

Forensic Investigation Report

Table of Contents

Table of Contents.....	1
Executive Summary	2
Overview and Case.....	4
I. Problem Statement.....	5
II. Overview.....	5
III. Case.....	5
IV. Forensics Procedure.....	6
Relevant Literature.....	8
I. Introduction and Overview.....	9
II. Legal Compliance.....	9
III. Processes.....	14
IV. Procedures.....	17
V. Theory of device.....	22
Processes and Procedures.....	27
I. Introduction.....	27
II. Chain of Custody	28

III. Tools	29
IV. Forensic procedure.....	32
Analysis.....	33
I. Introduction.....	34
II. Collected Evidence	39
III. Interpretations.....	63
IV. Evidence Table.....	64
Conclusion.....	70
I. Application.....	70
II. Alternatives.....	71
III. Future Work.....	71
Exhibits	72
References.....	74

Executive Summary

The following executive summary encapsulates the outcomes of a comprehensive digital forensics' investigation triggered by a suspected hacking incident involving an abandoned Dell CPi notebook computer, a wireless PCMCIA card, and an external homemade 802.11b antenna. This investigation's main objective was to identify traces of hacking software, ascertain evidence of its utilization, and uncover any data generated as a result. Furthermore, the inquiry aimed to definitively link the abandoned CPI notebook computer to its owner, Greg Schardt, alias "Mr. Evil," if applicable.

Employing industry-standard tools such as Autopsy and Kali Linux Forensic Mode, the investigative team meticulously acquired and analyzed digital evidence. The analysis uncovered the presence of several hacking tools and programs, including password-cracking utilities, network sniffers, network scanners, and proxy tools. Moreover, visits to online forums and websites associated with hacking and illicit activities strongly implicated the involvement of the suspect, "Mr. Evil," believed to be synonymous with Greg Schardt. The information regarding the owner of the laptop and OS installation also corroborates that the real culprit was "Greg Schardt" alias "Mr. Evil".

This investigation underscored the critical role of digital forensics methodologies in uncovering evidence pertinent to cybercrime incidents. It emphasized adherence to established processes and procedures in evidence collection and examination, including hash calculation, chain of custody maintenance, and utilization of approved forensic tools. The findings underscored the imperative for robust digital security measures to safeguard sensitive data and detect cyber threats

effectively. Notably, the evidence gathered during the investigation holds legal validity and can be presented as admissible evidence in a court of law.

In conclusion, this investigation yielded invaluable insights into the nature of the hacking incident and the methodologies employed by the perpetrator. It underscores the significance of leveraging digital forensics techniques to detect and investigate cybercrime incidents effectively. Implementing proactive security measures and harnessing forensic expertise can ultimately aid in preventing future incidents and safeguarding critical data.

Overview and Case

I. Problem Statement

Group 6 aims to analyze the evidence involving an abandoned CPi notebook computer, with the serial number VLQLW, alongside a wireless PCMCIA card and an external homemade 802.11b antenna, potentially linked to the suspect, Greg Schardt [1]. The goal is to identify traces of hacking software, evidence of its utilization, and any data generated as a result [1]. Additionally, the investigation seeks to establish a link between the computer and Greg Schardt [1]. Through hands-on experience with forensic tools and real-world case analysis, Group 6 aims to enhance their skills in identifying and recovering digital evidence.

II. Overview

An initial investigation revealed that an online persona known as "Mr. Evil," is believed to be an alias used by Greg Schardt. Information has surfaced indicating that Mr. Schardt partakes in illegal practices such as intercepting internet traffic to obtain sensitive information, including stealing credit card details, usernames, and passwords [1]. Insight provided by associates of Greg Schardt suggests he conducts this activity by strategically positioning his vehicle within range of wireless access points, notably at locations such as Starbucks [1].

The primary objective of this investigation is to identify any traces of hacking software, find evidence of its utilization, and uncover any data generated as a result. Additionally, the investigation seeks to establish a definitive link between the abandoned CPi notebook computer and Greg Schardt

III. Case

A CPi notebook computer, identified by the serial number VLQLW, was discovered abandoned alongside a wireless PCMCIA card and an external homemade 802.11b antenna [1].

The circumstances surrounding this discovery immediately raised concerns regarding potential involvement in illegal activities, prompting an investigation to establish any connections to the suspected individual, Greg Schardt [1].

In the modern era, technology is used everywhere in our daily lives. As a result, digital forensics is rapidly becoming an integral part of investigative processes [2]. For example, it is tough to find a criminal case today that doesn't have a connection to technology [2]. Digital forensics isn't just for law enforcement however, it is a tool used by many to conduct investigations [3]. Digital forensics investigation can reveal a great deal of information. Information such as the cause and implications of cyberattacks, identifying whether data was accessed or exfiltrated, retracing attackers' steps, identifying tools used, remediating attacks, identifying the duration of unauthorized access, and much more [3]. Digital forensics is useful field and training digital forensics will equip professionals with the knowledge needed to identify and recover digital evidence [4]. To gain the technical and practical skills needed to excel at digital forensics, a professional should have a good understanding of computer systems and operations and networks. [4]. The beginning few weeks of CIT 56200 focused on just that. The class focused on Windows, Linux, and Mac operating systems, and important details from each, as well as network infrastructure over a few weeks. Additionally, to excel at digital forensics a professional should try to gain hands-on experience with forensic software by using it in a realworld scenario [4]. For example, the Schardt case in this report or the cloud labs from Jones & Bartlett Learning. This project is an attempt to gain additional hands-on experience with using digital forensic tools and to gain experience with analyzing evidence, detecting and interpreting data, and report writing.

IV. Forensics Procedure

In this investigative scenario, as a digital forensic examiner, the focus of our team is on gathering comprehensive information concerning the missing Dell laptop. Essential details encompass the laptop's specifications, including the operating system, hard drive characteristics, installed software, and any stored user accounts or files. This prospective data has the potential to offer essential hints regarding the alleged hacking incident. Utilizing tools like `dcfldd` and `dc3dd` enables the creation of a DD image, facilitating in-depth analysis of the laptop's data.

Attention is also directed towards the wireless PCMCIA card and the external 802.11b antenna, both found alongside the laptop. Their potential role in hacking activities, particularly wireless communication interception, necessitates thorough examination. The setup suggests a possible intent for unauthorized data collection, with the devices likely enhancing wireless signal range and strength.

The presence of any hacking software or tools on the laptop is of utmost significance. This encompasses tools such as password crackers, network scanners, or other software typically associated with hacking endeavors.

Additionally, obtaining network logs and traffic data corresponding to the period when the suspect purportedly utilized the laptop can provide crucial insights. Analyzing these logs may reveal the nature of the attacker's activities and the network connections established.

Documentation of the forensic methodologies and tools employed throughout the investigation process is paramount for maintaining a comprehensive record of procedures and findings.

Upon discovery of the abandoned laptop, alongside the PCMCIA card and antenna, the local police promptly notified our forensics team, who subsequently arrived at the scene. The devices were secured and documented without any alterations or tampering. Detailed records were maintained, including the make, model, type, serial number, power state, and condition of each device, before they were securely stored in anti-static bags for protecting from electrostatic discharge (ESD).

Following proper protocols, the collected devices were transferred to the nearest Computer Forensics Laboratory (CFL) for processing and storage pending the legal formalities to start the evidence investigation. After obtaining legal approval, a DD image of the laptop was created using Kali Forensic mode, dcfldd, and dc3dd. This image was analyzed using Autopsy [5] to identify any presence of hacking software, evidence related to the suspected hacker, and the data contained within the laptop.

Relevant Literature

I. Introduction and Overview

It is vitally important that individuals dealing with digital forensic investigations adhere to applicable laws, regulations, and legal guidelines. The consequences of violating the standards above can be severe, potentially resulting in legal consequences or undermining the integrity of an investigation [6]. Since digital forensics is used often by law enforcement it is especially important that laws and compliance be met. Agencies must operate within the limits of the law when gathering and analyzing digital evidence, this is because any violation of legal rules can have serious repercussions [6].

II. Legal Compliance

One of the biggest laws to be aware of for law enforcement conducting an investigation is the Fourth Amendment. The Fourth Amendment serves as a vital safeguard against unreasonable searches and seizures by the government [7]. This fundamental protection extends to various contexts, including searches conducted within homes, interactions with individuals, searches of vehicles, encounters at schools or border checkpoints, and in our case the search and seizure of electronic devices [7].

In the United States of America, there are rules like the Exclusionary rule that stands as a legal safeguard against unlawful searches and seizures [8]. The Exclusionary rule will penalize law enforcement should they obtain evidence illegally by making evidence that is in violation of the Fourth Amendment inadmissible [8]. Interestingly though this rule only applies to law enforcement, and evidence that is unlawfully obtained from a private person is admissible in criminal courts [9]. Even though the rule could make illegally obtained evidence by private citizens admissible in criminal court, it doesn't mean that this is good practice. There is a myriad of laws that could be broken when collecting digital evidence. When law enforcement is investigating, a search warrant may be issued to search a device if there is probable cause to believe that the media contains evidence of a crime, fruits of crime, and an instrument of a crime [10]. Additionally, a device can be searched with consent or a court order. A search warrant must describe in particular the place to be searched for and the items to be seized [10]. For example, if a mobile phone was issued a search warrant you might see inside of the warrant the type of phone, maybe an Apple iPhone 14 with the model number, and the list of objects to be seized. These items could be phone calls, text messages, voicemails, emails, video, audio, photographs, etc. When a private investigation is being conducted a search warrant is typically not needed as

especially if it is an internal investigation of a network or systems where the investigators have lawful control over the infrastructure being investigated [10]. Other laws, regulations, and agreements would need to be complied with, however. In the United States there are a few important laws to be aware of. The first is the Cybersecurity information Sharing Act of 2015. This law allows the sharing of internet traffic information between the United States government and technology and manufacturing companies [11]. This sharing of information can be extremely critical for digital forensic investigations. Additionally, the Computer Fraud and Abuse Act or CFAA is good to be aware of. The CFAA is an important law for prosecutors to address cyber base crimes. The law criminalizes malicious computer usage and unauthorized access to computer systems [12]. Digital forensic investigators will rely often on the outlined definitions of the CFAA to determine whether an individual or organization has unlawfully accessed or obtained information [12]. For example, digital forensic investigators often will be hired to investigate cases of unauthorized access, and other malicious activities, which are criminalized by the CFAA.

Based on the case's facts, another law to be aware of is the ECPA or the Electronic Communications Privacy Act. The ECPA was enacted in 1986 [13]. The act is a federal statute governing the interception, use, and disclosure of electronic communications, protecting wire, oral, and electronic communications both in transit and when stored on computers [13]. The Electronic Communications Privacy Act (ECPA) holds significant importance in this case given the suspicion of illegal activities such as intercepting internet traffic and stealing sensitive information which Mr. Schardt is accused of. If Mr. Schardt is found to have violated the Electronic Communications Privacy Act (ECPA) through our investigation, he could face significant penalties depending on the nature and severity of the offense [14]. The penalties for

breaking the ECPA can include fines (up to \$250,000), imprisonment, or both [14]. For instance, under Title I of the ECPA, which deals with interception of wire, oral, or electronic communications, individuals convicted of the intentional interception, use, or disclosure of such communications without proper authorization could face fines and imprisonment for up to five years for a first offense [14]. Subsequent offenses may result in increased fines and longer periods of imprisonment [14]. Similarly, violations of Title II of the ECPA, which covers the protection of stored electronic communications and subscriber information, can lead to fines and imprisonment for up to one year for first-time offenders, with potential for harsher penalties for subsequent offenses [14]. The specific penalties imposed on Schardt would depend on various factors, including the extent of his involvement in the offense, any prior criminal history, and the discretion of the court handling the case [14]. Additionally, individuals whose information was stolen are entitled to bring civil suits and recover damages [14]. Since that is the main focus of our investigation it is good to be aware of it.

Sometimes digital forensic investigators will be tasked with investigating very sensitive information like medical records and financial data. Because of this it is important for digital forensic investigators to be versed in standards like the Health Insurance Portability and Accountability Act or HIPPA and the Payment Card Industry Data Security Standard or PCI DSS. Both standards impose strict privacy requirements and data security, which can impact digital forensic investigations.

For investigators who are investigating healthcare related incidents compliance with HIPPA is extremely important. If there is a data breach or suspected unauthorized access to personal health information it is important for digital forensic examiners to be compliant with HIPPA regulations. Should there be a failure to adhere to HIPPA it can result in severe penalties,

including fines and legal consequences [15]. Therefore, it is important to have a good understanding of HIPPA and ensure compliance with the requirements during an investigation. Doing so not only demonstrates professionalism, but it also can help ensure the confidentiality of sensitive data and mitigate potential legal problems.

Additionally, following PCI DSS is essential for digital forensic investigators handling cases involving payment card data breaches or fraud. PCI DSS outlines security measures to safeguard cardholder information, such as network segmentation, encryption, and regular security assessments [16]. When investigating incidents of payment card fraud or unauthorized access to cardholder data, forensic investigators must adhere to PCI DSS requirements to preserve the integrity of evidence and ensure compliance with industry standards [17]. Noncompliance with PCI DSS can lead to financial penalties, reputational damage, and loss of customer trust, underscoring the importance of incorporating PCI DSS principles into forensic investigation practices [17][18].

Now at this point those laws and regulations mentioned previously cover just the United States of America. In the digital world that we live in, individuals should not be surprised to find that digital crimes often transcend geography [19]. The fact that criminals can conduct cyberattacks from anywhere poses significant challenges for digital forensic investigators, as they must navigate a complex landscape of laws, regulations, and treaties that vary from one jurisdiction and country to another [20].

Probably the most important international laws that digital forensic investigators should be aware of is the General Data Protection Regulation or GDPR of the European Union. The GDPR is the strictest privacy and security law in the world [21]. It was put into effect in May of 2018 [21]. The GDPR imposes strict requirements on the handling and protection of personal

data of EU residents, regardless of where the data processing takes place. This means that even if a cybercrime originates outside the EU, if it involves the personal data of EU citizens [21].

Investigators must ensure compliance with GDPR provisions to avoid legal repercussions even if they are located outside of the EU [22].

Violators of the GDPR can expect harsh fines and penalties that can reach into the tens of millions of dollars [21]. In context of the GDPR digital forensic investigators will typically fall into the category of a Data processor, which is a third party that processes data on behalf of a data controller [21]. For example, typically investigators will be hired as a third party to conduct a forensic investigation. In this instance, investigators would be processing data on behalf of the organization that hired them and would be required to process the data in accordance with the instructions provided by the data controller as they own the data and can decide how it is processed [21]. The GDPR is just one of many international regulations that are in effect around the world. Digital forensic investigators must be mindful of the law pertaining to data and regional regulations, which may vary depending on the specifics of each investigation.

Another important set of rules that digital forensic investigators should be aware of are the Federal Rules for evidence. For instance, within the IMPD, digital examiners operating in the Digital Forensics Unit (DFU) frequently find themselves called upon to provide expert witness testimony in criminal trials, detailing their procedures regarding device examination. In this case, the rules important to these potential witnesses are FRE 701, FRE 702, FRE 703, FRE 704, and FRE 705.

Now even if we are investigating violations of the CSA, CFAA, and ECPA, we as investigators must follow those laws as well. This is why obtaining lawful permission is so important. Adherence to applicable laws, regulations, and legal guidelines is not just a

professional responsibility of a digital forensic examiner, but it is also a moral necessity [6] [23]. Violating these standards can have far-reaching consequences [6]. This could include jeopardizing the integrity of investigations and potentially leading to legal repercussions. Which we want to avoid at all costs.

III.Processes

The digital forensics process may change from one scenario to another. Typically, it encompasses four main stages: collection, examination, analysis, and reporting.

In the collection phase, digital evidence is acquired, often by seizing physical assets like computers, hard drives, or mobile phones. It is crucial to ensure that data integrity is preserved during this phase, which can be achieved by copying storage media or creating images of the original.

Moving to the examination phase, the focus is on identifying and extracting relevant data. This involves deciding whether to work on a live or dead system and determining which pieces of data are pertinent to the investigation within legal constraints.

The analysis phase utilizes the collected data to build or refute a case, answering key questions about data origin, modification, creation methods, and timing of activities. Additionally, the information's relevance to the case is evaluated, often involving reconstructing timelines and identifying behavioral patterns. This is the most time-consuming part of a forensic investigation and one's interpretation skills are tested. A good forensic investigator can interpret what the data means and its relevance to the case.

Finally, in the reporting phase, the synthesized data and analysis are presented in a format understandable to non-experts. These reports play a critical role in conveying information to stakeholders, ensuring clarity and accessibility while adhering to forensic reporting standards and guidelines.

In this forensic examination, the Forensics team adhered to fundamental principles before proceeding with their investigation. It is important to follow a systematic approach to establish the scene dimensions and identify potential safety and health hazards [24]. This involved meticulously assessing the environment to ensure the safety of personnel and preserve the integrity of the scene. Additionally, adhering to Locard's Exchange Principle, which suggests that every individual entering or exiting the scene can alter it, emphasized the importance of promptly securing the area to prevent contamination or tampering.

