

GROUP ASSIGNMENT
Introduction to Security Technologies
CT105-3-1-IST
APU1F1911

INSTRUCTIONS TO CANDIDATES:

- 1 Submit your assignment at the administrative counter.**
- 2 Students are advised to underpin their answers with the use of references (cited using the Harvard Name System of Referencing).**
- 3 Late submission will be awarded zero (0) unless Extenuating Circumstances (EC) are upheld.**
- 4 Cases of plagiarism will be penalized.**
- 5 The assignment should be bound in an appropriate style (comb bound or stapled).**
- 6 Where the assignment should be submitted in both hardcopy and softcopy, the softcopy of the written assignment and source code (where appropriate) should be on a CD in an envelope / CD cover and attached to the hardcopy.**
- 7 You must obtain 50% overall to pass this module**

Table of Contents

<u>1.0 Introduction.....</u>	<u>3</u>
<u>2.0 Threat Intelligence</u>	<u>4</u>
<u>2.1 What Is Threat Intelligence?.....</u>	<u>4</u>
<u>2.2 Why Is Threat Intelligence Important?.....</u>	<u>4</u>
<u>2.3 Types of Threat Intelligence.....</u>	<u>6</u>
<u>2.4 The Threat Intelligence Lifecycle.....</u>	<u>7</u>
<u>3.0 Managed security service provider (MSSP).....</u>	<u>9</u>
<u>3.1 Benefits of Hiring a Managed Security Service Provide.....</u>	<u>9</u>
<u>3.2 Reasons to Use Managed Security Services.....</u>	<u>9</u>
<u>3.3 what managed security service providers are used for?.....</u>	<u>10</u>
<u>3.4 Cost Effectiveness.....</u>	<u>11</u>
<u>3.5 SecureWorks.....</u>	<u>11</u>
<u>4.0 Individual.....</u>	<u>12</u>
<u>4.1 Fern Wi-Fi Cracker.....</u>	<u>12</u>
<u>4.2 Wireshark.....</u>	<u>18</u>
<u>4.3Nmap.....</u>	<u>28</u>
<u>5.0 References.....</u>	<u>32</u>

Introduction

In 2.0, There is Detailed research about Threat intelligence, that what is threat intelligence and why is it important, what are the types of it and its life cycle in that its six steps are explained that how data is gathered, how planning is done, how its analysed and how the care is taken of data to use it another time to keep its life cycle continuity.

Then there is 3.0, its about Managed security service provider (MSSP).

That, what is MSSP, what are the Benefits of Hiring a Managed Security Service Provider, Reasons to Use Managed Security Services and what managed security service providers are used for? Is it Cost Effectiveness or not and then finally and example of a company named SecureWorks?

In Individual part it's explained about three different tools by each team, tools: Fern Wi-Fi cracker that how is it used to crack Wi-Fi security through different methods, then Metasploit and Nmap also know Network Mapper; about their functionalities that how they work, why to use them and how to use them.

2.0 Threat Intelligence

2.1 What Is Threat Intelligence?

Threat intelligence is information that can deter or minimize cyber-attacks. Threat analysis provides you with information that helps make informed decisions about your security by answering some questions such as who targets you, what their motives and skills are, and what vulnerability measures you need to look for in your networks. According to Pokorny (2019), Gartner mentioned that threat intelligence is evidence focused on facts, including context, processes, metrics, consequences and action-oriented recommendations regarding a current or evolving danger or hazard to properties. This intelligence may be used to advise decisions about the reaction of the individual to the danger or hazard. The best intelligence systems use machine learning to simplify data collection and analysis, combine with the current solutions, add unstructured data from multiple sources, and then link the dots by presenting information on threat actors' vulnerability indicators (IOCs) and strategies, methods, and procedures (TTPs). Threat intelligence also divides into three subcategories which are strategic, tactical and operational. Strategic means that usually broader developments are intended for non-technical audiences while tactical is outlines of the threat actors' strategies, methods and processes for a more informed audience and Operational means that technical information about targeted attacks and campaigns.

2.2 Why Is Threat Intelligence Important?

According to Pokorny (2019), Recorded Future mentioned that they are motivated by three core beliefs to do their work which is threat intelligence is only helpful because it provides you with the information you need to make rational choices and respond. Today, the cybersecurity industry is experiencing various challenges which are increasingly active and devious threat actors, waves of useless data and false alarms through numerous, unconnected security technologies, and a large ability deficit. Some companies seek to integrate hazard data streams into their network but don't know what to do with all the extra info, adding to the workload of analysts who do not have the resources to determine what to analyse and what to ignore. Threat intelligence needs to be actionable; they need to be accurate and deliver in a way that those receiving it would understand. Another way that threat analysis is more actionable is because it combines seamlessly with all the already existing defence tools in the system. Recorded browser extension of Future, for instance, adds on top of all web-based security tools to offer

quick access to information such as vulnerability ratings, CVEs, signatures, domains and IP addresses right on the website.

The second belief is threat intelligence is for everyone. No matter what security position you work for, your job can be enhanced by threat intelligence. It's not a particular intelligence area intended just for expert researchers; it's the framework that brings meaning to all security operations in all sizes of organizations. The background that threat intelligence offers derives from network procedures, emergency response, vulnerability detection, malware prevention, risk assessment, and high-level compliance preparation and decision-making. However, to get those advantages without contributing to the workload, threat analysis has to be combined with the technologies and workflows on which you already rely and have low entry barriers. When viewed as a separate function within a larger defence framework rather than an integral aspect that enhances all other roles, the effect is that when they need it, many of the individuals who will profit significantly from the information of threats will not have access to it. Security operations departments will never keep up with all the warnings they receive; threat intelligence helps organize and process notifications and other risks automatically. Vulnerability management teams can accentuate the most critical vulnerabilities by leveraging vulnerability analysis to assess which weaknesses become the highest potential risk environment threats. Yet avoidance of theft, risk identification, and other high-level monitoring mechanisms are strengthened by crucial insights into threat actors and their strategies, methods, and procedures.

The third belief is people and machines can work better together. Computers can process and categorize raw data faster than humans at speeds orders of magnitude. On the other hand, people can conduct logical, large-picture analyses even more efficiently than any artificial intelligence, but only if they are not involved in tedious analysis and analysing vast quantities of data. When the two are partnered together, each function more intelligently, saving time and energy, cutting burnout, and enhancing overall efficiency.

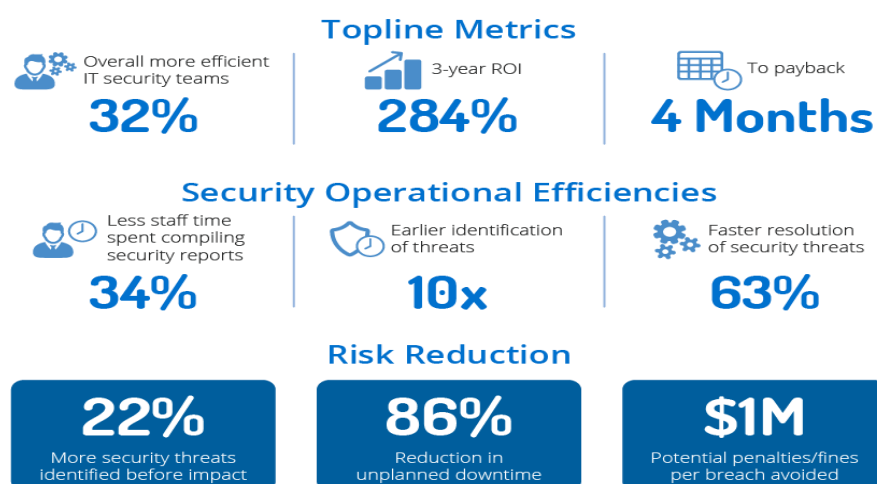


Fig :1.1

2.3 Types of Threat Intelligence

As explained above Threat intelligence divides into three subcategories which are strategic, tactical and operational.

Strategic threat intelligence: It is about broader developments are intended for non-technical audiences, top decisions made by officials and other executives of an organization, the content is usually less technical and is presented through reports or briefings for example: News from local and national media and Policy documents from nation-states. Good strategic intelligence provides key-insight into risk related areas, broad patterns in threat actor targets and tactics.

Tactical threat intelligence: tactical is outlines of the threat actors' strategies, methods and processes for a more informed audience How their organization could be attacked and ways to defend it against those attacks and mitigate them, reports about the attack vectors, tools, and infrastructure that attackers are using, including specifics about what vulnerabilities are being targeted and what exploits attackers, are leveraging, as well as what tools and strategies they use to avoid and delay detection of attack.

Operational intelligence is knowledge about cyberattacks, events, or campaigns. It gives specific understanding and insights to comprehend incident response teams understand the intent, nature, and timing of an attacks. What attack vector is being used, what vulnerabilities are being exploited, or what command and control domains are being employed. Consequently, there are a few barriers to gathering this kind of intelligence:

- **Access** — Threat teams communicate over encrypted and private channels, or may require proof of identity. There are also language problems with threat groups situated in countries.
- **Noise** — It can be tough and impossible to manually collect good intelligence from huge volume-based sources like social media and chat rooms.
- **Obfuscation** — To evade exposure, threat groups might setup obfuscation tactics as codenames.

2.4 The Threat Intelligence Lifecycle

Threat intelligence is a complete product that formed of a six-part cycle of data collection, processing, and analysis.

2.4.1. Planning and Direction

To produce actionable threat intelligence is to ask the correct question.

Actionable threat intelligence emphasis on an event, fact, or activity — strategic type of threat intelligence as broad, open-ended questions should be avoided.

Arrange your intelligence objectives formed on aspects like how closely they observe to your organization's core values, how large impact the resulting conclusion will have, and how time-sensitive the decision is.

One important guiding factor at this stage is understanding who will consume and benefit from the finished product — will the intelligence go to a team of analysts with technical expertise who need a quick report on a new exploit, or to an executive that's looking for a broad overview of trends to inform their security investment decisions for the next quarter?

2.4.2. Collection

The next step is to gather raw data that fulfills the requirements set in the first stage. It's best to collect data from a wide range of sources — internal ones like network event logs and records of past incident responses, and external ones from the open web, the dark web, and technical sources.

