Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

WIRELESS ROUTER FORENSICS: FINDING ARTIFACTS OF SUSPECT TRACES WITH A RASPBERRY PI AND KALI LINUX.

SYED ZAIN UL HASSAN
Department of Software Engineering, Superior University Lahore, Pakistan.
Email: zain.ravian@gmail.com

MUHAMMAD SHAIROZE MALIK
Department of MSIS, Superior University Lahore, Pakistan. Email: shairozemalik@lgu.edu.pk

MUHAMMAD WASEEM IQBAL
Ph.D., Associate Professor Department of Software Engineering, Superior University Lahore, Pakistan. Email: waseem.iqbal@superior.edu.pk

SHAHERYAR
MSCS, Superior University Lahore, Pakistan. Email: Shaheryarchattha362@gmail.com

MUHAMMAD ZUBAIR
MSIS Information Security, Superior University Lahore, Pakistan. Email: muhammadzubhair@gmail.com

MUHAMMAD REHMAN
Department of Computer Science and Information Technology, Vice Principal Superior College Jhang.
Email: rehmanicc@gmail.com

KHALID HAMID*
Ph.D. Scholar, Department of Computer Science, Superior University Lahore, Pakistan. Lecturer Computer Science at NCBA & E East Canal Campus Lahore. Email: khalid6140@gmail.com

Abstract

With 802.11's growth, law enforcement may have new hurdles to overcome when investigating cybercrimes. Wireless networks' complicated architecture makes it harder to discover artifacts than conventional networks. Modern digital forensic approaches face issues when developing forensic methodologies. Data integrity, privacy, password cracking, and IP address access are major issues. Digital forensics requires finding evidence. As the number of connected devices expands, it's important to collect and study their digital traces. Most of these devices are connected to a router, so they can instantly connect to the internet and use unlimited bandwidth. During a forensic investigation, there are two key concerns with wireless devices: discovering and safeguarding digital evidence and evaluating seized goods. In our research, "live" and "postmortem" forensics of router devices are used in investigations. We create a Wi-Fi router forensic framework using portable devices. This portable gadget can be used for live forensics at crime scenes. Our investigation uses a fourth-generation Raspberry Pi and Kali Linux version 2022.1, which runs open-source applications. This research project is inexpensive, portable, easy to put up, effective, and satisfying. This research studies how to find forensic data and where it is housed. It also examines forensic data retrieval. We employ Cisco, TP-Link, and Huawei routers to demonstrate our findings in real-time.

Keywords: Digital Forensics, Router Forensic, IP Traces Through The Router, Live Forensically, Crime Scene Router Forensic.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

1. INTRODUCTION

The IEEE 802.11 family of communication protocols is one of the few networking technologies that have become so popular in such a short amount of time [1]. Digital forensics is a relatively new field that tries to find, store, and analyze this kind of evidence [2]. "Wireless Internet access will create new issues for law enforcement," they added about wireless gadgets. Wireless computers are easier to move and harder to track than wired systems. Weak security makes it hard to discover the culprit. This research examines digital forensics from a wireless networking standpoint. This article discusses digital forensics in connection to upcoming technologies, focusing on 802.11-based wireless networking. This research discusses the different elements of a forensic inquiry, including what information and evidence can be uncovered through forensic analysis, where this information is housed, and what wireless technologies and protocols are needed.

1.1 Kali Linux

Kali Linux is an operating system (OS) that focuses on security. It is based on Debian and was made for computer forensics and advanced penetration testing. It was made by Mati Aharoni and Devon Kearns of Offensive Security [3], who took Backtrack and changed it. Kali Linux has several hundred tools [4] that are well-suited to different information security tasks, such as penetration testing, security research, computer forensics, and reverse engineering.

Backtrack was their old operating system for information security [5]. Kali 1.0.0, the first version of Kali Linux, came out in March 2013. At the moment, Offensive Security pays for and supports Kalin Linux. If you went to Kali's website (www.kali.org) [6] right now.

1.2 Raspberry Pi

Raspberry pi is the most popular hacking device, which is designed only for ethical hackers [7]. Raspberry Pi being portable, weighs much light and can be carried anywhere.

1.3 Wi-Fi is being used in crime

Because Wi-Fi may be configured in a variety of different ways, thieves have a variety of options available to them when it comes to how they might use wireless devices and networks. Because of the work done in this area, a taxonomy model of how wireless technology is abused has been developed [8].

1.3.1 Finding and connecting to a wireless network

Attacks can be made in two ways using wireless networks: against devices that are connected to the network [9]. Through this work, many areas of misuse in the wireless domain have been found. One thing to keep in mind is that some of these misuses could be seen as anti-forensics [10] because they are ways to hide or cover up possible digital evidence.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

1.4 Motivation

Digital forensics is still evolving. No guideline exists because there are so numerous devices, as seen in the chapter regarding related work. We won't set a rule because so many gadgets use their software or hardware. Instead, we want to learn about routers, which most connected devices use nowadays. By 2023, each person will have 1.6 mobile-connected devices, up from 1.2 in 2018 [11]. This demonstrates the importance of this research. IoT gadgets include phones, watches, TVs, sensors, etc., making digital investigations difficult. All of these devices can connect to a router (Wi-Fi hotspot) to transfer VoIP, video streams, messages, and other data across that gateway.

1.5 Why wireless forensics is important

Identify the suspect IP address behind the attack. The main goal is to give people the ways and tools they need to collect and study traffic on wireless networks. Wireless Network forensics is a key part of a security operations program [12] that works well. Wireless Network forensics is an important tool [13] for a defense team.

1.6 Risks involves in wireless network

Some of the risks include in a wireless network are:

1.6.1 Piggybacking

If you don't take the necessary precautions to secure your wireless network, anyone within range of your access point who possesses a computer that is capable of connecting wirelessly will be able to use it [14].

1.6.2 Wardriving

One kind of piggybacking is known as "war driving [15]" Because of the expansive broadcast range of wireless access points, it is possible to connect to the internet even while you are outside of your house and as far away as the street

1.6.3 Evil twin attacks

A public network access point is discovered, and the attacker puts up their system to imitate it in an evil twin attack [16].

1.6.4 Wireless sniffing

There are a lot of open access points, and most of them don't have any kind of security or encryption on their connection [17].

1.6.5 Unauthorized computer access

If you use a public wireless network that isn't secure and don't use secure file sharing, a malicious user might be able to access any directories and files that you unintentionally shared. Make sure that you don't share files and folders when you connect your devices to public networks [18].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

1.6.6 Shoulder surfing

People who intend to because you harm can easily spy on you as you type in public locations by just looking over your shoulder [19].

1.6.7 Theft of mobile devices

Not all bad actors will gain access to your data via wireless means. If an attacker physically seizes your device, they may have total access to all data and cloud accounts linked with it. Protection against loss or theft is essential, but if the worst happens, a little forethought may safeguard the data contained therein. Most mobile devices, including laptop computers, now fully encrypt stored data [20],

1.7 Problem Statement

Digital forensics is a new field whose research and practice are changing quickly. Lack of proper guidelines for collecting, analyzing, and presenting electronic evidence, the speed at which technology changes, criminals' use of anti-forensic techniques, investigators' use of free online tools, etc. are common problems.

