PD.TVZ.HR
POLYTECHNIC & DESIGN Vol. 13, No. 2, 2025.
Mrežna inačica: ISSN 2459-6302
Tiskana inačica: ISSN 1849-1995
DOI: 10.19279/TVZ.PD.2025-13-2-19

RJEŠAVANJE NIST HAKERSKOG SLUČAJA

SOLVING THE NIST HACKING CASE

Jan Lamza[1], Damir Delija[2]

Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia, Student
Zagreb University of Applied Sciences, Vrbik 8, 10000 Zagreb, Croatia

SAŽETAK

Rad ima za cilj prikazati rješavanje hakerskog slučaja pripremljenog od strane Nacionalnog instituta za standarde i tehnologiju (NIST) korištenjem forenzičkog alata Autopsy. Predstavljena je simulacija stvarnog incidenta koju je NIST učinio dostupnom javnosti u svrhu učenja i certificiranja. Slučaj je otkriven 20. rujna 2004. kada je pronađeno prijenosno računalo *Dell CPI* sa serijskim brojem *VLQLW* , bežičnom *PCMCIA* karticom i vanjskom 802.11b antenom kućne izrade. Pretpostavlja se da je računalo korišteno u svrhu neautoriziranog pristupanja, gdje je osumnjičeni Greg Schardt (pseud. „Mr. Evil“) parkirao svoje vozilo unutar dosega bežičnih pristupnih točaka (*Starbucks, T-mobile Hotspot*) i presretao internetski promet u pokušaju dobivanja brojeva kreditnih kartica, korisničkih imena i lozinki. Ovaj rad uključuje analizu scenarija, identifikaciju ključnih tragova i artefakata prethodno opisanog slučaja, korištenjem besplatnog alata Autopsy. Radom se želi s pomoću analize podataka tvrdoga diska, pokazati da je Greg Schardt uistinu haker pod pseudonimom „Mr. Evil“.

Ključne riječi: *forenzička analiza, Autopsy, simulacija incidenta, hakerski slučaj*

ABSTRACT

The paper aims to present the resolution of a hacking case prepared by the National Institute of Standards and Technology (NIST) using the forensic tool Autopsy. A simulation of a real incident prepared by the National Institute of Standards and Technology is presented and is available to the public for learning and certification purposes. The case was discovered on September 20, 2004, when an Dell CPI laptop with serial number VLQLW, a wireless PCMCIA card and a home-made external 802.11b antenna was found. It is assumed that the computer was used for unauthorised access purposes, where suspect Greg Schardt (pseud. Mr. Evil) parked his vehicle within range of wireless access points (Starbucks, T-mobile Hotspot) and intercepted Internet traffic in an attempt to obtain credit card numbers, user names and passwords. This paper includes scenario analysis, identification of key clues and artifacts of the previously described scenario, using the free Autopsy tool. The work aims to prove by means of hard disk data analysis that Greg Schardt truly is a hacker under the pseudonym „Mr. Evil“.

Keywords: *forensic analysis, Autopsy, incident simulation, hacking case*

1. UVOD
1. INTRODUCTION

Digital forensics plays a crucial role in the modern judicial system, particularly in cases involving computer-related crime. This paper focuses on a detailed forensic analysis of the “NIST Hacking Case,” exploring how digital traces can provide irrefutable evidence in criminal proceedings. The primary objective of the research is to demonstrate the application of digital forensic tools in the reconstruction and analysis of hacking activities. The case analysed is a simulation of a real-world cybercrime incident, in which the key individual is Greg Schardt, known by the pseudonym “Mr. Evil.” Within the forensic community, Greg Schardt

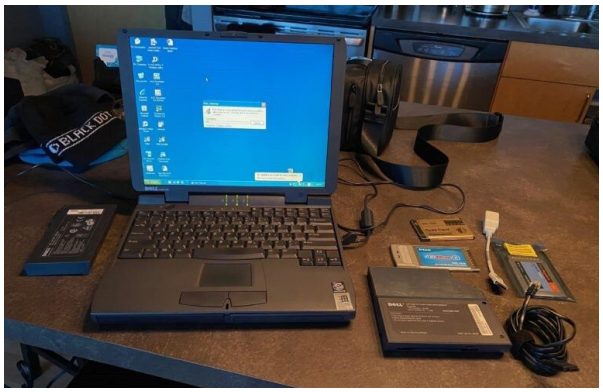
is recognized as a suspect in an actual case of unauthorised access to wireless networks. The case was constructed and made publicly available by the National Institute of Standards and Technology (NIST) for the purpose of education, testing, and certification of digital forensic tools and methodologies. By analysing the seized laptop belonging to Greg Schardt, the study demonstrates how digital evidence can be utilized to establish the perpetrator's identity, methods of attack, and the extent of the resulting damage. Particular emphasis is placed on forensic methodology, the identification of key digital artefacts, and their legal validity, with the broader aim of providing deeper insights into potential security vulnerabilities and proposing guidelines for their improvement. The selection of analytical tools was left to the investigator, to demonstrate that identical results can be obtained using multiple tools and approaches. The description of the case, as provided in the NIST Hacking Case, is as follows: "On 20 September 2004, in the apartment of Greg Schardt, a Dell CPI laptop computer (serial number VLQLW) was discovered and seized, along with a wireless PCMCIA card and a custom built external 802.11b antenna (Figure 1). Through police investigation and testimonies from Schardt's associates, it was determined that the laptop had been used for unauthorised access and interception of internet traffic to collect sensitive victim data. The collected data included credit card information, usernames, and passwords for the registration of various domains. The purpose of this data collection was the unlawful acquisition of financial gain to the detriment of the victims." The case description does not specify which forensic tool was used to create the forensic image of the laptop.