Trace Evidence is responsible for the examination of small (trace) particles of evidence left behind during a crime such as hair, fiber, paint, glass, tape, fire debris, and gunshot residue. This kind of evidence is often submitted in response to violent crimes including rape, homicide, robbery, arson, and hit-and-run incidents. Trace Evidence examinations are based on the Locard's Exchange Principle which states that any time two objects come into contact, there is an exchange of information. That exchange of information could be hairs in a sexual assault, paint in a hit and run, or glass in a breaking and entering [25]. Locard's principle also helps in crime scene reconstruction. Crime reconstruction is based at least in part on a firm understanding of Locard's exchange principle. This doctrine was enunciated early in the 20th century by Edmund Locard, the director of the first crime laboratory, in Lyon, France. Locard's Exchange Principle states that

with contact between two items, there will be an exchange of microscopic material. This includes fibers but extends to other microscopic materials like hair, pollen, paint, and soil.

By recognizing, documenting, and examining the nature and extent of evidentiary traces and exchanges in a crime scene, Dr. Locard postulated that criminals could be traced and later associated with locations, items of evidence, and persons (i.e., victims). The detection and identification of exchanged materials is interpreted to mean that two objects have been in contact. This is the cause-and-effect principle reversed; the effect is observed, and the cause is concluded. Understanding and accepting this principle of evidentiary exchange makes possible the reconstruction of contacts between objects and persons. Consequently, the incorporation of this principle into evidentiary interpretations is perhaps one of the most important considerations in the reconstruction of crime.

This principle holds in the digital world as well (although the concept of "crime scene" and "location" in general is not really defined) and, in fact, it holds whether someone is perpetrating a crime or not [26]. The famous The Westerfield-van Dam case of year 2002 also highlighted use of this principle [27].

Furthermore, the team prioritized planning, communication, and coordination as essential steps before proceeding with evidence collection. Developing a clear theory regarding the type of offense that occurred was crucial, as it allowed investigators to anticipate the evidence that might be present. In the specific case at hand, the team encountered a suspected abandoned laptop, prompting them to tailor their investigative approach accordingly.

The team ensured handling of original data with minimal contact. The team made copies of the information before the examination. This involved making complete bit-level copies of suspected storage devices using tools like EnCase and basic Linux commands. The team followed the

common practice of creating two copies of the drive, providing one for examination and keeping another as a backup.

The importance of handling original information with care stemmed from the risk of altering digital evidence each time it was touched. Even simple actions such as changing time/date stamps on files could compromise the validity of the evidence. Additionally, the principle of Locard's principle of transference [28] highlighted the necessity of preserving original information for review by other examiners, especially in situations involving opposing counsel hiring their own experts.

IV. Procedures

In digital forensics investigations, a range of procedures and protocols are employed to ensure the systematic collection, analysis, and presentation of evidence. One fundamental aspect is the establishment of a robust chain of custody, documenting the evidence's chronological history from collection to presentation in court. This protocol safeguards evidence integrity, ensuring it remains traceable to its original source without tampering.

Another critical procedure involves handling and preserving digital evidence to prevent contamination or alteration. Strict protocols dictate the use of write-blocking hardware or software to safeguard storage media, alongside meticulous documentation and secure storage practices. Forensic imaging techniques are utilized to create exact copies of storage devices, preserving original data while enabling analysis on duplicates, thus minimizing the risk of evidence compromise.

Procedures for data recovery employ specialized tools and techniques to retrieve deleted, hidden, or encrypted data. This may include file carving and memory analysis to reconstruct digital artifacts relevant to the investigation. During analysis, investigators follow systematic procedures such as file system analysis, keyword searching, and network traffic analysis to identify pertinent information, patterns, and anomalies.

Comprehensive documentation of investigation procedures, findings, and analysis is crucial for transparency and evidentiary admissibility. Reports generated during digital forensics investigations detail methodology, findings, interpretations, and any associated limitations or uncertainties. Legal and ethical compliance is paramount, requiring proper authorization, respect for privacy rights, and adherence to applicable laws and regulations.

Before initiating any forensic examination, the team developed an analysis plan to guide their work. This plan addressed various aspects such as evidence gathering methods, concerns about evidence alteration or destruction, appropriate tools for the investigation, and considerations related to the nature of the case (federal vs. state) affecting admissibility rules.

Creating an analysis plan is of paramount importance in digital forensics for several reasons such following: -

This first thing is focus and efficiency, as an analysis plan helps investigators stay focused on the objectives of the investigation. By outlining specific areas of interest, potential sources of evidence, and investigative techniques to be employed, it ensures that resources are allocated efficiently, and that the investigation proceeds in a structured manner.

Digital forensics investigations often involve vast amounts of data spread across various devices and storage mediums. An analysis plan ensures that all relevant sources of evidence are identified and examined thoroughly, minimizing the risk of overlooking critical information.

Adhering to legal and procedural requirements is essential in digital forensics investigations. An analysis plan helps ensure that investigative procedures comply with relevant laws, regulations, and organizational policies, thereby safeguarding the admissibility of evidence in court.

Digital forensics investigations can be complex and time-consuming, with various potential pitfalls and challenges. By developing an analysis plan, investigators can identify potential risks and develop strategies to mitigate them, thereby enhancing the overall effectiveness and integrity of the investigation.

An analysis plan serves as a roadmap for the investigation, documenting the rationale behind investigative decisions, methodologies employed, and evidence collected. This documentation is invaluable for maintaining transparency, accountability, and repeatability in the investigative process and for producing comprehensive reports for stakeholders.

Digital forensics investigations often involve limited resources, including time, manpower, and technology. An analysis plan helps prioritize tasks, allocate resources effectively, and manage expectations regarding the scope and duration of the investigation.

For this forensics examination case there are three members in the teams and an analysis plan provided a common framework for collaboration and communication. It ensured that all team members are aligned regarding the objectives, methods, and timelines of the investigation, thereby facilitating coordination and cooperation.

An essential step in the analysis plan involved creating an order of volatility to prioritize the collection of evidence based on its volatility level. This involved starting with the most volatile evidence, such as registers and cache, and proceeding to the least volatile sources like network topology.

The team also considered technical information collection considerations, including understanding the lifespan of information, collecting data quickly, and obtaining bit-level information. The lifespan of information varied based on factors such as network traffic duration or data stored in computer memory. Thus, the team acted swiftly to collect data before it became inaccessible or altered.

Collecting bit-level information was crucial for the investigation, as it provided the most accurate representation of data stored on hardware. This involved converting 1s and 0s into usable formats and evaluating whether unrelated bits were inserted. Bit-level tools enabled investigators to reconstruct file fragments, especially in cases where files were deleted or overwritten, providing a comprehensive view of the stored information beyond the file system's interpretation.

Forensic imaging is a crucial process in digital forensics examinations [29]. It involves creating a bit-by-bit, sector-by-sector copy of a physical storage device, such as a hard drive, USB drive, or solid-state drive (SSD). This process ensures that every single bit of data on the original storage device is accurately replicated in the forensic image.

In a bit-by-bit copy, every individual bit of data on the source storage device is duplicated onto the forensic image. This means that even the smallest unit of data, representing either a 0 or a 1, is faithfully reproduced. This level of precision is crucial in forensic investigations to maintain the integrity of the evidence.

Similarly, a sector-by-sector copy ensures that all sectors of the storage device are copied over to the forensic image, regardless of whether they contain active data, deleted data, or are unused. Sectors are the smallest addressable units on a storage device, typically containing 512 or 4096 bytes of data.

The forensic image includes not only the files and folders that are visible to the operating system (OS) but also unallocated space, free space, and slack space. Unallocated space refers to areas on the storage device not currently assigned to any file or data structure. Free space includes areas that are available for new data storage. Slack space refers to the area between the end of a file and the end of its allocated space in a sector.

One of the key advantages of forensic imaging is its ability to capture deleted files and fragments of data that may still reside on the storage device. Even though a file may have been deleted or the space it occupied marked as free, remnants of that file may persist in unallocated or slack space. Forensic examiners can analyze these remnants to potentially recover deleted evidence.

Maintaining the integrity and authenticity of digital evidence is paramount in forensic investigations. By creating a forensic image using a bit-by-bit, sector-by-sector copy process,

examiners can ensure that the original data remains unchanged throughout the examination process. This is essential for presenting the evidence in a court of law, where its admissibility may hinge on its integrity.

Forensic imaging prevents the loss of original data. These imaging tools and techniques are the only way to ensure that electronic data can be successfully admitted as evidence in a court or legal proceeding. Here the chain of custody is extremely important. It refers to a chronological trail that accounts for the possession, handling, and location of digital evidence from the moment it is collected to its presentation in court. This process is essential for establishing the integrity and authenticity of the evidence and ensuring its admissibility in legal proceedings.

Under US laws, particularly in criminal cases, the chain of custody is subject to rigorous scrutiny to ensure that the evidence presented in court is reliable and has not been tampered with or altered in any way.

V. Theory of device

The investigation was conducted on a Dell CPi notebook computer. It was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It has been determined that the operating system used on the laptop is Windows XP. Knowing how this operating system works will ensure that the laptop remains relatively unaltered during the investigation.

Most Windows operating systems like Window XP contain a registry, which is a repository that has all the information about the operating system. It will also store configuration information on any new program that was installed. For example, to find the installation date, the registry value

is stored in the “HKEY_LOCAL_MACHINE\Software” hive [30]. Another impotent registry to inspect is the "HKEY_CURRENT_USER" hive to learn about the currently logged-in user.

It would be imperative to determine the owner of this laptop and, by extension, the owner of the PCMCIA card and antennae. One can google how to locate the registry key which stores owner’s name. Its path should be “HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegisteredOwner”. The owner’s information is within the Local Machine hive.

A PCMCIA card can be viewed as an expansion card for a laptop. The PCMCIA card would also allow wireless network access. An IEEE 802.11b Wireless PCMICA card would be compatible with a type II or III PCMCIA slot. A laptop using Windows 98, 200, ME, or XP would instantly recognize the device and begin installation [33]. Upon successful installation, the PCMCIA card will be able to easily communicate with other IEEE 802.11b products [33]. With this setup, the laptop could connect to a wireless access point and collect traffic. The accompanying PCMCIA card will also prove useful.

A homemade 802.11b antennae was also discovered with the Dell laptop and PCMCIA card. It is possible to create a homemade antenna using common products such as aluminum cans [33].

With a simple search on Bing, one can find many tutorials on crafting a homemade one. There are even forums dating back to the early 2000s with users discussing crafting homemade antennas. Most of these designs involved physically aiming your antenna. To direct a homemade antenna’s signal, either the user must hold it in their hands or rig it to a simple tripod [33].

With Windows XP, there's a file called index.dat [33]. In Windows 7 and earlier versions used the index.dat file to index every website that was visited. It also contains Internet Cache, Cookies, History, and all emails sent or received through Outlook or Outlook Express [33]. Perhaps, searching through the laptop's index.dat file to check the user's search history to determine where they learned to make the antenna, where they planned to use the antenna, and for what purpose. Even if the user clears their browser history, the index.dat file should still house their data. It would be hard to remove both logically and physically. The attack could have cleaned it out, but since it was found connected to external devices, the index.dat file may still have data. One can use the freeware Index.dat Suite or Index.dat Scanner to view the index.dat file in Windows 7 or earlier [33].

It is suspected that this computer was used for hacking purposes. The antenna is most likely used to capture data from a nearby Wi-Fi network. Though, the antenna would need to avoid obstruction (like tree branches) to get a clear capture. 802.11b operated at 2.4 GHz, had an indoor range of 125 feet, with bandwidth of 11 mbps [30]. Also, since it's unregulated, 802.11b gear can incur interference from microwave ovens, cordless phones, and other appliances using the same 2.4 GHz range. However, by installing 802.11b gear at a reasonable distance from other appliances, interference can easily be avoided [34].

Disk and memory images were needed for processing. The disk image was acquired and created by FTK Imager. FTK Imager is a free data preview and imaging tool used to acquire electronic evidence in a forensically sound manner by creating copies of computer data without making changes to the original evidence.

The drives were imaged by using FTK Imager with evidence item and image mounting methods. FTK Imager is popularly used by law enforcement and, thus, shall be used in this case. This tool saves an image of a hard disk in one file or in segments that may be reconstructed later. Making copies of the computer data is necessary to preserve the integrity of the laptop.

When imaging, the “Verify Image” option will be selected by default. FTK Imager will create a cryptographic hash of the source drive and the image and compare them [30]. It helps preserve the integrity of the original laptop. The unallocated space of the disk must be examined for keywords. After that, it was analyzed by FTK Imager using evidence tree and Windows Explore methods. The last step in the process was reporting.

Autopsy was also used in this investigation. Autopsy is an easy to use, GUI-based program that allows you to efficiently analyze hard drives and smart phones [35]. Autopsy is important in the investigation as data files from the laptop are examined. With FTK, a disk image from the laptop will be generated. After the data source is added, ingest modules operate in the background to analyze the data. Depending on the size of the evidence, this process may take some time. Results are posted to the interface in real time and provide alerts as necessary.

As explained earlier, the Window XP also contains a registry that could contain information about the user of the laptop and any programs installed. It’s an important piece for a forensic investigation because of the great deal of information one could gather from it [30]. One registry to look at would Perhaps, there was a program that made use of homemade antennae.

Another location to examine would be the Recycle Bin. The user may have deleted some files to bury evidence. Since this laptop uses Windows XP, deleted files will be moved to a folder named “\Recycler\%SID%”, where %SID% is the security identifier (SID) of the currently logged-in user [30]. Each user on a Windows XP machine will have a hidden file called INFO32, which is created after the Recycle Bin is used. It keeps track of deleted files/folders, their original location, file size, and deletion time [30].

If the user already cleared Recycle Bin, there's no chance to restore deleted files from it. However, deleted data can still be recovered from the Windows XP computer as long as it has not been overwritten by new data [36]. Making sure that new data isn't added to this laptop will be imperative. Also, there are other recovery tools that allow one to retrieve deleted files from Windows XP.

One option could be using DiskDigger, which is described to be "easy-to-use." Although it can be downloaded free of charge, it would be best to use the commercial version of DiskDigger as the free version only recovers one file at a time and that would be time consuming. The commercial version allows multiple files to be recovered at once, cutting down on time. The program color codes the files based on how much was recovered. Green should mean that the entire file was recovered, yellow means a partial recovery, and red means that very little of the file was left [30].

Windows XP is also the first Windows operating system to have a firewall. Since all external traffic must come through the firewall, it is imperative that the firewall logs be examined

carefully. They usually contain valuable pieces of evidence. The user may have used decoy addresses [30].

Of course, log files will need to be viewed for the investigation. The user's activity will be documented in logs. Application logs record the time, date, and application identifier. It would reveal when an application was used. If the laptop has a packet sniffing application, knowing the time and date could help with the timeline of events [30].

Processes and Procedures

I. Introduction

The three most important processes in a forensic investigation are how evidence is preserved, who analyzes the evidence, and the standard required by the court. In our investigation, we're using Autopsy 4.21.0 to allow us to analyze disk images and search for evidence. Since we want to tamper with the evidence as little as possible, creating an image will ensure that we can still comb through the laptop's data without affecting the real device. Imaging a device will also allow our findings to be admissible in court [37]. We're also using CFREDS' Hacking Case Image as the base of our case. CFREDS is where we downloaded the image files of Mr. Schardt's

devices. By hashing the images with FTK imager after we downloaded them on Kali Linux, this ensures our evidence is reliable and our analysis is accurate.

II. Chain of Custody

Date & Time	Location	Description of Activity	Examiner
03/26/2024	Examiner's machine	Evidence collection: Downloaded DD images of the Dell CPI notebook computer, and laptop hardrive.	Group 6
03/26/2024	Examiner's machine	Evidence duplication and hashing.	Group 6
03/26/2024	Examiner's machine	Reconstructing drive image and formatting.	Group 6
03/26/2024	Examiner's machine	Imported drive image to Autopsy forensic tool	Group 6
03/26/2024	Examiner's machine	Conducted examination of	Group 6

		evidence using Autopsy	
03/31/2024	Examiner's machine	Examination complete	Group 6

III. Tools

In the forensic investigation of a hacking case, the use of certified and esteemed tools holds paramount importance in safeguarding the integrity and admissibility of evidence. In this context, four pivotal tools are discussed:

Autopsy 4.21.0 is widely acknowledged as a trusted open-source digital forensic tool and is instrumental in scrutinizing disk images and examining digital evidence. Built upon the Sleuth Kit, it furnishes users with a user-friendly interface conducive to conducting exhaustive forensic analyses.

Autopsy boasts several essential forensic features, each contributing to its efficacy in digital forensic investigations:

With its user-friendly web-based interface, Autopsy ensures accessibility for both seasoned professionals and novices in the field. This intuitive interface streamlines navigation through case details, evidence examination, and analysis, promoting efficiency in investigative processes.