This research is limited to demonstrating with examples some of the current methods and tools that can be used by people with an Intermediate level of knowledge in Computer Science and that just by knowing the name of the network, ESSID (black box test), that is around them, proceed to violate the protection systems, based on WEP, WPA PSK, WPA2 PSK with or without WPS, obtaining access to the Internet at no cost, even and with a little more effort, they would.

Business transactions, government services, and other commercial activities take place on open networks like the Internet. This has led to a rise in cyber threats and information security issues used by cybercriminals. Mistrust of communications and computer network technologies affects individuals and businesses globally. They often have different rules and laws. Complex communication and networking infrastructure make crimes harder to solve. Digital crimes leave hard-to-find traces because they involve lots of data.

This causes computer communities to use digital forensics to combat cybercrimes, giving law enforcement more work. Providing solid evidence requires well-prepared forensics professionals. Forensic procedures must keep up with new technology to achieve these goals. Digital forensics' role in law enforcement and data/network security is growing. Because of its importance, computer professionals, law enforcement, and practitioners have given network forensics a lot of attention. Network forensics still faces problems with digital evidence processing and other forensic procedures.

1.8 Research objective

The main goal is to analyze routers for useful information. Artifacts could be used as evidence or to learn more. For our research, we may want to know who's connected, system logs, time settings, etc. The next chapters will elaborate.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

1.9 Scope

We thought comparing three routers would be more informative. Two of these routers connect via SIM card and 4G technology. SIM cards could also be analyzed forensically, but we decided to focus on the router. HUAWEI WIFI AX3 Pro and TP-LINK TLMR6400 are our 4G router picks. As you can see in the section on related works, there hasn't been much forensics research on 4G routers. The Linksys EA7500 needs an Ethernet cable to work with Wi-Fi. To compare, we added a non-4G router.

1.10 Contribution

When I researched forensics, specifically routers, some papers only show forensic artifacts, not how they were found. Sharing our research results helps forensics. Our routers had problems. What we've learned about extracting useful data from our routers can be applied to other models or brands. Our paper can help with router forensics. It will speed up crime scene response.

1.11 Limitation

We had technical problems extracting data from router hardware. Our lab wasn't set up for that. We still used some hardware techniques, but as we said at the beginning of the paper, our lab didn't have the right equipment. We still discuss those techniques when we find them in research.

2. LITERATURE REVIEW

This chapter has all the information you need to understand our paper better, as well as a description of the methods used to get forensic artifacts from Wi-Fi routers. I also show what has already been done in the field of forensics. This gives us an idea of what has already been done in this area.

2.1 Triage

The purpose of digital forensics triage is to provide crime scene investigators with crucial information [21]. They will be able to immediately begin the investigation since they will know which gadgets are present, can be gathered, etc. has further details on a Korean triage approach that can be applied.

2.2 Volatile memory

The part of the device that allows for high-speed information storage is called the volatile memory. Only an electric current can read or write data from such memory since losing power would cause the data to be lost [22]. A router logging information in the system would be an example of a capability utilizing the area.

2.3 Non-volatile memory

The non-volatile memory may be thought of as the portion of the device's memory that is permanently written during device manufacture [23].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

2.4 Valuable forensic artifacts

Due to the lack of a clear definition for the term "artifact" in the field of digital forensics, suggested the usage of the term "Curated (digital) Forensic Artifact (CuFA)" [24].

2.5 Manual Extraction

A manual approach will be the first technique we employ in our inquiry. This includes all the data that an investigator may personally compile. In our instance, it will be through the router's web interface, which can be accessed by clicking on the various buttons. R. Ayers et al. [25] have discussed some of the drawbacks of this strategy, including the time-consuming nature of such an extraction method dependent on the volume of data to be analyzed.

2.6 Logical Extraction

For logical extraction, we require communication between the router and the forensics workstation. Both wired and wireless connections are possible [26].

2.7 Hardware Extraction

In our scenario, hardware-based extraction refers to the ability to access unprocessed data that is kept in memory. The investigator will be able to see a general overview of the router's internal file system thanks to that extraction procedure [27].

2.8 Wireless attacks related papers

This study shows [28] how to use the Hash cat method to crack the password on the Kali Linux OS to launch a wireless attack. In this study, a brute-force attack online and a straight attack offline are used to find the security holes. This study shows [29] in a cyber-investigation, the most important thing for law enforcement agencies (LEAs) to do is to look at call records. This study shows [30] to teach people about cyber security and demonstrate how simple it is to attack someone else's computers using a tiny device like a Raspberry Pi. This study shows [31] to take free WiFi for granted practically everywhere, from coffee shops to airports. This is beneficial in many ways, but it also increases the likelihood that hackers will fool people. This study shows [32] to evaluate and assess the security of a network, this educational project employs a second-generation Raspberry Pi that can run several open-source software applications. Students in their first year of college gain practical experience while learning more about computer hardware, operating systems, and network security by working on this project. This study shows [33] to use and improve the functionality of mobile devices like smartphones, tablets, and Internet of Things (IoT) apps, wireless networks are already commonplace. This has increased the need for improved testing techniques for wireless security as well as for more technically inclined individuals to receive wireless security training. This study shows [34] how IEEE 802.11 wireless network encryption and the Wi-Fi Protected Setup (WPS) function are used in the real world. There is a short history of how encryption methods and WPS came to be what they are today. The results have been a wireless scan of 802.11 networks in the capital city, and the results

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

have been looked at. This study shows [35] Kali Linux SQL injection, XSS, WordPress, and WPA2 attacks penetration testing in 2019. These days, a variety of threats and exploits can affect computers, smartphones, smart watches, printers, projectors, washing machines, refrigerators, and other mobile devices that connect to the Internet. This study shows [36] Wi-Fi has become a tempting target for security threats because it carries more than 75% of the last-mile mobile Internet traffic. In this work, we use a crowdsourced security checking system on 14 million mobile devices out in the wild to study a wide range of real-world Wi-Fi threats on a scale that has never been done before. This study shows [37] there are a lot of open-source hacking tools on the Internet and a lot of hacking tools built into the Kali Linux operating system, it is easy for people to learn how to hack and do it. This study shows [38] wireless devices are much more likely to be hacked than they used to be. Hackers can get into the system through the many holes in the WLAN. People don't know enough about how to keep themselves safe. This study shows [39] rolling Kali Linux 2016.2 OS. In this article, the author demonstrates how to use several tools in the Kali Linux 2016.2 operating system to carry out a de-authentication attack on an 802.11i wireless network. This study shows [40] wireless networks have become much more popular as a way to communicate because they are flexible, mobile, and easy to use. It is used everywhere, including hotels, restaurants, airports, businesses, and most homes right now. This study shows [41] Wireless Local Area Networks are widely used because they are portable, inexpensive to set up and maintain, and simple to install. The increasing usage of wireless networks has attracted attackers' attention. This study shows [42] both at work and home, smart mobile devices play a significant role in our lives. The quantity of data we leave behind increases as our use of these gadgets and our digital lives expand. This study shows [43] the benefits of wireless communication networks such as portability, flexibility, greater productivity, roaming capabilities, low installation costs, etc., but their security has remained a major worry [44-49].