To legally substantiate the assumption that Greg Schardt indeed used the laptop for the previously described criminal actions, a forensic image of the computer's disk contents was created. A forensic image is an exact copy of a disk's contents produced using a forensic duplication tool and stored in a designated format, in this case the so-called E01 or "Expert Witness One" format. The purpose of creating a forensic image is to preserve evidence and maintain the authenticity of the data on the computer [1],[9]. The equivalence between the data on the disk and the forensic image can be verified by comparing the hash signatures of the disk contents and the image contents [2].

Conducting active investigations directly on original data has been dismissed by the scientific community due to the potential for unintended modifications of the source data. When multiple individuals are involved in forensic analysis, the original forensic image is duplicated as needed, and before analysis begins, the hash values of the original forensic image and its copies are compared to confirm data integrity [2], [9]. Although a forensic image represents an authentic replica of the original data, it also has certain limitations. A forensic image cannot capture data from volatile or working memory (RAM), network traffic, or user activities that were not recorded on the disk. Consequently, critical information such as passwords in working memory, encrypted sessions, or malicious processes active at the time of seizure may be lost. The quality of a forensic image depends on the type and reliability of the acquisition tool used, as well as on the method by which the image is created; any inconsistency in this process may undermine the forensic validity of the evidence. Additionally, some forensic image formats, such as *E01*, support additional metadata and compression features but may be less interoperable across different tools, complicating analysis. In cases of significant disk damage, some "sectors" may fail to copy correctly, potentially resulting in partial or unreliable outcomes. For these reasons, it is essential to remain aware of the limitations of forensic imaging and account for them during image creation in order to preserve its legal validity and scientific reliability.

To verify the validity of the copied forensic image against the original, the hash is examined. Hash functions are mathematical functions that return a unique fixed-length value—known as a hash—for input data of any length. In digital forensics, hash algorithms (such as MD5, SHA-1, SHA-256) are used to verify data integrity, ensuring that source data has not been altered during analysis. During the creation of a computer's forensic image, the hash of the original data is compared with the hash value of

the image copy to confirm its authenticity and immutability. Since forensic analysis confirmed that the laptop was used for unauthorised access, the forensic image was, upon completion of the investigation, submitted to the National Institute of Standards and Technology (NIST) as training material. NIST made the forensic image publicly available on its CFReDS (*Computer Forensic Reference Data Sets*) portal [3], thereby enabling broader public access for educational and analytical purposes.



Slika 1 *zaplijenjeno prijenosno računalo, te popratni uređaji pronađeni u apartmanu*

Figure 1 *confiscated laptop with accompanying devices found in the apartment*

2. PRIPREMA ZA FORENZIČKU ANALIZU
2. PREPARATIONS FOR FORENSIC ANALYSIS

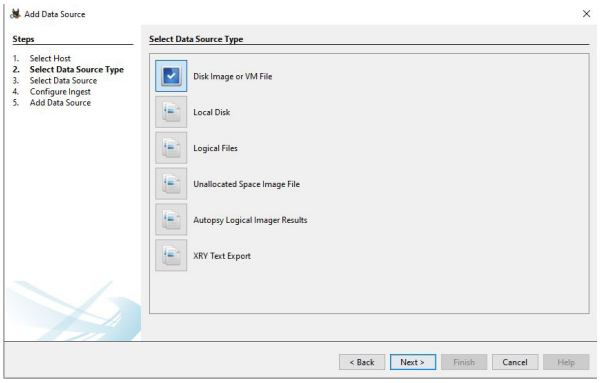
The process of forensic analysis involves preparing the necessary tools and equipment, collecting documents and copies of physical objects containing electronic evidence, extracting evidence from the collected material, and the analysing the gathered evidence [4],[9]. The tool used for forensic analysis is Autopsy, free, open-source software, developed by Basis Technology (now BasisTech, USA) [5]. Autopsy is a desktop digital forensics platform with a graphical interface. It is used by law enforcement, the military, and corporate investigators to examine computer-related incidents. It also enables the reconstruction of photographs from camera memory cards.

The recommended system requirements for using Autopsy include: Windows 10 (64-bit), Linux, or macOS operating system; Intel i5 or newer processor; at least 4 GB of RAM (8 GB recommended); and SSD storage with at least 1 GB of free space (depending on the size of the forensic image). Autopsy has also been used in real court cases, such as *State v. Bowersox* (USA), where it assisted in analysing the timeline of a suspect's activities. In cases involving child pornography, it supports rapid image searches and the detection of hidden files. The tool is also used by the FBI and local police departments in the United States for preliminary forensic data processing in digital evidence laboratories.