Threat data is usually thought of as lists of IoCs, such as malicious IP addresses, domains, and file hashes, but it can also include vulnerability information, such as the personally identifiable information of customers, raw code from paste sites, and text from news sources or social media.

2.4.3. Processing

After the raw data is collected, you need to analyse it, forming it with metadata tags and filtering out unnecessary and redundant data or negatives and false positives.

Today, even small system collect data on the demand of millions of log proceedings and hundreds of thousands of pointers every day. It's too much for human analysts to analyse and process it competently — the information gathering and processing should to be automatic to make sense of it.

Solutions like SIEMs are good to start with for the reason that they make it comparatively easy to assemble data with correlation rules that can be establish for a few diverse use cases, but they can only take in a limited number of data types.

If you're collecting unstructured data from many different internal and external sources, you'll need a more robust solution. Recorded Future uses machine learning and natural language processing to parse text from millions of unstructured documents across seven different languages and classify them using language-independent ontologies and events, permitting analysts to do powerful and instinctive searches that go beyond simple keywords and simple association rules.

2.4.4. Analysis

The next step is to make sense of the processed data. The goal of the analysis is to search for potential security issues and notify the relevant teams in a format that fulfils the intelligence requirements outlined in the planning and direction stage.

Threat intelligence can take numerous procedures steps depending on the main objectives and the intended audience, but the idea is to get the information of data into a format that the audience will comprehend. This can vary from basic threat lists to peer-reviewed reports.

2.4.5. Dissemination

The final product is then dispersed to its intended consumers. For threat intelligence to be actionable.

It also needs to be traced so that there is continuity and link between the intelligence cycles and the analysis and data is not lost. Use ticketing systems that join in with security systems to trace each stage of the intelligence cycle — tickets can be submitted when every time there is an intelligence request, written up, reviewed, and fulfilled by multiple people across diverse teams, all in one time.

2.4.6. Feedback

The last step is when the intelligence cycle is full circle, making it thoroughly connected to the initial planning and direction phase. After receiving the finished intelligence product, whoever made the initial request reviews it and determines whether their questions were answered. This automates the objectives and procedures of the next intelligence cycle, while making documentation and continuousness critical.

3.0 Managed security service provider (MSSP)

Managed security service provider (MSSP) is an organization or a company that provides security service; It's a network security service provides outsourced monitoring and management of security devices and systems. Most of the services consist of intrusion detection, virtual private network, managed firewall, anti-viral services and vulnerability scanning. MSSPs practice high-availability security function centres (either from their own facilities or from other data centre providers) to supply 24/7 services planned to leverage the amount of operational security staffs an enterprise must hire, train and retain to manage a suitable security stance.

3.1 Benefits of Hiring a Managed Security Service Provider

The primary advantage of managed security services is that the security expertise and extra staffing they supply. The ability for MSSPs to accomplish security procedures from an off-site location permits enterprises to have business as was as usual with minimal intrusion due to security initiatives, on other hand the MSSP interface maintains a continuing line of communication and seamless reporting to the business. MSSPs make sure that enterprise it's always up-to-date with the status of security issues, audits, and maintenance, enabling the hiring organization to specialise in security governance instead of administrative tasks.

There are a good range of security services being offered by MSSPs today, from full outsourcing of security programs to specialized services that specialise in a selected component of the enterprise's security (data protection, threat monitoring, regulatory compliance, management of network security tools and incident response and forensics). By subcontracting security, enterprises usually realize cost effecting by eradicating the requirement to take care of an entirely staffed, full-time, on-site IT department. Many corporations also claim MSSPs for quicker procedure times and better time-to-value on security capitals.

3.2 Reasons to Use Managed Security Services

Despite an increasing awareness of the necessity for proactive security measures, many enterprises still postpone implementing sound security initiatives until they've suffered a loss as a result of a data breach. The number of cyber threats is growing, and it's crucial that enterprises prioritize IT security as a result. Whether a corporation is deficient in security

program improvement or just wants to increase their security aptitudes, managed Security Service providers are an appreciated and valued option because:

- Managed security services offer continuous oversight, 24 hours a day, 7 days a week, and 365 days a year. Choosing to handle enterprise security in-house, without the assistance of an outsourced vendor, requires an outsized investment in manpower and technology.
- Cyber-attacks grow at an extremely fast pace, showing threat after another. Without the right security tools and resources, maintaining with evolving threats, addressing threats as they arise, and recovering from incidents detected too late can consume substantial resources.
- MSSPs have many operations through the world, and their attention on monitoring the threat site means they most of time have a distinct benefit over enterprises with an essential business function unrelated to security and technology. In other words, MSSPs focus on initial threat detection and protection, so conscripting the services of an MSSP ensures the enterprise to specialise in basic business activities while forgetting security concerns to the experts. Some of the opposite major advantages to enlisting the help of an MSSP is that these vendors can conduct vulnerability and penetration testing, perform security scans routinely, and lookout of other security supervision functions for the enterprise, freeing up enterprise IT to shift their attention to security program lapse and different activities that advance enterprise goals.

3.3 what managed security service providers are used for?

Companies can outsource to MSSPs any or all aspects of their IT security functions. MSSPs are usually responsible for some degree of continuous safety monitoring, risk evaluation, information on threats and control of intrusions. Organizations prefer to work with MSSPs for a spread of reasons; often this decision is driven by a scarcity of in-house resources or expertise surely areas of security or the need for security management and monitoring other than of usual working hours. In other cases, organizations will hire managed Security Service providers to conduct security audits or answer and investigate incidents. Some MSSPs offer services to support organizations in regulated industries that has got to meet

compliance requirements, like the insurance Portability and Accountability Act (HIPAA) or Europe's General Data Protection Regulation (GDPR).

3.4 Cost Effectiveness

In some cases, an organization will save money when working with the managed security service provider. Acquiring in-house cyber security personnel, for example, can be costly, so it can be cost-effective to work with an MSSP. An MSSP can also make savings on supplies, software tools and other operating costs for organizations.

3.5 SecureWorks

SecureWorks is an MSSP based in USA that provides cybersecurity solutions. The company combines machine learning with human intelligence to detect and respond threats faster and prevent attacks altogether (secureworks.com)

The company offers their services such as:

1. Managed Detection and Response - The team detects and responds to threats quickly through the use of embedded proprietary threat intelligence to automatically correlate endpoint, network and cloud activity and plan their course of action. Also, through machine learning datasets which are constantly updated, they find unknown threats.
2. Managed Security-
3. Incident Response
4. Adversarial Security Testing
5. Security Consulting
6. Threat Intelligence

4.0 Individual

4.1 Fern Wi-Fi Cracker

Fern Wi-Fi Cracker is a software that uses the Python Program Language as a wireless security audit system and an attack software application, which helps you to crack and retrieve WEP, WPA, and WPS keys as well as other network-based wireless or Ethernet network attacks. (kali tools, 2020)

Fern Wi-Fi Cracker currently supports the following features:

- WEP Cracking with Fragmentation, Chop-Chop, Caffè-Latte, Hirte, ARP Request Replay or WPS attack
- WPA/WPA2 Cracking with Dictionary or WPS based attacks
- Automatic saving of key in database on successful crack
- Automatic Access Point Attack System
- Session Hijacking (Passive and Ethernet Modes)
- Access Point MAC Address Geo Location Tracking
- Internal MITM Engine
- Brute force Attacks (HTTP, HTTPS, TELNET, FTP)
- Update Support

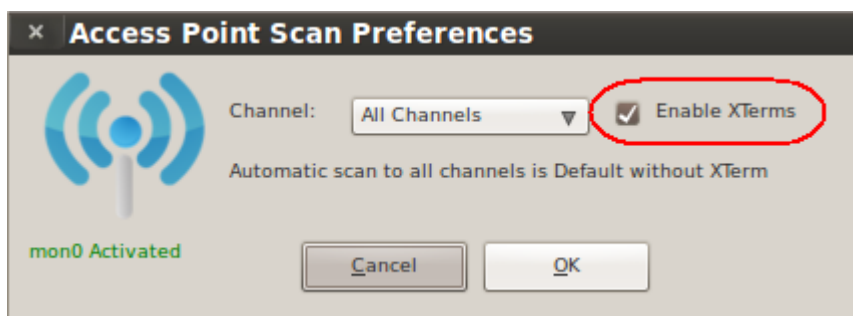
4.1.1 Introduction:

This is a step by step on how to

We need to bring up the Access Point Preferences screen. There we can set the channel option to either scan a single channel or multiple channels by default.

A useful feature is checking the Enable XTerms box, by ticking it we can open up the Terminal Windows to view the usage and see how it's running in the background.

We need to click OK after it is done



Back on the Fern home screen click the Scan for Access points button.

On the home screen of Fern, access points need to be scanned by clicking the following button



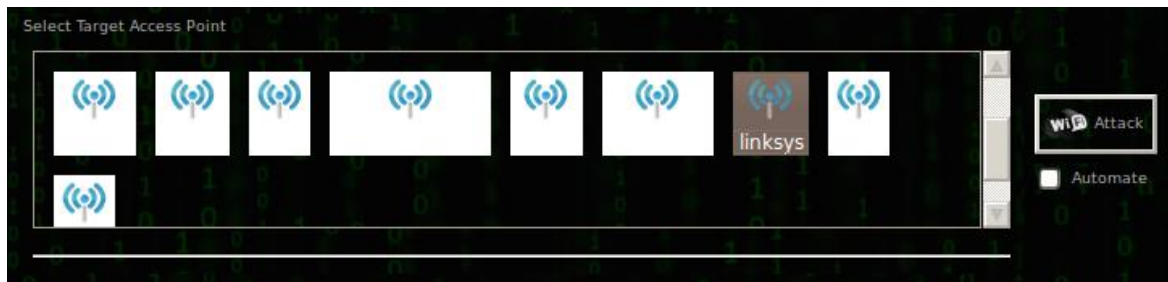
The WEP-compatible networks (no screen shot) are shown and the WPA-cabled networks are shown on two terminals. The top portion of the window displays the networks identified and any associated customer devices are on the bottom of the search terminal display. A linked client is required to execute a WPA attack. Once the customer re-authenticates to the Network, the most critical aspect of the attack can set off the wireless network and catch the 4-way handshake. You don't have a linked client in the network you want to pentest!

