me	5

Items

1. I fear others have more rewarding experiences than me.
2. I fear my friends have more rewarding experiences than me.
3. I get worried when I find out my friends are having fun without me.
4. I get anxious when I don't know what my friends are up to.
5. It is important that I understand my friends "in jokes."
6. Sometimes, I wonder if I spend too much time keeping up with what is going on.
7. It bothers me when I miss an opportunity to meet up with friends.
8. When I have a good time it is important for me to share the details online (e.g. updating status).
9. When I miss out on a planned get-together it bothers me.
10. When I go on vacation, I continue to keep tabs on what my friends are doing.

Calculating Individual Scores

Individual scores can be computed by averaging responses to all ten items and forms a reliable composite measure (α = .87 to .90).

How to Cite

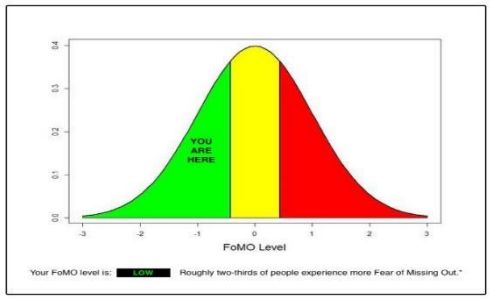
Przybylski, A. K., Murayama, K., DeHaan, C. R., & Gladwell, V. (2013). Motivational, emotional, and behavioral correlates of fear of missing out. *Computers in Human Behavior*, 29, 1814-1848.

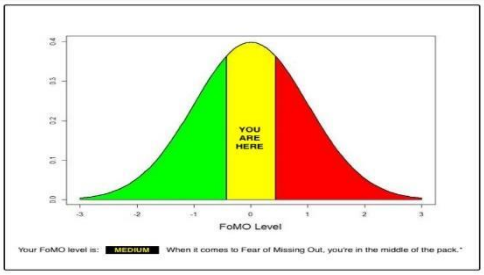
Notes on Use

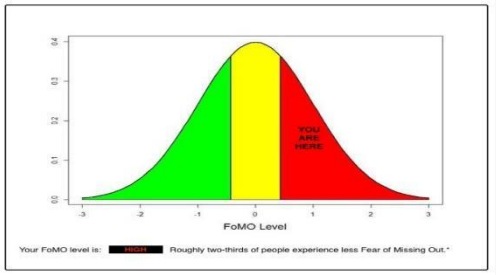
- Where and when possible, randomize the presentation order of these items.
- I am interested to hear about how the work is being used.
- This scale is provided free for personal and academic use.
- If you want to use this measure in a commercial or for profit organization let me know and we can work out licensing.

2.Fomo Quiz:

The FoMO Quiz is another measure to rate an individual's level of FoMO.This survey is also developed by Andrew Przybylski.The results are provided graphically as a curve of FoMO level v/s population distribution.