3. RESEARCH METHODOLOGY

This study will concentrate on the forensic examination of the Internet-to-Internet gateway between IoT devices (including PCs and other devices), as was already mentioned in the introduction. In the chapters that follow, we will explain the important information we seek while working and how we set up our lab for the various experiments. The forensic artifacts we collected from the router are shown in Table 1.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

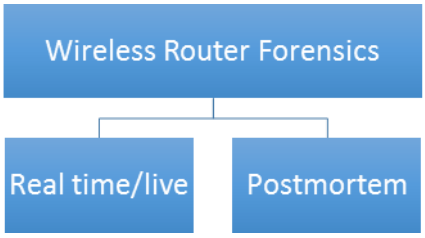
Table 1: Forensic artifacts

Sr. No.	Forensic artifacts.	Why do we look for that?
1.	Firmware type/version.	Looking for any alteration of the system.
2.	NTP settings.	Performing investigation using the correct time zone.
3.	IP addresses of authenticated users.	Able to associate an action to a certain user.
4.	Media Access Control (MAC) address of connected devices.	MAC address is unique to a device and therefore – a significant artifact for further investigations.
5.	User names generated from the connected Devices.	Names can often be linked to a certain Person.
6.	Configuration (files).	Service set identifier (SSID), SIM-card information, MAC address, etc. could allow the investigator to have more options to dig into.
7.	Logs.	Recreating a timeline of events that occurred, could contain user information that could be linked together.

3.1 Wi-Fi is one of the sources of evidence

Using 802.11-based wireless devices as digital evidence depends on several presumptions [50], including the ability to extract information from devices, the ability to evaluate and analyze that data, and the benefit. This is largely device-dependent. Wireless doesn't leave a physical trace, making it hard to find and track wireless items. A forensic investigation requires two main considerations. Finding digital evidence on wireless devices and analyzing seized items. "Live" and "postmortem" parts of an investigation as shown in figure 1.

Figure 1: Wi-Fi router forensic approaches

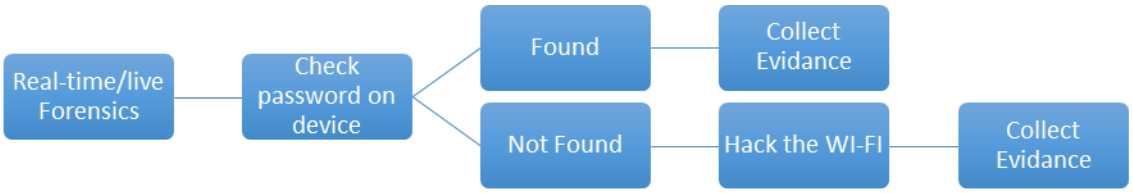


3.2 Real-time/live forensics

In a search-and-seizure scenario, there is a distinct technique to locate wireless gadgets due to their differences. Unlike the majority of electronic equipment that might contain digital evidence, wireless gadgets might not be visible from a great distance or even in plain sight. The real-time, live forensic flow diagram of the router is shown in Figure 2. However, these gadgets could remain in operation or be reachable from a distance. It makes sense from this perspective that lives.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

Figure 2: Real-time/live forensic



3.2.1 Steps involved

- The device remains powered on.
- Try to see the router login password on hardware devices.
- Try to see the Wi-Fi password on hardware devices.
- If not find a password.
- Try to Hack the Wi-Fi password.
- wlan0: First wireless network interface on the system.
- Stop the current processes which are using the WIFI interface.
- For the wlan0 to begin operating in monitor mode.
- To get a list of all the WIFI networks in the vicinity.
- airodump-ng is used for capturing packets [51].
- Name of the interface, which is wlan0mon (This name can be different on the different devices)
- See all of the clients that are currently connected to the target network.
- Launch a separate terminal window to detach the clients that are currently connected to the target network.
- When the client is disconnected from the network that is being targeted. He attempts to rejoin the network, and when he succeeds in doing so, you will see something in the terminal referred to as WPA handshake [46] in the window to the left of it.
- To decrypt the password. Launch the program that manages your files.

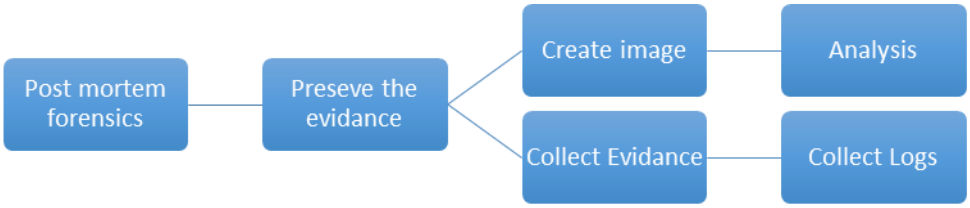
By routinely gathering, examining, and comparing network states, all of this data may be acquired. "Passive network detection" [52] refers to this. All that has to be done, just like with passive network detection, is to gather packet headers. The payloads of these packets are not significant. You might not have to be concerned about legal problems that might restrict how you employ packet sniffer headers and payloads if you use packet headers. Given that headers are not encrypted, you might also not need to be concerned about encryption limit restrictions.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

3.3 Post-mortem forensics

Post-mortem forensics refers to the investigation of wireless devices that can produce evidence after an event. If technology techniques such as communications interception systems are used in the forensic

Figure 3: Post-mortem forensics

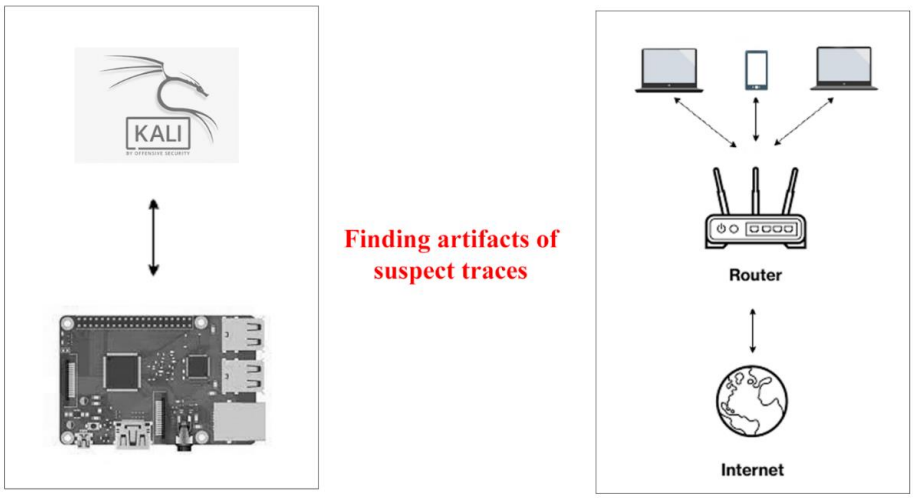


the procedure, they are not included in the post-mortem investigation. However, the results of the first may have an impact on the second while searching for information or leads for the investigation. It accomplishes this by learning as much as it can about the configuration of networks. A post-mortem investigation might further explore this data by inspecting the devices [53] to determine how they were previously linked to networks and looking for any signs of misuse being investigated.

3.4 Forensic Evidence

As we've already said, the goal of this research is to get useful forensic evidence from a router for an investigation. So, we had to set up a lab environment to simulate how real users interact with their different devices so that we could get data that looked like it came from real life and see if we could get any useful information from it. So, we'll use the following network topology to look at how the different routers work [54-56].