FERN (WPA SCAN)										
CH 6][Elapsed: 1 min][2013-07-01 19:14										
BSSID	PWR	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:25:9C:19:78:41	-24	100	7	0	6	54	WPA	TKIP	PSK	linksys
	-33	63	0	0	6	54e	WPA2	CCMP		
	-60	39	0	0	1	54e	WPA2	CCMP		
	-66	23	0	0	1	54	WPA2	CCMP		
	-64	29	4	0	6	54	WPA	TKIP		
	-70	9	0	0	7	54	WPA2	CCMP		
	-71	21	0	0	6	54	WPA2	CCMP		
	-71	8	0	0	4	54e	WPA2	CCMP		
	-71	12	0	0	10	54	WPA2	CCMP		
	-71	17	0	0	10	54e	WPA2	CCMP		
	-71	12	0	0	2	54e	WPA2	CCMP		
	-71	7	0	0	11	54e	WPA2	TKIP		
	-72	2	0	0	6	54e	WPA2	CCMP		
BSSID	STATION		PWR	Rate	Lost	Frames	Probe			
00:25:9C:19:78:41	00:26:82:		-15	0 -54	0	1				
			-1	1e- 0	0	1				
			-36	1e- 1	0	5				
			-64	0 - 1	0	1				
			-62	0 - 6	0	2				

On the home screen the detected networks will be popping up next to the WIFI WEP or WIFI WPA buttons



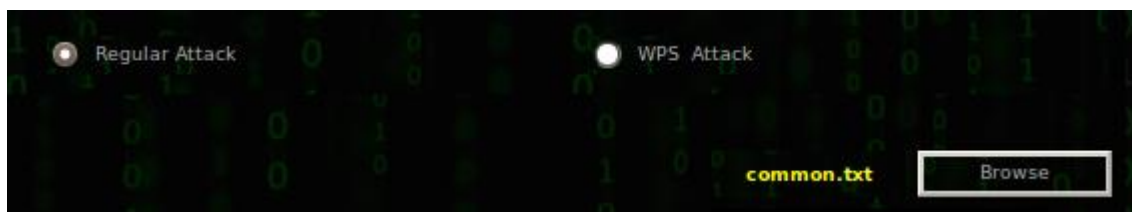
Clicking on the WIFI WEP or WPA button brings up the Attack screen along with the networks found. We need to select the AP to crack.



I will use the Regular Attack option, but there is a WPS Attack option and I believe Fern uses the Reaver utility to launch the WPS attack.

Usually the Regular attack option is used and this will be shown here. There is an additional WPS attack option which uses the 'Reaver' utility to launch the WPS attack.

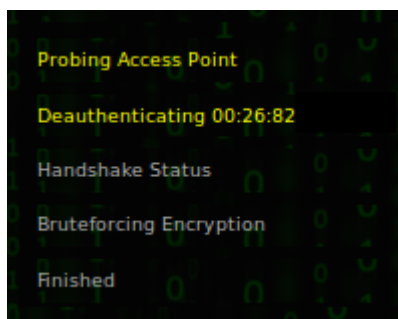
Common.txt is the wordlist provided by the Fern program but any wordlist downloaded or generated by yourself can be used when you click the browser button to point Fern to the file with the alternative wordlist.



With the Regular Attack and the wordlist selected we need to click the Attack button.



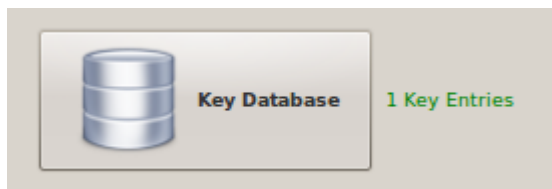
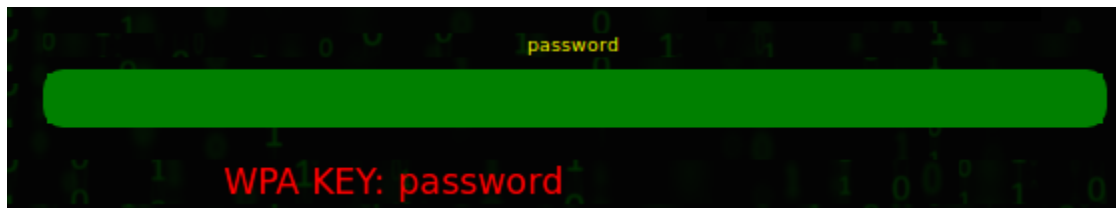
Fern will start the attack and on the left side of the screen the attack steps will turn yellow as Fern works through the various steps. The most important step is capturing the 4-way handshake and Fern will open an aireplay-ng Terminal window showing the progress of DE authentication (if XTerms is checked in the preferences) of the connected client.



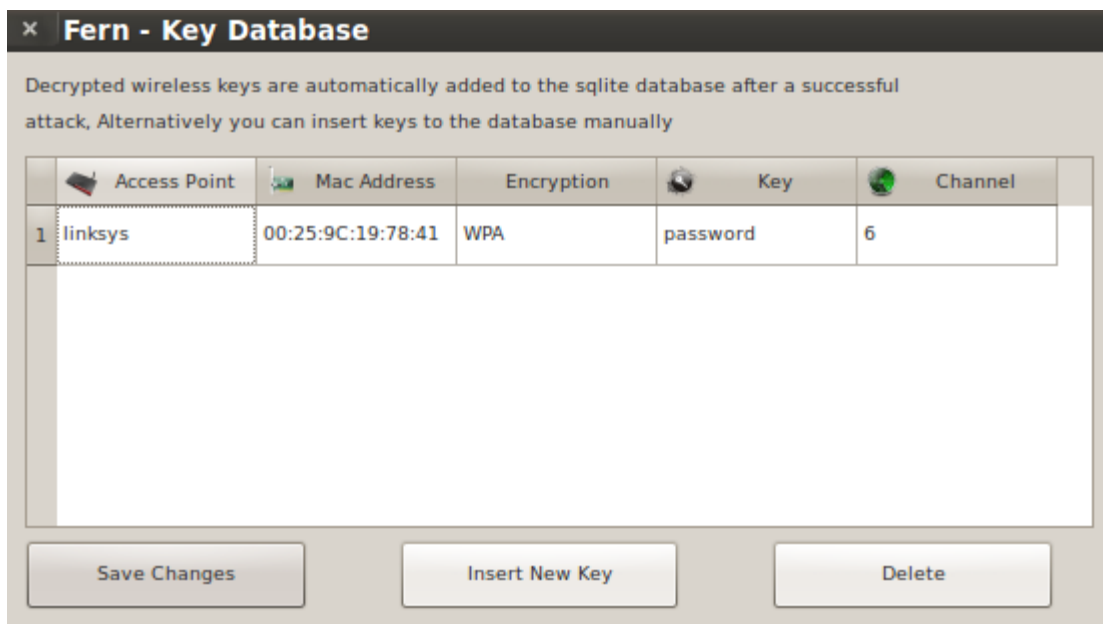
It may take several attempts to capture the 4-way handshake.

```
^ v x aireplay-ng
19:18:29 Waiting for beacon frame (BSSID: 00:25:9C:19:78:41) on channel 6
19:18:30 Sending 64 directed DeAuth. STMAC: [00:26:82: [15/18 ACKs]
19:18:30 Sending 64 directed DeAuth. STMAC: [00:26:82: [ 3/ 7 ACKs]
```

The brute force attack will start once fern has captured the handshake and if the WPA key in the wordlist is being used it will display the found key in Red.



The key database button will display the found keys



4.1.2 Other Features:

Fern WIFI Cracker contains a key database where it saves keys from networks that have been previously hacked.

Wireless networks and vulnerabilities

Wireless networks with poor security are often targeted by organized crime groups and cybercriminals. The attacks can be quite successful. Access to the business network can permit ransomware to be installed and the number of customers of tens or hundreds of thousands of credit / debit cards can be stolen if malware can be installed on POS systems. (web titan, 2018)

Many Businesses are Neglecting Wi-Fi Security

Several businesses have changed their protection roles from wired to wireless technologies. Wired networks typically have much simpler protections for wireless networks, which also contributes to flaws in poor implementation. A comprehensive risk analysis is often not conducted by many organizations, which does not recognize and fix such vulnerabilities. Wireless network attacks are popular due to these security vulnerabilities and the ease of which they are used.

Use of Default SSIDs and Passwords

Wi-Fi access points have a standard SSID and password to modify, but the default passwords are too often left in place. It makes connecting and manipulating the router, modifying settings or firmware, loading malicious scripts, or even modifying the DNS server simpler for an attacker, so that all traffic is sent to an IP of the attacker.

Placing an Access Point Where Tampering Can Occur

If the access point is located where it can be reached physically, it can be falsified. The connection point to factory default settings takes only seconds. Ensure that the access point is in a protected spot, for example a locked closet.

Use of Vulnerable WEP Protocol

The first protocol used to encrypt wireless traffic was the Wired Analog Privacy (WEP) protocol. WEP is intended to make wireless networking as secure as its wired equivalent, as its name suggests, but that doesn't protect WEP wireless networks.

WEP is based on the secure RC4 cypher. WEP makes the re-use of an initialization vector and keys are never a good idea to re-use them. It helps an intruder to quickly break encryption. In WEP, a variety of other flaws have been identified that do not make it secure.

Net Spectre – Remote Spectre Exploit

Spectre is a vulnerability that affects branch prediction microprocessors. It is possible to exploit the vulnerability to give an attacker access to selected virtual memory places to get sensitive data. To make use of this flaw, an attacker would first convince a user to upload and execute

malicious code or visit a website where JavaScript executes in the browser. Fortunately, the attack—called NetSpectre—is complex, so that an organization can be attacked much easier. There is also a low chance of abuse.

4.1.3 conclusion

It is easier to hack with utilities like Fern using a passphrase with a WPA or WPA2 passphrase. The Fern software is free for download and easy to use, and it is not used for legal wireless purposes by anyone.