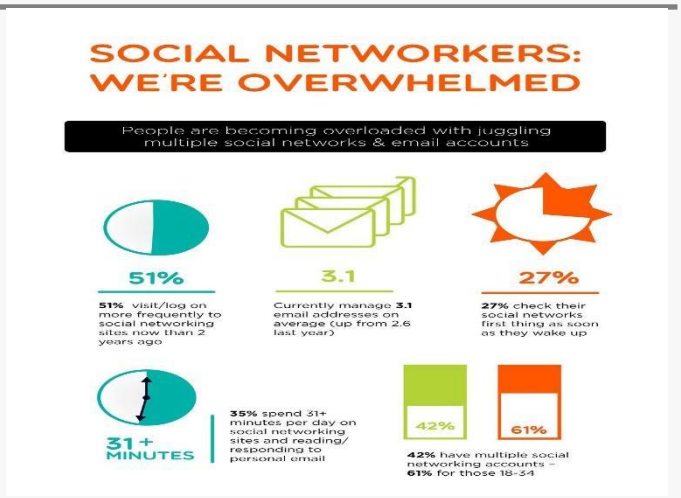




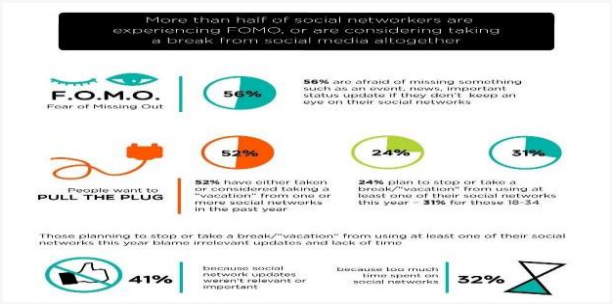
Based on Surveys and social sites analysisThe Relation between Social Media and FOMO:

- ✓ FOMO is the driving factor behind social media use and vice-versa.
- ✓ Social "One-upmanship".
- ✓ Social circumstances: Low levels of need satisfaction and life satisfaction are linked to high FoMO.

In fact, a new survey conducted by **MyLife.com** revealed 56% of people are afraid of missing out on events, news and important status updates if they are away from social networks.

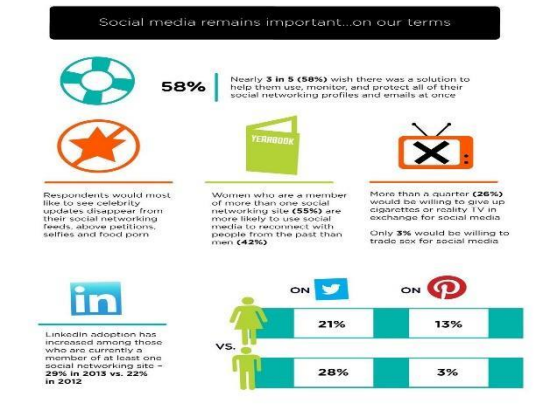


In the same vein, about 51% of people visit or log on more frequently to social networks than they did just two years ago. About 27% of participants check social sites as soon as they wake up? Many would trade other addictions to stay connected this way — about 26% percent said they would trade habits such as smoking cigarettes or reality TV for access to social networking sites.People are managing numerous social networking accounts as well.



About 42% of study participants have multiple accounts — and the percentage goes to 61% for those of ages of 18 and 34. The average person also manages 3.1 email addresses compared with 2.6 from last year.

Although 52% of respondent's accepted they have c taken a "vacation" from one ormoresocial networks in the past year, only 24% said they will likely follow through. Why? FOMO, of course.For a full look at how people are using social media and managing the many platforms, check out the info-graphic below.



► FOMO V/s JOMO:

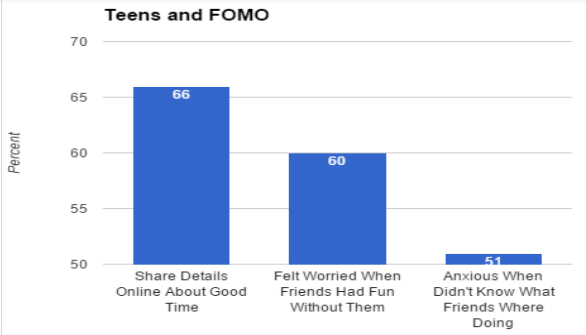
JOMO, is one that encourages us to understand what we want, why we want it, and how we are feeling now in the present.

Moving from FOMO to JOMO:

- Disconnect
- Reflect
- Reconnect
- Keep doing new

► TEENS AND FOMO:

Teens today are more likely to be sleep deprived. Nearly all teens go online daily, with a quarter online constantly.Only a third of independent school teens get 7+ hours of sleep each night.