A cornerstone of Autopsy's capabilities lies in its support for comprehensive disk image analysis. Whether sourced from hard drives, USB drives, or memory cards, Autopsy provides tools for scrutinizing disk partitions, file systems, and metadata, empowering examiners to delve into the minutiae of disk image contents.

Autopsy's robust search functionality facilitates thorough investigations by enabling the precise identification of pertinent files and artifacts. Through keyword searches within disk images, the team can swiftly uncover evidence germane to the case at hand.

The software's prowess extends to in-depth file system analysis, where teams can scrutinize file attributes, timestamps, and directory structures. This meticulous examination facilitates the reconstruction of file activity, aiding in the detection of anomalous behavior and the establishment of investigative leads.

Autopsy's support for timeline analysis proves invaluable in organizing and visualizing file system events chronologically. By creating timelines of file activity, teams can discern patterns, correlations, and event timelines, facilitating the reconstruction of digital incidents and enhancing the investigative process.

Further, Autopsy includes tools for artifact extraction from disk images, encompassing emails, chat messages, web history, and registry entries. These extracted artifacts furnish valuable insights into user activities and system interactions, bolstering the overall evidentiary foundation of investigations.

Autopsy also facilitates hash calculation and verification, allowing team to ascertain the integrity of evidence through cryptographic hashes such as MD5, SHA-1, and SHA-256. These hash values serve as crucial markers, ensuring data integrity and guarding against tampering throughout the investigative process.

Its robust capabilities render it indispensable for forensic examiners in uncovering evidence and constructing a compelling case. The utilization of Autopsy in this investigation underscores our commitment to upholding industry standards and best practices in forensic analysis.

At the crux of this investigation lies the Hacking Case Image provided by CFREDS (Computer Forensics Research and Education Directorate). CFREDS, renowned for furnishing high-quality forensic images for educational and investigative purposes, delivers a meticulously crafted artifact to simulate real-world scenarios. Laden with pertinent artifacts and evidence indicative of hacking activities, the Hacking Case Image enables us to conduct a thorough examination while adhering to ethical and legal standards.

Serving as a pivotal tool in this investigation, Kali Linux stands as a specialized Linux distribution tailored for penetration testing and digital forensics. Leveraging Kali Linux, the team orchestrated the creation of an evidence image from eight segregated parts of the forensic image. Moreover, Kali Linux facilitated hash value calculation, thereby ensuring data integrity and expediting evidence verification. Armed with an extensive suite of pre-installed tools and utilities tailored for forensic analysis, Kali Linux emerges as a dependable platform for navigating forensic examinations in intricate cases like this hacking incident.

Through the integration of Autopsy 4.21.0, the Hacking Case Image from CFREDS, and Kali Linux, the team underscores its commitment to employing reputable and accredited tools in forensic inquiries. These tools equip teams to conduct meticulous and defensible analyses, thereby contributing to the resolution of the hacking case with integrity and professionalism.

DCode is a FREE forensic utility for converting data found on desktop and mobile devices into human-readable timestamps [39]. It is the most comprehensive tool available for decoding timestamps. The software was designed to assist forensic examiners in identifying and decoding timestamp data during a forensic investigation.

IV. Forensic procedure

In digital forensics, the investigation involves the systematic examination of digital devices and data to uncover evidence for legal investigations. The use of validated and reliable tools is essential. These tools should adhere to industry standards and best practices. They help extract data without compromising its integrity. Many professionals request that forensically sound evidence must be a bit-by-bit copy of the original. Also, to ensure reliability, it is often advocated that the disk imaging process includes an audit trail that clearly records the success or failure of all or part of the copying process. [39]

First step is to take a picture of the laptop and all peripherals connected to the device.

There were two devices found along with the laptop: a wireless PCMCIA card and an external homemade 802.11b antennae. Next is to carefully search through the laptop without altering any existing settings or files. Obviously, we should tamper with the laptop directly as little as possible to preserve its integrity. A flash drive with FTK Imager will be inserted into the laptop to create an image. This way, nothing needs to be installed on the laptop itself.

On a machine other than the system to be imaged, we will install FTK Imager. Then, we will insert a flash drive formatted with either the FAT32 or NTFS file system. Once on the machine, the entire "FTK Imager" installation folder will be copied onto the USB drive. Once the file has been copied, the drive can be plugged into the target machine, the abandoned Dell laptop.

With the USB plugged into the laptop, Then, we will navigate to the folder where you extracted the files. Run FTK Imager.exe directly from the USB drive. Be mindful that error could occur while doing this step. Once it successfully completes, the next task will be acquiring volatile from a PC using FTK Imager.

With FTK Imager open, we navigate to the top left of the window, click on the "File" option, and select to capture memory option. We will be capturing the volatile memory of the PC or else the RAM. The memory dump contains juicy information which is useful to the investigators. When FTK asks for the source of the evidence, one will use the physical disk option, and which drive to pull the data [39].

With the source configurations established, next is to select the destination for the imaged copied. Here, one can choose a format for the image, such as "RAW (dd)" or "E01." The E01 format is recommended, as it allows for compression and the inclusion of metadata. With the E01 format, the user can choose the compression level and add a description or other relevant metadata. Additionally, you can choose to segment the image into smaller parts by specifying a maximum file size for each segment [39].

Now the imaging can begin. FTK Imager will create an exact copy of the hard drive, including any hidden or deleted data. This process may take a considerable amount of time, depending on the size of the hard drive and the chosen image format []. Following the

process, FTK Imager

hash for the image. To maintain the image's integrity, this hash value is essential [39].

To verify the image, choose "Verify Image" from the "File" menu and compare the hash value obtained with the original hard drive's hash value. The imaged copy's integrity is verified if the hash values match. This stage guarantees that the picture is a true representation of the original drive, hence it's crucial to record it [39].

Analysis

I. Introduction

The evidence in this hacking case comprises a Dell CPi notebook laptop, a wireless PCMCIA card, a homemade 802.11b external antenna, as well as DD and EnCase images of the computer generated during the investigation process. There is a suspicion that these devices were used for hacking purposes, specifically in intercepting internet traffic to acquire sensitive information such as credit card numbers, usernames, and passwords.

The objective of this investigation is to

discover evidence of any hacking software or data that might have been generated.

The local police stumbled upon a laptop, accompanied by a PCMCIA card and antennae, and promptly informed the team about the discovery. Upon arrival at the site, the team ensured the secure collection of the devices, meticulously documenting details such as make, model, type, serial number, power state, and condition. Each device was carefully labeled and stored in anti-static bags.

Subsequently, the collected devices were dispatched to the nearest Regional Computer Forensics Laboratory (RCFL), where they underwent processing and storage until the warrant for investigation was obtained. Once the warrant was secured, a DD image of the laptop was generated using Kali Forensic mode, dcfldd, and dc3dd. This DD image underwent thorough analysis using Autopsy to identify any presence of hacking software, evidence linking to the suspected hacker's identity, and examination of the data stored on the laptop.

In the realm of digital forensic investigation, every piece of evidence and information holds immense value in establishing a comprehensive understanding of the events in question. It is crucial to meticulously analyze each element to ascertain crucial details such as who was

involved, the actions undertaken, the methods employed, and the underlying motivations. Collected evidence not only sheds light on the perpetrator's intent but also potentially serves as legal evidence, providing valuable insights and supporting the investigative process. Through careful examination and interpretation of these evidentiary components, the team aimed to construct a thorough and accurate narrative of the events under scrutiny, enabling effective resolution and justice.

The Dell laptop encompasses comprehensive information regarding the operating system, specifics regarding the hard drive such as type and capacity, installed software, and any existing user accounts or stored files. Creation of a DD image using tools like dcfldd and dc3dd facilitates further analysis of the data housed within the laptop's hard drive.

Creating a forensic image of the laptop's hard drive using specialized tools like dcfldd and dc3dd is a critical step in the investigative process. This forensic image captures an exact replica of the digital evidence, preserving its integrity and ensuring that any subsequent analysis does not alter or compromise the original data. By scrutinizing this forensic image, the team can conduct

in-depth examinations of file systems, recover deleted or hidden data, and uncover artifacts relevant to the investigation.

The Dell laptop can play a pivotal role in the investigation by serving as a primary source of evidence and information. Its comprehensive nature provides the team with a wealth of data to analyze, aiding in the reconstruction of events and the identification of key findings crucial to the investigative process.

Analysis of the wireless PCMCIA card and external homemade 802.11b antenna: It's imperative to ascertain whether these peripherals were employed for illicit activities, potentially pertaining to hacking endeavors. Typically utilized for wireless communication, these devices might have been configured to intercept wireless signals, gathering information for unauthorized purposes such as data collection. By utilizing these devices, the perpetrator aimed to augment the range and potency of the wireless signal.

By scrutinizing these devices, the team aims to determine whether they were indeed employed in unlawful activities. The presence of a PCMCIA card and external antenna suggests a deliberate attempt to enhance wireless communication capabilities, potentially enabling the interception of wireless signals. This interception could facilitate the unauthorized gathering of sensitive information, including personal data, passwords, and other confidential details.

Furthermore, the configuration and usage patterns of these peripherals can provide valuable insights into the perpetrator's methods and intentions. By analyzing the settings and functionalities of the PCMCIA card and antenna, the team can reconstruct the perpetrator's

activities and discern their objectives.

Identification of any hacking software or tools present on the laptop: This involves detecting and documenting any tools or software utilized for hacking purposes, including but not limited to password cracking tools, network scanners, or other relevant applications.

By meticulously examining the laptop's software environment, the team aims to detect and document any tools or applications designed for hacking purposes. This includes password cracking tools, network scanners, remote access tools, and other relevant software commonly used by hackers.

The presence of such software can reveal the perpetrator's intentions and capabilities, shedding light on their expertise in cyber intrusion techniques and their potential access to sensitive information. Additionally, the documentation of these tools provides valuable evidence for legal proceedings, demonstrating the perpetrator's malicious intent and facilitating prosecution.

The identification of hacking software or tools on the laptop is essential for forensic investigation as it aids in understanding the nature of the cybercrime, establishing culpability, and safeguarding against future security threats.

Examination of network logs and traffic data: Whenever feasible, acquiring network logs and traffic data from the timeframe corresponding to when the suspect purportedly utilized the computer proves invaluable. Such data could yield crucial insights into the nature of the activities conducted by the attacker, as well as all network connections established during the said period.

Network logs and traffic data offer a comprehensive record of all network activities, including incoming and outgoing connections, data transfers, communication protocols used, and timestamps of events. By meticulously scrutinizing these logs, the team can reconstruct a detailed timeline of the suspect's online activities, including any attempts to access unauthorized resources or communicate with malicious entities.

Furthermore, network logs and traffic data is likely to help the team to identify patterns of behavior, establish correlations between different events, and uncover any anomalies or suspicious activities that may indicate unauthorized access or data exfiltration. This information is crucial for understanding the modus operandi of the attacker, determining the extent of the security breach, and assessing the potential impact.

Moreover, network logs and traffic data serve as valuable evidence in legal proceedings, providing concrete proof of the suspect's actions and intentions. They can be used to corroborate other findings gathered during the investigation and strengthen the case against the perpetrator.

IV. Evidence Table

Sr. No.	Items	Description
1.	Dell CPi notebook computer	Make: Dell Model: CPi Serial#: VLQLW The suspected laptop was used for hacking purposes.

2.	Laptop Hard Drive	Model: "IBM-DBCA-204860" Serial#: "HQ0RQQF7429" Drive Size: 4.5 GB All the intercepted data is present in the
----	-------------------	--

		hard drive and creating a DD image of the hard drive would help to investigate the data.
3.	Wireless card PCMCIA	The hacker might have used this device as an adapter to connect the homemade antenna.
4.	Homemade 802.11b antennae	The antenna is suspected to be used to increase the strength and range of the signals.
5.	DD Image	The DD image was created from the laptop hard drive and divided into 8 parts.
5.1.	SCHARDT.001	MD5 Hash value: 28A9B613 D6EEFE8A 0515EF0A 675BDEBD Sectors: 1301248
5.2.	SCHARDT.002	MD5 Hash value: C7227E7E EA82D218 66325739 7679A7C4 Sectors: 1301248
5.3.	SCHARDT.003	MD5 Hash value: EBBA35AC D7B8AA85 A5A7C13F 3DD733D2 Sectors: 1301248
5.4.	SCHARDT.004	MD5 Hash value: 669B6636 DCB4783F D5509C47 10856C59 Sectors: 1301248
5.5.	SCHARDT.005	MD5 Hash value: C46E5760 E3821522 EE81E675 422025BB Sectors: 1301248
5.6.	SCHARDT.006	MD5 Hash value: 99511901 DA2DEA77 2005B5D0 D764E750 Sectors: 1301248

5.7.	SCHARDT.007	MD5 Hash value: 99511901 DA2DEA77 2005B5D0 D764E750 Sectors: 1301248
5.8.	SCHARDT.008	MD5 Hash value: 8194A79A 5356DF79 883AE2DC 7415929F Sectors: 405524

II. Collected Evidence

As an examiner, Teams's initial step was to duplicate the evidence to ensure the preservation and security of the original data, safeguarding it from any inadvertent alterations during the investigative process. Utilizing the specialized forensic features of Kali Linux 2022.4 operating system, we conducted evidence acquisition. Given that the evidence was fragmented into eight parts, we proceeded to reconstruct the drive image within Kali Linux. Leveraging the cat command, we seamlessly reconstructed the evidence image. The resultant reconstructed drive image was formatted in .IMG, aligning with the compatible format for analysis within Autopsy. Downloaded all the evidence from the repository.

Figure 1 shows Mounted the shared folder on Kali Linux to create a combined image of part image evidence. for sharing folders with windows host.

```
(root@kali)-[/home/kali]
# sudo mkdir /mnt/shared_folder

(root@kali)-[/home/kali]
# mount -t vboxsf Mobile_Forensic_Project_Image /mnt/shared_folder
```

Figure 1: Mounting of folder on kali Linux

Figure 2 shows combined image from 8 segregated evidence

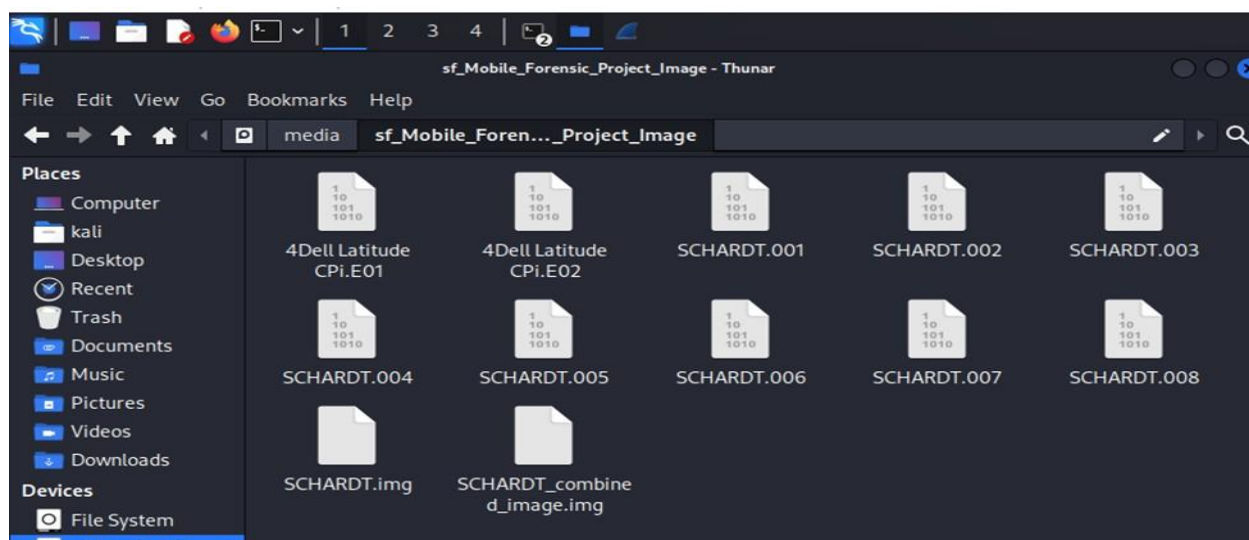


Figure 2: Combined image evidence

Hash calculation of combined image. Figure 3 shows calculation of hash value of created image. Hash calculation involves generating a unique alphanumeric string, known as a hash value or digest, from the contents of a file or data set. This hash value is computed using a cryptographic hashing algorithm MD5 and is representative of the entire data content. Even a slight alteration in the input data results in a completely different hash value.