With a WPA key an individual may enter the network and have an internet gateway or start other attacks. For example, the WPA key may be used to extend the attack to include data traffic decryption of legitimate customers on the wireless network

4.2 Wireshark

According to Porup (2018), Wireshark is the network traffic analyzer in the world, and an important resource for any qualified security or system administrator. This free software will help us to track network traffic in real time, and is always the best tool on our network for troubleshooting issues. Common problems that Wireshark can assist with troubleshooting include lost packets, latency problems and malicious network activities. It helps you to monitor the network traffic and offers filtering and digging tools into the traffic, zooming into the root cause of the problem. Administrators use it to detect unreliable network equipment that lose packets, problems with latency created by machines transmitting traffic halfway around the world, and attempts to exfiltrate data or even hack the company. Wireshark is a versatile software that requires solid understanding of the fundamentals of networking. To most commercial enterprises, this requires, to example, learning the TCP / IP stack, how to read and view packet headers and how routing, port forwarding, and DHCP function.

4.2.1 What does Wireshark do?

Wireshark intercepts traffic and transforms the binary data to a readable format for users. It makes it easier to distinguish which traffic crosses the network, how much of it, how much, how often delay there is between certain hops, and so on. Although Wireshark embraces more than two thousand network protocols, many of which are esoteric, rare, or obsolete, the average security specialist can find the most important utility in examining IP packets. Most of the

products on your network are typically TCP, UDP, and ICMP. Given the vast amount of traffic that flows across a normal business network, Wireshark's software to help you process the data makes it especially useful. Catch filters can only capture the types of traffic that you're interested in and view filters can help you zoom in on the traffic that you choose to review. To make it easier to find what you're searching for, the network protocol analyzer offers search methods including standard expressions and colored highlighting. The best way to find anomalous traffic is sometimes to capture everything and establish a baseline (Porup, 2018).

4.2.2 History of Wireshark

Porup (2018) stated that Wireshark's been going since 1998, when Gerald Combs invented it and named it Ethereal. It has provided tremendous amounts of user support and updates over the years and is generally regarded as the de facto network protocol analyzer usable today. Wireshark runs on both major and minor operating systems including popular Linux distros, Windows, OS X, OpenBSD, NetBSD, and FreeBSD. The system is free software, GPL licensed, and is thus free to download, distribute, and change.

4.2.3 Wireshark as a learning tool

Wireshark has so many hands-on applications that it's possible to forget what an important learning resource it can be. Lifting a car's hood is the perfect way to explain how an internal combustion engine functions, as well as raising the network traffic cover and watching packets pass through and diving down to the byte level and analyzing TCP headers is a great way to experience and show someone how the internet operates. Demystifying the engine operating our digital system will only lead to more educated corporate choices and smarter policy strategies, not to mention a more qualified workforce. Wireshark is also a staple to classroom curricula in many training environments, but at this stage the documents are sufficiently complete to enable a knowledgeable learner to quickly download the network protocol analyzer, sniff their local Wi-Fi access stage, and start analyzing data (Porup, 2018).

4.2.4 How to Capture Data Packets with Wireshark

When you open Wireshark, a welcome screen shows the network connections that are available on your current computer. An EKG-style line graph which represents live traffic on that network is shown to the right of each.

To start capturing packets using Wireshark:

1. Go to the menu bar and select Capture to select one or more networks.

Tip: Hold Shift key to select multiple networks.

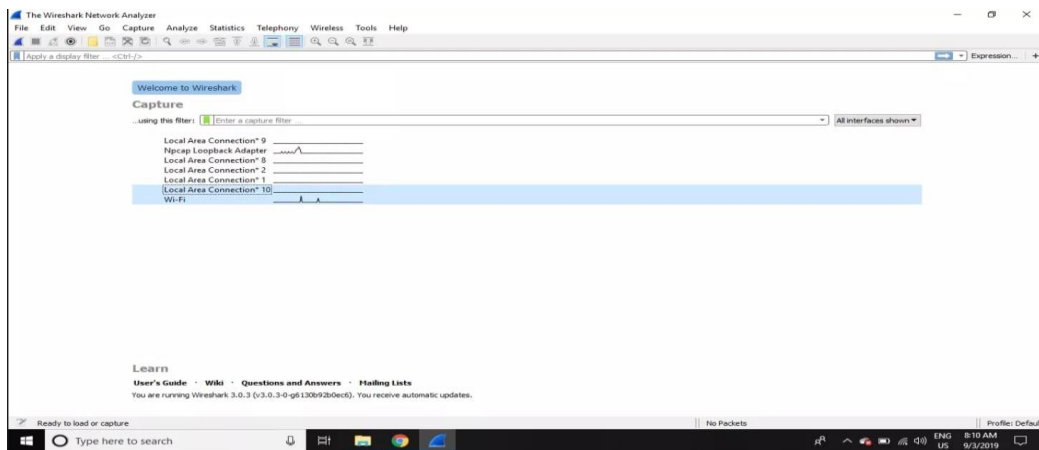


Figure 2: How to Capture Data Packets With Wireshark (Orgera, 2019)

2. Select Start in the Wireshark Capture Interfaces window.

Tip: There are other ways to get packet capture going. On the left side of the Wireshark toolbar, pick the shark fin, press Ctrl+E or double-click the network.

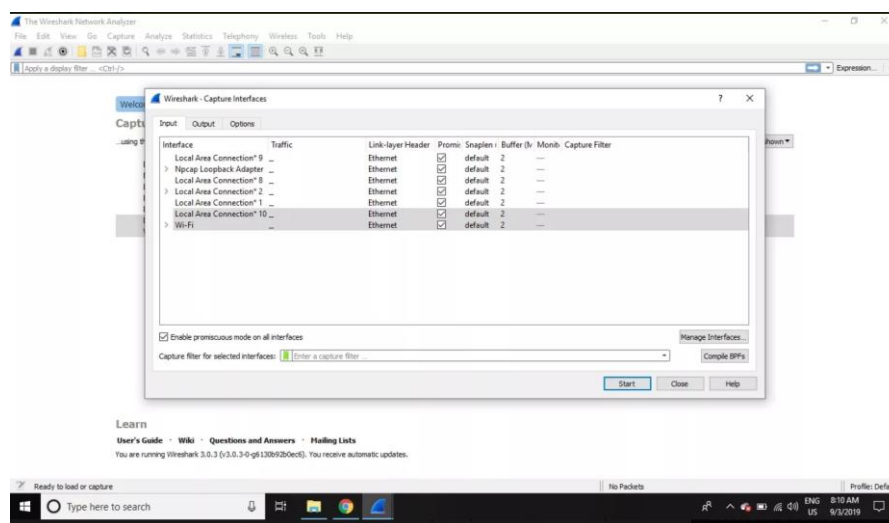


Figure 2.1: How to Capture Data Packets With Wireshark (Orgera, 2019)

3. Pick File > Save As, or pick an Export option for record capture.

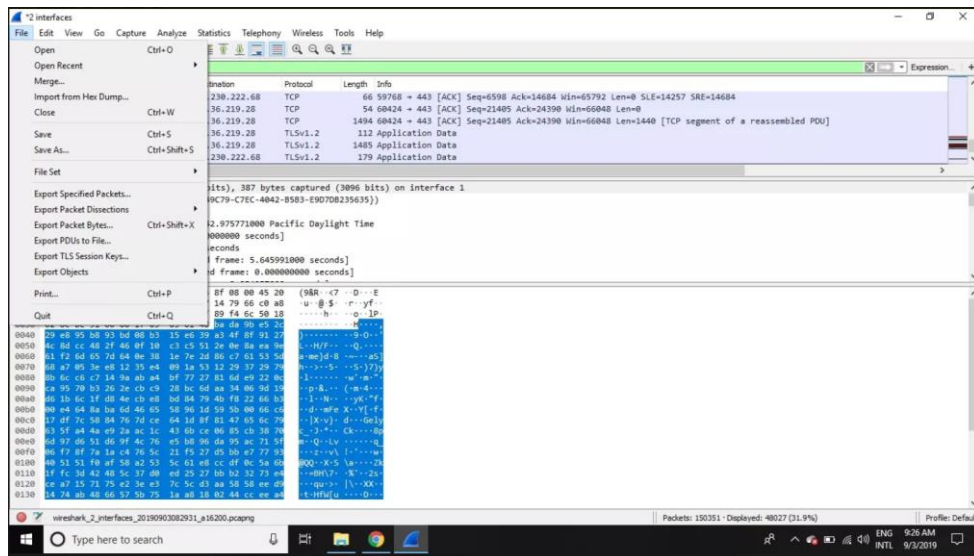


Figure 2.2: How to Capture Data Packets With Wireshark (Orgera, 2019)

4. Click Ctrl+E to stop recording. Alternatively, go to the Wireshark toolbar, and click the red Stop button next to the shark fin.

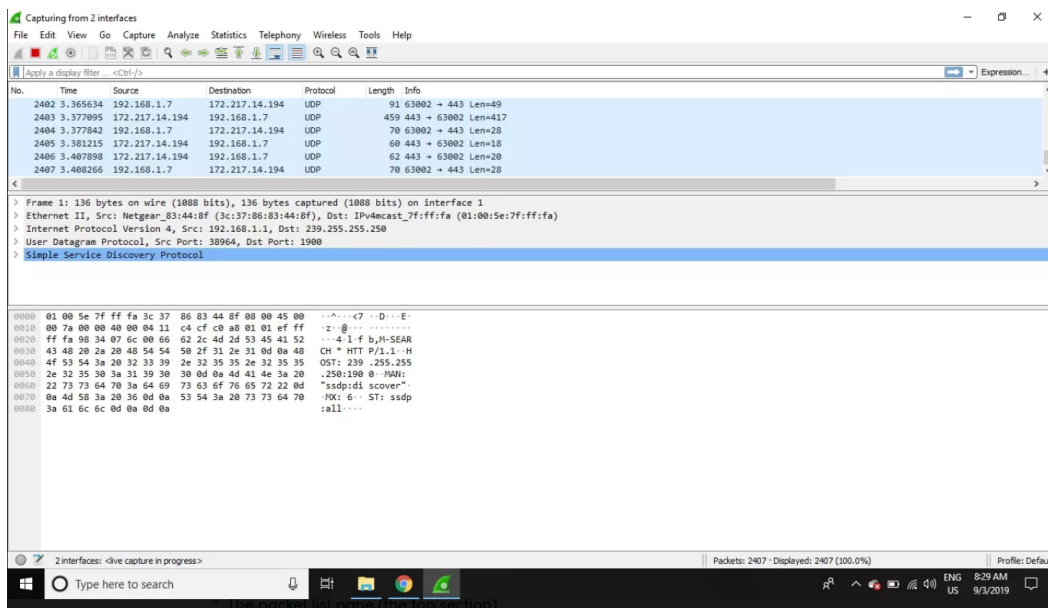


Figure 2.3: How to Capture Data Packets with Wireshark (Orgera, 2019)