►WAYS TO TACKLE FOMO

- ✓ If you have-to-have-now-or-you'll-die, put a pin on it
- ✓ Create reminders about your values
- ✓ Indulge in more outdoor activities such as trekking, hiking and sports.
- ✓ Use your free time to read books rather than people's posts and comments
- ✓ Dedicate family time regularly e.g. an hour or so every week
- ✓ Tell yourself it's okay to say no
- ✓ It's okay to say no if you can't afford it

► TREATMENT AND COUNSELLING

1. Individual therapy
2. Group therapy
3. Family counselling
4. Cognitive Behavioural Therapy (CBT)
5. Addiction counselling

► TECHNOLOGICAL SOLUTIONS TO FOMO

Artificial intelligence (AI) is back after years of being out of vogue. Platform vendors such as Microsoft, Facebook, Google, Apple, Amazon and IBM have all announced AI initiatives. Most recently, AI efforts centre around machine learning bot frameworks, which are being touted as the brains behind the next generation of human computer interaction. With bots, rather than use an app or website to order a pizza or file a vacation request, you will simply 'chat

with,' or 'talk to' a bot, who will figure out what you want and fulfill your request using simple conversation.

► CONCLUSION

In the short term, I predict we will see an increase in workplace FOMO induced by information overload.

Also due to exposure to more "Bad social media" will significantly increase fomo in young adults and teens too.But in the longer term, emerging tools and technologies that combine the best of AI with the best of human-computer interaction practices will aggregate disconnected information to support human decision making. We can already see this in current visualization and intelligent aggregation technologies, but we can expect to see many more such technologies emerge over the next few years.

►REFERENCES

[1] Abed, M.A., Hall, L.A., & Moser, D.K. (2011). Spielberger's state anxiety inventory: Development of a shortened version for

critically ill patients. Mental Health Nursing, 32 (4), 220-227.

[2] Dr. Sushma Kirtani,D.Ch, M.D.,D.N.B., PGD- AP, Pediatrician and Adolescent Physician, Goa

[3] https://www.quora.com/What-is-the-psychology-behind-FOMO-Why-is-it-so-powerful-And-what-type-of-people-are-the-most-sensitive-to-it

[4] Mr. David,Product Officer at harmon.ie

[5]https://mashable.com/2013/07/09/fear-of-missing-out/#h7KtekzgWiqX

[6] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online social networks:

challenges and opportunities," April 2010.

[7] R. G. Brody, "Flying under the radar: social engineering," International Journal of Accounting

and Information Management, vol. 20, pp. 335-347, 2012.

[8] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in

Proc. the 2005 ACM workshop on Privacy in the electronic society, 2005, pp. 71-80.

[9] D. Rosenblum, "What anyone can know: The privacy risks of social networking sites," Security

& Privacy, IEEE, vol. 5, pp. 40-49, 2007.

[10]https://www.researchgate.net/publication/282390744_SNcEH1C3UXSaTcNMHNLGNuLZqjGKbSrEMZGcgeDikpQiWRz278L458DuaLh.109773641.109773641.109773641.109773641.109773641.109773641dying_Abroad

[11]https://quizlet.com/290744131/chapter-12-relationships-with-friends-flash-cards/

[12] https://en.wikipedia.org/wiki/Fear_of_missing_out

[13]https://everipedia.org/wiki/lang_en/Fear_of_missing_out

Re-Defining
Video
Investigations

Lab Systems

iTECH
DIGITAL FORENSICS
Powering Data Forensics

Everything that you need for Video Investigations

- End-to-End Video Evidence Management
- Authentication of Videos & Images
- Image & Video Enhancement
- Deleted data recovery
- Video Analytics & A.I.

LABSTER-X

Designed for High Performance of Video Forensic Software

Kinesense · Impress · Mandet · IPSOTEK · DVR Examiner

Ideal Solution for Clearing all Pendency

- Forensic Science Laboratories
- Police & other LEA
- Smart Cities

Why iTECH ?