Autopsy is intuitive and easy to use, while also allowing extensions through additional modules. In this research, the tool was downloaded from the official website and installed (Figure 2). After installation, a new case was created, and the forensic image was loaded (Figure 3).

Figure 2 *ekran dobrodošlice instaliranog Autopsy alata*

Figure 2 *Autopsy welcome screen*



Slika 3 *izbor forenzičke slike u Autopsy alatu*

Figure 3 *selecting forensic disk image in Autopsy tool*

On the previously described CFReDS portal, a

Slika 4 *UNICODE prikaz forenzičke slike tvrdoga diska*

Figure 4 *UNICODE forensic image of hard disk*

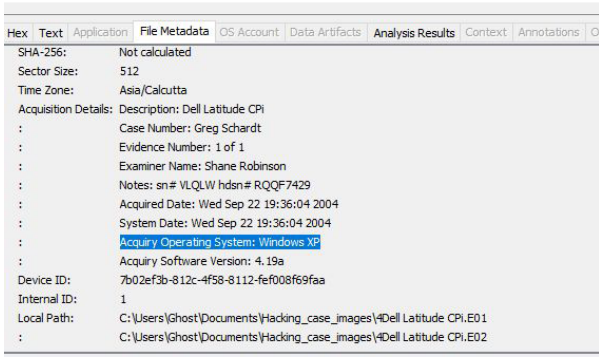
forensic image of the hard drive from the hacker case is available in *EnCase* format [6]. When an investigator (or forensic expert) uses the EnCase format to create a data backup, a procedure known as disk imaging is performed [7],[9]. During the creation of a forensic hard drive image, *EnCase* records the data in a series of separate files of 640 MB each, so the complete forensic image may consist of multiple such parts (E01 format). Each of these files stores the raw disk data in UNICODE encoding [8], allowing for consistent interpretation of the content. Despite being divided into multiple files, the final result is a single unified forensic image of the hard drive. Due to its practicality and widespread use, the *EnCase* format was used in this research. After the forensic image was loaded, the preparation phase for analysis was considered complete, followed by the extraction and interpretation of evidence.

3. REZULTATI FORENZIČKE ANALIZE

3. FORENSIC ANALYSIS RESULTS

Knowledge of the operating system used on the examined device is an important aspect of forensic analysis, as the OS influences the structure of the file system, the locations of artefacts, and the tools available to an attacker. In the acquisition metadata of the forensic image ("Acquisition Operating System" field, Figure 5), the Autopsy tool explicitly identified Windows XP as the installed operating system. This confirmation allows investigators to focus on locations and artefacts specific to Windows XP and to interpret the discovered records in their proper context.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
4Dell Latitude CPi.E01	Image	4871301120	512	Asia/Calcutta	7b02ef3b-81



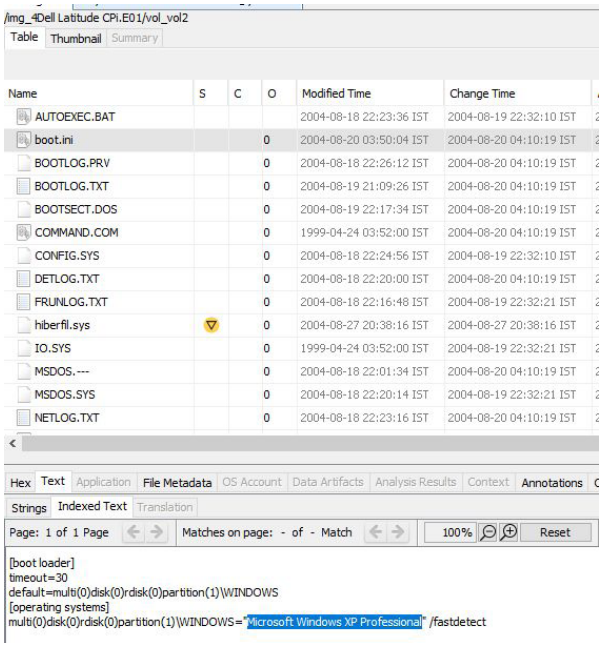
Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations

SHA-256:	Not calculated
Sector Size:	512
Time Zone:	Asia/Calcutta
Acquisition Details:	Description: Dell Latitude CPi
:	Case Number: Greg Schardt
:	Evidence Number: 1 of 1
:	Examiner Name: Shane Robinson
:	Notes: sn# VLQLW hdsn# RQQF7429
:	Acquired Date: Wed Sep 22 19:36:04 2004
:	System Date: Wed Sep 22 19:36:04 2004
:	Acquiry Operating System: Windows XP
:	Acquiry Software Version: 4.19a
Device ID:	7b02ef3b-812c-4f58-8112-fef008f69faa
Internal ID:	1
Local Path:	C:\Users\Ghost\Documents\Hacking_case_images\4Dell Latitude CPi.E01
:	C:\Users\Ghost\Documents\Hacking_case_images\4Dell Latitude CPi.E02

Slika 5 *informacije o operativnom sustavu*

Figure 5 *operating system information*

Additional information on the operating system was also found in the *boot.ini* file. The *boot.ini* file is a text file that contains information required during the computer's startup process, including detailed data about the operating system. The file is located at the "*C:\boot.ini*" path within the forensic image. By analysing this file—specifically by opening it in the Autopsy tool—an additional and useful detail was revealed: the use of the professional version of the *Windows XP* operating system (Figure 6).