Figure 4: Network topology of our lab environment



Raspberry Pi and Kali Linux

Wireless router forensics

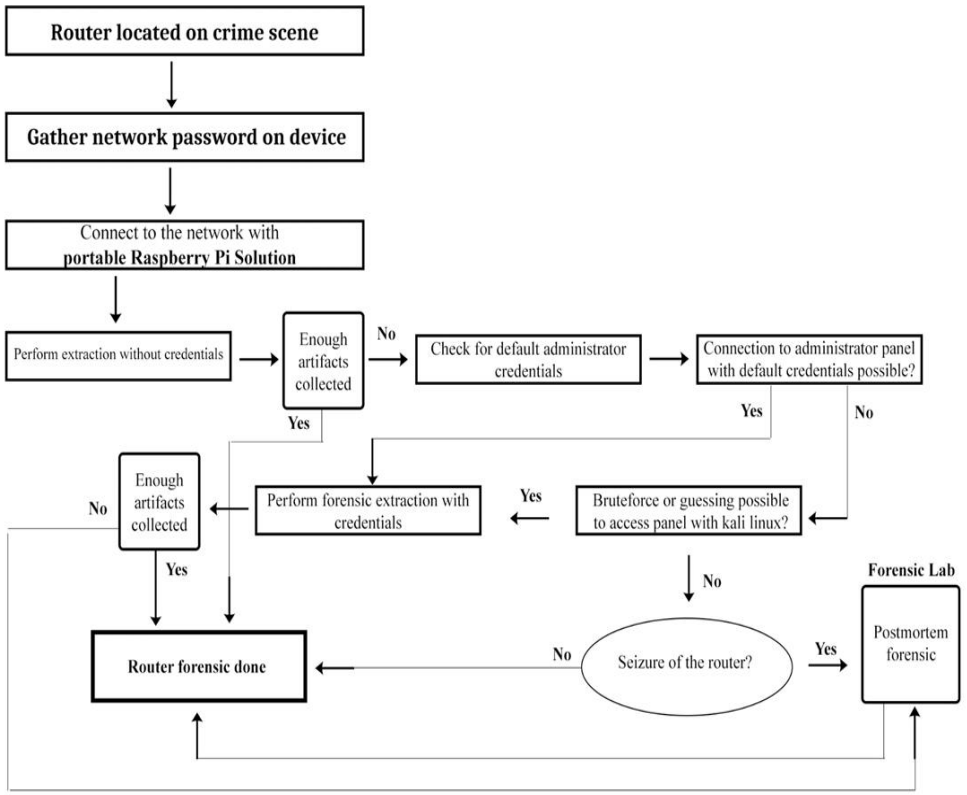
Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

We chose to set up an environment with two computers, one smartphone, and a Wi-Fi router so we could connect to the internet and do our research. An important part of our analysis is that all of the routers being looked at still have their factory settings. This is because most regular users wouldn't change these settings, not even the administrator's password. We decided to make connections between these different devices to see if we could get any useful information. When we talk about "traffic" in our research, we mean information that a real user could give us. Sending and receiving emails, sending messages with a smartphone, watching videos online, etc., are all examples of data streams. We won't give IP addresses directly to the machines in our topology because the routers use the Dynamic Host Configuration Protocol (DHCP) to give IP addresses randomly to all the machines that connect to them (first come, first served). In the following situations, we'll link the IP address we're looking at directly to the machine names from the topology.

3.5 Live acquisition

The forensic team should exercise considerable caution when conducting live investigations on a router since system adjustments cannot be performed. Even the smallest adjustment could undermine the entire inquiry and produce erroneous results. The Router investigation of our proposed solution.is shown in Figure 5.

Figure 5: Router investigation of the proposed solution



Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

- **show access lists:** Activates and displays all of the router's access lists. If for any reason the investigator is only interested in the IPv4 access lists, he can use the command "display IP access lists" to retrieve only those lists.
- **show users:** Shows a list of all the users who are currently connected to the router.
- **show file systems:** Displays the many file systems that are accessible.
- **Show clock detail:** Shows the current time and date on the router's system.
- **Show version:** Displays information regarding the Cisco IOS software that has been loaded.
- **Show running config:** Shows the configuration that is presently being executed in RAM.
- **Show startup config:** Shows the configuration that was stored in the NVRAM.
- **Show ip route:** Displays the IPv4 routing table of the router.
- **show ip arp** : Displays the ARP table of the router, which maps IP addresses to MAC addresses
- **Show logging:** Shows the current condition of the system log and the contents of the standard logging buffer for the system.
- **Show ip interface:** Displays the current status of all IPv4 interfaces, and the investigator can add the "brief" option to acquire a summary of those interfaces' current status.
- **Show interfaces:** Displays information regarding all of the interfaces in the chassis or a single interface that you choose.
- **Show tcp brief all:** Displays the status of all endpoints using the hostname format required by the Domain Name System. Endpoints that are currently in the LISTEN state will not be displayed if the "all" option is not selected.
- **Show ip sockets:** Information about IP sockets is displayed.

4. RESULTS AND DISCUSSION

In this chapter, we'll show the forensic analysis of the different routers we talked about in the "scope" section. First, we're going to show you what the router can do. Second, we'll talk about the forensic evidence that was found using manual, logical, and hardware methods. Lastly, at the end of each method, we show the results in a table that sums up what has been found.

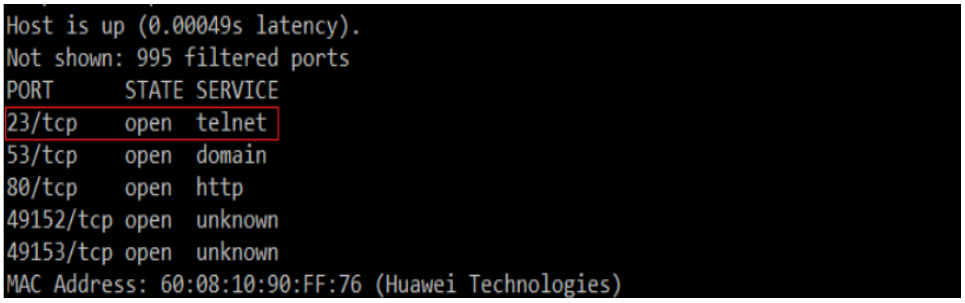
Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

4.1 Huawei WIFI AX3 Pro

Figure 6: HUAWEI WIFI AX3 Pro

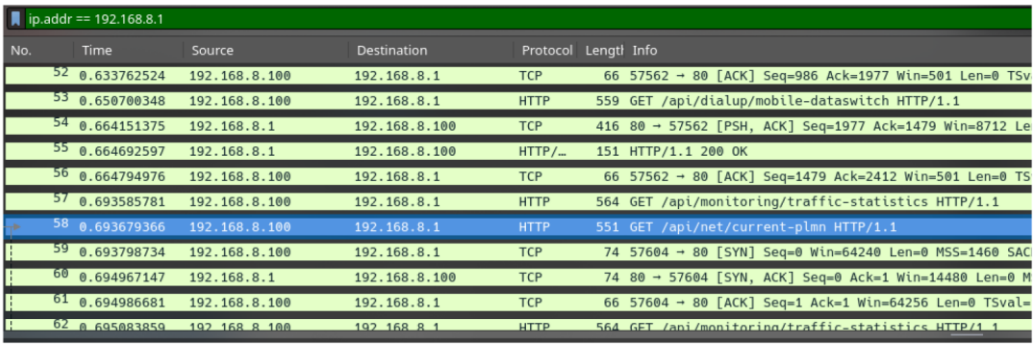
The specs that were found are not important for the investigation. The size of the memory (volatile and non-volatile), the operating system (OS), software versions, and other information would be a good place to start our investigation.