- High End Ergonomic Design
- Evidence-safe infrastructure
- Workstation fully customizable according to customer requirement
- Anti-static matt surface
- Variable mode with motorized height adjustable table (Bespoke)

MAKE IN INDIA

contact@labsystems.co.in | www.labsystems.co.in

Lab Systems

Request a Demo

NEW AGE AUDIO & VIDEO AUTHENTICATION LABORATORY

Image Enhancement & Authentication

Audio Analysis & Authentication

Video Enhancement & Authentication

CORE SERVICES

- Network & Cloud Forensics
- Mobile Forensics
- Audio Forensics
- CDR/IPDR Forensics
- Disk Forensics
- Video Forensics

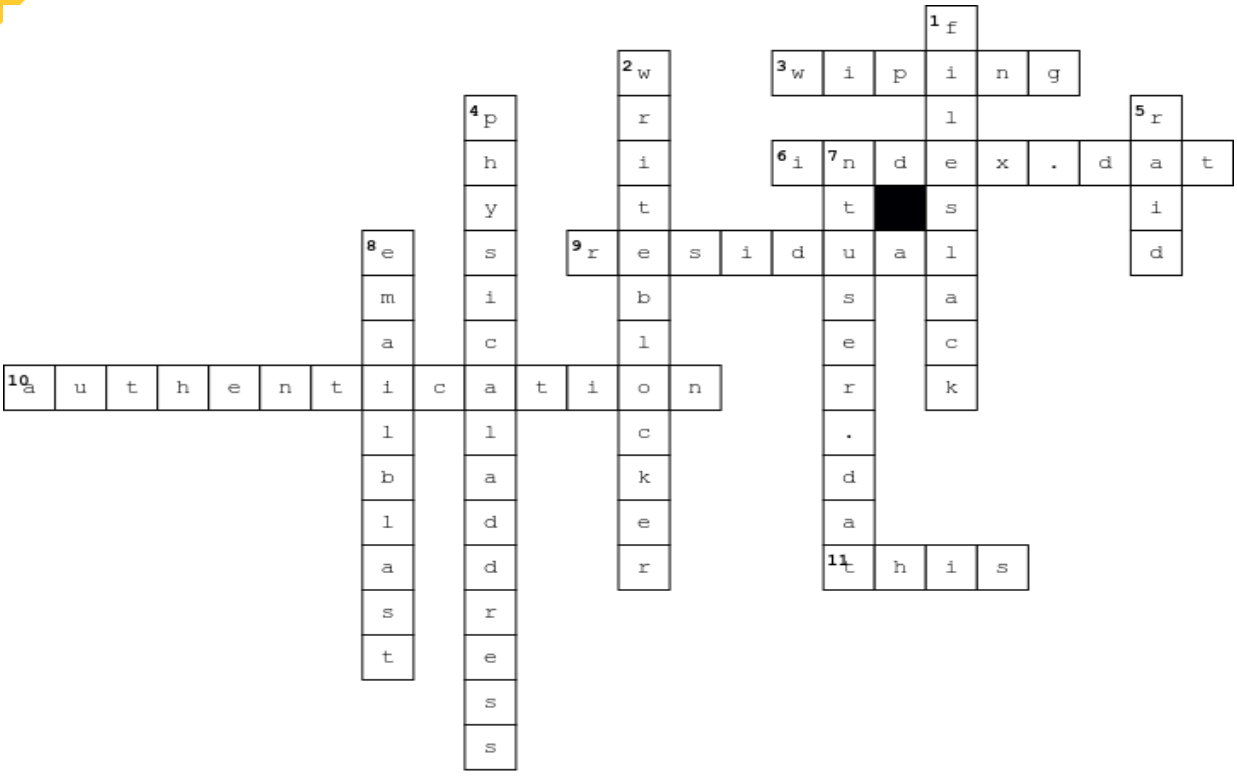
OUR PARTNERS

FOCLAR
FORENSIC MULTIMEDIA ANALYSIS

Anubhooti Solutions

LABSYSTEMS.CO.IN | CONTACT@LABSYTEMS.CO.IN | (022) 3251 4134

4N6 CROSSWORD- FEB 2022



Across

3. The first Police Crime Laboratory that was established here in 1910 by Edmond Locard.

5. A tool that analyses network packets for network testing and troubleshooting.

6. It is a tool being developed to allow authorities for visual access to hidden files on the Xbox hard drive.

9. Bertillon, the French police officer who was the first to apply the forensics in form of anthropometry.

11. A technique used by forensic experts in which analysts use a sophisticated microscope to view the physical state of all gates.