In the context of digital forensics, when creating a forensic image of a device's storage (such as a hard drive or a laptop's disk), it's essential to verify the integrity of the image file. This is where hash calculation of the combined image becomes significant. By calculating the hash value of the combined image - which comprises the data from the original device and potentially any additional data or metadata introduced during the forensic imaging process - the team can ensure that the image file remains unchanged and uncorrupted.

```
(root@kali) - [/media/sf_Mobile_Forensic_Project_Image]
# md5sum SCHARDT.img
aee4fcd9301c03b3b054623ca261959a SCHARDT.img

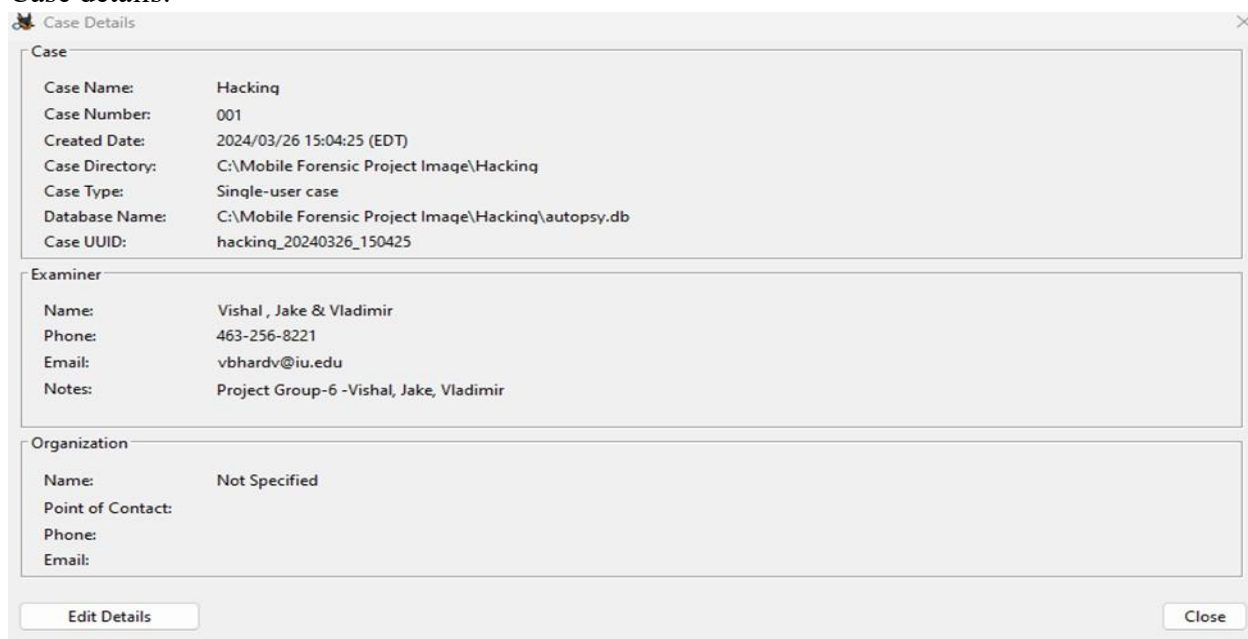
(root@kali) - [/media/sf_Mobile_Forensic_Project_Image]
#
```

Figure 3: Calculation of hash value of created image

On the windows system, Autopsy 4.21.0 was used to investigate and analyze the hard drive image. A new case was created on Autopsy using the case name “Hacking” and case number “001” was provided and the details of the examiner like name, phone number, and email were included.

Figure 4 below shows the case details in Autopsy. After the case was created, the hard drive image was added as a data source, and all ingest modules were run on the hard drive image to discover relevant findings. Figure 4 shows the evidence image being added as data source in Autopsy.

Case details: -



The screenshot shows the 'Case Details' window in Autopsy. It is divided into three main sections: Case, Examiner, and Organization. The Case section contains fields for Case Name, Case Number, Created Date, Case Directory, Case Type, Database Name, and Case UUID. The Examiner section contains fields for Name, Phone, Email, and Notes. The Organization section contains fields for Name, Point of Contact, Phone, and Email. At the bottom, there are 'Edit Details' and 'Close' buttons.

Case	
Case Name:	Hacking
Case Number:	001
Created Date:	2024/03/26 15:04:25 (EDT)
Case Directory:	C:\Mobile Forensic Project Image\Hacking
Case Type:	Single-user case
Database Name:	C:\Mobile Forensic Project Image\Hacking\autopsy.db
Case UUID:	hacking_20240326_150425

Examiner	
Name:	Vishal , Jake & Vladimir
Phone:	463-256-8221
Email:	vbhardv@iu.edu
Notes:	Project Group-6 -Vishal, Jake, Vladimir

Organization	
Name:	Not Specified
Point of Contact:	
Phone:	
Email:	

Buttons: Edit Details, Close

Figure 4: Case Details

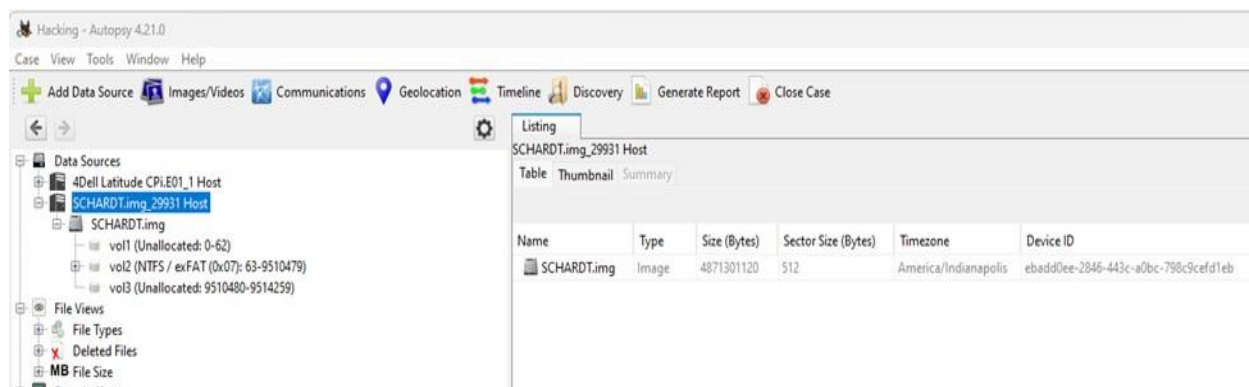


Figure 5- combined drive image added to Autopsy

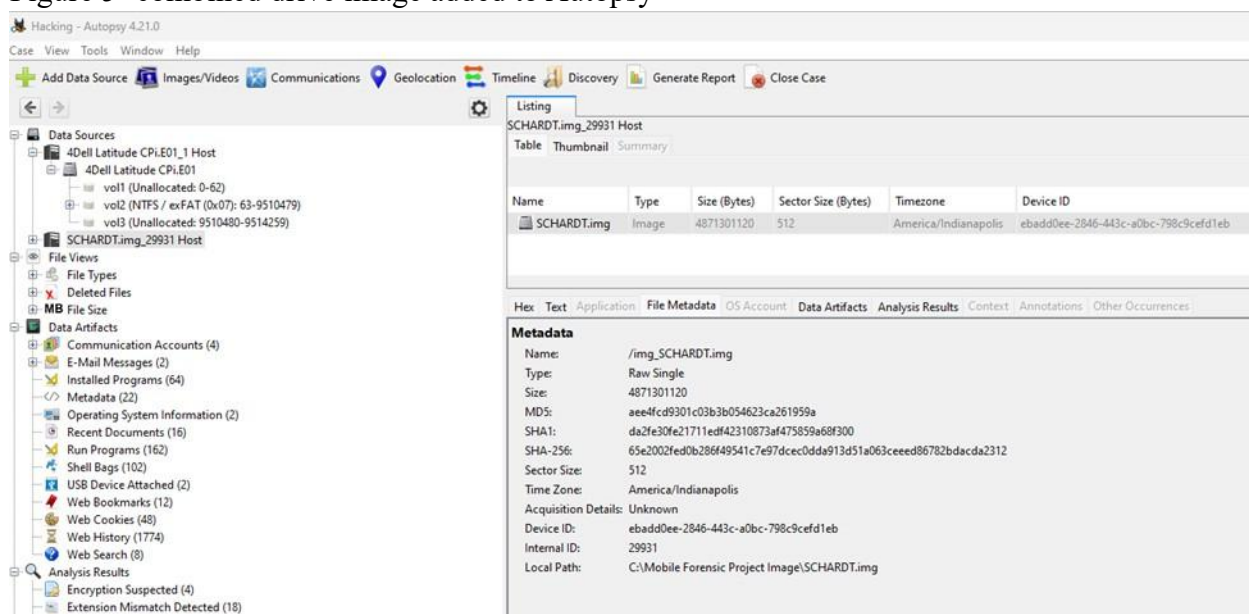


Figure 6. Hash values of combined image in Autopsy

It is same as calculated from Kali Linux command md5sum. Above Figure 5 shows the three different verification hash values which are MD5, SHA1 and SHA256, these hash values can be used to compare with acquisition hash value and image drive can be checked for integrity.

Figure 7 shows operating system information. Operating system information holds immense significance in digital forensics, providing essential context and guidance for forensic investigations. Understanding the specific operating system installed on a device, as depicted in Figure 7, is crucial for various aspects of forensic analysis. Firstly, it aids in the identification of

the system's architecture, file structures, and default configurations, which differ significantly between operating systems such as Windows, macOS, or Linux. This knowledge guides the selection of appropriate forensic tools and techniques tailored to the OS environment.

Additionally, operating system details inform the team about the generation of unique artifacts during normal operation, including system logs, registry entries (in the case of Windows), and configuration files. These artifacts often contain valuable evidence, such as timestamps, user activities, and system events, which are instrumental in reconstructing the sequence of events and extracting relevant information for the investigation.

Moreover, understanding the operating system's security posture is essential, as vulnerabilities and security features significantly impact forensic analysis. By comprehending the operating system's vulnerabilities and security features, the team can assess the reliability and completeness of their findings accurately. Overall, operating system information serves as a foundational element in digital forensics, enabling forensic analysts to effectively identify, analyze, and interpret evidence, contributing to the discovery of relevant facts and findings in forensic investigations.

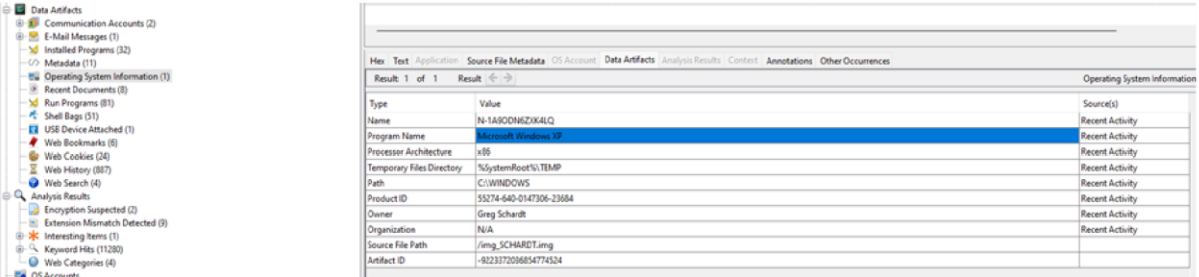


Figure 7. operating system information

Figure 8 shows OS account information. Figure 8, depicting operating system (OS) account information, holds paramount significance in digital forensics investigations as it provides crucial insights into user identities, access privileges, and potential security breaches. By

detailing user accounts configured on the system, including usernames, account types, and associated metadata. The team can understand user activities, trace digital interactions, and identify potential unauthorized access. Additionally, abnormal or unauthorized user accounts revealed in Figure 8 may indicate security threats or malicious activities, prompting further investigation. Ultimately, this information aids in establishing user accountability, attributing actions to specific individuals, and unraveling the circumstances surrounding digital incidents or crimes.

Name	S	C	O	Login Name	Host	Scope	Realm Name	Creation Time
S-1-5-21-2000478354-688789844-1708537768-1003			2	Mr. Evil	SCHARDT...	Local		2004-08-19 18:03:54 EST
S-1-5-19				LOCAL SERVICE	SCHARDT...	Local	NT AUTHORITY	
S-1-5-20				NETWORK SERVICE	SCHARDT...	Local	NT AUTHORITY	
S-1-5-18				SYSTEM	SCHARDT...	Local	NT AUTHORITY	
S-1-5-21-2000478354-688789844-1708537768-500			2	Administrator	SCHARDT...	Local		2004-08-19 11:59:34 EST
S-1-5-21-2000478354-688789844-1708537768-1002			2	SUPPORT_388945a0	SCHARDT...	Local		2004-08-19 17:35:19 EST
S-1-5-21-2000478354-688789844-1708537768-501			2	Guest	SCHARDT...	Local		2004-08-19 11:59:24 EST
S-1-5-21-2000478354-688789844-1708537768-1000			2	HelpAssistant	SCHARDT...	Local		2004-08-19 17:28:24 EST

Figure 8. OS Account Information

Installation date information is available through figure 9. Figure 9 shows The Windows installation date timestamp "1092955707" represents the number of seconds since the Unix epoch, which is January 1, 1970, at 00:00:00 UTC. This represents August 19, 2004, at 20:48:27 UTC.

The screenshot displays a digital forensics interface. On the left, a file tree shows the directory structure of a system. The main pane shows a table of files and folders. The right pane provides a detailed view of the 'software' directory, showing the 'CurrentVersion' registry path and its values.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
oemaut.sav				2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	262144	Allocated
SAM			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
SAMLOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
SecEvent.Evt			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	65536	Allocated
SECURITY			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	262144	Allocated
SECURITYLOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
software			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	8650752	Allocated
software.LOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
software.sav			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	630784	Allocated
SysEvent.Evt			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	65536	Allocated
system			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2621440	Allocated
system.LOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
system.sav			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	389120	Allocated
TempKey.LOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
userdiff			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	262144	Allocated
userdiff.LOG			2	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	2004-08-27 10:46:33 EST	1024	Allocated
userdiff.LOG				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated

Name	Type	Value
CurrentBuild	REG_SZ	1.511.1.0 (Obsolete data - do not use)
InstallDate	REG_DWORD	0x41252e3b (1092955707)
ProductName	REG_SZ	Microsoft Windows XP
RegDone	REG_SZ	(value not set)
RegisteredOrganization	REG_SZ	N/A
RegisteredOwner	REG_SZ	Greg Schardt
SoftwareType	REG_SZ	SYSTEM
CurrentVersion	REG_SZ	5.1
CurrentBuildNumber	REG_SZ	2600
BuildLab	REG_SZ	2600.xpclient.010817-1148
CurrentType	REG_SZ	Uniprocessor Free
SystemRoot	REG_SZ	C:\WINDOWS
SourcePath	REG_SZ	D:\
PathName	REG_SZ	C:\WINDOWS

Figure 9. Install date information. Figure 9, showcasing install date information, holds significant importance in digital forensics investigations due to its ability to provide key insights into the history and timeline of system events. The install date information allows the team to identify the dates when significant software or system changes occurred, such as the installation of new programs, updates, or modifications. This data is invaluable for reconstructing the sequence of events leading up to a digital incident or crime, as it can indicate when certain software or system configurations were introduced or altered. By correlating install date information with other forensic artifacts, analysts can establish timelines, identify potential points of compromise, and gain a deeper understanding of the circumstances surrounding the incident.

The registered owner of the laptop in question is Greg Schardt. This is evident from figure 10.

Figure 10, presenting owner information, holds considerable significance as it provides crucial

insights into the ownership and accountability of the digital device under scrutiny. This information typically includes details such as the registered owner's name, organization, contact information, and potentially other identifying attributes. By analyzing owner information, the team can establish ownership chains, identify potential suspects or persons of interest, and attribute specific actions or events to individuals. Additionally, owner information serves as a valuable starting point for conducting background checks, interviews, and further investigative inquiries to gather additional evidence or corroborate findings. Furthermore, in cases involving stolen or compromised devices, owner information can facilitate the recovery and return of the device to its rightful owner.

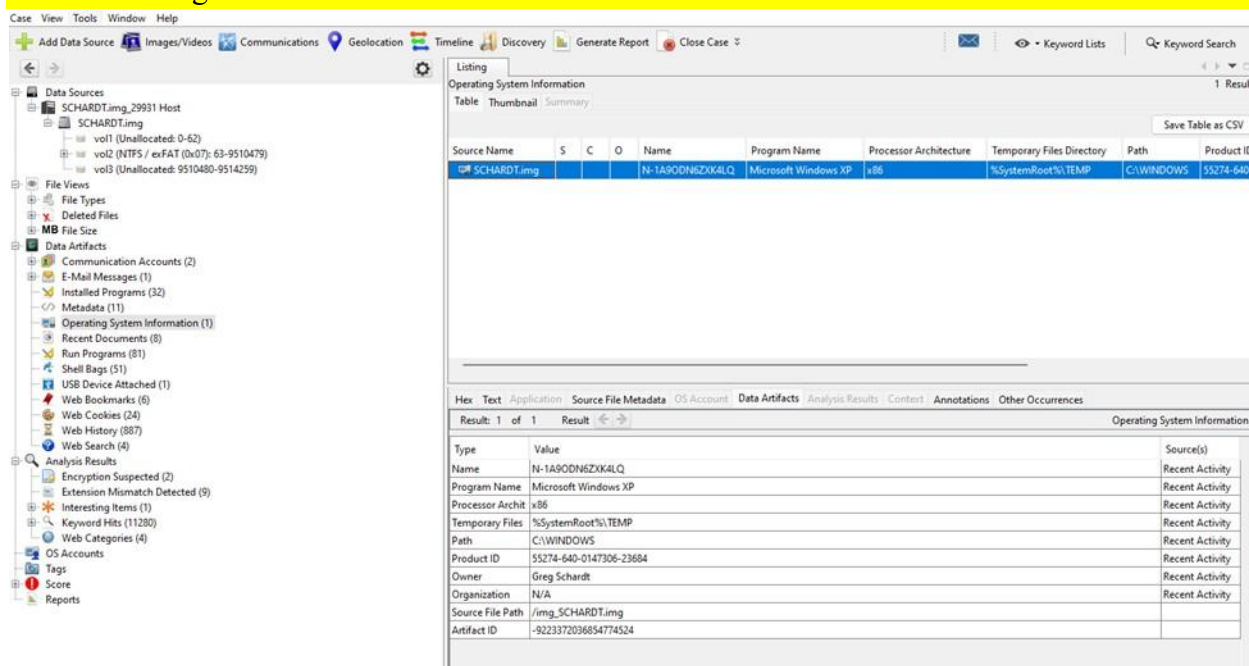


Figure 10. Owner information

Figure 11 shows installed application. Figure 11, displaying installed application information, holds significant importance due to its ability to provide insights into the software environment and user activities on the digital device under examination. By analyzing installed application data, the team can gain valuable insights into the purpose, functionality, and potential usage of the software installed on the system. This can help in understanding user behavior, identifying

potential security risks or vulnerabilities associated with specific applications, and reconstructing digital activities or events. The team found there are few hacking tools that the hacker might have used to gain information of connected users to the nearby network devices.