Figure 7: Result of NMAP scan on HUAWEI WiFi AX3 Pro



When we look at the interface, the router sends out traffic (also when we are not doing anything – an explanation can be found below). This Wireshark dump was taken from our host PC-A (192.168.8.100) when it was connected to the router's network (192.168.8.1) and the web interface was being used.

Figure 8: Wireshark dump of the HUAWEI WiFi AX3 Pro.

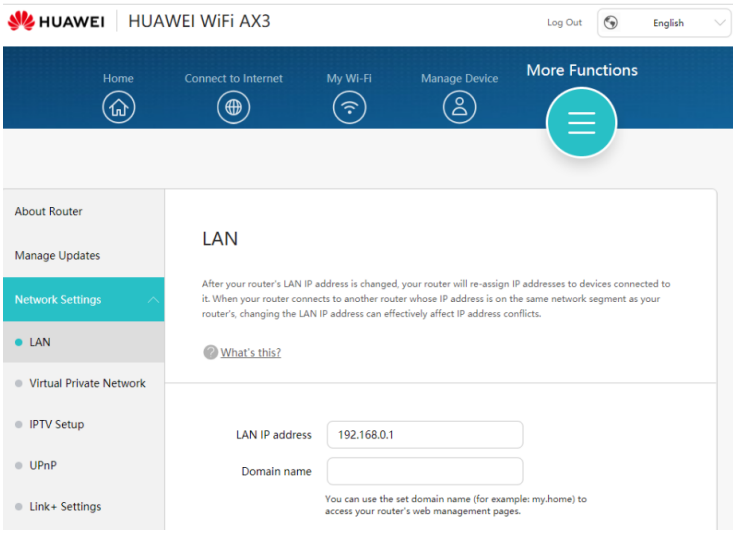


We noticed that the router (192.168.8.1) makes us (192.168.8.100) send the same requests about every 5 seconds. We made those requests so that we could update

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

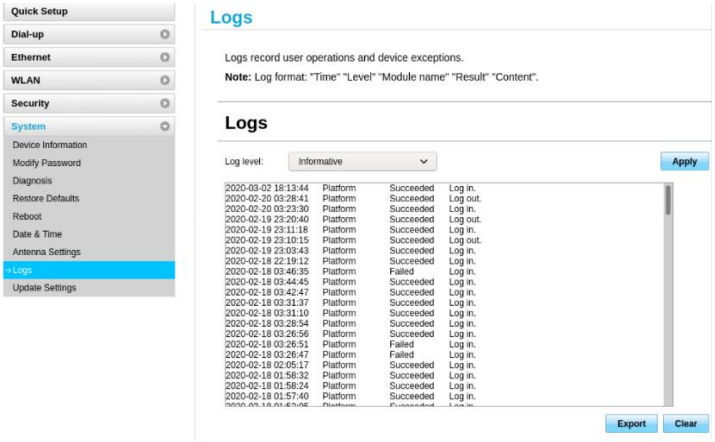
some information on the router, like how long our connection to the internet has been up.

Figure 9: Homepage of the HUAWEI WiFi AX3 Pro's web interface



On the first page, we can find out the ISP, how much data is being used, how long the router has been up, and how many people are connected.

Figure 10: Logs contained in the HUAWEI Wi-Fi AX3 Pro



We decided to see what these logs could do, and we found that sometimes a login isn't recorded when the session on a web page ends and the user reconnects. When you try to reconnect, you have to type in your username and password again.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

4.2 TP-Link ARCHER C7 AC1750

As for the HUAWEI WiFi AX3 Pro, those specs 1 are not important for forensics. In the next chapters, we'll show what we've learned right away. The results of TP-Link Archer C7 AC1750 Specifications manufacturers are shown in figure 11.

Figure 11: TP-Link Archer C7 AC1750– front side and backside

Before we can start to look into it, we need to know what services are running on the router so we can figure out what manual methods could be used.

Figure12: NMAP scan on TP-Link ARCHER C7 AC1750

```
Starting Nmap 5.00 ( http://nmap.org ) at 2012-11-27 03:30 IST
Interesting ports on 192.168.1.1:
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   closed telnet
25/tcp   closed smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv
MAC Address: BC:AE:C5:C3:16:93 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.58 seconds
```

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

Figure 13: DHCP system logs - TP-Link ARCHER C7 AC1750

Refresh Delete All

ID	Time	Type	Level	Log Content
9	2020-03-23 11:13:02	DHCPD	Notice	Send OFFER with ip 192.168.1.101
10	2020-03-23 11:13:02	DHCPD	Notice	Recv DISCOVER from 52:F9:A3:3F:25:D9
11	2020-03-23 10:53:15	DHCPD	Notice	Send ACK to 192.168.1.103
12	2020-03-23 10:53:14	DHCPD	Notice	Recv REQUEST from 44:85:00:A0:FD:DE
13	2020-03-23 10:53:14	DHCPD	Notice	Send OFFER with ip 192.168.1.103
14	2020-03-23 10:53:14	DHCPD	Notice	Recv DISCOVER from 44:85:00:A0:FD:DE
15	2020-03-23 10:52:30	DHCPD	Notice	Send ACK to 192.168.1.102
16	2020-03-23 10:52:30	DHCPD	Notice	Recv REQUEST from 18:5E:0F:82:2D:28

1 2 3 4 5 6 7 8 ... 25

Figure 14: Device information from backup file

RouterPassView - C:\Users\odin\Desktop\conf.bin

File Edit View Options Help

```
<?xml version="1.0"?>
<DslCpeConfig>
  <InternetGatewayDevice>
    <DeviceSummary val="InternetGatewayDevice:1.1[](Baseline:1, EthernetLAN:1)" />
    <LANDeviceNumberOfEntries val=1 />
    <DeviceInfo>
      <ManufacturerOUI val=CC32E5 />
      <SerialNumber val=CC32E5C6B33A />
      <HardwareVersion val="TL-MR6400 v4 00000002" />
      <SoftwareVersion val="1.10.0 0.9.1 v0001.0 Build 190521 Rel.38696n" />
      <UpTime val=279 />
      <X_TP_IsFD val=3 />
    </DeviceInfo>
```

4.3 Linksys EA7500

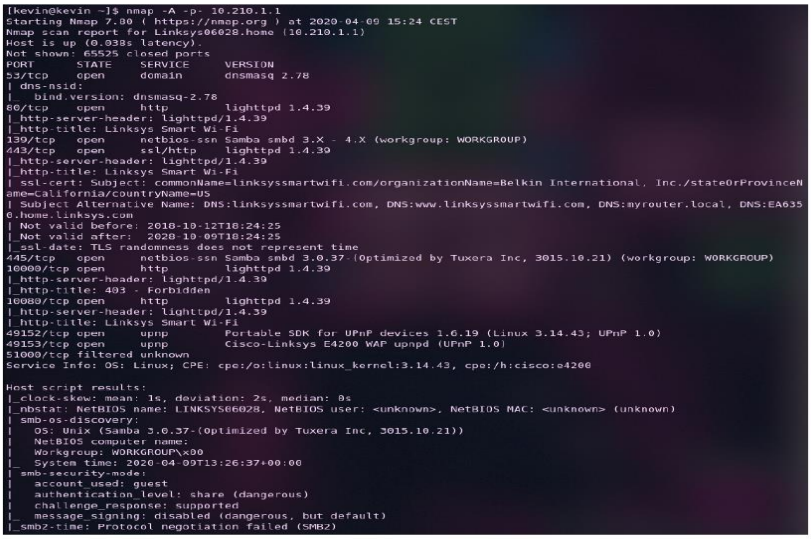
The specifications1 show that the SIM card properties are the same as the other two routers we looked at. As we've already said, the biggest difference between the Linksys EA7500 and the other two routers we looked at is that this one doesn't use 4G technology.