12. The act created when the first computer crime was recognized in 1978 Florida.

Down

1. A tool that supports KASLR (Kernel Address Space Layout Randomization) and analysis of processes in Memory dumps.

2. A technique used by Law Enforcement that has been able to use subpoenas to gather details on anonymous posts.

4. A tool that allows experts to extract EXIF (Exchangeable Image File Format) information from JPEG files.

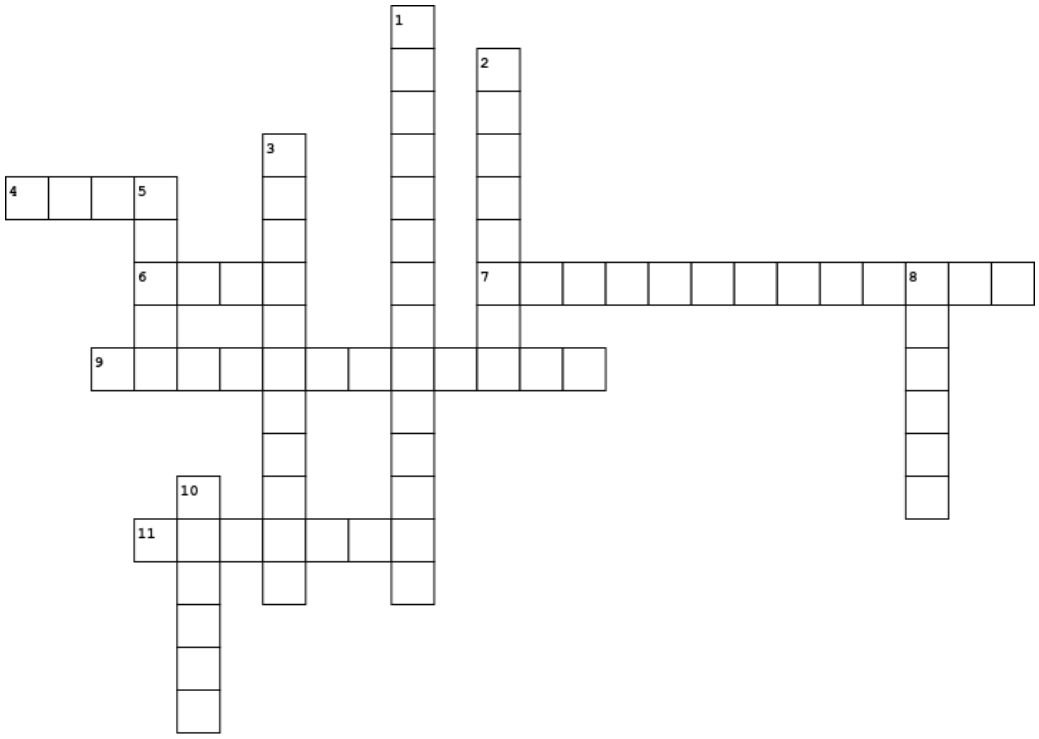
7. An Open Source tool that provides PIPI (Port Independent Protocol Identification) feature to support Digital Forensics.

8. A technique using which officer can take paper and obtain DNA of where the paper was touched by the suspect.

10. The most important step by LEA to preserve evidence in the crime scene.

Written By : Mr. Yugal Pathak

4N6 CROSSWORD- MAY 2021



Across

4 A variant of the well-known CryptoMix ransomware, which frequently targets Windows users.

6 A federal program, allowing the federal government to share monetary losses with insurers on commercial property/casualty (P/C) losses due to a Terrorist Attack.