How to View and Analyze Packet Contents

The application interface you recorded includes three major parts:

- The packet list pane
- The packet details pane
- The packet bytes pane

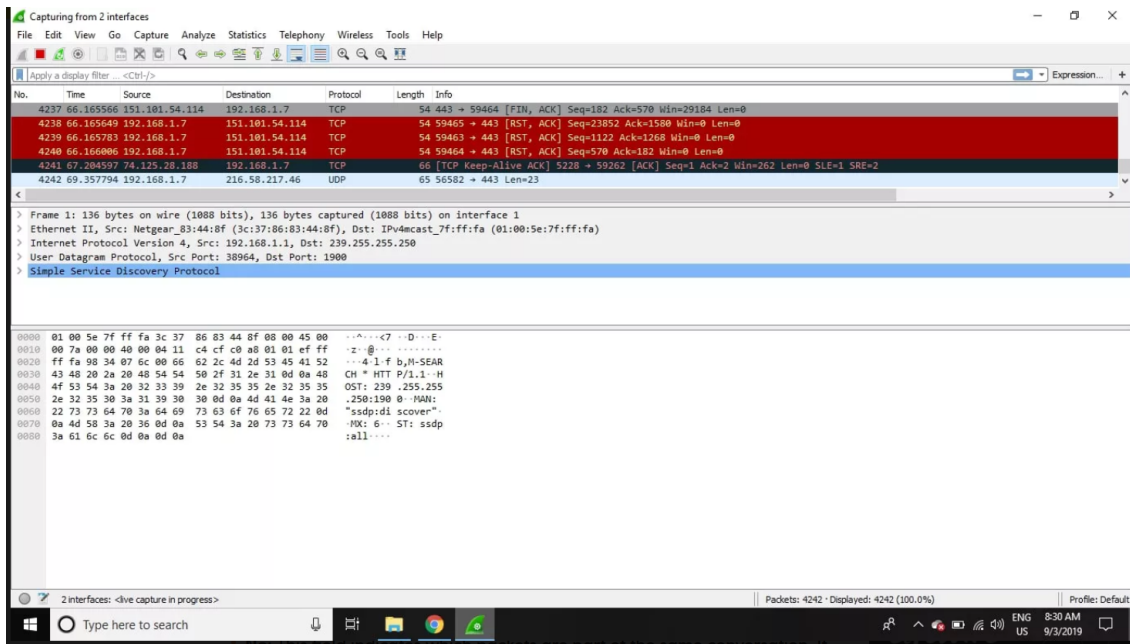


Figure 3: Packet list (Orgera, 2019)

Pick View > Time Display Format, to change the time mode to something more convenient such as the real time of day.

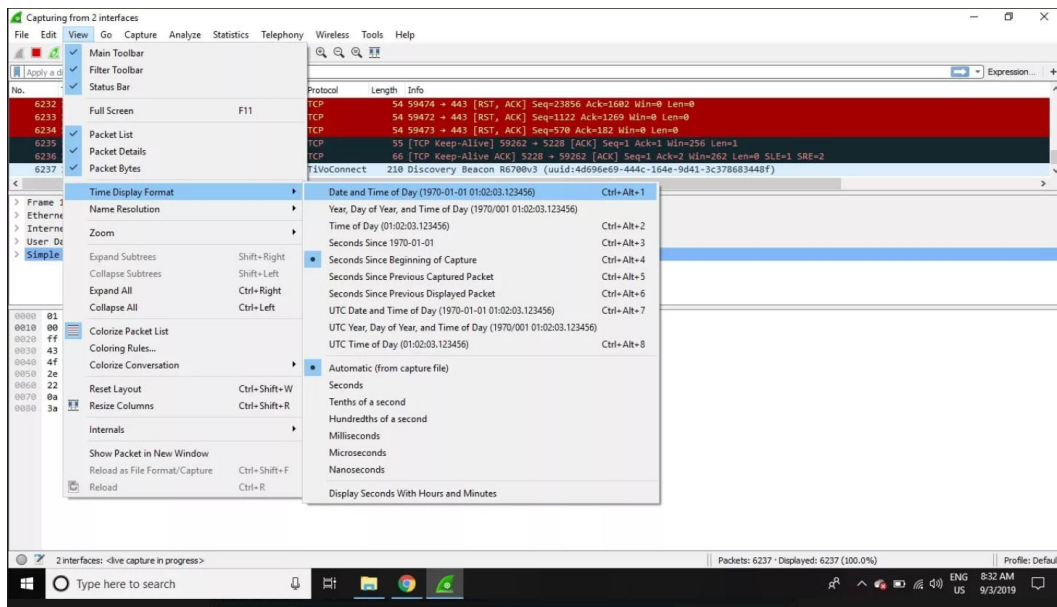


Figure 3.1: Packet (Orgera, 2019)

If you pick a packet in the top pane, you can find that one or more symbols appear in the column No. Open or closed brackets and a straight horizontal line signify that a packet or packet group is part of the same back-and-forth network communication. A split horizontal line means a packet doesn't become part of the discussion.

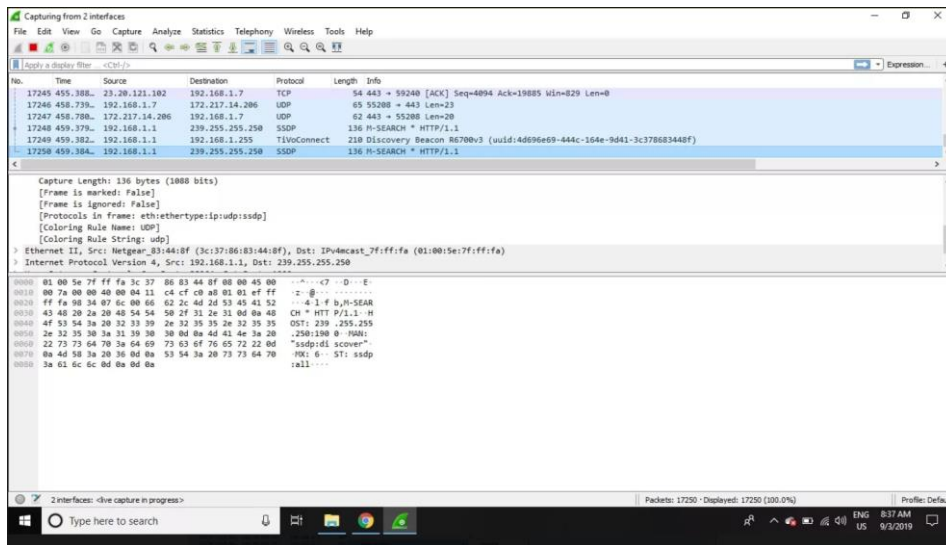


Figure 3.2: Packet details (Orgera, 2019)

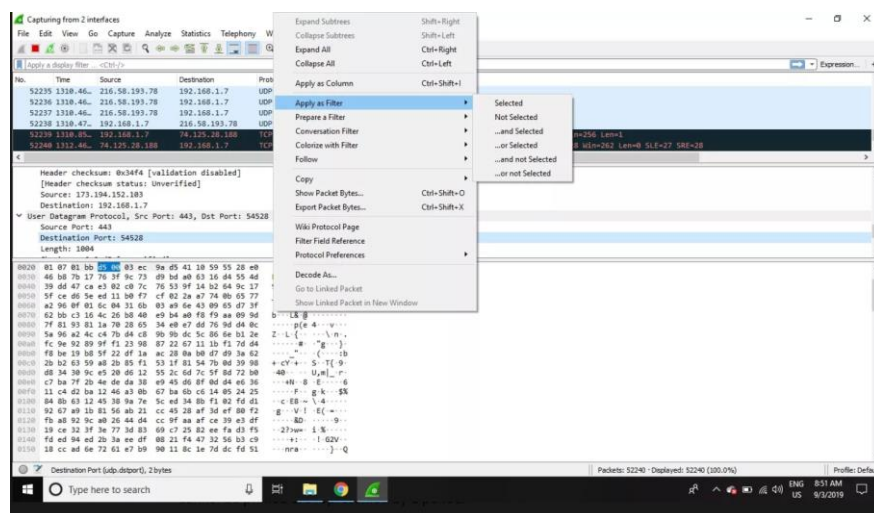


Figure 3.3: Packet bytes (Orgera, 2019)

At the bottom is the pane of packet bytes, which shows the chosen packet's raw data in a hexadecimal view. Alongside the data offset, this hex dump contains 16 hexadecimal bytes and 16 ASCII bytes. In the packet information pane, selecting a particular portion of this data immediately highlights the corresponding segment, and vice versa. Any bytes which are not printable are represented by a period.

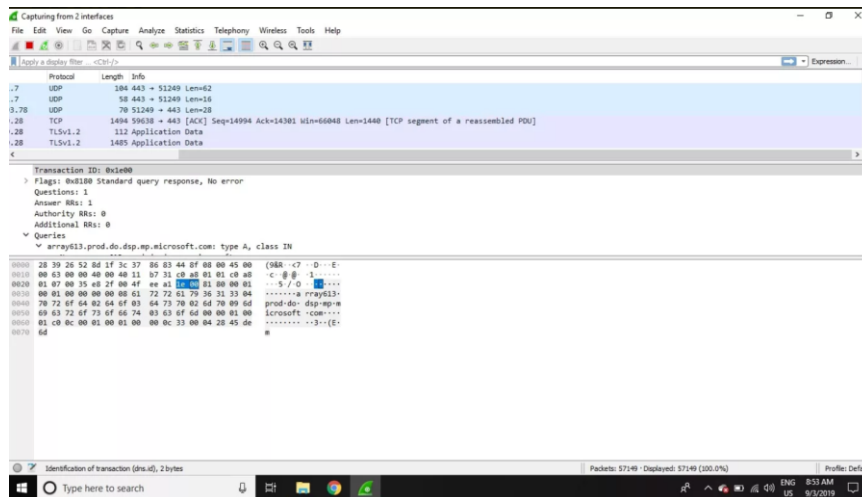


Figure 3.4: Packet bytes (Orgera, 2019)

To view this data in bit format as opposed to hexadecimal, right-click and pick as bits anywhere inside the window.