Figure 15: Linksys EA7500– front side and backside

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

We decided to see what these logs could do, and we found that sometimes a login isn't recorded when the session on a web page ends and the user reconnects.

Figure 16: NMAP scan result for Linksys EA7500



4.4 Result based on router vendor

Because of vendor-specific implementation, distributed routing infrastructures may have poor processing performance or even crash when subjected to the stress of routing dynamics. The results of collecting artifacts from various vendor router manufacturers are shown in table 2.

Table 2: Result based on router vendor

Vendor	Connectivity Accuracy (%)	Wi-Fi Password Cracking (%)	Gain Access to Admin Page (%)	Encryption bypass (%)	Forensic Artifacts Postmortem (%)	Forensic Artifacts Live (%)
Cisco	84	54	65	84	90	70
TP-Link	98	78	78	90	92	74
Huawei	94	93	80	94	95	80

4.5 Results based on WIFI-hacking tools

The 2.4 GHz and 5 GHz frequency bands are utilized by every wireless network to transmit and receive data. For the transmission of information or signals, this band has been further subdivided into multiple channels. Users experience slower speeds and a more sluggish overall Internet experience when these channels are congested with a high volume of traffic. The results of collecting artifacts from various vendor router manufacturers are shown in table 3.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

Table 3: Result based on WIFI-hacking tools

Vendor	Aircrack-ng	Kismet	Fern Wi-Fi Cracker	Wi-Fi te	Pixie WPS	Reaver	Wi-Fi te
Cisco	90	60	50	20	35	100	20
TP-Link	30	90	10	100	10	15	30
Huawei	100	10	50	25	35	40	10

4.6 Results based on password cracking tools

Usually, the decision to seize depends on what kind of investigation we are doing. The results of collecting artifacts from various vendor router manufacturers are shown in table 4. Since the seizure depends on other things, it is best if the router is left behind until all the needed information has been gathered on the scene.

Table 4: Result based on password cracking tools

Vendor	THC-Hydra	Hashcat	Pipal Password Analyzer	John the Ripper
Cisco	100	50	100	100
TP-Link	50	50	50	100
Huawei	100	100	50	100

4.7 Results based on protocols

A paper where they suggest a possible database of forensic artifacts that can be used as a point of reference will also be used to compare it to the stages of our flowchart. The results of collecting artifacts from various vendor router manufacturers are shown in table 5. As part of their research, they are making a database with a rating system for each piece of forensic evidence.

Table 5: Result based on protocols

Tools	Accuracy (%)	Wi-Fi Password Cracking	Gain Access to Admin Page	Encryption bypass	Forensic Artifacts
WEP	84.36%	Yes	No	No	Yes
WPA	95.0%	Yes	No	No	Yes
WPA2	98.39%	Yes	Yes	Yes	No
WPS	94.0%	Yes	Yes	No	Yes

4.8 Results based on forensic artifacts

If not, enough forensic artifacts were found without the administrator panel, the next step is to find the credentials to get into that panel, which is where most of the forensic artifacts are kept. For that, you only need to do a quick search online, since most companies list the default credentials on their websites. If you can't find it on the manufacturer's website, you can also look on the forums. The results of forensic artifacts from various vendor router manufacturers are shown in table 6. The results of forensic artifacts based on protocols of different vendor router manufacturers are shown in figure 55. Once the credentials are known, we have to connect to the router's management panel to start manually extracting forensic artifacts.

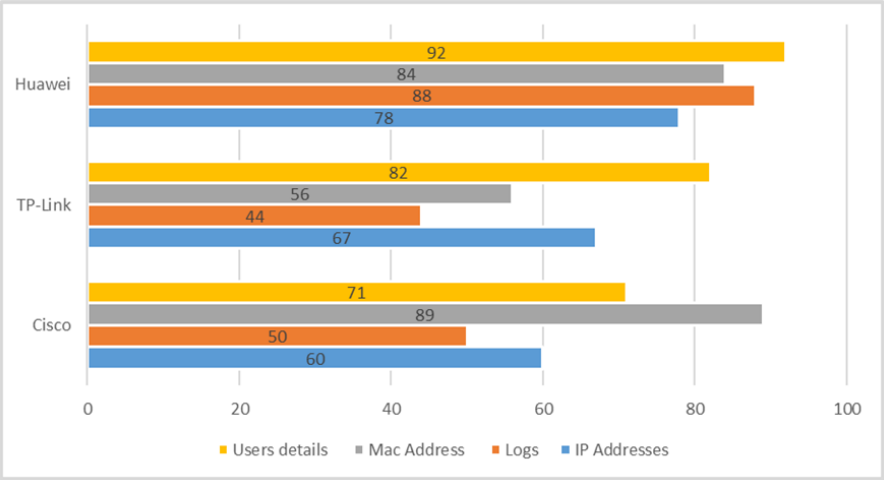
Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

Table 6: Result based on forensic artifacts

Vendor	IP Addresses (%)	Logs (%)	Mac Address (%)	Users details (%)
Cisco	60	50	89	71
TP-Link	67	44	56	82
Huawei	78	88	84	92

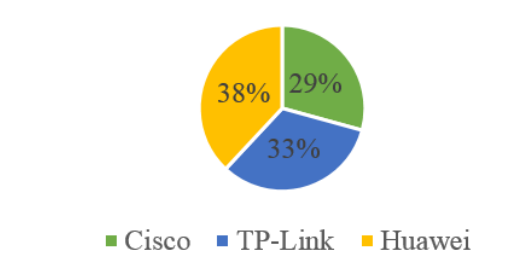
If not, enough forensic artifacts were found without the administrator panel, the next step is to find the credentials to get into that panel, which is where most of the forensic artifacts are kept.

Figure 17: Result based on forensic artifacts



If not, enough forensic artifacts were found without the administrator panel, the next step is to find the credentials to get into that panel. The results of IP addresses based on protocols of different vendor router manufacturers are shown in figure 56. Which is where most of the forensic artifacts are kept.

Figure 18: The success rate of IP Address artifacts from different vendor's routers

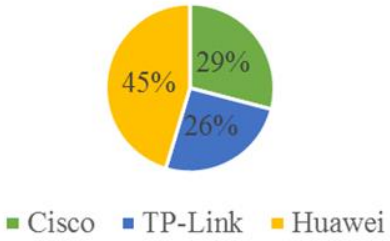


For that, you only need to do a quick search online, since most companies list the default credentials on their websites. If you can't find it on the manufacturer's website,

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

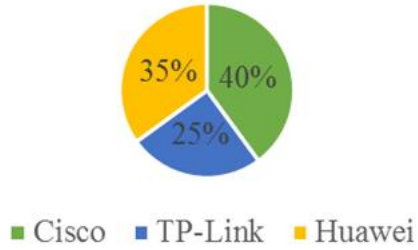
you can also look on the forums. The results of IP addresses based on logs of different vendor router manufacturers are shown in figure 19.