7 A teenager that conducted nightly break-ins into the tram depot of the city of Lodz in 2007.

9 The Botnet created by Russian Hacker Evgeniy Mikhailovich in order to spy on the user

11 In the month of May 2021, a huge leak of Customer data was experienced by this famous brand, globally.

Down

1. A Form of terrorism involving Computers, Technologies and Internet or MDM, etc.

2. A malware mobile application that charges app users large amounts of money despite users deleting those apps.

3. A virus that is rewritten with every iteration so that every succeeding version of the code is different from the proceeding one

5. A malware that acts by infecting the boot record of machines that use the Windows system and asking for ransom.

8. A ransomware infecting the city of Atlanta, and the Port of San Diego abruptly stopping services.

10. A group of computers running malicious programs that are remotely controlled by cybercriminals

Written By : Mr. Yugal Pathak

Introducing the Next Generation Cyber Range

Practice. Plan. Protect.

Cyber attacks threaten your organization. Every day these threats grow in sophistication and persistence. How your teams respond in the critical first moments will determine the impact to your organization.

SkyVirt Cyberrange offers best-in-class technology, high-impact training modules and ultra-realistic emulated/simulated environments that will help prepare your teams to mitigate losses and defend your organization successfully.

SkyVirt Cyber range

Can help you

- Train with the newest technologies in the cybersecurity landscape
- Test and secure your technology infrastructure
- Validate your incident response playbook
- Develop and continually enhance your security team's skills
- Build models of collaboration within your team
- Leverage proven methodologies to help you better detect and mitigate cyber threats

The SkyVirt Cyber Range has been developed to provide diverse organizations with greater access to state-of-the-art technology, in an effort to build cybersecurity resilience across India. We recognize the importance of building a culture of cybersecurity within your organization — and that this requires training everyone from senior leadership to your technology teams. Our Cyber Range provides a tailored experience for your needs as an organization, catering to different audiences with varying skill levels.

With real-world scenarios, advanced emulations/simulations and an immersive delivery experience, the SkyVirt Cyber Range helps organizations reinforce their security position and manage cyber risk across their different departments.

SkyVirt®, Hyper-Realistic Dynamic Hands-On Training Platform for Cyber Warriors

100%

Hands-on Lab Coverage with Training

Example Exercise Cyber-Security Domain

Various lab are available

Basic Cyber Security	Advance Cyber Security	Conceptual Lab	Global Lab
Information Gathering Network Scanning	Infrastructure Protection	Windows and Linux Administration	Cyber Incident Response
Cyber Training, Education, and Awareness	Vulnerability Assessment	Cyber Risk Analytics	Cyber War gaming
Many more..	Application Protection	Server Hardening	Security Operations Centre
	Enterprise Network Breach	IDS/IPS Configuration	Threat Intelligence and Analysis
	many more...	Many more...	Many more...

Basics | Intermediate | Advance

Concept Of Virtual Training Environment

- ✓ Concept of classroom at home
- ✓ No dependencies! plugins required at user end
- ✓ Unlimited hands on labs on IT infrastructure, attack/defence,
- ✓ digital forensics and AI & ML
- ✓ Highly scalable multi-tenancy & Concurrency cloud based platform
- ✓ Available in Internet Enabled mode as well as no internet as LAN Environment
- ✓ Design for IT Professionals, LEA. Defence & Academia

SkyVirt* CyberRange

https://cyberrange.skyvirt.tech/

India Office: SkyVirt®
15-G , VINAYAK COMPLEX, OPPS. MAA SATIYA ROAD UDAIPUR RAJSTHAN-313001 BHARAT(भारत)
info@skyvirt.tech |
Tel: +91-8770962145

There is no viable alternative for real-world experience. That's the motivation we made the

SkyVirt® -Cyber Range

Training Platform for Academia, Industries and Government

The **SkyVirt® -Cyber Range** platform provides an operationally focused approach to test skills and assess aptitude of both individuals and cyber defense teams by operational role and assignment.