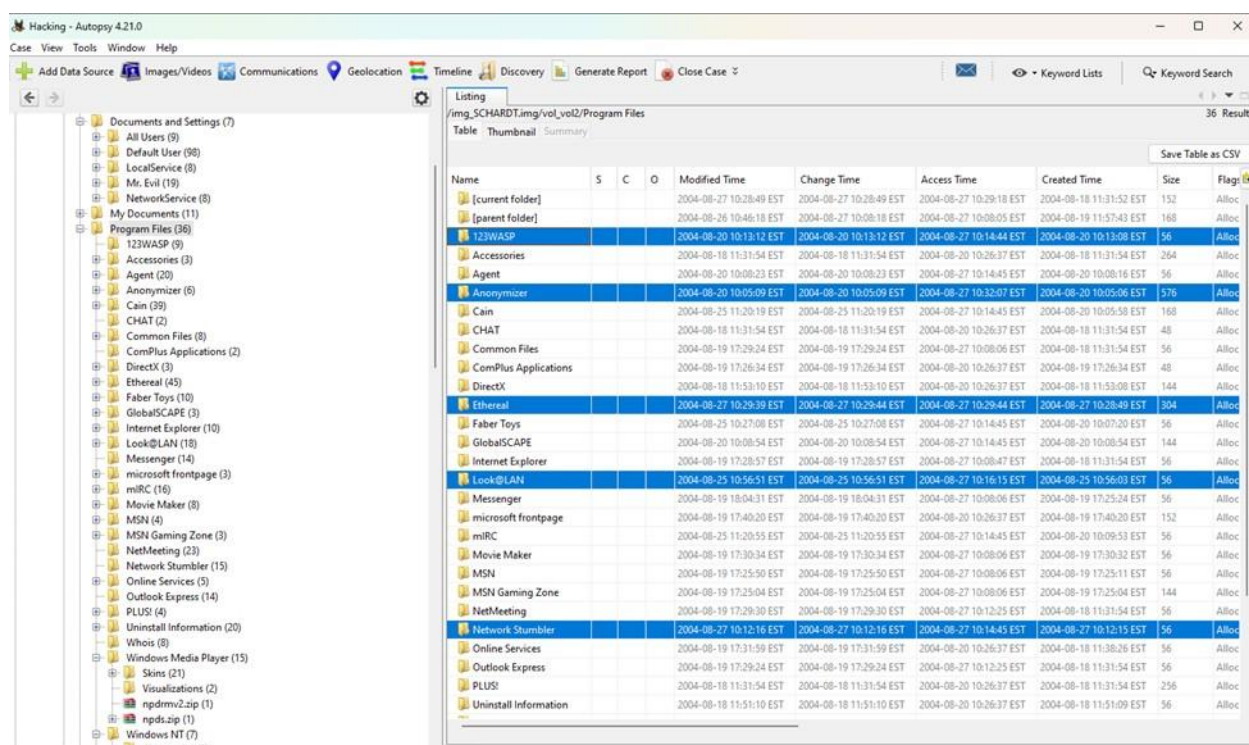


Figure 11: Installed application

Network Stumbler, also known as NetStumbler, is a Windows utility used for discovering and analyzing wireless networks [40]. It allows users to detect nearby wireless access points (APs) and identify their properties, such as signal strength, channel, encryption type, and network name (SSID). NetStumbler operates by passively scanning the airwaves for beacon frames broadcasted by wireless APs.

Look@LAN is a network monitoring tool designed to provide network administrators with detailed insights into their local area network (LAN)[41]. It allows users to scan their LAN for connected devices, identify IP addresses, MAC addresses, and other network information.

Look@LAN can detect active hosts, open ports, and network services running on devices within

the LAN. Additionally, it provides tools for network diagnostics, including ping and traceroute utilities. Overall, Look@LAN helps network administrators manage and troubleshoot their LAN infrastructure effectively.

An anonymizer is a tool or service that aims to enhance user privacy and security by masking their online activities and identity [42]. Anonymizers achieve this by redirecting internet traffic through proxy servers or virtual private networks (VPNs), thereby obscuring the user's IP address and encrypting their internet traffic. This helps users browse the web anonymously, preventing websites, internet service providers (ISPs), and other third parties from tracking their online behavior or identifying their location. Anonymizers are commonly used by individuals seeking to protect their privacy, bypass internet censorship, or access geo-restricted content.

Ethereal, now known as Wireshark, is a widely used network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network [44]. It supports a wide range of protocols and provides detailed information about each packet captured, including its source and destination, protocol type, and payload data. Wireshark is often used for network troubleshooting, protocol development, network security analysis, and education.

Figure 12 shows shutdown time.

The screenshot displays a forensic analysis interface. The top section shows a file list with columns for Name, S, C, O, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). The file 'system' is highlighted. Below the file list, the 'Analysis Results' tab is active, showing a tree view of system components. The 'ShutdownTime' registry value is selected, and its details are shown in the right pane.

Name	Type	Value
Directory	REG_EXPAND_SZ	%SystemRoot%
ErrorMode	REG_DWORD	0x00000000 (0)
NoInteractiveServices	REG_DWORD	0x00000000 (0)
SystemDirectory	REG_EXPAND_SZ	%SystemRoot%\system32
ShellErrorMode	REG_DWORD	0x00000001 (1)
ShutdownTime	REG_BIN	C4 FC 00 07 4D 8C C4 01

Figure 12: Shutdown time.

ShutdownTime is C4 FC 00 07 4D 8C C4 01, which is 2004-08-27 15:46:33.1092164 Z UTC

Used the tool DCode (figure 13) to convert hexadecimal time to human readable format.

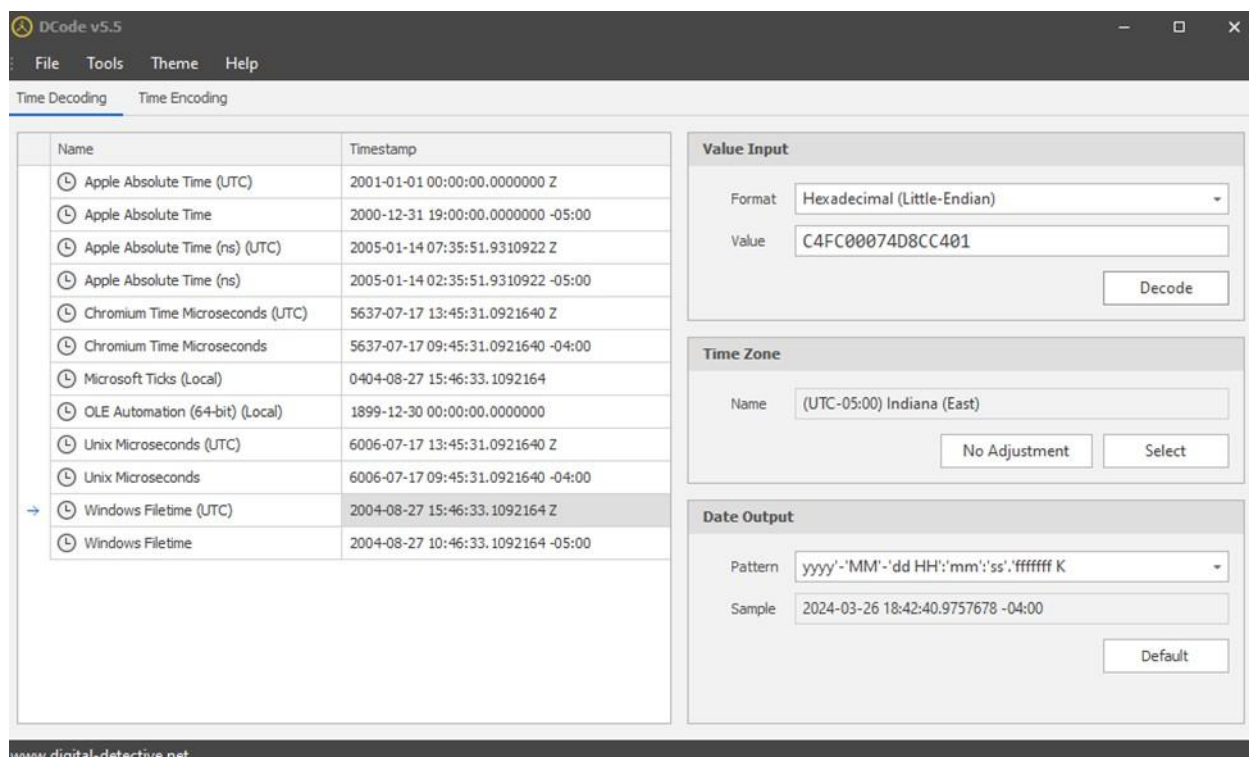


Figure 13: Shut down time converter.

The significance of the information provided in Figure 14, particularly the identification of the frequently logged-on user as "Mr. Evil" with 15 logins, cannot be understated in digital forensics investigations. This revelation serves as a critical lead in understanding user behavior and potential involvement in suspicious or malicious activities. By identifying a specific user associated with a significant number of logins, the team can focus their investigation on this individual, probing deeper into their activities, access privileges, and potential motives. Additionally, the designation of the username as "Mr. Evil" may suggest deliberate attempts to conceal one's identity or engage in illicit activities, warranting further scrutiny. Furthermore, this information enables the team to attribute specific actions or events to the identified user, aiding in the reconstruction of timelines and the establishment of culpability. Overall, the revelation provided in Figure 14 serves as a pivotal piece of evidence in digital forensics investigations,

guiding the team towards potential leads and contributing to the resolution of digital crimes and incidents.

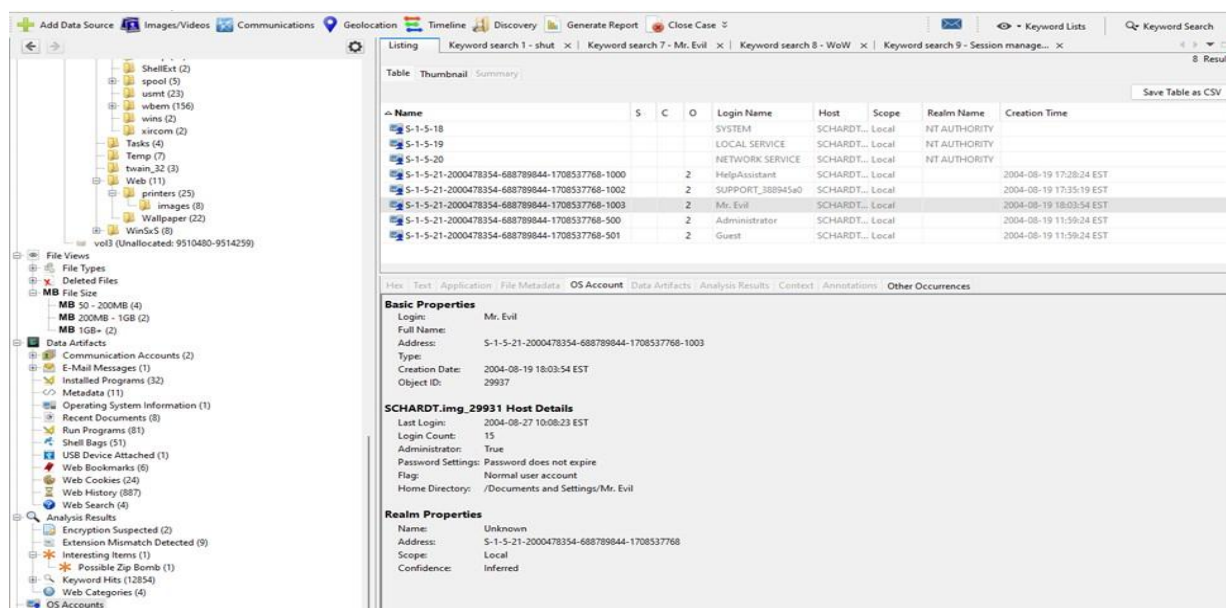


Figure 14: User logon information

As shown in figure 15 and 16, a search for the name of “Greg Schardt” reveals multiple hits. One of these proves that Greg Schardt is Mr. Evil and is also the administrator of this computer. What file is it? What software program does this file relate to? `irunin.ini`, `Look@LAN`: program to monitor user over lan.

[Look@LAN\irunin.ini](#) contains interesting info. According to it it has been found that several entries with name Mr.Evil, LANUSER: Mr.evil and RegOwner: Greg Schardt. Thus, both are the same users. `ISUSERNTADMIN` is set to true which means the user is administrator.

Listing Keyword search 13 - Greg Schardt x				
Keyword search				
Table Thumbnail Summary				
Save Table as CSV				
Name	Keyword Preview	Location	Modified Time	Ch
Operating System Information Artifact	306-23684Owner : «Greg Schardt«Organization : N/A	SCHARDT.img		
software	0oRegisteredOwner«Greg Schardt«26008XxCumSoft	/img_SCHARDT.img/vol_vol2/WINDOWS/repair/softw...	2004-08-19 17:49:11 EST	200
software	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.img/vol_vol2/WINDOWS/system32/c...	2004-08-27 10:46:33 EST	200
Unalloc_49981_351232_1683209728	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.img/vol_vol2/\$Unalloc/Unalloc_49981...	0000-00-00 00:00:00	000
Unalloc_49981_1684736000_3639811072	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.img/vol_vol2/\$Unalloc/Unalloc_49981...	0000-00-00 00:00:00	000
AppEvent.Evt	Registered Owner: «Greg Schardt«-----> Task List <-----	/img_SCHARDT.img/vol_vol2/WINDOWS/system32/c...	2004-08-27 10:46:29 EST	200
irunin.ini	HT%=:600%REGOWNER%=:«Greg Schardt«%REGORGA...	/img_SCHARDT.img/vol_vol2/Program Files/Look@L...	2004-08-25 10:56:10 EST	200
drwtsn32.log	Registered Owner: «Greg Schardt«-----> Task List <-----	/img_SCHARDT.img/vol_vol2/Documents and Setting...	2004-08-20 10:25:48 EST	200
Look@LAN Setup Log.txt	REG_SZValue data = «Greg Schardt«(On Error) User n	/img_SCHARDT.img/vol_vol2/WINDOWS/Look@LAN ...	2004-08-25 10:56:33 EST	200
f0256874.txt	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.img/vol_vol2/\$CarvedFiles/1/f025687...	0000-00-00 00:00:00	000

Figure 15: registered owner

Hacking - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing Keyword search 13 - Greg Schardt x

Keyword search

Table Thumbnail Summary

Save Table as CSV

Name	Keyword Preview	Location	Modified Time	Ch
Operating System Information Artifact	306-23684Owner : «Greg Schardt«Organization : N/A	SCHARDT.img		
software	0oRegisteredOwner«Greg Schardt«26008XxCumSoft	/img_SCHARDT.img/vol_vol2/WINDOWS/repair/softw...	2004-08-19 17:49:11 EST	200
software	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.img/vol_vol2/WINDOWS/system32/c...	2004-08-27 10:46:33 EST	200
Unalloc_49981_351232_1683209728	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.img/vol_vol2/\$Unalloc/Unalloc_49981...	0000-00-00 00:00:00	000
Unalloc_49981_1684736000_3639811072	Companyil SoName«Greg Schardt«C:\WINDOWS\Syst...	/img_SCHARDT.img/vol_vol2/\$Unalloc/Unalloc_49981...	0000-00-00 00:00:00	000
AppEvent.Evt	Registered Owner: «Greg Schardt«-----> Task List <-----	/img_SCHARDT.img/vol_vol2/WINDOWS/system32/c...	2004-08-27 10:46:29 EST	200
irunin.ini	HT%=:600%REGOWNER%=:«Greg Schardt«%REGORGA...	/img_SCHARDT.img/vol_vol2/Program Files/Look@L...	2004-08-25 10:56:10 EST	200
drwtsn32.log	Registered Owner: «Greg Schardt«-----> Task List <-----	/img_SCHARDT.img/vol_vol2/Documents and Setting...	2004-08-20 10:25:48 EST	200
Look@LAN Setup Log.txt	REG_SZValue data = «Greg Schardt«(On Error) User n	/img_SCHARDT.img/vol_vol2/WINDOWS/Look@LAN ...	2004-08-25 10:56:33 EST	200
f0256874.txt	REG_SZValue data = «Greg Schardt«(On Error) User no	/img_SCHARDT.img/vol_vol2/\$CarvedFiles/1/f025687...	0000-00-00 00:00:00	000