Slika 6 *detaljne informacije o operativnom sustavu, boot.ini pregled kroz Autopsy*

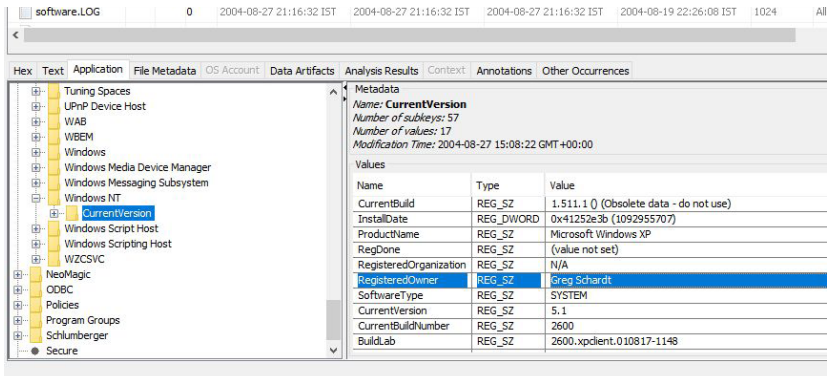
Figure 6 *detailed information about operating system, boot. ini trough Auttopsy view*

Similarly, by examining characteristic files within the forensic image using the Autopsy tool, additional relevant information was identified, confirming the results of the tool's automated forensic analysis.

To link the computer to the suspect, evidentiary materials such as registration identification and user names of specific accounts are required. The *Windows* operating system contains information about registered users, where a registered user is the individual to whom the product licence is assigned. Information about the registered user was found at the path "*C:\Windows\system32\config\Software\Microsoft\WindowsNT\CurrentVersion\RegisteredOwner*". The registry metadata identified Greg Schardt as the registered user of the operating system (Figure 7).

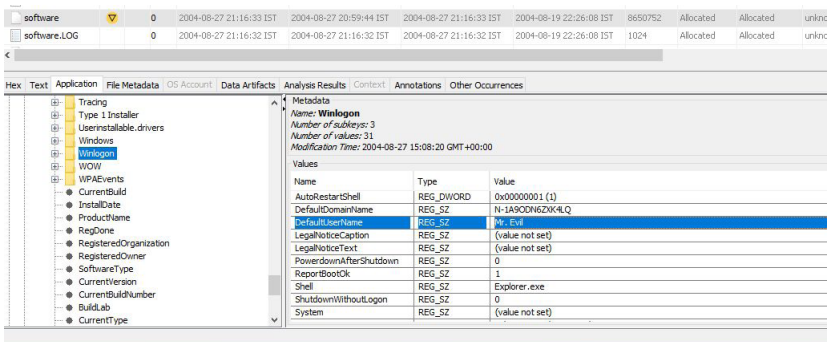
In addition to the registered user information, the username of the account was also found. The account name in the Windows operating system was located in the *winlogon* file. The *winlogon* file is used for user session security and for loading the user profile during startup or account lock. The *winlogon* registry key was located at "*C:\Windows\system32\config\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon*". The username within the file corresponds to the registry value *DefaultUserName* and has the value: Mr.Evil (Figure 8).

In forensic analysis, a highly valuable piece of information is the time when the computer was last used, specifically when it was shut



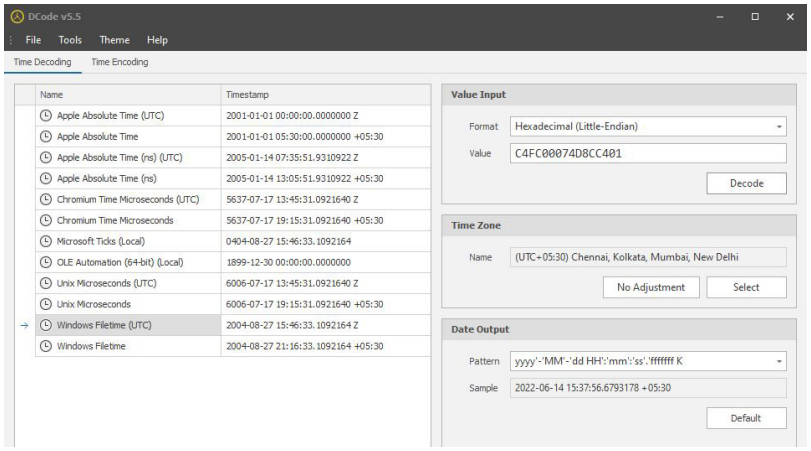
Slika 7 *Greg Schardt kao registrirani vlasnik*