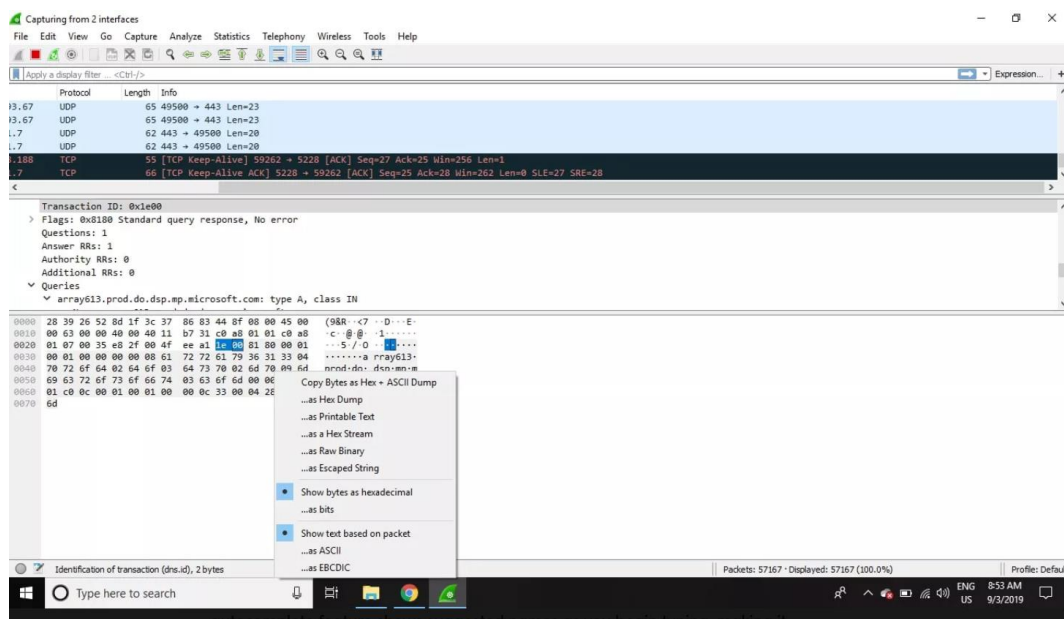


Figure 3.5: Packet bytes (Orgera, 2019)

4.2.5 How to Use Wireshark Filters

Capture filters inform Wireshark to capture only packets that meet specific criteria. Filters can also be added to a catch file that was generated to show only such packets. These are known as view filters. Wireshark offers by default a huge range of predefined filters. To use one of these existing filters, insert their name in the Apply a display filter entry field below the Wireshark toolbar or in the middle of the welcome screen in the Enter a capture filter. For instance, if you want to have TCP packets shown, type tcp. The Wireshark autocomplete function shows recommended names as you start typing, making it easy for the filter you are searching for to find the right name.

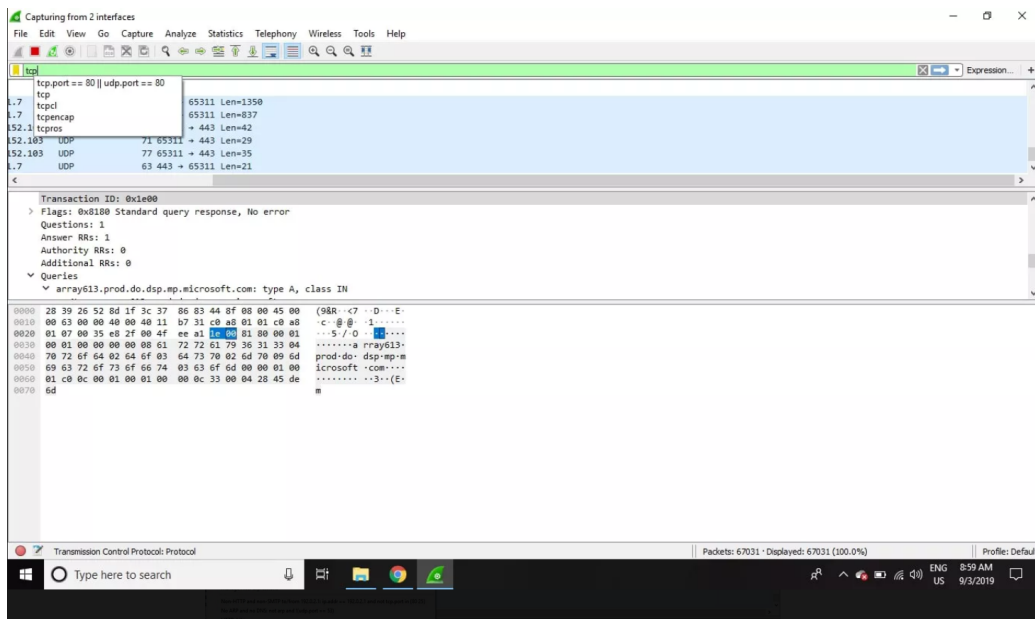


Figure 4: Wireshark Filters (Orgera, 2019)

Another way to pick a filter is to click the bookmark on the left side of the area of entry. To add, delete, or edit filters select **Manage Display Filters** or **Manage Filter Expressions**.

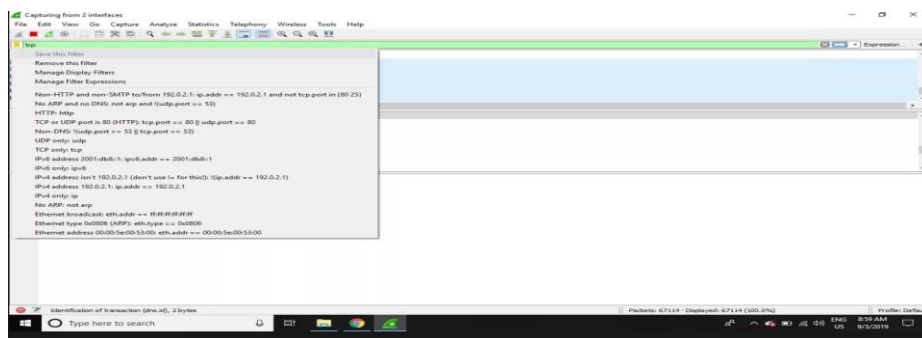


Figure 4.1: Wireshark Filters (Orgera, 2019)

To view a history drop-down chart, you can also use previously used filters by clicking the down arrow on the right side of the entry page.

4.2.6 Wireshark Color Rules

Although Wireshark's capture and display filters restrict the packets being recorded or shown on the screen, its colorization feature takes it a step further, it can differentiate between various types of packets based on their individual hue. This easily locates those packets in the packet list pane inside a saved collection by the color of their lines.

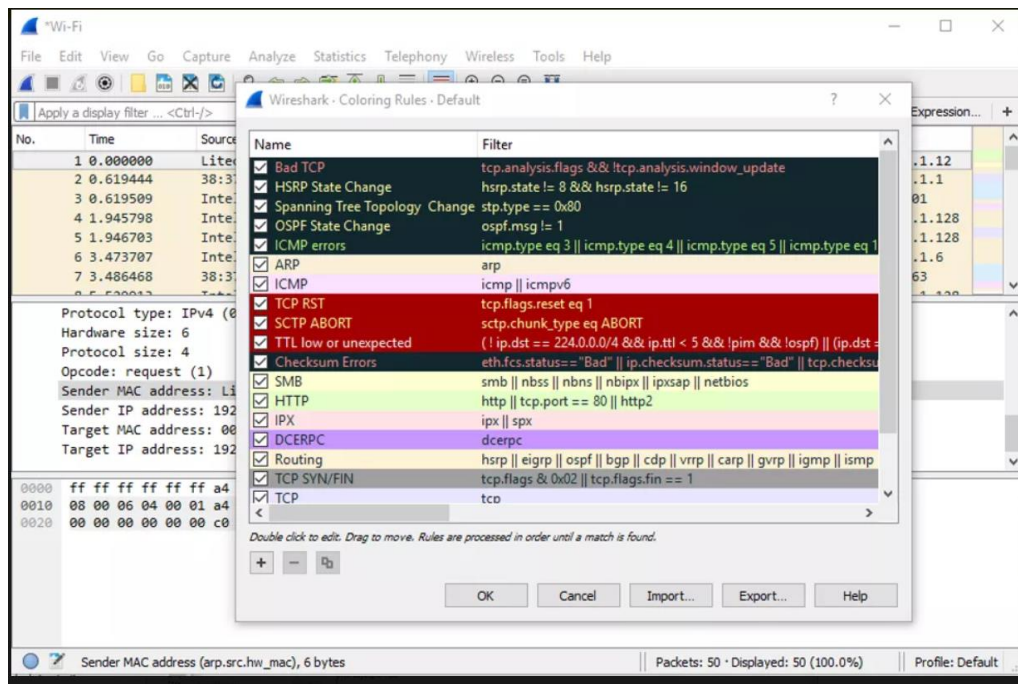


Figure 5: Wireshark Color Rules (Orgera, 2019)

Wireshark has about 20 coloring rules by default, each can be changed, disabled or removed. For an explanation of what each colour represents, click View > Colouring rules. You can also apply your own filters based on colour.