Within this framework, each trainee is assigned a Learning Plan that forms the baseline for a unique scoring approach that measures their proficiency and overall progress.

Four training delivery methods are utilizes within the Range framework to drive Cyber Defender proficiency:

- ✓ Classroom-Based Modules with Integrated EmulationSimulation Labs
- ✓ Self-Paced Security Challenges
- ✓ Team-Based Dynamic Exercises
- ✓ Custom Course Module Assessments and Delivery

To help organizations meeting such requirements, Synergy Systems has developed Cyber Range, a fit- for-purpose cybersecurity simulation platform that supports training, testing and research and development needs, providing: Realistic simulation of networks and technologies. Skills development training and development for incident response teams and other staff. Capacity to evaluate guidelines and incident response procedures. Ways to challenge people and working environments.

SkyVirt® -Cyber Range platform can also be used to evaluate security products and architectures in a managed virtual environment that is completely independent from the organization's operational processes without the risk of knock-on effects on day to day operations.

CYBER RANGE

- *Scalable and evaluative*
- *Realistic*
- *Versatile*
- *Hybrid*

SkyVirt® CyberRange

TRAINING & EVALUATION

TESTING & EMULATION

Educate & Train

Realistic and adaptable attack scenarios

Prepare your teams for real life scenarios, even the most challenging ones.

- ✓ Use of standard attack scenarios in an incremental skills-building approach.
- ✓ Design of scenarios to meet the specific issues each organization faces, with total user immersion.
- ✓ Expandable scenarios to take new threats into account.

Test & Analyse

Keeping pace with the latest threats

Connect your any Cyber Threat Intelligence platform, Make your ownSkyVirt® -Cyber Range Scenario's/Exercise according constantly updated with the latest threats as they emerge.

- ✓ New indicators of compromise added for even more realistic training experiences.
- ✓ Updates of system components (real or virtualized) put your security upgrades to the test.
- ✓ Continuous Improvement of embedded detection and response capabilities in a safe environment.

Challenge & Motivate

Skills development and operational experience

Training exercises, with contents and methods tailored to specific requirements.

- ✓ For an optimal transfer ok incident supervision and response skills.
- ✓ For evaluating trainees' progress at the different stages of their education with cyber-challenges that help each trainee to test his skills.
- ✓ The use of organization's own security components makes the training even more realistic and the people ready for their job.

Hyper-Realistic Training Ecosystem

- ✓ Real-World Security Tools
- ✓ Real-World Networks
- ✓ Real-World Cyberattacks
- ✓ Multiple Roles and Scenarios

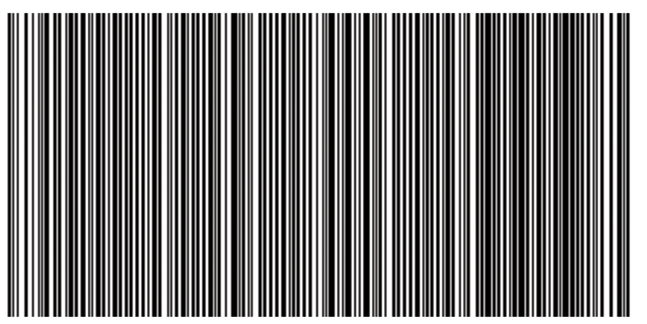
15-G , VINAYAK COMPLEX, OPPS. MAA SATIYA ROAD UDAIPUR RAJSTHAN-313001 BHARAT(भारत)

info@skyvirt.tech | Tel: +918770962145

https://cyberrange.skyvirt.tech/

Retail Selling Price - INR 500

Volume 4 | Issue 2 | MAY 2022 | INR 500



www.digital4n6journal.com