Figure 7 *Greg Schardt as registered owner*



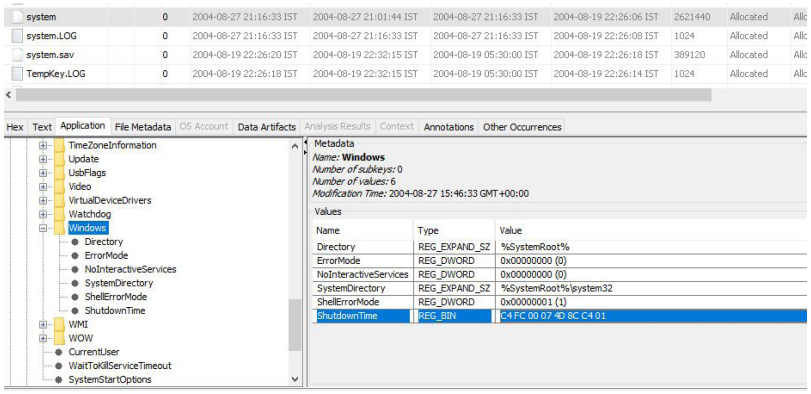
Slika 8 *ime windows korisničkog računa*

Figure 8 *windows profile username*



Slika 9 *zadnje vrijeme gašenja u UNIX formatu*

Figure 9 *last shutdown time in UNIX format*

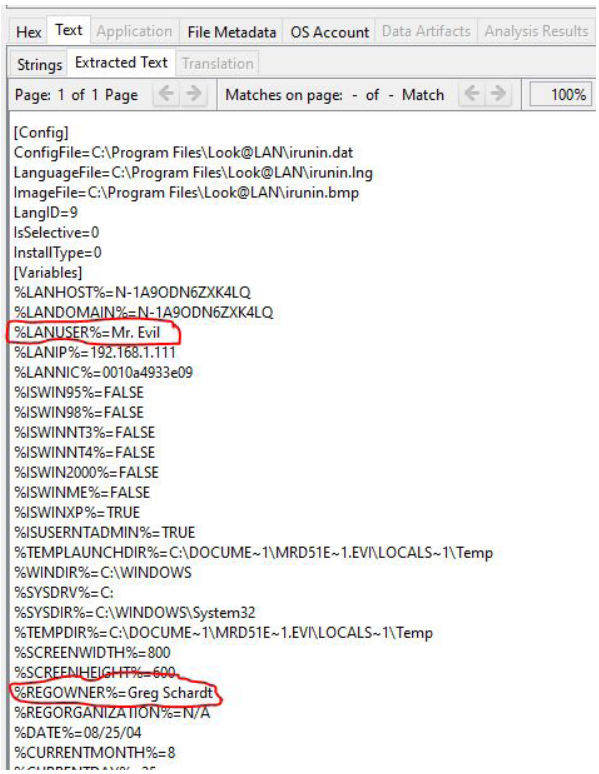


Slika 10 *zadnje vrijeme gašenja operativnog sustava u formatu čitljivom ljudima*

Figure 10 *last shutdown time in human readable format*

down. information about the last use of the computer can link the physical machine and the operating system to the time period during which the attack on the victim occurred. Data regarding the last system shutdown were found at the path "*C:\windows\system32\config\system\CurrentControlSet\Control\Windows\ShutdownTime*". The *ShutdownTime* registry contains the value of the last computer shutdown in hexadecimal format (Figure 9). To convert the hexadecimal value into the *Windows Filetime (UTC)* format (human-readable), a free tool called *DCode* was used (Figure 10). The decoded value was read as *2004-08-27 15:46:33.1092164 Z*.

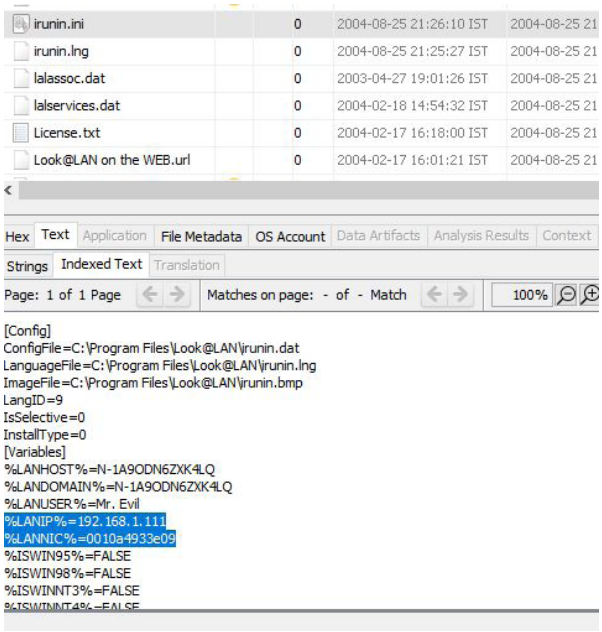
Although Greg Schardt was recorded as the registered user on the computer, and "Mr.Evil" as the account name, a forensic proof requires a computer record that directly links the registered user to the user account. At the path *C:\Program Files\Look@LAN\irunin.ini*, the registry entries *%LANUSER%* and *%REGOWNER%* were found, demonstrating the direct connection between the *LAN* user and the registered user (Figure 11).