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

Strings Extracted Text Translation

Page: 1 of 1 Page Matches on page: 1 of 2 Match 100% Reset Text Source: Search Results

(Variables)

%LANHOST%=:N-1A90DN6ZXK4LQ

%LANDOMAN%=:N-1A90DN6ZXK4LQ

%LANUSER%=:My Evil

%LANIP%=:192.168.1.111

%LANNIC%=:0010a493e09

%SWIN95%=:FALSE

%SWIN98%=:FALSE

%SWINNT%=:FALSE

%SWINNT4%=:FALSE

%SWIN2000%=:FALSE

%SWINME%=:FALSE

%SWINXP%=:TRUE

%USERNTADMIN%=:TRUE

%TEMPLAUNCHDIR%=:C:\DOCUMENT-1\MRD51E-1\EV\LOCALS-1\Temp

%WINDIR%=:C:\WINDOWS

%SYSTEMDRIVE%=:C:

%SYSTEMDRIVE%=:C:\WINDOWS\System32

%TEMPDIR%=:C:\DOCUMENT-1\MRD51E-1\EV\LOCALS-1\Temp

%SCREENWIDTH%=:800

%SCREENHEIGHT%=:600

%REGOWNER%=:Greg Schardt

%REGORGANIZATION%=:N/A

%DATE%=:08/25/04

%CURRENTMONTH%=:8

%CURRENTDAY%=:25

%CURRENTYEAR%=:2004

%CURRENTHOUR%=:10

Figure 16: User Information Delving into the Windows Registry, specifically navigating to the path

"C:\windows\system32\config\software\Microsoft\Windows NT\CurrentVersion\NetworkCards",

the team unearthed pivotal insights regarding the network configuration of the machine under scrutiny. Our examination uncovered the presence of a Compaq WL110 Wireless LAN PC Card, a crucial discovery shedding light on the network infrastructure utilized by the system. This revelation holds significant importance in our investigation as it provides concrete evidence of the specific network interface hardware employed by the machine. The identification of the Compaq WL110 Wireless LAN PC Card not only corroborates the presence of wireless networking capabilities but also signifies potential avenues for unauthorized access, data interception, or malicious activities.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location	MD5Hash
default.sav	1			2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	90112	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	636227c...
SAM	1			2004-08-27 21:16:33 IST	2004-08-20 04:05:21 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	e38943c...
SAM.LOG	1			2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	822c1f4...
SecEvent.Evt	1			2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	440705c...
SECURITY	1			2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	eed043c...
SECURITY.LOG	1			2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	506ceea...
software	1			2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	85af90c...
software.LOG	1			2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	41ae974...
software.sav	1			2004-08-19 22:26:29 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	630784	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	724000c...
SystemEvent.Evt	1			2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	06e154c...
system	1			2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	7671440	Allocated	Allocated	unknown	(img_4Cell Latitude CP.E01\vol_vol2\WINDOWS\system32...	5af17d4...

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
		File Manager	Metadata				
		Font Drivers	Name: 11				
		FontDP1	Number of subkeys: 0				
		FontMapper	Number of values: 2				
		Fonts	Values				
		FontSubstitutes	Name	Type	Value		
		GRE_Initialize	ServiceName	REG_SZ	(86FC0C96-3FF2-4D59-9ABA-C602F2138D02)		
		HotFix	Description	REG_SZ	Compaq WL110 Wireless LAN PC Card		
		ICM					
		Image File Execution Options					
		IME Compatibility					
		IMM					

And a Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met)
default.sav			1	2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	90112	Allocated	Allocated
SAM			1	2004-08-27 21:16:33 IST	2004-08-20 04:05:21 IST	2004-08-27 21:16:33 IST	2004-08-19 22:20:55 IST	262144	Allocated	Allocated
SAM.LOG			1	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-27 20:38:23 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
SecEvent.Evt			1	2004-08-19 22:29:15 IST	2004-08-19 22:32:15 IST	2004-08-19 22:29:15 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated
SECURITY			1	2004-08-27 21:16:33 IST	2004-08-20 04:34:03 IST	2004-08-27 21:16:33 IST	2004-08-19 22:28:55 IST	262144	Allocated	Allocated
SECURITY.LOG			1	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-27 21:02:56 IST	2004-08-19 22:28:55 IST	1024	Allocated	Allocated
software			1	2004-08-27 21:16:33 IST	2004-08-27 20:59:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:08 IST	8650752	Allocated	Allocated
software.LOG			1	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-27 21:16:32 IST	2004-08-19 22:26:08 IST	1024	Allocated	Allocated
software.sav			1	2004-08-19 22:26:20 IST	2004-08-19 22:32:15 IST	2004-08-19 05:30:00 IST	2004-08-19 22:26:18 IST	630784	Allocated	Allocated
System.Evt			1	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-27 21:16:29 IST	2004-08-19 22:29:15 IST	65536	Allocated	Allocated
system			1	2004-08-27 21:16:33 IST	2004-08-27 21:01:44 IST	2004-08-27 21:16:33 IST	2004-08-19 22:26:06 IST	2621440	Allocated	Allocated

Hex	Text	Application	File Metadata	Context	Results	Annotations	Other Occurrences
		File Manager					Metadata
		Font Drivers					Name: Description
		FontDPI					Type: REG_SZ
		FontMapper					Value
		Fonts					Xircom CardBus Ethernet 100 + Modem 56 (Ethernet Interface)
		FontSubstitutes					
		GRE_initialize					
		HotFix					
		ICM					
		Image File Execution Options					
		IME Compatibility					
		IMM					
		InFileMapping					
		LanguagePack					
		LastFontSweep					
		MCI					
		MCI Extensions					
		MCI32					
		Midmap					
		ModuleCompatibility					
		Network					
		NetworkCards					
		11					
		2					
		ServiceName					
		Description					

The discovery provides concrete evidence of the specific network interface card (NIC) utilized by Mr. Schardt's machine, indicating its capability to connect to wireless networks. Which is important since our investigation is looking into accusations of Mr. Schardt committing malicious wireless activity.

Additionally, if we were to go back and look at the irunin.ini file you can see the IP and MAC address of the computer.

```

Page: 1 of 1 Page  Matches on page: 1
[Variables]
%LANHOST% = N-1A90DN6ZK4LQ
%LANDOMAIN% = N-1A90DN6ZK4LQ
%LANUSER% = Mr. Evil
%LANIP% = 192.168.1.111
%LANNIC% = 0010a4933e09
%SWIN95% = FALSE
%SWIN98% = FALSE
%SWINNT3% = FALSE
%SWINNT4% = FALSE
%SWIN2000% = FALSE
%SWINME% = FALSE
%SWINXP% = TRUE

```

The IP of the device Mr. Evil uses is: 192.168.1.111 and the MAC address is: 0010a4933e09.

In the team's digital forensic investigation, knowing the IP and MAC addresses associated with Mr. Schardt's device is crucial for tracking their network activity. Additionally, this information will also serve as key evidence in legal proceedings brought against Mr. Schardt.

With this new knowledge we can gather more information. For example, the first 3 hex characters of the MAC address report the vendor of the card, which we can search for online. Knowing the vendor information can provide insights into the type of device being used and its capabilities.

MAC Address Lookup

Enter any MAC address, OUI, or IAB below to lookup the manufacturer, location, and more

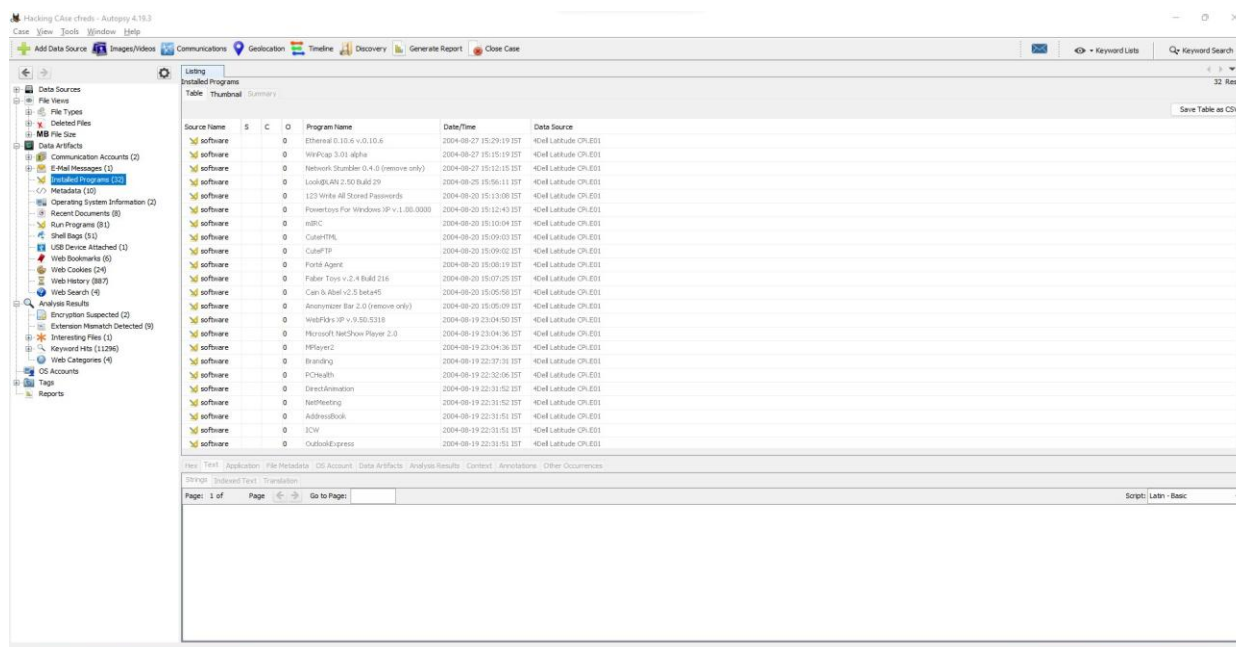
Where can I find my MAC Address?

MAC Address Details

Company	XIRCOM
Address	2300 CORPORATE CENTER DR. THOUSAND OAKS CA 91320 US
Range	00:10:A4:00:00:00 - 00:10:A4:FF:FF:FF
Type	IEEE MA-L

We can identify that it was manufactured by XIRCOM. XIRCOM is now a subsidiary of Intel, known for producing networking and connectivity products

Next, we found 6 installed programs that may be used for hacking. Installed programs in left-tree pane should list what was installed. Then, the programs are search on google and check which can be used for malicious activity.



By doing a quick Google search, we can conclude that these six programs are typically used for malicious activity. Additionally, we can get an idea as to what they can do.

Name	Function
123WASP	Freeware to get all passwords
Anonymizer	Tool to create a proxy
Cain & Abel v2.5 beta45	password recovery tool for Microsoft Windows
Ethereal	Packet sniffing tool
Look@LAN	Network monitoring tool

NetStumbler	wireless networking tool to hack wifi password
-------------	--

The discovery of installed tools such as "123WASP," "Anonymizer," "Cain & Abel v2.5 beta45," "Ethereal," "Look@LAN," and "NetStumbler" on the device we are investigating is crucial for our team as we are trying to connect Mr. Schardt with malicious activity. The discovery of these tools signifies a deliberate attempt to engage in unauthorized activities, including password retrieval, network monitoring, and potential exploitation of vulnerabilities. The presence of password recovery tools and network sniffers raises concerns regarding potential data breaches and unauthorized access to sensitive information. Additionally, the inclusion of tools like "NetStumbler" suggests an interest in exploiting wireless networks, which is the core of what we are investigating. Overall, these findings provide valuable insights into the suspect's tactics, capabilities, and potential criminal activities, and can help guide our investigative team towards uncovering the full extent of Mr. Schardt's activities [40].

Since the team discovered that Ethereal, which is a packet sniffing program capable of intercepting both wired and wireless internet packets, was identified among the installed software. We investigated where the TCP packets are captured and reconstructed. The team discovered that the captured packets are automatically saved to the user's \My Documents directory by default.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:10:31 IST	2004-08-27 21:05:53 IST	352	Allocated	Allocated	unknown	/img_4Dell Latitude
[parent folder]				2004-08-27 21:05:53 IST	2004-08-27 21:06:53 IST	2004-08-27 21:12:40 IST	2004-08-20 04:34:05 IST	56	Allocated	Allocated	unknown	/img_4Dell Latitude
preferences			3	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	2004-08-27 21:05:53 IST	40690	Allocated	Allocated	unknown	/img_4Dell Latitude
recent			3	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	2004-08-27 21:15:25 IST	1759	Allocated	Allocated	unknown	/img_4Dell Latitude


```

# Recent settings file for Ethereal 0.10.6.
#
# This file is regenerated each time Ethereal is quit.
# So be careful, if you want to make manual changes here.

##### Recent capture files (latest last) #####
Recent_capture_file: C:\Documents and Settings\Mr. Evil\interception

```

Upon reviewing the recent files, it was observed that the location where captured or intercepted data is stored is "eC:\Documents and Settings\Mr. Evil\interception." Additionally, the file responsible for storing intercepted data is named "interception". Since we know that Mr. Evil is an alias of Mr. Schardt, the information provides clear evidence of him capturing wireless information.

Viewing the file in a text format reveals that the victim he intercepted was using a Windows CE Pocket PC. The user was accessing mobile.msn.com during the time of the interception.

After viewing the intercepted file and its contents, the following move is to find the main user's web-based email address. It started by searching through the web history tab in the left side tree pane. However, there are 887 entries starting from the year 1989. Thus, the searches were reduced to the scope of the case i.e 2004. The timeline was filtered using the preset "Limit event types to -> web activity" and choosing detail view mode. This will show which URLs were visited. The web email is "mrevilruez@yahoo.com."

Yahoo mail, a popular web-based email service, saves copies of the email under

“ShowLetter[1].htm.” We go to “Keyword hits -> Email address -> req expression” and search for the email we found. There are copies inside one of the showletter.htm files.

To find Mr. Evil's SMTP email address, one does a keyword search for SMTP and looks for it in NTUSER.DAT file. The path to said file is "C:\Documents and Settings\Mr.

Evil\NTUSER.DAT.”

[illegible]

The SMTP information can help us discover Mr. Schardt's email address and shed light on his communication activities.

Next is to search for the NNTP (news server) settings for Mr. Evil. The Network News Transfer Protocol (NNTP) is the underlying protocol of UseNet, which is a worldwide discussion system which contains posts or articles which are known as news [44]. To find the address, we perform a keyword search for NNTP and look for it in NTUSER.DAT file.” The credentials are stated below:

Server name	Server username	Server password
news.dallas.sbcglobal.net	whoknowsme@sbcglobal.net	News.dallas.sbcglobal.netF6E2BA30

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
at.2600.cards.dbx			0	2004-09-21 02:57:17 ZST	2004-09-21 02:57:17 ZST	2004-09-21 02:57:17 ZST	2004-09-21 02:48:41 ZST	20752	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:48:41 ZST	14036	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:48:41 ZST	469716	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:48:41 ZST	600709	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:55:57 ZST	469716	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:49:20 ZST	2004-09-21 02:49:20 ZST	2004-09-21 02:49:20 ZST	2004-09-21 02:49:15 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:10 ZST	2004-09-21 02:57:10 ZST	2004-09-21 02:57:10 ZST	2004-09-21 02:55:25 ZST	277008	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:57:16 ZST	2004-09-21 02:54:25 ZST	20752	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:53:41 ZST	2004-09-21 02:53:41 ZST	2004-09-21 02:53:41 ZST	2004-09-21 02:52:54 ZST	600709	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:55 ZST	2004-09-21 02:50:55 ZST	2004-09-21 02:50:55 ZST	2004-09-21 02:50:36 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:49:24 ZST	2004-09-21 02:49:24 ZST	2004-09-21 02:49:24 ZST	2004-09-21 02:49:22 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:50 ZST	2004-09-21 02:50:50 ZST	2004-09-21 02:50:50 ZST	2004-09-21 02:50:46 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:52:54 ZST	2004-09-21 02:52:54 ZST	2004-09-21 02:52:54 ZST	2004-09-21 02:50:55 ZST	600709	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:57:07 ZST	2004-09-21 02:57:07 ZST	2004-09-21 02:57:07 ZST	2004-09-21 02:53:41 ZST	535252	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:54 ZST	2004-09-21 02:50:54 ZST	2004-09-21 02:50:54 ZST	2004-09-21 02:49:52 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:49:27 ZST	2004-09-21 02:49:27 ZST	2004-09-21 02:49:27 ZST	2004-09-21 02:49:25 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:43:58 ZST	2004-09-21 02:43:58 ZST	2004-09-21 02:43:58 ZST	2004-09-21 02:43:55 ZST	962	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:40:30 ZST	2004-09-21 02:40:30 ZST	2004-09-21 02:40:30 ZST	2004-09-21 02:40:30 ZST	143036	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:59 ZST	2004-09-21 02:50:59 ZST	2004-09-21 02:50:59 ZST	2004-09-21 02:43:25 ZST	4072416	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:49:31 ZST	2004-09-21 02:49:31 ZST	2004-09-21 02:49:31 ZST	2004-09-21 02:49:29 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:14 ZST	2004-09-21 02:50:14 ZST	2004-09-21 02:50:14 ZST	2004-09-21 02:50:10 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:50:23 ZST	2004-09-21 02:50:23 ZST	2004-09-21 02:50:23 ZST	2004-09-21 02:50:14 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...
at.2600.cards.dbx			0	2004-09-21 02:49:38 ZST	2004-09-21 02:49:38 ZST	2004-09-21 02:49:38 ZST	2004-09-21 02:49:37 ZST	76000	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Documents and Settings\...