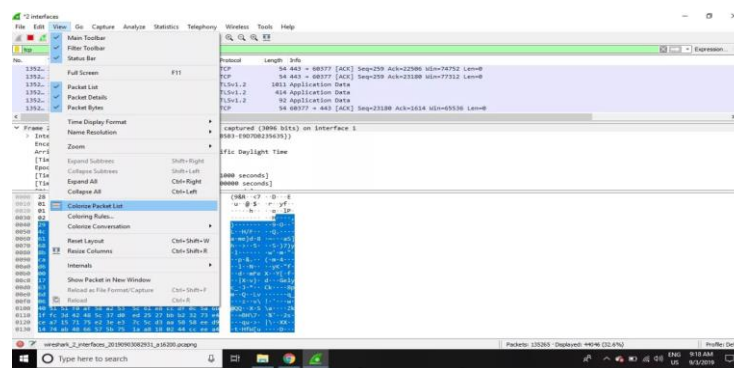


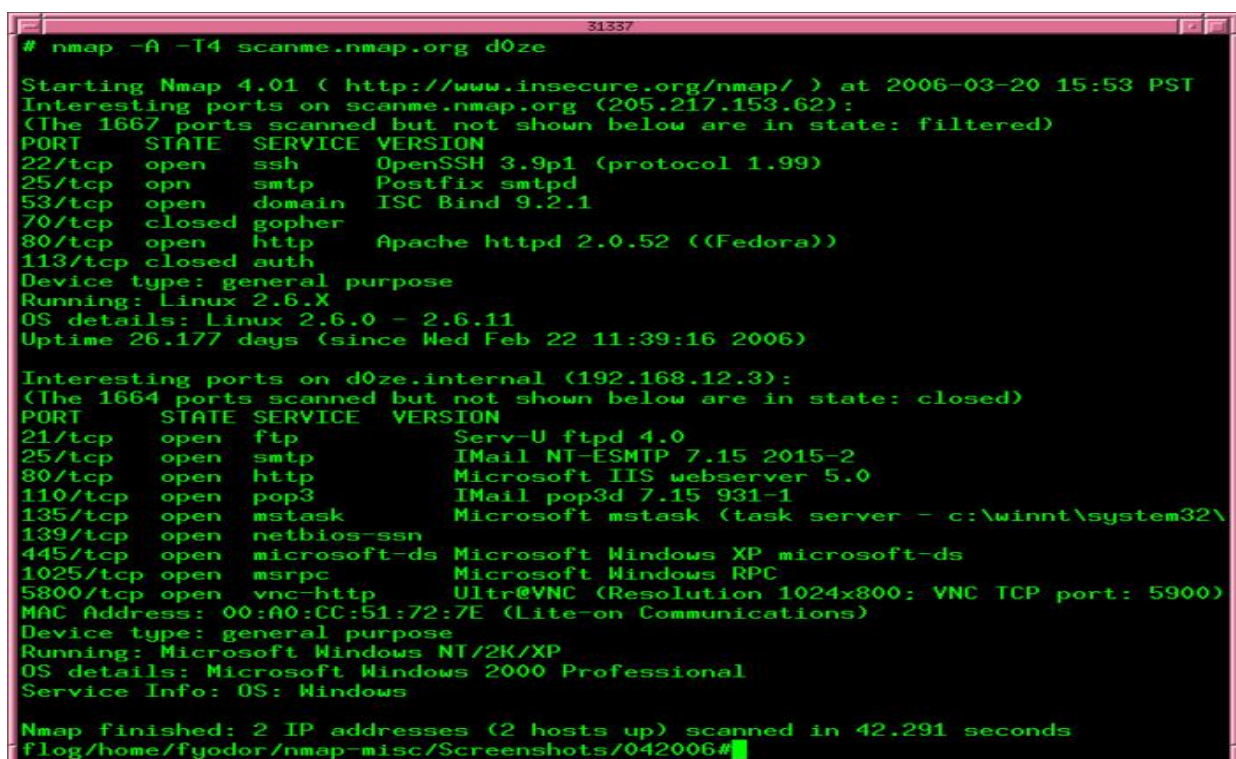
Figure 5.1: Wireshark Color Rules (Orgera, 2019)

4.3 Nmap

Nmap, stands for Network Mapper, it's a free, open-source tool for vulnerability scanning and network discovery. Nmap is used to identify what devices are running on the systems, finding hosts that are available and the vulnerabilities they have, finding open ports and detecting security risks.

Nmap can be used to monitor single hosts as well as various networks that involve many thousands of devices.

Nmap has changed over the time and is still very flexible, basically it's a port-scan tool, information gathering by sending raw packets to system ports. It verifies for responses and determines whether ports are open, closed or filtered in some way by, as an example, a firewall. Port scanning also have port discovery or enumeration.



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC Bind 9.2.1
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.0.52 ((Fedora))
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Serv-U ftpd 4.0
25/tcp    open  smtp     IMail NT-ESMTP 7.15 2015-2
80/tcp    open  http     Microsoft IIS webserver 5.0
110/tcp   open  pop3     IMail pop3d 7.15 931-1
135/tcp   open  mstask   Microsoft mstask (task server - c:\winnt\system32\
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp  open  msrpc    Microsoft Windows RPC
5800/tcp  open  vnc-http Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Nmap.org

4.3.1 History

Nmap was written in C++ and first introduced, with source code, in Phreak Magazine in September 1997. It's been extended with C, Perl and Python. Creator Gordon Lyon had adopted the pseudonym Fyodor Vaskevitch, which he picked up after reading Fyodor Dostoevsky's Notes from Underground, and still uses the handle Fyodor in his work on Nmap.

Over the years, Nmap has benefited from the contributions of a growing community of aficionados and developers, and it's now downloaded thousands of times a day. It has attained a grade of popularity in popular culture, becoming the go-to hacking tool featured in a dozen of movies.

The reason for Nmap's status is that it can be used on a variety of different operating systems. It runs macOS, Windows and supports Linux distributions including SUSE, Red Hat, kali, Mandrake and Fedora. It also runs on other OSes including BSD, Solaris, AIX and Amiga OS.

4.3.2 Why is Nmap important.

it's surprisingly efficient and is easy to install and to use. For example, you can use Nmap to profile your systems -- to get an idea what's running on them, what operating system they have installed, and what vulnerabilities they might have (when you're running services that you might not want to support). Though hackers use this tools to find facts in their missions -- putting out the network and looking for ways to attack the systems, it's normally used to get an up-to-date view of what systems might need to patch or protect, what services are running that might require users attention (or to be shut down). "fast scan" run on a single system. Note that the scan took .164 seconds. That certainly qualifies as fast. Another scan took a little longer but give few important clues.

4.3.3 Port scanning

The packets that Nmap sends out return with IP addresses and extra other data, allowing user to identify all types of network attributes, giving a profile or map of the network and allows to create a hardware and software list.

Various protocols use diverse types of packet structures. Nmap uses transport layer protocols including Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and SCTP (Stream Control Transmission Protocol), as well as supporting protocols like ICMP (Internet Control Message Protocol), used to send error messages.

The difference protocols serve various purposes and ports. For instance, the low resource overhead of UDP is appropriate for real-time streaming video, where you some packets are lost in coming back for speed.

Along with its many other features, Nmap fundamental port scanning and packet-capture capabilities are continuously being considered.

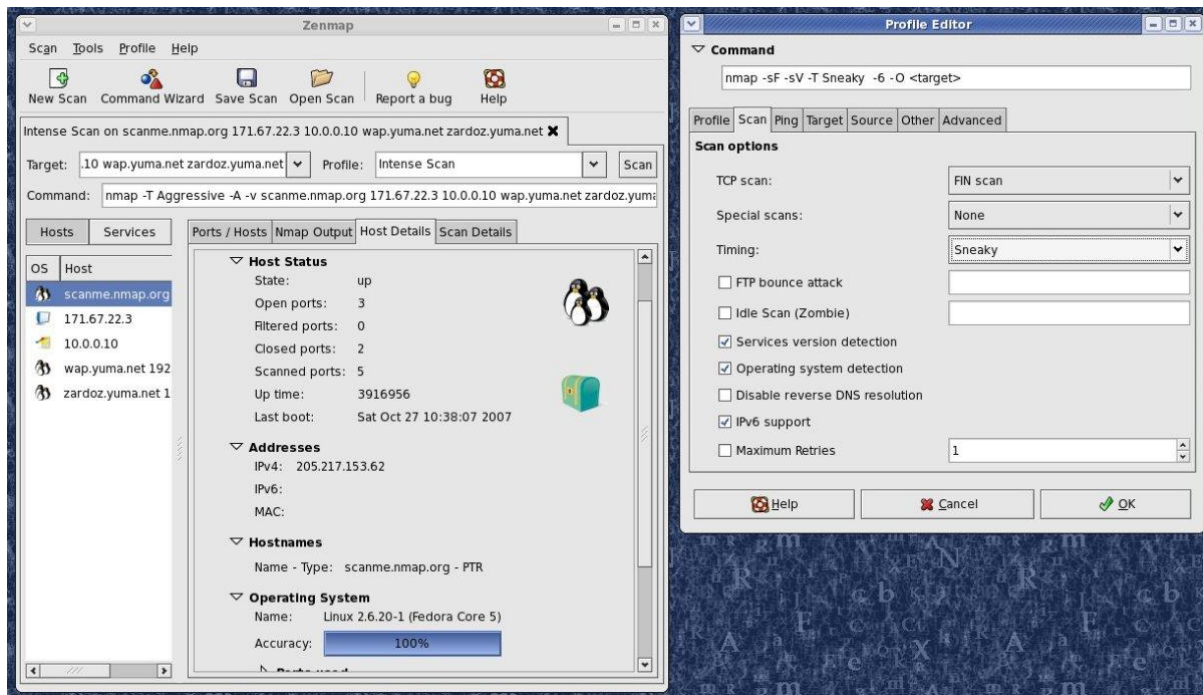
Focusing on Npcap packet capturing driver and library for Windows, it makes Nmap faster and more powerful on Windows and is now used by many other applications as well.

4.3.4 How to use Nmap

There is a good range of free network monitoring utilities also as free open-source vulnerability scanners available to network administrators and security auditors. What makes Nmap stand out because the tool IT and network managers got to know is its flexibility and power. While the idea of Nmap's functionality is port scanning, it allows for a spread of related capabilities including:

- Network mapping: Nmap can identify the devices on a network (also called host discovery), including servers, routers and switches, and the way they're physically connected.
- OS detection: Nmap can detect the operating systems running on network devices (also called OS fingerprinting), providing the seller name, the underlying OS , the version of the software and even an estimate of devices' uptime.

- Service discovery: Nmap can't only identify hosts on the network, but whether they're acting as mail, web or name servers, and therefore the particular applications and versions of the related software they're running.
- Security auditing: deciding what versions of operating systems and applications are running on network hosts lets network managers determine their vulnerability to specific flaws. If a network admin receives an alert a few vulnerabilities during a particular version of an application, for instance, she will scan her network to spot whether that software version is running on the network and take steps to patch or update the relevant hosts. Scripts also can automate tasks like detecting specific vulnerabilities.