Slika 11 *direktna poveznica između Gregg Schardta i pseudonima „Mr.Evil"*

Figure 11 *direct link between Greg Schardt and „Mr.Evil" pseudonym*

Knowledge of the IP (*Internet Protocol*) address and MAC (*Media Access Control*) address is crucial in forensic analysis and in identifying the attacker. The IP address enables identification of the laptop on the internet, while the *MAC* address provides identification at the local network level. Together, these addresses serve as evidence for confirming the identity of the laptop. The details of the *IP* and *MAC* addresses were found in the *irunin.ini* registry entries (Figure 12), located at *C:\Program Files\Look@LAN\irunin.ini*. Authorities often use the discovered *IP* address to request additional information about the attacker from the *ISP* (*Internet Service Provider*).



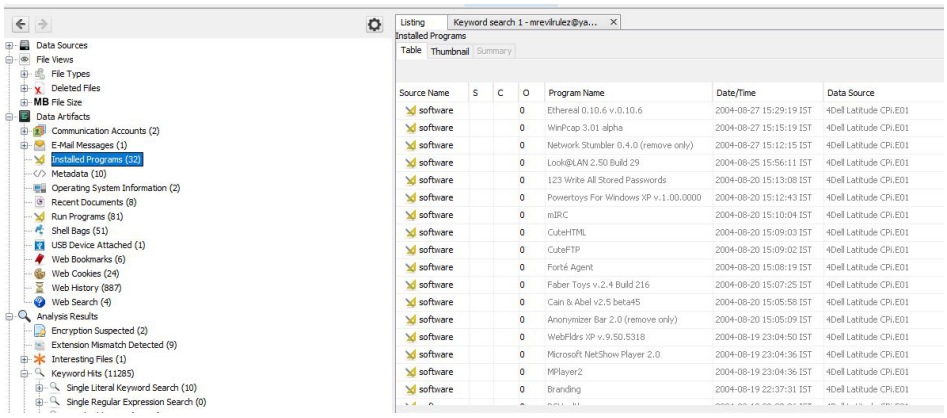
Slika 12 *IP i MAC adrese na forenzičkoj slici*

Figure 12 *IP and MAC addresses on forensic image*

Evidence in court proceedings can also include tools or applications installed or used on the attacker's device. Certain applications are developed solely for criminal activity and thus directly link the malicious user to the type of attack. Data on installed programmes in the "*Mr.Evil*" forensic image are found in the left selection pane of the Autopsy tool under *Data Artifacts -> Installed Programs* (Figure 13). Among the installed programmes, a total of six were identified as potentially usable for unauthorised access: *Cain & Abel v2.5 beta45* (a password-cracking tool), *Ethereal 0.10.6 v.0.10.6* (an advanced network analysis tool), *Network Stumbler 0.4.0* (a wireless LAN detection and attack tool), *Look@LAN 2.50 Build 29* (an advanced network monitoring tool), *123 Write All Stored Password* (a tool for printing all current user passwords that are logged and saved in the *Microsoft PWL file*), and *Anonymizer Bar 2.0* (a tool that attempts to provide internet anonymity).

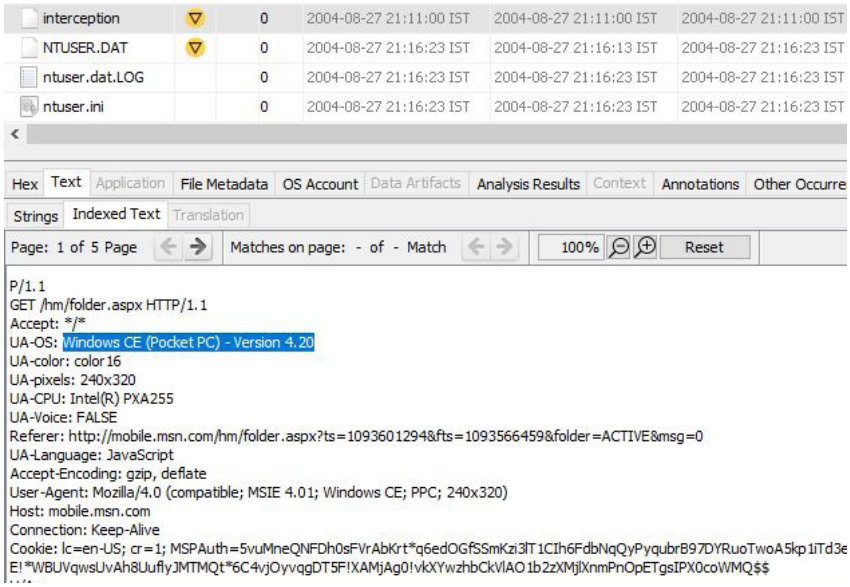
Based on the identified tools, insight can be gained into the types of hacking attacks. For example, Ethereal is a popular "*sniffing*" programme used to intercept both wired and wireless internet packets. The collected network traffic is saved in the attacker's default directory, in a file named *interception*. In this case, the full path on the attacker's forensic image is: *C:\Documents and Settings\Mr. Evil\interception*. Further analysis of the registries and the *interception* file provided information about the type of the victim's wireless device (Figure 14), as well as the website the victim accessed (Figure 15). The device used was identified as Windows CE (*Pocket PC*), and the website accessed by the victim was *mobile.msn.com*.