An IRC chat service called MIRC was found to be installed on his laptop. IRC is short for Internet Relay Chat, a chat system that allows people (even strangers) to message each other over the Internet in near real time [44]. IRCs have different channels based on the topic. There may be a channel (or channels) for hackers. He could be part of those channels. The discovery of MIRC was made while investigating the program files.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dr)	Flags(Meta)	Known	Location
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	287	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	49423	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	189776	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	224313	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	1949	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	288	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	2004-09-20 20:39:56 ZST	1194	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-21 00:46:33 ZST	2004-09-21 00:46:33 ZST	2004-09-21 00:46:33 ZST	2004-09-20 20:39:56 ZST	51930	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...
mirc.exe			0	2004-09-21 01:01:01 ZST	2004-09-21 01:01:01 ZST	2004-09-21 01:01:01 ZST	2004-09-20 20:39:56 ZST	968	Allocated	Allocated	unknown	Jing_KdellLatitude CH.E01\vol_v02\Program Files\mIRC\...

The user settings can be found in ini file inside mIRC directory located at “C:\Program Files\mIRC\mirc.ini. His user name is “Mini Me,” the email address is none@of.ya,

User	Email	nic	anic
Mini Me	none@of.ya		

Mini Me	none@of.ya	Mr	mrevilrulez
---------	------------	----	-------------

The IRC program can log chat sessions. So far, the chat logs of Chataholics.UnderNet,

Elite.Hackers.UnderNet, and thedarktower.AfterNET were stored on his computer. This could be valuable information as Mr. Evil may be exchanging information with members of the three chat groups.

Next part is to search if any executables are in the Recycle Bin. There are four executables found within the Recycle Bin: Dc1.exe, Dc2.exe, Dc3.exe, and Dc4.exe. The four executable files are not truly deleted. When Windows deletes files, they are just deallocated and removed from allocation table (i.e MFT table). but the data still exists in the location until it is overwritten. The files in the Recycle Bin are just transferred to the Recycler directory rather than being deallocated. File status can be seen in file metadata.

The screenshot shows the Autopsy 4.19.3 interface. The left pane displays the file system tree with 'Recycle Bin' expanded. The main pane shows a table of files in the Recycle Bin. The file 'Dc1.exe' is selected, and its metadata is displayed in the bottom pane.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location	MDS Hash	SHA-256 Hash
Current folder				2004-08-27 20:09:58 IST	2004-08-27 20:09:58 IST	2004-08-27 20:09:58 IST	2004-08-27 20:09:58 IST	96	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...		
Parent folder				2004-08-25 21:40:25 IST	2004-08-25 21:40:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:40:25 IST	328	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...		
Dc1.exe				2004-08-25 21:40:25 IST	2004-08-25 21:40:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:40:25 IST	216004	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	61a09f10b110a443a4a0b0847957	afdaa137513274
Dc2.exe				2004-08-27 20:41:07 IST	2004-08-27 20:42:30 IST	2004-08-27 20:41:07 IST	2004-08-27 20:41:07 IST	1324940	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	86a780a4e454472a73b7142873b0	f3ca47960b03
Dc3.exe				2004-08-27 20:41:07 IST	2004-08-27 20:41:07 IST	2004-08-27 20:41:07 IST	2004-08-27 20:41:07 IST	44217	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	5a053a3a4b99a3a3f0181b4a476	189a3077904
Dc4.exe				2004-08-27 20:59:47 IST	2004-08-27 20:59:47 IST	2004-08-27 20:59:47 IST	2004-08-27 20:59:47 IST	846562	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	007a5a2079542775a4b5a4f4b0	8678915a6a05
desktop.v				2004-08-25 21:40:25 IST	2004-08-25 21:40:25 IST	2004-08-27 20:42:30 IST	2004-08-25 21:40:25 IST	48	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	a80b0441a07a043032b6c12849b	2952da51a1a8
DPF02				2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-27 21:16:17 IST	2004-08-25 21:40:25 IST	3220	Allocated	Allocated	Unknown	./img_40x4 Latitude CP.E31144_und2RECYCLES-1-5-21...	f4b1a13006a150a0f6887703b1a2d	92b3a0d7300474

File Metadata for Dc1.exe:

```

Internal ID: 6300
From The Skouth Kikstat Took:
MFT Entry Header Values:
Entry: 11632 Sequence: 1
Logfile Sequence Number: 95072441
Allocated File
Size: 8
STANDARD_INFORMATION Attributes Values:
Flags: Archive
Owner ID: 0
Security ID: 105 (S-1-5-01-200478354-68769844-170833768-1003)
Created: 2004-08-25 21:41:07 (India Standard Time)
File Modified: 2004-08-25 21:41:07 (India Standard Time)
MFT Modified: 2004-08-25 21:40:25 (India Standard Time)
Accessed: 2004-08-25 21:40:25 (India Standard Time)
FILE_NAME Attribute Values:
Flags: Archive

```

Upon inspecting the File System directory of Deleted Files in left tree pane, the file system reports that there are 365 deleted files. Finally, an Anti-Virus check to verify if the laptop carries any viruses. Autopsy autoruns antivirus scans and any possible actors can be found inside "Interesting Files" category in left tree pane. The check reveals a file called "unix_hack.tgz,"

which is a zip bomb. A zip bomb is a malicious file that exploits a characteristic of the zip compressor to crash a system that processes it [47].

III. Interpretations

The forensic analysis of the evidence in the hacking case has revealed compelling insights into the activities and intentions of the suspect, Greg Schardt, operating under the alias "Mr. Evil." The presence of a Dell CPi notebook laptop, accompanied by a wireless PCMCIA card and a homemade 802.11b external antenna, indicates a deliberate effort to engage in illicit activities involving wireless network manipulation. The investigation, conducted with specialized forensic tools like Kali Linux and Autopsy, meticulously reconstructed the drive image and scrutinized digital artifacts to uncover pertinent details.

The findings shed light on Mr. Schardt's involvement in malicious activities, with installed programs and configuration files linking him to hacking tools such as NetStumbler, Look@LAN, Cain & Abel, Ethereal (Wireshark), and Anonymizer. This discovery underscores a deliberate attempt to exploit vulnerabilities in wireless networks for unauthorized access and data interception. Moreover, intercepted data stored in Mr. Schardt's My Documents directory, along with the presence of deleted executables and a zip bomb file, point to potential involvement in destructive activities aimed at system disruption.

The analysis not only establishes Mr. Schardt's identity but also provides valuable evidence for legal proceedings. The association between Greg Schardt and "Mr. Evil," as well as the discovery of hacking tools and intercepted data, forms a compelling case against him.

Furthermore, insights into Mr. Schardt's network activities, including email and news server settings, IRC chat logs, and deleted files, offer a comprehensive understanding of his criminal endeavors.

IV. Evidence Table

Sr. No.	Items	Description
1.	Dell CPi notebook computer	Make: Dell Model: CPi Serial#: VLQLW The suspected laptop was used for hacking purposes.
2.	Laptop Hard Drive	Model: "IBM-DBCA-204860" Serial#: "HQ0RQQF7429" Drive Size: 4.5 GB All the intercepted data is present in the hard drive and creating a DD image of the hard drive would help to investigate the data.
3.	Wireless card PCMCIA	The hacker might have used this device as an adapter to connect the homemade antenna.
4.	Homemade 802.11b antennae	The antenna is suspected to be used to increase the strength and range of the signals.
5.	DD Image	The DD image was created from the laptop hard drive and divided into 8 parts.
5.1.	SCHARDT.001	MD5 Hash value: 28A9B613 D6EEFE8A 0515EF0A 675BDEBD Sectors: 1301248

5.2.	SCHARDT.002	MD5 Hash value: C7227E7E EA82D218 66325739 7679A7C4 Sectors: 1301248
------	-------------	---

5.3.	SCHARDT.003	MD5 Hash value: EBBA35AC D7B8AA85 A5A7C13F 3DD733D2 Sectors: 1301248
5.4.	SCHARDT.004	MD5 Hash value: 669B6636 DCB4783F D5509C47 10856C59 Sectors: 1301248
5.5.	SCHARDT.005	MD5 Hash value: C46E5760 E3821522 EE81E675 422025BB Sectors: 1301248
5.6.	SCHARDT.006	MD5 Hash value: 99511901 DA2DEA77 2005B5D0 D764E750 Sectors: 1301248
5.7.	SCHARDT.007	MD5 Hash value: 99511901 DA2DEA77 2005B5D0 D764E750 Sectors: 1301248
5.8.	SCHARDT.008	MD5 Hash value: 8194A79A 5356DF79 883AE2DC 7415929F Sectors: 405524

Relevant Findings and Result

I. Observations:

Discovery of Suspected Hacking Equipment: The investigation revealed the discovery of a Dell CPi notebook laptop, a wireless PCMCIA card, and a homemade 802.11b antenna. These devices were suspected to be involved in hacking activities aimed at intercepting internet traffic for unauthorized access to sensitive information.

Evidence Collection and Processing: The investigative team meticulously collected and documented details of the seized devices, including make, model, serial numbers, and condition. The devices were dispatched to a Regional Computer Forensics Laboratory (RCFL) for processing and storage until a warrant for investigation was obtained.

Forensic Imaging and Analysis: Using specialized forensic tools like Kali Linux, Autopsy, and EnCase, the team generated a forensic image of the laptop's hard drive and conducted in-depth analysis to identify any presence of hacking software, data, or activities.

II. Lessons Learnings:

Importance of Forensic Imaging: In this investigation, the process of creating forensic images of the digital evidence, particularly the laptop's hard drive, proved critical for preserving its integrity and facilitating thorough analysis without altering or compromising the original data. This practice ensured that all relevant information was captured and maintained for future examination and legal proceedings.

Identification of Hacking Tools: The meticulous examination of software environments and installed applications on the suspect's laptop enabled the team to identify various tools commonly associated with hacking activities, including password recovery tools, network sniffers, and proxy creation tools. This learning underscores the importance of detailed scrutiny during forensic analysis to uncover evidence of illicit behavior and establish links to criminal activities.

Network Analysis: Through comprehensive analysis of network logs and traffic data, the investigative team gained valuable insights into the suspect's online activities, including attempts to access unauthorized resources, communication with malicious entities, and potential data exfiltration. This learning highlights the significance of network forensics in uncovering digital evidence and piecing together the timeline of events in cybercrime investigations.

Continuous Training and Skill Development: The complexity of this investigation underscored the importance of ongoing training and skill development for forensic analysts. Specific training in advanced digital forensic techniques, including network analysis and the use of specialized forensic tools, is essential to effectively handle complex cyber-crime cases and ensure that investigators remain up to date with the latest methodologies and technologies in the field.

III. Inferences:

Intent and Capabilities of Suspect: The presence of hacking tools such as NetStumbler, Look@LAN, Cain & Abel, Ethereal (Wireshark), Anonymizer, and others suggests a deliberate attempt to engage in illicit activities aimed at accessing sensitive information and exploiting vulnerabilities in wireless networks (Figure 11). The interception equipment including the homemade 802.11b antenna and PCMCIA wireless card further supports the notion of the

suspect's intent to manipulate wireless signals for potentially malicious purposes (Figure 1 and 2).

Identification of Suspect: The investigation uncovered significant evidence linking the registered owner of the laptop, Greg Schardt, with malicious activities conducted under the alias "Mr. Evil." The discovery of installed programs, such as Look@LAN which references both "Mr. Evil" and "Greg Schardt" in configuration files, reinforces the connection between the two identities (Figure 15 and 16).

Criminal Activities: The presence of captured and intercepted data stored in the "interception" file within Mr. Schardt's My Documents directory suggests unauthorized access and data interception activities (Figure 14). Examination of network configurations and communication protocols revealed in the investigation indicates potential involvement in online forums or chat groups related to hacking (Figure 16). Additionally, the discovery of deleted executables and a zip bomb file named "unix_hack.tgz" highlights potential involvement in malicious activities such as data destruction or system disruption (Figure 17).

Conclusion

I. Application

This entire investigation focused on whether Mr. Schardt was illegally intercepting wireless traffic. During our investigation we uncovered lots of information linking Mr. Schardt to the alleged crimes against him. By identifying Mr. Schardt as the owner of the laptop and tracing his trail of activities through looking at his usernames, email addresses, and network activity, we

have uncovered direct evidence of his involvement in the alleged cybercrimes. These artifacts of data will be extremely important in a criminal court to link Mr. Schardt to the crimes. The prosecution will most likely call us to the stand to testify to our finding to establish his involvement.

The discovery of hacking tools such as Cain & Abel v2.5 beta45, NetStumbler, and Ethereal on Mr. Schardt's computer implicates him in violating the Computer Fraud and Abuse Act (CFAA), a federal law in the United States that prohibits unauthorized access to computer systems. The CFAA specifically prohibits individuals from knowingly accessing a computer without authorization or exceeding authorized access to obtain information. In Mr. Schardt's case, the presence of these tools and other artifacts found on his device show an intent to engage in unauthorized activities, including network intrusion, data interception, and malicious exploitation of vulnerabilities in computer systems. We discovered through our investigation that Cain & Abel, for instance, is used for its password recovery capabilities, enabling users to retrieve passwords for various accounts and gain unauthorized access to sensitive information.

NetStumbler, is primarily used for scanning and mapping wireless networks, indicating an interest in exploiting vulnerabilities in wireless systems. Ethereal is a packet sniffing tool that allows users to capture and analyze network traffic, in fact we discovered PCAP files of captures that Mr. Schardt conducted. raising concerns about potential interception of sensitive data transmitted over networks.

Our likely testimony in court will be essential to establish a clear link between Mr. Schardt and the crimes. The prosecution will expect us to provide detailed explanations of the functionality of the discovered tools, how they were used, and the implications of their presence on Mr. Schardt's computer. Also, we need to understand our role as experts and what we can say. In the courtroom, it is important to remember that we are most likely going to be the only people there

with any understanding of digital forensics. Therefore, we have a duty to clearly explain ourselves and educate the court. So, we should be familiar with the Federal Evidence rules and have a good understanding of the relevant topics. Through our testimony, and by contextualizing our findings within the framework of the CFAA and relevant case law, we should be able to demonstrate how Mr. Schardt's actions meet the criteria for criminal activity under the different statutes.

II. Alternatives

Other methods that we could have used to conduct this investigation would have been to use different tools that are available. There are several tools that we could have utilized to analyze the evidence for Mr. Schardts activities. For example, we could have used Encase, which is a widely used tool in digital forensics that can be used for disk imaging, data recovery, and analysis of files [48]. We could have also used FTK or the forensic tool kit. This is another very popular tool that is used that offers similar features to Autopsy, which we used in our investigation. FTK allows for keyword searching, email parsing, registry examination, and more [49]. We use some of these features offered by Autopsy. We very easily could have used FTK and found the same results.

III. Future Work

This case took place in 2004. There's a 20-year change in technology. First, Windows XP is no longer supported, although it's still available for use. Digital forensics was less complex compared to today.

Digital devices such as computers, mobile phones, and external storage media were prevalent in 2004, but not as widespread as they are now in 2024. Investigators primarily dealt with desktop computers, laptops, and basic mobile phones.

It has become more challenging to get into all the nooks and crannies that can exist with data. Between changing encryption to different data artifacts that are proprietary and protected, examiners have more hurdles to overcome.

Digital forensics also must deal with new fundamental changes such as cloud computing, Internet of Things (IoT), remote digital forensics, and newer technologies such as artificial intelligence (AI). All of these have created extra complexity for the digital forensics space [50].