Figure 19: The success rate of logs artifacts from different vendor's routers



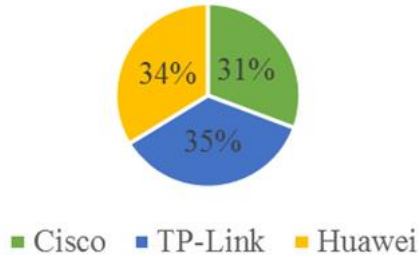
User detail, User IP, User Name, date, time, source and destination IP. Time of request, date of request, status code (web), Bytes of data sending and receiving. For that, you only need to do a quick search online, since most companies list the default credentials on their websites. The results of MAC address based on protocols of different vendor router manufacturers are shown in figure 58.

Figure 20: The success rate of Mac Address artifacts from different vendors' routers



Connecting to the network and typing in the IP address of the router in a browser is all it takes to make the connection. The passwords may have been changed. The results of IP address based on the rate of different vendor router manufacturers are shown in figure 59...

Figure 21: The success rate of Users details artifacts from different vendor's routers



Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

CONCLUSION

The field of digital forensics is vast. We choose to contribute to the field by analyzing routers because that sector is made up of so many different types and brands of equipment. The router is probably one of the first places to look for quick and effective triage at a crime scene. This makes it an important part of any digital investigation. When beginning an inquiry, a particular technique should be employed due to the significance of a router on the scene. It was clear from our research that by employing a live forensic approach using Raspberry PI and Kali Linux, we were able to retrieve details about the network topology (connected devices, IP addresses, MAC addresses, etc.) and other useful artifacts. Our research's main finding is that it will provide forensic analysts with a clear knowledge of the value of a live forensic technique. We also show how different vendors' tools and techniques, such as Huawei, Cisco, and TP-Link routers, can be used. So, our method can be used with many different router models and manufacturers, and it also lets analysts collect artifacts. This makes our research the basis for router forensics. The investigation revealed many areas where this activity might be strengthened going forward to have a greater impact. First, there is a staggering variety of routers available. A fascinating future project may be increasing the number of router devices to test them and find artifacts.

References

1. Chen, D. (2017, September). A Survey of IEEE 802.11 Protocols: Comparison and prospective. In 2017 5th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2017) (pp. 569-578). Atlantis Press.
2. Dalal, M., & Juneja, M. (2021). Steganography and Steganalysis (in digital forensics): a Cybersecurity guide. Multimedia Tools and Applications, 80(4), 5723-5771.
3. Cisar, P., & Pinter, R. (2019). Some ethical hacking possibilities in Kali Linux environment. Journal of Applied Technical and Educational Sciences, 9(4), 129-149.
4. Hamadi, A. (2019). Investigating vulnerabilities in a home network with Kali Linux.
5. Xiao, C., Bayer, K., Zheng, C., & Nayar, S. K. (2021, May). BackTrack: 2D Back-of-device Interaction through Front Touchscreen. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (pp. 1-8).
6. Aibekova, A., & Selvarajah, V. (2022, April). Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types. In 2022 IEEE International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-9). IEEE.
7. Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Mohammad, Q. H., & Alrabaee, S. (2020, April). Discovering public wi-fi vulnerabilities using raspberry pi and kali linux. In 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC) (pp. 1-4). IEEE.
8. Mirtskhulava, L., Globa, L., Meshveliani, N., & Gulua, N. (2019, September). Cryptanalysis of Internet of Things (IoT) Wireless Technology. In 2019 International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo) (pp. 1-4). IEEE.
9. Laaki, H., Miche, Y., & Tammi, K. (2019). Prototyping a digital twin for real time remote control over mobile networks: Application of remote surgery. Ieee Access, 7, 20325-20336.

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

10. Yaacoub, J. P. A., Noura, H. N., Salman, O., & Chehab, A. (2021). Digital forensics vs. Anti-digital forensics: Techniques, limitations and recommendations. arXiv preprint arXiv:2103.17028.
11. Dehury, C. (2021). Internet of Things and Edge Computing.
12. Ahmed, W., Shahzad, F., Javed, A. R., Iqbal, F., & Ali, L. (2021, April). Whatsapp network forensics: Discovering the ip addresses of suspects. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7). IEEE.
13. Easttom, C., & Adda, M. (2021, January). Application of the spectra of graphs in network forensics. In 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 0846-0852). IEEE.
14. Cresci, S., Lillo, F., Regoli, D., Tardelli, S., & Tesconi, M. (2019). Cashtag piggybacking: Uncovering spam and bot activity in stock microblogs on Twitter. ACM Transactions on the Web (TWEB), 13(2), 1-27.
15. Oughton, E. J., Kusuma, J., Peyronel, T., & Crowcroft, J. (2021). Wi-Fi Wardriving Studies Must Account for Important Statistical Issues. arXiv preprint arXiv:2101.06301.
16. Selvarathinam, N. S., Dhar, A. K., & Biswas, S. (2019, July). Evil twin attack detection using discrete event systems in IEEE 802.11 wi-fi networks. In 2019 27th Mediterranean Conference on Control and Automation (MED) (pp. 316-321). IEEE.
17. Lee, W. H., Liang, T. J., & Wang, H. C. (2022). An Innovative and Cost-Effective Traffic Information Collection Scheme Using the Wireless Sniffing Technique. Vehicles, 4(4), 996-1011.
18. Kostadinov, G., & Atanasova, T. (2019). Security policies for wireless and network infrastructure. Problems of Engineering Cybernetics and Robotics, 71, 14-19.
19. Bošnjak, L., & Brumen, B. (2020). Shoulder surfing experiments: A systematic literature review. Computers & Security, 99, 102023.
20. Davronbekov, D. A., Isroilov, J. D., & Akhmedov, B. I. (2019, November). Principle of organizing database identification on mobile devices by IMEI. In 2019 International Conference on Information Science and Communications Technologies (ICISCT) (pp. 1-5). IEEE.
21. Gentry, E., & Soltys, M. (2019). SEAKER: A mobile digital forensics triage device. Procedia computer science, 159, 1652-1661.
22. Mistry, N. R., & Dahiya, M. S. (2019). Signature based volatile memory forensics: a detection based approach for analyzing sophisticated cyber-attacks. International Journal of Information Technology, 11(3), 583-589.
23. Castelo Gómez, J. M., Roldán Gómez, J., Carrillo Mondéjar, J., & Martínez Martínez, J. L. (2019). Non-volatile memory forensic analysis in windows 10 iot core. Entropy, 21(12), 1141.
24. Balon, T., Herlopian, K., Baggili, I., & Grajeda-Mendez, C. (2021, August). Forensic Artifact Finder (ForensicAF): An Approach & Tool for Leveraging Crowd-Sourced Curated Forensic Artifacts. In The 16th International Conference on Availability, Reliability and Security (pp. 1-10).
25. Cambra Baseca, C., Sendra, S., Lloret, J., & Tomas, J. (2019). A smart decision system for digital farming. Agronomy, 9(5), 216.
26. Khalid Alabdulsalam, S., Duong, T. Q., Raymond Choo, K. K., & Le-Khac, N. A. (2022). An efficient IoT forensic approach for the evidence acquisition and analysis based on network link. Logic Journal of the IGPL.
27. Zhang, Y., Zhou, L., & Makris, Y. (2020). Hardware-based real-time workload forensics. IEEE Design & Test, 37(4), 52-58.