Potentially security-relevant files were also found



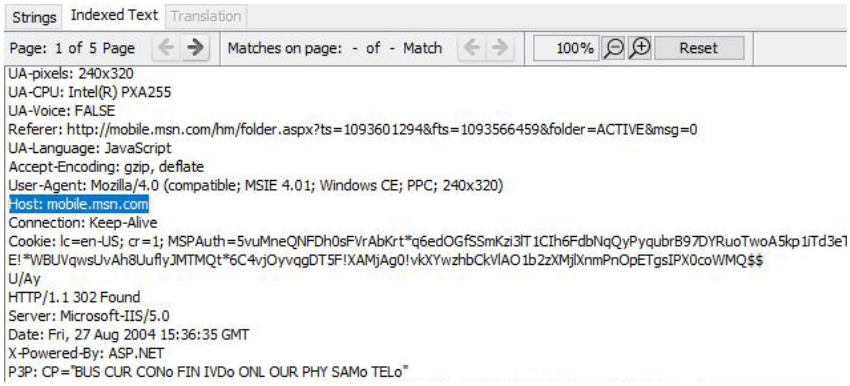
Slika 13 *lista instaliranih programa*

Figure 13 *list of installed programmes*



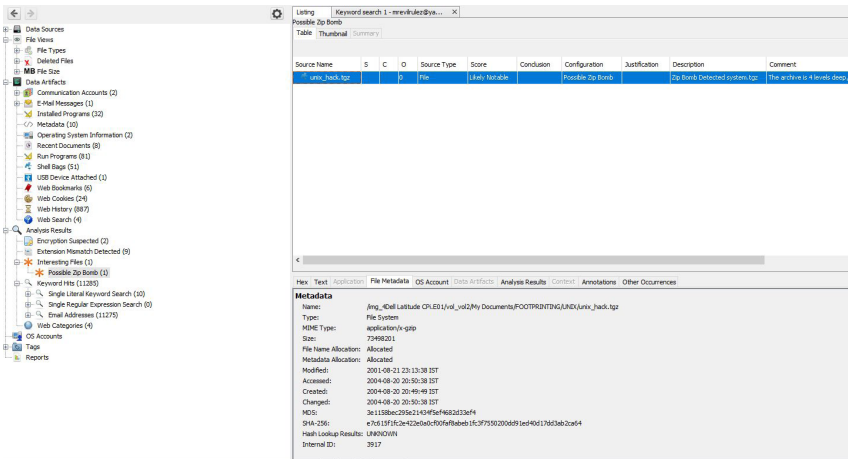
Slika 14 *vrsta bežičnog uređaja korištenog od strane žrtve*

Figure 14 *Type of wireless gadget used by the victim*



Slika 15 *web stranica kojoj je pristupila žrtva*

Figure 15 *Web address accessed by the victim*



Slika 16 *informacije o zip bombi*

Figure 16 *information about zip bomb*

on the forensic image of the laptop, which the Autopsy tool stores under *Interesting Files*. It was detected that the attacker's computer contained a "zip bomb." A zip bomb is a type of compressed archive file designed to create a large disparity between the compressed and decompressed content. The bomb consists of multiple nested archives within a main archive. Each level is nested and contains copies of the same archive, which can be recursive, meaning the pattern repeats at each level, and exponentially increases the total decompressed size. It is most often used to disable antivirus software or to carry out an attack while antivirus protection is disabled. The path of the zip bomb is "*C:\My Documents\FOOTPRINTING\UNIX\unix_hack.tgz*" (Figure 16).

4. OGRANIČENJA UPOTREBE ALATA AUTOPSY I USPOREDBA S DRUGIM FORENZIČKIM RJEŠENJIMA

4. LIMITATIONS OF USING AUTOPSY TOOL AND COMPARISON WITH OTHER FORENSIC SOLUTIONS

Although Autopsy was selected as the primary tool for forensic analysis in this study due to its availability, ease of use, and open-source nature, it is important to acknowledge its limitations and compare it with other forensic solutions. Autopsy is highly effective for basic analyses such as file browsing, metadata examination, and detection of known artefacts. However, its functionality in some areas lags behind commercial solutions such as *EnCase, FTK* (*Forensic Toolkit*), or *X-Ways Forensics*. For example, while Autopsy offers modularity and extensions, its capabilities for deep memory analysis, network traffic examination, or processing large data volumes are limited compared to these tools. *EnCase*, as the industry standard, provides advanced automation features, encrypted analysis, and more detailed reporting. *FTK* integrates a powerful indexing and searching system, enabling faster analysis of large datasets. Furthermore, Autopsy can sometimes be unreliable in decoding certain file formats or when dealing with sophisticated attacks involving anti-forensic techniques.