Computer-generated documents, including log files, weren't originally allowed in court cases because they were deemed hearsay. However, Case law and updates to the Federal Rules of Evidence have changed that. Rule 803 provides for the admissibility of a record or report that was "made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation [51]."

References

[1] PruthvirajS, "Pruthviraj-S/Computer-Forensics," *GitHub*, Oct. 22, 2023.

<https://github.com/Pruthviraj-S/Computer-Forensics> (accessed Mar. 01, 2024).

[2] "Why Is Computer Forensics Important? | NU.edu," *National University*, Feb. 16, 2019.

<https://www.nu.edu/blog/ask-an-expert-why-is-computer-forensics-important/>

- [3] “What Is Digital Forensics and When Do You Need It? - Cybersecurity | Digital Forensics | Crypto Investigations,” *ermprotect.com*, Apr. 10, 2022. <https://ermprotect.com/blog/whatis-digital-forensics-and-when-do-you-needit/#:~:text=Digital%20forensics%20is%20often%20a>
- [4] A. D. F. Solutions, “Why is Digital Forensic Training Important?,” *www.adfsolutions.com*.
<https://www.adfsolutions.com/news/why-is-digital-forensic-trainingimportant/#:~:text=Digital%20forensics%20training%20is%20an>
- [5] Autopsy. (n.d.). Autopsy: The Sleuth Kit. [Online]. Available: <https://www.autopsy.com/>.
(Accessed: March 12, 2024).
- [6] “Compliance and Workplace Investigations,” *Caplan & Earnest*.
<https://celaw.com/practiceareas/compliance-and-workplaceinvestigations/#:~:text=Violations%20of%20regulatory%20compliance%20regulations> (accessed Mar. 01, 2024).
- [7] United States Courts, “What Does the Fourth Amendment Mean?,” *United States Courts*.
<https://www.uscourts.gov/about-federal-courts/educational-resources/about-educationaloutreach/activity-resources/what-does-0>
- [8] Cornell Law School, “Exclusionary Rule,” *LII / Legal Information Institute*, 2017.
https://www.law.cornell.edu/wex/exclusionary_rule
- [9] Wikipedia Contributors, “Exclusionary rule,” *Wikipedia*, Feb. 06, 2024.
https://en.wikipedia.org/wiki/Exclusionary_rule#:~:text=Limitations%20on%20the%20exclusionary%20rule (accessed Mar. 04, 2024).
- [10] “Digital Search Warrants,” *Law Enforcement Cyber Center*.
<https://www.iacpcybercenter.org/prosecutors/digital-searchwarrants/#:~:text=A%20search%20warrant%20may%20be>

- [11] “Cybersecurity Information Sharing Act,” *Wikipedia*, Jan. 01, 2024.
https://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act#:~:text=The%20law%20allows%20the%20sharing (accessed Mar. 06, 2024).
- [12] U.S. Department of Justice, “9-48.000 - Computer Fraud and Abuse Act,” www.justice.gov, Feb. 19, 2015. <https://www.justice.gov/jm/jm-9-48000-computer-fraud>
- [13] Bureau of Justice Assistance, “Electronic Communications Privacy Act of 1986 (ECPA),” *Bureau of Justice Assistance*, 2023. <https://bja.ojp.gov/program/it/privacy-civilliberties/authorities/statutes/1285>
- [14] “Electronic Communications Privacy Act (ECPA),” *EPIC - Electronic Privacy Information Center*. <https://epic.org/ecpa/#:~:text=Individuals%20who%20violate%20ECPA%20face>
- [15] American Medical Association, “HIPAA violations & enforcement,” *American Medical Association*, 2023. <https://www.ama-assn.org/practice-management/hipaa/hipaaviolation-enforcement>
- [16] SecureFrame, “Secureframe: Build trust. Unlock growth.,” *Secureframe*.
<https://secureframe.com/hub/pci-dss/benefits-of-pci-dss-compliance>
- [17] “PCI Compliance - Cybersecurity | Digital Forensics | Penetration Testing | ERMProtect,” *ermprotect.com*, Mar. 02, 2020. <https://ermprotect.com/pci-compliance/> (accessed Mar. 22, 2024).
- [18] Oro, “PCI DSS fines and the consequences of non-compliance,” *Thoropass*, Sep. 15, 2023.
<https://thoropass.com/blog/compliance/pci-dss-fines-andpenalties/#:~:text=Indirect%20consequences%20of%20non%2Dcompliance&text=Businesses%20that%20fail%20to%20comply> (accessed Mar. 22, 2024).
- [19] S. Chen *et al.*, “Exploring the global geography of cybercrime and its driving forces,” *Humanities and Social Sciences Communications*, vol. 10, no. 1, Feb. 2023, doi:

<https://doi.org/10.1057/s41599-023-01560-x>.

- [20] N. Rakha, "Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations," *ResearchGate*, Oct. 16, 2023.

https://www.researchgate.net/publication/378197719_Cybercrime_and_the_Law_Addressing_the_Challenges_of_Digital_Forensics_in_Criminal_Investigations (accessed Mar. 22, 2024).

- [21] B. Wolford, "What Is GDPR, the EU's New Data Protection Law?," *GDPR.eu*, 2020.

<https://gdpr.eu/what-is-gdpr/>

- [22] "Does the GDPR apply to companies outside of the EU?," *GDPR.eu*, Nov. 18, 2018.

<https://gdpr.eu/companies-outside-of-europe/#:~:text=The%20GDPR%20does%20apply%20outside>

- [23] F. Sharevski, "Rules of professional responsibility in digital forensics: A comparative analysis," *Journal of Digital Forensics, Security and Law*, vol. 10, no. 2, 2015, doi:

<https://doi.org/10.15394/jdfsl.2015.1201>.

- [24] "How Crime Scene Investigation Works," Forensic Science Simplified, [Online]. Available:

<https://www.forensicsciencesimplified.org/csi/how.html> (Accessed: March 12, 2024).

- [25] North Carolina Department of Justice, "Trace Evidence," [Online]. Available:

<https://ncdoj.gov/crime-lab/trace-evidence/>. (Accessed: March 16, 2024).

- [26] W. C. Brown, "Introduction to Computer Science," [Online]. Available:

<https://www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l30/lec.html>.

(Accessed: March 16, 2024).

- [27] "From the archives: Westerfield verdict anniversary," [Online]. Available:

<https://www.sandiegouniontribune.com/news/local-history/story/2022-08-21/from-the-archives-westerfield-verdict-anniversary>. (Accessed: March 16, 2024).

- [28] "Forensic Methods and Labs - Forensic Methodologies," Digital Forensics, Investigation, and Response, Fourth Edition, ISBN 9781284228236, Chapter 3, pp. 1-3, . Available: <https://openpageebooks.jblearning.com/wr/viewer.html?skipLastRead=true&oneTimePasscode=ST-67345bea-dc29-4dd9-8c0c-a3e21ea76ebe&laun...> (Accessed: March 12, 2024).
- [29] TechTarget, "Forensic Image," [Online]. Available: <https://techtarget.com/whatis/definition/forensic-image>. (Accessed: March 16, 2024).
- [30] C. Easttom, *Digital Forensics, Investigation, and Response*. Jones & Bartlett Learning, 2021, pp. 210–211.
- [31] C. Wilson, "DCodeTM | Digital Detective," Digital Detective, Nov. 02, 2009. <https://www.digital-detective.net/dcode/> (accessed Mar. 31, 2024).
- [32] M. Kuo, Ed., "Wireless PCMCIA User Manual," <https://fccid.io/MCLT60H625/User-Manual/User-Manual-278003.pdf>, 2002. (Accessed: March 17, 2024).
- [33] E. Sandler, "802.11 Cantennas Done Up Homebrew Style - WiFi Planet," WiFi Planet, Sep. 22, 2021. <https://wi-fiplanet.com/802-11-cantennas-done-up-homebrew-style/> (accessed Mar. 17, 2024).
- [33] A. Khanse, "What Is Index.dat file? Index.dat Location, Removal, Reader, Viewer," The Windows Club, Apr. 11, 2014. <https://www.thewindowsclub.com/index-dat-file-windows> (accessed Mar. 24, 2024).
- [34] B. Mitchell, "802.11 WiFi Standards Explained," Lifewire, 2019. <https://www.lifewire.com/wireless-standards-802-11a-802-11b-g-n-and-802-11ac-816553> (accessed Mar. 23, 2024).
- [35] "The Sleuth Kit (TSK) & Autopsy: Open Source Digital Forensics Tools," *Sleuthkit.org*, 2019. <https://www.sleuthkit.org/index.php>

- [36] A. Dennis, “Methods to Recover Deleted Files from Windows XP,”
recoverit.wondershare.com, Mar. 18, 2024.
<https://recoverit.wondershare.com/computerrecovery/recover-deleted-files-from-windows-xp.html> (accessed Mar. 24, 2024).
- [37] “Chapter 2 - The Forensic Investigation Process,” Exterro.
<https://www.exterro.com/basicsof-digital-forensics/chapter-2-the-forensic-investigation-process> (accessed Apr. 14, 2024).
- [38] McKemmish, R., 2008, in IFIP International Federation for Information Processing, Volume 285; Advances in Digital Forensics IV; Indrajit Ray, Sujeet Shenoi; (Boston: Springer), pp. 3–15.
- [39] Processing a Hard Drive as Evidence: Using FTK Imager for Forensic Imaging and Integrity...,” Medium, Apr. 02, 2023. <https://medium.com/@M4rk7/processing-a-harddrive-as-evidence-using-ftk-imager-for-forensic-imaging-and-integrity-3fd82d04074c>
(accessed Apr. 06, 2024)
- [40] NetStumbler. (n.d.). NetStumbler. [Online]. Available: <https://www.netstumbler.com/>.
Accessed: March 31, 2024.
- [41] MajorGeeks. (n.d.). Look@LAN. [Online]. Available:
<https://www.majorgeeks.com/files/details/looklan.html>. Accessed: March 31, 2024.
- [42] 2ip.io. (n.d.). Anonim - Online IP Anonymity Check. [Online]. Available:
<https://2ip.io/anonim/>. Accessed: March 31, 2024.
- [43] Profibus. (n.d.). Download Ethereal/Wireshark. [Online]. Available:
<https://www.profibus.com/download/ethereal-wireshark>. Accessed: March 31, 2024.
- [44] O. Chalke, “Network News Transfer Protocol (NNTP),” GeeksforGeeks, Oct. 04, 2019.

<https://www.geeksforgeeks.org/network-news-transfer-protocol-nntp/> (accessed Mar. 31, 2024).

[45] “Forte Agent Newsreader Review,” [usenetreviews.org](https://www.usenetreviews.org).

<https://usenetreviews.org/newsreaders/forteagent/#:~:text=Forte%20Agent%20is%20a%20well-known%20newsreader> (accessed Mar. 31, 2024).

[46] “What is an Internet Relay Chat (IRC)?,” IONOS Digital Guide, Jan. 11, 2022.

<https://www.ionos.com/digitalguide/server/know-how/irc/> (accessed Mar. 31, 2024).

[47] V. F. Garcia, “How Does a Zip Bomb Work? | Baeldung on Computer Science,”

[www.baeldung.com](https://www.baeldung.com/cs/zip-bomb), May 09, 2022. <https://www.baeldung.com/cs/zip-bomb> (accessed Mar. 31, 2024).

[48] Wikipedia, “EnCase,” *Wikipedia*, Dec. 08, 2019. <https://en.wikipedia.org/wiki/EnCase>

[49] “FTK Forensics Toolkit - Digital Forensics Software Tools | Exterro,” *Exterro [Staging]*.

<https://www.exterro.com/digital-forensics-software/forensic-toolkit>

[50] C. Simms and J. P. Kakembo, “Digital IT Forensics Evolution Through Digital

Transformation,” *ISACA*, Jul. 11, 2022. <https://www.isaca.org/resources/news-and-trends/isacanow-blog/2022/digital-it-forensics-evolution-through-digital-transformation>

[51] C. Izuakor, “The Evolution of Digital Forensics,” *Veriato*, Mar. 03, 2020.

<https://veriato.com/blog/the-evolution-of-digital-forensics/> (accessed Apr. 06, 2024).

Exhibits

The items listed in the Exhibits section of this report remain in a secure chain of custody throughout the analysis process and were turned over to the investigating agency upon determining a conclusion. The items were acquired in March 2004.

Items

- Abandoned CPi notebook computer with serial number VLQLW
- Wireless PCMCIA card
- External homemade 802.11b antenna
- Homemade 802.11b antennae
- DD image segments (SCHARDT.001 to SCHARDT.008)
- Executable files found in the Recycle Bin (Dc1.exe, Dc2.exe, Dc3.exe, Dc4.exe)
- Zip bomb file "unix_hack.tgz"
- PCAP files of network captures conducted by Mr. Schardt

Additional Interesting Artifacts

- irunin.ini file containing Mr. Schardt's alias "Mr. Evil" and LAN information
- Agent.ini file belonging to Forte Agent containing email server settings
- Outlook Express settings found in NTUSER.DAT file
- *Chat logs from MIRC channels*

Chain of Custody

Date & Time	Location	Description of Activity	Examiner
03/26/2024	Examiner's machine	Evidence collection: Downloaded DD images of the Dell CPI notebook computer, and laptop hardrive.	Group 6
03/26/2024	Examiner's machine	Evidence duplication and hashing.	Group 6
03/26/2024	Examiner's machine	Reconstructing drive image and formatting.	Group 6
03/26/2024	Examiner's machine	Imported drive image to Autopsy forensic tool	Group 6
03/26/2024	Examiner's machine	Conducted examination of evidence using Autopsy	Group 6
03/31/2024	Examiner's machine	Examination complete	Group 6

Exhibit 1: Forensic Image of Suspect's Hard Drive

Description: This exhibit contains a forensic image of the suspect's hard drive obtained during the investigation.

Relevance: The forensic image was created using industry-standard tools and contains a bit-by-bit copy of the suspect's hard drive, preserving its original state for analysis. The image was used to discover the user's online activity and what he was doing.

Exhibit 2: IRC Message Logs

Description: This exhibit consists of forum post logs obtained from news and forum platforms used by the suspect.

Relevance: The logs reveal conversations relevant to the investigation, including discussions related to the alleged criminal activities. It also shows that Mr. Evil may have received additional information from third parties.

Exhibit 3: Homemade 802.11b antenna

Description: This exhibit consists of a homemade 802.11b antenna found along with the Dell laptop and the PCMCIA card.

Relevance: The antenna must have been used to generate a point-to-multipoint network configuration. If that's the case, the attacker could set up a rogue PtMP network to intercept or manipulate traffic.

Exhibit 4: PCMCIA Card

Description: This exhibit consists of a PCMCIA card found along with the Dell laptop and the homemade antenna.

Relevance: The PCMCIA card and external antenna suggests a deliberate attempt to enhance wireless communication capabilities, potentially enabling the interception of wireless signals.

Exhibit 5: Dc1.exe, Dc2.exe, Dc3.exe, Dc4.exe

Description: This exhibit includes executable files found in the Recycle Bin of the abandoned CPi notebook computer, namely Dc1.exe, Dc2.exe, Dc3.exe, and Dc4.exe.

Relevance: The presence of executable files in the Recycle Bin indicates potential software used by Mr. Schardt for malicious purposes. Analysis of these files may reveal their functionality, purpose, and connection to the alleged cybercrimes.

Exhibit 6: Zip Bomb File "unix_hack.tgz"

Description: This exhibit consists of a zip bomb file named "unix_hack.tgz" recovered from the abandoned CPi notebook computer.

Relevance: The zip bomb file is indicative of Mr. Schardt's involvement in malicious activities aimed at disrupting computer systems. Analysis of the file may reveal its composition, potential targets, and methods used by Mr. Schardt to execute the attack.

Exhibit 7: PCAP Files

Description: This exhibit comprises PCAP files obtained from network captures conducted by Mr. Schardt using the CPi notebook computer.

Relevance: The PCAP files contain captured network traffic, including packets transmitted and received by Mr. Schardt's device. Analysis of these files may uncover evidence of unauthorized network access, data interception, and other illicit activities attributed to Mr. Schardt.

Exhibit 8: irunin.ini File

Description: This exhibit consists of the irunin.ini file discovered during the investigation, containing references to Mr. Schardt's alias "Mr. Evil" and LAN-related information.

Relevance: The irunin.ini file provides evidence linking Mr. Schardt to the alias "Mr. Evil," indicating potential involvement in illicit activities. Additionally, LAN information found within the file may shed light on Mr. Schardt's network connections and activities.

Exhibit 9: Agent.ini

Description: This exhibit includes the Agent.ini file associated with Forte Agent, a newsreader application, containing email server settings.

Relevance: The Agent.ini file reveals email server configurations used by Mr. Schardt, providing insight into his email communication activities and potential involvement in cybercrimes.

Exhibit 10: NTUSER.DAT File

Description: This exhibit comprises Outlook Express settings extracted from the NTUSER.DAT file associated with Mr. Schardt's user profile.

Relevance: The Outlook Express settings offer valuable information about Mr. Schardt's email management preferences and server configurations, aiding in the investigation of his email correspondence and potential involvement in criminal activities.