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

28. Asaad, R. R. (2021). Penetration testing: Wireless network attacks method on Kali Linux OS. Academic Journal of Nawroz University, 10(1), 7-12.
29. Ahmed, W., Shahzad, F., Javed, A. R., Iqbal, F., & Ali, L. (2021, April). Whatsapp network forensics: Discovering the ip addresses of suspects. In 2021 11th IFIP International Conference on New Technologies, Mobility and Security (NTMS) (pp. 1-7). IEEE.
30. Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Mohammad, Q. H., & Alrabaee, S. (2020, April). Discovering public wi-fi vulnerabilities using raspberry pi and kali linux. In 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC) (pp. 1-4). IEEE.
31. Al Neyadi, E., Al Shehhi, S., Al Shehhi, A., Al Hashimi, N., Mohammad, Q. H., & Alrabaee, S. (2020, April). Discovering public wi-fi vulnerabilities using raspberry pi and kali linux. In 2020 12th Annual Undergraduate Research Conference on Applied Computing (URC) (pp. 1-4). IEEE.
32. BouSaba, C., Kazar, T., & Pizio, W. C. (2016, June). Wireless network security using Raspberry Pi. In 2016 ASEE Annual Conference & Exposition.
33. Carranza, A., Mayorga, D., DeCusatis, C., & Rahemi, H. (2018, July). Comparison of wireless network penetration testing tools on desktops and raspberry Pi platforms. In Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology, Boca Raton, FL, USA (pp. 18-20).
34. Kalniņš, R., Puriņš, J., & Alksnis, G. (2017). Security evaluation of wireless network access points. Applied Computer Systems, 21(1), 38-45.
35. Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. Indonesian Journal of Electrical Engineering and Computer Science, 12(2), 729-737.
36. Gao, D., Lin, H., Li, Z., Qian, F., Chen, Q. A., Qian, Z., ... & Liu, Y. (2021, September). A nationwide census on wifi security threats: prevalence, riskiness, and the economics. In MobiCom (pp. 242-255).
37. Musthyala, H., & Reddy, P. N. (2021, May). Hacking wireless network credentials by performing phishing attack using Python Scripting. In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 248-253). IEEE.
38. Pimple, N., Salunke, T., Pawar, U., & Sangoi, J. (2020, March). Wireless security—an approach towards secured wi-fi connectivity. In 2020 6th international conference on advanced computing and communication systems (ICACCS) (pp. 872-876). IEEE.
39. Joshi, D., Dwivedi, V. V., & Pattani, K. M. (2017). De-Authentication attack on wireless network 802.11 i using Kali Linux. International Research Journal of Engineering and Technology (IRJET), 4, 1666-1669
40. Kissi, M. K., & Asante, M. (2020). Penetration testing of IEEE 802.11 encryption protocols using Kali Linux hacking tools. International Journal of Computer Applications, 975, 8887.
41. Aung, M. A. C., & Thant, K. P. (2017, June). Detection and mitigation of wireless link layer attacks. In 2017 IEEE 15th international conference on software engineering research, management and applications (SERA) (pp. 173-178). IEEE.
42. Amundsen, A. E., & Ovens, K. M. (2017, December). Forensics analysis of Wi-Fi communication traces in mobile devices. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 3632-3637). IEEE
43. Ijemaru, G., Adeyanju, I., Olusuyi, K., Ofusori, T., Ngharamike, E., & Sobowale, A. A. (2018). Security challenges of wireless communications networks: a survey. Int. J. Appl. Eng. Res, 13, 5680-5692.

ISSN：1671-5497
E-Publication Online Open Access
Vol: 41 Issue: 12-2022
DOI 10.17605/OSF.IO/RK4YF

44. Khalid, H.; Muhammad, I.; Abaid, U.; Muhammad, A.; Ahmed, A.; Adel, B.; Khalid, A. K-Banhatti Sombor Invariants of Certain Computer Networks. Computers, Materials & Continua 2022, 73, 15.

45. Hamid, K.; Iqbal, M.; Arif, E.; Mahmood, Y.; Khan, A.; Kama, N.; Azmi, A.; Ikram, A. K-Banhatti Invariants Empowered Topological Investigation of Bridge Networks. cmc 2022, 73, 5423.

46. K. Hamid, M. W. Iqbal, M. U. Ashraf, A. M. Alghamdi, A. A. Bahaddad et al., "Optimized evaluation of mobile base station by modern topological invariants," Computers, Materials & Continua, vol. 74, no.1, pp. 363–378, 2023

47. K. Hamid, M. W. Iqbal, M. U. Ashraf, A. A. Gardezi, S. Ahmad et al., "Intelligent systems and photovoltaic cells empowered topologically by sudoku networks," Computers, Materials & Continua, vol. 74, no.2, pp. 4221–4238, 2023.

48. A. M. Alghamdi, K. Hamid, M. W. Iqbal, M. Usman Ashraf, A. Alshahrani et al., "Topological evaluation of certain computer networks by contraharmonic-quadratic indices," Computers, Materials & Continua, vol. 74, no.2, pp. 3795–3810, 2023.

49. K. Hamid, M. W. Iqbal, H. A. B. Muhammad, Z. Fuzail, Z. T. Ghafoor et al., “Usability evaluation of mobile banking applications in digital business as emerging economy,” International Journal of Computer Science & Network Security, vol. 22, no. 1, pp. 250–260, 2022.

50. Turnbull, B., & Slay, J. (2008, March). Wi-Fi network signals as a source of digital evidence: Wireless network forensics. In 2008 Third International Conference on Availability, Reliability and Security (pp. 1355-1360). IEEE.

51. Astuti, Y., Aspriyono, H., & Zulfiandry, R. (2021). Analysis of Wifi Network Security with Packet Sniffing Technique at RRI Bengkulu Public Broadcasting Institution. GATOTKACA Journal (Teknik Sipil, Informatika, Mesin dan Arsitektur), 2(2), 163-172.

52. Zaklouta, A. (2019). High-Speed Communication Scheme in OSI Layer 2 Research and Implementation.

53. Gupta, S., Mohan, N., & Kaushal, P. (2021). Passive image forensics using universal techniques: a review. Artificial Intelligence Review, 1-51.

54. Pigaiani, N., Bertaso, A., De Palo, E. F., Bortolotti, F., & Tagliaro, F. (2020). Vitreous humor endogenous compounds analysis for post-mortem forensic investigation. Forensic science international, 310, 110235.

55. Fikriyadi, F., Ritzkal, R., & Prakosa, B. A. (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. Jurnal Mantik, 4(3), 1658-1662.

56. Zaidan, D. T. (2021). Analyzing Attacking methods on Wi-Fi wireless networks pertaining (WEP, WPA-WPA2) security protocols. Periodicals of Engineering and Natural Sciences (PEN), 9(4), 1093-1101.