Therefore, in professional investigations, it is advisable to use a combination of tools depending on the nature of the case to ensure the most comprehensive and precise forensic analysis. Autopsy certainly holds an important place in education and basic analyses but in more serious cases, a critical approach to its capabilities and supplementation with other tools is recommended.

5. ZAKLJUČAK

5. CONCLUSION

This paper illustrates the complexity and significance of digital forensics in the contemporary field of information security. The analysis of the NIST hacker case using the Autopsy tool not only provided concrete evidence but also demonstrated how digital forensics can reveal complex patterns of malicious activity. Through detailed investigation of digital traces, the case highlights the importance of forensic precision and methodology in identifying and understanding hacking tactics.

The forensic image created on a Dell CPI computer served as the primary data source for the investigation. The analysis encompassed the operating system, registered users, system shutdown data, IP and MAC addresses, and installed hacking and network monitoring programmes. Particularly significant was the discovery of the Look@LAN application, a network monitoring tool whose logs directly linked the real user to the pseudonym Mr. Evil, as well as the presence of a zip bomb.

However, the analysis did not reveal all potentially relevant evidence. Notably absent were data from volatile memory (RAM) and network traffic, which could provide more detailed real-time insight into attacker activities. Such evidence could be collected in future investigations using specialized tools such as the Volatility Framework for memory analysis and Wireshark for capturing and interpreting network packets. These data were unavailable because the forensic analysis was performed on a powered-off system.

Key evidence found on the laptop included usernames, IP and MAC addresses, installed hacking tools, and logs from applications such as Look@LAN. These elements collectively confirm the connection between the name Greg Schardt and the pseudonym Mr. Evil, as well as the use of the computer for unauthorised access to wireless networks.

6. REFERENCE

6. REFERENCES

[1.] Nikkel, B.; Practical Forensic Imaging; No Starch Press; ISBN: 9781593278007, 1593278004; 2016.

[2.] Boddington, R.; Practical Digital Forensics; Packt Publishing; ISBN: 9781785881084, 1785881086; 2016.

[3.] NIST; What is CFReDS; https://cfreds.nist.gov/ [12.2.2024.]

[4.] Johnson, C.R.; Digital Investigations, The Forensic Process and Examination of Digital Evidence; Elsevier Science & Technology; ISBN: 9780128184424, 0128184426; 2021.

[5.] Carrier B.; Autopsy® is a digital forensics platform and graphical interface; https://www.sleuthkit.org/autopsy/ [23.2.2024.]

[6.] Olivier S., M.; Shenoi, S.; Advances in Digital Forensics II; Springer US; ISBN: 9780387368917, 0387368914; 2006.

[7.] Palaniappan S.; Abd M., A.; Digital Computer Forensic: Validation and Verification for Disk Imaging: A Comprehensive Validation and Verification (V&V) Disk Imaging Model for Court of Law Admissibility; LAP LAMBERT Academic Publishing; ISBN: 9783847326977, 384732697X; 2012.

[8.] Korpela, J.; Unicode Explained; O'Reilly Media; ISBN: 9780596101213, 059610121X; 2006.

[9.] Vandeven, S: Forensic Images: For Your Viewing Pleasure; https://www.sans.org/white-papers/35447 [23.2.2024]

AUTORI · *AUTHORS*

• **Jan Lamza** - Born in 1997 in Zagreb, attended elementary school in Zagreb, and completed high school at the Catholic boarding school Pazinski Kolegij s pravom javnosti. He graduated with a bachelor's degree in Computer Science from the Faculty of Engineering in Rijeka. He is an employee of the Ministry of the Interior. He is an outstanding graduate student in the master's programme of Information Security and Digital Forensics at the Polytechnic of Zagreb. His areas of interest include information security, digital forensics, software engineering, and artificial intelligence.

Korespondencija · *Correspondence*

janlamza12@gmail.com

• **Damir Delija** - PhD, Associate Professor – has been working at TVZ since 2017 and has held a PhD since 1989. He specializes in digital forensics and computer security and teaches these subjects in the master's programme in Information Security and Digital Forensics. During his career, he was a consultant at INsig2, where he was responsible for leading the digital forensics department. He specializes in Guidance Enterprise and EnCase software, UNIX, and network forensics. Damir is also a trainer with extensive knowledge of the Guidance product suite for digital forensics (Cybersecurity, eDiscovery, Enterprise, FIM) and digital forensics in general. He holds EnCE and UFED certifications, as well as certifications in cybersecurity, eDiscovery, EnScript, and various other Guidance Software products. Damir has conducted various trainings for law enforcement agencies and other organizations.

He holds a PhD in electrical engineering and is a versatile trainer and expert lecturer. During his professional career, he has worked on ship system automation, AIX and UNIX system administration, network administration, and is also an AIX systems trainer. He has participated in various projects related to the development and implementation of ICT systems and has been involved in general IT training and consulting. He also teaches at Algebra University College and the College of Information Technology in Zagreb.

Korespondencija · *Correspondence*

damir.delija@tvz.hr