NMap.org

Zen map is the graphical user interface for Nmap.

4.3.5 Commands for fine-tuning scans

One of the beauties of Nmap is that beginners with little system or network knowledge can start with simple commands for basic scanning, while professionals can cash in of more complex kinds of probes, which end in more fine-grained view of a network.

What you get once you use Nmap is actually an inventory of the targets you've scanned, alongside information related to those targets. the knowledge you receive depends on the type of scan you are doing – in other words, the commands you've used.

Depending on the command, scans don't necessarily generate tons of traffic and do not need to be very intrusive. Scanning all ports on all systems would be inefficient, primarily since only a fraction of obtainable ports are getting to be in use at anybody time (a system can have 65,535 TCP ports and 65,535 UDP ports). Different options leave finetuning or expanding scans. in commission version detection for instance, available options include:

- sV (enables version detection)

- `version-intensity` (sets scan intensity)
Intensity ranges between 0 and 9, and establishes the type of probes that you simply want to use. A lower-number intensity scan will look for common services, while a higher-number intensity scan can identify lesser-used services correctly but takes longer. Different commands also can, for instance, allow you to specify which ports or subnets to scan or skip.

Nmap includes a scripting engine using the Lua programming language to write down, save and share scripts that automate differing types of scans. Though they're frequently wont to check for well-known network infrastructure vulnerabilities, all kinds of tasks are often automated.

4.3.6 Zenmap, the Nmap GUI

Zenmap is that the Nmap security scanner graphical interface and provides for many options. It lets users do things like save scans and compare them, view topology maps, view displays of ports running on a number or all hosts on a network, and store scans during a searchable database.

5.0 Reference

Porup, J. M. (2018) What is Wireshark? What this essential troubleshooting tool does and how to use it [online] Available at: <https://www.csoononline.com/article/3305805/what-is-wireshark-what-this-essential-troubleshooting-tool-does-and-how-to-use-it.html> [Accessed 23 March 2020]

Orgera, S. (2019) How to Use Wireshark: A Complete Tutorial [online] Available at: <https://www.lifewire.com/wireshark-tutorial-4143298> [Accessed 23 March 2020]

WebTitan. 2018. *Most Common Wireless Network Attacks - Webtitan*. [online] Available at: <https://www.webtitan.com/blog/most-common-wireless-network-attacks/> [Accessed 24 March 2020].

Rapp, D., 2013. *Cracking WPA Using Fern Wifi Cracker*. [online] daleswifisec. Available at: <https://dalewifisec.wordpress.com/2013/07/02/cracking-wpa-using-fern-wifi-cracker/> [Accessed 24 March 2020].

Tools.kali.org. n.d. *Fern Wifi Cracker*. [online] Available at: <https://tools.kali.org/wireless-attacks/fern-wifi-cracker> [Accessed 24 March 2020].

Threatintelligence.com. n.d. *THREAT INTELLIGENCE / THE NEXT ERA IN SECURITY*. [online] Available at: <https://www.threatintelligence.com/> [Accessed 24 March 2020].

Pokorny, Z., 2019. *What Is Threat Intelligence? Definition And Examples*. [online] Recorded Future. Available at: <https://www.recordedfuture.com/threat-intelligence-definition/> [Accessed 24 March 2020].

Recorded Future. n.d. *Threat Intelligence: Everything You Need To Know | Recorded Future*. [online] Available at: <https://www.recordedfuture.com/threat-intelligence/> [Accessed 24 March 2020].

Evolve.threatintelligence.com. n.d. *Evolve Security Automation Overview | Evolve Security Automation*. [online] Available at: <https://evolve.threatintelligence.com/overview/> [Accessed 24 March 2020].

crowdstrike.com. 2019. *Threat Intelligence Guide | What Is Cyber Threat Intelligence?* [online] Available at: <https://www.crowdstrike.com/epp-101/threat-intelligence/> [Accessed 24 March 2020].

n.d. *Best Managed Security Services Providers*. [online] Available at: <https://www.g2.com/categories/managed-security-services> [Accessed 24 March 2020].

Rouse, M., n.d. *What Is Managed Security Service Provider (MSSP)? - Definition From Whatis.Com*. [online] SearchITChannel. Available at: <https://searchitchannel.techtarget.com/definition/MSSP> [Accessed 24 March 2020].

Gartner. n.d. *Managed Security Service Provider (Mssp)*. [online] Available at: <https://www.gartner.com/en/information-technology/glossary/mssp-managed-security-service-provider> [Accessed 24 March 2020].

Henry-Stocker, S., 2014. *Unix: Why You Should Love Nmap*. [online] Network World. Available at: <<https://www.networkworld.com/article/2695192/unix---why-you-should-love-nmap.html>> [Accessed 24 March 2020].

Rubens, P., 2015. *5 Key New Features In Nmap Network Security Tool*. [online] Esecurityplanet.com. Available at: <<https://www.esecurityplanet.com/network-security/5-key-new-features-in-nmap-network-security-tool.html>> [Accessed 24 March 2020].

Infosec Resources. 2019. *Nmap From Beginner To Advanced [Updated 2019]*. [online] Available at: <<https://resources.infosecinstitute.com/nmap/>> [Accessed 24 March 2020].

Marking Rubric

The assignment will be evaluated based on the following criteria:

Section 1: Research (PLO4 - Interpersonal Skills)

Marking Criteria	0-7 (Fail) (F)	8-9 (Marginal Fail) (D)	10-12 (Pass) (C- C C+)	13-14 (Credit) (B B+)	15-20 (Distinction) (A A+)	Marks Awarded
Report Format	Serious deficiencies in vocabulary & grammar, table of contents, page numbering, line spacing, consistent font	Noticeable deficiencies in vocabulary & grammar, table of contents, page numbering, line spacing, consistent font	Acceptable vocabulary & grammar, table of contents, page numbering, line spacing, consistent font	Few and minor deficiencies in vocabulary & grammar, table of contents, page numbering, line spacing, consistent font	Near perfect vocabulary & grammar, table of contents, page numbering, line spacing, consistent font	
Report Structure	Serious deficiencies in introduction & conclusion, diagram labelling, numbered section titles/subtitles, citations and references	Noticeable deficiencies in introduction & conclusion, diagram labelling, numbered section titles/subtitles, citations and references	Acceptable introduction & conclusion, diagram labelling, numbered section titles/subtitles, citations and references	Few and minor deficiencies in introduction & conclusion, diagram labelling, numbered section titles/subtitles, citations and references	Near perfect introduction & conclusion, diagram labelling, numbered section titles/subtitles, citations and references	
Quality of Research	Serious deficiencies in level of depth in the description of the topic and its importance	Noticeable deficiencies in level of depth in the description of the topic and its importance	Acceptable level of depth in the description of the topic in the context of security threats and countermeasures	Good level of depth in the description of the topic and current trends in security threats and countermeasures	Excellent in level of depth in the description of the topic and current trends in security threats and countermeasures	
Breadth and Selection of Sources	Serious deficiencies in the selection of sources and consideration of their credibility	Noticeable deficiencies in the selection of sources and consideration of their credibility	Acceptable level of breadth in the selection of sources and consideration of their credibility	Few and minor deficiencies in the selection of sources and consideration of their credibility	Excellent level of breadth in the selection of sources and consideration of their credibility	
Teamwork	No research progress report, Work Breakdown/ Peer Evaluation shows minimal effort to collaborate	Poor research progress report, Work Breakdown/ Peer Evaluation shows lack of engagement	Acceptable research progress report, Work Breakdown,/ Peer Evaluation shows division of tasks	Research progress report shows early engagement, Work Breakdown,/ Peer Evaluation shows collaborative effort	Research progress report shows substantial early progress, Work Breakdown,/ Peer Evaluation shows excellent collaborative effort	
Total Marks - Section 1						/ 100

Section 2: Tools Analysis with Demonstration

(PLO6 - Digital Skills)

Marking Criteria	0-7 (Fail) (F)	8-9 (Marginal Fail) (D)	10-12 (Pass) (C- C C+)	13-14 (Credit) (B B+)	15-20 (Distinction) (A A+)	Marks Awarded
Selection of Tool	Little or no evaluation provided to justify selection of the tool	Only general or superficial evaluation of alternative tools provided	Adequate justification for selecting the tool based on product reviews	Clear criteria used to justify selecting the tool based on comparison with others	Clear criteria used to justify selecting the tool based on analysis of objectives and alternatives	
Review of Features	Write-up shows no familiarity with accessing and using basic features of the tool	Write-up shows little familiarity with accessing and using basic features of the tool	Write-up shows good familiarity with accessing and using most features of the tool	Write-up shows investigation and experimentation with features of the tool	Write-up shows thorough investigation and experimentation with all features of the tool	
Technical Evaluation	Write-up shows little or no familiarity with techniques used in a simple tool	Write-up shows basic familiarity with techniques used in a simple tool	Write-up shows understanding of standard features and underlying techniques	Write-up includes selection of interesting features and underlying techniques	Write-up highlights unique features and underlying techniques	
Critical Evaluation	Little or no evaluation of the usefulness of the tool for meeting security objectives	General or superficial evaluation of the usefulness of the tool for meeting security objectives	Acceptable evaluation of the usefulness of the tool for meeting a specific security objective	Good evaluation of the strengths and weaknesses of the tool relative to specific security objectives	Thorough evaluation of the strengths and weaknesses of the tool relative to specific security objectives	
Presentation & Demo	Poor quality of visual aids / video, unable to explain and demonstrate accessing and using features of the tool	Marginal quality of visual aids / video, superficial or incomplete explanation and demonstration of accessing and using features of the tool	Acceptable quality of visual aids / video, able to explain and demonstrate accessing and using features of the tool	Creative use of visual aids / video, good explanation and demonstration of accessing and using features of the tool	Creative use of visual aids / video, in-depth explanation and demonstration of accessing and using features of the tool	
Total Marks - Section 2						/100

Total Marks Section 1 * 0.45	
Total Marks Section 2 * 0.55	
Final Mark	
Additional Comments :	